Tôhoku Math. J.
49 (1997), 203–215

ON THE IWASAWA INVARIANTS OF CERTAIN REAL ABELIAN FIELDS

HUMIO ICHIMURA* AND HIROKI SUMIDA

(Received November 7, 1995, revised February 20, 1996)

Abstract. For any totally real number field k and any prime number p, the Iwasawa lambda-invariant and the mu-invariant are conjectured to be both zero. We give a new efficient method to verify this conjecture for certain real abelian fields. The new features of our method compared with other existing ones are that we use effectively cyclotomic units and that we introduce a new way to apply p-adic L-functions to the conjecture.

1. Introduction. For a number field k and a prime number p, denote by $\lambda=\lambda_p(k)$ and $\mu=\mu_p(k)$ the Iwasawa λ-invariant and the μ-invariant associated to the ideal class group of the cyclotomic $\boldsymbol{Z}_p$-extension k_∞/k, respectively. For any totally real number field k and any p, it is conjectured that $\lambda_p(k)=\mu_p(k)=0$ (cf. Iwasawa [I3, p. 316], Greenberg [Gr]), which is often called Greenberg's conjecture. We already know that $\mu=0$ when k is abelian over $\boldsymbol{Q}$ (cf. Ferrero-Washington [FW]). When k is a real quadratic field, several authors have given some sufficient conditions for the conjecture to be true mainly in terms of units of the n-th layer k_n of the $\boldsymbol{Z}_p$-extension for some n (cf. [Ca], [Gr], [FK1], [FKW], [F1], [K], [FT], [T] and [FK2]). These conditions are roughly divided into two classes; the case $(\frac{k}{p})=1$ (cf., e.g. [FK1], [FT]), and the other case (cf., e.g. [FK2]). Calculating a system of fundamental units of k_0 or k_1 (cf., e.g. [FK1], [FT]) in the first case, or finding a "good" unit (in the sense of [FK2]) of k_n with $0\leq n\leq 3$ in the second case, they have shown that the conjecture is valid for many real quadratic fields with small discriminants and $p=3$. However, the conjecture is not yet settled, for example, when $k=\boldsymbol{Q}(\sqrt{254})$, $\boldsymbol{Q}(\sqrt{473})$ and $p=3$ (for which $(\frac{k}{p})=-1$). A reason for this is, as Takashi Fukuda kindly informed us, that one is required to have some information on the units of k_n with n at least 5(!) to apply the criterion of [FK2] to these fields.

The primary purpose of the present paper is to give a simple necessary and sufficient condition (Theorem, Corollary) for the conjecture when k is a real abelian field and $p>2$ for which p does not split in k and the couple (k, p) satisfies some further assumptions (C). It is given in terms of certain cyclotomic units and some polynomials related to a p-adic L-function. From our theorem, it is possible to derive criteria for the conjecture

* Partly supported by the Grants-in-Aid for Scientific Research, The Ministry of Education, Science and Culture, Japan.

1991 *Mathematics Subject Classification*. Primary 11R23.

involving only rational arithmetic (and no calculation of fundamental units) for several classes of real abelian fields. For example, we shall give such a criterion for certain real quadratic fields (Proposition 2). It is quite analogous to the classical one (cf. [W, Corollary 8.19]) for the Vandiver conjecture on p-divisibility of the class number of $\boldsymbol{Q}(\cos(2\pi/p))$, and is very suitable for computer calculation.

Let $k=\boldsymbol{Q}(\sqrt{m})$ be a real quadratic field with m square-free, and χ the associated primitive Dirichlet character. Denote by $\lambda_p^*(k)$ the λ-invariant of the power series associated the p-adic L-function $L_p(s, \chi)$. Then, we have an upper bound $\lambda_p(k) \leq \lambda_p^*(k)$ by the Iwasawa main conjecture proved by Mazur and Wiles [MW]. The assumptions (C) mentioned above are that p does not split in k (resp. $k(\sqrt{-3})$) when $p>3$ (resp. $p=3$) and that $\lambda_p^*(k)=1$ in the real quadratic case. These are satisfied when $p=3$ and $m=254$, 473. By using our criterion, we see by some computation that $\lambda_p(k)=0$ for $p=3$ (resp. 5, 7) and all $k=\boldsymbol{Q}(\sqrt{m})$ with $1<m<10^4$ (resp. 2×10^4, 3×10^4) satisfying the above conditions.

Recently, we have obtained a general criterion for the conjecture for real abelian fields without the assumptions (C). Since it is rather complicated, we confine ourselves in this paper to the simplest case (p does not split and $\lambda^*=1$) for giving a better illustration for our basic idea. The general case is dealt with in our subsequent paper.

Quite recently, Kraft and Schoof [KS] have given an effective method to check Greenberg's conjecture for real quadratic fields k with $(\frac{k}{p}) \neq 1$ and without the assumption $\lambda_p^*(k)=1$. The method is different from ours and is obtained from a different viewpoint. However, in practical computational application, both methods depend on some calculation of cyclotomic units modulo several prime ideals. A feature of ours compared with [KS] and other related works is that we have introduced a new way to apply p-adic L-functions to the conjecture. Actually, we use effectively a polynomial (see (1) in §2) defined for a zero of the power series associated to $L_p(s, \chi)$ and each $n \geq 0$.

This work is based upon our talk at the Number Theory Seminar, Komaba, Tokyo on January, 1995. We are grateful to the members of the seminar for providing us with warm atmosphere for investigating Greenberg's conjecture.

2. A Criterion for Greenberg's conjecture. Let p be a fixed odd prime number and χ a ($\bar{\boldsymbol{Q}}_p$-valued) nontrivial even primitive Dirichlet character. We impose five conditions (C1)–(C5) on the pair (p, χ). Let $k/\boldsymbol{Q}$ be the real abelian field associated to χ, and put $\Delta=\mathrm{Gal}(k/\boldsymbol{Q})$. Denote by χ_1 the odd primitive Dirichlet character corresponding to $\chi\omega^{-1}$, where ω is the Teichmüller character $\boldsymbol{Z}/p\boldsymbol{Z} \to \boldsymbol{Z}_p$. We first assume the following three conditions:

(C1) The exponent of Δ divides $p-1$.

(C2) There is only one prime ideal of k over p.

(C3) $\chi_1(p) \neq 1$.

We recall standard notation as follows: Let f be the conductor of χ and q the least common multiple of f and p. Let k_∞/k be the cyclotomic $\boldsymbol{Z}_p$-extension and k_n $(n\geq 0)$ its n-th layer. Let A_n be the Sylow p-subgroup of the ideal class group of k_n, and put $A_\infty=\text{proj lim}\,A_n$, where the projective limit is taken with respect to the relative norms. Let

$$e_\chi=\frac{1}{|\Delta|}\sum_{\sigma\in\Delta}\chi(\sigma)\sigma^{-1}$$

be the idempotent of the group ring $\bar{\boldsymbol{Q}}_p[\Delta]$ corresponding to χ. By (C1), this is an element of $\boldsymbol{Z}_p[\Delta]$. For a $\boldsymbol{Z}_p[\Delta]$-module M, denote the χ-component $e_\chi M$ by $M(\chi)$. Identifying the Galois group $\Gamma=\text{Gal}(k_\infty/k)$ with $\text{Gal}(k(\mu_{p^\infty})/k(\mu_p))$ in a natural way, we choose a topological generator γ of Γ so that $\zeta^\gamma=\zeta^{1+q}$ for all $\zeta\in\mu_{p^\infty}$. We identify, as usual, the completed group ring $\boldsymbol{Z}_p[[\Gamma]]$ with the power series ring $\Lambda=\boldsymbol{Z}_p[[T]]$ by $\gamma=1+T$. For a $\boldsymbol{Z}_p[\Delta][[\Gamma]]$-module M (for example, $M=A_\infty$), we regard $M(\chi)$ as a module over Λ by the above identification. By [I3, Theorem 8], $A_\infty(\chi)$ is finitely generated and torsion over Λ. Denote by λ_χ and μ_χ the λ-invariant and the μ-invariant, respectively, of the Λ-module $A_\infty(\chi)$.

Greenberg's conjecture for the pair (p, χ) is now stated as follows:

Conjecture (p, χ) $$\lambda_\chi=\mu_\chi=0\,.$$

As we mentioned in §1, we already know that $\mu_\chi=0$ (cf. [FW]). Because of the condition (C2), the above conjecture is valid when $A_0(\chi)=\{1\}$ (cf. [W, Proposition 13.22]). So, we further assume

(C4) $$A_0(\chi)\neq\{1\}$$

to exclude the trivial case.

To give our criterion, we need one more assumption and some notation related to the p-adic L-function $L_p(s, \chi)$ and cyclotomic units. By Iwasawa [I2], there exists a unique power series $g_\chi(T)$ in $\boldsymbol{Z}_p[[T]]$ such that

$$g_\chi((1+q)^{1-s}-1)=L_p(s,\chi)\,.$$

Denote by λ_χ^* and μ_χ^* the λ-invariant and the μ-invariant, respectively, of the power series g_χ. By [FW], we have $\mu_\chi^*=0$. By the Iwasawa main conjecture (proved by Mazur-Wiles [MW]), we have $\lambda_\chi\leq\lambda_\chi^*$. Therefore, to investigate Conjecture (p, χ), the case $\lambda_\chi^*=1$ is the first nontrivial case we have to consider. So, we finally assume that

(C5) $$\lambda_\chi^*=1\,.$$

By this assumption and $\mu_\chi^*=0$, we may uniquely write

$$g_\chi(T)=(T-\alpha)u(T)$$

for some $\alpha\in p\boldsymbol{Z}_p$ and a unit u of Λ. The Leopoldt conjecture for the pair (p, χ) (proved by Brumer [B]) asserts that $L_p(1, \chi)\neq 0$. Hence, we have $\alpha\neq 0$. Let p^e $(1\leq e<\infty)$ be the highest power of p dividing α. Put $\omega_n=\omega_n(T)=(1+T)^{p^n}-1$. The polynomials $X_n(T)$ ($\in \boldsymbol{Z}_p[T]$) and $Y_n(T)$ ($\in \boldsymbol{Z}[T]$) defined respectively by

$$(1)\qquad \begin{cases} \omega_n(T)=(T-\alpha)X_n(T)+\omega_n(\alpha) \\ Y_n(T)\equiv X_n(T) \bmod p^{n+e} \quad \text{and} \quad Y_n(T)\in \boldsymbol{Z}[T] \end{cases}$$

play a role in our paper. Let $e_{\chi,n}$ be an element of $\boldsymbol{Z}[\Delta]$ such that $e_{\chi,n}\equiv e_\chi \bmod p^{n+e}$ and the sum of the coefficients is zero. Define an element c_n of k_n by

$$(2)\qquad c_n=N_{\boldsymbol{Q}(\mu_{f_n})/k_n}(1-\zeta_{f_n})^{(r-1)e_{\chi,n}}\,.$$

Here, f_n is the conductor of k_n, ζ_{f_n} is a primitive f_n-th root of unity and r is the cardinality of the residue class field of the unique prime ideal of k over p. This element c_n is a unit of k_n (a cyclotomic unit) because the sum of the coefficients of $e_{\chi,n}$ is zero. Since $\boldsymbol{Z}[\Gamma]\supset \boldsymbol{Z}[T]$ by the identification $\gamma=1+T$, the polynomial $Y_n(T)$ can act on any element of the multiplicative group $k_n^\times$.

Now, our main result is stated as follows:

THEOREM. *Assume that the pair* (p,χ) *satisfies* (C1)–(C5). *Then,* $\lambda_\chi=0$ *if and only if the condition*

$$(\mathrm{H}_n)\qquad c_n^{Y_n(T)}\notin (k_n^\times)^{p^{n+e}}$$

holds for some $n\geq 0$.

From this theorem, we immediately obtain the following:

COROLLARY. *Under the assumptions of the Theorem, we have* $\lambda_\chi=0$ *if and only if*

$$c_n^{Y_n(T)} \bmod \mathfrak{l}\notin ((\boldsymbol{Z}/l\boldsymbol{Z})^\times)^{p^{n+e}}$$

for some $n\geq 0$ *and some prime ideal* $\mathfrak{l}$ *of* k_n *of degree one, where* $l=\mathfrak{l}\cap \boldsymbol{Q}$.

As we see in [I3], [Gr] and [FK2], Greenberg's conjecture is closely related to a capitulation problem in k_∞/k. The condition (H_n) is related to such a problem as follows: For each integer $n\geq 1$, put

$$h_n=|\operatorname{Ker}(A_0(\chi)\xrightarrow{i_n}A_n(\chi))|\,.$$

Here, i_n denotes the homomorphism induced from the inclusion $k_0\to k_n$.

PROPOSITION 1. *Assume that the pair* (p,χ) *satisfies* (C1)–(C5). *When* (H_0) *holds, we have* $h_1\neq 1$. *When* (H_0) *does not hold and* $n\geq 1$, *the condition* (H_n) *is equivalent to* $h_n\neq 1$.

REMARK 1. One can calculate the values λ_χ^*, e and $\alpha \bmod p^n$ by using the following approximation formula of Iwasawa [I2, §6]. Put $\dot{T}=(1+q)(1+T)^{-1}-1$ and $\dot{\omega}_n=\omega_n(\dot{T})$. For an integer a, denote by $\gamma_n(a)$ the integer satisfying

$$0 \leq \gamma_n(a) < p^n \quad \text{and} \quad \omega(a)(1+q)^{\gamma_n(a)} \equiv a \bmod p^{n+1} .$$

Then, we have

$$g_\chi(T) \equiv -\frac{1}{2qp^n} \sum_{a=1,(a,q)=1}^{qp^n} a\chi_1(a)(1+\dot{T})^{-\gamma_n(a)} \bmod \dot{\omega}_n .$$

Actually, several authors have already done such calculations in several cases. For examples, Iwasawa-Sims [IS], Buhler et al. [BCEM], Fukuda [F2], Wagstaff [Wa], Ernvall and Metsänkylä [EM].

REMARK 2. When $\lambda_\chi^* > 1$, Sumida [S] and Ozaki-Taya [OT] recently began investigation on the conjecture using not only some data on the units of k_n for some n but those on the distinguished polynomial associated to the power series g_χ.

REMARK 3. Strengthening extensively the technique of this paper, we shall give a general criterion for the conjecture for (p, χ) without the assumptions (C2)–(C5) in our subsequent paper.

3. Real quadratic case. We begin with the following lemma. Let (p, χ) be as in §2. Put $x_n = c_n^{Y_n(T)}$ for brevity.

LEMMA 1. *For any* $\sigma \in \mathrm{Gal}(k_\infty/\boldsymbol{Q})$, *we have* $x_n^\sigma \equiv x_n^u \bmod (k_n^\times)^{p^{n+e}}$ *for some* $u \in \boldsymbol{Z}_p^\times$.

PROOF. Since $\mathrm{Gal}(k_\infty/\boldsymbol{Q}) = \Delta \times \Gamma$, it suffices to deal with the case $\sigma \in \Delta$ or $\sigma = \gamma$. When $\sigma \in \Delta$, we see from the definition (2) of c_n that $x_n^\sigma \equiv x_n^{\chi(\sigma)} \bmod (k_n^\times)^{p^{n+e}}$. Assume $\sigma = \gamma$. Then, by (1) and $p^{n+e} | \omega_n(\alpha)$, we have

$$\gamma Y_n(T) = (1+T) Y_n(T) \equiv (1+\alpha) Y_n(T) + \omega_n(T) \bmod p^{n+e} .$$

Hence, $x_n^\gamma \equiv x_n^{1+\alpha} \bmod (k_n^\times)^{p^{n+e}}$. ■

Let k be a real quadratic field and χ the associated primitive Dirichlet character. We assume that the pair (p, χ) satisfies (C1)–(C5). First, we translate the condition (H_n) into a condition which involves only rational arithmetic and hence is very suitable for computer calculation. Next, we deal with some numerical examples when $p = 3$, 5 or 7.

We write

$$Y_n(T) = \sum_{j=0}^{p^n - 1} a_j (1+T)^j = \sum_{j=0}^{p^n - 1} a_j \gamma^j , \qquad a_j \in \boldsymbol{Z} .$$

The integers a_j are defined modulo p^{n+e}. Denote by σ the canonical isomorphism

$$\sigma : (\boldsymbol{Z}/f_n\boldsymbol{Z})^\times \simeq \mathrm{Gal}(\boldsymbol{Q}(\mu_{f_n})/\boldsymbol{Q}) , \quad \bar{a} \mapsto \sigma_a .$$

Let $\mathfrak{A}_n$ be the subgroup of $(\boldsymbol{Z}/f_n\boldsymbol{Z})^\times$ corresponding to $\mathrm{Gal}(\boldsymbol{Q}(\mu_{f_n})/k_n)$ under this isomorphism. Choose and fix an integer d with $(d, f_n) = 1$ such that $\sigma_d|_{\boldsymbol{Q}_n} = \mathrm{id}$ but

$\sigma_d|_k \neq \mathrm{id}$, $\boldsymbol{Q}_n$ being the n-th layer of the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$. The number r in the definition (2) of c_n is p^z with $z=2$ or 1 according as $p\nmid f$ or $p|f$. Then, we have

$$(3)\qquad x_n = c_n^{Y_n(T)} = N_{\boldsymbol{Q}(\mu_{f_n})/k_n}(1-\zeta_{f_n})^{(1-\sigma_d)Y_n(T)(p^z-1)/2}$$
$$= \left\{ \prod_{j,a} (1-\zeta_{f_n}^{a(1+q)^j})^{a_j} \Big/ \prod_{j,a} (1-\zeta_{f_n}^{ad(1+q)^j})^{a_j} \right\}^{(p^z-1)/2} .$$

Here, j runs over all integers with $0 \leq j < p^n$, and a runs over a complete set of representatives of $\mathfrak{A}_n$. For an integer n (≥ 0) and a prime number l with $l \equiv 1 \bmod f_n$, choose an integer s satisfying

$$(4)\qquad s \bmod l \text{ is of order } f_n \text{ in } (\boldsymbol{Z}/l\boldsymbol{Z})^\times .$$

For an integer x, denote by $\langle x \rangle_n$ the unique integer satisfying

$$\langle x \rangle_n \equiv x \bmod f_n , \qquad 0 \leq \langle x \rangle_n < f_n .$$

We put

$$c(n, l, s) = \left\{ \prod_{j,a} (1-s^{\langle a(1+q)^j \rangle_n})^{a_j} \Big/ \prod_{j,a} (1-s^{\langle ad(1+q)^j \rangle_n})^{a_j} \right\}^{(p^z-1)/2} .$$

As is easily seen, the rational number $c(n, l, s)$ is relatively prime to l. Because of (4) and $l \equiv 1 \bmod f_n$, there exists a prime ideal $\mathfrak{L}$ of $\boldsymbol{Q}(\mu_{f_n})$ over l of degree one such that $s \equiv \zeta_{f_n} \bmod \mathfrak{L}$, where ζ_{f_n} is the primitive f_n-th root of unity which appeared in (3). Then, we see from (3) that

$$x_n \equiv c(n, l, s) \bmod \mathfrak{l} = \mathfrak{L} \cap k_n$$

and that for each a with $(a, f_n) = 1$,

$$x_n^{\sigma_a} \equiv c(n, l, s^{\langle a \rangle_n}) \bmod \mathfrak{l} .$$

Therefore, by using Lemma 1, we observe that for each (n, l), the condition

$$c(n, l, s) \bmod l \notin ((\boldsymbol{Z}/l\boldsymbol{Z})^\times)^{p^{n+e}}$$

holds for some s satisfying (4) if and only if it holds for all such s. Then, we denote by $(\mathrm{H}'_{n,l})$ the above equivalent conditions. We put $f' = f$ or f/p according as $p \nmid f$ or $p|f$. Then, $(f', p) = 1$.

LEMMA 2. *$x_n \notin (k_n^\times)^{p^{n+e}}$ if and only if $x_n \notin (\boldsymbol{Q}(\mu_{f'p^{n+e}})^\times)^{p^{n+e}}$.*

PROOF. Put $K = \boldsymbol{Q}(\mu_{f'p^{n+e}})$ for brevity. It suffices to prove that $x_n \in (k_n^\times)^{p^{n+e}}$ if $x_n \in (K^\times)^{p^{n+e}}$. Assume that $x_n = y^{p^{n+e}}$ for some $y \in K$. Then, we have $y^{\sigma-1} \in \mu_{p^{n+e}}$ for any $\sigma \in \mathrm{Gal}(K/k_n)$. Let J be the non-trivial automorphism of K over the maximal real subfield K^+. We easily see that $x_n^2 = (y^{1+J})^{p^{n+e}}$ and that for any $\sigma \in \mathrm{Gal}(K/k_n)$

$$(y^{1+J})^{\sigma-1} \in K^+ \cap \mu_{p^{n+e}} = \{1\} .$$

Therefore, we must have $x_n \in (k_n^\times)^{p^{n+e}}$. ■

From all the above and the Chebotarev density theorem, we obtain the following:

PROPOSITION 2. *Let the notation be as above. For each integer $n \geq 0$, the condition* (H_n) *holds if and only if* $(\mathrm{H}'_{n,l})$ *holds for some prime number l with $l \equiv 1 \bmod f'p^{n+e}$.*

REMARK 4. Put $p^g = |A_0(\chi)|$. We see in §5 that $g \leq e$ and that (H_0) is equivalent to $g < e$ (Lemma 7).

Now, let us deal with some numerical examples. Let $p = 3$, 5 or 7 and m a positive square-free integer such that the real quadratic field $k = k(m) = \boldsymbol{Q}(\sqrt{m})$ satisfies (C1)–(C5). When $p = 3$, there are 133 (resp. 45) such k with $m \equiv 2 \bmod 3$ (resp. $m \equiv 0 \bmod 3$) in the range $0 < m < 10^4$, including $\boldsymbol{Q}(\sqrt{254})$ and $\boldsymbol{Q}(\sqrt{473})$. When $p = 5$ (resp. $p = 7$), there are 128 (resp. 86) such k in the range $0 < m < 2 \times 10^4$ (resp. $0 < m < 3 \times 10^4$).

Assume that $p = 3$ and $m = 254$ (resp. 473). Then, we have $g = e = 1$ and $\alpha \equiv 75$ (resp. 30) $\bmod 3^6$. Some computation shows that the condition $(\mathrm{H}'_{5,l})$ is satisfied with $l = 5925313$ (resp. 2068903). Hence, we get $\lambda_3 = \lambda_3(k(m)) = 0$ for $m = 254$ (resp. 473) by the Theorem and Proposition 2.

In a similar way, we observe that $\lambda_p(k) = 0$ for $p = 3$ (resp. 5, 7) and all the above $178 = 133 + 45$ (resp. 128, 86) real quadratic fields k. Tables 1 through 4 list up m corresponding to these k. Table 1 (resp. Table 2) is for $p = 3$ and m with $m \equiv 2 \bmod 3$ (resp. $m \equiv 0 \bmod 3$). Table 3 (resp. Table 4) is for $p = 5$ (resp. $p = 7$). In Table 1, those

TABLE 1. $p = 3$, $m \equiv 2 \bmod 3$.

	m										
$n_0 = 0$	257	326	359	506	842	1223	1367	1478	2495	2711	2726
	∘3137	3419	3941	3962	4283	4493	5303	5327	5369	5477	5741
	5903	6026	6209	6557	7415	7745	8399	8438	8543	8735	8909
	8930	9281	9749								
$n_0 = 1$	659	761	839	1091	1229	1373	1523	1787	1847	1907	2207
	2213	2459	2543	2993	3035	3062	3221	3281	3602	∘3719	4106
	4193	4649	4670	4706	4886	4934	4994	5099	5102	5261	5333
	5621	5738	6053	6311	6623	6686	6782	∘6809	7058	∘7226	7259
	7262	7319	7673	7721	7994	8051	8255	8267	8426	8447	8519
	8597	9149	9215	9218	9278	9293	9413	9419	9467	9551	9902
$n_0 = 2$	443	4238	4481	4511	4907	7643	7709	7883	8363	8837	
$n_0 = 3$	785	899	2429	2510	3158	3569	4286	7598	7601	8282	9995
$n_0 = 4$	2666	3047	5081	5297	7658	9590					
$n_0 = 5$	*254	*473	*1646	*6806							

Table 2. $p=3$, $m\equiv 0 \bmod 3$.

	m										
$n_0=0$	993	1866	2055	3981	5178	5511	5853	6681	6834	8130	9795
$n_0=1$	786	894	1101	1191	1929	2118	2298	2505	2703	3054	3261
	3873	4755	5637	5799	6807	7374	7473	7743	8373	9219	
$n_0=2$	1758	3594	4098	4215	5619	5898	6366	8418	9507		
$n_0=3$											
$n_0=4$	3846										
$n_0=5$	6798	7671									
$n_0=6$	∘9606										

Table 3. $p=5$.

	m										
$n_0=0$	982	3253	5615	5630	6563	6945	7282	7513	10438	11273	11342
	11818	12993	14163	14745	15887	16015	19078	19477			
$n_0=1$	727	1093	1327	2027	2335	2362	2602	2878	3238	3722	3967
	3970	4358	4555	4622	4757	4843	4865	4867	5107	5185	5777
	5927	6078	6085	6087	6113	6157	6395	7570	7705	7817	8023
	8707	8803	9235	9322	9410	9553	9670	9722	9742	9757	9803
	9847	9895	10067	10398	10567	10613	10678	10795	11215	11665	11722
	11937	12247	12322	12542	13015	13102	13133	13227	13235	13427	13693
	13742	13865	14398	15117	15127	15257	16118	16243	16257	16813	16957
	17737	17742	18195	18235	18237	18433	18497	18770	18803	19135	19317
	19543										
$n_0=2$	817	3585	3782	3997	6202	11095	12545	13763	15133	15473	15862
	16987	18215	18355	18370	19067						
$n_0=3$	3598	16637	18773								
$n_0=4$	2153										

m with $*$-mark are the ones for which $\lambda_3(k)=0$ is not proved by the previous investigations (cf. [Ca], [Gr], [FK2], [OT]). In the other cases, only few examples with $\lambda_p(k)=0$ are known by the previous investigations. Further, in the tables, $g=2$ for those m with $\circ$-mark, and $g=1$ for the others.

In view of Proposition 1, the smallest integer $n_0=n_0(m)$ for which $k(m)=\boldsymbol{Q}(\sqrt{m})$ satisfies (H_{n_0}) or $(\mathrm{H}'_{n_0,l})$ for some l is of interest. Though our method is not efficient at

TABLE 4. $p=7$.

	m										
$n_0=0$	2467	3811	4378	7510	9049	12977	16217	19081	20221	21581	26851
	27215	27937	28411	28426							
$n_0=1$	577	1294	1601	2026	4702	5039	5417	5626	5743	5827	5974
	6097	6151	8097	8587	9029	9289	9505	9539	10202	11021	11023
	11031	11035	11053	11794	12089	12655	13054	14122	14201	14395	15277
	16127	16471	16534	16901	17023	17162	18494	18949	19599	19614	19787
	20614	21223	21446	21994	22102	22417	22897	23413	23702	23974	24359
	24526	27667	28369	28609	28902	29203	29753	29785	29851		
$n_0=2$	15882	17335	17569	22921	29470						
$n_0=3$	14721										
$n_0=4$	2029										

calculating n_0, we can obtain an upper bound for n_0. Let a be an integer with $a \geq 2$. In Table 1 and Table 2 (resp. Table 3, Table 4), for each m in the row "$n_0=a$", we have checked that $k(m)$ satisfies $(\mathrm{H}'_{a,l})$ for some l of the first 5 (resp. 4, 3) prime numbers l with $l \equiv 1 \bmod f'p^{a+e}$ and that it does not satisfy $(\mathrm{H}'_{a-1,l})$ for all the first 20 (resp. 15, 10) prime numbers l with $l \equiv 1 \bmod f'p^{a+e-1}$. So, we have $n_0(m) \leq a$, but it is only plausible that $n_0(m)=a$. For those m in the row "$n_0=0$" (resp. "$n_0=1$"), we have checked, with the help of Remark 4, that $n_0(m)=0$ (resp. $n_0(m)=1$).

REMARK 5. There are some mistakes in Table 5.2 of [KS], for example, their data for $m=254$, 473. We are informed that they will correct them in their subsequent paper.

4. Proof of Theorem.

4-1. Preliminaries. Let (p, χ) be as in §2. We assume that it satisfies (C1)–(C5), and we use the same notation as in §2. From (C1) and (C2), there exists a unique prime ideal $\mathfrak{p}_n$ of k_n over p. Let $F_n(\subset \bar{\boldsymbol{Q}}_p)$ be the completion of k_n at $\mathfrak{p}_n$, and put $F_\infty = \bigcup F_n$. We always regard k_n to be embedded in F_n. The Galois groups Δ and Γ are identified, respectively, with $\mathrm{Gal}(F_0/\boldsymbol{Q}_p)$ and $\mathrm{Gal}(F_\infty/F_0)$ in an obvious way. Let E_n be the group of units of k_n and C_n the group of cyclotomic units of k_n in the sense of Hasse [H] and Gillard [Gil, §2-3]. Then, the unit c_n defined in §2 is an element of C_n. Let $\mathscr{U}_n$ be the group of principal units of F_n, and let $\mathscr{E}_n$ and $\mathscr{C}_n$ be the closures of $E'_n = E_n \cap \mathscr{U}_n$ and $C_n \cap \mathscr{U}_n$ in $\mathscr{U}_n$, respectively. Since the completed group ring $\boldsymbol{Z}_p[\Delta][[\Gamma]]$ acts on the groups $\mathscr{U}_n$, $\mathscr{E}_n$ and $\mathscr{C}_n$ naturally, we may regard the χ-components $\mathscr{U}_n(\chi)$, $\mathscr{E}_n(\chi)$ and $\mathscr{C}_n(\chi)$ as modules over Λ. Put

$$c'_n = N_{\boldsymbol{Q}(\mu_{fn})/k_n}(1-\zeta_{fn})^{(r-1)e_\chi}(\in \mathscr{C}_n(\chi)) .$$

We need the following fact due to Iwasawa [I1] and [Gi2].

LEMMA 3. (1) (cf. [Gi2, Theorem 2]) *We have isomorphisms over* Λ:

$$\begin{array}{ccl} \mathcal{U}_n(\chi) & \simeq & \Lambda/(\omega_n) \\ \cup & & \cup \\ \mathcal{C}_n(\chi) & \simeq & (g_\chi, \omega_n)/(\omega_n) = (T-\alpha, \omega_n)/(\omega_n)\,. \end{array}$$

(2) (cf. [Gi2, §4-2]) *The cyclic* Λ*-module* $\mathcal{C}_n(\chi)$ *is generated by* c'_n.

For this lemma, we need the assumptions (C2) and (C3). By the Leopoldt conjecture for (k_n, p) (proved by [B]), we have:

LEMMA 4 (cf. [W, §5-5]). *The inclusion* $E'_n \to \mathcal{E}_n$ *induces an isomorphism*

$$E'_n/E'^{p^{n+e}}_n \simeq \mathcal{E}_n/\mathcal{E}^{p^{n+e}}_n\,.$$

We also need the following:

LEMMA 5. *Under the above setting, we have* $\lambda_\chi = 0$ *if and only if* $\mathcal{U}_n(\chi) \supsetneqq \mathcal{E}_n(\chi)$ *for some* $n \geq 0$.

Though this assertion is more or less known, we give its proof for the sake of completeness in §5.

4-2. Proof of Theorem. First, we have to prove:

LEMMA 6. $(c'_n)^{X_n(T)}$ *is an element of* $\mathcal{U}_n(\chi)^{p^{n+e}}$, *and* $((c'_n)^{X_n(T)})^{1/p^{n+e}} (\in \mathcal{U}_n(\chi))$ *is a generator of* $\mathcal{U}_n(\chi)$ *over* Λ.

PROOF. Let $\boldsymbol{v}_n$ be any generator of $\mathcal{U}_n(\chi)$ over Λ. By Lemma 3(1), $\boldsymbol{v}_n^{T-\alpha}$ is a generator of $\mathcal{C}_n(\chi)$ over Λ. By Lemma 3(2), c'_n also is a generator of $\mathcal{C}_n(\chi)$. Therefore, we have

$$\boldsymbol{v}_n^{T-\alpha} = (c'_n)^f \quad \text{and} \quad c'_n = \boldsymbol{v}_n^{(T-\alpha)g}$$

for some $f(T)$, $g(T) \in \Lambda$. Then, since $\boldsymbol{v}_n^{(T-\alpha)fg} = \boldsymbol{v}_n^{T-\alpha}$, we obtain

$$(T-\alpha)fg \equiv T-\alpha \bmod \omega_n\,.$$

Since $\alpha \neq 0$ (see §2), we see from this that $f(0)g(0)=1$, and hence f is a unit of Λ. Put $\boldsymbol{u}_n = \boldsymbol{v}_n^{f^{-1}}$. Then, $\boldsymbol{u}_n$ generates $\mathcal{U}_n(\chi)$ over Λ and $\boldsymbol{u}_n^{T-\alpha} = c'_n$. Further, we have by the definition (1) of $X_n(T)$

$$\boldsymbol{u}_n^{-\omega_n(\alpha)} = \boldsymbol{u}_n^{\omega_n(T)-\omega_n(\alpha)} = \boldsymbol{u}_n^{(T-\alpha)X_n(T)} = (c'_n)^{X_n(T)}\,.$$

From this and $p^{n+e} \| \omega_n(\alpha)$, we obtain the assertion. ∎

Now, let us prove the Theorem. Let n (≥ 0) be any integer. By Lemma 6, we have $\mathcal{U}_n(\chi) = \mathcal{E}_n(\chi)$ if and only if $((c'_n)^{X_n(T)})^{1/p^{n+e}} \in \mathcal{E}_n(\chi)$, or equivalently if and only if $(c'_n)^{X_n(T)} \in \mathcal{E}_n(\chi)^{p^{n+e}}$. However, by the isomorphism in Lemma 4, the class $[c_n^{Y_n(T)}]$ is mapped to the class $[(c_n')^{X_n(T)}]$. It follows from this that $\mathscr{U}_n(\chi)=\mathscr{E}_n(\chi)$ if and only if $c_n^{Y_n(T)} \in E_n^{p^{n+e}}$. Then, we obtain our Theorem from Lemma 5. ■

5. Proof of Proposition 1. In this section, we prove Lemma 5 and Proposition 1. Let (p, χ) be as before. We assume that it satisfies (C1)–(C5), and use the same notation as in the preceding sections. Let M be the maximal pro-p abelian extension over k_∞ unramified outside p, and L the maximal unramified pro-p abelian extension over k_∞. The Galois groups $\mathrm{Gal}(M/k_\infty)$, $\mathrm{Gal}(M/L)$ and $\mathrm{Gal}(L/k_\infty)$ are considered as modules over $\boldsymbol{Z}_p[\Delta][[\Gamma]]$ in a natural way. By the assumptions (C1), (C2) and the Iwasawa main conjecture, we have the following isomorphism over Λ:

$$(5) \qquad Y=\mathrm{Gal}(M/k_\infty)(\chi)\simeq \boldsymbol{Z}_p[[T]]/(T-\alpha)\,(\simeq \boldsymbol{Z}_p)\,.$$

Let M_n (resp. L_n) be the maximal abelian extension over k_n contained in M (resp. L). Then, by class field theory, we have (cf. [Co, Theorem 1])

$$(6) \qquad \mathrm{Gal}(M_n/L_n)(\chi)\simeq(\mathscr{U}_n/\mathscr{E}_n)(\chi)\,,\quad I=\mathrm{Gal}(M/L)(\chi)\simeq \mathrm{proj}\lim(\mathscr{U}_n/\mathscr{E}_n)(\chi)\,.$$

Here, the projective limit is taken with respect to the relative norms.

Proof of Lemma 5. By (5), we have $\lambda_\chi=0$ if and only if the inertia group I is nontrivial. However, we see from (6) that I is nontrivial if and only if $\mathscr{U}_n(\chi)\supsetneqq\mathscr{E}_n(\chi)$ for some n since the norm map $\mathscr{U}_{m+1}(\chi)\to\mathscr{U}_m(\chi)$ is surjective. ■

Let $M(\chi)$ be the intermediate field of M/k_∞ fixed by $\mathrm{Gal}(M/k_\infty)(\psi)$ for all ($\bar{\boldsymbol{Q}}_p$-valued) characters ψ of Δ with $\psi\neq\chi$. We put

$$M_n(\chi)=M_n\cap M(\chi)\,,\quad L_n(\chi)=L_n\cap M(\chi)\,.$$

Then, we have

$$(7) \qquad \mathrm{Gal}(M_n(\chi)/k_\infty)\simeq \boldsymbol{Z}_p[[T]]/(T-\alpha,\,\omega_n)\simeq \boldsymbol{Z}/p^{n+e}\boldsymbol{Z}\,.$$

Put $p^g=|A_0(\chi)|$. Since $L_0(\chi)\subseteq M_0(\chi)$, we see that $A_0(\chi)\simeq\boldsymbol{Z}/p^g\boldsymbol{Z}$ and $g\leq e$. As we have seen at the end of §4-2, the condition (H_n) is equivalent to $\mathscr{U}_n(\chi)\supsetneqq\mathscr{E}_n(\chi)$. From this, we easily see that if (H_n) holds for some n, then so does (H_m) for any $m\geq n$. We put

$$n_0=\min\{n\,|\,(\mathrm{H}_n)\text{ holds}\}=\min\{n\,|\,\mathscr{U}_n(\chi)\supsetneqq\mathscr{E}_n(\chi)\}\,.$$

Then, $0\leq n_0\leq\infty$. From (6) and (7), we easily get:

Lemma 7. *We have $n_0=0$ if and only if $g<e$.*

Proposition 1 is an immediate consequence of the following:

Proposition 3. *According as $n_0=0$ or $1\leq n_0\leq\infty$, we have*

$$h_n=\begin{cases} p^n & n\le g \\ p^g & n\ge g \end{cases} \quad \textit{or} \quad h_n=\begin{cases} 1 & n\le n_0-1 \\ p^{n-n_0+1} & n_0-1\le n\le n_0+e-1 \\ p^g=p^e & n\ge n_0+e-1\,. \end{cases}$$

In what follows, we identify by (5) the Galois group Y with the additive group $\boldsymbol{Z}_p$ on which $T=\gamma-1$ acts via multiplication by α. To prove the above proposition, we need the following:

LEMMA 8. *$I=p^g\boldsymbol{Z}_p$ or $p^{n_0+e-1}\boldsymbol{Z}_p$ according as $n_0=0$ or $1\le n_0\le\infty$. Here, $p^\infty\boldsymbol{Z}_p$ means $\{0\}$.*

PROOF. Assume that $1\le n_0<\infty$ (hence, $g=e$ by Lemma 7). By the definition of n_0 and (6), we have

$$M_{n_0-1}(\chi)=L_{n_0-1}(\chi) \quad \text{but} \quad M_{n_0}(\chi)\supsetneqq L_{n_0}(\chi)\,.$$

Then, we get $I=p^{n_0+e-1}\boldsymbol{Z}_p$ because of $Y=\boldsymbol{Z}_p$ and (7). The assertion for the other cases is proved in a similar way. ■

PROOF OF PROPOSITION 3. By [I3, Theorem 8], we have the following commutative diagram:

$$\begin{array}{ccc} A_0(\chi) & \xrightarrow{i_n} & A_n(\chi) \\ \wr\| & & \wr\| \\ Y/(I+\omega_0 Y) & \xrightarrow{\times v_n} & Y/(I+\omega_n Y)\,. \end{array}$$

Here, $v_n=\omega_n(T)/\omega_0(T)$ and $\times v_n$ denotes the map

$$y\,\mathrm{mod}(I+\omega_0 Y)\to v_n y\,\mathrm{mod}(I+\omega_n Y)\,.$$

Since $v_n y=v_n(\alpha)y$ by (5), we easily obtain our assertion from the diagram, (5) and Lemma 8. ■

REFERENCES

[B] A. BRUMER, On the units of algebraic number fields, Mathematika 14 (1967), 121–124.

[BCEM] J. P. BUHLER, R. E. CRANDALL, R. ERNVALL AND T. METSÄNKYLÄ, Irregular primes and cyclotomic invariants to four million, Math. Comp. 61 (1993), 151–153.

[Ca] A. CANDIOTTI, Computations of Iwasawa invariants and K_2, Compositio Math. 29 (1974), 89–111.

[Co] J. COATES, p-adic L-functions and Iwasawa's theory, Algebraic Number Fields (Durham Symposium; ed. by A. Fröhlich), Academic Press, London (1975), 269–353.

[EM] R. ERNVALL AND T. METSÄNKYLÄ, Computation of the zeros of p-adic L-functions, Math. Comp. 58 (1992), 815–830.

[F1] T. FUKUDA, Iwasawa's λ-invariants of certain real quadratic fields, Proc. Japan Acad. Ser. A 65 (1989), 260–262.

[F2] T. FUKUDA, Iwasawa λ-invariants of imaginary quadratic fields, J. College Industrial Technology

Nihon Univ. (Corrigendum: to appear, ibid.) 27 (1994), 35–88.

[FK1] T. Fukuda and K. Komatsu, On $\boldsymbol{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan 38 (1986), 95–102.

[FK2] T. Fukuda and K. Komatsu, A capitulation problem and Greenberg's conjecture of real quadratic fields, Math. Comp. 65 (1996), 313–318.

[FKW] T. Fukuda, K. Komatsu and H. Wada, A remark on the λ-invariant of real quadratic fields, Proc. Japan Acad. Ser. A 62 (1986), 318–319.

[FT] T. Fukuda and H. Taya, The Iwasawa λ-invariants of $\boldsymbol{Z}_p$-extensions of real quadratic fields, Acta Arith. 69 (1995), 277–292.

[FW] B. Ferrero and L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. 109 (1979), 377–395.

[Gi1] R. Gillard, Remarques sur les unités cyclotomiques et unités elliptiques, J. Number Theory 11 (1979), 21–48.

[Gi2] R. Gillard, Unités cyclotomiques, unités semi locales et $\boldsymbol{Z}_l$-extensions II, Ann. Inst. Fourier 29 (1979), 1–15.

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

[H] H. Hasse, Über die Klassenzahl Abelescher Zahlkörper, Akademie Verlag, Berlin (1952).

[I1] K. Iwasawa, On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan 16 (1964), 42–82.

[I2] K. Iwasawa, Lectures on p-adic L-functions, Ann. of Math. Stud. no. 74, Princeton Univ. Press, Princeton, N.J. (1972).

[I3] K. Iwasawa, On $\boldsymbol{Z}_l$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246–326.

[IS] K. Iwasawa and C. Sims, Computation of invariants in the theory of cyclotomic fields, J. Math. Soc. Japan 18 (1966), 86–96.

[K] J. S. Kraft, Iwasawa invariants of CM fields, J. Number Theory 32 (1989), 65–77.

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

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\boldsymbol{Q}$, Invent. Math. 76 (1984), 179–330.

[OT] M. Ozaki and H. Taya, A note on Greenberg's conjecture of real abelian number fields, Manuscripta Math. 88 (1995), 311–320.

[S] H. Sumida, Greenberg's conjecture and the Iwasawa polynomial, to appear in J. Math. Soc. Japan.

[T] H. Taya, On the Iwasawa λ-invariants of real quadratic fields, Tokyo J. Math. 16 (1993), 121–130.

[Wa] S. S. Wagstaff, Jr., Zeros of p-adic L-functions, II, Number Theory Related to Fermat's Last Theorem (Cambridge, Mass., 1981), Progr. Math. vol. 26, Birkhäuser, Boston, Mass., (1982), 297–308.

[W] L. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Math. no. 83, Springer, New York (1982).

Department of Mathematics
Yokohama City University
22–2 Seto, Kanazawa-ku
Yokohama, 236
Japan

Faculty of Integrated Arts and Sciences
Hiroshima University
Higashi-Hiroshima, 739
Japan