A Note on the Iwasawa λ -Invariants of Real Abelian Number Fields

Manabu OZAKI[†] and Hisao TAYA^{‡*}

[†]*Department of Information and Computer Science, Waseda University,
Okubo, Tokyo 169-8555, Japan*

[‡]*Graduate School of Information Sciences, Tohoku University,
Katahira, Sendai 980-8577, Japan*

Received December 17, 1997; final version accepted August 28, 1998

Let k be a real abelian number field with Galois group Δ and p an odd prime number. Assume that the order of Δ is not divisible by p . Let Ψ be an irreducible $\mathbf{Q}_p$ -character of Δ . Denote by $\lambda_p(\Psi)$ the Ψ -component of the λ -invariant associated to the cyclotomic $\mathbf{Z}_p$ -extension of k . Then Greenberg conjecture for the Ψ -components states that $\lambda_p(\Psi)$ is always zero for any Ψ and p . Although some efficient criteria for the conjecture to be true are given, very little is known about it except for $k = \mathbf{Q}$ or the trivial character case.

There is another λ -invariant. Denote by $\lambda_p^*(\Psi)$ the λ -invariant associated to the p -adic L -function related to Ψ . One can know $\lambda_p^*(\Psi)$ by computing the Iwasawa power series attached to Ψ . The Iwasawa main conjecture proved by Mazur and Wiles says that the inequality $\lambda_p(\Psi) \leq \lambda_p^*(\Psi)$ holds. In this paper, we give a necessary and sufficient condition for this inequality to be strict in terms of special values of p -adic L -functions. This result enables us to obtain a criterion for Greenberg's conjecture for Ψ -components to be true when the corresponding Iwasawa power series is irreducible.

KEYWORDS: Iwasawa invariants, p -adic L -functions, Galois groups, real abelian fields

0 Introduction

Let p be an odd prime number. As usual, we denote by $\mathbf{Z}_p$ the ring of p -adic integers, by $\mathbf{Q}_p$ the field of p -adic numbers, and by $\mathbf{Q}$ the field of rational numbers. For a group G , $\#G$ denotes the order of G if G is finite, and $\#G = \infty$ means that G is infinite.

Let k be a real abelian number field with Galois group Δ . For the cyclotomic $\mathbf{Z}_p$ -extension k_∞ of k with Galois group Γ , we denote by k_n the n -th layer of k_∞ over k , by L_n (resp. L_∞) the maximal unramified abelian pro- p -extension of k_n (resp. k_∞), and by M_n (resp. M_∞) the maximal abelian pro- p -extension of k_n (resp. k_∞) which is unramified outside the primes above p . Then $L_\infty = \bigcup_{n \geq 0} L_n$, $M_\infty = \bigcup_{n \geq 0} M_n$, and $\Delta \times \Gamma$ acts on the Galois groups $\text{Gal}(L_\infty/k_\infty)$ and $\text{Gal}(M_\infty/k_\infty)$ by conjugation in a natural way.

From now on, we assume the the order of Δ is not divisible by p . Let Ψ be a $\mathbf{Q}_p$ -valued character of Δ defined and irreducible over $\mathbf{Q}_p$. Such a Ψ is called an irreducible $\mathbf{Q}_p$ -character of Δ . For each such Ψ , let us put

$$e_\Psi = \frac{1}{\#\Delta} \sum_{\delta \in \Delta} \Psi(\delta) \delta^{-1}.$$

By the assumption on the order of Δ , e_Ψ is an idempotent of the group ring $\mathbf{Z}_p[\Delta]$. For any $\mathbf{Z}_p[\Delta]$ -module X , we put $X^\Psi = e_\Psi X$, which is called the Ψ -component of X . Then $X = \bigoplus_\Psi X^\Psi$ where Ψ runs over all irreducible $\mathbf{Q}_p$ -characters of Δ . Let ψ be an irreducible component of Ψ over the algebraic closure $\bar{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. Note that ψ is also considered a primitive p -adic Dirichlet character. We denote by O_ψ the ring generated over $\mathbf{Z}_p$ by the values of ψ , and by K_ψ the field generated over $\mathbf{Q}_p$ by the values of ψ . Then O_ψ and K_ψ are uniquely determined, independent of the choice of ψ , and also $e_\Psi \mathbf{Z}_p[\Delta] \simeq O_\psi$ by the correspondence $e_\Psi \delta \leftrightarrow \psi(\delta)$, $\delta \in \Delta$, for a fixed ψ . Thus, for any $\mathbf{Z}_p[\Delta][[\Gamma]]$ -module X , X^Ψ becomes an $O_\psi[[\Gamma]]$ -module. Let γ be a fixed topological generator of Γ . We identify the completed group ring $O_\psi[[\Gamma]]$ with the power series ring $\Lambda_\psi = O_\psi[[T]]$, as usual, by the correspondence $\gamma \leftrightarrow 1 + T$. Hence, for any $\mathbf{Z}_p[\Delta][[\Gamma]]$ -module X (e.g., $\text{Gal}(L_\infty/k_\infty)$ or $\text{Gal}(M_\infty/k_\infty)$), X^Ψ is considered a Λ_ψ -module.

As is well-known, both $\text{Gal}(L_\infty/k_\infty)^\Psi$ and $\text{Gal}(M_\infty/k_\infty)^\Psi$ are finitely generated torsion Λ_ψ -modules (cf. [Gr2], [Iw2] or [Wa]). For any finitely generated torsion Λ_ψ -module X , we denote by $\text{char}_{\Lambda_\psi}(X)$ the characteristic ideal of X in Λ_ψ . Let $f_\psi(T)$ be a generator of $\text{char}_{\Lambda_\psi}(\text{Gal}(L_\infty/k_\infty)^\Psi)$. By the p -adic Weierstrass preparation theorem (cf. [Wa, Theorem 7.3]) and the Ferrero-Washington theorem [FW], we may write $f_\psi(T)$ uniquely in the following form:

* This research partially supported by the Grant-in-Aid for Encouragement of Young Scientists, The Ministry of Education, Science, Sports and Culture, Japan.

$$f_\Psi(T) = P_\Psi(T)u_\Psi(T),$$

where $P_\Psi(T)$ is a distinguished polynomial in Λ_Ψ and $u_\Psi(T)$ is a unit power series in Λ_Ψ . Recall that a distinguished polynomial in Λ_Ψ is one whose leading coefficient is 1 and whose remaining coefficients are all divisible by a uniformizer of O_Ψ . Now, we denote by $\lambda_p(\Psi)$ the degree of $P_\Psi(T)$, which we call the Ψ -component of the λ -invariant $\lambda_p(k)$ associated to k_∞/k (this is called the χ -part of $\lambda_p(k)$ in our previous paper [OT], χ being a p -adic Dirichlet character of Δ). Note that $\lambda_p(k) = \sum_\Psi d_\Psi \lambda_p(\Psi)$, where Ψ runs over all irreducible $\mathbf{Q}_p$ -characters of Δ and d_Ψ is the degree of K_Ψ over $\mathbf{Q}_p$. This $\lambda_p(\Psi)$ is a λ -invariant associated to an algebraic object, namely, the Ψ -component of the ideal class group of the cyclotomic $\mathbf{Z}_p$ -extension of k . As we know below, there is another λ -invariant, which is associated to an analytic object, namely, the p -adic L -function related to Ψ .

Let ζ_{p^n} be a primitive p^n -th root of unity and let κ be the p -adic unit in $\mathbf{Z}_p$ satisfying $\zeta_{p^n}^\kappa = \zeta_{p^n}^{\tilde{\gamma}}$ for all integers $n \geq 1$, where $\tilde{\gamma}$ is the element of $\text{Gal}(k_\infty(\zeta_p)/k(\zeta_p))$ satisfying $\tilde{\gamma}|_{k_\infty} = \gamma$. We regard ψ as a primitive p -adic Dirichlet character. In the case where Ψ is non-trivial, Iwasawa [Iw1] (or [Wa, Theorem 7.10]) constructed a power series $g_\Psi(T) \in \Lambda_\Psi$ such that

$$g_\Psi(\kappa^s - 1) = L_p(s, \psi),$$

where $L_p(s, \psi)$ is the Kubota-Leopoldt's p -adic L -function associated to ψ . We call $g_\Psi(T) \in \Lambda_\Psi$ the Iwasawa power series corresponding to the p -adic L -function associated to ψ . Again, by the p -adic Weierstrass preparation theorem and the Ferrero-Washington theorem, we may write $g_\Psi(T)$ in a unique way,

$$g_\Psi(T) = Q_\Psi(T)v_\Psi(T),$$

where $Q_\Psi(T)$ is a distinguished polynomial in Λ_Ψ and $v_\Psi(T)$ is a unit power series in Λ_Ψ . We denote by $\lambda_p^*(\Psi)$ the degree of $Q_\Psi(T)$, which is called the λ -invariant associated to the p -adic L -function related to Ψ . Note that this depends only on Ψ and not on the choice of ψ .

In our previous paper [OT], we investigated Greenberg's conjecture for Ψ -components and gave a criterion for the conjecture to be true when the corresponding Iwasawa power series is an irreducible element in the unique factorization ring Λ_Ψ in an ordinary sense. Here, Greenberg's conjecture states that both of the Iwasawa λ - and μ -invariants are always zero for any totally real number field and any prime number (cf. [Gr1], also [Iw2, page 316]). In the case treated here, since k is abelian, the μ -invariant is zero by the Ferrero-Washington theorem [FW]. Hence, Greenberg's conjecture is equivalent to the statement called Greenberg's conjecture for Ψ -components that $\lambda_p(\Psi) = 0$ for any (non-trivial) Ψ . We would like to refer the reader to the paper [IS] and the papers cited in it (especially Kraft-Schoof [22], Kurihara [23] in [IS]), which together comprise recent important works in the study of Greenberg's conjecture. In spite of these works, very little is known about $\lambda_p(\Psi)$ -invariants except for $k = \mathbf{Q}$ or the trivial cases as in the following remark.

Remark 0.1 We have two cases for which Greenberg's conjecture is trivially true. One is that if $g_\Psi(T)$ is a unit power series in Λ_Ψ , then $\lambda_p(\Psi) = 0$ because of the inequality below between two λ -invariants. Another is that if Ψ_0 is the trivial character of Δ , then $\lambda_p(\Psi_0) = 0$ because e_{Ψ_0} is the norm from k to $\mathbf{Q}$ and $\lambda_p(\mathbf{Q}) = 0$.

On the other hand, we can calculate $\lambda_p^*(\Psi)$ -invariants by using Iwasawa power series attached to Ψ . The Iwasawa main conjecture proved by Mazur and Wiles [MW] tells us that

$$\text{char}_{\Lambda_\Psi}(\text{Gal}(M_\infty/k_\infty)^\Psi) = \dot{g}_\Psi(T)\Lambda_\Psi, \quad (1)$$

where $\dot{g}_\Psi(T) = g_\Psi(\kappa(1+T)^{-1} - 1)$. Since $k_\infty \subset L_\infty \subset M_\infty$, we have the following inequality:

$$\lambda_p(\Psi) \leq \lambda_p^*(\Psi).$$

The purpose of this paper is to give a necessary and sufficient condition for this inequality to be strict in terms of special values of p -adic L -functions (see Theorem 1.1). This is shown by a necessary and sufficient condition for the inequality to be strict in terms of certain finite Galois groups (Theorem 1.7) and by a relationship between these Galois groups and p -adic L -functions (Proposition 1.9). As an immediate consequence of this result, we can obtain a criterion for Greenberg's conjecture for Ψ -components to be true when the corresponding Iwasawa power series is irreducible (see Corollary 1.4). We also give an explicit version of Theorem 1.7 (or Theorem 1.1) for the case of real quadratic fields (see Proposition 1.10).

1 Statements of theorems

To describe our theorems, we prepare more notation in addition to the previous one. Let $\mathbf{Q}_n$ be the n -th layer of the cyclotomic $\mathbf{Z}_p$ -extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$. For a p -adic Dirichlet character ϕ_n of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$ and an irreducible $\mathbf{Q}_p$ -character Ψ of Δ , let us put

$$L_p(s, \Psi\phi_n) = \prod_{\psi} L_p(s, \psi\phi_n)$$

where the product runs over all irreducible components ψ of Ψ over $\bar{\mathbf{Q}}_p$. Then we denote by

$$L_p(s, \Psi\Phi_n) = \prod_{\phi_n} L_p(s, \Psi\phi_n)$$

where the product runs over all p -adic Dirichlet character ϕ_n of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$, and by

$$L_p^*(s, \Psi\Phi_n) = \prod_{\phi_n \neq 1} L_p(s, \Psi\phi_n),$$

where the product runs over all non-trivial p -adic Dirichlet characters ϕ_n of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$. When $\psi\phi_n$ is non-trivial, $L_p(s, \psi\phi_n)$ has non-zero value at $s = 1$, hence so do both $L_p(s, \Psi\Phi_n)$ and $L_p^*(s, \Psi\Phi_n)$. For the sake of convenience, we put

$$L_p^*(s, \Psi\Phi_0) = 1 \quad \text{and} \quad L_p(s, \Psi) = \prod_{\psi} L_p(s, \psi),$$

where the product runs over all irreducible components ψ of Ψ over $\bar{\mathbf{Q}}_p$. Then $L_p(s, \Psi\Phi_0) = L_p(s, \Psi)$ and $L_p^*(s, \Psi\Phi_n) = L_p(s, \Psi\Phi_n)/L_p(s, \Psi)$. Further, let A_n be the Sylow p -subgroup of the ideal class group of k_n , A_n^{Ψ} the Ψ -component of A_n , and v_p the p -adic valuation normalized by $v_p(p) = 1$. Then our main theorem is as follows. The proof is given in Section 3.

Theorem 1.1 *Let k be a real abelian number field with Galois group Δ and p an odd prime number. Assume that the order of Δ is not divisible by p . Let Ψ be a non-trivial irreducible $\mathbf{Q}_p$ -character of Δ . Then $\lambda_p(\Psi) < \lambda_p^*(\Psi)$ if and only if*

$$v_p(L_p^*(1, \Psi\Phi_n)\#A_0^{\Psi}/\#A_n^{\Psi}) \neq 0 \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(\Psi) < \lambda_p^*(\Psi)$ if and only if

$$v_p(L_p(1, \Psi\Phi_n)/\#A_n^{\Psi}) \neq 0 \quad \text{for some integer } n \geq 0.$$

Remark 1.2 Both $L_p^*(1, \Psi\Phi_n)\#A_0^{\Psi}/\#A_n^{\Psi}$ and $L_p(1, \Psi\Phi_n)/\#A_n^{\Psi}$ appearing in the above theorem are p -integral elements, namely, these are in $\mathcal{O}_{\Psi\Phi_n}$.

Remark 1.3 In [Ich2], Ichimura dealt with the following inequality which is weaker than Greenberg's conjecture:

$$\lambda_p(\Psi) \leq \max \{0, \lambda_p^*(\Psi) - 1\}?$$

And, for any fixed odd prime number p , he gives some families of infinitely many real quadratic fields k for which $\lambda_p^*(\psi) \geq 1$ and the inequality is valid, where ψ is the non-trivial p -adic Dirichlet character associated to k (for details, see [Ich2]).

From Theorem 1.1 and equality (2) in Section 2, the next corollary immediately follows.

Corollary 1.4 *With the same assumptions as in Theorem 1.1, further assume that $g_{\Psi}(T)$ is a non-unit and irreducible element in Λ_{Ψ} . Then $\lambda_p(\Psi) = 0$ if and only if*

$$v_p(L_p^*(1, \Psi\Phi_n)\#A_0^{\Psi}/\#A_n^{\Psi}) \neq 0 \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(\Psi) = 0$ if and only if

$$v_p(L_p(1, \Psi\Phi_n)\#A_n^{\Psi}) \neq 0 \quad \text{for some integer } n \geq 0.$$

Moreover, we can obtain the following corollary to the corollary above. A similar result is given independently by both Kraft [Kr, Theorem 3] and Ichimura [Ich1, Remark 2].

Corollary 1.5 *Under the same hypotheses as in Theorem 1.1, further assume that there is only one prime ideal above p in k . Then if $v_p(L_p(1, \Psi)/\#A_0^{\Psi}) \neq 0$, then $\lambda_p(\Psi) < \lambda_p^*(\Psi)$. In addition, assume that $g_{\Psi}(T)$ is a non-unit and irreducible element in Λ_{Ψ} . Then if $v_p(L_p(1, \Psi)/\#A_0^{\Psi}) \neq 0$, then $\lambda_p(\Psi) = 0$.*

Remark 1.6 Let k , p and Ψ be as in Theorem 1.1. Assume that k has degree prime to p . Then if $v_p(L_p(1, \Psi)) = 0$, then $\lambda_p(\Psi) = 0$. In fact, since $L_p(1, \Psi) \equiv L_p(0, \Psi) \pmod{p}$, if $v_p(L_p(1, \Psi)) = 0$, then $g_{\Psi}(T)$ is a unit pow-

er series in Λ_Ψ . Hence $\text{Gal}(M_\infty/k_\infty)^\Psi = \{0\}$ by [MW] and [Gr2] (this also follows from Proposition 1.9 in this section directly). In particular, $\lambda_p(\Psi) = 0$.

In order to prove Theorem 1.1, following a comment of Greither [Gt], we first slightly improve our previous result in [OT] as follows.

Theorem 1.7 *Let k , p and Ψ be as in Theorem 1.1. Assume that the order of Δ is not divisible by p . Then $\lambda_p(\Psi) < \lambda_p^*(\Psi)$ if and only if*

$$\#\text{Gal}(M_n/L_n)^\Psi > \#\text{Gal}(M_0/L_0)^\Psi \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(\Psi) < \lambda_p^(\Psi)$ if and only if*

$$\text{Gal}(M_n/L_n)^\Psi \neq \{0\} \quad \text{for some integer } n \geq 0.$$

This theorem is more or less known, but we give its proof in Section 2 as the reader see the difference between previous and present proofs. Note that $\text{Gal}(M_n/L_n)^\Psi$ is finite for a non-trivial Ψ , because Leopoldt's conjecture is valid for abelian fields (cf. [Co, Lemma 8 in Appendix]) and $\text{Gal}(k_\infty/k_n)^\Psi = \{0\}$ for a non-trivial Ψ .

The next corollary immediately follows from Theorem 1.7 and equality (2) in Section 2 (see [OT, Theorem 1]).

Corollary 1.8 *With the same assumptions as in Theorem 1.7, further assume that $g_\Psi(T)$ is a non-unit and irreducible element in Λ_Ψ . Then $\lambda_p(\Psi) = 0$ if and only if*

$$\#\text{Gal}(M_n/L_n)^\Psi > \#\text{Gal}(M_0/L_0)^\Psi \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(\Psi) = 0$ if and only if

$$\text{Gal}(M_n/L_n)^\Psi \neq \{0\} \quad \text{for some integer } n \geq 0.$$

To connect Theorem 1.7 with Theorem 1.1, we need the following proposition, which describes a relation between the non-zero value of $L_p(s, \Psi\Phi_n)$ at $s = 1$ and the order of the finite Galois group $\text{Gal}(M_n/k_\infty)^\Psi$. The proof is given in Section 3.

Proposition 1.9 *Let k , p and Ψ be as in Theorem 1.1. Assume that the order of Δ is not divisible by p . Then*

$$\#\text{Gal}(M_n/k_\infty)^\Psi = p^{v_p(L_p(1, \Psi\Phi_n))}$$

for all integers $n \geq 0$.

Finally, we give here an explicit version of Theorem 1.7 (or Theorem 1.1) for the case of real quadratic fields. Let k be a real quadratic field and p an odd prime number. We denote by ψ the non-trivial p -adic Dirichlet character associated to k . Note that $O_\psi = \mathbb{Z}_p$, $\Lambda_\psi = \mathbb{Z}_p[[T]]$, $A_n = A_n^\psi$ and $\lambda_p(k) = \lambda_p(\psi)$ in this case. Let $R_p(k_n)$ be the p -adic regulator of k_n and $\log_p$ the p -adic logarithm, and further, we put

$$\delta = \begin{cases} 0 & \text{if } p \text{ is unramified in } k, \\ \frac{1}{2} & \text{if } p \text{ is ramified in } k. \end{cases}$$

Then, by Lemmas 4, 5 in [OT] and the fact that $\text{Gal}(M_n/L_n)^\psi = \text{Gal}(M_n/k_\infty L_n)^\psi$, one can easily rewrite Theorem 1.7 (or Theorem 1.1) as follows.

Proposition 1.10 *Let k be a real quadratic field and p an odd prime number. Denote by ψ the non-trivial p -adic Dirichlet character associated to k , and by ε (> 1) the fundamental unit of k . Then $\lambda_p(\psi) < \lambda_p^*(\psi)$ if and only if*

$$v_p(R_p(k_n)) > (n+1)p^n - \frac{p^n - 1}{p - 1} - n - 1 + v_p(\log_p(\varepsilon)) \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(\psi) < \lambda_p^(\psi)$ if and only if*

$$v_p(R_p(k_n)) > (n+1)p^n - \frac{p^n - 1}{p - 1} - n - \delta \quad \text{for some integer } n \geq 0.$$

The following is an immediate corollary to the theorem above (see [OT, Theorem 2]).

Corollary 1.11 *Let k, p, ψ and ε be as in Proposition 1.10. Assume that $g_\psi(T)$ is a non-unit and irreducible element in Λ_ψ . Then $\lambda_p(k) = 0$ if and only if*

$$v_p(R_p(k_n)) > (n+1)p^n - \frac{p^n - 1}{p-1} - n - 1 + v_p(\log_p(\varepsilon)) \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\lambda_p(k) = 0$ if and only if

$$v_p(R_p(k_n)) > (n+1)p^n - \frac{p^n - 1}{p-1} - n - \delta \quad \text{for some integer } n \geq 0.$$

Further, we define the constant $n_\varepsilon \in \mathbb{N}$ by

$$\mathfrak{p}^{n_\varepsilon} \| ((\varepsilon^{p^{N(\mathfrak{p})-1}} - 1)p^{-1}) \text{ in } k,$$

where $\mathfrak{p}$ denotes a prime ideal of k over p and N the norm from k to $\mathbb{Q}$. Then it is easy to see that

$$v_p(R_p(k)) = \begin{cases} n_\varepsilon & \text{if } p \text{ is unramified in } k, \\ \frac{n_\varepsilon}{2} & \text{if } p \text{ is ramified in } k. \end{cases}$$

Here we make some remarks regarding the constant n_ε . First, if p is ramified in k , then n_ε is odd, so $v_p(R_p(k))$ is half-integral (non-integral). Next, if $p \neq 3$ or $d_k \not\equiv 6 \pmod{9}$, then n_ε satisfies $\mathfrak{p}^{n_\varepsilon} \| (\varepsilon^{N(\mathfrak{p})-1} - 1)$ in k , d_k being the discriminant of k . In particular, we may define n_ε by this property in such a case.

The following is the analogous version of Corollary 1.5 for the case of real quadratic fields (see [OT, Corollaries 1 and 2]).

Corollary 1.12 *Under the same hypotheses as in Proposition 1.10, further assume that there is only one prime ideal above p in k . Then if $n_\varepsilon > 1$, then $\lambda_p(\psi) < \lambda_p^*(\psi)$. In addition, assume that $g_\psi(T)$ is a non-unit and irreducible element in Λ_ψ . Then if $n_\varepsilon > 1$, then $\lambda_p(k) = 0$.*

2 Proof of Theorem 1.7

In this section, we prove Theorem 1.7. The same notation as in the preceding section is used continuously. For an irreducible $\mathbb{Q}_p$ -character Ψ of Δ , we put $X = \text{Gal}(L_\infty/k_\infty)^\Psi$ and $Y = \text{Gal}(L_\infty/L_0 k_\infty)^\Psi$, which are finitely generated torsion Λ_Ψ -modules. It is clear that $\text{char}_{\Lambda_\Psi}(X) = \text{char}_{\Lambda_\Psi}(Y)$. We put

$$\omega_n = (1+T)^{p^n} - 1 \in \Lambda_\Psi, \quad v_n = \frac{\omega_n}{\omega_0} \in \Lambda_\Psi$$

for all integers $n \geq 0$. As is well-known,

$$\text{Gal}(L_n/k_n) \simeq \text{Gal}(L_\infty/k_\infty)/v_n \text{Gal}(L_\infty/L_0 k_\infty)$$

and

$$\text{Gal}(M_n/k_\infty) \simeq \text{Gal}(M_\infty/k_\infty)/\omega_n \text{Gal}(M_\infty/k_\infty)$$

for all integers $n \geq 0$ (cf. [Iw2, Theorem 6 and Section 3.2]). In particular, by taking the Ψ -component of the former isomorphism, we have

$$\text{Gal}(L_n/k_n)^\Psi \simeq X/v_n Y$$

for all integers $n \geq 0$. As mentioned in the preceding section, $\text{Gal}(k_\infty/k_n)^\Psi = \{0\}$ and $\text{Gal}(M_n/L_n)^\Psi$ is finite for any non-trivial Ψ . First, we show the following lemma.

Lemma 2.1 *Let k, p and Ψ be as in Theorem 1.7. Assume that the order of Δ is not divisible by p . Then $\text{Gal}(M_\infty/L_\infty)^\Psi \neq \{0\}$ if and only if*

$$\#\text{Gal}(M_n/L_n)^\Psi > \#\text{Gal}(M_0/L_0)^\Psi \quad \text{for some integer } n \geq 1.$$

Moreover, if there is only one prime ideal above p in k , then $\text{Gal}(M_\infty/L_\infty)^\Psi \neq \{0\}$ if and only if

$$\text{Gal}(M_n/L_n)^\Psi \neq \{0\} \quad \text{for some integer } n \geq 0.$$

Proof. First, we assume that $\text{Gal}(M_\infty/L_\infty)^\Psi = \{0\}$. Then $X = \text{Gal}(M_\infty/k_\infty)^\Psi$ and $Y = \text{Gal}(M_\infty/L_0 k_\infty)^\Psi$. Hence, $X/\omega_n X \simeq \text{Gal}(M_n/k_n)^\Psi$ for all integers $n \geq 0$. We also note that $X \supset v_n Y \supset \omega_n X$ for all integers $n \geq 0$, because $X/\omega_n X \simeq \text{Gal}(M_n/k_\infty)^\Psi$ and $X/v_n Y \simeq \text{Gal}(L_n k_\infty/k_\infty)^\Psi$.

Now, from the fact that $X/v_n Y \simeq \text{Gal}(L_n/k_n)^\Psi$ and $Y \subseteq X$, it follows that $Y/v_n Y$ is finite for all integers $n \geq 0$. Thus $\text{char}_{\Lambda_\Psi}(Y)$ is prime to v_n . Since $Y = \text{Gal}(M_\infty/L_0 k_\infty)^\Psi$, Y has no non-trivial finite Λ_Ψ -submodule. Hence, the multiplication-by- v_n map from $Y/\omega_0 X$ to $Y/\omega_n X$ is injective, which implies that

$$Y/\omega_0 X \simeq v_n Y/\omega_n X$$

for all integers $n \geq 0$. Consequently, we obtain

$$\begin{aligned} \#\text{Gal}(M_n/L_n)^\Psi &= \#(X/\omega_n X)/\#(X/v_n Y) \\ &= \#(v_n Y/\omega_n X) = \#(Y/\omega_0 X) \\ &= \#(X/\omega_0 X)/\#(X/Y) \\ &= \#\text{Gal}(M_0/L_0)^\Psi \end{aligned}$$

for all integers $n \geq 0$.

Conversely, we assume that $\#\text{Gal}(M_n/L_n)^\Psi \leq \#\text{Gal}(M_0/L_0)^\Psi$ for all integers $n \geq 1$. Since $M_\infty = \bigcup_{n \geq 0} M_n$ and $L_\infty = \bigcup_{n \geq 0} L_n$, we find that

$$\text{Gal}(M_\infty/L_\infty)^\Psi \simeq \varprojlim_n \text{Gal}(M_n/L_n)^\Psi,$$

where the projective limit is taken with respect to the restriction maps. This implies that $\text{Gal}(M_\infty/L_\infty)^\Psi$ is finite. Since $\text{Gal}(M_\infty/k_\infty)^\Psi$ has no non-trivial finite Λ_Ψ -submodule, it follows that $\text{Gal}(M_\infty/L_\infty)^\Psi = \{0\}$. Thus we have proved the first assertion.

Next we assume that there is only one prime ideal above p in k . Then

$$\text{Gal}(L_n/k_n)^\Psi \simeq X/\omega_n X$$

for all integers $n \geq 0$ (cf. [Wa, Lemma 13.15]). Therefore, if $\text{Gal}(M_\infty/L_\infty)^\Psi = \{0\}$, then $\text{Gal}(M_n/k_n)^\Psi \simeq X/\omega_n X \simeq \text{Gal}(L_n/k_n)^\Psi$, and hence $\text{Gal}(M_n/L_n)^\Psi = \{0\}$ for all integers $n \geq 0$. Conversely, if $\text{Gal}(M_n/L_n)^\Psi = \{0\}$ for all integers $n \geq 0$ then the above projective limit implies that $\text{Gal}(M_\infty/L_\infty)^\Psi = \{0\}$. Consequently the second assertion also follows. $\square$

Proof of Theorem 1.7. Recall that $\lambda_p(\Psi) = \deg P_\Psi(T)$ and $\lambda_p^*(\Psi) = \deg Q_\Psi(T)$. Here $P_\Psi(T)$ is the distinguished polynomial related to a generator $f_\Psi(T)$ of $\text{char}_{\Lambda_\Psi}(\text{Gal}(L_\infty/k_\infty)^\Psi)$, and $Q_\Psi(T)$ is the distinguished polynomial related to $g_\Psi(T) \in \Lambda_\Psi$ corresponding to $L_p(s, \psi)$, ψ being an irreducible component of Ψ over $\bar{\mathbf{Q}}_p$.

From the Iwasawa main conjecture proved by Mazur and Wiles [MW] and the equality

$$\text{char}_{\Lambda_\Psi}(\text{Gal}(M_\infty/k_\infty)^\Psi) = \text{char}_{\Lambda_\Psi}(\text{Gal}(M_\infty/L_\infty)^\Psi) \text{char}_{\Lambda_\Psi}(\text{Gal}(L_\infty/k_\infty)^\Psi), \quad (2)$$

it follows that

$$\begin{aligned} \lambda_p(\Psi) < \lambda_p^*(\Psi) &\Leftrightarrow \text{char}_{\Lambda_\Psi}(\text{Gal}(M_\infty/L_\infty)^\Psi) \neq \Lambda_\Psi \\ &\Leftrightarrow \#\text{Gal}(M_\infty/L_\infty)^\Psi = \infty. \end{aligned}$$

Since $\text{Gal}(M_\infty/L_\infty)^\Psi$ is a Λ_Ψ -submodule of $\text{Gal}(M_\infty/k_\infty)^\Psi$, it also has no non-trivial finite Λ_Ψ -submodule. Hence, $\#\text{Gal}(M_\infty/L_\infty)^\Psi = \infty$ is equivalent to $\text{Gal}(M_\infty/L_\infty)^\Psi \neq \{0\}$. Therefore Theorem 1.7 immediately follows from Lemma 2.1. $\square$

3 Proofs of Proposition 1.9 and Theorem 1.1

We continue with the same notation as in the previous sections. Before starting the proofs of Proposition 1.9 and Theorem 1.1, we require two lemmas. The following is an easy exercise.

Lemma 3.1 *Let Λ be a power series ring over the ring of integral elements in a finite extension of $\mathbf{Q}_p$. Let g , h_1 and h_2 be power series in Λ . Assume that h_2 is prime to g . Then*

$$\Lambda/(g, h_1) \simeq (g, h_2)/(g, h_1 h_2),$$

where (g_1, g_2) denotes the ideal of Λ generated by g_1 and g_2 for $g_1, g_2 \in \Lambda$.

Next lemma can be proved by a standard argument in the theory of Λ_Ψ -modules. But it is a key lemma in the proof of Proposition 1.9, so we give its proof for the sake of completeness.

Lemma 3.2 *Let k , p and Ψ be as in Theorem 1.1. Let g be a power series in Λ_Ψ and put $\omega_n = (1 + T)^{p^n} - 1$. Assume that the order of Δ is not divisible by p and also that g is prime to ω_n . Then*

$$v_p(\#(\Lambda_\Psi/(g, \omega_n))) = d_\Psi v_p\left(\prod_{\zeta^{p^n}=1} g(\zeta - 1)\right),$$

where the product runs over all p^n -th roots ζ of unity and d_Ψ is the degree of K_Ψ over $\mathbf{Q}_p$.

Proof. First, note that $\Lambda_\Psi/(g, \omega_n)$ is finite because g is prime to ω_n . Let φ be the Euler function. Then

$$(\Lambda_\Psi/(g, \omega_n))^{\oplus \varphi(p^n)} \simeq \Lambda_\Psi/(g, \omega_n) \otimes_{O_\Psi} (O_\Psi^{\oplus \varphi(p^n)}).$$

Let ζ_{p^n} be a primitive p^n -th root of unity. By the assumption on the order of Δ , we have $\mathbf{Z}_p[\zeta_{p^n}] \cap O_\Psi = \mathbf{Z}_p$. Hence we obtain

$$\begin{aligned} \Lambda_\Psi/(g, \omega_n) \otimes_{O_\Psi} (O_\Psi^{\oplus \varphi(p^n)}) &\simeq \Lambda_\Psi/(g, \omega_n) \otimes_{O_\Psi} O_\Psi[\zeta_{p^n}] \\ &\simeq O_\Psi[\zeta_{p^n}][[T]]/(g, \omega_n). \end{aligned}$$

Since

$$\omega_n = \prod_{\zeta^{p^n}=1} (T - (\zeta - 1))$$

is prime to g in $O_\Psi[\zeta_{p^n}][[T]]$, it follows from Lemma 3.1 that

$$\#(O_\Psi[\zeta_{p^n}][[T]]/(g, \omega_n)) = \#(\oplus_{\zeta^{p^n}=1} O_\Psi[\zeta_{p^n}][[T]]/(g, T - (\zeta - 1))).$$

Hence one can see that

$$\#(\Lambda_\Psi/(g, \omega_n))^{\varphi(p^n)} = \prod_{\zeta^{p^n}=1} \#(O_\Psi[\zeta_{p^n}]/(g(\zeta - 1))).$$

On the other hand, since the order of Δ is not divisible by p , the ramification index and the residue degree of $K_\Psi(\zeta_{p^n})/\mathbf{Q}_p$ are $\varphi(p^n)$ and d_Ψ , respectively. Thus,

$$\#(O_\Psi[\zeta_{p^n}]/(g(\zeta - 1))) = p^{d_\Psi \varphi(p^n) v_p(g(\zeta - 1))}.$$

Therefore, we obtain

$$\#(\Lambda_\Psi/(g, \omega_n))^{\varphi(p^n)} = \prod_{\zeta^{p^n}=1} p^{d_\Psi \varphi(p^n) v_p(g(\zeta - 1))},$$

and hence

$$\#(\Lambda_\Psi/(g, \omega_n)) = p^{d_\Psi v_p(\prod_{\zeta^{p^n}=1} g(\zeta - 1))},$$

which is the desired result. $\square$

In the introduction, we recall the Iwasawa power series corresponding to the p -adic L -function associated to a Dirichlet character of the first kind. We also recall the Iwasawa power series in the case where a Dirichlet character is not of the first kind. Let ψ be an irreducible component of Ψ over $\bar{\mathbf{Q}}_p$ and let ϕ_n be a p -adic Dirichlet character of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$. Then ψ is of the first kind and ϕ_n is of the second kind. By Iwasawa's construction of p -adic L -functions (cf. [Iw1] or [Wa, Theorem 7.10]), for a non-trivial Dirichlet character $\psi\phi_n$, there exists a unique power series $g_\psi(T) \in \Lambda_\Psi$ such that

$$g_\psi(\zeta_{\phi_n} \kappa^s - 1) = L_p(s, \psi\phi_n)$$

where κ is as in the introduction, and $\zeta_{\phi_n} = \phi_n(\kappa)^{-1}$ is a p^n -th root of unity. Now we can prove Proposition 1.9.

Proof of Proposition 1.9. It is well-known that $\text{char}_{\Lambda_\Psi} \text{Gal}(M_\infty/k_\infty)^\Psi$ is prime to ω_n because $\text{Gal}(M_n/k_\infty)^\Psi$ is finite in the case where k is abelian. Hence, since $\text{Gal}(M_\infty/k_\infty)^\Psi$ has no non-trivial finite Λ_Ψ -submodule, the Iwasawa main conjecture proved by Mazur and Wiles (see (1) in the introduction) and Lemma 1 in [OT] (cf. Lemma 8.6 in [Ru]) imply that

$$\#\text{Gal}(M_n/k_\infty)^\Psi = \#(\Lambda_\Psi/(\dot{g}_\psi, \omega_n))$$

for all integers $n \geq 0$, where $\dot{g}_\psi(T) = g_\psi(\kappa(1+T)^{-1} - 1)$. Therefore, we obtain from Lemma 3.2 that

$$\#\text{Gal}(M_n/k_\infty)^\Psi = p^{d_\Psi v_p(\prod_{\zeta^{p^n}=1} \dot{g}_\psi(\zeta - 1))}.$$

Since $L_p(1, \psi\phi_n) = g_\psi(\zeta_{\phi_n} \kappa - 1) = \dot{g}_\psi(\zeta_{\phi_n}^{-1} - 1)$ and since ζ_{ϕ_n} runs through all p^n -th roots of unity as ϕ_n runs through all p -adic Dirichlet characters of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$, it follows that

$$\#\text{Gal}(M_n/k_\infty)^\Psi = p^{d_\Psi v_p(\prod_{\phi_n} L_p(1, \psi\phi_n))}$$

for all integers $n \geq 0$, where the product runs over all p -adic Dirichlet characters ϕ_n of $\text{Gal}(\mathbf{Q}_n/\mathbf{Q})$. For any other irreducible component ψ' of Ψ over $\bar{\mathbf{Q}}_p$, we have

$$v_p\left(\prod_{\phi_n} L_p(1, \psi\phi_n)\right) = v_p\left(\prod_{\phi_n} L_p(1, \psi'\phi_n)\right).$$

Hence

$$d_\Psi v_p\left(\prod_{\phi_n} L_p(1, \psi\phi_n)\right) = v_p\left(\prod_{\psi} \prod_{\phi_n} L_p(1, \psi\phi_n)\right),$$

because the number of all irreducible components of Ψ over $\bar{\mathbf{Q}}_p$ is equal to d_Ψ . Therefore the desired result follows immediately. This completes the proof of Proposition 1.9. $\square$

Finally, we prove Theorem 1.1.

Proof of Theorem 1.1. By the non-triviality of Ψ , $\text{Gal}(k_\infty/k_n)^\Psi = \{0\}$ for all integers $n \geq 0$. Hence $\text{Gal}(M_n/k_\infty)^\Psi = \text{Gal}(M_n/k_n)^\Psi$, which implies that

$$\#\text{Gal}(M_n/k_\infty)^\Psi = \#\text{Gal}(M_n/L_n)^\Psi \#\text{Gal}(L_n/k_n)^\Psi$$

for all integers $n \geq 0$. Therefore, it follows from Proposition 1.9 that

$$v_p(\#\text{Gal}(M_n/L_n)^\Psi) = v_p(L_p(1, \Psi\Phi_n)/\#A_n^\Psi)$$

for all integers $n \geq 0$. Consequently, our assertion directly follows from Theorem 1.7. $\square$

REFERENCES

- [Co] J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic Number Fields (Durham Symposium, 1975, ed. by A. Fröhlich), 269–353, Academic Press, 1977.
- [FW] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.
- [Gr1] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
- [Gr2] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), 85–99.
- [Gt] C. Greither, A. M. S. Math. Review **97b**:11128 (1997), 824.
- [Ich1] H. Ichimura, *On a normal integral bases problem over cyclotomic $\mathbf{Z}_p$ -extensions*, J. Math. Soc. Japan **48** (1996), 689–703.
- [Ich2] H. Ichimura, *A note on the Iwasawa λ -invariants of real quadratic fields*, Proc. Japan Acad. **72A** (1997), 28–30.
- [IS] H. Ichimura and H. Sumida, *On the Iwasawa λ -invariants of certain real abelian fields II*, International J. Math. **7** (1996), 721–744.
- [Iw1] K. Iwasawa, *Lectures on p-Adic L-Functions*, Ann. of Math. Studies No. **74**, Princeton Univ. Press: Princeton, N. J., 1972.
- [Iw2] K. Iwasawa, *On $\mathbf{Z}_l$ -extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.
- [Kr] J. S. Kraft, *Iwasawa invariants of CM fields*, J. Number Theory, **32** (1989), 65–77.
- [MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of $\mathbf{Q}$* , Invent. Math. **76** (1984), 179–330.
- [OT] M. Ozaki and H. Taya, *A note on Greenberg's conjecture for real abelian number fields*, Manuscripta Math. **88** (1995), 311–320.
- [Ru] K. Rubin, *The Main conjecture*, Appendix to: Cyclotomic Fields I and II (Combined 2nd ed.), by S. Lang, Graduate Texts in Math. Vol. 121. Springer-Verlag, New York, Heidelberg, Berlin 1990.
- [Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. Vol. 83. Springer-Verlag, New York, Heidelberg, Berlin 1982.

Manabu OZAKI**

E-mail address: ozaki@math.shimane-u.ac.jp

Hisao TAYA

E-mail address: taya@math.is.tohoku.ac.jp

**Present Address: Department of Mathematics, Shimane University, Nishikamatsu-cho, Matsue 690-8504, JAPAN