JOURNAL OF NUMBER THEORY **24**, 107–113 (1986)

A Note on Iwasawa Invariants and the Main Conjecture

LESLIE JANE FEDERER

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109

Communicated by D. J. Lewis

Received October 26, 1984

We fix a rational prime p, possibly 2, and a CM field K. Let $A_{K_\infty}^-$ denote the minus component of the p-primary class group of K_∞, the basic $\mathbb{Z}_p$-extension of K. The Pontryagin dual $(A_{K_\infty}^-)^\vee$ is a noetherian, torsion $\mathbb{Z}_p[[T]]$-module whose characteristic polynomial we denote by $f(T)$. Iwasawa's Main Conjecture relates the algebraically defined $f(T)$ to an analytically defined power series $F(T)$ given by a p-adic L-function. Using the analytic class number formula, we give evidence for it based on the Iwasawa invariants of $f(T)$ and $F(T)$. I would like to thank Benedict H. Gross for suggesting this approach. © 1986 Academic Press, Inc.

I. PRELIMINARIES

Let K be a CM field with maximal totally real subfield k, $G(K/k)=\{1, J\}$. Let $\mathbb{Q}_\infty$ be the (unique) $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Set $k_\infty = k\mathbb{Q}_\infty$, $K_\infty = K\mathbb{Q}_\infty$, and $G_\infty = G(k_\infty/k)$. By k_n we denote the unique subfield of k_∞ with $[k_n : k] = p^n$. Let $K_n = Kk_n$.

Let μ_{2p} denote the group of $2p$th roots of unity. Let u be a fixed topological generator of $1+2p[k \cap \mathbb{Q}_\infty : \mathbb{Q}]\, \mathbb{Z}_p$. If ζ is a p-power root of unity, define $\sigma_u(\zeta) = \zeta^u$. Then σ_u is a topological generator of $G(k_\infty(\mu_{2p})/k(\mu_{2p}))$ and its restriction to k_∞, denoted σ, is a topological generator of G_∞.

If $n \leqslant m$, there is a natural map $A_{K_n} \to A_{K_m}$ of p-class groups and we let $A_{K_\infty} = \varinjlim A_{K_n}$ relative to these homomorphisms. We define A_{k_∞} similarly. The norm maps from K_n to k_n induce a natural exact sequence

$$1 \to B \to A_{K_\infty} \xrightarrow{\mathbb{N}} A_{k_\infty} \to 1$$

of discrete G_∞-modules. When p is odd, clearly

$$B = A_{K_\infty}^- = \{C \in A_{K_\infty} \mid C^{1+J} = 1\}$$

and in fact this is true even when $p=2$ [$F1$]. The Pontryagin dual

0022-314X/86 $3.00

Copyright © 1986 by Academic Press, Inc.
All rights of reproduction in any form reserved.

$B^v = \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ has a natural structure as a compact $\mathbb{Z}_p[G_\infty]$-module, and we give it the structure of $\mathbb{Z}_p[[T]]$-module, by requiring T act as $\sigma - 1$. Then B^v is a noetherian, torsion $\mathbb{Z}_p[[T]]$-module [W], hence has a characteristic polynomial $f(T)$.

Let $\chi: G(K_\infty/k) \to \{\pm 1\}$ be the quadratic character corresponding to the imaginary quadratic extension K_∞/k_∞ and let $\theta: G(K_\infty/k) \to \mathbb{C}_p^\times$ be the p-adic Teichmüller character.

Fix an isomorphism $\tau: \mathbb{C}_p \to \mathbb{C}$. If $\psi: G(K_\infty/k) \to \mathbb{C}_p^\times$ is a character, the p-adic L-function $L_p(\psi\theta, s)$ is the unique continuous function from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ whose values are related to those of the Artin L-series $L(\psi^\tau, s)$ by

$$\{L_p(\psi\theta, n)\}^\tau = \prod_{\not{p} \mid p} (1 - \psi^\tau(\not{p})\, \mathbb{N}\not{p}^{-n})\, L(\psi^\tau, n)$$

for all $n \leqslant 0$ with $n \equiv 1 \bmod [\mathbb{Q}(\mu_p): \mathbb{Q}]$.

Let S denote the set of places of k which ramify in K or which divide p or infinity. There is a unique power series $F(T) \in \mathbb{Z}_p[[T]]$ such that if $\psi: G(K_\infty/k) \to \mathbb{C}_p^\times$ is a one dimensional character with $\psi(J) = -1$ and conductor in S, then

$$L_p(\psi\theta, s) = \begin{cases} F(\psi\theta(\sigma^{-1})\, u^s - 1) & \text{if } K_\infty \neq k_\infty(\mu_{2p}) \\ \dfrac{F(\psi\theta(\sigma^{-1})\, u^s - 1}{\psi\theta(\sigma)\, u^{1-s} - 1} & \text{if } K_\infty = k_\infty(\mu_{2p}). \end{cases}$$

The power series $F(T)$ is a twist of the power series given by the Deligne–Ribet measure [S].

II. The Problem

Given a power series $g(T) \in \mathbb{Z}_p[[T]]$, the Weierstrass preparation theorem [W] guarantees that we may uniquely write

$$g(T) = p^{\mu_g} b(T)\, u(T),$$

where $u(T) \in \mathbb{Z}_p[[T]]^*$ and $b(T)$ is a product of distinguished irreducible polynomials (i.e., irreducible polynomials of the form $T^n + a_1 T^{n-1} + \cdots + a_n$ with $a_i \in p\mathbb{Z}_p$, $i = 1,..., n$). Let $\lambda_g = \deg b(T)$. The integers μ_g and λ_g are the Iwasawa invariants of $g(T)$.

In this paper we give a simple proof that $F(T)$ and $2^{[k:\mathbb{Q}]} f(T)$ have the same Iwasawa invariants, i.e.,

$$\lambda_F = \lambda_f \quad \text{and} \quad \mu_F = \begin{cases} \mu_f & \text{if } p \text{ is odd} \\ [k : \mathbb{Q}] + \mu_f & \text{if } p = 2. \end{cases} \qquad (*)$$

Note that the Main Conjecture of Iwasawa theory conjectures that $F(T)$ is the product of $2^{[k:\mathbb{Q}]}f(T)$ and an element of $\mathbb{Z}_p[[T]]^*$, hence predicts (*). Iwasawa [I] proved (*) in the case $K=\mathbb{Q}(\mu_m)$ and $p \mid 2m$, and in (C), Coates claimed that if p is odd and $K \supseteq \mu_p$, (*) may be proved using the analytic class number formula. Mazur and Wiles [MW] have proved the Main conjecture whenever p is odd, k is abelian, and $K=k(\mu_{2p})$.

III. The Proof

Step 1. *The Analytic Class Number Formula*

Let h_{k_n} and h_{K_n} denote the class numbers of k_n and K_n and E_{k_n} and E_{K_n} their unit groups. Let μ_{K_n} signify the group of roots of unity of K_n. The unit index $Q_{K_n/k_n}=[E_{K_n}:\mu_{K_n}E_{k_n}]$, which is equal to 1 or 2, stabilizes for sufficiently large n [K]:

$$Q_{K_n/k_n}=Q_{K_{n-1}/k_{n-1}} \qquad \text{for} \quad n \gg 0.$$

The analytic class number formula applied to the extension K_n says that

$$\prod_{\psi} L(\psi^\tau\chi^\tau, 0) = 2^{[k_n:\mathbb{Q}]}\frac{h_{K_n}}{h_{k_n}}\cdot\frac{1}{|\mu_{K_n}|}\cdot\frac{1}{Q_{K_n/k_n}},$$

where the product is over all characters $\psi\colon G(k_n/k)\to\mathbb{C}_p^\times$. Looking at the class number formula for K_{n-1} as well as for K_n, we find

$$\begin{aligned}\prod_{\psi_n} L(\psi_n^\tau\chi^\tau, 0) &= 2^{[k_n:\mathbb{Q}]-[k_{n-1}:\mathbb{Q}]}\frac{h_{K_n}/h_{k_n}}{h_{K_{n-1}}/h_{k_{n-1}}}\,\frac{|\mu_{K_{n-1}}|}{|\mu_{K_n}|}\,\frac{Q_{K_{n-1}/k_{n-1}}}{Q_{K_n/k_n}}\\ &= 2^{(p^n-p^{n-1})[k:\mathbb{Q}]}\frac{h_{K_n}/h_{k_n}}{h_{K_{n-1}}/h_{k_{n-1}}}\,\frac{|\mu_{K_{n-1}}|}{|\mu_{K_n}|}\,\frac{Q_{K_{n-1}/k_{n-1}}}{Q_{K_n/k_n}},\end{aligned}$$

where ψ_n runs over all characters $\psi_n\colon G(k_n/k)\to\mathbb{C}_p^\times$ of *exact* order p^n. Hence

$$\prod_{\psi_n} L(\psi_n^\tau\chi^\tau, 0) = 2^{(p^n-p^{n-1})[k:\mathbb{Q}]}\frac{h_{K_n}/h_{k_n}}{h_{K_{n-1}}/h_{k_{n-1}}} \times \begin{cases} 1 & \text{if} \quad K_\infty \neq k_\infty(\mu_{2p}) \\ \dfrac{1}{p} & \text{if} \quad K_\infty = k_\infty(\mu_{2p}) \end{cases}$$

for $n \gg 0$.

On the other hand, by the definition of the p-adic L-function,

$$\left\{\prod_{\psi_n} L_p(\psi_n\chi\theta, 0)\right\}^\tau = \prod_{\psi_n}\prod_{\mathfrak{p}/p}(1-\chi^\tau(\mathfrak{p})\,\psi_n^\tau(\mathfrak{p}))\,L(\psi_n^\tau\chi^\tau, 0)$$

$$= \prod_{\psi_n} L(\psi_n^\tau\chi^\tau, 0) \qquad \text{for} \quad n \gg 0.$$

Therefore,

$$\left\{\prod_{\psi_n} L_p(\psi_n\chi\theta, 0)\right\}^\tau = 2^{(p^n-p^{n-1})[k;\mathbb{Q}]}\,\frac{h_{K_n}/h_{k_n}}{h_{K_{n-1}}/h_{k_{n-1}}}$$

$$\times \begin{cases} 1 & \text{if} \quad K_\infty \neq k_\infty(\mu_{2p}) \\ \dfrac{1}{p} & \text{if} \quad K_\infty = k_\infty(\mu_{2p}). \end{cases}$$

Step 2. *The Power Series* $F(T)$

We write $\alpha \sim \beta$ to indicate that α and β are p-adic numbers with the same valuation.

As in Step 1, ψ_n will always signify a p-adic character of $G(k_n/k)$ of exact order n.

Since $\prod_{\zeta,\zeta^{p^n}=1,\zeta^{p^{n-1}}\neq 1}(1-\zeta)=p$, if $b(T)$ is a distinguished polynomial

$$\prod_{\substack{\zeta \\ \zeta^{p^n}=1 \\ \zeta^{p^{n-1}}\neq 1}} b(\zeta-1) \sim p^{\deg b}.$$

Therefore, taking a Weierstrass preparation for $F(T)$,

$$\prod_{\substack{\zeta \\ \zeta^{p^n}=1 \\ \zeta^{p^{n-1}}\neq 1}} F(\zeta-1) \sim p^{(p^n-p^{n-1})\mu_F+\lambda_F}.$$

Hence

$$\prod_{\psi_n} F(\psi_n(\sigma^{-1})-1) \sim p^{(p^n-p^{n-1})\mu_F+\lambda_F},$$

and if $p=2$,

$$\prod_{\psi_n} F(-\psi_n(\sigma^{-1})-1) \sim p^{(p^n-p^{n-1})\mu_F+\lambda_F}.$$

Therefore, we always have

$$\text{(i)}\qquad \prod_{\psi_n} F(\chi\theta(\sigma^{-1})\,\psi_n(\sigma^{-1})-1)\sim p^{(p^n-p^{n-1})\mu_F+\lambda_F}.$$

Next observe that

$$\begin{aligned}\prod_{\substack{\zeta\\ \zeta^{p^n}=1}} (\zeta u-1) &= u^{p^n}\prod_{\substack{\zeta\\ \zeta^{p^n}=1}}(\zeta-u^{-1})\\ &= \pm u^{p^n}(u^{-p^n}-1)\\ &= \pm 1(1-u^{p^n})\\ &\sim p^n 2p[\mathscr{k}\cap\mathbb{Q}_\infty:\mathbb{Q}],\qquad n\gg 0.\end{aligned}$$

Consequently,

(ii) $\prod_{\psi_n}(\chi\theta(\sigma^{-1})\psi_n(\sigma)u-1)\sim\prod_{\zeta,\zeta^{p^n}=1,\zeta^{p^{n-1}}\neq 1}(\zeta u-1)\sim p$ for $n\gg 0$.

Let us now recall the fundamental relationship between $F(\chi\theta\psi_n(\sigma^{-1})\,u^s-1)$ and $L_p(\psi_n\chi\theta, s)$:

$$L_p(\psi_n\chi\theta,s)=\begin{cases} F(\chi\theta\psi_n(\sigma^{-1})\,u^s-1) & \text{if}\quad K_\infty\neq\mathscr{k}_\infty(\mu_{2p})\\ \dfrac{F(\chi\theta(\sigma^{-1})\,\psi_n(\sigma^{-1})\,u^s-1)}{\chi\theta(\sigma^{-1})\,\psi_n(\sigma^{-1})\,u^s-1} & \text{if}\quad K_\infty=\mathscr{k}_\infty(\mu_{2p}).\end{cases}$$

Combining this with (i) and (ii) yields

$$\prod_{\psi_n} L_p(\psi_n\chi\theta,0)\sim p^{(p^n-p^{n-1})\mu_F+\lambda_F}\times\begin{cases}1 & \text{if}\quad K_\infty\neq\mathscr{k}_\infty(\mu_{2p})\\ \dfrac{1}{p} & \text{if}\quad K_\infty=\mathscr{k}_\infty(\mu_{2p}),\end{cases}$$

whence Step 1 gives us

$$2^{(p^n-p^{n-1})[\mathscr{k}:\mathbb{Q}]}\times\frac{h_{K_n}/h_{\mathscr{k}_n}}{h_{K_{n-1}}/h_{\mathscr{k}_{n-1}}}\sim p^{(p^n-p^{n-1})\mu_F+\lambda_F}$$

Step 3. *The Polynomial* $f(T)$

Iwasawa has proved [W] that there are integers $\lambda_{\mathscr{k}}$, λ_K, $\mu_{\mathscr{k}}$, μ_K, $v_{\mathscr{k}}$, and v_K such that

$$h_{K_n}\sim p^{p^n\mu_K+n\lambda_K+v_K}\qquad\text{for}\quad n\gg 0$$

and

$$h_{\mathscr{k}_n}\sim p^{p^n\mu_{\mathscr{k}}+n\lambda_{\mathscr{k}}+v_{\mathscr{k}}}\qquad\text{for}\quad n\gg 0.$$

Moreover, the exactness of

$$1 \to B \to A_{K_\infty} \to A_{k_\infty} \to 1$$

yields

$$\lambda_f = \lambda_K - \lambda_k \qquad \text{and} \qquad \mu_f = \mu_K - \mu_k.$$

Hence

$$p^{(p^n - p^{n-1})\mu_f + \lambda_f} \sim \frac{h_{K_n}/h_{k_n}}{h_{K_{n-1}}/h_{k_{n-1}}} \qquad \text{for} \quad n \gg 0.$$

Combining this with the result of Step 2 we have

$$2^{(p^n - p^{n-1})[k:\mathbb{Q}]} p^{(p^n - p^{n-1})\mu_f + \lambda_f} \sim p^{(p^n - p^{n-1})\mu_F + \lambda_F} \qquad \text{for} \quad n \gg 0.$$

Therefore

$$\lambda_F = \lambda_f$$

and

$$\mu_F = \begin{cases} \mu_f & \text{if } p \text{ is odd} \\ \mu_f + [k:\mathbb{Q}] & \text{if } p = 2. \end{cases}$$

as desired.

IV. Remark

When k is a field for which Leopoldt's conjecture holds and $K_\infty = k_\infty(\mu_{2p})$, one can give an alternate proof of our result by looking at $F(u-1)$. It is based on a Kummer theoretic interpretation of B and class field theory (see [C], [F1], and [F2]).

References

[C] J. Coates, "p-Adic L-functions and Iwasawa Theory, in Algebraic Number Fields" (A. Frohlich, Ed.), Academic Press, New York, 1977, pp. 269–353.

[F1] L. J. Federer, "p-Adic L-functions, Regulators, and Iwasawa Modules," Ph.D. thesis, Princeton Univ., Princeton, N.J., 1982.

[F2] L. J. Federer, R-generalized S-class groups, Kummer theory, and characteristic power series, to appear.

[I] K. Iwasawa, "Lectures on p-adic L-Functions," Annals of Math. Studies, No. 74, Princeton Univ. Press, Princeton, 1972.

[K] Y. Kida, On cyclotomic $\mathbb{Z}_2$-extensions of J-fields, *J. Number Theory* **14** (1982), 340–352.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **32** (1984), 179–330.

[S] J. P. Serre, Sur le résidu de la function zeta p-adique d'un corps de nombres, *Comptes Rendus* **287** (1978), 183–188.

[W] L. Washington, "Introduction to Cyclotomic Fields," GTM 63, Springer-Verlag, Berlin, 1982.