Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 457–462

On Sinnott's Proof of the Vanishing of the Iwasawa Invariant μ_p

Lawrence C. Washington

To my teacher, Professor Iwasawa, on his seventieth birthday

In [3], W. Sinnott gave a new proof of the result of B. Ferrero and the present author [1] that the Iwasawa invariant μ_p vanishes for cyclotomic $\mathbb{Z}_p$-extensions of abelian number fields. The original proof was based on Iwasawa's construction of p-adic L-functions [2] and also used the concept of p-adic normal numbers. Sinnott replaced the results on normal numbers with a purely algebraic independence result (Lemma 2 below), which enabled him to work in the context of p-adic measures and distributions and to prove that (approximately) the μ-invariant of a rational function equals the μ-invariant of its Γ-transform. In the present note, we show that Sinnott's proof can be translated back into the language of Iwasawa power series. It is amusing to note that the step involving the Γ-transform, while not very difficult to begin with, is now replaced by the even simpler observation that if a prime divides the coefficients of a polynomial then it still divides them after a permutation of the exponents.

We first introduce the standard notation (see [4, p. 386] for more details): p is a prime; $q=4$ if $p=2$ and $q=p$ if p is odd; χ is an odd Dirichlet character of conductor f, where f is assumed to be of the form d or qd with $(d, p)=1$ (i.e., χ is a character of the first kind); $q_n=dqp^n$; $i(a)=-\log_p(a)/\log_p(1+q_0)$ for $a \in \mathbb{Z}_p$, where $\log_p$ is the p-adic logarithm; $\mathcal{O}=\mathbb{Z}_p[\chi(1), \chi(2), \cdots]$; (π) is the prime of $\mathcal{O}$; $\Lambda=\mathcal{O}[\![T]\!]$; $K=$field of fractions of $\mathcal{O}$; α runs through the $\phi(q)$-th (2nd or $(p-1)$-st) roots of unity in $\mathbb{Z}_p$; $\langle a\rangle$ is defined for $a \in \mathbb{Z}_p^\times$ by $a=\omega(a)\langle a\rangle$, where ω is the Teichmüller character; $\{y\}$ is the fractional part of $y \in \mathbb{Q}$; $\omega_n(T)=(1+T)^{p^n}-1$; and

$$B(y)=(1+q_0)\{y\}-\{(1+q_0)y\}-\frac{q_0}{2}.$$

Received December 24, 1987.
Revised April 25, 1988.
Research supported in part by N.S.F. and the Max-Planck-Institut für Mathematik, Bonn.

Note that

$$\sum_{py\equiv z \ (\mathrm{mod}\ \mathbf{Z})} B(y)=B(z)$$

for any z. Let

$$f_\alpha^n(T)=\sum_{\substack{a\equiv\alpha(q)\\ a\ (\mathrm{mod}\ q_n)}} B\left(\frac{a}{q_n}\right)\chi(a)(1+T)^{a(1+q_0)} \quad (\mathrm{mod}\ \omega_n(T)).$$

Since $f_\alpha^{n+1}(T)\equiv f_\alpha^n(T)(\mathrm{mod}\ \omega_n(T))$, there exists a power series $f_\alpha(T)\in\Lambda$ with $f_\alpha(T)\equiv f_\alpha^n(T)$ $(\mathrm{mod}\ \omega_n(T))$ for all $n\geq 0$.

Lemma 1.

$$f_\alpha(T)=\frac{(1+q_0)\sum_{\substack{0<a<q_0\\ a\equiv\alpha(q)}}\chi(a)(1+T)^{a(1+q_0)}-\sum_{\substack{0<a<q_0(1+q_0)\\ a\equiv\alpha(q)}}\chi(a)(1+T)^a}{(1+T)^{q_0(1+q_0)}-1}.$$

We postpone the proof until the end. Note that $f_\alpha(T)$ is a rational function and $f_\alpha(T)=f_{-\alpha}((1+T)^{-1}-1))$. Let

$$h_\alpha^n(T)=\sum_{\substack{a\equiv\alpha(q)\\ a\ (\mathrm{mod}\ q_n)}} B\left(\frac{a}{q_n}\right)\chi(a)(1+T)^{(\alpha^{-1}a-1)(1+q_0)/q} \quad (\mathrm{mod}\ \omega_n(T)).$$

Then, just as with $f_\alpha(T)$, there exists $h_\alpha(T)\in\Lambda$ with $h_\alpha(T)\equiv h_\alpha^n(T)$ $(\mathrm{mod}\ \omega_n(T))$ for all $n\geq 0$. It is easy to see that

$$(1+T)^{1+q_0}h_\alpha((1+T)^q-1)=f_\alpha((1+T)^{\alpha^{-1}}-1).$$

Finally, we state the crucial result of Sinnott.

Lemma 2 (Sinnott [3]). *For each $\phi(q)$-th root of unity α, let $F_\alpha(T)\in\Lambda\cap K(T)$. Suppose*

$$\sum_\alpha F_\alpha((1+T)^\alpha-1)\in\pi\Lambda.$$

Then there exist constants $c_\alpha\in\mathcal{O}$ such that

$$F_\alpha(T)+F_{-\alpha}((1+T)^{-1}-1)\equiv c_\alpha \quad (\mathrm{mod}\ \pi\Lambda)$$

for all α (see the appendix for a proof).

We can now give the proof that $\mu_p=0$. It is well known [4, p. 131] that $\mu_p=0$ for all abelian number fields if and only if $\mu_{\chi\omega}=0$ for all odd Dirichlet characters $\chi\neq\omega^{-1}$ of the first kind, where $\mu_{\chi\omega}$ is defined as follows. Let $\frac{1}{2}f(T, x\omega) \in \Lambda$ be the Iwasawa power series attached to the p-adic L-function $L_p(s, \chi\omega)$. Then $\mu_{\chi\omega}$ is the largest μ (possibly fractional) such that $p^{-\mu}\frac{1}{2}f(T, \chi\omega)$ is p-integral (with coefficients in some extension of $\mathcal{O}$). It is possible [4, p. 122] to write

$$f(T, \chi\omega) = \frac{g(T, \chi\omega)}{h(T, \chi\omega)}$$

where

$$h(T, \chi\omega) = 1 - \frac{1+q_0}{1+T} \quad \text{and} \quad \frac{1}{2}g(T, \chi\omega) \in \Lambda.$$

Since the μ-invariant of h is 0, it follows that $\frac{1}{2}f$ and $\frac{1}{2}g$ have the same μ-invariant. Iwasawa's construction of g [4, pp. 119–123] shows that

$$\frac{1}{2}g(T, \chi\omega) \equiv \frac{1}{2} \sum_{a \pmod{q_n}} \left((1+q_0)\left\{\frac{a}{q_n}\right\} - \left\{\frac{(1+q_0)a}{q_n}\right\}\right)\chi(a)(1+T)^{i(a)-1}$$
$$\mod (\pi, \omega_n(T))$$

for all $n \geq 0$. Since χ is odd we may insert a term $q_0/2$ and multiply by $1+T$ to obtain

$$(1+T)\frac{1}{2}g(T, \chi\omega) \equiv \frac{1}{2} \sum_{a \pmod{q_n}} B\left(\frac{a}{q_n}\right)\chi(a)(1+T)^{i(a)} \mod (\pi, \omega_n(T)).$$

Since $\omega_n(T) \equiv T^{p^n} \pmod{p}$, we find that

$$\mu_{\chi\omega} > 0 \Rightarrow \frac{1}{2} \sum_{a \pmod{q_n}} B\left(\frac{a}{q_n}\right)\chi(a)(1+T)^{i(a)} \equiv 0 \pmod{(\pi, \omega_n(T))}$$
$$\text{for all } n \geq 0.$$

Note that $i(a) \equiv i(b) \pmod{p^n} \Leftrightarrow \langle a \rangle \equiv \langle b \rangle \pmod{qp^n} \Leftrightarrow (\langle a \rangle - 1)/q \equiv (\langle b \rangle - 1)/q \pmod{p^n}$. Therefore, changing $i(a)$ to $(\langle a \rangle - 1)(1+q_0)/q$ (this is essentially the Γ-transform) permutes exponents mod p^n and does not affect divisibility by π. Consequently,

$$\mu_{\chi\omega} > 0 \Rightarrow \frac{1}{2} \sum_{a \pmod{q_n}} B\left(\frac{a}{q_n}\right)\chi(a)(1+T)^{(\langle a \rangle - 1)(1+q_0)/q} \equiv 0$$
$$\pmod{(\pi, \omega_n(T))} \text{ for all } n$$
$$\Rightarrow \frac{1}{2} \sum_{\alpha} h_\alpha(T) \equiv 0 \pmod{\pi}$$
$$\Rightarrow \frac{1}{2} \sum_{\alpha} h_\alpha((1+T)^q - 1) \equiv 0 \pmod{\pi}$$
$$(\text{since } (1+T)^q - 1 \equiv T^q \pmod{p})$$

$$\Rightarrow \frac{1}{2} \sum_{\alpha} f_\alpha((1+T)^{\alpha^{-1}}-1) \equiv 0 \pmod{\pi}$$

$$\Rightarrow f_\alpha(T) = \frac{1}{2} f_\alpha(T) + \frac{1}{2} f_{-\alpha}((1+T)^{-1}-1) \equiv b_\alpha \pmod{\pi}$$

for some constant $b_\alpha \in \mathcal{O}$, for all α. Let $\alpha=1$. The coefficient of $1+T$ in the numerator of $f_1(T)$ is $-\chi(1)=-1 \neq 0 \pmod{\pi}$. If $f_1(T) \equiv b_1 \pmod{\pi}$ then

$$((1+T)^{q_0(1+q_0)}-1)b_1 \equiv (\text{numerator}) \pmod{\pi},$$

which is impossible, since the left side does not have $1+T$ to the first power. This contradiction proves that $\mu_{\chi_\omega}=0$ for all χ, hence that $\mu_p=0$, as claimed.

We now prove Lemma 1. We have

$$((1+T)^{q_0(1+q_0)}-1)f_\alpha^n(T) \equiv \sum_\alpha \left(B\left(\frac{a-q_0}{q_n}\right)-B\left(\frac{a}{q_n}\right)\right)\chi(a)(1+T)^{a(1+q_0)} \pmod{\omega_n(T)}.$$

Working temporarily in $K[T]$ mod $\omega_n(T)$, we have

$$\sum_{a \equiv \alpha} \left(\left\{\frac{a-q_0}{q_n}\right\}-\left\{\frac{a}{q_n}\right\}\right)\chi(a)(1+T)^{a(1+q_0)}$$

$$= \sum_{\substack{0<a<q_0 \\ a\equiv\alpha(q)}} \chi(a)(1+T)^{a(1+q_0)} - \sum_{\substack{0<a<q_n \\ a\equiv\alpha(q)}} \frac{q_0}{q_n}\chi(a)(1+T)^{a(1+q_0)}$$

$$\equiv \sum_{\substack{0<a<q_0 \\ a\equiv\alpha(q)}} \chi(a)(1+T)^{a(1+q_0)} - \sum_{\substack{0<a<q_n \\ a\equiv\alpha(q)}} \frac{q_0}{q_n}\chi(a)(1+T)^{a}$$

(change a to $a(1+q_0)^{-1} \pmod{q_n}$ in the second sum). Also

$$\sum_{a \equiv \alpha} \left(\left\{\frac{a(1+q_0)-q_0(1+q_0)}{q_n}\right\}-\left\{\frac{a(1+q_0)}{q_n}\right\}\right)\chi(a)(1+T)^{a(1+q_0)}$$

$$\equiv \sum_{a} \left(\left\{\frac{a-q_0(1+q_0)}{q_n}\right\}-\left\{\frac{a}{q_n}\right\}\right)\chi(a)(1+T)^{a}$$

$$\equiv \sum_{\substack{0<a<q_0(1+q_0) \\ a\equiv\alpha(q)}} \chi(a)(1+T)^{a} - (1+q_0) \sum_{\substack{0<a<q_n \\ a\equiv\alpha(q)}} \frac{q_0}{q_n}\chi(a)(1+T)^{a}$$

(we assume $q_n > q_0(1+q_0)$). Therefore

$$((1+T)^{q_0(1+q_0)}-1)f_\alpha^n(T) \equiv (1+q_0) \sum_{\substack{0<a<q_0 \\ a\equiv\alpha(q)}} \chi(a)(1+T)^{a(1+q_0)} - \sum_{\substack{0<a<q_0(1+q_0) \\ a\equiv\alpha(q)}} \chi(a)(1+T)^{a}.$$

This congruence is in $K[T] \bmod \omega_n(T)$. By Gauss's Lemma, it is actually a congruence in $\Lambda \bmod \omega_n(T)$. Letting $n \to \infty$, we obtain Lemma 1.

Appendix. Proof of Lemma 2

For completeness, we include a proof of Lemma 2, following Sinnott [3].

Lemma A. *Let p be prime and let $\mathbb{F}$ be a field of characteristic p. Let $a_1, \cdots, a_n \in \mathbb{Z}_p$ be linearly independent over $\mathbb{Q}$. Then $(1+T)^{a_1}, \cdots, (1+T)^{a_n}$ are algebraically independent over $\mathbb{F}$ in $\mathbb{F}((T))$.*

Proof. Suppose we have a relation

$$\sum b_D(1+T)^{d_1a_1+\cdots+d_na_n}=0, \quad b_D \in \mathbb{F},$$

where the sum is over n-tuples of nonnegative integers and $b_D=0$ for almost all D. Changing $(1+T)$ to $(1+T)^x$, with $x \in \mathbb{Z}_p$ yields the relation

$$\sum b_D(1+T)^{(d_1a_1+\cdots+d_na_n)x}=0 \quad \text{for all } x \in \mathbb{Z}_p.$$

Since the exponents $d_1a_1+\cdots+d_na_n$ are all distinct by hypothesis, we may apply Artin's theorem on linear independence of characters to conclude that $b_D=0$ for all D.

Lemma B. *Let $\mathbb{F}$ be any field, let $X_1, \cdots, X_n, Z$ be independent indeterminates over $\mathbb{F}$, and let $Y_1, \cdots, Y_m$ be nontrivial elements of the subgroup of $\mathbb{F}(X_1, \cdots, X_n)^\times$ generated by $X_1, \cdots, X_n$. Assume in addition that $Y_i^a=Y_j^b$ with $i \neq j$ and $a, b \in \mathbb{Z}$ occurs only when $a=b=0$. Then a relation of the form*

$$r_1(Y_1)+\cdots+r_m(Y_m)=0 \quad \textit{with } r_j(Z) \in \mathbb{F}(Z)$$

can only happen when $r_j(Z) \in \mathbb{F}$ for all j.

Proof. We may enlarge $\mathbb{F}$ if necessary so that $\mathbb{F}^\times$ has an element t of infinite order. Suppose we have a relation in which not all r_j are constant and suppose m is chosen to be minimal. Then no r_j can be constant, otherwise we could shorten the relation. Since the X's are algebraically independent and the Y's are nontrivial, Y_1 is transcendental over $\mathbb{F}$. Therefore $m \geq 2$. We may write

$$Y_j=\prod_i X^{a_{ij}} \quad \text{with } a_{ij} \in \mathbb{Z}.$$

Since Y_1 and Y_2 are multiplicatively independent, there exist integers

$b_1, \cdots, b_n$ such that

$$\sum_i a_{i1}b_i=0, \qquad \sum_i a_{i2}b_i\neq 0.$$

In general, let $c_j=\sum a_{ij}b_i$. Changing X_i to $X_i t^{b_i}$ in the relation, then subtracting, yields

$$\sum_{j=2}^{m} r_j(Y_j)-r_j(Y_j t^{c_j})=0.$$

Since t has infinite order, $c_2\neq 0$, and r_2 is not constant, it follows easily that $r_2(Z)-r_2(Zt^{c_2})\notin \mathbb{F}$. Therefore we have a relation of length $m-1$, contradicting the minimality of m. This proves Lemma B.

We can now prove Lemma 2. Let $\mathbb{F}=\mathcal{O}/\pi\mathcal{O}$ and regard F_α as an element of $\mathbb{F}(T)$. Let A be the additive subgroup of $\mathbb{Z}_p$ generated by the set V of $\phi(q)$-th roots of unity. Let $a_1, \cdots, a_n$ be a $\mathbb{Z}$-basis for A and let $\eta_1, \cdots, \eta_m$ $(m=\frac{1}{2}\phi(q))$ be a set of representatives for V modulo ± 1. Let

$$X_i=(1+T)^{a_i},\ i=1, \cdots, n; \qquad Y_j=(1+T)^{\eta_j},\ j=1, \cdots, m,$$

and let

$$r_j(Z)=F_{\eta_j}(Z-1)+F_{-\eta_j}(Z^{-1}-1).$$

Lemma A implies that the X's are algebraically independent, and it is clear that the r's, X's, and Y's satisfy the hypotheses of Lemma B. Therefore Lemma 2 follows.

Remark. The proof of Lemma 2 given above and the proofs of the results on normal numbers used in [1] have certain formal similarities. It would be interesting to be able to deduce one from the other.

References

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

[2] K. Iwasawa, Lectures on p-adic L-functions, Annals of Math. Studies, Princeton Univ. Press, Princeton, N.J., 1972.

[3] W. Sinnott, On the μ-invariant of the Γ-transform of a rational function, Invent. math., **75** (1984), pp. 273–282.

[4] L. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

Department of Mathematics
University of Maryland
College Park, MD 20742
U.S.A.