COMPOSITIO MATHEMATICA

WARREN M. SINNOTT

On p-adic L-functions and the Riemann-Hurwitz genus formula

Compositio Mathematica, tome 53, nº 1 (1984), p. 3-17

<http://www.numdam.org/item?id=CM_1984__53_1_3_0>

Compositio Mathematica 53 (1984) 3–17.

ON p-ADIC L-FUNCTIONS AND THE RIEMANN-HURWITZ GENUS FORMULA

Warren M. Sinnott [1]

Introduction

Let p be a prime number, and let $\mathbb{Q}_\infty$ be the $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For any number field F, the compositum $F_\infty = F\mathbb{Q}_\infty$ is called the basic $\mathbb{Z}_p$-extension of F. Let F be a CM-field, with maximal real subfield F^+, and for each integer $n \geqslant 0$, let F_n be the unique extension of F in F_∞ of degree p^n over F. Let h_n^* denote the relative class number of F_n/F_n^+. The growth of $\mathrm{ord}_p(h_n^*)$ as $n \to \infty$ is described by a basic result of Iwasawa (cf. [8]):

$$\mathrm{ord}_p\left(h_n^*\right) = \mu^* p^n + \lambda^* n + \nu^*,$$

for certain integers $\mu^* \geqslant 0$, $\lambda^* \geqslant 0$, and ν^*, and for n sufficiently large.

In [11], Y. Kida proved a striking analogue of the classical Riemann-Hurwitz genus formula from the theory of compact Riemann surfaces, by describing the behavior of λ^* in p-extensions under the assumption $\mu^* = 0$. A special case of Kida's result is the following (for the most general formulation, see Theorem 4.1, below).

Let E be a CM-field which is a p-extension of F (i.e. if E' denotes the Galois closure of E over F, $\mathrm{Gal}(E'/F)$ is a p-group). Suppose that $p > 2$, and that F contains the p-th roots of unity. Finally suppose that $\mu_F^* = 0$. Then

$$2\lambda_E^* - 2 = [E_\infty : F_\infty]\left(2\lambda_F^* - 2\right) + \sum_w \left(e(w/v) - 1\right),$$

where w runs over (non-archimedean) places on E_∞ which do not lie above p and are split for the extension E_∞/E_∞^+. For each such w, v denotes its restriction to F_∞, and $e(w/v)$ denotes the ramification index of w over v.

Kida's proof uses classical techniques from algebraic number theory, namely genus theory for the fields F_n. Iwasawa [10] found a second proof, using Galois cohomology. Actually, Iwasawa proves more, determining, when E_∞/F_∞ is Galois, the representation of $\mathrm{Gal}(E_\infty/F_\infty)$ on the minus

[1] Partially supported by the National Science Foundation.

part of the Iwasawa module of E_∞, tensored with $\mathbb{Q}_p$. Iwasawa's result is thus an analogue for number fields of a theorem of Chevalley and Weil [3]. Kida's formula follows from Iwasawa's result by taking degrees.

In this paper, we give a third proof of Kida's formula, using the theory of p-adic L-functions. As this paper was being written, we discovered the earlier work of G. Gras [6,7], who used the Kubota-Leopoldt functions to prove Kida's formula when E and F are abelian over $\mathbb{Q}$. Thus the present paper may be viewed as an extension of Gras's approach to arbitrary CM-fields.

A brief statement of the results we need from the theory of p-adic L-functions is included in §2; given these results, the rest of the paper is relatively self-contained. In §3, we discuss the relation, due to Iwasawa, between the invariants μ^* and λ^* and p-adic L-functions. Finally, in §4, we show how to derive Kida's theorem from the results in §2 and §3.

§1. Preliminaries and notation

Let p be a prime number, which will remain fixed throughout. The units $\mathbb{Z}_p^\times$ of the p-adic integers $\mathbb{Z}_p$ can be written as an internal direct product

$$\mathbb{Z}_p^\times = V_p \cdot (1 + 2p\mathbb{Z}_p),$$

where V_p is the group of roots of unity in $\mathbb{Z}_p$, i.e. $|V_p| = p - 1$ if $p > 2$, and $|V_2| = 2$. The projections onto the first and second factors are denoted by ω and $\langle\ \rangle$, respectively.

Let G be a profinite abelian group; the completed group ring of G over $\mathbb{Z}_p$ will be denoted by Λ_G, and may be defined by $\Lambda_G = \varprojlim \mathbb{Z}_p[G/U]$, where U runs over the open subgroups of G. Following Mazur, the elements of Λ_G may be viewed as $\mathbb{Z}_p$-valued measures on G. If α is an element of Λ_G, and if $f\colon G \to R$ is a continuous map of G into a profinite $\mathbb{Z}_p$-module R, the integral of f with respect to α is defined by

$$\int_G f \mathrm{d}\alpha = \lim \sum_{g \bmod U} f(g)\alpha(gU).$$

If R is a profinite $\mathbb{Z}_p$-algebra, and $\chi\colon G \to R^\times$ a continuous homomorphism, χ indices a continuous homomorphism $\Lambda_G \to R$ which we again denote by χ. We have the integration formula

$$\int_G \chi \mathrm{d}\alpha = \chi(\alpha).$$

The notion of a pseudo-measure, introduced by Serre [13], will be useful in what follows. An element α of the total ring of fractions of Λ_G

satisfying $(1-g)\alpha \in \Lambda_G$ for all $g \in G$ is called a *pseudo-measure*. Let R be a profinite $\mathbb{Z}_p$-algebra, and suppose that R is an integral domain. If χ is a non-trivial homomorphism of G into $R^\times$, we may define

$$\int_G \chi \mathrm{d}\alpha = \int_G \chi \mathrm{d}\beta/(1-\chi(h)), \tag{1.1}$$

where $h \in G$ is chosen so that $\chi(h) \neq 1$, and $\beta = (1-h)\alpha$. The right hand side lies in the quotient field of R, and is independent of h.

Let $\mathfrak{o}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$, and let $f(T) = a_0 + a_1 T + a_2 T^2 + \ldots$ be a non-zero power series with coefficients in $\mathfrak{o}$. We define

$$\mu(f) = \min\{\mathrm{ord}_p a_i : i \geqslant 0\}$$

$$\lambda(f) = \min\{i \geqslant 0 : \mathrm{ord}_p a_i = \mu(f)\}.$$

Clearly we have $\mu(fg) = \mu(f) + \mu(g)$, $\lambda(fg) = \lambda(f) + \lambda(g)$, if f, g are non-zero elements of $\mathfrak{o}[[T]]$; we may use these relations to define μ and λ on the non-zero elements of the quotient field of $\mathfrak{o}[[T]]$.

Finally, if $F \subseteq E$ are fields, and if v is a place on E, then $v|F$ denotes the restriction of v to F.

§2. *p*-adic L-functions

Let K be a totally real number field, and let S be a finite set of (non-archimedean) places on K, containing the set S_p of places dividing p. The maximal abelian extension of K (in a fixed algebraic closure $\overline{K}$) unramified outside S and ∞ will be denoted by K_S, and we put $G_S = \mathrm{Gal}(K_S/K)$. Since $S \supseteq S_p$, K_S contains the group μ_{p^∞} of all p-power roots of unity. The action of G_S on μ_{p^∞} induces a character

$$\mathbb{N} : G_S \to \mathbb{Z}_p^\times,$$

via the formula

$$\zeta^\sigma = \zeta^{\mathbb{N}\sigma} \qquad \text{for} \quad \sigma \in G_S, \quad \zeta \in \mu_{p^\infty}.$$

The symbol $\mathbb{N}$ is used for the following reason. If $\mathfrak{a}$ is an ideal of K prime to S, let $\sigma_\mathfrak{a}$ denote the image of $\mathfrak{a}$ in G_S under the Artin map. Then we have

$$\mathbb{N}\sigma_\mathfrak{a} = \mathbb{N}\mathfrak{a},$$

where $\mathbb{N}\mathfrak{a}$ denotes as usual the absolute norm of $\mathfrak{a}$. Using the decomposition $x = \omega(x)\langle x\rangle$ $(x \in \mathbb{Z}_p^\times)$, we obtain from $\mathbb{N}$ two important characters of G_S:

$$\theta(\sigma) = \omega(\mathbb{N}\sigma), \quad \kappa(\sigma) = \langle \mathbb{N}\sigma\rangle.$$

The fixed field of the kernel of θ is $K(\mu_{2p})$; the fixed field of the kernel of κ is denoted by K_∞; it is the basic $\mathbb{Z}_p$-extension of K.

Let S_∞ denote the set of embeddings of K into $\mathbb{R}$. If v is such an embedding, we let σ_v denote the element of G_S corresponding to complex conjugation under any embedding $K_S \to \mathbb{C}$ extending v. Clearly

$$\mathbb{N}\sigma_v = -1, \quad v \in S_\infty.$$

If χ is any homomorphism of G_S into a field we call χ *even* if $\chi(\sigma_v) = 1$ for all $v \in S_\infty$, and *odd* if $\chi(\sigma_v) = -1$ for all $v \in S_\infty$. Thus $\mathbb{N}$ and θ are odd, but κ is even.

For any character χ of G_S of finite order, with values in $\mathbb{C}_p^\times$, we let $L_S^*(\chi, s)$ denote the p-adic L-function attached to χ. $L_S^*(\chi, s)$ is defined by means of the values of classical complex L-functions at negative integers, as follows. Let ψ be any character of G_S of finite order, with values in $\mathbb{C}_p^\times$, and let $k = \mathbb{Q}(\psi)$ denote the subfield of $\mathbb{C}_p$ generated by the values of ψ. Let $\rho: k \to \mathbb{C}$ be any embedding, so that $\rho \circ \psi$ is a $\mathbb{C}$-valued character of G_S. By a theorem of Siegel, the complex L-function value $L_S(\rho \circ \psi, 1-n)$ $(n = 1, 2, 3\ldots)$ lies in $\rho(k)$, and $\rho^{-1}L_S(\rho \circ \psi, 1-n)$ is *independent* of the choice of ρ. In view of this we denote $\rho^{-1}L_S(\rho \circ \psi, 1-n)$ simply by $L_S(\psi, 1-n)$. Then $L_S^*(\chi, s)$ is the (unique) continuous function of $s \in \mathbb{Z}_p - \{1\}$, with values in $\mathbb{C}_p$, satisfying

$$L_S^*(\chi, 1-n) = L_S(\chi\theta^{-n}, 1-n), \tag{2.1}$$

for $n = 1, 2, 3, \ldots$. It follows from the functional equation of the complex L-functions that $L_S^*(\chi, s)$ is not identically 0 only when χ is even.

The existence of p-adic L-functions was proved by Deligne and Ribet [4] and P. Cassou-Noguès [1], and their results also imply (Serre [13]) the existence of a pseudo-measure α_S on G_S such that

$$L_S^*(\chi, s) = \int_{G_S} \chi\kappa^{1-s} d\alpha_S, \tag{2.2}$$

for any character χ as above and any $s \in \mathbb{Z}_p$ (with $s \neq 1$ if $\chi = 1$).

We shall need the following consequence of (2.2). Since $\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, we may choose an element γ in the Sylow pro-p-subgroup of G_S whose restriction to K_∞ is a topological generator of $\mathrm{Gal}(K_\infty/K)$. Let Γ be the subgroup of G_S generated topologically by γ. Then $\Gamma \simeq \mathbb{Z}_p$, and G_S

is the internal direct product of the subgroups $A = \mathrm{Gal}(K_S/K_\infty)$ and Γ. Now let ϕ be the homomorphism of G_S into $\mathbb{Z}_p[[T]]^\times$ that is trivial on A and m aps γ to $\kappa(\gamma)(1+T)^{-1}$. Let χ be a character of G_S of finite order, with values in the ring of integers $\mathfrak{o}$ of a finite extension of $\mathbb{Q}_p$. Then $\chi\phi$ is a continuous function on G_S with values in $\mathfrak{o}[[T]]$, so we may integrate $\chi\phi$ with respect to the pseudo-measure α_S; we put

$$\tilde{L}_S(\chi, T) = \int_{G_S} \chi\phi \mathrm{d}\alpha_S. \tag{2.3}$$

$\tilde{L}_S(\chi, T)$ lies in the quotient field of $\mathfrak{o}[[T]]$, and, from (2.2), we have

$$L_S^*(\chi, s) = \tilde{L}_S(\chi, \kappa(\gamma)^s - 1).$$

Let ψ be a character of G_S trivial on A and of finite order. Then ψ is determined by $\psi(\gamma)$, which is a p-power root of unity. It follows immediately from (2.3) that

$$\tilde{L}_S(\chi\psi, T) = \tilde{L}_S\big(\chi, \psi(\gamma)^{-1}(1+T) - 1\big). \tag{2.4}$$

Let S' be a finite set of places on K containing S; if χ is a character of G_S, χ may be viewed as a character of $G_{S'}$ via the natural restriction map $G_{S'} \to G_S$. Then

$$L_{S'}^*(\chi, s) = L_S^*(\chi, s) \prod_{\mathfrak{p} \in S' \sim S} \big(1 - \chi\theta^{-1}(\sigma_\mathfrak{p})\langle \mathbb{N}\mathfrak{p}\rangle^{-s}\big),$$

as follows easily from (2.1) and the existence of an Euler product for the complex L-functions. It follows that

$$\tilde{L}_{S'}(\chi, T) = \tilde{L}_S(\chi, T) \prod_{\mathfrak{p} \in S' \sim S} E_\mathfrak{p}(T), \tag{2.5}$$

where $E_\mathfrak{p}(T)$ is the element of $\mathfrak{o}[[T]]$ satisfying

$$E_\mathfrak{p}\big(\kappa(\gamma)^s - 1\big) = 1 - \chi\theta^{-1}(\sigma_\mathfrak{p})\langle \mathbb{N}\mathfrak{p}\rangle^{-s}$$

Explicitly, define $t = t(\sigma_\mathfrak{p}) \in \mathbb{Z}_p$ by

$$\sigma_\mathfrak{p} \equiv \gamma^t \bmod A.$$

Since κ is trivial on A, this implies

$$\kappa(\sigma_\mathfrak{p}) = \langle \mathbb{N}\mathfrak{p}\rangle = \kappa(\gamma)^t,$$

and therefore

$$E_{\mathfrak{p}}(T) = 1 - \chi\theta^{-1}(\sigma_{\mathfrak{p}})(1+T)^{-t}, \quad t = t(\sigma_{\mathfrak{p}}). \tag{2.6}$$

We can use (2.5) and (2.6) to see how the μ and λ invariants of $\tilde{L}_S(\chi, T)$ change when S is replaced by S'. For brevity, let

$$\mu_S(\chi) = \mu(\tilde{L}_S(\chi, T)),$$

$$\lambda_S(\chi) = \lambda(\tilde{L}_S(\chi, T)),$$

when χ is even (so that $\tilde{L}_S(\chi, T) \neq 0$). Then we have the following lemma.

LEMMA 2.1: *Let χ be an even character of G_S, of finite order, and let S' be a finite set of places of K containing S. Then*

$$\mu_{S'}(\chi) = \mu_S(\chi),$$

and

$$\lambda_{S'}(\chi) = \lambda_S(\chi) + \sum_{\mathfrak{p}}{}' g(\mathfrak{p}),$$

where the summation is taken over places $\mathfrak{p}$ in $S' \sim S$ such that $\chi\theta^{-1}(\sigma_{\mathfrak{p}})$ has p-power order and $g(\mathfrak{p})$ denotes the number of places of K_∞ lying above $\mathfrak{p}$.

PROOF: It is well known (and is proved again below) that $g(\mathfrak{p})$ is finite for any non-archimedean place $\mathfrak{p}$ on K. Let $\mathfrak{p} \in S' \sim S$, and write

$$-t(\sigma_{\mathfrak{p}}) = p^a \cdot u \qquad a \geqslant 0, \quad u \in \mathbb{Z}_p^\times.$$

Then

$$E_{\mathfrak{p}}(T) \equiv 1 - \chi\theta^{-1}(\sigma_{\mathfrak{p}})(1 + T^{p^a})^u \bmod p\mathfrak{o}[[T]]$$

$$\equiv 1 - \chi\theta^{-1}(\sigma_{\mathfrak{p}}) - \chi\theta^{-1}(\sigma_{\mathfrak{p}})uT^{p^a} \bmod\left(p, T^{p^a+1}\right)\mathfrak{o}[[T]].$$

It follows that

$$\mu\left(E_{\mathfrak{p}}(T)\right) = 0,$$

$$\begin{aligned} \lambda\left(E_{\mathfrak{p}}(T)\right) &= p^a && \text{if } \chi\theta^{-1}(\sigma_{\mathfrak{p}}) \text{ is a } p\text{-power root of unity} \\ &= 0 && \text{otherwise.} \end{aligned}$$

Now, the decomposition group $D_{\mathfrak{p}}$ of $\mathfrak{p}$ for the extension K_∞/K is generated (topologically) by

$$\sigma_{\mathfrak{p}}|_{K_\infty} \equiv \gamma^{t(\sigma_{\mathfrak{p}})} \equiv \gamma^{-p^a u} \bmod A.$$

It follows that the index of $D_{\mathfrak{p}}$ in $\mathrm{Gal}(K_\infty/K)$ is p^a. Thus $g(\mathfrak{p})$ is finite and equal to p^a, as desired. This completes the proof.

The main result of this section is the following proposition, which gives some information on $\mu_S(\chi)$ and $\lambda_S(\chi)$ when χ is varied.

PROPOSITION 2.1: *Let χ be an even character of G_S of finite order, and ψ an even character of G_S of p-power order. First suppose that $p > 2$. Then*

$$\mu_S(\chi) = 0 \qquad \text{if and only if} \qquad \mu_S(\chi\psi) = 0,$$

in which case

$$\lambda_S(\chi) = \lambda_S(\chi\psi).$$

If $p = 2$, $\mu_S(\chi)$ and $\mu_S(\chi\psi)$ are at least equal to $d = [K:\mathbf{Q}]$. However

$$\mu_S(\chi) = d \qquad \text{if and only if} \qquad \mu_S(\chi\psi) = d,$$

in which case we have again

$$\lambda_S(\chi) = \lambda_S(\chi\psi).$$

PROOF: Let $\mathfrak{o}$ be the ring of integers in a finite extension of $\mathbf{Q}_p$ containing the values of both χ and ψ, and let π be a local parameter in $\mathfrak{o}$.

First suppose $p > 2$. Let $\beta = (1-\gamma)\alpha_S$. Then β is a *measure* on G_S, so we have the congruence

$$\int_{G_S} \chi\psi\phi \mathrm{d}\beta \equiv \int_{G_S} \chi\phi \mathrm{d}\beta \bmod \pi\mathfrak{o}[[T]].$$

Hence, by (1.2) and (2.3),

$$(1-\chi\psi\phi(\gamma))\tilde{L}_S(\chi\psi, T) \equiv (1-\chi\phi(\gamma))\tilde{L}_S(\chi, T) \bmod \pi\mathfrak{o}[[T]]. \tag{2.7}$$

Now $\chi(\gamma)$, $\psi(\gamma)$ are p-power roots of unity (since $\Gamma \simeq \mathbb{Z}_p$), and $\kappa(\gamma) \equiv$

1 mod p. Hence

$$1-\chi\psi\phi(\gamma)\equiv 1-\chi\phi(\gamma)\equiv 1-(1+T)^{-1} \bmod \pi\mathfrak{o}[[T]]$$

so these power series have μ-invariant 0 and λ-invariant 1. Hence (2.7) shows that

$$\mu_S(\chi\psi)=0 \qquad \text{if and only if} \qquad \mu_S(\chi)=0,$$

and, if this is the case,

$$\lambda_S(\chi\psi)=\lambda_S(\chi),$$

as desired.

When $p=2$, the argument is almost the same, but we need some additional results, due to Deligne and Ribet, on the 2-divisibility of 2-adic L-functions. Let H be the subgroup of G_S generated by the "real Frobenii" σ_v, $v\in S_\infty$. H is a finite group of exponent 2. Then the following fact is proved in [4] (see also Ribet [12]): the direct image $\overline{\beta}$ of the measure $\beta=(1-\gamma)\alpha_S$ under the map $G_S\to G_S/H$ is divisible by 2^d (i.e. $2^{-d}\overline{\beta}$ takes values in $\mathbb{Z}_2$). Since χ and ϕ are both *even* characters of G_S, we have that

$$2^{-d}(1-\chi\phi(\gamma))\tilde{L}_S(\chi,T)=\int_{G_S/H}\chi\phi \mathrm{d}(2^{-d}\overline{\beta})$$

lies in $\mathfrak{o}[[T]]$. Since $\mu(1-\chi\phi(\gamma))=0$, this shows $\mu_S(\chi)\geqslant d$. Similarly, since ψ is even, $\mu_S(\chi\psi)\geqslant d$. The rest of the argument proceeds as above, with G_S replaced by G_S/H and $\beta=(1-\gamma)\alpha_S$ by $2^{-d}\overline{\beta}$. This concludes the proof.

Let χ and S be as above. If S is as small as possible, i.e. if S consists precisely of the places dividing p and the places for which χ is ramified, we omit the subscript S from our notations: thus $L^*(\chi,s)$, $\mu(\chi)$, $\lambda(\chi)$, etc.. With this notation, we summarize the results of this section in the following theorem.

THEOREM 2.1: *Let χ and ψ be even characters of* $\mathrm{Gal}(K^{ab}/K)$ *of finite order, and suppose that the order of ψ is a power of p. Then $\mu(\chi)\geqslant$ $d\,\mathrm{ord}_p(2)$, $\mu(\chi\psi)\geqslant d\,\mathrm{ord}_p(2)$, and*

$$\mu(\chi)=d\,\mathrm{ord}_p(2) \qquad \text{if and only if} \qquad \mu(\chi\psi)=d\,\mathrm{ord}_p(2).$$

Now suppose that $\mu(\chi)=\mu(\chi\psi)=d\,\mathrm{ord}_p(2)$, and that the order of χ is prime to p. Let L be the extension of K corresponding to $\chi\theta^{-1}$ (resp. χ if

$p = 2$), *and put* $L_\infty = LK_\infty$. *Then*

$$\lambda(\chi\psi) = \lambda(\chi) + N,$$

where N *is the number of places* v *on* K_∞ *satisfying the conditions*

(i) v *does not lie above* p, *and* $v|K$ *is ramified for* ψ.

(ii) v *splits completely in* L_∞.

PROOF: The statement about the μ-invariants is immediate from Lemma 2.1 and Proposition 2.1.

Let S (resp. T) be the set of places of K that either divide p or are ramified for χ (resp. $\chi\psi$). Since χ and ψ have relatively prime orders, T contains S. By Proposition 2.1 and Lemma 2.1,

$$\lambda(\chi\psi) = \lambda_T(\chi\psi) = \lambda_T(\chi) = \lambda(\chi) + M,$$

where $M = \Sigma'_{\mathfrak{p}} g(\mathfrak{p})$, the summation taken over those places $\mathfrak{p}$ in $T \sim S$ for which $\chi\theta^{-1}(\sigma_{\mathfrak{p}})$ has p-power order. Since χ is here assumed to have order prime to p, and θ has order prime to p if $p > 2$ (and order $2 = p$ if $p = 2$), this condition on $\mathfrak{p}$ may be restated as $\chi\theta^{-1}(\sigma_{\mathfrak{p}}) = 1$ (resp. $\chi(\sigma_{\mathfrak{p}}) = 1$ if $p = 2$), i.e. $\mathfrak{p}$ splits completely in L. This last is, for any extension v of $\mathfrak{p}$ to K_∞, equivalent to the assertion that v splits completely in L_∞, and $g(\mathfrak{p})$ is by definition the number of extensions of $\mathfrak{p}$ to K_∞. So M is the number of places v on K_∞ which split completely in L_∞ and satisfy $v|K \in T \sim S$. Such v satisfy (i) and (ii); conversely if a place v on K_∞ satisfies (i) and (ii), then v splits completely in L_∞, and $v|K$ lies in T ($v|K$ ramified for ψ implies $v|K$ ramified for $\chi\psi$, since χ and ψ have relatively prime orders) but not in S (for $v|K$ splits completely in L). This completes the proof.

§3. The analytic class number formula

Let F be any number field, $\zeta(F, s)$ its zeta function. The functional equation for $\zeta(F, s)$ and the formula for the residue of $\zeta(F, s)$ at $s = 1$ together imply that

$$\lim_{s \to 0} \zeta(F, s)/s^{r_1 + r_2 - 1} = -hR/w. \tag{3.1}$$

Here, as usual, r_1 denotes the number of real embeddings, r_2 the number of complex embeddings, h the class number, R the regulator, and w the number of roots of unity of F.

Now let F be a CM-field, with maximal real subfield F^+. Let ϵ be the quadratic character of F^+ corresponding to the extension F/F^+. Then we have a factorization

$$\zeta(F, s) = \zeta(F^+, s)L(\epsilon, s).$$

Applying (3.1) also to the field F^+, we find that

$$L(\epsilon, 0) = 2^d h^* / wQ.$$

Here d is the degree of F^+ over $\mathbb{Q}$, h^* is the relative class number of F/F^+, w is as above the number of roots of unity in F, and Q denotes the index $[E : WE^+]$, where E (resp. E^+) is unit group of F (resp. F^+), and W is the group of roots of unity in F. Hence

$$h^* = wQ2^{-d}L(\epsilon, 0); \tag{3.2}$$

this formula is called the analytic class number formula for h^*.

Let p be a prime number, $\mathbb{Q}_\infty$ the $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and let $F_\infty = F\mathbb{Q}_\infty$. For each integer $n \geqslant 0$, there is a unique extension F_n of F in F_∞ of degree p^n over F. Each F_n is again a CM-field, and we may use (3.2) to obain information on the behavior of the relative class number h_n^* of F_n/F_n^+ as n varies.

We will use a subscript n to refer to objects attached to F_n. From (3.2), we have

$$h_n^* = w_n Q_n 2^{-d_n} L(\epsilon_n, 0) = w_n Q_n 2^{-d_n} \prod_{\psi} L(\epsilon\psi, 0);$$

the product on the right is taken over all characters ψ of $\mathrm{Gal}(F_n^+/F^+)$, and the L-functions on the right are attached to F^+. Clearly $d_n = dp^n$ for $n \geqslant 0$; the behavior of W_n and Q_n is also predictable, at least for n large:

LEMMA 3.1: *There is an integer $n_0 \geqslant 0$ such that*

$$(a)\ w_n = w_{n_0} p^{(n-n_0)\delta}, \quad \textit{for } n \geqslant n_0, \textit{ where } \delta = 0 \textit{ or } 1.$$
$$(b)\ Q_n = Q_{n_0}, \quad \textit{for } n \geqslant n_0.$$

COROLLARY: *For $n \geqslant n_0$,*

$$h_n^* = h_{n_0}^* p^{(n-n_0)\delta} \prod_{\psi}{}' 2^{-d} L(\epsilon\psi, 0), \tag{3.3}$$

the product taken over all characters ψ of $\mathrm{Gal}(F_n^+/F^+)$ *that are non-trivial on* $\mathrm{Gal}(F_n^+/F_{n_0}^+)$.

PROOF: The corollary is immediate from the lemma and (3.2). To see part (a) of the lemma, suppose first that the number of roots of unity in F_∞ is finite. It is then clear that w_n is independent of n for n large, say $n \geqslant n_0$, i.e. (a) holds with $\delta = 0$. Now suppose that the number of roots of unity in F_∞ is infinite. The group of roots of unity of order prime to p in F_∞ is finite in any case, and so lies in F_{n_0} for some $n_0 > 0$. Hence w_n/w_{n_0} is a power of p for $n \geqslant n_0$. It is easy to check by Galois theory that we must have $F_n = F_{n_0}(\mu_{p^{n-n_0}w_{n_0}})$ for $n \geqslant n_0$, and this implies (a) with $\delta = 1$.

To prove (b), we need the following description of Q. Let j denote the nontrivial automorphism of F/F^+; j corresponds under any embedding $F \hookrightarrow \mathbb{C}$ to complex conjugation. Hence, by a theorem of Kronecker, η^{1-j} is a root of unity for any unit $\eta \in E$. From this it follows that $E/WE^+ \simeq E^{1-j}/W^2 \subseteq W/W^2$. Hence Q is either 1 or 2, and $Q = 2$ if and only if $E^{1-j} = W$. It is immediate from this description that the following two implications are valid, for any $m \geqslant n \geqslant 0$:

(1) Suppose that the inclusion $W_n \hookrightarrow W_m$ is surjective on the 2-power roots of unity. Then $Q_n = 2$ implies $Q_m = 2$.

(2) Suppose that the norm map from W_m to W_n is surjective. Then $Q_m = 2$ implies $Q_n = 2$.

Now, if the number of 2-power roots of unity in F_∞ is finite, (1) may be used, provided that n is sufficiently large; on the other hand, if the number of 2-power roots of unity in F_∞ is infinite, then $p = 2$, and it is well known that the norm maps W_m onto W_n for $m \geqslant n > 0$, so (2) applies. In either case, we see easily that Q_n is independent of n for n sufficiently large. This completes the proof.

Remark: The above proof shows that $\delta = 1$ occurs precisely if F_∞ contains all the p-power roots of unity. An equivalent formulation in terms of characters is as follows. F_∞ contains the p-power roots of unity if it contains μ_p (resp. μ_4 if $p = 2$). If p is odd, $F^+(\mu_p)$ is then an extension of F^+ in F_∞ of degree prime to p, hence $F = F^+(\mu_p)$, and so $\epsilon\theta = 1$. Thus $\delta = 1$ if and only if $\epsilon\theta = 1$ (when p is odd).

If $p = 2$, let ψ denote the non-trivial character of F_1^+/F^+, F_1^+ being of course the first layer of the $\mathbb{Z}_p$-extension F_∞^+/F^+. If F_∞ contains the 2-power roots of unity, the $F^+(\mu_4)$ is an imaginary quadratic extension of F^+ in F_∞; hence $\theta = \epsilon$ or $\epsilon\psi$. So, when $p = 2$, $\delta = 1$ is equivalent to $\epsilon\theta = 1$ or ψ.

We use (3.3) to relate the μ^* and λ^* invariants of the $\mathbb{Z}_p$-extension F_∞/F to the μ and λ invariants of certain p-adic L-functions. In fact, Iwasawa [9] showed that, when F is a cyclotomic field, one could give a proof of the existence of μ^* and λ^* from (3.3), using the Kubota-Leopoldt functions; and Coates [2] pointed out that the standard properties of p-adic L-functions would make the proof work in general (see also [5]).

Proposition 3.1: *There are integers* $\mu^* \geqslant 0$, $\lambda^* \geqslant 0$ *and* ν^* *such that*

$$\mathrm{ord}_p(h_n^*) = \mu^* p^n + \lambda^* n + \nu^*,$$

for n sufficiently large. In fact

$$\mu^* = \mu_S(\epsilon\theta) - d\,\mathrm{ord}_p(2)$$

$$\lambda^* = \lambda_S(\epsilon\theta) + \delta,$$

where δ is defined in Lemma 3.1, *and S is the set of places of F^+ that ramify in F_∞.*

PROOF: Let n_0 be sufficiently large, so that the conclusions of Lemma 3.1 hold; we may suppose also that $F_\infty^+/F_{n_0}^+$ is totally ramified at all places dividing p. If ψ is a character of finite order of $\mathrm{Gal}(F_\infty^+/F^+)$, with values in $\mathbb{C}_p^\times$, non-trivial on $\mathrm{Gal}(F_\infty^+/F_{n_0}^+)$, then S (as defined in Proposition 3.1) is precisely the set of places for which $\epsilon\psi$ is ramified. Hence, by (2.1), we have,

$$L(\epsilon\psi, 0) = L_S^*(\epsilon\psi\theta, 0) = \tilde{L}_S\big(\epsilon\theta, \psi(\gamma)^{-1} - 1\big). \tag{3.4}$$

The second equality comes from (2.4).

Now let $n \geqslant n_0$, and combine (3.3) and (3.4). As ψ varies over characters of $\mathrm{Gal}(F_n^+/F^+)$ that are nontrivial on $\mathrm{Gal}(F_n^+/F_{n_0}^+)$, $\psi(\gamma)^{-1}$ will vary over roots of unity ζ in $\mathbb{C}_p^\times$ satisfying $\zeta^{p^n} = 1$, $\zeta^{p^{n_0}} \neq 1$. Hence

$$h_n^* = h_{n_0}^* p^{(n-n_0)\delta} \prod_\zeta{}' 2^{-d} \tilde{L}_S(\epsilon\theta, \zeta - 1), \tag{3.5}$$

with ζ satisfying $\zeta^{p^n} = 1$, $\zeta^{p^{n_0}} \neq 1$. Now if the order of ζ is p^m, and if m is sufficiently large, it is easy to see that

$$\begin{aligned}\mathrm{ord}_p \tilde{L}_S(\epsilon\theta, \zeta - 1) &= \mu_S(\epsilon\theta) + \lambda_S(\epsilon\theta)\ \mathrm{ord}_p(\zeta - 1)\\ &= \mu_S(\epsilon\theta) + \lambda_S(\epsilon\theta)/\big(p^{m-1}(p-1)\big).\end{aligned}$$

Hence, increasing n_0 if necessary, we have from (3.5)

$$\mathrm{ord}_p h_n^* = \big(\mu_S(\epsilon\theta) - d\,\mathrm{ord}_p(2)\big)p^n + \big(\lambda_S(\epsilon\theta) + \delta\big)n + C,$$

for $n \geqslant n_0$ and some integer C independent of n. This completes the proof of the proposition.

§4. Kida's formula

Let F be a CM-field with maximal real subfield F^+, and let E be a CM-field which is a p-extension of F (i.e. if E' is the Galois closure of E over F, then $\mathrm{Gal}(E'/F)$ is a p-group). Wherever appropriate we use subscripts E and F to distinguish between objects attached to E and those attached to F. The aim of this section is to prove the following theorem of Y. Kida [11]:

THEOREM 4.1: $\mu_F^* = 0$ *if and only if* $\mu_E^* = 0$, *and when this is the case*,

$$\lambda_E^* - \delta_E = [E_\infty : F_\infty](\lambda_F^* - \delta_F) + \sum_{w'} (e(w'/v') - 1) - \sum_{w} (e(w/v) - 1),$$

the summations taken over all places w' on E_∞ (resp. w on E_∞^+) which do not lie above p, and $v' = w'|F_\infty$ (resp. $v = w|F_\infty^+$).

PROOF: If $F \subseteq E \subseteq D$ is a tower of CM-fields, with D/F a p-extension, it is easy to check that if the theorem holds for any two of the extensions E/F, D/E, D/F, it holds for the third. This allows us to reduce first to the case E/F Galois and then to the case E/F cyclic of degree p. Hence we suppose that E/F is cyclic of degree p in the following.

If $E = F_1$ (the first layer of the basic $\mathbb{Z}_p$-extension F_∞/F), it is immediately that

$$\mu_E^* = p\mu_F^*, \quad \lambda_E^* = \lambda_F^*, \quad \delta_E = \delta_F,$$

so the theorem is valid in this case.

Now suppose that $E \cap F_\infty = F$. The extension of E^+ corresponding to the character $\epsilon_E \theta_E$ is contained in $E(\mu_{2p})$, hence is abelian over F^+ Hence we have a factorization

$$L^*(\epsilon_E \theta_E, s) = \prod_\psi L^*(\epsilon_F \theta_F \psi, s), \tag{4.1}$$

with ψ running over the characters of $\mathrm{Gal}(E^+/F^+)$. Since $E \cap F_\infty = F$, we have an isomorphism $\mathrm{Gal}(E_\infty/E) \simeq \mathrm{Gal}(F_\infty/F)$ under restriction, so we may choose a topological generator γ_E of $\mathrm{Gal}(E_\infty/E)$ such that $\gamma_F = \gamma_E | F_\infty$ is a topological generator of $\mathrm{Gal}(F_\infty/F)$. From this it is clear that (4.1) implies

$$\tilde{L}(\epsilon_E \theta_E, T) = \prod_\psi \tilde{L}(\epsilon_F \theta_F \psi, T). \tag{4.2}$$

Let $d = [F^+ : \mathbb{Q}]$, so that $[E^+ : \mathbb{Q}] = pd$. Taking μ-invariants in (4.2) and subtracting $pd\,\mathrm{ord}_p(2)$ from both sides, we obtain

$$\mu(\epsilon_E \theta_E) - pd\,\mathrm{ord}_p(2) = \sum_\psi \mu(\epsilon_F \theta_F \psi) - d\,\mathrm{ord}_p(2).$$

By Theorem 2.1, the left hand side and each term on the right is nonnegative; moreover, the terms on the right are either all positive or all 0. Hence $\mu(\epsilon_E\theta_E) = pd\ \mathrm{ord}_p(2)$ if and only if $\mu(\epsilon_F\theta_F) = d\ \mathrm{ord}_p(2)$, or, by Proposition 3.1, $\mu_E^* = 0$ if and only if $\mu_F^* = 0$. Thus the first part of the theorem is proved.

We suppose now that $\mu_E^* = \mu_F^* = 0$. Taking λ-invariants in (4.2), we find

$$\lambda(\epsilon_E\theta_E) = \sum_{\psi}\lambda(\epsilon_F\theta_F\psi). \tag{4.3}$$

At this point it is convenient to separate the cases $p > 2$ and $p = 2$. Suppose $p > 2$. By Theorem 2.1, with $K = F^+$ and $\chi = \epsilon_F\theta_F$,

$$\lambda(\epsilon_F\theta_F\psi) = \lambda(\epsilon_F\theta_F) + N, \qquad \text{if} \quad \psi \neq 1,$$

where N is the number of places v on F_∞^+ such that (i) $v|F^+$ does not divide p but is ramified for ψ, and (ii) v splits in F_∞. Thus

$$\lambda(\epsilon_E\theta_E) = p\lambda(\epsilon_F\theta_F) + (p-1)N.$$

However, any place v on F^+ satisfying (i) ramifies in E_∞^+, and so has a unique extension w on E_∞^+, and $e(w/v) = p$. From this it is easy to see that the formula of the theorem holds for E/F, using Proposition 3.1.

Now suppose $p = 2$. Applying Theorem 2.1 with $\chi = 1$ we find

$$\lambda(\epsilon_F\theta_F) = \lambda(1) + N, \quad \lambda(\epsilon_F\theta_F\psi) = \lambda(1) + N',$$

where N (resp. N') is the number of places v on F_∞^+ such that $v|F^+$ does not divide 2 but is ramified for $\epsilon_F\theta_F$ (resp. $\epsilon_F\theta_F\psi$). Here ψ denotes the non-trivial character of E^+/F^+. The second condition is vacuous in this case. Eliminating $\lambda(1)$ and continuing as above, we find

$$\lambda(\epsilon_E\theta_E) = 2\lambda(\epsilon_F\theta_F) + N' - N.$$

In view of Proposition 3.1, we have only to show that

$$N' - N = \sum_{w'}\left(e(w'/v') - 1\right) - \sum_{w}\left(e(w/v) - 1\right) \tag{4.4}$$

where w' (resp. w) runs over places of E_∞ (resp. E_∞^+) not dividing 2, and $v' = w'|F_\infty$, $v = w|F_\infty^+$. This can be seen as follows. If v is a place on F_∞^+ not dividing 2, let $N(v) = 1$ if $v|F^+$ is ramified for ϵ_F, and put $N(v) = 0$ otherwise; similarly let $N'(v) = 1$ if $v|F^+$ is ramified for $\epsilon_F\psi$, $N'(v) = 0$

otherwise. Since θ_F is ramified only for the primes above 2, we have

$$N = \sum_v N(v), \quad N' = \sum_v N'(v),$$

where v runs over the places on F_∞^+ that do not divide 2. For any such v, let L_v be the fixed field of the inertia group of v for the extension E_∞/F_∞^+. There are five possibilities for L_v; a case by case examination shows that

$$N'(v) - N(v) = \sum_{w'} \left(e(w'/v') - 1 \right) - \sum_{w} \left(e(w/v) - 1 \right),$$

the summations on the right taken over the places w' on E_∞ (resp. places w on E^+) lying over v; we note that v always splits completely in L_v (the residue field of F_∞^+ at v contains the maximal 2-extension of the prime field). Summing over places v that do not lie above 2, we obtain (4.4). This concludes the proof.

References

[1] P. Cassou-Noguès: Valeurs aux entiers négatifs des fonctions zêta et fonctions zêta p-adiques. *Inv. Math. 51* (1979) 29–59.

[2] J. Coates: p-adic L-functions and Iwasawa theory. In: *Algebraic Number Fields*, ed. by A. Fröhlich, Academic Press, New York (1977) pp. 269–353.

[3] C. Chevalley and A. Weil: Über das Verhalten der Integrale erster Gattung bei Automorphismen des Funktionenkörpers. *Hamb. Abh. 10* (1934) 358–361.

[4] P. Deligne and K. Ribet: Values of abelian L-functions at negative integers over totally real fields. *Inv. Math. 59* (1980) 227–286.

[5] Leslie Jane Federer: Ph.D. thesis, Princeton Univ., Princeton, 1982.

[6] G. Gras, Sur la construction des fonctions L p-adiques abéliennes, Seminaire Delange-Pisot-Poitou (Théorie des nombres), 1978/79, n° 22.

[7] G. Gras, Sur les invariants lambda d'Iwasawa des corps abéliens. *Pub. Math. de la Fac. des Sci. de Besançon* (1978/79).

[8] K. Iwasawa: On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc. 65* (1959) 183–226.

[9] K. Iwasawa: Lectures on p-adic L-functions. *Ann. Math. Studies 74*, Princeton University Press, Princeton (1972).

[10] K. Iwasawa: Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tôhoku Math. J.* (Second Series) *33(2)* (1981) 263–288.

[11] Y. Kida: l-extensions of CM-fields and cyclotomic invariants. *J. Number Theory 12* (1980) 519–528.

[12] K. Ribet: Report on p-adic L-functions over totally real fields. Soc. Math. de France, *Astérisque 61* (1979) 177–192.

[13] J.-P. Serre: Sur le résidu de la fonction zêta p-adique d'un corps de nombres. *C.R. Acad. Sc. Paris 287* (1978) 183–188.

(Oblatum 5-VIII-1982)

Institute for Advanced Study
Olden Lane
Princeton, NJ 08540
USA

Current address:

Department of Mathematics
Ohio State University
Columbus, OH 43210
USA