WARREN M. SINNOTT

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

Compositio Mathematica, tome 53, n° 1 (1984), p. 3-17

<http://www.numdam.org/item?id=CM_1984__53_1_3_0>
ON \textsc{p}-ADIC L-FUNCTIONS AND THE RIEHMANN-HURWITZ
GENUS FORMULA

Warren M. Sinnott

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 \( n \geq 0 \), let \( F_n \) be the unique extension of \( F \) in \( F_\infty \) of degree \( p^n \) over \( F \). Let \( h_n^* \) denote the relative class number of \( F_n/F^{+^n} \). The growth of \( \text{ord}_p(h_n^*) \) as \( n \to \infty \) is described by a basic result of Iwasawa (cf. \([8]\)):

\[
\text{ord}_p(h_n^*) = \mu^* p^n + \lambda^* n + \nu^*,
\]

for certain integers \( \mu^* \geq 0, \lambda^* \geq 0, \) and \( \nu^* \), 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 \( \lambda^* \) 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 \( F \), \( \text{Gal}(E'/F) \) is a \( p \)-group). Suppose that \( p > 2 \), and that \( F \) contains the \( p \)-th roots of unity. Finally suppose that \( p \equiv q \). Then

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

where \( w \) runs over (non-archimedean) places on \( E_\infty \) which do not lie above \( p \) and are split for the extension \( E_\infty/E^{+^\infty} \). For each such \( w, v \) denotes its restriction to \( F_\infty \), 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 \( E_\infty/F_\infty \) is Galois, the representation of \( \text{Gal}(E_\infty/F_\infty) \) 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 $\mu^*$ and $\lambda^*$ 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 $\mathbb{Z}_p^*$ of the $p$-adic integers $\mathbb{Z}_p$ can be written as an internal direct product

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

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 $\omega$ 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 $\Lambda_G$, and may be defined by $\Lambda_G = \lim \mathbb{Z}_p[G/U]$, where $U$ runs over the open subgroups of $G$. Following Mazur, the elements of $\Lambda_G$ may be viewed as $\mathbb{Z}_p$-valued measures on $G$. If $\alpha$ is an element of $\Lambda_G$, and if $f: G \to R$ is a continuous map of $G$ into a profinite $\mathbb{Z}_p$-module $R$, the integral of $f$ with respect to $\alpha$ is defined by

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

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

$$\int_G \chi d\alpha = \chi(\alpha).$$

The notion of a pseudo-measure, introduced by Serre [13], will be useful in what follows. An element $\alpha$ of the total ring of fractions of $\Lambda_G$
satisfying \((1 - g)\alpha \in \Lambda \alpha\) 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 \(\chi\) is a non-trivial homomorphism of \(G\) into \(R^\times\), we may define

\[
\int_G \chi \mathrm{d}\alpha = \int_G \chi \mathrm{d}\beta/(1 - \chi(h)),
\]

(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 \(f(T) = a_0 + a_1T + a_2T^2 + \ldots\) be a non-zero power series with coefficients in \(\mathfrak{o}\). We define

\[
\mu(f) = \min\{\text{ord}_\mathfrak{p} a_i : i \geq 0\}
\]

\[
\lambda(f) = \min\{i \geq 0 : \text{ord}_\mathfrak{p} a_i = \mu(f)\}.
\]

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 \(\mu\) and \(\lambda\) 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 \(\infty\) will be denoted by \(K_S\), and we put \(G_S = \text{Gal}(K_S/K)\). Since \(S \supseteq S_p\), \(K_S\) contains the group \(\mu_{p^\infty}\) of all \(p\)-power roots of unity. The action of \(G_S\) on \(\mu_{p^\infty}\) induces a character

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

via the formula

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

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 decomposi-
tion $x = \omega(x)\langle x \rangle \ (x \in \mathbb{Z}_p^\times)$, we obtain from $\mathbb{N}$ two important characters of $G_S$:

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

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

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

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

If $\chi$ is any homomorphism of $G_S$ into a field we call $\chi$ 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 $\theta$ are odd, but $\kappa$ is even.

For any character $\chi$ of $G_S$ of finite order, with values in $\mathbb{C}_p^\times$, we let $L^*_S(\chi, s)$ denote the $\mathbb{p}$-adic $L$-function attached to $\chi$. $L^*_S(\chi, s)$ is defined by means of the values of classical complex $L$-functions at negative integers, as follows. Let $\psi$ 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 $\psi$. 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 $\rho$. 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

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

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 $\chi$ is even.

The existence of $\mathbb{p}$-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 $\alpha_S$ on $G_S$ such that

$$L^*_S(\chi, s) = \int_{G_S} \chi k^{1 - n} \, d\alpha_S, \quad (2.2)$$

for any character $\chi$ 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 $\text{Gal}(K_\infty/K) = \mathbb{Z}_p$, we may choose an element $\gamma$ in the Sylow pro-$p$-subgroup of $G_S$ whose restriction to $K_\infty$ is a topological generator of $\text{Gal}(K_\infty/K)$. Let $\Gamma$ be the subgroup of $G_S$ generated topologically by $\gamma$. Then $\Gamma \simeq \mathbb{Z}_p$, and $G_S$
is the internal direct product of the subgroups $A = \text{Gal}(K_S/K_\infty)$ and $\Gamma$.

Now let $\phi$ be the homomorphism of $G_S$ into $\mathbb{Z}_p[[T]]$ that is trivial on $A$ and maps $\gamma$ to $\kappa(\gamma)(1 + T)^{-1}$. Let $\chi$ 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 $\alpha_S$; we put

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

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

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

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

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

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

$$L^\chi_{S'}(\chi, s) = L^\chi_S(\chi, s) \prod_{\nu \in S' - S} \left(1 - \chi \theta^{-1}(\sigma_\nu) \langle N\nu \rangle^{-s}\right),$$

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

$$\tilde{L}_{S'}(\chi, T) = \tilde{L}_S(\chi, T) \prod_{\nu \in S' - S} E_\nu(T), \quad (2.5)$$

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

$$E_\nu(\kappa(\gamma)^s - 1) = 1 - \chi \theta^{-1}(\sigma_\nu) \langle N\nu \rangle^{-s}.$$  

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

$$\sigma_\nu \equiv \gamma' \mod A.$$  

Since $\kappa$ is trivial on $A$, this implies

$$\kappa(\sigma_\nu) = \langle N\nu \rangle = \kappa(\gamma)'$$.
and therefore

$$E_v(T) = 1 - \chi\theta^{-1}(\sigma_v)(1 + T)^{-t}, \quad t = t(\sigma_v).$$

(2.6)

We can use (2.5) and (2.6) to see how the $\mu$ and $\lambda$ 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 $\chi$ is even (so that $\tilde{L}_S(\chi, T) \neq 0$). Then we have the following lemma.

**Lemma 2.1**: Let $\chi$ 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

$$\lambda_{S'}(\chi) = \lambda_S(\chi) + \sum' g(\nu),$$

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

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

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

Then

$$E_\nu(T) \equiv 1 - \chi\theta^{-1}(\sigma_\nu)(1 + T^{p^a})^u \mod p \circ [[T]]$$

$$\equiv 1 - \chi\theta^{-1}(\sigma_\nu) - \chi\theta^{-1}(\sigma_\nu) u T^{p^a} \mod (p, T^{p^{a+1}}) \circ [[T]].$$

It follows that

$$\mu(E_\nu(T)) = 0,$$

$$\lambda(E_\nu(T)) = p^a \quad \text{if} \ \chi\theta^{-1}(\sigma_\nu) \text{ is a } p\text{-power root of unity}$$

$$= 0 \quad \text{otherwise.}$$
Now, the decomposition group $D_v$ of $v$ for the extension $K_\infty/K$ is generated (topologically) by

$$
\sigma_v|_{K_\infty} \equiv \gamma^{(\alpha_v)} \equiv \gamma^{-p^u} \text{ mod } A.
$$

It follows that the index of $D_v$ in $\text{Gal}(K_\infty/K)$ is $p^u$. Thus $g(v)$ is finite and equal to $p^u$, 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 $\chi$ is varied.

**Proposition 2.1:** Let $\chi$ be an even character of $G_S$ of finite order, and $\psi$ an even character of $G_S$ of $p$-power order. First suppose that $p > 2$. Then

$$
\mu_S(\chi) = 0 \quad \text{if and only if} \quad \mu_S(\chi \psi) = 0,
$$
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 $d = [K:Q]$. However

$$
\mu_S(\chi) = d \quad \text{if and only if} \quad \mu_S(\chi \psi) = d,
$$
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 $Q_p$ containing the values of both $\chi$ and $\psi$, and let $\pi$ be a local parameter in $\mathfrak{o}$.

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

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

Hence, by (1.2) and (2.3),

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

(2.7)

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

1 \text{ mod } p. \text{ Hence }

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

so these power series have \( \mu \)-invariant 0 and \( \lambda \)-invariant 1. Hence (2.7) shows that

\[
\mu_s(\chi \psi) = 0 \quad \text{if and only if} \quad \mu_s(\chi) = 0,
\]

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" \( \sigma_v, v \in S_\infty \). \( H \) is a finite group of exponent 2. Then the following fact is proved in [4] (see also Ribet [12]): the direct image \( \tilde{\beta} \) of the measure \( \beta = (1 - \gamma)\alpha_s \) under the map \( G_s \rightarrow G_s/H \) is divisible by \( 2^d \) (i.e. \( 2^{-d}\tilde{\beta} \) takes values in \( \mathbb{Z}_2 \)). Since \( \chi \) and \( \phi \) are both \textit{even} characters of \( G_s \), we have that

\[
2^{-d}(1 - \chi \phi(\gamma)) \tilde{L}_s(\chi, T) = \int_{G_s/H} \chi \phi d(2^{-d}\tilde{\beta})
\]
lies in \( o[[T]] \). Since \( \mu(1 - \chi \phi(\gamma)) = 0 \), this shows \( \mu_s(\chi) \geq d \). Similarly, since \( \psi \) is even, \( \mu_s(\chi \psi) \geq d \). The rest of the argument proceeds as above, with \( G_s \) replaced by \( G_s/H \) and \( \beta = (1 - \gamma)\alpha_s \) by \( 2^{-d}\tilde{\beta} \). This concludes the proof.

Let \( \chi \) 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 \( \chi \) 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.

\textbf{Theorem 2.1:} Let \( \chi \) and \( \psi \) be even characters of \( \text{Gal}(K^{ab}/K) \) of finite order, and suppose that the order of \( \psi \) is a power of \( p \). Then \( \mu(\chi) \geq d \text{ ord}_p(2), \mu(\chi \psi) \geq d \text{ ord}_p(2), \) and

\[
\mu(\chi) = d \text{ ord}_p(2) \quad \text{if and only if} \quad \mu(\chi \psi) = d \text{ ord}_p(2).
\]

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

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

(ii) $v$ splits completely in $L_\infty$.

**Proof:** The statement about the $\mu$-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 $\chi$ (resp. $\chi \psi$). Since $\chi$ and $\psi$ 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 $M = \sum_v g(v)$, the summation taken over those places $v$ in $T \sim S$ for which $\chi \theta^{-1}(\sigma_p)$ has $p$-power order. Since $\chi$ is here assumed to have order prime to $p$, and $\theta$ has order prime to $p$ if $p > 2$ (and order $2 = p$ if $p = 2$), this condition on $v$ may be restated as $\chi \theta^{-1}(\sigma_p) = 1$ (resp. $\chi(\sigma_p) = 1$ if $p = 2$), i.e. $v$ splits completely in $L$. This last is, for any extension $v$ of $p$ to $K_\infty$, equivalent to the assertion that $v$ splits completely in $L_\infty$, and $g(v)$ is by definition the number of extensions of $v$ to $K_\infty$. So $M$ is the number of places $v$ on $K_\infty$ which split completely in $L_\infty$ and satisfy $v|K \in T \sim S$. Such $v$ satisfy (i) and (ii); conversely if a place $v$ on $K_\infty$ satisfies (i) and (ii), then $v$ splits completely in $L_\infty$, and $v|K$ lies in $T$ ($v|K$ ramified for $\psi$ implies $v|K$ ramified for $\chi \psi$, since $\chi$ and $\psi$ 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

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

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 $\epsilon$ 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

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

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

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

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 $n \geq 0$, there is a unique extension $F_n$ of $F$ in $F_\infty$ of degree $p^n$ over $F$. Each $F_n$ is again a CM-field, and we may use (3.2) to obtain 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

$$h_n^* = w_nQ_n2^{-d_n}L(\epsilon_n, 0) = w_nQ_n2^{-d_n}\prod_{\psi}L(\epsilon\psi, 0);$$

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

**Lemma 3.1:** There is an integer $n_0 \geq 0$ such that

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

(b) \quad $Q_n = Q_{n_0}$, \quad for $n \geq n_0$.

**Corollary:** For $n \geq n_0$,

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

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

**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 $F_\infty$ is finite. It is then clear that $w_n$ is independent of $n$ for $n$ large, say $n \geq n_0$, 


i.e. (a) holds with $\delta = 0$. Now suppose that the number of roots of unity in $F_\infty$ is infinite. The group of roots of unity of order prime to $p$ in $F_\infty$ 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 $n \geq n_0$. It is easy to check by Galois theory that we must have $F_n = F_{n_0}(\mu_{p^{n-n_0}})$ for $n \geq n_0$, 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, $\eta^{1-j}$ is a root of unity for any unit $\eta \in E$. From this it follows that $E/WE^+ = E^{1-j}/W^2 \subseteq W/W^2$. 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 $m \geq n \geq 0$:

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 $F_\infty$ 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 $F_\infty$ is infinite, then $p = 2$, and it is well known that the norm maps $W_m$ onto $W_n$ for $m \geq n > 0$, 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 $F_\infty$ contains all the $p$-power roots of unity. An equivalent formulation in terms of characters is as follows. $F_\infty$ contains the $p$-power roots of unity if it contains $\mu_p$ (resp. $\mu_4$ if $p = 2$). If $p$ is odd, $F^+(\mu_p)$ is then an extension of $F^+$ in $F_\infty$ 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 $\psi$ denote the non-trivial character of $F_2^+ / F^+$, $F_2^+$ being of course the first layer of the $\mathbb{Z}_p$-extension $F_\infty^+ / F^+$. If $F_\infty^+$ contains the 2-power roots of unity, the $F^+(\mu_4)$ is an imaginary quadratic extension of $F^+$ in $F_\infty$; hence $\theta = \epsilon$ or $\epsilon \psi$. So, when $p = 2$, $\delta = 1$ is equivalent to $\epsilon \theta = 1$ or $\psi$.

We use (3.3) to relate the $\mu^*$ and $\lambda^*$ invariants of the $\mathbb{Z}_p$-extension $F_\infty/F$ to the $\mu$ and $\lambda$ 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 $\mu^*$ and $\lambda^*$ 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 $\mu^* \geq 0$, $\lambda^* \geq 0$ and $\nu^*$ such that

$$\text{ord}_p(h^*_n) = \mu^*p^n + \lambda^*n + \nu^*,$$
for \( n \) sufficiently large. In fact
\[
\mu^* = \mu_S(\epsilon \theta) - d \text{ord}_p(2)
\]
\[
\lambda^* = \lambda_S(\epsilon \theta) + \delta,
\]
where \( \delta \) is defined in Lemma 3.1, and \( S \) is the set of places of \( F^+ \) that ramify in \( F_\infty^+ \).

**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 \( \psi \) is a character of finite order of \( \text{Gal}(F_\infty^+/F^+) \), with values in \( \mathbb{C}_p^\times \), non-trivial on \( \text{Gal}(F_\infty^+/F_{n_0}^+) \), then \( S \) (as defined in Proposition 3.1) is precisely the set of places for which \( \psi \) is ramified. Hence, by (2.1), we have,
\[
L(\epsilon \psi, 0) = L_S^*(\epsilon \psi \theta, 0) = \tilde{L}_S(\epsilon \theta, \psi(\gamma)^{-1} - 1).
\]
The second equality comes from (2.4).

Now let \( n \geq n_0 \), and combine (3.3) and (3.4). As \( \psi \) varies over characters of \( \text{Gal}(F_n^+/F^+) \) that are nontrivial on \( \text{Gal}(F_n^+/F_{n_0}^+) \), \( \psi(\gamma)^{-1} \) will vary over roots of unity \( \xi \) in \( \mathbb{C}_p^\times \) satisfying \( \xi^{p^n} = 1, \xi^{p^n_0} \neq 1 \). Hence
\[
h_n^* = h_{n_0}^* p^{(n-n_0)\delta} \prod \xi 2^{-d} \tilde{L}_S(\epsilon \theta, \xi - 1),
\]
with \( \xi \) satisfying \( \xi^{p^n} = 1, \xi^{p^n_0} \neq 1 \). Now if the order of \( \xi \) is \( p^m \), and if \( m \) is sufficiently large, it is easy to see that
\[
\text{ord}_p \tilde{L}_S(\epsilon \theta, \xi - 1) = \mu_S(\epsilon \theta) + \lambda_S(\epsilon \theta) \text{ord}_p(\xi - 1)
\]
\[
= \mu_S(\epsilon \theta) + \lambda_S(\epsilon \theta)/(p^{m-1}(p-1)).
\]
Hence, increasing \( n_0 \) if necessary, we have from (3.5)
\[
\text{ord}_p h_n^* = (\mu_S(\epsilon \theta) - d \text{ord}_p(2)) p^n + (\lambda_S(\epsilon \theta) + \delta)n + C,
\]
for \( n \geq n_0 \) 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 \( \text{Gal}(E'/F) \) 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**: $\mu^*_E = 0$ if and only if $\mu^*_E = 0$, and when this is the case, 

$$
\lambda^*_E - \delta_E = [E_\infty : F_\infty](\lambda^*_F - \delta_F) 
+ \sum_{w'} \left( e\left(\frac{w'}{v'}\right) - 1\right) - \sum_w \left( e\left(\frac{w}{v}\right) - 1\right),
$$

the summations taken over all places $w'$ on $E_\infty$ (resp. $w$ on $E_\infty^+$) 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 $F_\infty/F$), it is immediately that

$$
\lambda^*_E = \lambda^*_F, \quad \delta_E = \delta_F,
$$

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

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

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

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

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

$$
\mu(\epsilon_E \theta_E) - pd \text{ ord}_p(2) = \sum_{\psi} \mu(\epsilon_F \theta_F \psi) - d \text{ ord}_p(2).$$
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 \( \mu(\epsilon_F \theta_E) = pd \text{ord}_F(2) \) if and only if \( \mu(\epsilon_F \theta_E) = d \text{ord}_F(2) \), or, by Proposition 3.1, \( \mu^*_F = 0 \) 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 \( \lambda \)-invariants in (4.2), we find

\[
\lambda(\epsilon_F \theta_E) = \sum_\psi \lambda(\epsilon_F \theta_E \psi) \tag{4.3}
\]

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 \( \chi = \epsilon_F \theta_E \),

\[
\lambda(\epsilon_F \theta_E \psi) = \lambda(\epsilon_F \theta_E) + N, \quad \text{if} \quad \psi \neq 1,
\]

where \( N \) is the number of places \( v \) on \( F^+_\infty \) such that (i) \( v | F^+ \) does not divide \( p \) but is ramified for \( \psi \), and (ii) \( v \) splits in \( F^-_\infty \). Thus

\[
\lambda(\epsilon_F \theta_E) = p\lambda(\epsilon_F \theta_E) + (p - 1)N.
\]

However, any place \( v \) on \( F^+ \) satisfying (i) ramifies in \( E^+_\infty \), and so has a unique extension \( w \) on \( E^+_\infty \), 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 \( x = 1 \) we find

\[
\lambda(\epsilon_F \theta_E) = \lambda(1) + N, \quad \lambda(\epsilon_F \theta_E \psi) = \lambda(1) + N',
\]

where \( N \) (resp. \( N' \)) is the number of places \( v \) on \( F^+_\infty \) such that \( v | F^+ \) does not divide 2 but is ramified for \( \epsilon_F \theta_E \) (resp. \( \epsilon_F \theta_E \psi \)). Here \( \psi \) 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

\[
\lambda(\epsilon_F \theta_E) = 2\lambda(\epsilon_F \theta_E) + N' - N.
\]

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

\[
N' - N = \sum_{w'} (e(w'/v') - 1) - \sum_w (e(w/v) - 1) \tag{4.4}
\]

where \( w' \) (resp. \( w \)) runs over places of \( E^-_\infty \) (resp. \( E^+_\infty \)) not dividing 2, and \( v' = w' | F^+_\infty, v = w | F^+_\infty \). This can be seen as follows. If \( v \) is a place on \( F^+_\infty \) not dividing 2, let \( N(v) = 1 \) if \( v | F^+ \) is ramified for \( \epsilon_F \), 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 $\theta_F$ 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 $F_\infty^+$ 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 $E_\infty/F_\infty^+$. There are five possibilities for $L_v$; a case by case examination shows that

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

the summations on the right taken over the places $w'$ on $E_\infty$ (resp. places $w$ on $E^+$) lying over $v$; we note that $v$ always splits completely in $L_v$ (the residue field of $F_\infty^+$ 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


(Oblatum 5-VIII-1982)

Riemann-Hurwitz formula

(17)

Institute for Advanced Study
Olden Lane
Princeton, NJ 08540
USA

Current address:
Department of Mathematics
Ohio State University
Columbus, OH 43210
USA