ACTA ARITHMETICA
LX.2 (1991)

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

by

Sang G. Han (Taejon)

Introduction. Let p be an odd prime. $\mathbb{Q}_\infty$ will denote 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 totally real number field, and let ε be an odd character associated to an abelian extension E/F. Also let $\vartheta = \mathbb{Z}_p[\text{images of } \varepsilon]$. Let N denote the absolute norm. Let μ_p denote the group of pth roots of unity. Then by the work of P. Deligne and K. Ribet [Ri], there exists a p-adic L-function $L_p(\varepsilon\omega, s)$ so that for all $n > 0$,

$$L_p(\varepsilon\omega, 1-n) = L(\varepsilon\omega^{1-n}, 1-n) \prod [1 - \varepsilon\omega^{1-n}(q) N q^{n-1}]$$

where q runs over the primes of F which lie over p, and ω is the Teichmüller character for $F(\mu_p)/F$. The action of $\Gamma = \mathrm{Gal}(F_\infty/F) \cong \mathrm{Gal}(F(\mu_p)_\infty/F(\mu_p))$ on p-power roots of unity is given by a homomorphism $\kappa : \Gamma \to \mathbb{Z}_p^\times$. Let γ_0 be a topological generator of Γ. Let $\kappa_0 = \kappa(\gamma_0)$. Then we have an element $f_{\varepsilon\omega}(T)$ in the quotient field of $\Lambda = \vartheta[[T]]$ such that

$$f_{\varepsilon\omega}(\kappa_0^s - 1) = L_p(\varepsilon\omega, s) \quad \text{for all } s \text{ in } \mathbb{Z}_p - \{1\}\,.$$

Let F_n denote the nth layer of F_∞/F. Let e_n denote the exponent of the exact power of p dividing the class number of F_n. One of the principal results of Iwasawa theory states that there exist fixed integers $\mu \ge 0, \lambda \ge 0$, and ν such that $e_n = \mu p^n + \lambda n + \nu$ for all n sufficiently large. Iwasawa conjectured that $\mu = 0$ for any basic $\mathbb{Z}_p$-extension. The conjecture is known to be true when F is abelian over $\mathbb{Q}$. The general case still remains to be shown. In particular, suppose F is a CM-field. Consider the basic $\mathbb{Z}_p$-extension of F^+. Then the invariants decompose into plus and minus parts to give $\mu = \mu^- + \mu^+$, $\lambda = \lambda^- + \lambda^+$, and $\nu = \nu^- + \nu^+$ [Wa].

Let k be a finite extension of $\mathbb{Q}_p$. Let π be a prime element of k, ϑ the ring of integral elements of k, and f the residue degree of $k/\mathbb{Q}_p$. Let $\Lambda = \vartheta[[T]]$. We call a polynomial $a_0 + a_1 T + \ldots + a_n T^n \in \Lambda$ *distinguished* if $a_n = 1$ and $a_i \in \pi\vartheta$ for all $0 \le i \le n-1$.

Theorem 1. *There exists a unique homomorphism* $M:\Lambda^\times\to\Lambda^\times$ *such that*:

(1) $M(U)((1+T)^p-1)=\prod U(\zeta(1+T)-1)$ *for all* U *in* $\Lambda^\times$ *where the product is over the* p^f*-th roots of unity.*

(2) M *is continuous in* (p,T)*-adic topology.*

(3) *For any* U *in* $\Lambda^\times$, $M^\infty(U)=\lim M^n(U)$ *exists.*

(4) *Let* U_1 *and* U_2 *be in* $\Lambda^\times$. *Assume that* $U_1=U_2 \mod \pi$. *Then*

$$M^\infty U_1=M^\infty U_2\,.$$

We call M *Coleman's norm operator.*

Proof. See [Han], or [Wa] where this is proved for $f=1$.

Let us recall the natural decomposition $\vartheta^\times=W\times(1+\pi\vartheta^\times)$ where W is the set of all roots of unity in ϑ whose order is prime to p. We know that $|W|=p^f-1$. Hence for any element α of $\vartheta^\times\subseteq\Lambda^\times$, $M^\infty(\alpha)=\omega(\alpha)$. Let $T-\beta$ be a distinguished polynomial of $\Lambda^\times$. Then

$$M(T-\alpha)((1+T)^p-1)=\prod(\zeta(1+T)-1-\alpha)=(1+T)^p-(1+\alpha)^p\,.$$

So

$$M(T-\alpha)=T+1-(1+\alpha)^p\,,\qquad M^\infty(T-\alpha)=T\,.$$

So for any distinguished polynomial $D(T)$ of degree λ, we can show that $M^\infty D=T^\lambda$ by considering the Coleman operator over the splitting field of $D(T)$. We extend M from $\Lambda^\times$ to Λ, then to $\Lambda_{(\pi)}$ by multiplicativity.

Let $g(T)=a_0+a_1T+a_2T^2+\ldots$ be a non-zero element of Λ. We define

$$\mu(g)=\min\{\operatorname{ord}_p a_i\}\,,\qquad \lambda(g)=\min\{j:\mu(g)=\operatorname{ord}_p a_j\}\,.$$

Clearly we have $\mu(fg)=\mu(f)+\mu(g)$, $\lambda(fg)=\lambda(f)+\lambda(g)$, if f, g are non-zero elements of Λ; we may use these relations to define μ- and λ-invariants of the non-zero elements of the quotient field of Λ. Finally, by the Weierstrass preparation theorem, any element $f(T)$ in the quotient field of Λ is uniquely factorized as follows:

$$f(T)=\pi^a\frac{P(T)}{Q(T)}U(T)\,,\qquad a=\text{an integer}\,,$$

where $P(T)$, $Q(T)$ are relatively prime distinguished polynomials and $U(T)$ is a unit of Λ. We define f^∞ to be $M^\infty U(0)$. If $f(T)$ is in Λ, then $a=\mu(f)$, $Q(T)=1$, degree of $P(T)=\lambda(f)$. We easily see that if $\mu(f)=0$, then $M^\infty f=T^{\lambda(F)}f^\infty+$ (higher degree terms).

Kida's formula. In [Ki], Kida proved an analogue of the classical Riemann–Hurwitz genus formula, by describing the behaviour of the λ^--invariants in p-extensions of CM-fields under the assumption $\mu^-=0$ for the fields involved. A special case of Kida's result is the following (for the most general formulation, see [Ki] or [Si]):

Let E/K be a CM-field which is a finite p-extension (i.e. if E' denotes the Galois closure of E for K, then $\mathrm{Gal}(E'/K)$ is a finite p-group). Suppose that K contains μ_p. Finally, suppose that $\mu_K^- = 0$. Then $\mu_E^- = 0$ and

$$2\lambda_E^- - 2 = [E_\infty : F_\infty](2\lambda_K^- - 2) + \sum_w (e(w) - 1)$$

where w runs over finite primes on E_∞ which do not lie above p and are split for the extension E/E^+, and $e(w)$ denotes the ramification index of w in E_∞/K_∞.

Let ε_E and ε denote the odd characters of E/E^+ and K/K^+ respectively. Note that $\lambda(f_{\varepsilon_E\omega}) = \lambda_E^- - \delta_E$ where $\delta_E = 1$ if μ_p is contained in E and 0 otherwise [Si]. So Kida's formula can be viewed as a relation between $\lambda(f_{\varepsilon_E\omega})$ and $\lambda(f_{\varepsilon\omega})$.

Our aim is to generalize Kida's formula to arbitrary odd characters associated with an abelian extension, of degree prime to p, of a totally real number field under the assumption that the μ-invariant of our character is zero. Let E, F be totally real number fields, $[E : F] < \infty$, and let E be a p-extension of F. Let ε be an odd character of F whose order is prime to p. We will compare the λ-invariants of $f_{\varepsilon\omega}$ and $f_{\varepsilon_E\omega}$, where ε_E is defined by $\varepsilon_E = \varepsilon \cdot \mathrm{Norm}_{E/F}$. Note that this definition of ε_E agrees with the notation in the above remarks about Kida's formula. For each intermediate field $F \subseteq L \subseteq E$, ε induces an odd character $\varepsilon_L = \varepsilon \cdot \mathrm{Norm}_{L/F}$. For any finite prime w in L, $\varepsilon_L(w) = \varepsilon(v)^{f(w/v)}$ where $v = w|_F$ and $f(w/v)$ is the residue degree of w over v. Fix a topological generator γ_0 of $\mathrm{Gal}(F_\infty/F)$. Define κ_0 as in the introduction. We define a map

$$\alpha = \alpha_L : \{\text{finite primes of } L \text{ which do not divide } p\} \to \mathbb{Z}_p$$

where $\alpha_L(w)$ is defined by $\langle Nw \rangle = \kappa_0^{\alpha(w)}$. Define $[\alpha(w)]$ to be $\alpha(w)|\alpha(w)|$, i.e. $[\alpha(w)]$ is the unit part of $\alpha(w)$. Note that $[\alpha_L(w)] = [\alpha_F(w|_F)]$. So we will denote $[\alpha_L(w)]$ by $[\alpha(w)]$ from now on. Finally, let $k = \mathbb{Q}_p(\mu_p$, images of $\varepsilon)$.

THEOREM 2. *If $\mu(f_{\varepsilon\omega}) = 0$, then $\mu(f_{\varepsilon_E\omega}) = 0$ and*

$$\lambda(f_{\varepsilon_E\omega}) = [E_\infty : F_\infty]\lambda(f_{\varepsilon\omega}) + \sum_{\varepsilon(q)=1} (e(w) - 1) \tag{1}$$

where the summation is over all finite primes w of E_∞ which do not divide p, $e(w) =$ ramification index of w in E_∞/F_∞ and $q = w|_F$. Moreover,

$$f_{\varepsilon_E\omega}^{\infty} = f_{\varepsilon\omega}^{\infty[E_\infty:F_\infty]} \prod_{\varepsilon(q)\neq 1} (1 - \varepsilon(q)^{|\alpha(q)|})^{e(w)-1} \prod_{\varepsilon(q)=1} [\alpha(q)]^{e(w)-1} \tag{2}$$

where the product is taken over all finite primes w in E_∞ as in (1). (*For any w on E, $\varepsilon_E(w) = 1$ or $\varepsilon_E(w) \neq 1$ according as $\varepsilon(w|_F) = 1$ or $\varepsilon(w|_F) \neq 1$;*

and $\varepsilon(w)^{|\alpha(w)|}$ *denotes the unique* $|\alpha(w)|^{-1}$*-th root of* $\varepsilon(w)$ *in the image of* ε*.)*

Proof. We will first prove the theorem when E/F is a cyclic extension of degree p. Notice that without loss of generality we may assume $F_\infty \cap E = F$. Otherwise the theorem holds trivially. So we may assume that $\gamma_E = \gamma_F$. We have a factorization of the complex L-function $L(\varepsilon_E, s)$ into

$$L(\varepsilon_E, s) = \prod L(\varepsilon\phi, s)$$

where ϕ runs through all characters of E/F. So we have the corresponding factorization for p-adic L-functions as follows:

$$L_p(\varepsilon_E\omega, s) = \prod L_p(\varepsilon\omega\phi, s)\,.$$

So $f_{\varepsilon_E\omega}(T) = \prod f_{\varepsilon\omega\phi}(T)$. Let $S = \{q \nmid p : q$ is a finite prime of F which ramifies in $E/F\}$ and let $f_{\varepsilon\omega,S}(T)$ be the power series corresponding to

$$L_{p,S}(\varepsilon\omega, s) = L_p(\varepsilon\omega, s)\prod(1 - \varepsilon(q)\langle Nq\rangle^{-s})$$

where the product is over q in S. So $f_{\varepsilon\omega,S}(T) = f_{\varepsilon\omega}(T)\prod E_q(T)$ where $E_q(T) = 1 - \varepsilon(q)(1+T)^{-\alpha(q)}$. On the other hand, $f_{\varepsilon\omega\phi}(T) = f_{\varepsilon\omega,S}(T) \mod \pi\Lambda_{(\pi)}$ for $\phi \neq 1$ (see proof of Proposition 2.1 in [Si]. Roughly speaking, $f_{\varepsilon\omega\phi}(T)$ is the integral of $\varepsilon\omega\phi$ on some Galois group. But since $\operatorname{Im}\phi = \mu_p$, $\phi = 1 \mod (\zeta_p - 1)$ and $f_{\varepsilon\omega\phi}(T)$ is congruent to the integral of $\varepsilon\omega$, which is $f_{\varepsilon\omega}(T)$, up to some Euler factors). Hence for $\phi \neq 1$ we have

$$f_{\varepsilon\omega\phi}(T) = f_{\varepsilon\omega}(T)\prod E_q(T) \mod \pi\Lambda_{(\pi)}\,.$$

So we have

$$f_{\varepsilon_E\omega}(T) = f_{\varepsilon\omega}(T)^p \prod(1 - \varepsilon(q)(1+T)^{-\alpha(q)})^{p-1} \mod \pi\Lambda_{(\pi)}\,.$$

Obviously the μ-invariant of $E_q(T)$ is zero. So $\mu(f_{\varepsilon_E\omega}) = 0$. Now, the decomposition group D_q of q has index $p^{1/|\alpha(q)|}$ in $\mathrm{Gal}(F_\infty/F)$. By comparing the Weierstrass degrees of the above congruence equation, we get equation (1).

Let us apply the limit M^∞ of Coleman's norm operator to $E_q(T)$. Since

$$Mf((1+T)^p - 1) = \prod f(\zeta(T+1) - 1)$$

and

$$1 - \varepsilon(q)(1+T)^{-\alpha(q)} = (1 - \varepsilon(q)^{|\alpha(q)|}(1+T)^{-[\alpha(q)]})^{1/|\alpha(q)|} \mod \pi\Lambda\,,$$

we have

$$
\begin{aligned}
M^{\infty}E_q(T) &= M^{\infty}(1-\varepsilon(q)(1+T)^{-\alpha(q)}) \\
&= M^{\infty}(1-\varepsilon(q)^{|\alpha(q)|}(1+T)^{-[\alpha(q)]})^{1/|\alpha(q)|} \\
&= \begin{cases} (1-\varepsilon(q)^{|\alpha(q)|}(1+T)^{-[\alpha(q)]})^{1/|\alpha(q)|} & \text{if } \varepsilon(q)\neq 1, \\ [\alpha(q)]^{1/|\alpha(q)|}T^{1/|\alpha(q)|} + (\text{higher degree terms}) & \text{if } \varepsilon(q)=1. \end{cases}
\end{aligned}
$$

By comparing the unit parts we have equation (2).

The induction is carried out as follows: We have just proved the case when E/F is a cyclic extension of degree p. Assume that the theorem is true for any Galois extension with degree less than p^n. Let E/F be a Galois extension with degree p^n. Since $\mathrm{Gal}(E/F)$ is a finite p-group, there is a proper normal subgroup and thereby a proper subfield L which is normal over F. The theorem holds for the two Galois extensions E/L and L/F by the induction hypothesis. Combining the two formulas we get the formula for E/F. When E/F is not Galois one proves the theorem as follows: Compare the formulas for E'/E and E'/F where E' is the Galois closure of E over F. The only crucial point in this induction process is that $\varepsilon(w)^{|\alpha(w)|}$ and $[\alpha(w)]$ depend only on $w|_F$ for any prime w appearing in the counting. However, note that the numbers in (2) will depend on the choice of the topological generator γ_0.

LEMMA 3. *Let α be in C_p and* $\mathrm{ord}_p(\alpha-1)>0$. *Then*

$$
\lim_{n\to\infty}\frac{1-\alpha^{p^n}}{p^n} = -\log\alpha\,.
$$

Proof. Let $\alpha = 1+\beta$. So $\mathrm{ord}_p(\beta)>0$. Then for $n\gg 0$,

$$
\begin{aligned}
&\frac{1-\alpha^{p^n}}{p^n} + \log\alpha \\
&= -\sum_{1\le k\le p}\frac{1}{p^n}\binom{p^n}{k}\beta^k + \sum_{1\le k}\frac{(-1)^{k-1}}{k}\beta^k \\
&= -\sum_{1\le k}\frac{(p^n-1)(p^n-2)\dots(p^n-k+1)}{k!}\beta^k \\
&\qquad + \sum_{1\le k}\frac{(-1)^{k-1}}{k}\beta^k \qquad \mathrm{mod}\,(\text{high } p\text{-power}) \\
&= \sum_{1\le k}\left(\frac{(-1)^{k-1}(k-1)!}{k!}+\frac{(-1)^k}{k}\right)\beta^k = 0 \qquad \mathrm{mod}\,(\text{high } p\text{-power})\,.
\end{aligned}
$$

So the lemma is proved.

Let K be a CM-field, U the unit group of K, U^+ the unit group of K^+, $W = W(K)$ the group of roots of unity in K, and w_K=cardinality of W. Then $Q_K = [E : WE^+]$ is 1 or 2.

Let $h^-(K)$ denote the relative class number of K/K^+.

THEOREM 4. *Let K be a CM-field. Let K_n be the n-th layer of K_∞, $f(T)$ the* (*quotient of*) *power series associated to $L_p(\varepsilon\omega, s)$ where ε is the odd character of K/K^+. Let ν^- be one of the Iwasawa invariants of K/K^+. If no prime above p splits in K/K^+, then*

$$\nu^- = \mathrm{ord}_p \prod \log \beta$$

where β runs over all roots of $f(T)$ counting multiplicity. (*Even in case when μ_p are in K and Leopoldt's conjecture is false for K and p, we still assume that $f(T)$ has a pole at $s = 1$. In other words, we assume that $\kappa_0 - 1$ is a root of $f(T)$.*) *Moreover*,

$$\lim_{n\to\infty} h^-(K_n)/p^{\mu^- p^n + \lambda^- n} = 2^{-b(K)}\omega(2)^{-[K:\mathbb{Q}]}[w_K]Q_K f^\infty_{\varepsilon\omega} \prod(-\log \beta)$$

where $[w_K]$ and Q_K denotes the stabilized values of $[w_{K_n}]$ and Q_{K_n}, $b(K) =$ number of primes above p in K^+_∞ which are inert in K_∞/K^+_∞. The above limit will be denoted by h^∞_K.

Proof. Let ε_n be the odd character for K_n/K_n^+. We know that

$$L(\varepsilon_n, 0) = \prod L(\varepsilon\phi, 0)$$

where ϕ runs over all characters of K_n^+/K^+. Let $d_n = [K_n^+ : \mathbb{Q}]$, $w_n = w_{K_n}$, $Q_n = Q_{K_n}$. Since no prime above p splits,

$$\begin{aligned} h^-(K_n) &= 2^{-d_n} w_n Q_n L(\varepsilon_n, 0) \\ &= 2^{-d_n} w_n Q_n \frac{L_p(\varepsilon_n\omega, 0)}{\prod_{q|p \text{ in } K}(1-\varepsilon(q))} \\ &= 2^{-d_n} w_n Q_n \frac{\prod L_p(\varepsilon\omega\phi, 0)}{\prod_{q|p \text{ in } K}(1-\varepsilon(q))}\,. \end{aligned}$$

So for $n \gg 0$,

$$\begin{aligned} h^-(K_n) &= 2^{-d_n} w_n Q_n 2^{-b(K)} \prod L_p(\varepsilon\phi, 0) \\ &= 2^{-d_n} w_n Q_n 2^{-b(K)} \prod f(\zeta - 1) \end{aligned}$$

where the product is over p^nth roots of unity. So

$$h^-(K_n) = 2^{-d_n} w_n Q_n 2^{-b(K)} (M^n f)(0)\,.$$

Since $\mathrm{ord}_p\, w_K = \mathrm{ord}_p(1 - \delta_K\gamma_0)$,

$$\mathrm{ord}_p\, w_n = n + \mathrm{ord}_p(1 - \delta_K\gamma_0) = \mathrm{ord}_p\, M^n(T + 1 - \delta_K\gamma_0)(0)\,.$$

So

$$\lim h^-(K_n)/p^{\mu^- p^n+\lambda^- n} = 2^{-b(K)}\omega(2)^{-[K:\mathbb{Q}]}[w_K]Q_K f_{\varepsilon\omega}^\infty \prod_\beta (-\log\beta)$$

by Lemma 3. And

$$\nu^- = \mathrm{ord}_p \lim h^-(K_n)/p^{\mu^- p^n+\lambda^- n} = \mathrm{ord}_p \prod_\beta \log\beta\,.$$

Assume that E/K is a p-extension of CM-fields. If $\mu_E^- = \mu_K^- = \lambda_E^- = \lambda_F^- = 0$ and the primes above p do not split in K/K^+, then $\nu_K^- = \nu_E^- = 0$. Then by Theorems 2 and 4

$$\begin{aligned}\frac{2^{-b(E)}h_E^\infty}{[w_E]Q_E} &= \left(\frac{2^{-b(K)}h_K^\infty}{[w_K]Q_K}\right)^{[E_\infty:K_\infty]} \prod_{\varepsilon(q)\neq 1}(1-\varepsilon(q)^{|\alpha(q)|})^{e(w)-1}\\ &= \left(\frac{2^{-b(K)}h_K^\infty}{[w_K]Q_K}\right)^{[E_\infty:K_\infty]} 2^{\Sigma(e(w)-1)}\end{aligned}$$

where the summation is the same as in Theorem 2. (For $n \gg 0$, since p is odd, Sylow 2-subgroup of $W(E_n)$ = Sylow 2-subgroup of $W(K_n)$. This implies $Q_K = Q_E$ in this case.)

By looking at the orders of K_2-groups of $\mathbb{Z}_p$-extensions [Co1], one can get a genus formula and a limit formula similar to those of this paper. Assuming some conjectures of algebraic K-theory, one may get similar formulas for higher K-groups. Also Theorem 3 of [Iw] gives Kida's formula immediately. Furthermore, in some cases Kida's formula is the relation between the number of generators of a free pro-p-group and a subgroup of finite index. So it could be interpreted as a weak form of Schreier's theorem for finitely generated free pro-p-groups.

Acknowledgement. I sincerely thank the referee for pointing out many mistakes in this paper.

References

[Ca] P. Cassou-Nogues, *p-adic L-functions for totally real number fields*, in: Proceedings of the Conference on p-adic Analysis, Report 7806, Katholieke Univ., Nijmegen, 1978, 24–37.

[Co1] J. Coates, *On K_2 and some classical conjectures in algebraic number theory*, Ann. of Math. 95 (1972), 99–116.

[Co2] —, *p-adic L-functions and Iwasawa theory*, in: Algebraic Number Fields, A. Fröhlich (ed.), Academic Press, New York 1977, 269–353.

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

[G-M] R. Gold and M. Madan, *Iwasawa invariants*, Comm. Algebra 13 (7) (1985), 1559–1578.

[Han] S. Han, *Two applications of p-adic L-functions*, Thesis, Ohio State University, 1987.

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

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

[Ri] K. Ribet, *Report on p-adic L-functions over totally real fields*, Astérisque 61 (1979), 177–192.

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

[Si] W. Sinnott, *On p-adic L-functions and the Riemann–Hurwitz genus formula*, Compositio Math. 53 (1984), 3–17.

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, Springer, New York 1982.

DEPARTMENT OF MATHEMATICS
KAIST
YUSUNG-GU, TAEJON 305-701
SOUTH KOREA
E-MAIL: SGHAN@KIT.KAIST.AC.KR

Received on 9.1.1986
and in revised form on 18.2.1991 (1585)