PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 104, Number 1, September 1988

KIDA'S THEOREM FOR A CLASS OF NONNORMAL EXTENSIONS

ROBERT GOLD AND MANOHAR MADAN

(Communicated by Larry J. Goldstein)

ABSTRACT. Let E, F be $\mathbf{Z}_p$-fields of CM-type such that E/F is an extension of degree p. Let L, the normal closure of E/F, be such that $\mathrm{Gal}(L/F)$ has a normal subgroup of order p. Denote the fixed field of this group by K. We prove a Kida type formula which describes the minus part of the Iwasawa lambda invariant of E in terms of the lambda invariants of F and K.

1. Introduction. Let p be an odd prime. Let $\mathbf{Q}_n$ be the unique cyclic extension of degree p^n contained in the cyclotomic field of p^{n+1}th roots of unity and $\mathbf{Q}_\infty = \bigcup_{n\geq 0} \mathbf{Q}_n$. A $\mathbf{Z}_p$-field is the composite of $\mathbf{Q}_\infty$ with a finite extension of $\mathbf{Q}$. A $\mathbf{Z}_p$-field F of CM-type is a totally imaginary $\mathbf{Z}_p$-field which is a quadratic extension of a totally real $\mathbf{Z}_p$-field F^+. Let A_F^- denote the subgroup of the p-class group of F consisting of classes c such that $c^J = c^{-1}$, J denoting complex conjugation.

A well-known conjecture of Iwasawa on the vanishing of the μ-invariant implies that $A_F^- \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\lambda_F^-}$ for some nonnegative integer λ_F^-, where $\mathbf{Q}_p$, $\mathbf{Z}_p$ denote the field of p-adic numbers and the ring of p-adic integers, respectively. Our object, in this paper, is to prove the following generalization of Kida's Theorem [**K**].

THEOREM. *Let E, F be $\mathbf{Z}_p$-fields of CM-type such that E/F is an extension of degree p. Let L, the normal closure of E/F, be such that* $\mathrm{Gal}(L/F)$ *has a normal subgroup of order p. Denote the fixed field of this group by K. Then $\mu_K^- = 0$ implies $\mu_F^- = \mu_E^- = 0$, and*

$$\lambda_E^- = \lambda_F^- + \frac{p-1}{[K:F]}(\lambda_K^- + t - \delta),$$

where t is the number of non-p-primes of K^+ that ramify in L^+ and split in K, and δ is 1 *or* 0 *according as K does or does not contain the pth roots of unity.*

We give two proofs of this theorem, one arithmetic-algebraic and the other analytic. The first proof is based on an analysis of the action of $\mathrm{Gal}(L/F)$ on the p-elementary subgroup of A_L^-. It uses some facts proved in [**GM**]. The analytic proof uses relations between nonabelian p-adic L-functions. As in [**S**], the critical fact used in this proof is a relation, due to Iwasawa, between p-adic L-functions and Iwasawa invariants.

Kida's theorem is the analogue of a formula of Deuring and Safarevic, a special case of which relates the Hasse-Witt invariants of the function fields of a cyclic extension of degree p such that the field of constants k is an algebraically closed

Received by the editors January 7, 1987 and, in revised form, August 13, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R23; Secondary 11R29.

field of characteristic p. In this case, Rück [**R**] has proved the corresponding generalization. His proof is analytic. Our arithmetic-algebraic proof remains valid in the function field case and, in fact, it holds also in the truly analogous situation when k is the $\mathbf{Z}_p$-extension of a finite field. Using some facts from [**DM**], the reader can easily supply the details.

2. The arithmetic algebraic proof. By a theorem of Iwasawa [**I**], $\mu_K^- = 0$ implies $\mu_L^- = 0$. Thus, the p-elementary subgroup of A_L^- is finite of rank λ_L^-. Since the kernels of the conorm maps $A_F^- \to A_E^-$, $A_E^- \to A_L^-$ are finite, it follows that the p-elementary subgroups of A_E^-, A_F^- are also finite, i.e. $\mu_F^- = 0$, $\mu_E^- = 0$.

The assumption that $\mathrm{Gal}(L/K)$ is a normal subgroup of order p of the Galois group of the normal closure L/F of E/F implies that $\mathrm{Gal}(L/F)$ is a semidirect product of $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L/E)$, the latter is a cyclic group of order d dividing $p-1$. Let $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$, $\mathrm{Gal}(L/E) = \langle\tau\rangle$ and $\tau\circ\tau^{-1} = \sigma^r$. Let X_L denote the p-elementary subgroup of A_L^-. For $i = 1, 2, \ldots, p-1, p$, let

$$X_i = \{c : c \in X_L, c^{(1-\sigma)^i} = 1\}. \tag{1}$$

We have the descending chain of τ-invariant subspaces

$$X_L = X_p \supset X_{p-1} \supset \cdots \supset X_2 \supset X_1 \supset X_0 = (1).$$

Denoting by $\mathbf{F}_p$ the finite field with p elements, we recall the following facts from [**GM**].

$$\begin{aligned} \dim_{\mathbf{F}_p} X_1 &= \begin{cases} \lambda_K^- + t - \delta, & \text{if } t > 0, \\ \lambda_K^-, & \text{if } t = 0, \end{cases} \\ \dim_{\mathbf{F}_p}(X_p/X_{p-1}) &= \begin{cases} \lambda_K^-, & \text{if } t > 0, \\ \lambda_K^- - \delta, & \text{if } t = 0. \end{cases} \end{aligned} \tag{2}$$

For the divisible module A_L^-, we have

$$A_L^- \cong A_1^{a_1} \oplus A_{p-1}^{a_{p-1}} \oplus A_p^{a_p}, \tag{3}$$

where A_1 denotes the trivial G-module $\mathbf{Q}_p/\mathbf{Z}_p$, A_p denotes the divisible regular representation $(\mathbf{Q}_p/\mathbf{Z}_p)[x]/x^p - 1$, and A_{p-1} denotes the divisible faithful representation $(\mathbf{Q}_p/\mathbf{Z}_p)[x]/x^{p-1} + \cdots + x + 1$, for uniquely determined integers a_1, a_{p-1}, a_p.

We separate the ramified and the unramified cases.

L/K ramified. As shown in [**GM**], in this case, $H^{-1}(G, A_L^-) = 1$, $H^{-1}(G, A_1) \cong \mathbf{Z}/p\mathbf{Z}$. Therefore, restricting the decomposition (3) to X_L, we have

$$X_L \cong \left(\frac{\mathbf{F}_p[x]}{(1-x)^{p-1}}\right)^{a_{p-1}} \oplus \left(\frac{\mathbf{F}_p[x]}{(1-x)^p}\right)^{a_p}. \tag{4}$$

Using (2), it follows that

$$\begin{aligned} \dim_{\mathbf{F}_p}(X_i/X_{i-1}) = a_{p-1} + a_p = \lambda_K^- + t - \delta, \qquad i = 1, 2, \ldots, p, \\ \dim_{\mathbf{F}_p}(X_p/X_{p-1}) = a_p = \lambda_K^-. \end{aligned}$$

To evaluate the order of X_E, the p-elementary subgroup of A_E^-, we observe that $(d,p)=1$ implies that it is injected in X_L and can be identified with the subgroup $X_L^{\langle\tau\rangle}$ of X_L consisting of classes which are invariant under τ. We consider the map

$$X_i/X_{i-1} \to X_1, \qquad i=1,2,\dots,p-1,$$

defined by

$$\overline{x} = xX_{i-1} \to x^{(1-\sigma)^{i-1}} = y.$$

By (2), this is an isomorphism of groups. Moreover

$$\begin{aligned}
\overline{x}^\tau = \overline{x} = \overline{x^\tau} &\Leftrightarrow (x^\tau)^{(1-\sigma)^{i-1}} = x^{(1-\sigma)^{i-1}} \\
&\Leftrightarrow x^{\tau(1-\sigma)^{i-1}\tau^{-1}} = (x^{(1-\sigma)^{i-1}})^{\tau^{-1}} \\
&\Leftrightarrow x^{(1-\sigma^\tau)^{i-1}} = (x^{(1-\sigma)^{i-1}})^{\tau^{-1}} \\
&\Leftrightarrow (x^{(1-\sigma)^{i-1}})^{r^{i-1}} = (x^{(1-\sigma)^{i-1}})^{\tau-1} \\
&\Leftrightarrow y^{r^{i-1}} = y^{\tau^{-1}} \\
&\Leftrightarrow y^\tau = y^{r^{1-i}}.
\end{aligned}$$

Thus, the τ-invariant elements correspond to the eigenspace of X_1 for the eigenvalue r^{1-i}. Also, $(1-\sigma)^{p-1}$ maps X_p/X_{p-1} onto X_K injected in X_L and the τ-invariant elements of A_K^- are precisely the elements of A_F^-. Considering that d is the order of r modulo p and $\dim_{\mathbf{F}_p} X_1 = t + \lambda_K^- - \delta$, we have, in this ramified case,

$$\lambda_E^- = \lambda_F^- + \frac{p-1}{d}\dim_{\mathbf{F}_p} X_1 = \lambda_F^- + \frac{p-1}{d}(\lambda_K^- + \tau - \delta).$$

L/K unramified. As shown in [**GM**], in this case $H^0(G, A_L^-) = 1$, $H^0(G, A_{p-1}) = 1$. Therefore, $a_{p-1} = 0$ in the decomposition (3). Thus, restricting to X_L, we have

$$X_L \cong \left(\frac{\mathbf{F}_p[x]}{1-x}\right)^{a_1} \oplus \left(\frac{\mathbf{F}_{[}x]}{(1-x)^p}\right)^{a_p}. \tag{5}$$

Using (2), it follows that

$$\dim_{\mathbf{F}_p}(X_i/X_{i-1}) = a_p = \lambda_K^- - \delta, \qquad i=2,\dots,p.$$
$$\dim_{\mathbf{F}_p} X_1 = a_1 + a_p = \lambda_K^-.$$

We consider the isomorphisms

$$X_i/X_{i-1} \to X_2^{1-\delta}, \qquad i=2,3,\dots,p,$$

induced by

$$\overline{x} = xX_{i-1} \to x^{(1-\sigma)^{i-1}}.$$

As in the ramified case, one can show that the τ-invariant elements correspond to the eigenspace for the eigenvalue r^{1-i}. Further the space of τ-invariant elements of X_1 has dimension λ_F^-. Therefore, λ_E^-, the dimension of the τ-invariant elements of X_p is given by

$$\lambda_E^- = \lambda_F^- + \frac{p-1}{d}(\lambda_K^- - \delta).$$

This completes the arithmetic-algebraic proof of the theorem.

3. The analytic proof. This proof will involve a combination of the techniques of Rück [**R**] and Sinnott [**S**].

First we descend to the finite level. There exist finite number fields F_0, E_0, K_0, L_0 such that $L = L_0 \cdot \mathbf{Q}_\infty$, $F = F_0 \cdot \mathbf{Q}_\infty$, $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(L_0/F_0)$, etc.

Let χ_K denote the regular character of $\mathrm{Gal}(L_0/K_0)$ minus the trivial character of that group. Let χ_E be defined similarly for $\mathrm{Gal}(L_0/E_0)$ and χ_F for $\mathrm{Gal}(K_0/F_0)$. Let $\widehat{\chi}_E$, $\widehat{\chi}_K$ be the characters of $\mathrm{Gal}(L_0/F_0)$ induced from χ_E, χ_K and $\overline{\chi}_F$ the character of $\mathrm{Gal}(L_0/F_0)$ deduced from χ_F in the obvious way. Then Rück [**R**] proves

$$d \cdot \widehat{\chi}_E = d \cdot \overline{\chi}_F + (d-1)\widehat{\chi}_K. \tag{6}$$

We will use Sinnott's method (and notation) to deduce from (6) a relation among p-adic L-functions and, consequently, a relation on λ-invariants. Let S be the set of places (in any appropriate field) which ramify in L_0/F_0^+ together with all places over p. Now (6) gives the following relation among complex L-functions with Euler factors at S omitted.

$$\prod_{\substack{\psi \in \mathrm{Gal}(L_0/E_0)\hat{} \\ \psi \neq 1}} L_S(s, \rho\psi, E_0^+)^d = \prod_{\substack{\psi \in \mathrm{Gal}(K_0/F_0)\hat{} \\ \psi \neq 1}} L_S(s, \rho\psi, F_0^+) \prod_{\substack{\psi \in \mathrm{Gal}(L_0/K_0)\hat{} \\ \psi \neq 1}} L_S(s, \rho\psi, K_0^+)^{d-1}$$

where $\rho = \varepsilon\theta$ for ε the odd quadratic character of F_0/F_0^+, L_0/L_0^+, etc. and θ the Teichmüller character of $F_0^+(\zeta_p)/F_0^+$.

Using the standard properties of complex L-functions we can rewrite this equation as

$$\frac{L_S(s, \rho, L_0^+)^d}{L_S(s, \rho, E_0^+)^d} = \frac{L_S(s, \rho, K_0^+)^d}{L_S(s, \rho, F_0^+)^d} \cdot \frac{L_S(s, \rho, L_0^+)^{d-1}}{L_S(s, \rho, K_0^+)^{d-1}}$$

which simplifies to

$$\frac{L_S(s, \rho, L_0^+)}{L_S(s, \rho, K_0^+)} \cdot L_S(s, \rho, F_0^+)^d = L_S(s, \rho, E_0^+)^d.$$

This yields

$$\left\{ \prod_{\substack{\psi \in \mathrm{Gal}(L_0/K_0)\hat{} \\ \psi \neq 1}} L_S(s, \rho\psi, K_0^+) \right\} \cdot L_S(s, \rho, F_0^+)^d = L_S(s, \rho, E_0^+)^d.$$

Let $\widetilde{L}_S(\chi, k, T)$ be the Iwasawa power series defined by the interpolation property

$$\widetilde{L}_S(\chi, k, \kappa^{1-n} - 1) = L_S(1-n, \chi\theta^{-n}, k)$$

where κ generates $\mathrm{Aut}_{k(\zeta_p)}(k(\zeta_{p^\infty}))$ viewed as a subgroup of $1 + p\mathbf{Z}_p$.

Our basic equation holds for $L_S(s, \chi, k)$ replaced by $\widetilde{L}_S(\chi, k, T)$.

Denoting (as in [S]) the λ-invariant of the power series $\widetilde{L}_S(\chi, k, T)$ by $\lambda_S(\chi, k)$, we obtain

$$\sum_{\substack{\psi \in \mathrm{Gal}(L_0/K_0)\hat{} \\ \psi \neq 1}} \lambda_S(\rho\psi, K_0^+) + d \cdot \lambda_S(\rho, F_0^+) = d \cdot \lambda_S(\rho, E_0^+).$$

By Proposition 2.1 in Sinnott [S] and the fact that $\mathrm{Gal}(L_0/K_0)$ has order p, we have

$$\frac{p-1}{d}\lambda_S(\rho, K_0^+) + \lambda_S(\rho, F_0^+) = \lambda_S(\rho, E_0^+). \tag{7}$$

It remains now to relate each $\lambda_S(\rho, k_0^+)$ to the corresponding λ_k^-. But $\lambda_k^- = \lambda_{S'}(\rho, k_0^+) + \delta(k)$ [S, Proposition 3.1] where S' is the set of places of k_0^+ which ramify in $k_0 \cdot Q_\infty/k_0^+$. The required relation is given [S, Lemma 2.1] by

$$\lambda_S(\rho, k_0^+) = \lambda_k^- + \sum_{\mathscr{P}}^{(k)} g(\mathscr{P}) - \delta(k) \quad \text{for } k = F, E, K \tag{8}$$

where the sum is over all places $\mathscr{P}$ in S/k which are not ramified in k/k_0^+ such that $\mathscr{P}$ is split in k_0/k_0^+, $g(\mathscr{P})$ is the number of places of k^+ lying over $\mathscr{P}$, and $\delta(k) = 1, 0$ as k contains a pth-root of unity or not.

In light of (7) and (8), the theorem will follow if we can show that

$$\frac{p-1}{d}\sum_{\mathscr{P}}^{(K)} g(\mathscr{P}) + \sum_{\mathscr{P}}^{(F)} g(\mathscr{P}) - \sum_{\mathscr{P}}^{(E)} g(\mathscr{P}) = \frac{p-1}{d}t.$$

This equality can be verified by considering the contribution to both members of each non-p-prime $\mathscr{P}$ of F_0^+ which is ramified in L_0/F_0^+. This is achieved by a nontrivial but routine and somewhat tedious examination of cases depending on the splitting behavioir of $\mathscr{P}$ in L_0/F_0^+. We omit the proof.

4. Remarks. 1. As stated in the Introduction, Kida's Theorem is an analogue of a theorem of Deuring and Safarevic. It may also be viewed as a formal analogue of the Riemann-Hurwitz genus formula.

2. Our theorem generalizes Kida's Theorem to a class of extensions of degree p. The restriction to extensions of degree p is not essential. Using induction, it can be routinely extended (as in [K, Sa, S]) to extensions E/F such that for the normal closure L, $\mathrm{Gal}(L/F)$ is the semidirect product of the normal subgroup $\mathrm{Gal}(L/K)$ of p-power order and the cyclic subgroup $\mathrm{Gal}(L/E)$ of order dividing $p-1$.

3. We give an example of the application of our theorem.

Let $F = \mathbf{Q}(\sqrt{-6})$ and $E = \mathbf{Q}(\sqrt{-6}, \alpha)$ where α is a root of $x^3 - 11x - 11$. The field $\mathbf{Q}(\alpha)$ is a totally real cubic of discriminant $11^2 \cdot 17$ and normal closure $\mathbf{Q}(\alpha, \sqrt{17})$. Therefore $K^+ = \mathbf{Q}(\sqrt{17})$, $K = \mathbf{Q}(\sqrt{17}, \sqrt{-6})$, $L = \mathbf{Q}(\sqrt{17}, \sqrt{-6}, \alpha)$ and 11 is totally ramified in L/K. Since 3 does not divide the class number of K and there is a unique prime over 3 in K, the invariant λ_K^-, λ_F^- are both zero [W]. It is easy to check that $t = 1$ and $\delta = 0$. Hence by the formula of our theorem, $\lambda_E^- = 1$ and $\lambda_L^- = 2$.

REFERENCES

[**DM**] J. D'Mello and M. Madan, *Class group rank relations in* $\mathbf{Z}_l$*-extensions*, Manuscripta Math. **41** (1983), 75–107.

[**GM**] R. Gold and M. Madan, *Galois representations of Iwasawa modules*, Acta Arith. **46** (1986), 243–255.

[**I**] K. Iwasawa, *On the* μ*-invariants of* $\mathbf{Z}_l$*-extensions*, Number Theory, Algebraic Geometry and Commutative Algebra, Kinokuniya, Tokyo, 1973.

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

[**R**] H.-G. Rück, *Hass-Witt-invariants and dihedral extensions*, Math. Z. **191** (1986), 513–517.

[**Sa**] I. R. Safarevic, *On p-extensions*, Amer. Math. Soc. Transl. (2) **4** (1954).

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

[**W**] L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, Berlin and New York, 1982.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210