R. Greenberg
Nagoya Math. J.
Vol. 67 (1977), 139-158

ON p-ADIC L-FUNCTIONS AND CYCLOTOMIC FIELDS. II

RALPH GREENBERG*

1. Introduction

Let p be a prime. If one adjoins to $\boldsymbol{Q}$ all p^n-th roots of unity for $n = 1, 2, 3, \cdots$, then the resulting field will contain a unique subfield $\boldsymbol{Q}_\infty$ such that $\boldsymbol{Q}_\infty$ is a Galois extension of $\boldsymbol{Q}$ with $\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q}) \cong \boldsymbol{Z}_p$, the additive group of p-adic integers. We will denote $\mathrm{Gal}(\boldsymbol{Q}_\infty/\boldsymbol{Q})$ by Γ. In a previous paper [6], we discussed a conjecture relating p-adic L-functions to certain arithmetically defined representation spaces for Γ. Now by using some results of Iwasawa, one can reformulate that conjecture in terms of certain other representation spaces for Γ. This new conjecture, which we believe may be more susceptible to generalization, will be stated below.

Let $\boldsymbol{Q}_p$ be the field of p-adic numbers and let Ω_p be an algebraic closure of $\boldsymbol{Q}_p$. Let ψ be an even primitive Dirichlet character which takes its values in Ω_p and which is of the first kind (this means that the conductor of ψ is not divisible by p^2 if p is odd or by 8 if $p = 2$). Let K be the cyclic extension of $\boldsymbol{Q}$ associated to ψ by class field theory and let $K_\infty = K\boldsymbol{Q}_\infty$, the cyclotomic $\boldsymbol{Z}_p$-extension of K. Let M_∞ denote the maximal abelian pro-p-extension of K_∞ in which only primes of K_∞ dividing p are ramified. (We also allow the infinite primes to be ramified, although this could happen only if $p = 2$). Now Γ can be identified in a natural way with $\mathrm{Gal}(K_\infty/K)$ and, by means of this identification, we can consider $\mathrm{Gal}(M_\infty/K_\infty)$ as a Γ-module. One can then define quite simply a certain representation space W_ψ for Γ over Ω_p (see Section 2).

In [11], Leopoldt and Kubota have constructed a p-adic L-function $L_p(s, \psi)$ for every primitive even Dirichlet character ψ. This function is defined for all $s \in \boldsymbol{Z}_p$ (except for $s = 1$ if ψ is the principal character ψ_0) and takes its values in Ω_p. Now it follows easily from a result of

Received September 10, 1976.
* This research was supported in part by National Science Foundation Grant MCS75-09446 A01.

Iwasawa that there exists a power series $G_\psi^*(T)$ whose coefficients are integers in the field $\boldsymbol{Q}_p(\psi)$ generated by the values of ψ and which has the property that

$$L_p(1-s,\psi) = \frac{G_\psi^*(\kappa_0^s - 1)}{(\kappa_0^s - 1)^\delta},$$

where κ_0 is a certain p-adic unit defined in [6] and $\delta = 1$ or 0 according to whether ψ is principal or non-principal. We use the notation $G_\psi^*(T)$ since this power series can be constructed quite simply from the power series denoted by $G_\psi(T)$ in [6]. Let $g_\psi^*(T)$ denote the monic polynomial whose roots (counting multiplicity) are precisely the (finitely-many) roots of the power series $G_\psi^*(T)$ in Ω_p. Let γ_0 be a fixed topological generator for Γ (corresponding to the choice of κ_0) and let $h_\psi(T)$ denote the characteristic polynomial of $\gamma_0 - 1$ acting on W_ψ. We now state the conjecture referred to above.

CONJECTURE. $\qquad h_\psi(T) = g_\psi^*(T)$.

At the end of Section 2, we will discuss several results supporting this conjecture (mostly translations of analogous results proved in [6]).

In Section 3, we will consider a slightly more general question. Let S be any finite set of primes of K containing all primes dividing p. Let $M_\infty(S)$ denote the maximal abelian pro-p-extension of K_∞ in which only primes of K_∞ dividing primes in S are ramified. Then $\mathrm{Gal}\,(M_\infty(S)/K_\infty)$ can be considered as a Γ-module and one can therefore construct a representation space $W_\psi(S)$ for Γ. Denote by $h_{\psi,S}(T)$ the characteristic polynomial of $\gamma_0 - 1$ acting on $W_\psi(S)$. On the other hand, consider the (usually) non-primitive Dirichlet character ψ_S defined by $\psi_S(a) = \psi(a)$ if a is not divisible by any prime in S and $\psi_S(a) = 0$ otherwise. One can then easily define a p-adic L-function $L_p(s,\psi_S)$ for the non-primitive character ψ_S and, just as above, one can define a corresponding power series $G_{\psi_S}^*(T)$ and a polynomial $g_{\psi_S}^*(T)$. As a consequence of the conjecture stated above, we will show that $h_{\psi,S}(T) = g_{\psi_S}^*(T)$. In the particular case when S contains only the primes dividing p, the function $L_p(s,\psi_S)$ is the same as $L_p(s,\psi)$ and therefore $g_{\psi,S}^*(T) = g_\psi^*(T)$. Of course, $h_{\psi,S}(T) = h_\psi(T)$ also. The above result is closely related to Proposition 3.4 in Coates' and Lichtenbaum's paper [3].

In Section 4, we will discuss the structure of the torsion subgroup of $\mathrm{Gal}\,(M_\infty/K_\infty)$ as a Γ-module and its relationship to p-adic L-functions.

In this connection, the prime $p = 2$ seems especially interesting. It is known that every coefficient of the power series $G_\psi^*(T)$ is divisible by 2. Correspondingly, the μ-invariant of the Γ-module $\mathrm{Gal}(M_\infty/K_\infty)$ is non-zero for $p = 2$. In our previous paper [6] and in most of this paper we have tended to ignore (mainly for simplicity) the torsion subgroup of various Γ-modules by tensoring with Ω_p and thus forming representation spaces for Γ. This allows us to avoid difficulties that occur when p divides $[K: \boldsymbol{Q}]$. (In [3], the Γ-modules themselves are studied but often with the assumption that p does not divide $[K: \boldsymbol{Q}]$.) This section is therefore meant to complement the previous sections.

In the concluding section of this paper, we will show that the conjecture stated above (together with the analogous conjecture for the torsion subgroup of $\mathrm{Gal}(M_\infty/K_\infty)$ described at the end of Section 4) leads to a solution of a question recently raised by G. Gras in [5]. Let K be a totally real abelian extension of $\boldsymbol{Q}$ and let p be an odd prime not dividing $[K: \boldsymbol{Q}]$. It is a well-known result that the class number of K is essentially (except for the contribution of primes dividing $[K: \boldsymbol{Q}]$ and the prime 2) equal to the index of the so-called cyclotomic units C_K of K in the full unit group E_K of K. Now, although the p-primary subgroups of the ideal class group of K and of the group E_K/C_K can have quite different structures as groups, they seem to have a close relationship as Galois modules for $\mathrm{Gal}(K/\boldsymbol{Q})$. This is the question we will study in Section 5.

2. Equivalence of two conjectures

In this section, we will prove that the conjecture stated in the introduction to this paper is equivalent to the one stated in the introduction of [6]. Although this result follows immediately from results of [10], we will try to give a fairly self-contained account. The basis of the argument is Kummer theory.

Let K be a totally real abelian extension of $\boldsymbol{Q}$ of the first kind (but not necessarily cyclic for now). Thus $K \cap \boldsymbol{Q}_\infty = \boldsymbol{Q}$ and $K_\infty = K\boldsymbol{Q}_\infty$ is a Galois extension of $\boldsymbol{Q}$ with $G = \mathrm{Gal}(K_\infty/\boldsymbol{Q})$ isomorphic (by restriction) to $\Delta \times \Gamma$, where $\Delta = \mathrm{Gal}(K/\boldsymbol{Q})$. Let M_∞ be defined as in the introduction. Let $Y = Y_K = \mathrm{Gal}(M_\infty/K_\infty)$. Then G acts on Y as follows: If $g \in G$ and $y \in Y$, we define $g(y) = \bar{g}y\bar{g}^{-1}$, where $\bar{g}$ denotes any extension of g to an automorphism of M_∞. Now it will be apparent later that $Y \cong \boldsymbol{Z}_p^d$

$\times T$ as a Z_p-module, where d is an integer and T is a torsion group of bounded exponent (see Theorem 3 of [7]). Thus, letting $W_K = Y \otimes_{Z_p} \Omega_p$, we see that W_K is a finite dimensional representation space for G. If ψ is any Ω_p-valued character of the group Δ, we define

$$W_\psi = \{w \in W_K \mid \delta(w) = \psi(\delta)w \text{ for all } \delta \in \Delta\} .$$

Thus for each such ψ we obtain the representation space W_ψ for Γ. Now if ψ is any even Ω_p-valued Dirichlet character of the first kind, then, by class field theory, ψ can also be considered as a character of Δ for some choice of K, and hence one can associate to ψ a representation space for Γ which we also denote by W_ψ. (It can be easily seen that a different choice of K will provide an equivalent representation space for Γ.)

Now let $\bar{K} = K(\zeta_p)$ (or $K(i)$ if $p = 2$), where ζ_p is a primitive p-th root of unity. To simplify the notation in the following, we assume that K has been chosen so that $[\bar{K}: K] = 2$, i.e. K is the maximal real subfield of $\bar{K}$. The field $\bar{K}_\infty = \bar{K}\boldsymbol{Q}_\infty$ will contain all roots of unity of order a power of p. Let $\bar{M}_\infty$ denote the maximal p-ramified abelian pro-p-extension of $\bar{K}_\infty$. We will study this extension from the point of view of Kummer theory.

Let $n \geq 1$ and let $P_n = \{a \in \bar{K}_\infty^\times \mid \sqrt[p^n]{a} \in \bar{M}_\infty\}$. Since the primes of $\bar{K}$ dividing p are totally ramified in $\bar{K}_\infty$, it is clear that $a \in P_n$ if and only if $(a) = \mathfrak{a}^{p^n}$, where $\mathfrak{a}$ is a fractional ideal in $\bar{K}_m$ for some m, (where $\bar{K}_m$ denotes the unique subfield of $\bar{K}_\infty$ of degree p^m over $\bar{K}$). Let $\bar{Y} = \mathrm{Gal}(\bar{M}_\infty/\bar{K}_\infty)$. If $a \in P_n$ and $y \in \bar{Y}$, we define $(a, y) = y(\sqrt[p^n]{a})/\sqrt[p^n]{a}$, which is a p^n-th root of unity. If $g \in \mathrm{Gal}(\bar{K}_\infty/\boldsymbol{Q})$, then g acts on $\bar{Y}$ (just as defined before for Y) and one can easily see that

$$(g(a), g(y)) = g((a, y))$$

for all $a \in P_n$ and $y \in \bar{Y}$. In particular, if J is the non-trivial element of $\mathrm{Gal}(\bar{K}_\infty/K_\infty)$ (i.e. complex conjugation), then

$$(J(a), J(y)) = (a, y)^{-1} .$$

Now let $\bar{M}_\infty^+$ denote the maximal subfield of $\bar{M}_\infty$ which is abelian over K_∞. Note that $M_\infty \bar{K}_\infty = \bar{M}_\infty^+$ (for $p = 2$, $M_\infty = \bar{M}_\infty^+$). It is clear that $\mathrm{Gal}(\bar{M}_\infty/\bar{M}_\infty^+)$ is $(1 - J)\bar{Y}$, the commutator subgroup of $\mathrm{Gal}(\bar{M}_\infty/K_\infty)$. Let $R_n = \{a \in P_n \mid \sqrt[p^n]{a} \in \bar{M}_\infty^+\}$. One can describe R_n more simply as follows.

If $a \in P_n$, then $a \in R_n$ if and only if $(a, (1-J)y) = 1$, or equivalently $(aJ(a), y) = 1$, for all $y \in \overline{Y}$. This would imply that $aJ(a) \in (\overline{K}_\infty^\times)^{p^n}$. Thus $R_n = \{a \in P_n \mid aJ(a) \in (\overline{K}_\infty^\times)^{p^n}\}$. If we let $\overline{Y}_+ = \mathrm{Gal}(\overline{M}_\infty^+/\overline{K}_\infty)$, then by Kummer theory it follows that $\overline{Y}_+/\overline{Y}_+^{p^n}$ and $R_n/(\overline{K}_\infty^\times)^{p^n}$ are dual to each other.

Now let $\overline{A}_n$ denote the p-primary subgroup of the ideal class group of $\overline{K}_n$ and let $\overline{A}_\infty = \varinjlim \overline{A}_n$, where the direct limit is taken with respect to the maps $\overline{A}_n \to \overline{A}_m$ induced by the inclusion $\overline{K}_n \to \overline{K}_m$ for $m \geq n \geq 0$. There is a natural homomorphism $\varphi_n : P_n \to \overline{A}_\infty$ defined by $\varphi_n(a) = \mathrm{Cl}(\mathfrak{a})$ if $a \in P_n$ and $\mathfrak{a}^{p^n} = (a)$. Here $\mathfrak{a}$ is an ideal in $\overline{K}_m$ for some m and $\mathrm{Cl}(\mathfrak{a})$ is the image of the ideal class of $\mathfrak{a}$ in the direct limit $\overline{A}_\infty$. It is clear that φ_n is a $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$-homomorphism and that their kernel of φ_n contains $(\overline{K}_\infty^\times)^{p^n}$. If we let $\overline{A}_\infty^- = \{c \in \overline{A}_\infty \mid cJ(c) = 1\}$, then φ_n gives a homomorphism from R_n to $\overline{A}_\infty^-$.

Assume now that p is odd. We will show that φ_n induces an isomorphism of $R_n/(\overline{K}_\infty^\times)^{p^n}$ onto the subgroup of $\overline{A}_\infty^-$ of elements of order dividing p^n. Let $a \in R_n \cap \mathrm{Ker}(\varphi_n)$. Then $a = b^{p^n} \cdot u$, where $b \in \overline{K}_\infty^\times$ and u is a unit in the ring of integers of $\overline{K}_\infty$. Also $uJ(u) \in (\overline{K}_\infty^\times)^{p^n}$. Since p is odd, it is not hard to see that b and u can be chosen so that $uJ(u) = 1$. However, it follows from this that u is a root of unity and hence a p^n-th power in $\overline{K}_\infty^\times$. Thus $R_n \cap \mathrm{Ker}(\varphi_n) = (\overline{K}_\infty^\times)^{p^n}$. Now let $c \in \overline{A}_\infty^-$, $c^{p^n} = 1$. Since p is odd, one can find an ideal of the form $\mathfrak{a} = \mathfrak{b}/J(\mathfrak{b})$ in c, where $\mathfrak{b}^{p^n} = (b)$ is principal. Thus, $\mathfrak{a}^{p^n} = (a)$, where $a = b/J(b)$. Then $a \in R_n$ and $\varphi_n(a) = c$.

The above remarks allow us to define a pairing of $\overline{A}_\infty^-$ and $\overline{Y}_+$ into the group of p-power roots of unity. If $c \in \overline{A}_\infty^-$, choose n large enough so that $c^{p^n} = 1$ and choose $a \in R_n$ so that $\varphi_n(a) = c$. Then if $y \in \overline{Y}_+$, we define $\langle c, y \rangle = (a, y)$. This is a well-defined perfect pairing (considering $\overline{A}_\infty^-$ with the discrete topology). Also, if $g \in \mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$, then

$$\langle g(c), g(y) \rangle = g(\langle c, y \rangle)$$

for all $c \in \overline{A}_\infty^-$ and $y \in \overline{Y}_+$.

Now there is a natural homomorphism κ from $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$ to the group of p-adic units defined by

$$g(\zeta_{p^n}) = \zeta_{p^n}^{\kappa(g)}$$

for all n. The pairing defined in the previous paragraph therefore has the property that

$$\langle g(c), y\rangle = \langle c, \kappa(g)g^{-1}(y)\rangle$$

for all $c \in \overline{A}_\infty^-$, $y \in \overline{Y}_+$, and $g \in \mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$. We will let X denote the Pontrjagin dual of $\overline{A}_\infty$. If $g \in \mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$ and $x \in X$, we define $g(x)$ by

$$g(x)(c) = x(g(c))$$

for all $c \in \overline{A}_\infty$. If $X^- = \{x \in X \mid xJ(x) = 1\}$, then X^- is clearly the dual of $\overline{A}_\infty^-$. Thus X^- and $\overline{Y}_+$ are isomorphic as topological groups. Now consider $\dot{X}^-$, a topological group identical to X^- but with a new action of $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$ defined by $g \circ x = \kappa(g)g^{-1}(x)$. Then $\dot{X}^-$ and $\overline{Y}_+$ are isomorphic as $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$-modules. However, $J \circ x = x$ for $x \in X^-$ and so X^- and $\overline{Y}_+$ can be considered as $\mathrm{Gal}(K_\infty/\boldsymbol{Q})$-modules. Also, $\overline{Y}_+$ is isomorphic to Y as a $\mathrm{Gal}(K_\infty/\boldsymbol{Q})$-module and therefore we have the following proposition:

PROPOSITION 1. *Let p be an odd prime. Then $\dot{X}^-$ and Y are isomorphic as* $\mathrm{Gal}(K_\infty/\boldsymbol{Q})$*-modules.*

We will now consider $p = 2$. Since we are allowing the infinite primes to be ramified in M_∞/K_∞, it is clear that M_∞ contains $N_\infty = K_\infty(\sqrt[2]{u} \mid u \in E_\infty)$, where E_∞ is the group of units from the ring of integers of K_∞. Let $Y_0 = \mathrm{Gal}(M_\infty/N_\infty)$ so that $Y/Y_0 = \mathrm{Gal}(N_\infty/K_\infty)$ is isomorphic to the dual of E_∞/E_∞^2 (with a twisted $\mathrm{Gal}(K_\infty/\boldsymbol{Q})$ action). Thus it is obvious that the Γ-module Y has non-zero μ-invariant. We will describe E_∞/E_∞^2 more precisely in Section 4. On the other hand, Y_0 is closely related to $\overline{A}_\infty^-$ and X^-. In fact, Y_0 and $\dot{X}^-$ are pseudo-isomorphic as G-modules (i.e. there is a G-homomorphism between them with finite kernel and cokernel). To see this, we must use the fact that $\overline{A}_\infty$ and X have μ-invariant equal to zero and hence X is finitely generated as a $\boldsymbol{Z}_p$-module. (This has been proved by B. Ferrero in [4] when $K/\boldsymbol{Q}$ is abelian and $p = 2$ or 3.) It follows from this that $(\overline{A}_\infty^-)^2$ is of finite index in $\overline{A}_\infty^-$ and therefore the union of the images $\varphi_n(R_n)$ is also of finite index in $\overline{A}_\infty^-$. Also, one can verify easily that $R_n \cap \mathrm{Ker}(\varphi_n)$ contains $(E_\infty)^{2^{n-1}} \cdot (\overline{K}_\infty^\times)^{2^n}$ as a subgroup of finite index. In addition, X^- is pseudo-isomorphic to the dual of $\overline{A}_\infty^-$ and the dual of E_∞/E_∞^2 is pseudo-isomorphic to the twisted version of itself referred to above. (This last fact will be more evident later.) Combining all of these remarks, we obtain the following proposition.

PROPOSITION 2. *Let $p = 2$. The $\mathrm{Gal}(K_\infty/\boldsymbol{Q})$-module Y contains a submodule Y_0 pseudo-isomorphic to $\dot{X}^-$ such that Y/Y_0 is pseudo-isomorphic to the dual of E_∞/E_∞^2.*

We can now relate the structure of the representation space W_ψ (defined above) and another representation space V_χ for Γ. Let $\bar{\Delta} = \mathrm{Gal}(\overline{K}/\boldsymbol{Q})$ so that $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q}) \cong \bar{\Delta} \times \Gamma$. If $V_{\overline{K}} = X \otimes_{Z_p} \Omega_p$ and if χ is an Ω_p-valued character of $\bar{\Delta}$, we define

$$V_\chi = \{v \in V_{\overline{K}} \mid \delta(v) = \chi(\delta)v \text{ for all } \delta \in \bar{\Delta}\} .$$

The representation space for Γ defined in [6] and also denoted by V_χ is equivalent to the one just defined here. (In [6], we use the inverse limit $X' = \varprojlim \overline{A}_n$ with respect to the norm maps instead of X. But X is the adjoint of X' and so X and X' are pseudo-isomorphic as $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$-modules. Letting $V_{\overline{K}}^- = \{v \in V_{\overline{K}} \mid J(v) = -v\} = \sum_{\text{odd } \chi} V_\chi$, we see that $V_{\overline{K}}^- \cong X^- \otimes_{Z_p} \Omega_p$. Let ω denote the restriction of κ to $\bar{\Delta}$. (This of course corresponds to the Dirichlet character ω defined in [6].) If we define $\dot{V}_{\overline{K}}^-$ and $\dot{V}_\chi$ in the same way as $\dot{X}^-$, then Propositions 1 and 2 show that $\dot{V}_{\overline{K}}^-$ and W_K are isomorphic as representation spaces for $\mathrm{Gal}(\overline{K}_\infty/\boldsymbol{Q})$ and in this isomorphism $\dot{V}_\chi$ is mapped to W_ψ where χ and ψ are related by the equation $\chi\psi = \omega$ (considering ψ as a character of $\bar{\Delta}$ with $\psi(J) = +1$). In the terminology of [6], the primitive Dirichlet characters corresponding to χ and ψ would be dual.

We therefore have proved the following proposition.

PROPOSITION 3. *If $\chi\psi = \omega$, then $\dot{V}_\chi$ and W_ψ are isomorphic as representation spaces for Γ.*

We can now easily relate the conjecture stated in the introduction with the conjecture stated in [6]. Let χ and ψ be as in Proposition 3. If γ_0 is a fixed topological generator of Γ and if $\kappa_0 = \kappa(\gamma_0)$, then clearly an element β of Ω_p will be an eigenvalue of $\gamma_0 - 1$ acting on V_χ if and only if $\kappa_0(1 + \beta)^{-1} - 1$ is an eigenvalue of $\gamma_0 - 1$ acting on W_ψ (and with the same multiplicity). Thus if $f_\chi(T)$ denotes the characteristic polynomial of $\gamma_0 - 1$ acting on V_χ (as in [6]), then the roots of $f_\chi(T)$ determine in this way the roots of $h_\psi(T)$. On the other hand, the roots of $g_\psi^*(T)$ and the polynomial $g_\psi(T)$ defined in [6] are related in exactly the same way because the transformation $s \to 1 - s$ corresponds to the transformation $T \to \kappa_0(1 + T)^{-1} - 1$. Thus the conjecture that $h_\psi(T) = g_\psi^*(T)$ is equivalent

to the conjecture stated in [6] that $f_\chi(T) = g_\psi(T)$. All of the results proved in [6] can be translated to similar results about W_ψ and $h_\psi(T)$. Thus Theorem 1 of [6] gives us the following proposition.

PROPOSITION 4. *Let ψ be an even character of the first kind. Then $g_\psi^*(\gamma_0 - 1)$ annihilates W_ψ.*

Proposition 4 immediately implies several results. For example, every root of $h_\psi(T)$ must also be a root of $g_\psi^*(T)$. Then, using the fact that $L_p(1-n, \psi) \neq 0$ for $n \geq 2$, we see that $h_\psi(\kappa_0^n - 1) \neq 0$ for $n \geq 2$. On the other hand, it follows from the definition of p-adic L-functions that $L_p(0, \psi)$ is zero precisely when $\chi(p) = 1$. The condition $\chi(p) = 1$ also determines exactly when $h_\psi(\kappa_0 - 1) = 0$ and so $\kappa_0 - 1$ is a root of $g_\psi^*(T)$ if and only if it is a root of $h_\psi(T)$. It is also interesting to consider the case $n = 0$. The non-vanishing of the p-adic regulator of the abelian extension K of $\boldsymbol{Q}$ (a result proved by Brumer in [1]) implies that $h_\psi(0) \neq 0$. But Brumer's result together with Leopoldt's evaluation of $L_p(1, \psi)$ (see [9]) also implies that $L_p(1, \psi) \neq 0$ and therefore $g_\psi^*(0) \neq 0$.

We will close this section by describing some results concerning the degrees of the above polynomials. It is clear from Proposition 3 that $f_\chi(T)$ and $h_\psi(T)$ have the same degree when $\chi\psi = \omega$. It is also clear that $g_\psi(T)$ and $g_\psi^*(T)$ have the same degree. By using our assumptions that $[\overline{K}: K] = 2$, Theorem 2 of [6] implies immediately that

$$\sum_\psi \deg (h_\psi(T)) = \sum_\psi \deg (g_\psi^*(T))$$

where ψ varies over all characters belonging to K. However, by making use of a recent result of J. Coates (Theorem 1.13 of [2]) together with Leopoldt's residue formula for the p-adic zeta function of totally real abelian number fields, one obtains the following improvement. We assume that p is odd.

PROPOSITION 5. *Let K be any abelian totally real number field of the first kind. Then, as ψ varies over all characters belonging to K,*

$$\sum_\psi \deg (h_\psi(T)) = \sum_\psi \deg (g_\psi^*(T)) \, .$$

The proof of this result is completely analogous to the proof of Theorem 2 in [6]. Also, by considering various K's, one obtains the same conclusion if ψ varies over a set of characters conjugate over $\boldsymbol{Q}$.

Finally, just as in [6], if the character ψ has the property that $[\boldsymbol{Q}(\psi):\boldsymbol{Q}] = [\boldsymbol{Q}_p(\psi):\boldsymbol{Q}_p]$, then one can conclude that $h_\psi(T)$ and $g^*_\psi(T)$ have the same degree.

3. *p*-adic *L*-functions for non-primitive characters

Let ψ be a primitive even Ω_p-valued Dirichlet character. Then, as explained in Section 4 of [6], one can easily define an element $L(1-n,\psi)$ of Ω_p for every $n \geq 1$ which can be considered as a p-adic analogue of the corresponding values of a complex Dirichlet L-function. If S is a finite set of primes containing p, we let ψ_S be as defined in Section 1. Thus, if S contains some primes which do not divide the conductor of ψ, then ψ_S is a non-primitive character and it is natural to define the following analogues of the values of a complex non-primitive Dirichlet L-series:

$$L(1-n,\psi_S) = L(1-n,\psi)\prod_{\ell\in S}(1-\psi(\ell)\ell^{n-1}) .$$

If $S=\{p\}$, then $L(1-n,\psi_S) = L^*(1-n,\psi)$ in the notation of [6] and the p-adic L-function $L_p(s,\psi)$ of Leopoldt and Kubota is completely determined by the property

$$L_p(1-n,\psi) = L^*(1-n,\psi)$$

for all $n \equiv 0 \pmod{p-1}$ (or mod 2 if $p=2$). Now if ℓ is a prime different from p, we write ℓ, as usual, in the form $\ell = \omega(\ell)\langle\ell\rangle$, where $\langle\ell\rangle \equiv 1 \pmod p$ (or 4 if $p=2$). Then $1-\psi(\ell)\ell^{n-1} = 1-\psi\omega^{-1}(\ell)\langle\ell\rangle^{n-1}$ for $n \equiv 0 \pmod{p-1 \text{ or } 2}$. We thus define a function $L_p(s,\psi_S)$ by

$$L_p(s,\psi_S) = L_p(s,\psi)\prod_{\ell\in S_0}(1-\psi\omega^{-1}(\ell)\langle\ell\rangle^{-s}) .$$

Here we are letting $S_0 = S-\{p\}$. This function, which is defined and continuous for all $s\in\boldsymbol{Z}_p$ (except perhaps $s=1$) has the property

$$L_p(1-n,\psi_S) = L(1-n,\psi_S)$$

for all $n \equiv 0 \pmod{p-1 \text{ or } 2}$. Note that if $S=\{p\}$, then $L_p(s,\psi_S)$ is identical to $L_p(s,\psi)$.

By multiplying the power series $G^*_\psi(T)$ by certain other power series corresponding to the primes ℓ in $S_0 = S-\{p\}$, one can form a power series $G^*_{\psi_s}(T)$ with the property that

$$L_p(1-s,\psi_S)=\frac{G^*_{\psi S}(\kappa_0^s-1)}{(\kappa_0^s-1)^\delta}\ .$$

The power series $G^*_{\psi S}$ is associated with a polynomial $g^*_{\psi S}(T)$ which is divisible by $g^*_\psi(T)$. It is not hard to describe the roots of $g^*_{\psi S}(T)/g^*_\psi(T)$ corresponding to each $\ell\in S_0$. If one writes $\langle\ell\rangle=\kappa_0^{a_\ell}$, where a_ℓ is a p-adic integer, then these roots are precisely the roots of the power series

$$1-\psi\omega^{-1}(\ell)\langle\ell\rangle^{-1}(1+T)^{a_\ell}\ .$$

If $\psi\omega^{-1}(\ell)$ is not a p-power root of unity, this power series is invertible and no new roots occur. If $\psi\omega^{-1}(\ell)$ is a p-power root of unity, then the new roots are those of the polynomial

$$(1+T)^{p^{e_\ell}}-(\langle\ell\rangle\omega\psi^{-1}(\ell))^{u_\ell^{-1}}\ ,$$

where $a_\ell=p^{e_\ell}\cdot u_\ell$ with u_ℓ a p-adic unit. We must now relate these roots to the eigenvalues of γ_0-1 acting on a certain representation space for Γ. Now $\mathrm{Gal}\,(M_\infty(S)/K_\infty)\otimes_{Z_p}\Omega_p$ is a representation space for $\mathrm{Gal}\,(K_\infty/\boldsymbol{Q})=\Delta\times\Gamma$ whose ψ-component we denote by $W_\psi(S)$. We will soon see that $W_\psi(S)$ is finite dimensional. Since $M_\infty\subset M_\infty(S)$, it is clear that the ψ-component of $\mathrm{Gal}\,(M_\infty(S)/M_\infty)\otimes_{Z_p}\Omega_p$, which we will denote by $U_\psi(S_0)$, is contained in $W_\psi(S)$ and that the corresponding quotient space $W_\psi(S)/U_\psi(S_0)$ is isomorphic to W_ψ (as a representation space for Γ). The characteristic polynomial of γ_0-1 on $U_\psi(S_0)$ is obviously $h_{\psi S}(T)/h_\psi(T)$. We will show that the characteristic polynomial is also $g^*_{\psi S}(T)/g^*_\psi(T)$ and thus that

$$h_{\psi S}(T)/h_\psi(T)=g^*_{\psi S}(T)/g^*_\psi(T)\ .$$

Therefore, the conjecture stated in the introduction is equivalent to the statement that $h_{\psi S}(T)=g^*_{\psi S}(T)$.

To study the structure of $U_\psi(S_0)$, we will examine $M_\infty(S)$ from the point of view of Kummer theory. We still assume that $[\overline{K}\colon K]=2$. Let B denote the subgroup of $\overline{K}_\infty^\times$ consisting of all S_0-units b such that $bJ(b)=1$. Now, for each $\ell\in S_0$, there are only finitely many primes of $\overline{K}_\infty$ lying over ℓ, and therefore B (modulo all roots of unity in $\overline{K}_\infty$) is a finitely generated group. Let $L_{S_0}=\overline{K}_\infty(\{\sqrt[p^n]{b}\mid b\in B,\ n\geq 0\})$. The field L_{S_0} is clearly contained in $M_\infty(S)\overline{K}_\infty$. In fact, for odd p, $M_\infty(S)\overline{K}_\infty=L_{S_0}M_\infty$. To see this, we observe that $\overline{K}_\infty(\sqrt[p^n]{a})\subseteq M_\infty(S)\overline{K}_\infty$ if and only if $aJ(a)\in(\overline{K}_\infty^\times)^{p^n}$ and (a) can be written as $\mathfrak{b}\mathfrak{c}^{p^n}$, where $\mathfrak{b}$ is an ideal (in

some $\overline{K}_m$) divisible only by primes dividing those in S. There is an integer t such that $\mathfrak{b}^t$ is principal. Then, if p is odd, one finds that a^t can be expressed in the form $a^t = bc$, where $b \in B$ and (c) is a p^{n+r}-th power of an ideal in $\overline{K}_\infty$, where p^r is the highest power of p dividing t. It follows that

$$\overline{K}_\infty(\sqrt[p^n]{a}) = \overline{K}_\infty(\sqrt[p^{n+r}]{a^t}) \subseteq \overline{K}_\infty(\sqrt[p^{n+r}]{b})\overline{K}_\infty(\sqrt[p^{n+r}]{c}) \subseteq L_{S_0} \cdot M_\infty .$$

Therefore, $M_\infty(S)\overline{K}_\infty = L_{S_0}M_\infty$. Now, it is easy to see that $[L_{S_0} \cap (M_\infty\overline{K}_\infty) : \overline{K}_\infty] < \infty$. We conclude that $U_\psi(S_0)$ is isomorphic to the ψ-component of $\mathrm{Gal}\,(L_{S_0}/\overline{K}_\infty) \otimes_{Z_p} \Omega_p$. We also see (although we won't need this result) that

$$W_\psi(S) \cong U_\psi(S_0) \times W_\psi$$

as representation spaces for Γ. For $p = 2$, the above argument can be modified and one finds that $[M_\infty(S)\overline{K}_\infty : L_{S_0}M_\infty]$ is finite (although not necessarily 1). We still obtain the same conclusion about $U_\psi(S_0)$.

Now it is not difficult to describe the action of the Galois group $\mathrm{Gal}\,(\overline{K}_\infty/\boldsymbol{Q}) = \Delta \times \Gamma$ on $B \otimes_Z \Omega_p$ and hence, by Kummer theory, the structure of $U_\psi(S_0)$. For each $\ell \in S_0$, we let B_ℓ denote the subgroup of B consisting of ℓ-units. The above Galois group acts on the primes of $\overline{K}_\infty$ dividing ℓ transitively. The kernel of this action is the decomposition group $D(\ell)$ of any prime dividing ℓ and is generated by the inertia group (which is contained in Δ since $\ell \neq p$) and by a (Frobenius) automorphism $\sigma(\ell)$ which we write in the form $\sigma(\ell) = \delta(\ell)\gamma(\ell)$, where $\delta(\ell) \in \Delta$ and $\gamma(\ell) \in \Gamma$. Note that $\gamma(\ell) = \gamma_0^{a_\ell}$, where a_ℓ has been defined earlier in this section. The representation of $\mathrm{Gal}\,(\overline{K}_\infty/\boldsymbol{Q})$ on $B_\ell \otimes_Z \Omega_p$ is obtained (in an obvious way) from that part of the regular representation of $\mathrm{Gal}\,(\overline{K}_\infty/\boldsymbol{Q})/D(\ell)$ on which J acts as multiplication by -1. If $J \in D(\ell)$, then of course B_ℓ consists only of the roots of unity in $\overline{K}_\infty$ and so $B_\ell \otimes_Z \Omega_p$ is trivial.

Now let χ be the character of Δ determined by $\chi\psi = \omega$. We must find the eigenvalues of γ_0 on the χ-components of $B_\ell \otimes_Z \Omega_p$. This χ-component will be trivial if ℓ divides the conductor of χ, or equivalently ψ. Taking into account our description of the kernel of the action of $\mathrm{Gal}\,(\overline{K}_\infty/\boldsymbol{Q})$ on B_ℓ, it is clear that $\gamma(\ell)$ must act on the χ-component as multiplication by $\chi(\delta(\ell))^{-1} = \chi(\ell)^{-1}$ (identifying χ with the corresponding primitive Dirichlet character). Thus the corresponding eigenvalues of γ_0

satisfy the equation $x^{p^{e_\ell}} = \chi(\ell)^{-(u_\ell^{-1})}$. Note that unless $\chi(\ell)$ is a p-power root of unity, the χ-component is trivial. In this case, each of the roots of the above equation is actually an eigenvalue of γ_0 and with multiplicity one. Thus, by Kummer theory, the prime ℓ contributes the following eigenvalues of γ_0 acting on $U_\psi(S_0)$: the roots of the equation $(\kappa_0/x)^{p^{e_\ell}} = \chi(\ell)^{-(u_\ell^{-1})}$, or $x^{p^{e_\ell}} = (\kappa_0^{a_\ell}\chi(\ell))^{u_\ell^{-1}} = (\langle\ell\rangle\omega\psi^{-1}(\ell))^{u_\ell^{-1}}$. Comparing this with our previous description of the roots of $g_{\psi S}^*(T)$ coming from the Euler factor for ℓ, we find that we have proved the following result.

PROPOSITION 6. *The polynomials $h_{\psi S}(T)/h_\psi(T)$ and $g_{\psi S}^*(T)/g_\psi^*(T)$ are equal.*

4. The torsion subgroup of Gal (M_∞/K_∞)

In previous sections, we have discussed the structure of certain representation spaces for Γ constructed from $Y = \mathrm{Gal}\,(M_\infty/K_\infty)$. For odd primes p, it seems quite likely that the μ-invariant of the Γ-module Y is zero. (By Proposition 1, the Γ-modules X^- and Y have the same μ-invariant.) The following proposition (which is due to Iwasawa, although our proof is new) would then show that the torsion subgroup of Y is trivial and hence that not much is lost by considering $Y \otimes_{Z_p} \Omega_p$ instead of Y itself.

PROPOSITION 7. *If p is odd, Y contains no non-trivial finite Γ-submodule.*

Proof. By Proposition 1, it is enough to show that $\overline{A}_\infty^-$ contains no Γ-invariant subgroup of finite index >1. We will actually prove this for $\overline{A}_\infty$. (For odd p, $\overline{A}_\infty^-$ is a direct summand of $\overline{A}_\infty$.) Let C be such a subgroup. There exists an integer n_0 such that $\gamma_0^{p^n}$ acts trivially on $\overline{A}_\infty/C$ for all $n \geq n_0$. If $a \in \overline{A}_\infty$, but $a \notin C$, then for a large enough value of n, there will exist an ideal class $\bar{a} \in \overline{A}_n$ such that $\bar{a} \to a$ under the mapping $\overline{A}_n \to \overline{A}_\infty$. Since the primes dividing p are totally ramified in $\overline{K}_m/\overline{K}_n$ for $m \geq n$, one can show that the norm map $N_{m,n}$ from $\overline{K}_m$ to $\overline{K}_n$ induces a surjective map from $\overline{A}_m$ to $\overline{A}_n$. We may choose $n \geq n_0$ and it then follows that $a \bmod C$ is a p^{m-n}-th power in $\overline{A}_\infty/C$. This is of course impossible if m is large enough and we conclude that $C = \overline{A}_\infty$. This proves the above proposition.

If $p = 2$, Proposition 7 remains valid, but we plan to discuss this in a more general context in a subsequent paper. In addition, it is

definitely true, as we pointed out previously, that the μ-invariant of Y is non-zero. More precisely, we have the following proposition.

PROPOSITION 8. *If $p = 2$, the torsion subgroup of Y is pseudo-isomorphic to $\Lambda/(2)\,[\Delta]$, where $\Delta = \mathrm{Gal}\,(K/\boldsymbol{Q})$. Thus, the μ-invariant of Y is $[K:\boldsymbol{Q}]$.*

Remark. In the above proposition, Λ denotes the power series ring $\boldsymbol{Z}_p[[T]]$, where $T = \gamma_0 - 1$. Thus $\Lambda/(2)$ is the group ring for Γ over $\boldsymbol{Z}/(2)$ as defined in the theory of profinite groups. Thus $\Lambda/(2)\,[\Delta]$ is actually the group ring for $\mathrm{Gal}\,(K_\infty/\boldsymbol{Q}) = \Delta \times \Gamma$ over $\boldsymbol{Z}/(2)$.

Proof. It is known that the μ-invariant of X^- is zero for $p = 2$ (see [4]). Thus by Proposition 2, the torsion subgroup of Y is pseudo-isomorphic to the dual of E_∞/E_∞^2 as a $\Lambda[\Delta]$-module.

Now let $n \geq 0$ and let φ_i, $i = 1, \cdots, [K_n:\boldsymbol{Q}]$, be the distinct embeddings of K_n into $\boldsymbol{R}$. Let E_n denote the unit group of K_n. We claim that the mapping

$$E_n \to \prod_{i=1}^{[K_n:\boldsymbol{Q}]} \boldsymbol{R}^x/(\boldsymbol{R}^x)^2$$

induced from the φ_i's has the index of its image bounded as $n \to \infty$. This will follow if we show that the *strict* ideal class group of K_n has a bounded number of elements of order 2. If this were not so, K_n would have an extension of type $(\boldsymbol{Z}/(2))^{d_n}$ where only infinite primes are ramified and where $d_n \to \infty$ as $n \to \infty$. However, translating such extensions to $\overline{K}_n$ would give unramified extensions of the above type, which would contradict the fact that $\overline{A}_\infty$ has μ-invariant zero (see [4]).

It follows that there is a homomorphism from E_n/E_n^2 to $\boldsymbol{Z}/(2)[\mathrm{Gal}\,(K_n/\boldsymbol{Q})]$ with bounded kernel and cokernel. In addition, one can show that the mappings from E_n/E_n^2 to $(E_\infty/E_\infty^2)^{\Gamma_n}$, where $\Gamma_n = \mathrm{Gal}\,(K_\infty/K_n)$ have bounded kernel and cokernel. Combining these facts, one deduces the above proposition.

We will end this section by speculating about the relation between p-adic L-functions and the structure of the torsion subgroup of Y. Let ψ be an even Dirichlet character of the first kind and let π be a uniformizing parameter for $\boldsymbol{Q}_p(\psi)$. Let m_ψ denote the largest integer such that π^{m_ψ} divides all of the coefficients of the power series $G_\psi^*(T)$ (or equivalently $G_\psi(T)$). Note that for odd p, m_ψ is exactly as defined in

Section 4 of [6] and is probably equal to zero (see Theorem 2 of [6]). On the other hand, for $p = 2$, m_ψ is different than in [6]. It is positive and is such that $\pi^{m_\psi}/2$ is a unit in $\boldsymbol{Q}_p(\psi)$. It is not hard to make a reasonable guess about the relationship between the integers m_ψ and the structure of the torsion subgroup of Y_{K_ψ}, where K_ψ is the cyclic extension of $\boldsymbol{Q}$ corresponding to ψ by class field theory. If ψ has order prime to p, then Conjecture 2.3 of [3] would include a description of this relationship. In general, write $\psi = \psi_1\psi_2$, where ψ_1 has order prime to p and ψ_2 has p-power order. It is easy to show that if ψ' is any conjugate of ψ over $\boldsymbol{Q}_p$, then $m_\psi = m_{\psi'}$. Let Ψ be the sum of all the $\boldsymbol{Q}_p$-conjugates of ψ, Ψ_1 and Ψ_2 the sums of the $\boldsymbol{Q}_p$-conjugates of ψ_1 and ψ_2. Then $\Psi = \Psi_1\Psi_2$. Let e_{Ψ_1} be the idempotent corresponding to Ψ_1 in the group ring $\boldsymbol{Z}_p[\mathrm{Gal}\,(K_\psi/K_{\psi_2})]$. Let $Y_{\Psi_1} = e_{\Psi_1}Y_{K_\psi}$. If ψ has order prime to p, then the invariant $\mu = \mu(Y_{\Psi_1})$ should be related to m_ψ by the equation

$$p^\mu = N_{\boldsymbol{Q}_p(\psi)/\boldsymbol{Q}_p}(\pi)^{m_\psi}\cdot u\ ,$$

where u is a unit in $\boldsymbol{Z}_p$.

However, if the order of ψ is divisible by p and if σ denotes an element of order p in $\mathrm{Gal}\,(K_\psi/\boldsymbol{Q})$, then the above equation should hold for $\mu = \mu((\sigma - 1)Y_{\Psi_1})$. From Proposition 8, one can see that these statements are valid for $p = 2$. If the conjecture that $\mu(Y) = 0$ for odd p is valid, then the above statements are again (trivially) valid.

5. A conjecture of G. Gras

In this section, we will assume that K is a totally real abelian extension of $\boldsymbol{Q}$ and that p is an odd prime not dividing $[K:\boldsymbol{Q}]$. Let E_K be the group of units of K, and let C_K be the subgroup of cyclotomic units of K. Let A_K be the p-primary subgroup of the ideal class group of K. Let B_K denote the p-primary subgroup of E_K/C_K. In this section, we will discuss the following conjecture of G. Gras (see [5]).

CONJECTURE. A_K and B_K have isomorphic Jordan-Holder series as $\boldsymbol{Z}_p[\mathrm{Gal}\,(K/\boldsymbol{Q})]$-modules.

Our assumptions on p allow us to take a simplified definition of C_K. For a more precise definition, see Hasse [8] or Leopoldt [12]. Our definition is as follows: Let $F/\boldsymbol{Q}$ be cyclic with conductor f so that $F \subseteq \boldsymbol{Q}(\zeta_f)$, where ζ_f is any primitive f-th root of unity. Then α_F

$= N_{\boldsymbol{Q}(\zeta_p)/F}(\zeta_p - 1)$ is an element of F (although not necessarily a unit). Let H_K be the subgroup of $K^\times$ generated by α_F and its conjugates for *all* cyclic subfields F of K. We then define

$$C_K = H_K \cap E_K .$$

We remark that it is known that A_K and B_K have the same order (since p is odd and does not divide $[K:\boldsymbol{Q}]$.) In this section, we will show that the conjecture stated in the introduction (together with the conjecture stated at the end of Section 4) actually implies Gras' conjecture. We begin by outlining our approach.

Let $\Delta = \mathrm{Gal}(K/\boldsymbol{Q})$. The simple modules over $R = \boldsymbol{Z}_p[\Delta]$ are easily described. They must have exponent p and so correspond precisely to the irreducible representations of Δ over $\boldsymbol{Z}/(p)$. Let Ψ be any irreducible character of Δ over $\boldsymbol{Q}_p$ and let e_Ψ be the corresponding idempotent (which is contained in R since $p \nmid |\Delta|$). It is not hard to see that $\overline{\Psi} = \Psi \bmod p$ is an irreducible character for Δ over $\boldsymbol{Z}/(p)$ and that all irreducible characters are obtained in this way. The corresponding simple R-module is $e_\Psi R/p(e_\Psi R)$. If D is any finite R-module, then $e_\Psi D$ will have order $(p^{\Psi(1)})^r$ where the exponent r will be the number of times the simple module attached to Ψ occurs in a Jordan-Holder series for D. Thus, to prove Gras' conjecture, we must show that

$$|e_\Psi A_K| = |e_\Psi B_K|$$

for all Ψ. If $\Psi = \Psi_0$ (the trivial character of Δ), then one can easily show that both sides are equal to 1. We will therefore assume from now on that $\Psi \neq \Psi_0$.

Now consider $U_K = \prod_\mathfrak{p} U_\mathfrak{p}$, where $\mathfrak{p}$ runs over all primes of K dividing p. Here we are letting $U_\mathfrak{p}$ denote the group of units in the $\mathfrak{p}$-adic completion of K. Both E_K and C_K can be embedded in U_K in a natural way and we denote their closures in U_K by $\overline{E}_K$ and $\overline{C}_K$. Then, if $\Psi \neq \Psi_0$, it is known that $e_\Psi(U'_K/\overline{C}'_K)$ is finite. (This is Brumer's theorem [1]. Here U'_K and $\overline{C}'_K$ denote the subgroups of U_K and $\overline{C}_K$ whose components are principal units. Thus U'_K and $\overline{C}'_K$ are $\boldsymbol{Z}_p$-modules and hence R-modules so that $e_\Psi(U'_K/\overline{C}'_K)$ makes sense.) Let M_0 be the maximal abelian p-ramified pro-p-extension of K and let L be the maximal abelian unramified p-extension of K, so that $K \subseteq L \subseteq M_0$. Then by class field theory one sees that

$$\mathrm{Gal}\,(L/K) \cong A_K$$

and

$$\mathrm{Gal}\,(M_0/L) \cong (U'_K/\bar{E}'_K)$$

canonically. On the other hand,

$$(\bar{E}'_K/\bar{C}'_K) \cong B_K\ .$$

Thus, in order to prove Gras' conjecture, one must show that $e_{\mathfrak{P}}(U'_K/\bar{C}'_K)$ and $e_{\mathfrak{P}}\,\mathrm{Gal}\,(M_0/K)$ have the same order for $\mathfrak{P} \neq \mathfrak{P}_0$ (the latter group is finite because M_0/K_∞ is a finite extension, by Brumer's theorem again). By assuming the conjectural relationship between p-adic L-functions and the structure of Y_K, we can calculate the order of $e_{\mathfrak{P}}\,\mathrm{Gal}\,(M_0/K)$ in terms of the values of p-adic L-functions at $s = 1$. On the other hand, by a rather interesting calculation, we can also express the order of $e_{\mathfrak{P}}(U'_K/\bar{C}'_K)$ in terms of the values of p-adic L-functions at $s = 1$. The equality of the orders of these groups will then be obvious (conjecturally).

To compute the order of $e_{\mathfrak{P}}\,\mathrm{Gal}\,(M_0/K)$, we observe that M_0 is the maximal abelian extension of K contained in M_∞ and so $\mathrm{Gal}\,(M_0/K_\infty) \cong Y_K/TY_K$, where $T = \gamma_0 - 1$. Thus, if we let $Y_{\mathfrak{P}} = e_{\mathfrak{P}}Y_K$, then, for $\mathfrak{P} \neq \mathfrak{P}_0$, we must find the order of $Y_{\mathfrak{P}}/TY_{\mathfrak{P}}$. To do this, we consider an arbitrary noetherian and torsion Λ-module $\mathscr{Y}$. It is known that $\mathscr{Y}$ is pseudo-isomorphic to a direct sum $\mathscr{Y}' = \sum_{i=1}^{t} \mathscr{Y}_i$, where each $\mathscr{Y}_i$ is a Λ-module of the form $\mathscr{Y}_i = \Lambda/(f_i(T))$ with $f_i(T)$ either a power of p or a monic polynomial whose non-leading terms are divisible by p (a so-called distinguished polynomial). If $f_i(T) = p^{e_i}$, then it is not hard to see that $|\mathscr{Y}_i/T\mathscr{Y}_i| = p^{e_i}$. If $f_i(T)$ is a polynomial of degree ℓ_i (and of the above type), then $\mathscr{Y}_i$ is a free $\boldsymbol{Z}_p$-module of rank ℓ_i and $f_i(T)$ is the characteristic polynomial of T acting on $\mathscr{Y}_i$. It follows that $|\mathscr{Y}_i/T\mathscr{Y}_i|$ is just the power of p dividing the determinant $f_i(0)$ of T acting on $\mathscr{Y}_i$. Now the μ-invariant of the Λ-module $\mathscr{Y}$ is defined as $\mu(\mathscr{Y}) = \sum e_i$, where the sum is over those i's for which $f_i(T)$ is a power of p. The product $f(T) = \prod f_i(T)$ of the remaining polynomials can be described as the characteristic polynomial of T acting on the vector space $\mathscr{Y} \otimes_{\boldsymbol{Z}_p} \Omega_p$. Now if we make the additional assumption that $\mathscr{Y}$ contains no non-trivial finite Λ-submodule (so that $\mathscr{Y}$ is isomorphic to a submodule of $\mathscr{Y}'$ of finite index), then it is not hard to prove that $\mathscr{Y}/T\mathscr{Y}$ and $\mathscr{Y}'/T\mathscr{Y}'$ have the same order (see Section 6 of [3]). Thus $|\mathscr{Y}/T\mathscr{Y}|$ is equal to the power

of p dividing $p^\mu f(0)$, where $\mu = \mu(\mathscr{Y})$. These observations apply to the Λ-module $\mathscr{Y} = Y_\Psi$ by Proposition 7. In this case, $\mathscr{Y} \otimes_{Z_p} \Omega_p$ is isomorphic to $\sum_\psi W_\psi$ and so $f(T) = \prod_\psi h_\psi(T)$, where ψ varies over the one dimensional constituents of Ψ. Now conjecturally $h_\psi(T) = g_\psi^*(T)$ and $p^\mu / \prod_\psi \pi^{m_\psi}$ is a unit of $\mathscr{O}_\psi$. Since $L_p(1, \psi)$ is equal to $\pi^{m_\psi} g_\psi^*(0)$ up to a unit of $\mathscr{O}_\psi$, it follows that conjecturally the order of $e_\Psi \operatorname{Gal}(M_0/K)$ is equal to the power of p dividing

$$\prod_\psi L_p(1, \psi) ,$$

where ψ varies over the constituents of Ψ. We should mention that, although we have assumed that $\Psi \neq \Psi_0$, our last statement is valid also for $\Psi = \Psi_0$ since both quantities are infinite.

We now consider the group $e_\Psi(U'_K/\bar{C}'_K) \cong e_\Psi U'_K / e_\Psi \bar{C}'_K$. It will be useful to compare the structure of U'_K as an R-module with $D_K = \mathscr{O}_K \otimes_Z Z_p$, where $\mathscr{O}_K$ denotes the ring of integers of the number field K. Of course, D_K is just the direct sum of the completions of $\mathscr{O}_K$ at the primes dividing p and U_K is the group of units in D_K. Let $D_K(1)$ be the direct sum of the maximal ideals in these completions so that $D_K(1)$ is an ideal of D_K and let $D_K(n) = D_K(1)^n$ for $n \geq 1$. We also let $U_K(n) = 1 + D_K(n)$. Then $U'_K = U_K(1)$. By a simple (and familiar) argument, one can show that $U_K(n)/U_K(n+1)$ is isomorphic to $D_K(n)/D_K(n+1)$ as an R-module for all $n \geq 1$. For $n \geq 2$, much more is true. The p-adic logarithm allows one to define an R-homomorphism

$$\log_p : U'_K \to D_K$$

(the image is in fact contained in $D_K(1)$ since the ramification index of each prime dividing p is $\leq p - 1$) and this induces an R-isomorphism

$$\log_p : U_K(n) \xrightarrow{\sim} D_K(n)$$

for all $n \geq 2$. For $n = 1$, this may have a non-trivial kernel. However, $\bar{C}'_K$ is torsion-free and so is mapped injectively by $\log_p$. In addition, if $\Psi \neq \Psi_0$, then $e_\Psi \bar{C}'_K$ contains $e_\Psi U_K(n)$ for sufficiently large n. One can see that

$$e_\Psi \bar{C}'_K / e_\Psi U_K(n) \cong e_\Psi \log_p(\bar{C}'_K) / e_\Psi D_K(n) .$$

But since $e_\Psi U'_K / e_\Psi U_K(n)$ and $e_\Psi D_K(1) / e_\Psi D_K(n)$ have the same order, it is obvious that

$$|e_\Psi U'_K / e_\Psi \bar{C}'_K| = |e_\Psi D_K(1) / e_\Psi \log_p(\bar{C}'_K)| .$$

Thus, we must now calculate the index of $e_\Psi \log_p(\bar{C}'_K)$ in $e_\Psi D_K(1)$.

Let F be the cyclic extension of $\boldsymbol{Q}$ corresponding to Ψ (or any of its constituents). The element α_F defined earlier is not necessarily a unit of F but one can form a unit α_F^e/a, where $(e,p)=1$ and a is some rational integer. Let $\alpha'_F = (\alpha_F^e/a)^d$, where d is chosen so that $(d,p)=1$ and $\alpha'_F \equiv 1 \pmod{\mathfrak{p}}$ for all primes $\mathfrak{p}$ of K dividing p. Then, considering α'_F as an element of U'_K, it is not hard to show that $(\alpha'_F)^{e_\Psi}$ generates $e_\Psi \bar{C}'_K$ as an R-module (we are mixing additive and multiplicative notation). Thus $e_\Psi \log(\bar{C}'_K)$ is generated as an R-module by $e_\Psi \log_p(\alpha'_F)$. We can also find a generator for $e_\Psi D_K(1)$. Let f be the conductor of F and let $\tau_F = \mathrm{Tr}_{\boldsymbol{Q}(\zeta_f)/F}(\zeta_f)$, where ζ_f is a primitive f-th root of 1. Then, using the fact that p is at most tamely ramified in the field $\boldsymbol{Q}(\zeta_f)$, one can show that $e_\Psi \tau_F$ generates $e_\Psi D_K$ as an R-module. (Here we are identifying τ_F with $\tau_F \otimes 1$ in $D_K = \mathcal{O}_K \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p$.) Now we must distinguish two cases. If $p \nmid f$, then $e_\Psi D_K(1)$ will be generated by $e_\Psi p \tau_F$. If $p \mid f$, then one can easily show that Ψ does not "occur" in $D_K/D_K(1)$ because the action of the inertia group for p in Δ must be trivial. It follows that $e_\Psi \tau_F$ in fact generates $e_\Psi D_K(1)$.

To simplify the rest of this calculation, we make the following observation. Let ψ be a one dimensional character of Δ contained in Ψ and let $\mathcal{O}_\psi$ denote the ring of integers in the field $\boldsymbol{Q}_p(\psi)$ generated by values of ψ. Let A be any finite R-module. We form $A \otimes_{\boldsymbol{Z}_p} \mathcal{O}_\psi$, which can be considered as a module over $\mathcal{O}_\psi[\Delta]$. Let e_ψ be the idempotent corresponding to ψ. Then it is not hard to see that $e_\Psi A$ has the same order as $e_\psi(A \otimes_{\boldsymbol{Z}_p} \mathcal{O}_\psi)$.

We can apply this observation to the module $e_\Psi D_K(1)/e_\Psi \log_p(\bar{C}'_K)$. Calculating within the $\mathcal{O}_\psi$-algebra $\tilde{D}_K = D_K \otimes_{\boldsymbol{Z}_p} \mathcal{O}_\psi$ instead of D_K, we must compute the index of the $\mathcal{O}_\psi$-module generated by $e_\psi \log_p(\alpha'_F)$ in the $\mathcal{O}_\psi$-module generated by $e_\psi p \tau_F$ of $p \nmid f$ or by $e_\psi \tau_F$ if $p \mid f$. The character ψ corresponds to a primitive Dirichlet character of conductor f (which we also denote by ψ) and it is clear that

$$e_\psi \tau_F = \frac{1}{d} \sum_{n=1}^{f} \psi^{-1}(n) \zeta_f^n = \frac{1}{d} \tau(\psi^{-1}) ,$$

where $d = |\Delta|$ and $\tau(\psi^{-1})$ is of course a Gaussian sum. Similarly, $e_\psi \log_p(\alpha'_F)$ is equal (up to a p-adic unit) to $\sum_{n=1}^{f} \psi^{-1}(n) \log_p(\zeta_f^n - 1)$.

(Here we are using the "extended" p-adic logarithm defined in [9], Chapter 4.) The ratio of this sum to $p\tau(\psi^{-1})$ if $p \nmid f$ or to $\tau(\psi^{-1})$ if $p \mid f$ is an element of $\mathcal{O}_\psi$ whose norm from $\mathcal{O}_\psi$ to $\boldsymbol{Z}_p$ is the index that we wish to compute. Now we recall that the value of the p-adic L-function $L_p(s, \psi)$ at $s = 1$ is given by (see [9], Chapter 5):

$$L_p(1, \psi) = -\left(1 - \frac{\psi(p)}{p}\right)\frac{\tau(\psi)}{f}\sum_{n=1}^{f} \psi^{-1}(n) \log_p(\zeta_f^n - 1) .$$

By taking into account the fact that $\tau(\psi)\tau(\psi^{-1}) = \pm f$ and that $\psi(p) = 0$ if and only if $p \mid f$, we see that up to a unit in $\mathcal{O}_\psi$ the factor in front of the sum is either $1/p\tau(\psi^{-1})$ if $p \nmid f$ or $1/\tau(\psi^{-1})$ if $p \mid f$. Thus, it should now be clear that the order of $e_{\mathfrak{w}} U'_K / e_{\mathfrak{w}} \overline{C}'_K$ is the power of p dividing

$$N_{\boldsymbol{Q}_p(\psi)/\boldsymbol{Q}_p}(L_p(1, \psi)) = \prod_{\psi'} L_p(1, \psi') ,$$

where ψ' varies over all $\boldsymbol{Q}_p$-conjugates of ψ. Comparing this with the (conjectural) order of $e_{\mathfrak{w}} \operatorname{Gal}(M_0/K)$, we obtain the following result.

PROPOSITION 9. *Assume that the conjectures stated in the introduction and at the end of Section* 4 *are valid for all characters* ψ *attached to* K. *Then Gras' conjecture is also valid for* K.

REFERENCES

[1] A. Brumer, On the units of algebraic number fields, Mathematika, **14** (1967), 121–124.

[2] J. Coates, p-adic L-functions and Iwasawa theory, to appear in Proceedings of symposium on algebraic number theory held in Durham, England, 1975.

[3] J. Coates, S. Lichtenbaum, On ℓ-adic zeta functions, Ann. of Math., **98** (1973), 498–550.

[4] B. Ferrero, Iwasawa invariants of abelian number fields, to appear.

[5] G. Gras, Classes d'ideaux des corps abeliens et nombres de Bernoulli generalises, Ann. Inst. Fourier, **27** (1977), 1–66.

[6] R. Greenberg, On p-adic L-functions and cyclotomic fields, Nagoya Math. Jour., **56** (1975), 61–77.

[7] ——, On the Iwasawa invariants of totally real number fields, Amer. Jour. of Math., **98** (1976), 263–284.

[8] H. Hasse, Uber die Klassenzahl abelscher Zahlkorper, Akademie Verlag, Berlin, 1952.

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

[10] ——, On Z_ℓ-extensions of algebraic number fields, Ann. of Math., **98** (1973), 246–326.

[11] T. Kubota, H. Leopoldt, Eine p-adische Theorie der Zetawerte (Teil I), J. Reine Angew. Math., **213** (1964), 328–339.

[12] H. Leopoldt, Uber Einheitengruppe und Klassenzahl reeller abelscher Zahlkorper, Abh. Deutsche Akad. Wiss. Berlin Math. 2. (1954).

Brandeis University