ILLINOIS JOURNAL OF MATHEMATICS
Volume 25, Number 2, Summer 1981

STICKELBERGER RELATIONS AND TAME EXTENSIONS OF PRIME DEGREE

BY

L. N. CHILDS[1]

Introduction

Let K be an algebraic number field with ring of integers $O = O_K$. Let L be a Galois extension of K with group G, and with ring of integers O_L. The extension L/K has a normal integral basis if there exists an element α of O_L so that $\{\sigma(\alpha) \mid \sigma \text{ in } G\}$ is a basis of O_L as an O_K-module, or equivalently, O_L is free of rank one as a module over the group ring $O_K G$. The extension L/K is tame if for each prime ideal p of O_K, the ramification index e_p of p in L is relatively prime to p. A theorem of E. Noether asserts that tameness of L/K is a necessary and sufficient condition for O_L to be a locally free (hence projective) $O_K G$-module of rank one. Thus tameness of L/K is a necessary condition for the existence of a normal integral basis for L/K.

Let G be abelian, and let Cl $(O_K G)$ be the group of isomorphism classes of rank one projective $O_K G$-modules. Let $R(O_K G)$ be the set of classes of Cl $(O_K G)$ which are represented by rings of integers of tame Galois extensions of K with Galois group G. Then $R(O_K G)$ measures the extent to which tameness fails to suffice for the existence of normal integral bases.

In case G is cyclic of order l, prime, and K contains a primitive lth root of unity ζ, L. McCulloh [7] showed that $R(O_K G)$ is generated by the set of classes which are images under action by elements in the Stickelberger ideal J of $Z[\Delta]$, $\Delta = \text{Aut } G$ (as defined in Section 2 below). The purpose of this paper is to show that one inclusion of McCulloh's equality holds without assuming existence of ζ, namely, that classes in the image of the Stickelberger ideal are represented by rings of integers of tame extensions.

A consequence of our result is to show anew that the classical Kummer-Stickelberger relations on the ideal class group of $\mathbf{Z}[\zeta]$, ζ a primitive lth root of unity, l prime, are a consequence of the Hilbert-Speiser theorem (tame abelian extensions of Q have normal integral bases). Our derivation is different from both the proof via Gauss sums [5, Section 105–109] and the proof of [1], and shows that McCulloh's result is not just an analogue but a generalization of the Stickelberger result for extensions of prime degree (cf. [7, (1.3.2)]).

Our method of proof is essentially a Galois descent argument.

Received May 23, 1979.

[1] Partially supported by the National Science Foundation.

For the remainder of the paper, l is a prime number, ζ is a fixed primitive lth root of unity, $\lambda = 1 - \zeta$. G is cyclic of order l with fixed generator σ, $\hat{G}$ is the group of complex characters of G; χ_0, χ_1 in $\hat{G}$ send σ to $1, \zeta$, respectively. Let $\Delta = \text{Aut}(G)$. If δ in Δ acts by $\delta(\sigma) = \sigma^a$, $0 < a < l$, we write $a = t(\delta)$. Any non-trivial element χ of $\hat{G}$ may be written as $\chi = \chi_1 \delta$ for some δ in Δ.

Let $\Omega = \text{Gal}(Q[\zeta]/Q)$. If γ in Ω acts by $\gamma(\zeta) = \zeta^a, 0 < a < l$, write $a = t(\gamma)$. We let γ in Ω act on χ in $\hat{G}$ by $\gamma(\chi) = \gamma \cdot \chi$.

We refer to [7] for unexplained notation and proofs of numerous facts used here. I wish to thank L. McCulloh for several stimulating discussions, S. Ullom for informing me of reference [6], and the University of Illinois at Urbana for its hospitality during the research on this paper.

1. Cl (OG)

Let K be a number field, $K_\zeta = K[\zeta]$, O be the ring of integers of K, O_ζ the ring of integers of K_ζ, $\Gamma = \text{Gal}(K_\zeta/K)$. We wish to describe Cl (OG) and Cl $(O_\zeta G)$. We use the description of Jacobinsky and Frohlich [2] which describes the class group in terms of ideals of a maximal order. Namely, Cl $(O_\zeta G)$ is identified as the cokernel of the map

$$U(O_{\zeta,l}G) \xrightarrow{i} \text{Map}(\hat{G}, I_\zeta)$$

where $O_{\zeta,l}$ is the semi-local ring obtained by localizing O_ζ with respect to the multiplicative set $\mathbf{Z} - l\mathbf{Z}$, I_ζ is the collection of fractional ideals of K_ζ prime to (l), Map $(\hat{G}, I_\zeta)$ is the set of functions from $\hat{G}$ to I_ζ, $U(\ )$ is the units functor, and $i(\beta)(\chi) = (\chi(\beta))$, the principal ideal generated by $\chi(\beta)$, for β in $U(O_{\zeta,l}G)$.

We denote by ϕ_ζ the canonical map from Map $(\hat{G}, I_\zeta)$ onto the cokernel, which we identify with Cl $(O_\zeta G)$.

The description of Cl $(O_\zeta G)$ is based on the fact that the maximal order of $O_\zeta G$ is $\otimes_{\chi \in \hat{G}} O_\zeta e_\chi$, where

$$e_\chi = \frac{1}{l} \sum_{i=0}^{l-1} \chi(\sigma^{-i})\sigma^i,$$

hence Map $(\hat{G}, I_\zeta)$ is the group of fractional ideals of the maximal order of $K_\zeta G$ which are prime to (l).

In a similar way we may identify Cl (OG) as the cokernel of the map

$$U(O_l G) \xrightarrow{i} \text{Map}_\Gamma(\hat{G}, I_\zeta),$$

where $\mathbf{n} \in \text{Map}_\Gamma(\hat{G}, I_\zeta)$ if $\mathbf{n} \in \text{Map}(\hat{G}, I_\zeta)$ and $\mathbf{n}(\gamma\chi) = \gamma(\mathbf{n}(\chi))$ for all γ in Γ. This description may be obtained by either identifying the group of fractional ideals prime to l of the maximal order $\overline{OG}$ of KG with its image in Map $(\hat{G}, I_\zeta)$ under the map induced from the inclusion from $\overline{OG}$ to $\overline{O_\zeta G}$; or it may be obtained from [3, p. 428].

We let ϕ be the canonical map from $\mathrm{Map}_\Gamma(\hat{G}, I_\zeta)$ onto $\mathrm{Cl}\,(OG)$. Putting the two sequences together gives the commutative diagram with exact rows,

$$(*)\qquad \begin{array}{ccccccc} U(O_l G) & \longrightarrow & \mathrm{Map}_\Gamma\,(\hat{G}, I_\zeta) & \xrightarrow{\ \phi\ } & \mathrm{Cl}\,(OG) & \longrightarrow & 1 \\ \cap & & \cap & & \downarrow & & \\ U(O_{\zeta,l} G) & \longrightarrow & \mathrm{Map}\,(\hat{G}, I_\zeta) & \xrightarrow{\ \phi_\zeta\ } & \mathrm{Cl}\,(O_\zeta G) & \longrightarrow & 1, \end{array}$$

where the rightmost vertical map is induced from the inclusion map $OG \subset O_\zeta G$.

It is a fact [7, (2.4.1)] that if $\mathbf{m}$ is in $\mathrm{Map}\,(\hat{G}, I_\zeta)$ and has the property that $\mathbf{m}(\chi) = (a_\chi)$ where $a_\chi \equiv 1(\mathrm{mod}\ (\lambda^{l-1}))$, then $\phi_\zeta(\mathbf{m}) = (1)$. We will generalize this useful fact below.

Let δ in $\Delta = \mathrm{Aut}\ G$ act on $\mathbf{n}$ in $\mathrm{Map}\,(G, I_\zeta)$ by $\delta(\mathbf{n})(\chi) = \mathbf{n}(\chi \cdot \delta)$. With this action the bottom line of (*) is a Δ-sequence [7, (2.3.1)]; it is straightforward to verify that the top sequence of (*) is also a Δ-sequence.

The above description of $\mathrm{Cl}\,(OG)$ is in terms of ideals. The rings of integers we study are naturally presented as modules. Here is the translation into ideal classes.

Let P be a rank one projective OG-module. Since $O_l G$ is semi-local, $P_l = O_l Gv$ for some v in P_l, hence $P_{\zeta,l} = O_{\zeta,l} Gv$, where $P_\zeta = O_\zeta \otimes_O P$. Then for each χ in $\hat{G}$, $e_\chi P_\zeta \subseteq e_\chi K_\zeta Gv = K_\zeta e_\chi v$; so $e_\chi P_\zeta = \mathbf{n}(\chi) e_\zeta v$ for some fractional ideal $\mathbf{n}(\chi)$. Since $P_l = O_l Gv$, $\mathbf{n}(\chi)$ is prime to l, so is in I_ζ. To show $\mathbf{n}$ is a Γ-map we note that Γ acts on $P_\zeta = O_\zeta \otimes P$ by acting on the left factor; hence $\gamma(e_x P_\zeta) = \gamma(e_\chi) P_\zeta = e_{\gamma(\chi)} P_\zeta$. Then $\gamma(e_\chi P_\zeta) = \gamma \mathbf{n}(\chi) \gamma e_\chi v = \gamma \mathbf{n}(\chi) e_{\gamma(\chi)} v$, whereas $e_{\zeta(\chi)} P_\zeta = \mathbf{n}(\gamma\chi) e_{\gamma(\chi)} v$, and so $\mathbf{n}(\gamma\chi) = \gamma \mathbf{n}(\chi)$ for all γ in Γ. Hence $\mathbf{n}$ is in $\mathrm{Map}_\Gamma\,(\hat{G}, I_\zeta)$.

The class $\mathrm{cl}\,(P)$ of P is then $\phi(\mathbf{n})$ in $CL\,(OG)$.

2. The theorem

As above, G is cyclic of prime order l, K is a number field with ring of integers O. Define $\mathrm{Cl}^0\,(OG) = \ker \mathrm{Cl}\,(\chi_0)$, χ_0 the trivial character on G. Define $R(OG)$ to be those classes in $\mathrm{Cl}\,(OG)$ which are represented by rings of integers of tame extensions of K with Galois group G. By [7, (1.2.1)], $R(OG) \subseteq \mathrm{Cl}^0\,(OG)$.

We wish to identify $R(OG)$ inside $\mathrm{Cl}^0\,(OG)$. Recall that $\Delta = \mathrm{Aut}\,(G)$, and σ is a fixed generator of G. For $\delta \in \Delta$, let $\delta(\sigma) = \sigma^{t(\delta)}$ with $0 < t(\delta) < l$. Let $\theta = \sum_{\delta \in \Delta} t(\delta)\delta^{-1}$. Let $J = [(l^{-1}\theta)\mathbf{Z}\Delta] \cap \mathbf{Z}\Delta$, the Stickelberger ideal.

Let A be the $\mathbf{Z}$-submodule of $\mathbf{Z}\Delta$ with basis consisting of l and the elements $\delta - t(\delta)$ for $\delta \neq 1$ in Δ. Then [7, (4.1.3)] $(l^{-1}\theta)A = J$.

Now Δ, hence $\mathbf{Z}\Delta$, acts on $\mathrm{Cl}^0\,(OG)$ by functoriality. Let $\mathrm{Cl}^0\,(OG)^J$ be the subgroup of $\mathrm{Cl}^0\,(OG)$ generated by c^α, α in J. Our result is:

THEOREM. *Let G be cyclic of prime order l, and K be a number field with ring of integers O. Then* $\mathrm{Cl}^0\,(OG)^J \subseteq R(OG)$.

McCulloh's Theorem [7] is:

If in addition K contains a primitive lth root of unity ζ, then $\mathrm{Cl}^0\,(OG)^J = R(OG)$.

Now let J' be the image of J in $\mathbf{Z}\Omega$, $\Omega = \mathrm{Gal}\,(\mathbf{Z}[\zeta]/\mathbf{Z})$, under the isomorphism $\mathbf{Z}\Delta \cong \mathbf{Z}\Omega$ given by $\delta \leftrightarrow \gamma$ if $t(\delta) = t(\gamma)$.

COROLLARY. $\mathrm{Cl}\,(\mathbf{Z}[\zeta])^{J'} = (1)$.

This gives the classical Kummer-Stickelberger relations on $\mathrm{Cl}\,(\mathbf{Z}[\zeta])$ [5, Satz 136].

Proof of Corollary. We specialize to $K = Q$, $O = \mathbf{Z}$. Then $R(\mathbf{Z}G) = (1)$, by the Hilbert-Speiser theorem [5, Satz 132]. Hence $\mathrm{Cl}^0\,(\mathbf{Z}G)^J = (1)$. But $\mathrm{Cl}^0\,(\mathbf{Z}G) = \mathrm{Cl}\,(\mathbf{Z}G)$; and $\mathrm{Cl}\,(\mathbf{Z}G) \cong \mathrm{Cl}\,(\mathbf{Z}[\zeta])$ under the map induced by sending $\sigma \to \zeta$, by Rim's theorem [8]. Since this isomorphism is evidently compatible with the isomorphism of $\mathbf{Z}\Delta$ with $\mathbf{Z}\Omega$, the corollary is immediate.

The rest of the paper is devoted to the proof of the theorem.

3. Proof of the theorem

Denote by $\mathrm{Map}^0_\Gamma\,(\hat{G}, I_\zeta)$ the set of maps $\mathbf{m}$ in $\mathrm{Map}_\Gamma\,(\hat{G}, I_\zeta)$ such that $\mathbf{m}(\chi_0) = (1)$, and $\mathrm{Map}^0_\Gamma\,(\hat{G}, I_\zeta)^J$ the subgroup generated by $\mathbf{m}^\alpha$, α in J. (Recall α is in $\mathbf{Z}[\Delta]$, and δ in Δ acts on $\mathbf{m}$ by $\delta(\mathbf{m})(\chi) = \mathbf{m}(\chi \circ \delta)$.)

Let M be a class in $\mathrm{Cl}^0\,(OG)^J$, represented by $\mathbf{m}'$ in $\mathrm{Map}^0_\Gamma\,(\hat{G}, I_\zeta)^J$. By [7, Lemma (4.1.5)], there exists $\mathbf{a}'$ in $\mathrm{Map}^0_\Gamma\,(\hat{G}, I_\zeta)$ such that for all α in A,

(1) $$\mathbf{a}'^{\theta\alpha/l} = \mathbf{m}'^{\alpha}.$$

We follow the proof of [7, (4.2.1)], to construct a tame extension L of K_ζ, but we do it in such a way that L will descend to a tame extension N of K with $\mathrm{cl}\,(O_N) = M$. Let $R(\lambda^l)$ be the group of principal fractional ideals (a) with $a \equiv 1$ (mod λ^l), a in $O_{l,\zeta}$.

Observe that $\Gamma = \mathrm{Gal}\,(K_\zeta/K)$ maps 1-1 by restriction into $\Omega = \mathrm{Gal}\,(Q(\zeta)/Q)$. For each coset representative δ of Ω mod Γ, let $\mathbf{a}(\delta\chi_1)$ be a prime of K_ζ in the same class in $I_\zeta/R(\lambda^l)$ as $\mathbf{a}'(\delta\chi_1)$, such that $\mathbf{a}(\delta\chi_1)$ splits completely from K. (Recall that χ_1 in $\hat{G}$ satisfies $\chi_1(\sigma) = \zeta$.) Choose the $\mathbf{a}(\delta\chi_1)$ also so that for different δ, the $\mathbf{a}(\delta\chi_1)$ contract to distinct primes of K. Such a choice is possible since the Dirichlet density of primes of K_ζ which split completely from Q is 1, hence in each class of $I_\zeta/R(\lambda^l)$ there are infinitely many such primes (see [6, p. V-3] or [4, p. 215].

For $\gamma \in \Gamma$, let $\mathbf{a}(\gamma\delta\chi_1) = \gamma\mathbf{a}(\delta\chi_1)$, and set $\mathbf{a}(\chi_0) = (1)$. Then for $\chi \neq \chi_0$ in $\hat{G}$, the $\mathbf{a}(\chi)$ form a collection of distinct primes. Moreover $\mathbf{a}$ is in $\mathrm{Map}^0_\Gamma\,(G, I_\zeta)$, and $\mathbf{a} = \mathbf{a}'(\mathbf{u})$ where $(\mathbf{u})$ is in $\mathrm{Map}^0_\Gamma\,(\hat{G}, R(\lambda^l))$. From (1) we get $(\mathbf{u})^\theta\mathbf{m}'^l = \mathbf{a}^\theta$.

For any γ in Γ and χ in $\hat{G}$, $(\mathbf{u}(\gamma\chi)) = (\gamma\mathbf{u}(\chi))$, so we may alter $\mathbf{u}(\chi)$ by a global unit if necessary so that $\mathbf{u}(\gamma\chi) = \gamma\mathbf{u}(\chi)$ (see proof of the lemma below).

Let $\mathbf{u}^\theta(\chi_1) = u_\theta$, and set $L = K_\zeta[Z]/(Z^l - u_\theta) = K_\zeta[z]$, where $z^l = u_\theta$. Because (u_θ) is in $R(\lambda^l)$, it follows from [7. (3.1.1)] that L/K_ζ is tame; moreover, since the $\mathbf{a}(\chi)$ are distinct primes, the proof of [7, (4.2.1)] goes through to show that cl $(O_L) = \phi_\zeta(\mathbf{m}')$ where

$$\phi_\zeta\colon \mathrm{Map}^0\ (\hat{G}, I_\zeta) \to \mathrm{Cl}^0\ (O_\zeta G)$$

is as in Section 1 above.

The rest of the argument proceeds as follows.

(i) $\Gamma = \mathrm{Gal}\ (K_\zeta/K)$ extends to a group $\bar{\Gamma}$ of automorphisms of L in such a way that $\bar{\Gamma}$ and $G = \mathrm{Gal}\ (L/K_\zeta)$ commute, hence the fixed filed $L^{\bar{\Gamma}} = N$ is a Galois extension of K with group G.

(ii) N/K is tame.

(iii) cl $(O_N) = \phi(\mathbf{m}')$.

These arguments will complete the proof.

Proof of (i). To define an action of $\Gamma = \mathrm{Gal}\ (K_\zeta/K)$ on L, it suffices to define the action on z. So we look at $\gamma(u_\theta)$ for γ in Γ. Since $\mathbf{u}$ is a Γ-map, for any γ in Γ,

$$\gamma(u_\theta) = \prod_\beta \gamma(\mathbf{u}(\chi_1\beta^{-1})^{t(\beta)}) = \prod_\beta \mathbf{u}(\gamma\chi_1\beta^{-1})^{t(\beta)}$$

where β runs through $\Delta = \mathrm{Aut}\ (G)$.

There is an isomorphism of Γ into Δ which takes γ in Γ, acting on ζ by $\gamma(\zeta) = \zeta^{t(\gamma)}$, to γ_1 in Δ, where $\gamma_1(\sigma) = \sigma^{t(\gamma)}$. Hence

$$\begin{aligned}\gamma(u_\theta) &= \prod_\beta \mathbf{u}(\chi_1\gamma_1\beta^{-1})^{t(\beta)} \\ &= \prod_{\eta\in\Delta} \mathbf{u}(\chi_1\eta^{-1})^{t(\eta\gamma_1)} \\ &= \prod_{\eta\in\Delta} \mathbf{u}(\chi_1\eta^{-1})^{t(\eta)t(\gamma_1)} \cdot u(\chi_1\eta^{-1})^{r(\eta,\gamma_1)l}\end{aligned}$$

where $r(\eta, \gamma_1)l = t(\eta\gamma_1) - t(\eta)t(\gamma_1)$. Hence

$$\gamma(u_\theta) = (u_\theta)^{t(\gamma)} \cdot \left[\prod_{\eta\in\Delta} \mathbf{u}(\chi_1\eta^{-1})^{r(\eta,\gamma_1)}\right]^l = (u_\theta)^{t(\gamma)}s_\gamma^l.$$

where s_γ is the quantity inside the brackets. Since $\mathbf{u}(\chi) \equiv 1 \pmod{\lambda^l}$ for all $\chi \in \hat{G}$, $s_\gamma \equiv 1 \pmod{\lambda^l}$.

Now in L, $z^l = u_\theta$. So for each γ in Γ, we define an extension $\bar{\gamma}$ of γ to L by $\bar{\gamma}(z) = z^{t(\gamma)}s_\gamma$. Then $\bar{\gamma}$ is a well-defined extension of γ to L.

Let $\bar{\Gamma}$ be the set of extensions $\bar{\gamma}$.

The maps $\sigma^i\bar{\gamma}$, σ in G, $\bar{\gamma}$ in $\bar{\Gamma}$, form a set of $[G: 1]\,[\Gamma: 1] = [L: K]$ distinct K-automorphisms of L, for if $\sigma^i\bar{\gamma} = \sigma^j\bar{\gamma}'$, then their respective values on z are equal, namely,

$$\zeta^{it(\gamma)}z^{t(\gamma)}s_\gamma = \zeta^{jt(\gamma')}z^{t(\gamma')}s'_\gamma,$$

hence $t(\gamma) = t(\gamma')$, $\gamma = \gamma'$, hence $i = j$. So L is a Galois extension of K with Galois group $H = \{\sigma^i\bar{\gamma} \mid i = 0, \ldots, l-1; \bar{\gamma} \text{ in } \Gamma\}$.

It is quickly checked that $\bar{\gamma}$ and σ^i commute on L. So H is abelian.

Now Γ is cyclic, being a subgroup of Gal $(Q[\zeta]/Q)$. Let γ generate Γ. Then $\bar{\gamma}$ either has order $[\Gamma{:}1]$ in H, or, since G has index l in H, generates all of H. In the latter case, $\bar{\gamma}^l$ restricts to $\gamma^l = \gamma$ (since $[\Gamma: 1]$ divides $[Q[\zeta]: Q] = l - 1$) and $\bar{\gamma}^l$ has order $[\Gamma: 1]$ in H. So, replacing $\bar{\gamma}$ by $\bar{\gamma}^l$ if necessary, we can assume that $\bar{\gamma}$ generates a subgroup $\bar{\Gamma}$ of H, $\bar{\Gamma}$ restricts isomorphically to Γ on K_ζ, and $H = \bar{\Gamma} \times G$.

For future reference we note that since $\bar{\gamma}(z) = z^{t(\gamma)}s_\gamma$ with $s_\gamma \equiv 1 \pmod{\lambda^l}$, then $\bar{\gamma}^i(z) = z^{t(\gamma^i)}s'_i$ with $s'_i \equiv 1 \pmod{\lambda^l}$. This is easily seen by induction. So we may assume, with or without the replacement of $\bar{\gamma}$ by $\bar{\gamma}^l$, that

$$\bar{\gamma}(z) = z^{t(\gamma)}c_\gamma \tag{2}$$

for some c_γ in $O_{\zeta,l}$ with $c_\gamma \equiv 1 \pmod{\lambda^l}$.

We let N be the fixed field of $\bar{\Gamma}$. Then N is a Galois extension of K with group G, and $N_\zeta = L$. This completes part (i) of the proof.

Proof of (ii). We know $L = N \cdot K_\zeta \cong N \otimes_K K_\zeta$. Since $[N : K] = l$, the ramification index of any prime P of K divides l, so will always be prime to the characteristic of O_K/P if P does not lie over (l). Suppose, then, that P is a prime ideal of O_K lying over (l). Then the ramification index $e_P(N/K)$ divides $e_P(K_\zeta/K) \cdot e_{P'}(L/K_\zeta)$ where P' is any prime of K_ζ lying over P. But L/K_ζ is tame, so $e_P(L/K_\zeta) = 1$; also $e_P(K_\zeta/K)$ divides $[K_\zeta : K] < l - 1$. Since $e_P(N/K)$ divides l, $e_P(N/K) = 1$. Hence no P lying over (l) ramifies in N, and N/K is tame.

Proof of (iii) (the class of O_N in Cl (OG) is M). Following the last paragraph of Section 1, we find the class of O_N in Cl (OG) by first finding a suitable normal basis element of $O_{N,l}$. Our candidate is

$$v_0 = \frac{1}{l}\left(1 + \sum_{\delta}\sum_{\gamma\in\Gamma}\bar{\gamma}(z^{t(\delta)})\right) \quad \text{in } L$$

where δ runs through a set of coset representatives of Γ in $\Omega = $ Gal $(Q[\zeta]/Q)$.

Evidently v_0 is fixed by Γ, so is in N. To show that v_0 generates a normal basis, we need to show that v_0 is in $O_{N,l}$ and that the discriminant of $\{\sigma(v_0)\}_{\sigma \text{ in } G}$ is a unit of $O_{N,l}$.

To show that v_0 is in $O_{N,l}$, we recall from (2) that $\gamma(z) = z^{t(\gamma)}c_\gamma$ with $c_\gamma \equiv 1$ (mod λ^l), and $z^l = u_\theta \equiv 1$ (mod λ^l). Thus in the expression for v_0, we may write

$$\bar{\gamma}(z^{t(\delta)}) = (z^{t(\gamma)}c_\gamma)^{t(\delta)} = z^{t(\gamma)t(\delta)}c_\gamma^{t(\delta)} = z^{t(\gamma\delta)}z^{lr(\gamma,\delta)}c_\gamma^{t(\delta)}.$$

We set $d_{t(\gamma\delta)} = u_\theta^{r(\gamma,\delta)}c_\gamma^{t(\delta)}$; then $d_{t(\gamma\delta)}$ is in $O_{\zeta,l}$,

$$d_{t(\gamma\delta)} \equiv 1 \ (\text{mod } \lambda^l) \quad \text{and} \quad \gamma(z)^{t(\delta)} = z^{t(\delta)}d_{t(\gamma\delta)}.$$

Since $\gamma\delta$ runs through all elements of Ω, $t(\gamma\delta)$ runs through all i, $1 \le i \le l-1$, so

$$v_0 = \frac{1}{l}\sum_{i=0}^{l-1} z^i d_i = \frac{1}{l}\sum_{i=0}^{l-1} z^i + \sum_{i=0}^{l-1} \frac{(d_i - 1)}{l} z^i.$$

The first term is in $O_{L,l}$ by [7, (3.3.3)], and the second has coefficients of z^i which are in $O_{\zeta,l}$ since $d_i \equiv 1$ (mod λ^l) and $(l) = (\lambda^{l-1})$. Hence v_0 is in $N \cap O_{L,l} = O_{N,l}$.

To compute the discriminant of $\{\sigma_j(v_0)\}_{j=0,\ldots,l-1}$ we note that

$$\sigma^j(v_0) = \frac{1}{l}\sum_{i=0}^{l-1} \zeta^{ij}z^i d_i \quad \text{for each } j,\ 0 \le j \le l-1.$$

So

$$\begin{pmatrix} v_0 \\ \sigma(v_0) \\ \\ \sigma^{l-1}(v_0) \end{pmatrix} = \frac{1}{l}\begin{pmatrix} d_0 & d_1 & d_2 \\ d_0 & \zeta d_1 & \zeta^2 d_2 \\ d_0 & \zeta^2 d_1 & \zeta^4 d_2 \\ \vdots & & \end{pmatrix} \cdots \begin{pmatrix} z^1 \\ z^2 \\ \vdots \end{pmatrix}$$

hence

$$\Delta\{\sigma^j(v_0)\} = \frac{(d_0 d_1 d_2 \cdots)^2}{l^{2l}} \det (\zeta^{ij})^2 \Delta\{z^i\}.$$

Now $\Delta\{z^i\} = \pm(u_\theta)^{l-1}l^l$, and $\det(\zeta^{ij})^2 = l^l$, so we get

$$\Delta\{\sigma^j(v_0)\} = \pm(d_0 d_1 d_2 \cdots)^2(u_\theta)^{l-1},$$

a unit of $O_{\zeta,l}$. Thus $\{\sigma^i(v_0)\}$ is a normal basis of $O_{N,l}/O_l$.

Following the prescription of the last paragraph of Section 1, we let $\mathbf{n}$ in Map (G, I_ζ) be such that for each χ in $\hat{G}$, $e_\chi O_L = \mathbf{n}(\chi)e_\chi v_0$. Then we find that $\mathbf{n}(\gamma\chi) = \gamma\mathbf{n}(\chi)$ for γ in Γ, just as in the last paragraph of Section 1. Hence $\mathbf{n}$ is in Map_Γ $(\hat{G}, I_\zeta)$. The class of O_N in Cl (OG) is then $\phi(\mathbf{n})$.

We need to show that cl $(O_N) = \phi(\mathbf{m}')$. For this we use

LEMMA (cf. [7, (2.4.1)]). *If* $\mathbf{m}, \mathbf{n}$ *are in* Map_Γ $(\hat{G}, I_\zeta)$, *and for each* δ *in* Δ *there exists* (u_δ) *in* $R(\lambda^l)$ *so that* $\mathbf{m}(\chi_1\delta) = (u_\delta)\mathbf{n}(\chi_1\delta)$, *then* $\phi(\mathbf{m}) = \phi(\mathbf{n})$ *in* Cl (OG).

Proof of lemma. Since $\mathbf{m}$ and $\mathbf{n}$ are Γ-maps, it follows that for all γ in Γ, the ideals $(\gamma(u_\delta))$ and $(u_{\gamma\delta})$ are equal. Hence $\gamma(u_\delta)$ and $u_{\gamma\delta}$ differ by a unit factor in O_ζ which is $\equiv 1 \pmod{\lambda^l}$. Fix a set T of coset representatives of Ω mod Γ and replace $u_{\gamma\delta}$ by $\gamma(u_\delta)$ for $\gamma \neq 1$, δ in T. Then $\gamma(u_\delta) = u_{\gamma\delta}$ for all δ in Ω, γ in Γ.

Let

$$\beta = e_{\chi 0} + \sum_{\delta \text{ in } \Omega} u_\delta e_{\chi_1 \delta} \quad \text{where} \quad e_\chi = \frac{1}{l} \sum_\tau \chi(\tau)\tau^{-1} \text{ in } K_\zeta G.$$

We show β is in $U(O_l G)$.

Since $u_\delta \equiv 1 \pmod{\lambda^l}$, there exist s_δ in $O_{\zeta,l}$ so that $u_\delta = 1 + l\lambda s_\delta$. Hence

$$\beta = e_{\chi 0} + \sum_\delta (1 + l\lambda s_\delta) e_{\chi_1 \delta} = 1 + \sum s_\delta \lambda (l e_{\chi_1 \delta})$$

which is in $O_{\zeta,l}G$. Similarly for $\beta^{-1} = e_{\chi 0} + \sum u_\delta^{-1} e_{\chi_1 \delta}$. So β is in $U(O_{\zeta,l}G)$. Since $u_{\gamma\delta} = \gamma(u_\delta)$ for γ in Γ, both β and β^{-1} are in $O_l G$. So β is in $U(O_l G)$.

Now the image of β in $\mathrm{Map}_\Gamma\ (\hat{G}, I_\zeta)$ is $(\mathbf{u})$, $\mathbf{u}(\chi_0) = 1$, $\mathbf{u}(\chi_1\delta) = u_\delta$. So $\phi(\mathbf{u}) = (1)$ in $\mathrm{Cl}\,(OG)$, and $\phi(\mathbf{m}) = \phi(\mathbf{u})\phi(\mathbf{n}) = \phi(\mathbf{n})$. That proves the lemma.

We write $\mathbf{m} \sim \mathbf{n}$ if $\mathbf{m}$, $\mathbf{n}$ are in $\mathrm{Map}\,(\hat{G}, I_\zeta)$ and $\mathbf{m}(\chi_1\delta) = (u_\delta)\mathbf{n}(\chi_1\delta)$ with u_δ in $R(\lambda^l)$.

Returning to the proof that $\mathrm{cl}\ (O_N) = \phi(\mathbf{m}')$, we need to show that $\phi(\mathbf{n}) = \phi(\mathbf{m}')$.

Let $v = (1/l) \sum z^i$. Then $e_\chi O_L = \mathbf{m}(\chi) e_\chi v$ and $\mathbf{m} \sim \mathbf{m}'$, by [7, proof of (4.2.1)]. We have $\mathbf{n}(\chi) e_\chi v_0 = e_\chi O_L = \mathbf{m}(\chi) e_\chi v$. Now

$$e_{\chi_1\delta} v = \frac{1}{l} z^{t(\delta)} \quad \text{and} \quad e_{\chi_1\delta} v_0 = \frac{1}{l} z^{t(\delta)} d_{t(\delta)}$$

by the argument of [7, p. 573, line 9]. Thus $\mathbf{n}(\chi_1\delta)(d_{t(\delta)}) = \mathbf{m}(\chi_1\delta)$ for all δ in $\Delta = \mathrm{Aut}\ (G)$. But $d_{t(\delta)} \equiv 1 \pmod{\lambda^l}$, as we observed in showing v_0 was in $O_{N,l}$. So $\mathbf{n} \sim \mathbf{m}$. Thus $\mathbf{n} \sim \mathbf{m}'$.

Now both $\mathbf{n}$ and $\mathbf{m}'$ are in $\mathrm{Map}_\Gamma\ (\hat{G}, I_\zeta)$, and we have $\phi(\mathbf{m}') = M$, the class in $\mathrm{Cl}^0\ (OG)^J$ we began with, and $\phi(\mathbf{n})$ is the class of O_N. Thus, by the lemma, $M = \mathrm{cl}\ (O_N)$ in $\mathrm{Cl}^0\ (OG)$. Since N is a tame extension of K, the proof is complete.

Note. Leon McCulloh informs me that he has subsequently obtained results (forthcoming) which substantially generalize the theorem of this paper.

REFERENCES

1. A. FRÖHLICH, "Stickelberger without Gauss sums" in *Algebraic number fields*, Proc. Durham Symposium, Academic Press, New York, 1977, 589–608.
2. ———, *Locally free modules over arithmetic orders*, J. für Math., vol. 274/275 (1975), pp. 112–124.

3. ———, *Arithmetic and Galois module structure for tame extensions*, J. für Math., vol. 286/287 (1976), pp. 380–440.
4. H. HEILBRONN, "Zeta-functions and *L*-functions" in J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, New York, 1967, pp. 204–230.
5. D. HILBERT, "Die Theorie der algebraischen Zahlkörper" in *Ges. Abh.*, vol. I, Chelsea, New York, 1965, pp. 63–363.
6. K. IWASAWA, "Class fields" in *Seminar on complex multiplication*, Chapter V, Springer Lecture Notes in Math., vol. 21, Springer, New York, 1966.
7. L. MCCULLOH, "A Stickelberger condition on Galois module structure for Kummer extensions of prime degree" in *Algebraic number fields*, Proc. Durham Symp., Academic Press, 1977, pp. 561–588.
8. D. S. RIM, *Modules over finite groups*, Ann. of Math., vol. 69 (1959), pp. 700–712.

STATE UNIVERSITY OF NEW YORK AT ALBANY
ALBANY, NEW YORK