JOURNAL OF NUMBER THEORY 51, 118–129 (1995)

Trace Forms and Stickelberger Relations

JORGE MORALES*

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918

Communicated by Alan C. Woods

Received March 9, 1992; revised February 2, 1993

DEDICATED TO PROFESSOR PIERRE E. CONNER ON THE OCCASION OF HIS 60TH BIRTHDAY

Let N/K be a tamely ramified abelian extension of odd degree and let $G = \mathrm{Gal}(N/K)$. This paper studies the equivariant isometry class of the trace form $t_{N/K}$ restricted to the square root of the inverse different $A_{N/K}$. The failure of $A_{N/K}$ to admit an orthonormal normal basis is measured by an invariant $\rho_{N/K}$ in the unitary class group $\mathrm{UCl}(O_K G)$. This paper shows that for Kummer extensions of odd prime degree, there are Stickelberger-like conditions that determine when a class in $\mathrm{UCl}(O_K G)$ can be realized as the ρ-invariant of some tame G-extension.

1. INTRODUCTION

Let K be a number field and let N/K be an abelian extension of *odd* degree with Galois group G. It follows from Hilbert's formula [16, Chap. IV, Proposition 4] that the different $\mathfrak{D}_{N/K}$ has even order at all finite places of N. Thus $\mathfrak{D}_{N/K}$ admits a square root and we denote by $A_{N/K}$ the ideal $\mathfrak{D}_{N/K}^{-1/2}$. It is easy to verify that $A_{N/K}$ is preserved by G and is self-dual with respect to the trace form $t_{N/K}(x, y) = \mathrm{Tr}_{N/K}(xy)$ (this property actually characterizes $A_{N/K}$ uniquely among the fractional ideals of N). In this paper we shall be concerned with the study of the pair $(A_{N/K}, t_{N/K})$ as a G-equivariant symmetric bilinear form over O_K.

Let t_G be the standard symmetric bilinear form on the group algebra KG, that is, the form for which the group elements form an orthonormal basis over K. Clearly this form is G-invariant. A pair (L, b) consisting of an $O_K G$-lattice L and a G-invariant symmetric bilinear form $b\colon L \times L \to O_K$ is said to belong to the *principal genus* if (L, b) and $(O_K G, t_G)$ are everywhere

* Research supported in part by the NSF under Grant DMS-9205129.

0022-314X/95 $6.00

locally isometric as G-forms. We show that there is a natural one-to-one correspondence between the G-isometry classes of forms in the principal genus and the elements of the unitary class group $\mathrm{UCl}(O_K G)$ (see next section).

A sufficient condition for $(A_{N/K}, t_{N/K})$ to be in the principal genus is that N/K be tamely ramified. Hence, when N/K is tame, the form $(A_{N/K}, t_{N/K})$ defines a class $\rho_{N/K}$ in the unitary class group $\mathrm{UCl}(O_K G)$. We define the subset of *realizable classes* of $\mathrm{UCl}(O_K G)$ by

$$\mathrm{RU}(O_K G) = \{\rho_{N/K} : N/K \text{ tame } G\text{-extension}\}.$$

The main result of this paper is that for Kummer extensions of prime odd order the subset $\mathrm{RU}(O_K G)$ is actually a subgroup and is characterized by a hermitian version of the Stickelberger relations. More precisely, let Δ be the automorphism group of G and let $S \subset \mathbb{Z}\Delta$ be the hermitian Stickelberger ideal (see Section 3 for the definition). Let $\mathrm{Cl}(O_K G)$ be the locally free class group of $O_K G$. Our main result is that there is a natural homomorphism

$$S \underset{\mathbb{Z}\Delta}{\otimes} \mathrm{Cl}(O_K G) \to \mathrm{UCl}(O_K G),$$

whose image is exactly $\mathrm{RU}(O_K G)$. In particular, $\mathrm{RU}(O_K G)$ is a subgroup, which is not obvious *a priori*.

Note the analogy of the above result with McCulloh's characterization of the subset $R(O_K G) = \{\mathrm{cl}(O_N) : N/K \text{ tame } G\text{-extension}\}$ of the locally free class group $\mathrm{Cl}(O_K G)$. In [12] McCulloh showed the inequality $R(O_K G) = \mathrm{Cl}^0(O_K G)^J$, where $J \subset \mathbb{Z}\Delta$ is the classical Stickelberger ideal and $\mathrm{Cl}^0(O_K G)$ is the kernel of the homomorphism $\mathrm{Cl}(O_K G) \to \mathrm{Cl}(O_K)$ induced by the augmentation map. Our computations in Section 3 are largely inspired by McCulloh's methods.

2. The Unitary Class Group

Let $\mathscr{L}$ denote the set of $O_K G$-lattices L of KG such that (L, t_G) is in the principal genus, i.e., such that (L, t_G) is everywhere locally G-isometric to the unit form $(O_K G, t_G)$.

The following theorem characterizes $\mathscr{L}$.

(2.1) Theorem. *Let $L \subset KG$ be an $O_K G$-lattice. Then L is in $\mathscr{L}$ if and only if $LL^* = O_K G$.*

Proof. Suppose that L is in $\mathscr{L}$. Then for all primes $\mathfrak{p}$ the localization $L_\mathfrak{p}$ admits a generator $u_\mathfrak{p}$ with $u_\mathfrak{p} u_\mathfrak{p}^* = 1$. Thus $L_\mathfrak{p} L_\mathfrak{p}^* = u_\mathfrak{p} u_\mathfrak{p}^* O_{K_\mathfrak{p}} G = O_{K_\mathfrak{p}} G$ for all primes $\mathfrak{p}$.

Conversely, suppose that $LL^* = O_K G$. Then L is invertible as a fractional $O_K G$-ideal, therefore projective over $O_K G$, and hence locally free. Write $L_{\mathfrak{p}} = u_{\mathfrak{p}} O_{K_{\mathfrak{p}}} G$ for all primes $\mathfrak{p}$. The following computation shows that L is self-dual with respect to t_G:

$$\begin{aligned} t_G(x, L_{\mathfrak{p}}) \subseteq O_{K_{\mathfrak{p}}} &\Leftrightarrow t_G(x, u_{\mathfrak{p}} g) \subseteq O_{K_{\mathfrak{p}}} \qquad \text{for all} \quad g \in G \\ &\Leftrightarrow t_G(u_{\mathfrak{p}}^* x, g) \subseteq O_{K_{\mathfrak{p}}} \qquad \text{for all} \quad g \in G \\ &\Leftrightarrow u_{\mathfrak{p}}^* x \in O_{K_{\mathfrak{p}}} G \\ &\Leftrightarrow u_{\mathfrak{p}} u_{\mathfrak{p}}^* x \in u_{\mathfrak{p}} O_{K_{\mathfrak{p}}} G = L_{\mathfrak{p}} \\ &\Leftrightarrow x \in L_{\mathfrak{p}} \end{aligned}$$

(note that $u_{\mathfrak{p}} u_{\mathfrak{p}}^*$ is a unit of $O_{K_{\mathfrak{p}}} G$). Thus L is self-dual. By [8, Corollary 2.4], we may conclude that L belongs to $\mathscr{L}$. ∎

(2.2) COROLLARY. *$\mathscr{L}$ is a group with respect to multiplication.*

Proof. Follows immediately from the condition $LL^* = O_K G$. ∎

Let $KG^{(1)}$ be the subgroup of $KG^\times$ of units satisfying $uu^* = 1$. Note that $KG^{(1)}$ is the automorphism group of the G-form (KG, t_G). The group $KG^{(1)}$ acts on $\mathscr{L}$ by multiplication and its orbits are precisely the isometry classes in the principal genus.

(2.3) DEFINITION. The *unitary class group* $\mathrm{UCl}(O_K, G)$ is defined by the exact sequence

$$KG^{(1)} \xrightarrow{i} \mathscr{L} \to \mathrm{UCl}(O_K G) \to 0,$$

where $i(u) = uO_K G$.

It follows from the considerations above that $\mathrm{UCl}(O_K G)$ classifies the G-isometry classes of lattices in $\mathscr{L}$. It is known from general results (see, for instance, [14, Theorem 1.1]) that $\mathrm{UCl}(O_K G)$ is a finite group. The canonical projection $\mathscr{L} \to \mathrm{UCl}(O_K G)$ will be denoted by ucl.

Remark. Using an equivariant version of the weak Hasse principle we can see that actually every G-form (M, b) in the principal genus can be embedded isometrically and equivariantly into (KG, t_G) and hence is G-isometric to some form (L, t_G) with L in $\mathscr{L}$. Therefore $\mathrm{UCl}(O_K G)$ classifies in fact *all* the forms in the principal genus.

Now let N/K be a tame G-extension. Choose an equivariant isometry $f\colon (N, t_{N/K}) \to (KG, t_G)$ (this is possible by Bayer and Lenstra [1]). Then $f(A_{N/K})$ is self-dual with respect to t_G and, by tameness, is locally free over

$O_K G$. These conditions ensure that $f(A_{N/K})$ is in $\mathscr{S}$ (see [8, Corollary 2.4]). Thus we can define

$$\rho_{N/K} = \mathrm{ucl}(f(A_{N/K})).$$

Since f is unique up to multiplication by an element of $KG^{(1)}$, the definition of $\rho_{N/K}$ is independent of the choice of f.

The *realizable subset* $\mathrm{RU}(O_K G)$ of $\mathrm{UCl}(O_K G)$ is by definition

$$\mathrm{RU}(O_K G) = \{\rho_{N/K} : N/K \text{ is a tame } G\text{-extension}\}.$$

It follows from the results in [6; 8, Theorem 4.1] that for $K = \mathbb{Q}$, the realizable subset $\mathrm{RU}(\mathbb{Z}G)$ is reduced to the identity. It follows from examples contained in [2] that this need not be the case for general K. In the next section we shall investigate the nature of $\mathrm{RU}(O_K G)$ for G of odd prime order l and K containing the lth roots of unity.

Remark. In [8], we associated to every tame G-extension N/K a canonical lattice $M_{N/K}$ in $O_K[G]$ such that $(M_{N/K}, t_G)$ is locally everywhere G-isometric to $(O_N, t_{N/K})$. From [8, Theorem 3.3], the invariant $\rho_{N/K}$ also measures the failure of $(O_N, t_{N/K})$ to be globally equivariantly isometric to $(M_{N/K}, t_G)$.

3. Kummer Extensions of Prime Degree

Throughout this section we let l denote an odd prime number and G the cyclic group of order l. We shall also assume that the ground field K contains the lth roots of unity. Our first goal is to calculate for a G-extension N/K the invariant $\rho_{N/K}$ in $\mathrm{UCl}(O_K G)$. Letting $N = K(\sqrt[l]{a})$ for a suitable $a \in K$, we shall express $\rho_{N/K}$ in terms of the $\mathfrak{p}$-valuations of a.

The following notation will be in the force henceforth.

$O_\mathfrak{p}$	the $\mathfrak{p}$-adic completion of O_K.
$O_{(l)}$	the semi-localization of O_K at l, i.e., the ring $\{x \in K \mid \mathrm{ord}_\mathfrak{p}(x) \geqslant 0 \text{ for all } \mathfrak{p} \mid l\}$.
$\mathfrak{J}$	the group of ideals of K relatively prime to l.
$\mathfrak{l}$	the ideal generated in O_K by $(\xi - 1)$, where ξ is a primitive lth root of unity.
$\hat{G}$	the character group of G.
$\mathbb{Z}\hat{G}^+$	the subgroup of the group ring $\mathbb{Z}\hat{G}$ of elements fixed by the canonincal involution $\chi \mapsto \chi^*$.
e_χ	the idempotent in KG corresponding to the character $\chi \in \hat{G}$.
Δ	the automorphism group of G.

δ_r the automorphism of G given by $\delta_r(g) = g^r$ $(r \not\equiv 0 \pmod{l})$.

$t(r)$ the unique integer with $t(r) \equiv r \pmod{l}$ and $|t(r)| \leqslant (l-1)/2$.

$\bar{K}$ the algebraic closure of K.

In order to determine $\rho_{N/K}$ we will use a particular presentation of the unitary class group. Let $\mathfrak{g}\colon \mathbb{Z}\hat{G}/\mathbb{Z}\hat{G}^+ \to \mathfrak{J}$ be a homomorphism. We attach to $\mathfrak{g}$ a lattice $L(\mathfrak{g})$ in KG by prescribing its local components:

$$L(\mathfrak{g})_{\mathfrak{p}} = \begin{cases} O_{\mathfrak{p}}G & \text{if } \mathfrak{p} \mid l, \\ \sum_\chi \mathfrak{g}(\chi)\, O_{\mathfrak{p}} e_\chi & \text{if } \mathfrak{p} \nmid l \end{cases}.$$

Note that $L(\mathfrak{g})\, L(\mathfrak{g})^* = O_K G$, since $\mathfrak{g}(\chi)\, \mathfrak{g}(\chi^*) = 1$. Hence $L(\mathfrak{g})$ represents a class $L_*(\mathfrak{g})$ in $\mathrm{UCl}(O_K G)$.

(3.1) THEOREM. *The above construction yields a presentation*

$$O_{(l)}G^{(1)} \xrightarrow{\ \iota\ } \mathrm{Hom}(\mathbb{Z}\hat{G}/\mathbb{Z}\hat{G}^+, \mathfrak{J}) \xrightarrow{\ L_*\ } \mathrm{UCl}(O_K G) \to 0, \tag{1}$$

where $O_{(l)}G^{(1)}$ is the subgroup of elements u in $O_{(l)}G^\times$ satisfying $uu^* = 1$.

Proof. Let $u \in O_{(l)}G^{(1)}$ and write $u = \sum_\chi u_\chi e_\chi$. The map ι is defined by $\iota(u)(\chi) = u_\chi O_K$. It is obvious from the definition of L that $\mathrm{Im}(\iota) = \mathrm{Ker}(L_*)$. Thus we shall only check the surjectivity of L_*. The image of L_* in $\mathrm{UCl}(O_K G)$ consists precisely in the ideal classes that admit a representative J such that $O_{(l)}J = O_{(l)}G$. Starting out with an ideal I in KG with $II^* = O_K G$, we shall show that there exists $u \in KG$ with $uu^* = 1$ and such that $J = uI$ fulfills the condition $O_{(l)}J = O_{(l)}G$.

Since the ring $O_{(l)}G$ is semi-local the ideal $IO_{(l)}$ is principal. Let $a \in KG$ be a generator for $IO_{(l)}$ and let $b = aa^*$. Since $II^*O_{(l)} = bO_{(l)}G = O_{(l)}G$, the element b must be a unit in the ring $O_{(l)}G$. We shall show that there exists a unit c in $O_{(l)}G$ such that $b = cc^*$. Let $\varepsilon\colon KG \to K$ be the augmentation map. Since $\varepsilon(b) = \varepsilon(a)^2$ is a unit in $O_{(l)}$, replacing a by $a\varepsilon(a)^{-1}$ we may assume that $\varepsilon(a) = 1$.

Since l is odd, it is enough to show that b^l can be written in the form $b^l = cc^*$ for some unit c of $O_{(l)}G$. Using the well-known congruence $z^l \equiv \varepsilon(z)^l \pmod{l}$ for $z \in O_K G$, we have $b^l \equiv 1 \pmod{l}$. Let $e_0 \in KG$ be the idempotent corresponding to the trivial character of G and choose an idempotent $e \in KG$ such that $e_0 + e + e^* = 1$ and $ee^* = 0$ (recall that K contains the lth roots of unity and therefore KG is split over K). Let $c = e_0 + b^l e + e^*$. Clearly $cc^* = b^l$. Write $b^l = 1 + lw$, with w in $O_{(l)}G$. With this notation we have $c = 1 + lew$, which shows that c is in $O_{(l)}G$, as required.

Write $l = 2k+1$ and let $u = a^{-1}b^{-k}c$. By the construction of c we have $uu^* = 1$. Thus the ideal $J = uI$ is in the same class as I and, since b and c are units of $O_{(l)}G$, we have $JO_{(l)} = uaO_{(l)}G = O_{(l)}G$, as desired. ∎

Let N/K be a tame G-extension and choose a primitive element $\alpha \in N$ such that $a = \alpha^l$ is in K and satisfies $a \equiv 1 \pmod{l'}$ (this is always possible by tameness; see [12, Proposition 3.1.1]). Let $\psi \in \hat{G}$ be the character defined by $\psi(g) = \alpha^g/\alpha$.

(3.2) PROPOSITION. *Let* $\mathfrak{f}\colon \hat{G} \to \mathfrak{I}$ *be the map defined at the character* $\chi = \psi^r$ *by the condition*

$$|\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}(\psi^r)^l a^{t(r)})| \leqslant (l-1)/2 \qquad \textit{for all primes} \quad \mathfrak{p}. \tag{2}$$

Then $\mathfrak{f}$ *induces a homomorphism* $\mathbb{Z}\hat{G}/\mathbb{Z}\hat{G}^+ \to \mathfrak{I}$ *and* $L_*(\mathfrak{f}) = \rho_{N/K}$.

Proof. Let $\mathbf{r}\colon \bar{K}\otimes_K N \to \bar{K}G$ be the canonical homomorphism given by $\mathbf{r}(x\otimes y) = \sum_{g\in G} xy^g g^{-1}$. It is very easy to verify that $\mathbf{r}$ is $\bar{K}G$-equivalent and that it transforms the trace form $t_{N/K}$ on $\bar{K}\otimes_K N$ into the canonical standard form t_G on $\bar{K}G$. For an element $y \in N$ and a character $\chi \in \hat{G}$ we denote by $(y \mid \chi)$ the resolvent of y with respect to χ, that is,

$$(y \mid \chi) = \sum_{g\in G} \chi^*(g)\, y^g.$$

Clearly we have

$$\mathbf{r}(1\otimes y) = \sum_{\chi\in\hat{G}} (y \mid \chi)\, e_\chi,$$

where e_χ is the idempotent correspondent to the character χ. The resolvent $(y \mid \chi)$ has the property

$$(y \mid \chi)^g = \chi(g)(y \mid \chi).$$

In particular, $\alpha^{-r}(y \mid \psi^r)$ is invariant under G for all integers r, that is, it lies in the ground field K. Thus we can write

$$(A_{N/K} \mid \psi^r) = \mathfrak{f}(\psi^r)\, \alpha^{t(r)} \tag{3}$$

for some ideal $\mathfrak{f}(\psi^r)$ of K. Since $\mathbf{r}$ is an isometry, $\mathbf{r}(O_N\otimes A_{N/K})$ is a locally free self-dual lattice in NG and by Theorem 2.2 it must satisfy the equality $\mathbf{r}(O_N\otimes A_{N/K})\ \mathbf{r}(O_N\otimes A_{N/K})^* = O_N G$. This in turn implies $(A_{N/K} \mid \psi^r)(A_{N/K} \mid \psi^{*r}) = (1)$. By (3) we have $\mathfrak{f}(\psi^r)\,\mathfrak{f}(\psi^{*r}) = (1)$.

Let $\mathfrak{p}$ be a prime of K above l. Since N/K is tame, the prime $\mathfrak{p}$ is unramified and therefore $\mathbf{r}(O_N\otimes A_{N/K})_{\mathfrak{p}} = \mathbf{r}(O_N\otimes O_N)_{\mathfrak{p}} = \mathbf{r}(O_N)_{\mathfrak{p}}\, G$. Hence $(O_N)_{\mathfrak{p}}(A_{N/K} \mid \psi^r)_{\mathfrak{p}} = (O_N)_{\mathfrak{p}}$. Since α was chosen relatively prime to l, we must have $\mathfrak{f}(\chi)_{\mathfrak{p}} = (1)$. Hence $\mathfrak{f}(\chi)$ is relatively prime to l.

On the other hand, for a prime $\mathfrak{p}$ not dividing l we have

$$\begin{aligned}\mathbf{r}(1\otimes A_{N/K})_{\mathfrak{p}} &= \sum_{\chi\in G}(A_{N/K}\mid\chi)_{\mathfrak{p}}\, e_{\chi}\\ &= \sum_{r \bmod l}\mathfrak{f}(\psi^r)_{\mathfrak{p}}\, \alpha^{t(r)} e_{\psi^r}.\end{aligned}$$

Thus, letting $u=\sum_r \alpha^{t(r)} e_{\psi^r}$, we have

$$\mathbf{r}(1\otimes A_{N/K}) = L(\mathfrak{f})\, u.$$

This shows that $\mathfrak{f}$ is a representative of the class of $\rho_{N/K}$ (observe that $u^{-1}\mathbf{r}$ gives a G-isometry between $A_{N/K}$ and $L(\mathfrak{f})$).

We shall now show that $\mathfrak{f}$ satisfies the inequality (2) (and therefore it is determined by this condition). On the one hand, since $A_{N/K}$ is an O_N-ideal and is stable by G, we have $(A_{N/K}\mid\chi)\, O_N\subseteq A_{N/K}$. On the other hand, by self-duality, $(A_{N/K}\mid\chi)(A_{N/K}\mid\chi^*)\, O_N = O_N$. Thus

$$A_{N/K}^{-1}\subseteq (A_{N/K}\mid\chi)\, O_N\subseteq A_{N/K} \tag{4}$$

for all $\chi\in\hat{G}$. Let $\mathfrak{P}$ be a prime of N. Taking $\mathfrak{P}$-valuations in (4), we have

$$-\operatorname{ord}_{\mathfrak{P}}(A_{N/K})\geqslant \operatorname{ord}_{\mathfrak{P}}(A_{N/K}\mid\chi)\, O_N)\geqslant \operatorname{ord}_{\mathfrak{P}}(A_{N/K}). \tag{5}$$

Using (3) we obtain the inequalities

$$-\operatorname{ord}_{\mathfrak{P}}(A_{N/K})\geqslant \operatorname{ord}_{\mathfrak{P}}(\mathfrak{f}(\psi^r)) + t(r)\operatorname{ord}_{\mathfrak{P}}(\alpha)\geqslant \operatorname{ord}_{\mathfrak{P}}(A_{N/K}). \tag{6}$$

For $\mathfrak{P}$ unramified over K we have $\operatorname{ord}_{\mathfrak{P}}(A_{N/K})=0$ and $\operatorname{ord}_{\mathfrak{p}}(a) = l\operatorname{ord}_{\mathfrak{P}}(\alpha)$. Thus

$$l\operatorname{ord}_{\mathfrak{P}}(\mathfrak{f}(\psi^r)) + t(r)\operatorname{ord}_{\mathfrak{p}}(a) = 0.$$

This proves (2) for unramified $\mathfrak{p}$ (observe that $\operatorname{ord}_{\mathfrak{p}}(a)\equiv 0 \pmod{l}$ in this case).

For $\mathfrak{P}$ ramified over K we have $\operatorname{ord}_{\mathfrak{P}}(A_{N/K}) = -(l-1)/2$, $\operatorname{ord}_{\mathfrak{p}}(a) = \operatorname{ord}_{\mathfrak{P}}(\alpha)$, and $\operatorname{ord}_{\mathfrak{P}}(\mathfrak{f}(\psi^r)) = l\operatorname{ord}_{\mathfrak{p}}(\mathfrak{f}(\psi^r))$. Replacing these values in (6) shows (2) also in this case. ∎

We shall now characterize the classes produced by the construction above. The automorphism group Δ acts in an obvious way on the groups appearing in (1) and it is not difficult to see that (1) is actually a presentation of $\mathrm{UCl}(O_K G)$ as Δ-modules. We define the *hermitian Stickelberger element* ϕ in $\mathbb{Z}\Delta$ by

$$\phi = \sum_{\substack{r=-(l-1)/2\\ r\neq 0}}^{(l-1)/2} r\delta_r^{-1}.$$

Note the resemblance of ϕ with the classical Stickelberger element

$$\theta = \sum_{r=1}^{l-1} r\delta_r^{-1}$$

(see [11, 12]). Note also that ϕ and θ are related by the congruence $\phi \equiv \theta \pmod{l}$.

Similarly, we define the *hermitian Stickelberger ideal* by

$$S = \frac{\phi}{l}\, \mathbb{Z}\Delta \cap \mathbb{Z}\Delta.$$

Some technical statements are needed to prove our main result in this section.

(3.3) LEMMA. *Let $\mathfrak{g}$: $\hat{G} \to \mathfrak{J}$ be the map defined by*

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{g}(\psi^r)) = \begin{cases} 1 & \text{if } \; r\cdot \operatorname{ord}_{\mathfrak{p}}(a) \equiv 1 \pmod{l}, \\ 0 & \text{otherwise}. \end{cases}$$

Then

$$\mathfrak{g}^{\phi}(\psi^r) = \mathfrak{f}(\psi^r)^l\, a^{t(r)}. \tag{7}$$

Proof. By direct computation,

$$\begin{aligned} \operatorname{ord}_{\mathfrak{p}}(\mathfrak{g}^{\phi}(\psi^r)) &= \sum_{s \in \mathbb{F}_l^*} t(s) \operatorname{ord}_{\mathfrak{p}}(\mathfrak{g}(\psi^{s^{-1}r})) \\ &= t(r\cdot \operatorname{ord}_{\mathfrak{p}}(a)) \\ &= (t(r\cdot \operatorname{ord}_{\mathfrak{p}}(a)) - t(r)\operatorname{ord}_{\mathfrak{p}}(a)) + t(r)\operatorname{ord}_{\mathfrak{p}}(a) \\ &= \operatorname{ord}_{\mathfrak{p}}(\mathfrak{f}(\psi^r)^l\, a^{t(r)}). \quad \blacksquare \end{aligned}$$

Let $T \subset \mathbb{Z}\Delta$ be the subgroup generated by l and $\delta_r - r$ $(1 \leqslant r \leqslant l-1)$. It can be easily verified that T is a $\mathbb{Z}\Delta$-ideal.

(3.4) LEMMA. *Let $\mathfrak{f}$ and $\mathfrak{g}$ be as above. Then*

$$L_*(\mathfrak{f})^{\alpha} = L_*(\mathfrak{g}^{\phi\alpha/l}) \tag{8}$$

for all $\alpha \in T$.

Proof. It is sufficient to prove (8) for the generators of T. For $\alpha = l$, this follows from (7). Nox let $\alpha = \delta_s - s$. Applying α to (7), we have

$$\mathfrak{g}^{\phi\alpha}(\psi^r) = \mathfrak{f}^{l\alpha}(\psi^r)\, a^{t(rs) - st(r)}.$$

Hence

$$\mathfrak{g}^{\phi\alpha/l}(\psi^r) = \mathfrak{f}^{\alpha}(\psi^r)\, a^{(t(rs) \quad st(r))/l}$$

(observe that $t(rs) - st(r) \equiv 0 \pmod{l}$). Since $a \equiv 1 \pmod{l}$, the function $\psi^r \mapsto a^{(t(rs) \quad st(r))/l}$ lies in the kernel of L_* for all $1 \leqslant s \leqslant l-1$. Thus $L_*(\mathfrak{f})^{\alpha} = L_*(\mathfrak{g}^{\phi\alpha/l})$. ∎

(3.5) Lemma. *The ideal $T \subset \mathbb{Z}\Delta$ satisfies the equalities*

(1) $[\mathbb{Z}\Delta : T] = l$.

(2) $\phi\mathbb{Z}\Delta + T = \mathbb{Z}\Delta$.

(3) $S = (\phi/l)\, T$.

Proof. Let $c: \Delta \to \mathbb{F}_l^{\times}$ be the character given by $c(\delta_r) \equiv r \pmod{l}$. By definition T is the kernel of the induced ring homomorphism $c: \mathbb{Z}\Delta \to \mathbb{F}_l$. In particular T has index l in $\mathbb{Z}\Delta$. By direct computation, we see that $c(\phi) = -1$. Hence $\phi\mathbb{Z}\Delta + T = \mathbb{Z}\Delta$, as required. This proves (1) and (2). By direct computation we see $\phi(\delta_r - r) \equiv 0 \pmod{l}$, thus $\phi T \subseteq lS$. Conversely, $lS \subseteq \phi\mathbb{Z}\Delta \cap T = \phi T$ by (2). ∎

We are now ready to state and prove our main theorem. Recall that $\mathrm{RU}(O_K G)$ denotes the subset of $\mathrm{UCL}(O_K G)$ of realizable classes.

(3.6) Theorem. *Let $S = (\phi/l)\, \mathbb{Z}\Delta \cap \mathbb{Z}\Delta$. Then the map*

$$v: S \otimes_{\mathbb{Z}\Delta} \mathrm{Cl}(O_K G) \to \mathrm{UCl}(O_K G)$$
$$\gamma \otimes \mathrm{cl}(I) \mapsto \mathrm{ucl}(I^{\gamma})$$

is well-defined and its image is $\mathrm{RU}(O_K, G)$. *In particular*, $\mathrm{RU}(O_K G)$ *is a subgroup of* $\mathrm{UCl}(O_K G)$.

Proof. Let I be a locally free lattice in KG and $\gamma \in S$. We shall see that I^{γ} defines a class in the unitary class group. Let $\sigma = \delta_{-1}$ (i.e., the automorphism of G given by group inversion). It is easy to see from the definition of ϕ that $(1+\sigma)\, S = 0$, hence, for $\gamma \in S$, we have

$$I^{\gamma}(I^{\gamma})^* I^{\gamma(1+\sigma)}$$
$$= O_K G.$$

Similarly, for $u \in KG^{\times}$ we have

$$u^{\gamma}(u^{\gamma})^* = 1. \tag{9}$$

This shows that the class of I^{γ} in $\mathrm{UCl}(O_K G)$ depends solely on the class of I in $\mathrm{Cl}(O_K G)$. Therefore the correspondence $(\gamma, I) \mapsto I^{\gamma}$ induces a well-defined map

$$\nu\colon S \otimes_{\mathbb{Z}\Delta} \mathrm{Cl}(O_K G) \to \mathrm{UCl}(O_K G),$$

which is clearly a $\mathbb{Z}\Delta$-homomorphism.

We shall show now that the realizable classes lie in the image of ν. Let N/K be a tame G-extension and let $\mathfrak{f}\colon \mathbb{Z}\hat{G}/\mathbb{Z}\hat{G}^{+} \to \mathfrak{J}$ be the homomorphism associated with N by Proposition 3.2. By Lemma 3.4 we have for all $\alpha \in T$ the following equality in $\mathrm{UCl}(O_K G)$:

$$\begin{aligned} L_*(\mathfrak{f})^{\alpha} &= L_*(\mathfrak{g}^{\phi\alpha/l}) \\ &= \nu(\mathrm{cl}(L(\mathfrak{g})) \otimes \phi\alpha/l). \end{aligned}$$

In particular, we have for all $\alpha \in T$

$$L_*(\mathfrak{f})^{\alpha} \equiv 1 \qquad (\mathrm{mod}\ \mathrm{Im}(\nu)),$$

and also,

$$\begin{aligned} L_*(\mathfrak{f})^{\phi} &= \nu(\mathrm{cl}(L(\mathfrak{f})) \otimes \phi) \\ &\equiv 1 \qquad (\mathrm{mod}\ \mathrm{Im}(\nu)). \end{aligned}$$

Thus, by Lemma 3.5, part (2),

$$L_*(\mathfrak{f}) = 1 \qquad (\mathrm{mod}\ \mathrm{Im}(\nu)),$$

that is, the realizable classes are contained in the image of ν.

We shall now show that $\mathrm{Im}(\nu)$ is contained in $\mathrm{RU}(O_K G)$. Since T has index l in $\mathbb{Z}\Delta$ (Lemma 3.5, part (1)) and $|\Delta| = l - 1$ is not divisible by l, the ideal T is locally free as a $\mathbb{Z}\Delta$-module. By the Chinese Remainder Theorem, we may choose a single $\beta \in T$ such that

$$T \otimes \mathbb{Z}_p = \beta \mathbb{Z}_p \Delta$$

for all primes p dividing $|\mathrm{Cl}(O_K G)|$. By Lemma 3.5, part (3), we have $S = (\phi/l)\, T$ and therefore all the elements of $\mathrm{Cl}(O_K G) \otimes_{\mathbb{Z}\Delta} S$ can be written in the form

$$\mathrm{cl}(L(\mathfrak{g})) \otimes (\phi\beta/l), \tag{10}$$

with $\mathfrak{g}\colon \mathbb{Z}\hat{G} \to \mathfrak{J}$.

Let I represent a class in $\mathrm{Im}(\nu)$. By (10) we may assume

$$I = L(\mathfrak{g}^{\phi\beta/l})$$

for some $g \in \mathrm{Hom}(\mathbb{Z}\hat{G}, \mathfrak{I})$. For each character $\chi \in \hat{G}$ we choose a prime ideal $\mathfrak{h}(\chi)$ in the ray class of $\mathfrak{g}^{\beta}(\chi)$ modulo $\mathfrak{l}^l$. Since there are infinitely many such primes, we may assume that the $\mathfrak{h}(\chi)$ are all distinct. Thus we have

$$\mathfrak{f}^l u^{\phi} = \mathfrak{h}^{\phi}, \tag{11}$$

where $\mathfrak{f} = \mathfrak{g}^{\phi\beta/l} \in \mathrm{Hom}(\mathbb{Z}\hat{G}/\mathbb{Z}\hat{G}^{+}, \mathfrak{I})$ and $u \in \mathrm{Hom}(\mathbb{Z}\hat{G}, K^{\times})$ has the property $u(\chi) \equiv 1 \pmod{\mathfrak{l}^l}$ for all $\chi \in \hat{G}$.

Let $\psi \in \hat{G}$ be a fixed generator and define $v: \hat{G} \to K^{\times}$ by

$$v(\psi^r) = u^{\phi(\delta_r - t(r))/l}(\psi) \tag{12}$$

for $r \neq 0$ and $v(1) = 1$. Note that $\phi(\delta_r - t(r)) \equiv 0 \pmod{l}$ and that $v(\psi^r)\, v(\psi^{*r}) = 1$ by (9). Letting $a = u^{\phi}(\psi)$ we can write (12) in the form

$$u^{\phi}(\psi^r) = v(\psi^r)^l a^{t(r)},$$

and by substituting in (11) we obtain

$$(v\mathfrak{f})(\psi^r)^l a^{t(r)} = \mathfrak{h}^{\phi}(\psi^r). \tag{13}$$

Now, by construction of h we have

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{h}^{\phi}(\psi^r)) = \begin{cases} t(s) & \text{if } \mathfrak{h}(\psi^m) = \mathfrak{p} \text{ with } sm \equiv r \pmod{l} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

This shows that a is not an lth power in K (otherwise, by (13), $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{h}^{\phi}(\psi^r))$ would be always divisible by l).

Let $\alpha = \sqrt[l]{a}$ and let $N = K(\alpha)$. Let G act on N by $\alpha^g = \psi(g)\,\alpha$. Since $a \equiv 1 \pmod{\mathfrak{l}^l}$, the extension N/K is tame (see [12, Proposition 3.1.1]). From (14) we obtain the inequality $|\mathrm{ord}_{\mathfrak{p}}(\mathfrak{h}^{\phi}(\psi^r))| \leqslant (l-1)/2$. By (13) and Proposition 3.2 we conclude that $L_*(v\mathfrak{f}) = \rho_{N/K}$. Note that since v satisfies the condition $v(\chi) \equiv 1 \pmod{l}$, we have

$$\sum_{\chi \in \hat{G}} v(\chi)\, e_{\chi} \in O_{(l)} G^{(1)}.$$

Thus $L_*(v) = 1$ and therefore $L_*(\mathfrak{f}) = \rho_{N/K}$. ∎

ACKNOWLEDGMENT

The author is indebted to the referee for her or his helpful detailed suggestions.

REFERENCES

1. E. BAYER AND H. W. LENSTRA, Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359–373.
2. J. BRINKHUIS, Normal integral bases and the Spiegelungsatz of Scholz, preprint, 1990.
3. PH. CASSOU-NOGUÈS AND M. J. TAYLOR, Local root numbers and hermitian Galois module structure of rings of integers, *Math. Ann.* **263** (1983), 251–261.
4. PH. CASSOU-NOGUÈS AND M. J. TAYLOR, The trace form and Swan modules, *Bull. London Math. Soc.* **22** (1990), 422–428.
5. P. E. CONNER AND R. PERLIS, "A Survey of Trace Forms of Algebraic Number Fields," *World Sci. Publ.*, Singapore, 1984.
6. B. EREZ, The Galois structure of the square root of the inverse different, *Math. Z.* **208** (1991), 239–255.
7. B. EREZ AND M. J. TAYLOR, Hermitian modules in Galois extensions of number fields and Adams operations, *Ann. of Math.* **135** (1992), 271–296.
8. B. EREZ AND J. MORALES, The hermitian structure of rings of integers in odd degree abelian extensions, *J. Number Theory* **40**, No. 1 (1992), 92–104.
9. A. FRÖHLICH, "Classgroups and Hermitian Modules," Birkhäuser, Boston/Basel/Stuttgart, 1984.
10. A. FRÖHLICH, "Galois Module Structure of Algebraic Integers," Ergebnisse (3), Band 1, Springer-Verlag, Berlin/New York, 1983.
11. A. FRÖHLICH, "Stickelberger without Gauss sums," *in* "Algebraic Number fields, L-Functions and Galois Properties" (A. Fröhlich, Ed.), pp. 589–607, Academic Press, London/New York, 1977.
12. L. MCCULLOH, A Stickelberger condition on Galois module structure for Kummer extensions of prime degree, *in* "Algebraic Number Fields, L-Functions and Galois Properties" (A. Fröhlich, Ed.), pp. 561–587, Academic Press, London/New York, 1977.
13. L. MCCULLOH, Galois module structure of abelian extensions, *J. Reine Angew. Math.* **375/376** (1987).
14. J. MORALES, Integral bilinear forms with a group action, *J. Algebra* **98**, No. 2 (1986), 470–484.
15. J. MORALES, Hermitian class numbers in group rings, *Bull. London Math. Soc.* **22** (1990), 321–332.
16. J.-P. SERRE, "Local Fields," Graduate Texts in Mathematics, Vol. 67, Springer-Verlag, Berlin/New York, 1979.
17. M. J. TAYLOR, Rings of integers and trace forms for tame extensions of odd degree, *Math. Z.* **202**, No. 3 (1989), 313–341.