JOURNAL OF NUMBER THEORY 40, 92–104 (1992)

The Hermitian Structure of Rings of Integers in Odd Degree Abelian Extensions

BOAS EREZ*

Université de Genève, Section de Mathématiques, Case postale 240, 1211 Genève 24, Switzerland

AND

JORGE MORALES†

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

Communicated by H. Zassenhaus

Received September 15, 1989; revised August 9, 1990

In this paper we begin by considering the equivariant genus of quite arbitrary hermitian forms over a group ring $O_K[G]$, where O_K is the ring of integers in a number field K and G is an abelian group of odd order. The result we obtain is then applied to the case where G is the Galois group of a tamely ramified extension E/K and the form is the one obtained by restricting the bilinear trace form $t_{E/K}$ to the ring O_E of integers in E. More precisely let $A_{E/K}$ be the unique fractional ideal in E whose square is the inverse different of the extension E/K; then we construct a locally free ideal $M_{E/K}$ in $O_K[G]$ such that $M_{E/K}A_{E/K} = O_E$ and we show that when equipped with the multiplication form t_G on $K[G]$, then $(M_{E/K}, t_G)$ lies in the equivariant genus of $(O_E, t_{E/K})$. Finally we show that when $K = \mathbb{Q}$, then $(O_L, t_{L/K})$ (respectively $(A_{E/K}, t_{E/K})$) is actually isometric to $(M_{E/K}, t_G)$ (respectively $(O_K[G], t_G)$).

INTRODUCTION

We recall that the trace form of a finite separable field extension E/K is the symmetric K-bilinear form $t_{E/K}$ on E given by $t_{E/K}(x, y) = \mathrm{Tr}_{E/K}(xy)$. If the extension E/K is normal then the Galois group $G = \mathrm{Gal}(E/K)$ acts as isometries on this form. It is natural to take this additional structure into account. It has been shown (see Conner–Perlis [4, V.3.3] for $K = \mathbb{Q}$ and

* To whom correspondence should be addressed at Department of Mathematics, Harvard University, One Oxford Street, Cambridge, MA 02178.

† Supported by a grant from Louisiana State University Council on Research.

0022-314X/92 $3.00

Bayer–Lenstra [2] for a general field) that if G has *odd* order, then the trace form $t_{E/K}$ is *equivariantly* isometric to the standard form $t_G(g, h) = \delta_{gh}$ on the group algebra $K[G]$. Thus, in the case of number fields, the lattice $(O_E, t_{E/K})$ is *equivariantly* isometric to a full $O_K[G]$-lattice in the group algebra $K[G]$. If, in addition, the extension E/K is tame then by Noether's Theorem the ring of integers O_E is locally free as an $O_K[G]$-module (see [8, Theorem 3, p. 26]). We are thus naturally led to investigate the equivariant isometry classes of *locally free* $O_K[G]$-lattices in $(K[G], t_G)$ for a given group G of odd order. In this article we restrict our attention to the case when G is abelian.

In Section 2 we show that the equivariant genus of (L, t_G), where L is a locally free $O_K[G]$-lattice in $K[G]$, is determined by the class of the associated torsion module $L^\#/L$ (Theorem 2.3). As an application we show that the equivariant genus of $(O_E, t_{E/K})$, where E/K is a tame abelian extension of odd degree, is determined by the inertia subgroups (see Corollary 2.6). We also show that in tame cyclic extensions the equivariant genus of $(O_E, t_{E/K})$ is determined by the discriminant of E/K (Corollary 2.7). We show by means of a counterexample (Example 2.9) that this result is no longer true for non-cyclic extensions.

In Section 3 we investigate the equivariant isometry class of $(O_E, t_{E/K})$ by means of a canonically defined $O_K[G]$-lattice $M_{E/K}$ in $K[G]$. The form $(M_{E/K}, t_G)$ turns out to always be in the genus of $(O_E, t_{E/K})$ (Proposition 3.1). Moreover, $(M_{E/K}, t_G)$ has the following remarkable property: the forms $(O_E, t_{E/K})$ and $(M_{E/K}, t_G)$ are G-isometric if and only if the ideal $A_{E/K} = \mathfrak{D}_{E/K}^{-1/2}$ in E possesses a self-dual normal basis over O_K (Theorem 3.3).

In Section 4 we consider the case $K = \mathbb{Q}$. It is proved there that $A_{E/\mathbb{Q}}$ has a self-dual normal basis if and only if $E/\mathbb{Q}$ is *weakly* ramified (Theorem 4.1). In particular if $E/\mathbb{Q}$ is tame, this result implies—in virtue of our results of Section 3—that $(O_E, t_{E/\mathbb{Q}})$ and $(M_{E/\mathbb{Q}}, t_G)$ are G-isometric (Corollary 4.4).

To end this introduction we mention that B. Erez and M. Taylor in their recent work [7] were able to generalize part of the results of the present paper to not necessarily abelian extensions. In particular they define a module which generalizes the "comparison" module $M_{E/K}$ and which allows them to obtain somewhat more precise results than those contained in [11].

1. Terminology and Notation

Here we recall the terminology and the notation that are used in the next sections. Let k be a commutative ring and G a finite group. The canonical involution on $k[G]$ (i.e., the involution induced by inverting elements

in the group) will be denoted by $\alpha \mapsto \bar{\alpha}$. A *hermitian form* over $k[G]$ is a pair (M, h) where M is a finitely generated left $k[G]$-module and $h: M \times M \to k[G]$ is a map $k[G]$-linear in the first variable that satisfies the symmetry condition $h(x, y) = \overline{h(y, x)}$. Using the canonical $k[G]$-isomorphism

$$\mathrm{Hom}_k(M, k) \to \mathrm{Hom}_{k[G]}(M, k[G])$$

$$f \mapsto \left(x \mapsto \sum_{g \in G} f(g^{-1}x)\, g \right)$$

we shall identify the set of hermitian forms over $k[G]$ with the set of G-invariant symmetric k-bilinear forms. Two symmetric G-invariant forms (M, t) and (M', t') over k are said to be *G-isometric* if there is a $k[G]$-isomorphism $\phi: M \to M'$ such that $t'(\phi(x), \phi(y)) = t(x, y)$ for all x, y in M.

Let now K be a number field and let O_K be the ring of integers of K. Let (M, t) and (M', t') be G-invariant symmetric belinear forms over O_K.

(1.1) DEFINITION. We say that (M, t) and (M', t') are in the *same class* if they are G-isometric over O_K. We say that they are in the *same equivariant genus* (or simply in the *same genus*) if (M_v, t) and (M'_v, t') are G-isometric over the completions O_{K_v} for all places v of K (archimedean and non-archimedean).

In order to compare trace forms arising from different Galois extensions of a given field, we need to introduce the following definition.

(1.2) DEFINITION. Let G and G' be finite groups. Let (M, t) (respectively (M', t')) be a G-invariant (respectively G'-invariant) form over O_K. We say that (M, t) and (M', t') are in the *same genus* (respectively *same class*) if there exists an isomorphism $\phi: G \to G'$ such that (M, t) and $(\phi_* M', \phi_* t')$ are in the same genus (respectively same class). Here $(\phi_* M', \phi_* t')$ means (M', t') endowed with the G-structure induced by ϕ.

2. THE EQUIVARIANT GENUS OF THE TRACE FORM

The following notation is used throughout this section:

G is a finite abelian group of odd order

K is a number field

O_K is the ring of integers of K

$\mathfrak{p}$ is a prime ideal of O_K

$k(\mathfrak{p})$ is the residue field $O_K/\mathfrak{p}$

$K_\mathfrak{p}$ is the $\mathfrak{p}$-adic completion of K

$O_{K_\mathfrak{p}}$ is the ring of integers of $K_\mathfrak{p}$

In general the subscript $\mathfrak{p}$ means local completion at $\mathfrak{p}$.

In this section we characterize the genus of (L, t_G), where L is a locally free $O_K[G]$-lattice in $K[G]$. We begin by proving two technical results that are used in the proof of the main theorem.

(2.1) LEMMA. *Let k be a field and let V be a simple self-dual $k[G]$-module. Let $l = \mathrm{End}_{k[G]}(V)$. Then the adjoint involution (with respect to any equivariant symmetric or skew-symmetric form on V) is trivial on l if and only if V is the trivial 1-dimensional $k[G]$-module.*

Proof. Take g in G. Since G is abelian, the linear map $g: V \to V$ can be regarded as a $k[G]$-endomorphism of V. If the adjoint involution on V is trivial, we have $gx = g^{-1}x$ for $x \in V$. Since G has odd order, this implies that G acts trivially on V. ∎

For any commutative ring k, the group ring $k[G]$ will be regarded as a C_2-module, where the generator of C_2 acts by the canonical involution.

(2.2) LEMMA. *The inclusion $O_{K_\mathfrak{p}}[G] \to K_\mathfrak{p}[G]$ induces an injective homomorphism between the Tate cohomology groups*

$$\hat{H}^0(C_2, \mathrm{O}_{K_\mathfrak{p}}[G]^*) \to \hat{H}^0(C_2, K_\mathfrak{p}[G]^*).$$

Proof. Let $x \in O_{K_\mathfrak{p}}[G]^*$ be a representative of an element in the kernel of the homomorphism $\hat{H}^0(C_2, O_{K_\mathfrak{p}}[G]^*) \to \hat{H}^0(C_2, K_\mathfrak{p}[G]^*)$; that is, $x = y\bar{y}$ for some y in $K_\mathfrak{p}[G]^*$. Since G is abelian, the group algebra $K_\mathfrak{p}[G]$ is isomorphic to a product of fields

$$K_\mathfrak{p} \times E_1 \times \cdots \times E_m \times (F_1 \times F_1) \times \cdots \times (F_n \times F_n),$$

where the involution, by Lemma 2.1, induces non-trivial maps on the factors E_i and switches the components of $(F_j \times F_j)$. Suppose first that $\mathfrak{p}$ does not divide the order of G. In this case, the group ring $O_{K_\mathfrak{p}}[G]$ is a maximal order (see [5, Proposition 27.1, p. 582]). Therefore

$$O_{K_\mathfrak{p}}[G] = O_{K_\mathfrak{p}} \times O_{E_1} \times \cdots \times O_{E_m} \times (O_{F_1} \times O_{F_1}) \times \cdots \times (O_{F_n} \times O_{F_n}).$$

Observe that by the hypothesis on $\mathfrak{p}$ the field E_i is unramified over the field fixed by the involution (E_i is obtained from $K_\mathfrak{p}$ by adjoining dth roots of unity, where d is a divisor of $|G|$). In particular $\hat{H}^0(C_2, O_{E_i}^*) = 0$ (see for instance [10, Chapter V]). Note that the components $O_{F_j} \times O_{F_j}$ do not contribute to $\hat{H}^0(C_2, O_{K_\mathfrak{p}}[G]^*)$. Hence the augmentation

map $\varepsilon: O_{K_\mathfrak{p}}[G] \to O_{K_\mathfrak{p}}$ induces an isomorphism $\varepsilon: \hat{H}^0(C_2, O_{K_\mathfrak{p}}[G]^*) \to \hat{H}^0(C_2, O_{K_\mathfrak{p}}^*) = O_{K_\mathfrak{p}}^*/O_{K_\mathfrak{p}}^{*2}$. We have $\varepsilon(x) = \varepsilon(y)^2 \in O_{K_\mathfrak{p}}^{*2}$, thus x represents 0 in $\hat{H}^0(C_2, O_{K_\mathfrak{p}}[G]^*)$.

Suppose now that $\mathfrak{p}$ divides $|G|$. Let $\mathfrak{r}$ be the radical of $O_{K_\mathfrak{p}}[G]$. The ring $O_{K_\mathfrak{p}}[G]/\mathfrak{r}$ is a product of finite fields, and, by Lemma 2.1, the group C_2 acts non-trivially on all components except for the component corresponding to the trivial one-dimensional $k(\mathfrak{p})[G]$-module. Thus the augmentation map $\varepsilon: O_{K_\mathfrak{p}}[G] \to O_{K_\mathfrak{p}}$ induces an isomorphism $\varepsilon: \hat{H}^0(C_2, (O_{K_\mathfrak{p}}[G]/\mathfrak{r})^*) \to \hat{H}^0(C_2, k(\mathfrak{p})^*) = k(\mathfrak{p})^*/k(\mathfrak{p})^{*2}$. Since $\varepsilon(x) = \varepsilon(y)^2$ there exists $z_1 \in O_{K_\mathfrak{p}}[G]^*$ such that $x \equiv z_1 \bar{z}_1 \pmod{\mathfrak{r}}$. We shall construct by induction a sequence $\{z_m\}_{m \geq 1}$ with the property $x \equiv z_m \bar{z}_m \pmod{\mathfrak{r}^m}$ for all m. By completeness of $O_{K_\mathfrak{p}}[G]$ with respect to the $\mathfrak{r}$-adic topology, this sequence will converge to a limit z satisfying $x = z\bar{z}$, and this will prove the lemma. Here is the induction step: suppose $x \equiv z_m \bar{z}_m \pmod{\mathfrak{r}^m}$ and let $w = x - z_m \bar{z}_m$. Since $\mathfrak{p}$ is not a dyadic prime, we have $\hat{H}^0(C_2, \mathfrak{r}^m/\mathfrak{r}^{m+1}) = 0$. Thus there exists s in $\mathfrak{r}^m$ such that $w \equiv s\bar{z}_m + \bar{s}z_m \pmod{\mathfrak{r}^{m+1}}$ (observe that z_m is a unit). We set $z_{m+1} = z_m + s$. By the construction of s we have $x \equiv z_{m+1}\bar{z}_{m+1} \pmod{\mathfrak{r}^{m+1}}$. ∎

(2.3) THEOREM. *Let L and M be locally free $O_K[G]$-lattices in $K[G]$ on which the form t_G takes values in O_K. The following are equivalent:*

(a) *(L, t_G) and (M, t_G) are in the same equivariant genus.*

(b) *$L^\sharp/L$ and $M^\sharp/M$ are isomorphic as $O_K[G]$-modules (where as usual $^\sharp$ denotes the dual with respect to t_G).*

Proof. The implication (a) ⇒ (b) is obvious, so let us prove (b) ⇒ (a). Let $\mathfrak{p}$ be a prime ideal. Locally M and N are free $O_{K_\mathfrak{p}}[G]$-modules of rank one. Thus there exists $u \in K_\mathfrak{p}[G]^*$ such that $L_\mathfrak{p} = uM_\mathfrak{p}$. An easy calculation shows that $L_\mathfrak{p}^\sharp = \bar{u}^{-1} M_\mathfrak{p}^\sharp$. Consequently we have

$$M_\mathfrak{p}^\sharp/M_\mathfrak{p} \cong L_\mathfrak{p}^\sharp/L_\mathfrak{p} = \bar{u}^{-1} M_\mathfrak{p}^\sharp/uM_\mathfrak{p} \cong M_\mathfrak{p}^\sharp/u\bar{u}M_\mathfrak{p}.$$

Hence $u\bar{u}$ is a unit of $O_{K_\mathfrak{p}}[G]$. By the construction of u, $u\bar{u}$ represents an element of the kernel of the natural map $\hat{H}^0(C_2, O_{K_\mathfrak{p}}[G]^*) \to \hat{H}^0(C_2, K_\mathfrak{p}[G]^*)$ which is, by Lemma 2.2, an injective homomorphism. Therefore there exists $v \in O_{K_\mathfrak{p}}[G]^*$ such that $v\bar{v} = u\bar{u}$. Let $w = uv^{-1}$. Clearly w satisfies $w\bar{w} = 1$ and thus gives the desired isometry. ∎

(2.4) COROLLARY. *The locally free $O_K[G]$-lattices in $K[G]$ which are self-dual with respect to t_G belong to the principal genus (i.e., the genus of $(O_K[G], t_G)$).*

In order to apply Theorem 2.3 to the trace form, we need to know the structure of the torsion module $\mathfrak{D}_{E/K}^{-1}/O_E$ for an abelian extension E/K,

where the *inverse different* $\mathfrak{D}_{E/K}^{-1}$ of the extension E/K is by definition the dual of O_E with respect to the trace form. The structure of $\mathfrak{D}_{E/K}^{-1}/O_E$ is given by a result of S. Chase [3, Theorem 1.8]. We reformulate this result in the particular case of an abelian group:

(2.5) PROPOSITION (S. Chase). *Let E/K be a tame abelian extension with Galois group G. Let $\mathfrak{p}$ be a prime in K. Then there is an isomorphism of $O_K[G]$-modules*

$$(\mathfrak{D}_{E/K}^{-1}/O_E)_{\mathfrak{p}} \cong k(\mathfrak{p})[G]/(\sigma_{\mathfrak{p}}),$$

where $\sigma_{\mathfrak{p}} = \sum_{\tau} \tau$, with τ running over all elements of the inertia subgroup $T_{\mathfrak{p}}$.

Proposition 2.5 together with Theorem 2.3 says that the genus of the trace form is determined by the inertia subgroups. Here is a more precise statement:

(2.6) COROLLARY. *Let E/K and E'/K be two tame odd degree abelian extensions. Then $(O_E, t_{E/K})$ and $(O_{E'}, t_{E'/K})$ are in the same genus (in the sense of Definition* 1.2) *if and only if there exists an isomorphism $\phi\colon \mathrm{Gal}(E/K) \to \mathrm{Gal}(E'/K)$ such that $\phi T_{\mathfrak{p}}(E/K) = T_{\mathfrak{p}}(E'/K)$ for all primes $\mathfrak{p}$ of K.*

(2.7) COROLLARY. *Let E/K and E'/K be tame cyclic extensions of odd degree. If E/K and E'/K have the same degree and discriminant, then their trace forms $(O_E, t_{E/K})$ and $(O_{E'}, t_{E'/K})$ are in the same genus (in the sense of Definition* 1.2).

Proof. Let n be the common degree of E/K and E'/K. Let $\mathfrak{p}$ be a prime of K. Let e (respectively e') be the ramification index of $\mathfrak{p}$ in E/K (respectively in E'/K). By tameness (see [9, Chapter 3, Section 2, Proposition 8]) we have

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}_{E/K}) &= \mathrm{ord}_{\mathfrak{p}}(N_{E/K}(\mathfrak{D}_{E/K})) \\ &= (n/e)(e-1). \end{aligned}$$

By hypothesis $\mathfrak{d}_{E/K} = \mathfrak{d}_{E'/K}$, thus the equality above implies $e = e'$. Let $\phi\colon \mathrm{Gal}(E/K) \to \mathrm{Gal}(E'/K)$ be any isomorphism. Since $\mathrm{Gal}(E/K)$ is cyclic and $|T_{\mathfrak{p}}(E/K)| = e = e' = |T_{\mathfrak{p}}(E'/K)|$ we must have $\phi T_{\mathfrak{p}}(E/K) = T_{\mathfrak{p}}(E'/K)$. We conclude by applying Corollary 2.6. ∎

(2.8) *Remark.* P. E. Conner and R. Perlis proved in the case $K = \mathbb{Q}$ and the degree $[E:\mathbb{Q}]$ a prime number that $(O_E, t_{E/\mathbb{Q}})$ and $(O_{E'}, t_{E'/\mathbb{Q}})$ are in the same *class* (in the sense of Definition 1.2). See [4]. See also [1, Remarque 5.6].

Corollary 2.7 is no longer true if we do not assume that the Galois group is cyclic. Here is a counterexample:

(2.9) EXAMPLE. *Let l be an odd prime number. Then there exist two tame normal extensions $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ with* $\mathrm{Gal}(E/\mathbb{Q})$ *and* $\mathrm{Gal}(E'/\mathbb{Q})$ *both isomorphic to $C_l \times C_l$ and with the same discriminant such that $(O_E, t_{E/\mathbb{Q}})$ and $(O_{E'}, t_{E'/\mathbb{Q}})$ are not in the same genus (in the sense of Definition* 1.2).

Proof. Let p_i $(i=1, 2, 3)$ be distinct prime numbers such that $p_i \equiv 1 \pmod{l}$ (such primes exist by Dirichlet's Density Theorem). Let $\mathfrak{f} = p_1 p_2 p_3$ and $\Gamma = (\mathbb{Z}/\mathfrak{f}\mathbb{Z})^*$. Let L be the subfield of the cyclotomic field $\mathbb{Q}(\mathfrak{f})$ fixed by the subgroup Γ^l of l-powers of elements in Γ. By the construction of L we have $\mathrm{Gal}(L/\mathbb{Q}) = \Gamma/\Gamma^l \cong C_l \times C_l \times C_l$. One can easily check that the primes p_i $(i=1, 2, 3)$ are ramified in L and that $\mathrm{Gal}(L/\mathbb{Q})$ is the direct product of its three inertia subgroups $T_{p_i}(L/\mathbb{Q})$ $(i=1, 2, 3)$. Let $H \subset \mathrm{Gal}(L/\mathbb{Q})$ be a subgroup of order l and let $E = L^H$. It is easy to see that $\mathfrak{d}_{E/\mathbb{Q}} = (p_1 p_2 p_3)^{l(l-1)}$ (i.e., all three primes ramify) if and only if the canonical projection $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(E/\mathbb{Q})$ induces an isomorphism $T_{p_i}(L/\mathbb{Q}) \to T_{p_i}(E/\mathbb{Q})$ for $i=1, 2, 3$. The latter condition is equivalent to

$$T_{p_i}(L/\mathbb{Q}) \cap H = \{1\} \qquad \text{for} \quad i=1, 2, 3. \tag{1}$$

To continue the proof we need the following ad hoc lemma

(2.10) LEMMA. *Let H and H' be subgroups of* $\mathrm{Gal}(L/\mathbb{Q})$ *satisfying the condition* (1). *Let $E = L^H$ and $E' = L^{H'}$. The following conditions are equivalent*

(a) *There exists an automorphism Φ:* $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ *such that $\Phi(H) = H'$ and $\Phi T_{p_i}(L/\mathbb{Q}) = T_{p_i}(L/\mathbb{Q})$ for $i=1, 2, 3$.*

(b) *There exists an isomorphism ϕ:* $\mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{Gal}(E'/\mathbb{Q})$ *such that $\phi T_{p_i}(E/\mathbb{Q}) = T_{p_i}(E'/\mathbb{Q})$ for $i=1, 2, 3$.*

Proof. (a) $\Rightarrow$ (b) follows immediately from the remarks above. We shall prove (b) $\Rightarrow$ (a). Let ϕ: $\mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{Gal}(E'/\mathbb{Q})$ be such that $\phi T_{p_i}(E/\mathbb{Q}) = T_{p_i}(E'/\mathbb{Q})$ for $i=1, 2, 3$. Since H and H' satisfy condition (1), we can define Φ_i: $T_{p_i}(L/\mathbb{Q}) \to T_{p_i}(L/\mathbb{Q})$ as the unique isomorphism such that the diagram

$$\begin{array}{ccc} T_{p_i}(L/\mathbb{Q}) & \xrightarrow{\Phi_i} & T_{p_i}(L/\mathbb{Q}) \\ \downarrow & & \downarrow \\ T_{p_i}(E/\mathbb{Q}) & \xrightarrow[\phi]{} & T_{p_i}(E'/\mathbb{Q}) \end{array}$$

commutes. Since $\mathrm{Gal}(L/\mathbb{Q}) = \prod_{i=1}^{3} T_{p_i}(L/\mathbb{Q})$ we define $\Phi = \prod_{i=1}^{3} \Phi_i$. Clearly Φ has the required properties. ∎

End of the Proof of 2.9. For $i=1, 2, 3$ choose σ_i in $T_{p_i}(L/\mathbb{Q})$ to be different from the identity. Let H be the subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ generated by $h=\sigma_1\sigma_2\sigma_3$ and let H' be the subgroup generated by $h'=\sigma_1\sigma_2$. Clearly H and H' satisfy condition (1) and there is no Φ: $\mathrm{Gal}(L/\mathbb{Q})\to\mathrm{Gal}(L/\mathbb{Q})$ satisfying (a) of (2.10). By Lemma 2.10 there is no intertia-preserving isomorphism $\mathrm{Gal}(E/\mathbb{Q})\to\mathrm{Gal}(E'/\mathbb{Q})$ (where $E=L^H$ and $E'=L^{H'}$). Thus, by Corollary 2.6, the trace forms $(O_E, t_{E/\mathbb{Q}})$ and $(O_{E'}, t_{E'/\mathbb{Q}})$ are *not* in the same genus. Note however that $\mathfrak{d}_{E/\mathbb{Q}}=\mathfrak{d}_{E'/\mathbb{Q}}$ since H and H' satisfy the condition (1). ∎

3. The Class of the Trace Form

Let E/K be a tame abelian extension of odd degree and let $G=\mathrm{Gal}(E/K)$. In this section we study the *class* of $(O_E, t_{E/K})$ as a G-invariant form. We will define a full lattice $M_{E/K}$ in $O_K[G]$ such that $(M_{E/K}, t_G)$ is in the same genus as $(O_E, t_{E/K})$ and in many cases even represents the G-isometry class of $(O_E, t_{E/K})$. Let $\mathfrak{p}$ be a prime in K and let $\mathfrak{P}$ be a prime of E above $\mathfrak{p}$. Let Π in $\mathfrak{P}$ be a uniformizing parameter. For τ in $T_{\mathfrak{p}}$ we define $\theta_{\mathfrak{p}}(\tau)\equiv\tau(\Pi)/\Pi \pmod{\mathfrak{P}}$. It is well known that $\theta_{\mathfrak{p}}$ is a homomorphism $T_{\mathfrak{p}}\to(O_E/\mathfrak{P})^*$ independent of the choice of Π. The image of $\theta_{\mathfrak{p}}$ actually lies in the smaller field $k(\mathfrak{p})=O_K/\mathfrak{p}$. Moreover, in the tame situation this homomorphism is injective (see [10, Chapter IV, Section 2, Proposition 7]). The character $\theta_{\mathfrak{p}}$ can be lifted to a character $T_{\mathfrak{p}}\to O_{K_{\mathfrak{p}}}^*$ that we shall also denote by $\theta_{\mathfrak{p}}$. We define a family of idempotents $\{\varepsilon_{\mathfrak{p}}^{(i)}\}$ in the group ring $O_{K_{\mathfrak{p}}}[G]$ by $\varepsilon_{\mathfrak{p}}^{(i)}=(1/e)\sum_{\tau\in T_{\mathfrak{p}}}\theta_{\mathfrak{p}}^i(\tau^{-1})\tau$. Let $\varepsilon_{\mathfrak{p}}=\sum_{i=0}^{(e-1)/2}\varepsilon_{\mathfrak{p}}^{(i)}$. We define now the $O_K[G]$-module $M_{E/K}$ by setting

$$(M_{E/K})_{\mathfrak{p}}=\mathfrak{p}O_{K_{\mathfrak{p}}}[G]+\varepsilon_{\mathfrak{p}}O_{K_{\mathfrak{p}}}[G]$$

for all primes K. Note that for unramified $\mathfrak{p}$ we have $(M_{E/K})_{\mathfrak{p}}=O_{K_{\mathfrak{p}}}[G]$.

(3.1) Proposition. (a) *$M_{E/K}$ is locally free.*

(b) *$(M_{E/K}, t_G)$ and $(O_E, t_{E/K})$ are in the same equivariant genus.*

Proof. (a) Let π be a uniformizer in $K_{\mathfrak{p}}$. Let $\alpha=\pi+\varepsilon_{\mathfrak{p}}$. The identities

$$\pi=[\pi(1+\pi)^{-1}\varepsilon_{\mathfrak{p}}+(1-\varepsilon_{\mathfrak{p}})]\alpha$$

$$\varepsilon_{\mathfrak{p}}=(1+\pi)^{-1}\varepsilon_{\mathfrak{p}}\alpha$$

show that α generates $(M_{E/K})_{\mathfrak{p}}$ over $O_{K_{\mathfrak{p}}}[G]$.

(b) From (a) we have $(M_{E/K})_{\mathfrak{p}} = \alpha O_{K_{\mathfrak{p}}}[G]$. Thus

$$\begin{aligned}(M_{E/K})_{\mathfrak{p}}^{\xi}/(M_{E/K})_{\mathfrak{p}} &= \bar{\alpha}\ {}^{1}O_{K_{\mathfrak{p}}}[G]/\alpha O_{K_{\mathfrak{p}}}[G] \\ &\cong O_{K_{\mathfrak{p}}}[G]/\alpha\bar{\alpha}\ {}^{1}O_{K_{\mathfrak{p}}}[G] \\ &= O_{K_{\mathfrak{p}}}[G]/(M_{E/K}\overline{M_{E/K}})_{\mathfrak{p}}. \end{aligned} \tag{2}$$

We now calculate $(M_{E/K}\overline{M_{E/K}})_{\mathfrak{p}}$. Using the definition of $M_{E/K}$ we have

$$\begin{aligned}(M_{E/K}\overline{M_{E/K}})_{\mathfrak{p}} &= (\pi, \varepsilon_{\mathfrak{p}})(\pi, \overline{\varepsilon_{\mathfrak{p}}}) \\ &= (\pi^2, \pi\varepsilon_{\mathfrak{p}}, \pi\overline{\varepsilon_{\mathfrak{p}}}, \varepsilon_{\mathfrak{p}}\overline{\varepsilon_{\mathfrak{p}}}) \\ &= (\pi^2, \pi\varepsilon_{\mathfrak{p}}, \pi(1+\varepsilon_{\mathfrak{p}}^{(0)}), \varepsilon_{\mathfrak{p}}^{(0)}) \\ &= (\pi^2, \pi\varepsilon_{\mathfrak{p}}, \pi, \varepsilon_{\mathfrak{p}}^{(0)}) \\ &= (\pi, \varepsilon_{\mathfrak{p}}^{(0)}) \end{aligned} \tag{3}$$

(here we use the identities $\varepsilon_{\mathfrak{p}} + \overline{\varepsilon_{\mathfrak{p}}} = 1 + \varepsilon_{\mathfrak{p}}^{(0)}$ and $\varepsilon_{\mathfrak{p}}\overline{\varepsilon_{\mathfrak{p}}} = \varepsilon_{\mathfrak{p}}^{(0)}$). In the notation of Proposition 2.5, we have $\varepsilon_{\mathfrak{p}}^{(0)} = (1/e)\sigma_{\mathfrak{p}}$. Thus, by combining (2), (3), and Proposition 2.5, we have

$$\begin{aligned}(M_{E/K})_{\mathfrak{p}}^{\xi}/(M_{E/K})_{\mathfrak{p}} &\cong O_{K_{\mathfrak{p}}}[G]/(\pi, \sigma_{\mathfrak{p}}) \\ &= k(\mathfrak{p})[G]/(\sigma_{\mathfrak{p}}) \\ &\cong (\mathfrak{D}_{E/K}^{-1}/O_E)_{\mathfrak{p}}. \end{aligned} \tag{4}$$

We conclude by applying Theorem 2.3. ∎

By Hilbert's formula for the order of the different at a given prime in terms of the ramification groups (see [10, Chapter IV, Section 2, Proposition 4]) it is clear that the different $\mathfrak{D}_{E/K}$ of an odd degree Galois extension is the square of an ideal. We set $A_{E/K} = \mathfrak{D}_{E/K}^{-1/2}$. It is readily checked that $A_{E/K}$ is a self-dual lattice with respect to the trace form. Moreover, in the tame case, $A_{E/K}$ is locally free as a Galois module (see [12]). The following proposition relates $A_{E/K}$ to $M_{E/K}$.

(3.2) PROPOSITION. $M_{E/K}A_{E/K} = O_E$.

Proof. Let $\mathfrak{p}$ be a prime in K and $\mathfrak{P}$ a prime of E above $\mathfrak{p}$. Let $\Pi \in \mathfrak{P}$ be a uniformizing parameter. Let $0 \leqslant i \leqslant (e-1)/2$ and $1 \leqslant j \leqslant (e-1)/2$. We shall show

$$\varepsilon_{\mathfrak{p}}^{(i)}\mathfrak{P}^{-j} \subset \mathfrak{P}^{-j+1}.$$

Indeed the module $\mathfrak{P}^{-j}/\mathfrak{P}^{-j+1}$ has dimension one over $O_E/\mathfrak{P}$ and has Π^{-j} as a basis. For τ in T_p we have $\tau(\Pi^{-j}) \equiv \theta^j(\tau^{-1})\,\Pi^{-j} \pmod{\mathfrak{P}^{-j+1}}$. Thus

$$\varepsilon_{\mathfrak{p}}^{(i)}(\Pi^{-j}) \equiv (1/e)\left(\sum_{\tau \in T_{\mathfrak{p}}} \theta^{i+j}(\tau^{-1})\right)\Pi^{-j} \pmod{\mathfrak{P}^{-j+1}}.$$

On the other hand, since θ is injective and $1 \leqslant i+j \leqslant e-1$, the homomorphism $\theta^{i+j}\colon T_{\mathfrak{p}} \to O_{K_{\mathfrak{p}}}^{*}$ is not trivial. Thus $\sum_{\tau \in T_{\mathfrak{p}}} \theta^{i+j}(\tau^{-1}) = 0$. Consequently, since $T_{\mathfrak{p}}$ acts $(O_E/\mathfrak{P})$-linearly on $\mathfrak{P}^{-j}/\mathfrak{P}^{-j+1}$, we have $\varepsilon_{\mathfrak{p}}^{(i)}[\mathfrak{P}^{-j}/\mathfrak{P}^{-j+1}] = 0$. Since $\varepsilon_{\mathfrak{p}}^{(i)}$ is an idempotent element, applying j times $\varepsilon_{\mathfrak{p}}^{(i)}$ to $\mathfrak{P}^{-j}$ yields $\varepsilon_{\mathfrak{p}}^{(i)}\mathfrak{P}^{-j} \subset O_{E_{\mathfrak{P}}}$. In particular $\varepsilon_{\mathfrak{p}}^{(i)}\mathfrak{P}^{-(e-1)/2} \subset O_{E_{\mathfrak{P}}}$. Thus $\varepsilon_{\mathfrak{p}}(A_{E/K})_{\mathfrak{p}} \subset (O_E)_{\mathfrak{p}}$. This shows $M_{E/K}A_{E/K} \subset O_E$. To finish the proof, we will show that $M_{E/K}A_{E/K}$ and O_E have both the same index in $A_{E/K}$. On the one hand, since $A_{E/K}$ is locally free, we have

$$\dim_{k(\mathfrak{p})}(A_{E/K}/M_{E/K}A_{E/K})_{\mathfrak{p}} = \dim_{k(\mathfrak{p})}(O_K[G]/M_{E/K})_{\mathfrak{p}}.$$

On the other hand, using (4) we have

$$\begin{aligned}\dim_{k(\mathfrak{p})}(O_K[G]/M_{E/K})_{\mathfrak{p}} &= \tfrac{1}{2}\dim_{k(\mathfrak{p})}((M_{E/K}^{\sharp}/M_{E/K})_{\mathfrak{p}}) \\ &= \tfrac{1}{2}\dim_{k(\mathfrak{p})}(\mathfrak{D}_{E/K}^{-1}/O_E)_{\mathfrak{p}} \\ &= \dim_{k(\mathfrak{p})}(A_{E/K}/O_E)_{\mathfrak{p}}. \quad \blacksquare\end{aligned}$$

(3.3) THEOREM. *The following conditions are equivalent*

(a) $(O_E, t_{E/K})$ *is G-isometric to* $(M_{E/K}, t_G)$.

(b) $(A_{E/K}, t_{E/K})$ *is G-isometric to* $(O_K[G], t_G)$.

Proof. (a) $\Rightarrow$ (b). Let $\phi\colon O_E \to M_{E/K}$ be a G-isometry. We extend ϕ to an isometry $E \to K[G]$. Using Proposition 3.2 we have

$$\begin{aligned}M_{E/K} &= \phi(O_E) \\ &= \phi(M_{E/K}A_{E/K}) \\ &= M_{E/K}\phi(A_{E/K}).\end{aligned}$$

Now, by Proposition 3.1, the module $M_{E/K}$ is locally free, and therefore is invertible as an $O_K[G]$-ideal in $K[G]$. Thus we must have $\phi(A_{E/K}) = O_K[G]$.

(b) $\Rightarrow$ (a). Let $\psi\colon O_K[G] \to A_{E/K}$ be an isometry. Using again Proposition 3.2 we have

$$\begin{aligned}\psi(M_{E/K}) &= M_{E/K}\psi(O_K[G]) \\ &= M_{E/K}A_{E/K} \\ &= O_E. \quad \blacksquare\end{aligned}$$

4. The Absolute Case

In this section we prove that condition (b) of Theorem 3.3 is fulfilled for absolute extensions. We actually give a more general result which characterizes absolute abelian extensions such that the square root of the inverse different has a self-dual normal basis.

(4.1) Theorem. *Let $E/\mathbb{Q}$ be an abelian extension of odd degree and let $G = \mathrm{Gal}(E/\mathbb{Q})$. The following conditions are equivalent*

(a) *There exists a G-isometry between $(A_{E/\mathbb{Q}}, t_{E/\mathbb{Q}})$ and $(\mathbb{Z}[G], t_G)$.*

(b) *$A_{E/\mathbb{Q}}$ is free over $\mathbb{Z}[G]$.*

(c) *For all primes p the second ramification subgroups $G_2(p, E/\mathbb{Q})$ are reduced to the identity.*

Proof. (a) clearly implies (b) and (b) implies (c) by the work of Ullom [12, 2.1]. So, there remains to prove that (c) implies (a). The next two lemmas show that it is sufficient to consider two types of extensions:

Type I. Odd degree extensions $E/\mathbb{Q}$ of odd prime conductor.

Type II. Extensions of odd prime degree p and conductor p^2.

These two types of extensions had already been dealt with in [6] (observe that the argument given there under 2.2 extends to cover all Type I extensions).

(4.2) Lemma. *The field E is contained in the compositum L of absolute abelian fields $E^{(p)}/\mathbb{Q}$ such that*

(i) *$E^{(p)}/\mathbb{Q}$ is ramified only at p and totally ramified there.*

(ii) *The degree $[E^{(p)} : \mathbb{Q}]$ equals the ramification index of p in $E/\mathbb{Q}$.*

Proof. Let $\mathfrak{f}$ be the conductor of $E/\mathbb{Q}$. For a prime p we write $\mathfrak{f} = p^z m$ with p not dividing m. Then $E^{(p)}$ is nothing but the subfield of $\mathbb{Q}(p^z)$ corresponding to the group X_p of the p-components of Dirichlet characters attached to $E/\mathbb{Q}$. For more details see [13, Theorem 3.5]. ∎

(4.3) Lemma. (i) *Let $K \subset E \subset L$ be a tower of odd degree abelian extensions and let $G = \mathrm{Gal}(L/K)$, and $H = \mathrm{Gal}(L/E)$. If $(A_{L/K}, t_{L/K})$ is G-isometric to $(O_K[G], t_G)$ then $\mathrm{Tr}_{L/E}(A_{L/K}) = A_{E/K}$ and $(A_{E/K}, t_{E/K})$ is (G/H)-isometric to $(O_K[G/H], t_{G/H})$.*

(ii) *Let $K/\mathbb{Q}$ and $F/\mathbb{Q}$ be two odd degree Galois extensions whose discriminants are relatively prime and let $L = KF$. Then*

$$(A_{L/\mathbb{Q}}, t_{L/\mathbb{Q}}) = (A_{K/\mathbb{Q}} \otimes_{\mathbb{Z}} A_{F/\mathbb{Q}}, t_{K/\mathbb{Q}} \otimes t_{F/\mathbb{Q}}).$$

Proof. (i) Choose a self-dual normal generator x of $A_{L/K}$ over $O_K[G]$, and let $y = \mathrm{Tr}_{L/E}(x)$. Then y is a self-dual normal generator of $A_{E/K}$ over $O_K[G/H]$. Indeed, y is a normal generator and

$$\begin{aligned}\mathrm{Tr}_{E/K}(y^2) &= \mathrm{Tr}_{E/K}(\mathrm{Tr}_{L/E}(x)\, y)\\ &= \mathrm{Tr}_{L/K}(xy)\\ &= \mathrm{Tr}_{L/K}(x\, \mathrm{Tr}_{L/E}(x))\\ &= \sum_{\sigma \in H} \mathrm{Tr}_{L/K}(x\sigma(x))\\ &= 1.\end{aligned}$$

(ii) By the assumption on the discriminants, $O_K \otimes_{\mathbb{Z}} O_F = O_L$ (see [9, Chapter 3, Section 3, Proposition 17]). Since $A_{L/\mathbb{Q}}$ is the unique O_L-ideal self-dual with respect to the trace form $t_{L/\mathbb{Q}}$, we must have $A_{L/\mathbb{Q}} = A_{K/\mathbb{Q}} \otimes_{\mathbb{Z}} A_{F/\mathbb{Q}}$. ∎

Proof of (c) ⇒ (a). The condition (c) implies that the fields $E^{(p)}$ of Lemma 4.2 are actually of Type I and Type II. As already mentioned at the beginning of the proof, condition (a) holds for these fields, so by part (ii) of Lemma 4.3, we see that (a) holds for L. We conclude by taking the trace from L down to E and using part (i) of Lemma 4.3. ∎

As an immediate consequence of Theorems 3.3 and 4.1 we have:

(4.4) COROLLARY. *Let $E/\mathbb{Q}$ be an abelian tame extension of odd degree. Let $G = \mathrm{Gal}(E/\mathbb{Q})$. Then $(O_E, t_{E/\mathbb{Q}})$ is G-isometric to $(M_{E/\mathbb{Q}}, t_G)$.*

ACKNOWLEDGMENT

The authors are grateful to the referee for his/her helpful observations.

REFERENCES

1. C. BACHOC AND B. EREZ, Forme trace et ramification sauvage, *Proc. London Math. Soc. (3)* **61** (1990), 209–226.
2. E. BAYER AND H. W. LENSTRA, Forms in odd degree extensions and self-dual normal bases, *Amer. J. Math.* **112** (1990), 359–373.
3. S. CHASE, Ramification invariants and torsion Galois module structure in number fields, *J. Algebra* **91** (1984), 207–257.
4. P. E. CONNER AND R. PERLIS, "A Survey of Trace Forms of Algebraic Number Fields," World Scientific, Singapore, 1984.
5. C. CURTIS AND I. REINER, "Methods of Representation Theory," Wiley, New York, 1981.

6. B. EREZ, The Galois structure of the trace form in extensions of odd prime degree, *J. Algebra* **118** (2) (1988), 438–446.
7. B. EREZ AND M. J. TAYLOR, Hermitian modules in Galois extensions of number fields and Adams operations, *Annals of Math.*, to appear.
8. A. FRÖHLICH, Galois module structure of algebraic integers, *in* "Ergebnisse (3)," Vol 1, Springer-Verlag, Berlin, 1983.
9. S. LANG, "Algebraic Number Theory," Addison–Wesley, Reading, MA, 1970.
10. J.-P. SERRE, Local fields, *in* "Graduate Texts in Mathematics," Vol. 67, Springer-Verlag, Berlin/New York, 1972.
11. M. J. TAYLOR, Rings of integers and trace forms for tame extensions of odd degree, *Math. Z.* **202** (1989), 313–341.
12. S. ULLOM, Normal bases in Galois extensions of number fields, *Nagoya Math. J.* **34** (1969), 153–167.
13. L. C. WASHINGTON, Introduction to cyclotomic fields, *in* "Graduate Texts in Mathematics," Vol. 83, Springer-Verlag, Berlin/New York, 1982.