HERMITIAN CLASS NUMBERS IN GROUP RINGS

JORGE MORALES

Introduction

Let G be a finite group and let K be a number field. Let $u \mapsto \bar{u}$ denote the canonical involution on the group ring $K[G]$ (that is, the involution induced by inversion of the elements in G). Two left $O_K[G]$-ideals L and M in $K[G]$ are said to be *isometric* if there exists u in $K[G]$ satisfying $u\bar{u} = 1$ and such that $Lu = M$. The ideals L and M are said to be *in the same genus* if for each prime $\mathfrak{p}$ of K there exists $u_{\mathfrak{p}} \in K_{\mathfrak{p}}[G]$ satisfying $u_{\mathfrak{p}}\bar{u}_{\mathfrak{p}} = 1$ and such that $L_{\mathfrak{p}}u_{\mathfrak{p}} = M_{\mathfrak{p}}$. The number of distinct isometry classes in the genus of L is called *the hermitian class number* of L and will be denoted by $h(L)$. It is well known that this number is finite (see, for instance, [7]). The main result in this paper is an analytic formula for $h(L)$ in the case where K is totally real, G is abelian of odd order, and L is locally free (Theorem 1.16).

It is worthwhile to mention that the results in this paper can be applied to compute the equivariant class number of the trace form restricted to the integers in an abelian tame extension of odd degree E/K, assuming that K is a totally real field. Indeed, let G be the Galois group of E/K. Using the existence of a normal basis of E over K which is self-dual with respect to the trace form (see [**1**, **2**]), we see that the ring of integers of E is equivariantly isometric to an $O_K[G]$-lattice in $K[G]$. Furthermore, this lattice is locally free by tameness (see also [**4**]).

Except for the results on Tamagawa numbers, which will be used without proof, this paper is self-contained. The reader interested in the general theory of Tamagawa numbers should refer to Weil [**12**] and Ono [**8**, **9**].

1. *The class number formula*

The following notation will be used throughout this paper.

G	a finite abelian group of odd order
K	a number field
O_K	the ring of integers of K
$\mathfrak{p}$	a prime ideal of K
v	a place of K
$k(\mathfrak{p})$	the residue field $O_K/\mathfrak{p}$
K_v	the v-adic completion of K
O_{K_v}	the ring of integers of K_v (by definition $O_{K_v} = K_v$ if v is an archimedean place)
$k[G]$	the group ring over k (where k is any commutative ring)

Received 18 September 1989.

1980 *Mathematics Subject Classification* 10C07, 10C30, 12A80.

Research supported by a grant from Louisiana State University Council on Research.

Bull. London Math. Soc. 22 (1990) 321–332

$R(G)$ the representation group of G over an algebraically closed field of characteristic 0 (that is, the free abelian group on the set of absolutely irreducible characters of G)

$R_F(G)$ the subgroup of $R(G)$ generated by the F-rational characters (F a field of characteristic 0)

$W_G(k)$ the group $\{x \in k[G] : x\bar{x} = 1\}$

$U_G(k)$ the group $\{x \in k[G] : x\bar{x} = 1 \text{ and } \varepsilon(x) = 1\}$, where ε is the augmentation map

For any abelian group M equipped with an involution $x \mapsto x^*$ we denote by M^+ the subgroup $\{x \in M : x^* = x\}$ and by M^- the subgroup $\{x \in M : x^* = -x\}$. This notation will be applied in particular to the ring $k[G]$ (equipped with the involution induced by group inversion) and to the representation ring $R(G)$ equipped with the involution defined by $\alpha^*(g) = \alpha(g^{-1})$ for a virtual character α in $R(G)$.

Note that $W_G(k)$ is the automorphism group of the standard hermitian form $\mu_G(x, y) = x\bar{y}$ on the group ring $k[G]$. Regarded as a group scheme U_G is the connected component of the identity in W_G (see [11] for the definitions).

PROPOSITION 1.1. *Let L be an $O_K[G]$-lattice in the group ring $K[G]$. Then*
(a) *if L is locally free then the stability subgroup $U_G(K)_L$ is equal to $U_G(O_K)$,*
(b) *if the field K is totally real then $U_G(O_K) = G$.*

Proof. (a) If L is locally free then $L_\mathfrak{p}$ is free for all primes $\mathfrak{p}$ of K and therefore $\mathrm{End}_G(L_\mathfrak{p}) = O_{K_\mathfrak{p}}[G]$. Hence $\mathrm{End}_G(L) = O_K[G]$. The assertion (a) follows easily now from this fact.

(b) Let $u = \sum_g u_g g \in O_K[G]$ be such that $u\bar{u} = 1$. In particular we must have $\sum_g u_g^2 = 1$. In a totally real field, the latter relation implies that there is exactly one $g \in G$ such that u_g is equal to ± 1 and the others are zero. Thus $u = \pm g$ for some $g \in G$. If, in addition, $\varepsilon(u) = 1$ then $u = g$.

Let $\mathbb{A}_K$ be the adèle ring of K and let $\mathbb{A}_K^\infty$ be the product $\prod_v O_{K_v}$, where v runs over all places of K. With this notation we have the following.

PROPOSITION 1.2. *Let $L \subset K[G]$ be a locally free $O_K[G]$-lattice. Then the group $U_G(\mathbb{A}_K)/U_G(\mathbb{A}_K^\infty)\, U_G(K)$ acts freely and transitively on the set of classes in the genus of L.*

Proof. Observe that if u satisfies $u\bar{u} = 1$ then $\varepsilon(u) = \pm 1$ and $\varepsilon(u)\, u$ is in $U_G(K)$. Hence the classes with respect to the entire automorphism group are the same as the classes with respect to the smaller group $U_G(K)$. So $U_G(\mathbb{A}_K)$ acts transitively on the set of classes in a fixed genus. The obvious local version of part (a) of Proposition 1.1 implies that the stability subgroup of the class of L is $U_G(\mathbb{A}_K^\infty)\, U_G(K)$.

COROLLARY 1.3. *For any locally free $O_K[G]$-lattice L in $K[G]$ we have $h(L) = h(O_K[G])$.*

REMARK 1.4. The group $U_G(\mathbb{A}_K)/U_G(\mathbb{A}_K^\infty)\, U_G(K)$ can also be regarded as an 'ideal class group' in the following way. Let $\mathscr{I}^1(O_K[G])$ be the group of $O_K[G]$-ideals $\mathfrak{a}$ in $K[G]$ satisfying $\mathfrak{a}\bar{\mathfrak{a}} = O_K[G]$. Let $\mathscr{P}^1(O_K[G])$ be the subgroup of $\mathscr{I}^1(O_K[G])$ of principal ideals $aO_K[G]$ with $a\bar{a} = 1$. Then $U_G(\mathbb{A}_K)/U_G(\mathbb{A}_K^\infty)\, U_G(K)$ is canonically isomorphic to the quotient $\mathscr{I}^1(O_K[G])/\mathscr{P}^1(O_K[G])$.

Henceforth we shall assume that K is totally real. Note in particular that under this hypothesis $U_G(K_v)$ is a compact group for the archimedean places v of K; thus $U_G(\mathbb{A}_K^\infty)$ is compact as well.

COROLLARY 1.5. *Let h be the hermitian class number of $O_K[G]$ and let μ be any Haar measure on $U_G(\mathbb{A}_K)$. Then*

$$h = |G| \frac{\mu(U_G(\mathbb{A}_K)/U_G(K))}{\mu(U_G(\mathbb{A}_K^\infty))}. \tag{1}$$

Proof. By Proposition 1.1(b) we have $U_G(\mathbb{A}_K^\infty) \cap U_G(K) = G$. Corollary 1.5 follows now from Proposition 1.2 and the exact sequence

$$0 \longrightarrow U_G(\mathbb{A}_K^\infty)/G \longrightarrow U_G(\mathbb{A}_K)/U_G(K) \longrightarrow U_G(\mathbb{A}_K)/U_G(\mathbb{A}_K^\infty)\, U_G(K) \longrightarrow 0.$$

Our goal is now to evaluate h using (1) and choosing for μ the canonical Tamagawa measure. We recall here its definition. Let ω be a non-zero alternating m-form on $K[G]^-$, where $m = \dim_K(K[G]^-) = \frac{1}{2}(|G|-1)$. The form ω can be extended to an invariant differential m-form on the group $U_G(K_v)$ for all places v of K (note that $K_v[G]^-$ is the Lie algebra of $U_G(K_v)$). The invariant measure induced by ω on $U_G(K_v)$ will be denoted by $|\omega|_v$. The Tamagawa measure μ on $U_G(\mathbb{A}_K)$ is defined by

$$\mu = \prod_v |\omega|_v \tag{2}$$

where v runs over all places of K. This product should be understood as follows: the Tamagawa measure μ is the unique invariant measure on $U_G(\mathbb{A}_K)$ such that the volume of the compact open subgroup $U_G(\mathbb{A}_K^\infty)$ is given by

$$\mu(U_G(\mathbb{A}_K^\infty)) = \prod_v \int_{U_G(O_{K_v})} |\omega|_v. \tag{3}$$

(We recall the convention $O_{K_v} = K_v$ if v is an archimedean place.) It will become apparent *a posteriori* that this product is conditionally convergent. Thus in our particular case there is no need to introduce Ono's 'canonical correcting factors' (see [8]). It is clear from the product formula that μ does not depend on the particular choice of the form ω. We recall that the Tamagawa number of U_G is, by definition,

$$\tau(U_G) = \mu(U_G(\mathbb{A}_K)/U_G(K)) \tag{4}$$

(see [12]).

The local measures $|\omega|_v$ do depend on the choice of ω. In order to simplify the local computations we normalize ω in the following way: let $G = \{1, g_1, g_1^{-1}, \ldots, g_m, g_m^{-1}\}$ and let $u_i = g_i - g_i^{-1}$ for $i = 1, \ldots, m$. We define ω as the unique alternating m-form on $K[G]^-$ such that

$$\omega(u_1, u_2, \ldots, u_m) = 1. \tag{5}$$

With this agreement in mind, we define the *local density* of U_G at v by

$$\delta_v(U_G) = \int_{U_G(O_{K_v})} |\omega|_v. \tag{6}$$

To calculate $\delta_p(U_G)$ at a finite prime $\mathfrak{p}$ we need the following lemma.

LEMMA 1.6. *For $v \geqslant 2\,\mathrm{ord}_{\mathfrak{p}}(2)+1$ we have*

$$[W_G(O_K/\mathfrak{p}^v): U_G(O_K/\mathfrak{p}^v)] = 2|2|_{\mathfrak{p}}^{-1}.$$

Proof. There is an exact sequence

$$0 \longrightarrow U_G(O_K/\mathfrak{p}^v) \longrightarrow W_G(O_K/\mathfrak{p}^v) \xrightarrow{\varepsilon} \mu_2(O_K/\mathfrak{p}^v) \longrightarrow 0$$

where $\mu_2(O_K/\mathfrak{p}^v) = \{x \in O_K/\mathfrak{p}^v : x^2 = 1\}$ and ε is the augmentation map. Hence $[W_G(O_K/\mathfrak{p}^v): U_G(O_K/\mathfrak{p}^v)] = |\mu_2(O_K/\mathfrak{p}^v)|$. On the one hand, from the exact sequence

$$0 \longrightarrow \mu_2(O_K/\mathfrak{p}^v) \longrightarrow (O_K/\mathfrak{p}^v)^* \xrightarrow{2} (O_K/\mathfrak{p}^v)^* \longrightarrow (O_K/\mathfrak{p}^v)^*/(O_K/\mathfrak{p}^v)^{*2} \longrightarrow 0,$$

we obtain

$$|\mu_2(O_K/\mathfrak{p}^v)| = [(O_K/\mathfrak{p}^v)^* : (O_K/\mathfrak{p}^v)^{*2}].$$

On the other hand, by Hensel's Lemma, the reduction mod $\mathfrak{p}^v$ induces an isomorphism $O_{K_{\mathfrak{p}}}^*/O_{K_{\mathfrak{p}}}^{*2} \to (O_K/\mathfrak{p}^v)^*/(O_K/\mathfrak{p}^v)^{*2}$ for $v \geqslant 2\,\mathrm{ord}_{\mathfrak{p}}(2)+1$. We conclude the proof by using the equality $[O_{K_{\mathfrak{p}}}^* : O_{K_{\mathfrak{p}}}^{*2}] = 2|2|_{\mathfrak{p}}^{-1}$ (see, for instance, [**6**, Chapter II, §4]).

PROPOSITION 1.7. *For a finite prime $\mathfrak{p}$ the following equality holds:*

$$\delta_{\mathfrak{p}}(U_G) = |U_G(k(\mathfrak{p}))|\, q^{-m} \tag{7}$$

where $q = \mathbf{N}(\mathfrak{p})$ and $m = \dim U_G = (|G|-1)/2$.

Proof. Let λ and μ be alternating forms of maximum degree on $O_K[G]$ and $O_K[G]^+$ respectively, which take the value 1 on an O_K-basis. Let $\phi: O_K[G] \to O_K[G]^+$ be the map defined by $\phi(x) = x + \bar{x}$. An easy calculation shows $\omega \wedge \phi^*(\mu) = (\text{unit})\,2\lambda$ (recall that ω is chosen as in (5)). Let $\Phi: O_{K_{\mathfrak{p}}}[G] \to O_{K_{\mathfrak{p}}}[G]^+$ be the algebraic map $\Phi(x) = \bar{x}x$. Note that $d\Phi|_1 = \phi$. Since $\Phi^{-1}(1) = W_G(O_{K_{\mathfrak{p}}})$, we obtain

$$\int_{W_G(O_{K_{\mathfrak{p}}})} |\omega|_{\mathfrak{p}} = |2|_{\mathfrak{p}} \lim_{v\to\infty} \frac{\left(\int_{\Phi^{-1}(S_v)} |\lambda|_{\mathfrak{p}}\right)}{\left(\int_{S_v} |\mu|_{\mathfrak{p}}\right)}$$

where $S_v = 1 + \mathfrak{p}^v O_{K_{\mathfrak{p}}}[G]^+$. Since $\Phi^{-1}(S_v)$ is the union of t classes modulo $\mathfrak{p}^v O_{K_{\mathfrak{p}}}[G]$, where $t = |W_G(O_K/\mathfrak{p}^v)|$, we have

$$\int_{\Phi^{-1}(S_v)} |\lambda|_{\mathfrak{p}} = |W_G(O_K/\mathfrak{p}^v)|\, q^{-v(2m+1)}.$$

On the other hand, by Lemma 1.6, we have $|W_G(O_K/\mathfrak{p}^v)| = 2|2|_{\mathfrak{p}}^{-1}|U_G(O_K/\mathfrak{p}^v)|$ for $v \geqslant 2\,\mathrm{ord}_{\mathfrak{p}}(2)+1$. Hence

$$\begin{aligned} \int_{U_G(O_{K_{\mathfrak{p}}})} |\omega|_{\mathfrak{p}} = \frac{1}{2}\int_{W_G(O_{K_{\mathfrak{p}}})} |\omega|_{\mathfrak{p}} &= \frac{1}{2}|2|_{\mathfrak{p}} \lim_{v\to\infty} \frac{|W_G(O_{K_{\mathfrak{p}}}/\mathfrak{p}^v)|}{q^{mv}} \\ &= \lim_{v\to\infty} \frac{|U_G(O_{K_{\mathfrak{p}}}/\mathfrak{p}^v)|}{q^{mv}}. \end{aligned} \tag{8}$$

The next step consists in showing that $|U_G(O_{K_\mathfrak{p}}/\mathfrak{p}^\nu)|\,q^{-m\nu}$ is independent of ν. Let $i: k(\mathfrak{p})[G]^- \to U_G(O_K/\mathfrak{p}^{\nu+1})$ be the map defined by $i(x) = 1+\pi^\nu x$, where π is a uniformizing parameter for $\mathfrak{p}$. Let $j: U_G(O_K/\mathfrak{p}^{\nu+1}) \to U_G(O_K/\mathfrak{p}^\nu)$ be the canonical reduction. We shall see that the sequence

$$0 \longrightarrow k(\mathfrak{p})[G]^- \xrightarrow{\ i\ } U_G(O_K/\mathfrak{p}^{\nu+1}) \xrightarrow{\ j\ } U_G(O_K/\mathfrak{p}^\nu) \longrightarrow 0 \tag{9}$$

is exact. Indeed, one sees easily that $1+\pi^\nu x$ belongs to $U_G(O_K/\mathfrak{p}^{\nu+1})$ if and only if $x+\bar{x} \equiv 0 (\mathrm{mod}\,\mathfrak{p})$. Hence $\mathrm{Im}\,(i) = \mathrm{Ker}\,(j)$. Let $y \in O_K[G]$ be such that $y\bar{y} \equiv 1 (\mathrm{mod}\,\mathfrak{p}^\nu)$ and $\varepsilon(y) \equiv 1 (\mathrm{mod}\,\mathfrak{p}^\nu)$. Let $z = (1-y\bar{y})\pi^{-\nu}$ and $a = (1-\varepsilon(y))\pi^{-1}$. We check readily that $\varepsilon(z) \equiv 2a (\mathrm{mod}\,\mathfrak{p}^\nu)$. Thus there exists $w \in O_K[G]$ such that $z \equiv w+\bar{w} (\mathrm{mod}\,\mathfrak{p}^\nu)$. Set $x = y+\pi^\nu w\bar{y}^{-1}$ in the localization $O_{K_\mathfrak{p}}[G]$. A direct calculation shows that $x\bar{x} \equiv 1 (\mathrm{mod}\,\mathfrak{p}^{\nu+1})$. By the construction of x we have $j(x) = y$. Therefore j is surjective. From the exact sequence (9) we have

$$|U_G(O_K/\mathfrak{p}^{\nu+1})|\,q^{-(\nu+1)m} = |U_G(O_K/\mathfrak{p}^\nu)|\,q^{-\nu m} = \ldots = |U_G(k(\mathfrak{p}))|\,q^{-m}.$$

Putting this together with (8) proves the proposition.

We shall now show that $\delta_\mathfrak{p}(U_G)$ depends only on the subgroup of G of elements of order relatively prime to $\mathfrak{p}$. Let p be the characteristic of $k(\mathfrak{p})$ and let G_p be the Sylow p-subgroup of G.

PROPOSITION 1.8. *With the notation above, we have*

$$\delta_\mathfrak{p}(U_G) = \delta_\mathfrak{p}(U_{G/G_p}).$$

Proof. Since $|G|$ is odd we can assume that p is different from 2. Let $k = k(\mathfrak{p})$ and let $\mathfrak{r}$ be the radical of $k[G]$. The exact sequence

$$1 \longrightarrow M \longrightarrow k[G]^* \longrightarrow k[G/G_p]^* \longrightarrow 1 \tag{10}$$

induces an exact sequence

$$1 \longrightarrow M^- \longrightarrow U_G(k) \longrightarrow U_{G/G_p}(k) \longrightarrow 1 \tag{11}$$

where $M^- = \{u \in M : u\bar{u} = 1\}$ (use $p \neq 2$ for the surjectivity of $U_G(k) \to U_{G/G_p}(k)$). Clearly the map $\mathfrak{r} \to M$ given by $x \mapsto 1+x$ is a bijection that preserves the involution. Thus $|M| = |\mathfrak{r}|$ and $|M^+| = |\mathfrak{r}^+|$ (we recall that the superscript $+$ denotes the points fixed by the involution). Let H be the subgroup of G of elements of order relatively prime to p. It is easy to see that the set $B = \{(g-1)h : g \in G_p \backslash \{1\} \text{ and } h \in H\}$ is a basis of $\mathfrak{r}$ over k and that the canonical involution acting on B has no fixed points. Thus

$$\dim_k(\mathfrak{r}^+) = \dim_k(\mathfrak{r}^-) = \tfrac{1}{2}\dim_k(\mathfrak{r}). \tag{12}$$

On the other hand, since p is odd, the group M is the direct product of M^+ and M^-. Using this fact together with (12) we have

$$\begin{aligned} |M^-| &= |M|\,|M^+|^{-1} \\ &= |\mathfrak{r}|\,|\mathfrak{r}^+|^{-1} \\ &= |\mathfrak{r}|^{1/2} \\ &= q^{(a-b)/2} \end{aligned}$$

where $q = |k|$, $a = |G|$ and $b = |G_p|$. Using (11) we obtain

$$|U_G(k)|\,q^{-(a-1)/2} = |U_{G/G_p}(k)|\,q^{-(b-1)/2}.$$

We finish the proof by applying Proposition 1.7.

The following lemma shows how to calculate the number of rational points of an algebraic torus over a finite field.

LEMMA 1.9. *Let V be an algebraic torus over the finite field k and let X be the module of algebraic characters of V, written additively. Let σ be the Frobenius automorphism in $\Omega = \mathrm{Gal}(\bar{k}/k)$ and A the matrix of σ acting on X. Then*

$$|V(k)| = |\det(qI - A)|$$

where $q = |k|$.

Proof. Using the natural Ω-isomorphism (see [9, Section 1.1])

$$V(\bar{k}) = \mathrm{Hom}(X, \bar{k}^*)$$

and taking the points fixed by Ω, we obtain

$$V(k) = \mathrm{Hom}_{\Omega}(X, \bar{k}^*) = \mathrm{Hom}(X/(q-\sigma)X, \bar{k}^*).$$

The module $X/(q-\sigma)X$ is finite and its order is relatively prime to q. Thus $|\mathrm{Hom}(X/(q-\sigma)X, \bar{k}^*)| = |X/(q-\sigma)X| = |\det(qI - A)|$.

In order to apply the lemma above to the computation of the local densities, we need to understand the Galois structure of the module of algebraic characters of $U_G(\bar{K})$. We recall that $R(G)$ denotes the representation ring of G. The subgroup of $R(G)$ of elements fixed by the canonical involution $\alpha \mapsto \alpha^*$ is denoted by $R^+(G)$. Similarly, the subgroup of $R(G)$ of elements α satisfying $\alpha^* = -\alpha$ is denoted by $R^-(G)$. Let $\bar{K}$ be the algebraic closure of K and let $\Omega = \mathrm{Gal}(\bar{K}/K)$. We shall regard $R^-(G)$ as an Ω-module, the group Ω acting naturally on $R^-(G)$ by conjugation of characters. The following proposition relates $R^-(G)$ to the algebraic group $U_G(\bar{K})$.

PROPOSITION 1.10. *The group $U_G(\bar{K})$ is an algebraic torus and its character group is isomorphic to $R^-(G)$ as an Ω-module.*

Proof. We first observe that there is an exact sequence of Ω-modules

$$0 \longrightarrow R^+(G) \longrightarrow R(G) \xrightarrow{\phi} R^-(G) \longrightarrow 0$$

where $\phi(\alpha) = \alpha - \alpha^*$. Thus $R^-(G)$ is isomorphic to $R(G)/R^+(G)$. For an irreducible character $\chi \in \hat{G}$ we denote by e_χ the corresponding indecomposable idempotent of the algebra $\bar{K}[G]$. Consider the map

$$\begin{aligned} \mathrm{Hom}(R(G)/R^+(G), \bar{K}^*) &\longrightarrow U_G(\bar{K}) \\ f &\longmapsto \sum_{\chi \in \hat{G}} f(\chi)\, e_\chi. \end{aligned}$$

It is readily checked that this map is an isomorphism and is Ω-equivariant. This shows that $U_G(\bar{K})$ is an algebraic torus and that its character module is

$$R(G)/R^+(G) \cong R^-(G).$$

(The reader unfamiliar with duality theory for algebraic tori should see, for instance, [8, Section 1.1].)

Let E/K be the extension obtained by adjoining to K the nth roots of 1, where n is the order of G. The action of $\Omega = \mathrm{Gal}(\bar{K}/K)$ on $R^-(G)$ factors through the finite abelian quotient $\Gamma = \mathrm{Gal}(E/K)$. Let $\mathfrak{p}$ be a prime ideal of K and let $\mathfrak{P}$ be a prime of E lying above $\mathfrak{p}$. Let p be the characteristic of the residue field $k(\mathfrak{p})$.

LEMMA 1.11. *Let $\Gamma_{\mathfrak{P}} \subset \Gamma$ be the stability subgroup of $\mathfrak{P}$ and let $T_{\mathfrak{P}} \subset \Gamma_{\mathfrak{P}}$ be the inertia subgroup. Let G_p denote the Sylow p-subgroup of G. Then*

$$R^-(G)^{T_{\mathfrak{P}}} \cong R(G_p)^{T_{\mathfrak{P}}} \otimes_{\mathbf{Z}} R^-(G/G_p)$$

as Γ-modules.

Proof. The canonical splitting $G = G_p \times G/G_p$ induces an isomorphism $R(G) \cong R(G_p) \otimes_{\mathbf{Z}} R(G/G_p)$. Since $T_{\mathfrak{P}}$ acts trivially on $R(G/G_p)$, we have, on the one hand,

$$R(G)^{T_{\mathfrak{P}}} \cong R(G_p)^{T_{\mathfrak{P}}} \otimes_{\mathbf{Z}} R(G/G_p). \tag{13}$$

On the other hand, a virtual character in $R(G_p)^{T_{\mathfrak{P}}}$ takes its values in the intersection $E^{T_{\mathfrak{P}}} \cap K(\mu_{p^m})$, where $p^m = |G_p|$. Since $\mathfrak{p}$ is unramified in $E^{T_{\mathfrak{P}}}$ and is totally ramified in $K(\mu_{p^m})$, the intersection $E^{T_{\mathfrak{P}}} \cap K(\mu_{p^m})$ must be equal to K, which is totally real by hypothesis. Therefore $R(G_p)^{T_{\mathfrak{P}}}$ is fixed by the canonical involution. Hence

$$R^-(G)^{T_{\mathfrak{P}}} \cong R(G_p)^{T_{\mathfrak{P}}} \otimes_{\mathbf{Z}} R^-(G/G_p). \tag{14}$$

(Note that the actions of C_2 and $T_{\mathfrak{P}}$ commute with each other.)

Let $A: \Gamma \to \mathrm{GL}_s(\mathbb{C})$ be a representation and let $\mathfrak{p}$ be a prime ideal of K. We set

$$A(\mathfrak{p}) = \frac{1}{e} \sum_{\tau \in T_{\mathfrak{P}}} A(\tau \sigma_{\mathfrak{P}})$$

where $\sigma_{\mathfrak{P}} \in \Gamma_{\mathfrak{P}}$ represents the Frobenius automorphism of $O_E/\mathfrak{P}$, and e is the order of $T_{\mathfrak{P}}$. Let χ be the character of A. We recall that the L-function associated with A (or with χ) has the Euler product representation

$$L(s, \chi) = \prod_{\mathfrak{p}} |\det(I - A(\mathfrak{p})\,\mathbf{N}(\mathfrak{p})^{-s})|^{-1} \tag{15}$$

for $\mathrm{Re}(s) > 1$. The product is taken over all primes $\mathfrak{p}$ of K (see [**6**, Chapter XII, §2]).

Henceforth we shall use the following notation: for a finite abelian group G we denote the representation $\Gamma \to \mathrm{GL}(R^-(G) \otimes_{\mathbf{Z}} \mathbb{C})$ by A_G. The character of A_G will be denoted by χ_G.

LEMMA 1.12. *With the notation above, we have*

$$\det(I - A_G(\mathfrak{p})\,q^{-1}) = \det(I - A_{G/G_p}(\mathfrak{p})\,q^{-1})^{n_p}$$

where $q = \mathbf{N}(\mathfrak{p})$ and $n_p = \dim R_K(G_p)$.

Proof. From the proof of Lemma 1.11 we know that Γ acts trivially on $R(G_p)^{T_{\mathfrak{P}}} = R_K(G_p)$. Thus

$$I - A_G(\mathfrak{p})\,q^{-1} = (I - A_{G/G_p}(\mathfrak{p})\,q^{-1}) \otimes I_{n_p}$$

where I_{n_p} is the $n_p \times n_p$ identity matrix. The lemma follows from this identity by taking determinants.

COROLLARY 1.13. *For every prime ideal* $\mathfrak{p}$ *of* K *we have*

$$\delta_{\mathfrak{p}}(U_G)^{n_p} = |\det(I - A_G(\mathfrak{p})\, q^{-1})|.$$

Proof. The algebra $k(\mathfrak{p})[G/G_p]$ is semisimple, thus the reduction mod $\mathfrak{p}$ of U_{G/G_p} is an algebraic torus. Its character module is $R^-(G/G_p)$ by the same argument as in Proposition 1.10. Applying Lemma 1.9 to U_{G/G_p} yields

$$|U_{G/G_p}(k(\mathfrak{p}))| = |\det(qI - A_{G/G_p}(\mathfrak{p}))|.$$

Thus, by Proposition 1.7 (applied to G/G_p) and Proposition 1.8, we have

$$\delta_{\mathfrak{p}}(U_G) = |\det(I - A_{G/G_p}(\mathfrak{p})\, q^{-1})|.$$

Taking n_pth powers on both sides of this equation and using Lemma 1.12, we obtain the desired equality.

COROLLARY 1.14. *The product*

$$\prod_{\mathfrak{p}} \delta_{\mathfrak{p}}(U_G),$$

as $\mathfrak{p}$ *runs over the prime ideals of* K *with* $\mathbf{N}(\mathfrak{p})$ *in increasing order, is convergent and*

$$\prod_{\mathfrak{p}} \delta_{\mathfrak{p}}(U_G) = L(1, \chi_G)^{-1} \prod_{\mathfrak{p} \text{ divides } |G|} \delta_{\mathfrak{p}}(U_G)^{1-n_{\mathfrak{p}}}.$$

(*Recall that* χ_G *is the character of* $R^-(G)$ *as a* Γ*-module and* $n_p = \dim R_K(G_p)$.)

Proof. Since χ_G does not contain the trivial character, the function $L(s, \chi_G)$ is holomorphic at $s = 1$. It is known (see [3, Section 109]) that the Euler product decomposition (15) can be extended to $s = 1$ provided the primes are ordered by increasing norm. (At $s = 1$ the product (15) does not converge absolutely.)

We finish by applying Corollary 1.13. Note that $n_p = 1$ if p does not divide $|G|$.

Our next goal is to calculate the local densities at archimedean places. Let $G = \{1, g_1, g_1^{-1}, \ldots, g_m, g_m^{-1}\}$ and let $u_i = g_i - g_i^{-1}$ for $i = 1, \ldots, m$.

LEMMA 1.15. *For every archimedean place* v *of* K *we have*

$$\delta_v(U_G) = |G|^{m/2} (2\pi)^m.$$

Proof. We fix an embedding $K \hookrightarrow \mathbb{R}$. Let $\hat{G} = \{1, \chi_1, \chi_1^{-1}, \ldots, \chi_m, \chi_m^{-1}\}$. Let $e_1, \ldots, e_m$ be the idempotents of $\mathbb{C}G$ corresponding to the characters $\chi_1, \ldots, \chi_m$. Let $v_i = \sqrt{-1}(\bar{e}_i - e_i)$ for $i = 1, \ldots, m$. With this notation, we have

$$u_i = \sum_{j=1}^{m} (\chi_j(g_i) - \chi_j(g_i^{-1}))(\sqrt{-1})\, v_j.$$

Let M be the $m \times m$ matrix whose ij-entry is $\chi_j(g_i) - \chi_j(g_i^{-1})$. An elementary computation shows that $M^* M = |G|\, I_m$. Hence $|\det(M)| = |G|^{m/2}$. Let $dy_1, \ldots, dy_m$ be the dual basis of the basis $v_1, \ldots, v_m$ of $\mathbb{R}[G]^-$. The previous calculation shows

$$\int_{U_G(\mathbf{R})} |\omega| = |G|^{-m/2} \int_{U_G(\mathbf{R})} |dy_1 \wedge \ldots \wedge dy_m|. \tag{16}$$

Observe that $U_G(\mathbb{R}) = S^1 \times \ldots \times S^1$ and that the form dy_t induces the canonical measure on the circle S^1. This observation and (16) prove the lemma.

We are now ready to prove our main result in this section.

THEOREM 1.16. *Let h be the hermitian class number of $O_K[G]$. Then*

$$h = 2^n(2\pi)^{-mr}|G|^{(1+mr/2)}L(1,\chi_G)\prod_{p \text{ divides } |G|}\delta_p(U_G)^{n_p-1} \tag{17}$$

where $m = (|G|-1)/2$, $r = [K:\mathbb{Q}]$, $n = \dim R_K(G)-1$ and $n_p = \dim R_K(G_p)$.

Proof. Consider the decomposition of the group algebra

$$K[G] = K \oplus E_1 \oplus E_2 \oplus \cdots \oplus E_n.$$

Since K is totally real, the canonical involution on $K[G]$ induces a non-trivial involution on E_t (in fact, it turns out to be complex conjugation; see [3, (5.37)]). Let F_t be the subfield of E_t fixed by this involution. Let $U_t = \mathrm{Ker}(N_{E_t/F_t})$; we shall regard U_t as an algebraic group over F_t. Clearly, U_G has a decomposition

$$U_G = \prod_{t=1}^{n}\mathrm{Res}_{F_t/K}(U_t)$$

where $\mathrm{Res}_{F_t/K}$ is the 'restriction of scalars' functor (see [12, 1.3] for the definition). We know that the Tamagawa number is multiplicative and invariant by restriction of scalars (see [9, Section 2]). Thus $\tau(U_G) = \prod\tau(U_t)$. On the other hand, since U_t is the special orthogonal group of a quadratic form in two variables, by the Siegel–Tamagawa Theorem we have $\tau(U_t) = 2$ (see [12, Chapter 4]). Thus $\tau(U_G) = 2^n$. Starting out with (1) we substitute using (3), (4) and (6), and apply Corollary 1.14 and Lemma 1.15.

2. *Examples*

In this section the ground field will be the field of rational numbers $\mathbb{Q}$. For a positive integer ν we shall denote by $\mathbb{Q}(\nu)$ the cyclotomic field of νth roots of unity. We recall that the *relative class number* of $\mathbb{Q}(\nu)$ is the ratio

$$h_\nu^- = \frac{\text{class number of } \mathbb{Q}(\nu)}{\text{class number of } \mathbb{Q}(\nu)^+}$$

where $\mathbb{Q}(\nu)^+$ is the maximal real subfield of $\mathbb{Q}(\nu)$ (see [10, Chapter 4]). In this section we shall compare numerically using formula (17) the hermitian class number of $\mathbb{Z}[G]$ to the relative class numbers of the cyclotomic components of $\mathbb{Q}[G]$ for G elementary abelian and for G cyclic of order pq.

The following two lemmas will be used to calculate the character χ_G of Theorem 1.16. We recall that a character modulo d (that is, a homomorphism $\psi:(\mathbb{Z}/d\mathbb{Z})^* \to \mathbb{C}^*$) is said to be *odd* if $\psi(-1) = -1$. Otherwise, it is said to be *even*. Let Γ_d denote the group $(\mathbb{Z}/d\mathbb{Z})^*$. The cyclic group of order two acts on Γ_d by $\gamma \mapsto -\gamma$. This action induces a C_2-module structure on the group ring $\mathbb{Z}[\Gamma_d]$.

LEMMA 2.1. *The character of $\mathbb{Z}[\Gamma_d]^-$ as a Γ_d-module is equal to the sum of all odd characters modulo d.*

Proof. The canonical map $\Gamma_d \to \Gamma_d/\{\pm 1\}$ induces an exact sequence of Γ_d-modules

$$0 \longrightarrow \mathbb{Z}[\Gamma_d]^- \longrightarrow \mathbb{Z}[\Gamma_d] \longrightarrow \mathbb{Z}[\Gamma_d/\{\pm 1\}] \longrightarrow 0.$$

Hence

$$\begin{aligned}\operatorname{char}(\mathbb{Z}[\Gamma_d]^-) &= \operatorname{char}(\mathbb{Z}[\Gamma_d]) - \operatorname{char}(\mathbb{Z}[\Gamma_d/\{\pm 1\}]) \\ &= \sum_{\psi} \psi - \sum_{\psi \text{ even}} \psi \\ &= \sum_{\psi \text{ odd}} \psi.\end{aligned}$$

The sum of all odd characters mod d will be denoted by σ_d. With this notation we have the following.

LEMMA 2.2. *The character of $R^-(C_n)$ as a Γ_n-module is equal to*

$$\sum_{d|n} \sigma_d.$$

Proof. For $d|n$ let X_d be the subset of $\hat{C}_n$ of elements of order exactly equal to d. Clearly Γ_d acts freely and transitively on X_d. Thus $R(C_n) = \mathbb{Z}[\hat{C}_n]$ admits a splitting as a Γ_n-module

$$R(C_n) \cong \bigoplus_{d|n} \mathbb{Z}[\Gamma_d].$$

It is easy to see that this is also a splitting as C_2-modules. (Recall that the involution on $\mathbb{Z}[\Gamma_d]$ considered here is induced by multiplication by -1 in Γ_d, and *not* by group inversion.) Hence

$$R^-(C_n) \cong \bigoplus_{d|n} \mathbb{Z}[\Gamma_d]^-.$$

We finish the proof by applying Lemma 2.1.

EXAMPLE 2.3. Let p be an odd prime number and G an elementary abelian p-group of rank t. Let h be the hermitian class number of $\mathbb{Z}[G]$. With this notation, the following formula holds:

$$h = (h_p^-)^n p^s$$

where

$$n = \frac{p^t - 1}{p - 1} \quad \text{and} \quad s = (p^t - 1)\left[\frac{(t-1)}{4} - \frac{1}{(p-1)}\right] + t.$$

Proof. In the notation of Theorem 1.16, we have $|G| = p^t$, $m = (p^t - 1)/2$, $n = (p^t - 1)/(p - 1)$, $r = 1$ and $\delta_p(U_G) = 1$. The group $\hat{G}$ breaks up into $(n+1)$ different Γ_p-orbits: one orbit reduced to the trivial character and n orbits each containing $p - 1$ elements. Thus the representation ring $R(G) = \mathbb{Z}[\hat{G}]$ has a decomposition as a Γ_p-module:

$$R(G) \cong \mathbb{Z} \oplus \mathbb{Z}[\Gamma_p] \oplus \cdots \oplus \mathbb{Z}[\Gamma_p]$$

where the factor $\mathbb{Z}[\Gamma_p]$ is repeated n times. Hence

$$R^-(G) \cong \mathbb{Z}[\Gamma_p]^- \oplus \cdots \oplus \mathbb{Z}[\Gamma_p]^-.$$

By applying Lemma 1.1, we obtain

$$\chi_G = n\sigma_p.$$

By the multiplicativity property of L-series (see [6, Chapter XII, §2]) we have $L(1,\chi_G) = L(1,\sigma_p)^n$. Rewriting formula (17) in this particular case gives

$$h = \left[\frac{2p\cdot p^{(p-1)/4}}{(2\pi)^{(p-1)/2}} L(1,\sigma_p)\right]^n p^s.$$

The expression within the square brackets turns out to be the formula for the relative class number of the cyclotomic field $\mathbb{Q}(p)$ (see [10, Chapter 4]).

EXAMPLE 2.4. Let p and q be distinct odd prime numbers, let $G = C_{pq}$ and let h be the hermitian class number of $\mathbb{Z}[G]$. The following formula holds:

$$h = \frac{|U_{C_p}(\mathbb{F}_q)|\,|U_{C_q}(\mathbb{F}_p)|}{2pq} h_p^- h_q^- h_{pq}^-.$$

Proof. By Lemma 2.2 we have $\chi_G = \sigma_p + \sigma_q + \sigma_{pq}$. Thus, by the multiplicativity property of L-series, we obtain $L(1,\chi_G) = L(1,\sigma_p)\,L(1,\sigma_q)\,L(1,\sigma_{pq})$. In the notation of Theorem 1.16 we have $r = 1$, $n = 3$, $m = (pq-1)/2$ and $n_p = n_q = 2$. Thus formula (17) yields

$$\begin{aligned} h &= 2^3(2\pi)^{-(pq-1)/2}(pq)^{(pq-3)/4} L(1,\chi_G)\,\delta_p(U_G)\,\delta_p(U_G) \\ &= \left[\frac{2p\cdot p^{(p-1)/4}}{(2\pi)^{(p-1)/2}} L(1,\sigma_p)\right]\left[\frac{2q\cdot q^{(q-1)/4}}{(2\pi)^{(q-1)/2}} L(1,\sigma_q)\right] \\ &\quad\times\left[\frac{4pq\cdot p^{(p-2)(q-1)/4} q^{(q-2)(p-1)/4}}{(2\pi)^{(p-1)(q-1)/2}} L(1,\sigma_{pq})\right]\frac{|U_{C_p}(\mathbb{F}_q)|\,|U_{C_q}(\mathbb{F}_p)|}{2pq}. \end{aligned}$$

We recall that by Propositions 1.7 and 1.8 we have

$$\delta_p(U_G) = \delta_p(U_{C_q}) = |U_{C_q}(\mathbb{F}_p)|\,p^{-(q-1)/2}.$$

We finish the proof by observing that the expressions within the square brackets are the classical formulas for h_p^-, h_q^- and h_{pq}^- (see [10, Chapter 4]).

References

1. E. BAYER and H. W. LENSTRA, 'Forms in odd degree extensions and self-dual normal bases', *Amer. J. Math.*, to appear.
2. P. E. CONNER and R. PERLIS, *A survey of trace forms of algebraic number fields* (World Scientific Publishing, Singapore, 1984).
3. C. CURTIS and I. REINER, *Methods of representation theory*, Vol. II (John Wiley, New York, 1987).
4. B. EREZ and J. MORALES, 'The hermitian structure of rings of integers in abelian extensions', preprint, 1989.
5. E. LANDAU, *Handbuch des Lehre der Verteilung der Primzahlen I* (Teubner, Leipzig/Berlin, 1909).
6. S. LANG, *Algebraic number theory* (Addison-Wesley, Reading, Mass., 1970).
7. J. MORALES, 'Integral bilinear forms with a group action', *J. Algebra* 98 (1986) 470–484.
8. T. ONO, 'Arithmetic of algebraic tori', *Ann. of Math.* 74 (1961) 101–139.
9. T. ONO, 'On Tamagawa numbers', *Proc. Sympos. Pure Math.* IX (Amer. Math. Soc., Providence, R.I., 1966), pp. 122–132.
10. L. C. WASHINGTON, *Introduction to cyclotomic fields*, Graduate Texts in Math. (Springer, Berlin/New York, 1982).

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