AN INJECTIVITY RESULT FOR HERMITIAN FORMS OVER LOCAL ORDERS

LAURA FAINSILBER AND JORGE MORALES

Abstract. Let Λ be a ring endowed with an involution $a \mapsto \tilde{a}$. We say that two units a and b of Λ fixed under the involution are *congruent* if there exists an element $u \in \Lambda^\times$ such that $a = ub\tilde{u}$. We denote by $\mathcal{H}(\Lambda)$ the set of congruence classes. In this paper we consider the case where Λ is an order with involution in a semisimple algebra A over a local field and study the question whether the natural map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ induced by inclusion is injective. We give sufficient conditions on the order Λ for this map to be injective and give applications to hermitian forms over group rings.

Introduction and motivation

Let R be a ring endowed with an involution $\tilde{}\,: R \to R$ (that is, an anti-automorphism of order 2). For a left R-module M we denote by M^* the dual module $\operatorname{Hom}_R(M,R)$ with the left R-module structure given by $(a\phi)(m) = \phi(m)\tilde{a}$, for all $a \in R$, $\phi \in \operatorname{Hom}_R(M,R)$, $m \in M$.

Let $\epsilon \in R$ be a fixed central element satisfying $\tilde{\epsilon}\epsilon = 1$, for example $\epsilon = \pm 1$. A (unimodular) *ϵ-hermitian form* over R is a pair (M,h) consisting of a reflexive R-module M and an isomorphism of R-modules $h : M \to M^*$ satisfying $h^* = \epsilon h$. The notion of isometry of ϵ-hermitian forms is defined in the obvious way.

It is a natural question to ask for a classification of ϵ-hermitian forms over R. An obvious necessary condition for two forms (M_1,h_1) and (M_1,h_2) to be isometric is that their underlying R-modules M_1 and M_2 be isomorphic. This leads us to fix an R-module M and consider the set of all ϵ-hermitian forms on M.

Assuming that this set is not empty, we fix once and for all an ϵ-hermitian form $h_0 : M \to M^*$ and we equip the endomorphism ring $\Lambda = \operatorname{End}_R(M)$ with the involution given by

$$\tilde{f} = h_0^{-1} f^* h_0. \qquad (1)$$

A straightforward calculation shows that all the ϵ-hermitian forms on M are of the form $h = h_0 a$, with $a \in \Lambda^\times$ satisfying $\tilde{a} = a$, and that two such forms $h = h_0 a$ and $g = h_0 b$ are isometric if and only if there exists $u \in \Lambda^\times$ such that $ua\tilde{u} = b$. Note that this is a particular case of the so-called *transfer to the endomorphism ring* in hermitian categories (see [15, Chapter 7, Section 4] or [13]).

The above construction motivates the introduction of the following equivalence relation for any ring Λ equipped with an involution $\tilde{}$.

$$a \sim b \iff \text{there exists } u \in \Lambda^\times \text{ such that } ua\tilde{u} = b$$

The second–named author was supported by Louisiana Education Quality Support Fund grant No LEQSF(RF1995-97)-RD-A-40.

on the set of units of Λ fixed under the involution. We shall denote the set of equivalence classes by $\mathcal{H}(\Lambda)$. Two elements equivalent in the above sense will be called *congruent.* Many classification problems in the theory of quadratic and hermitian forms can be reduced to determining the congruence classes in a suitable algebra with involution [3, 6, 8, 9, 11, 12, 13, 15]. Note that $\mathcal{H}(\Lambda)$ is also the cohomology set $H^1(C_2, \Lambda^\times)$ in non-abelian cohomology, where the non-trivial element in C_2 acts via $\lambda \mapsto \tilde{\lambda}^{-1}$.

In this article, we shall deal with the case where Λ is an order in a finite-dimensional algebra over a local field.

The following notation will be in force throughout the paper:

K : a field complete with respect to a discrete valuation
$\mathcal{O}$: the valuation ring of K
k : the residue field of $\mathcal{O}$, assumed to be finite of characteristic $\neq 2$
A : a semisimple K-algebra equipped with an involution $\tilde{}: A \to A$
Λ : an $\mathcal{O}$-order in A, stable under the involution, such that $A = K \otimes_{\mathcal{O}} \Lambda$.

The main question that we shall address in this paper is whether the canonical map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ induced by the inclusion $\Lambda \hookrightarrow A$ is injective.

For instance, as an easy consequence of the classification of unimodular quadratic forms over $\mathcal{O}$ by their determinant, one sees that if $A = M_n(K)$ and $\Lambda = M_n(\mathcal{O})$, and the involution is transposition, then $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective. A simple example (see the next section) shows that even in the local case one cannot expect the map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ to be injective in general.

We show that $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective if Λ is a hereditary order in a semisimple algebra (hence in particular if it is a maximal order) or if it projects onto an order for which the property holds (see Theorem 3.1 for a precise statement). We also show that if $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective then this property extends to the endomorphism rings of the self-dual projective modules over Λ. As a consequence, we prove that if two unimodular hermitian forms on projective Λ-modules are isometric over A, then they are isometric over Λ.

A particularly interesting case is when $\Lambda = \mathcal{O}G$, the group algebra over $\mathcal{O}$ of a finite group G. We show that $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective if G is of odd order, or if the p-Sylow subgroup of G is normal, where p is the characteristic of the residue field k.

1. Hereditary orders

In this section we consider the case where Λ is a hereditary order. We recall that an order Λ is *left hereditary* if all its left ideals are projective as Λ-modules. One defines in a similar manner the notion of *right hereditary*, but it is known that these two notions are equivalent [14, Theorem 40.1]; so we shall simply write *hereditary.*

The structure of hereditary orders is known (see [14, Theorem 39.14]) and they include in particular the maximal orders [5, Section 26].

Theorem 1.1. *If Λ is a hereditary order in A then the natural map*

$$\mathcal{H}(\Lambda) \to \mathcal{H}(A)$$

is injective.

Proof. Let a and b be representatives of classes in $\mathcal{H}(\Lambda)$ that are congruent in A. Let $u \in A^\times$ be such that $ua\tilde{u} = b$. We show that the hermitian form $(\Lambda^2, < a, -b >)$ is isometric to the hyperbolic plane $\mathbf{H}(\Lambda)$.

Consider the homomorphism $\phi : \Lambda^2 \to A$ of left Λ-modules given by $\phi(x, y) = x - yu$. Since Λ is hereditary, the image $\phi(\Lambda^2)$, which is isomorphic to an ideal in Λ, is a projective Λ-module; hence $M := \ker \phi$ is a direct factor of Λ^2. One verifies immediately that the left submodule $M \subset \Lambda^2$ is equal to its orthogonal $M^\perp$ with respect to $< a, -b >$. By a result of Knebush [15, Lemma 7.3.7], the form $< a, -b >$ is stably isometric to $\mathbf{H}(\Lambda)$. Since Witt cancellation holds for Λ [15, Theorem 7.10.9], this shows that actually $< a, -b > \simeq \mathbf{H}(\Lambda)$ as forms over Λ. But we also have $\mathbf{H}(\Lambda) \simeq < a, -a >$; hence, by Witt cancellation again, we conclude $< a > \simeq < b >$ over Λ. □

We give below a simple example of a (non-hereditary!) order Λ for which the map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is not injective.

Example. Let π be a uniformizing parameter in $\mathcal{O}$, and let $\varepsilon \in \mathcal{O}$ be a unit which is not a quadratic residue modulo π.

Let $A = M_2(K)$, with the involution given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & c\pi^{-2} \\ b\pi^2 & d \end{pmatrix}, \tag{2}$$

and let $\Lambda \subset M_2(\mathcal{O})$ be the subring defined by

$$\Lambda = \left\{ \begin{pmatrix} a & b \\ c\pi^2 & d \end{pmatrix} \; : \; a, b, c, d \in \mathcal{O} \right\}.$$

One verifies readily that Λ is stable under the involution (2). The matrix $\begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$ is congruent to the identity matrix in $\mathcal{H}(A)$ but not in $\mathcal{H}(\Lambda)$. So in this case $\mathcal{H}(\Lambda)$ does not map injectively into $\mathcal{H}(A)$.

The ring Λ is actually the endomorphism ring of the arrow $(1, \pi^2) : \mathcal{O}^2 \to \mathcal{O}^2$ associated with the quadratic form $< 1, \pi^2 >$ (see [3]), and $\mathcal{H}(\Lambda)$ corresponds to the set of (non-unimodular) forms $\{< 1, \pi^2 >, < \varepsilon, \varepsilon\pi^2 >, < 1, \varepsilon\pi^2 >, < \varepsilon, \pi^2 >\}$. The defect in injectivity reflects the fact that the first two forms and the last two become isometric over K.

2. Reduction of the set $\mathcal{H}(\Lambda)$

In order to generalize the result above to a certain class of rings which are not hereditary, in particular to certain group rings, we reduce the study of the set $\mathcal{H}(\Lambda)$ of congruence classes of involution-invariant invertible elements of Λ to the study of simple factors carrying involutions of orthogonal type in the semi-simplification of Λ.

Lemma 2.1 (Reduction modulo the radical)**.** *Let Λ be an algebra over a complete local ring as above. Reduction modulo the Jacobson radical of Λ induces a bijective map $\mathcal{H}(\Lambda) \simeq \mathcal{H}(\Lambda/\mathrm{rad}\,\Lambda)$.*

Remark. Lemma 2.1 follows from more general known theorems ([2, Theorem 5.1] or [1, Theorem 10.3]). We include an ad-hoc proof for the convenience of the reader. For even more general analogues in hermitian categories, see [9], or [15, Theorem 7.4.4].

Proof. We first prove that the reduction map is surjective from the set Λ^+ of invertible elements of Λ fixed under the involution, onto the set $(\Lambda/\mathrm{rad}\,\Lambda)^+$ of invertible elements of $\Lambda/\mathrm{rad}\,\Lambda$ fixed by the involution. Indeed, say $[\alpha]$ is invertible in $\Lambda/\mathrm{rad}\,\Lambda$ and invariant under the involution, then $\gamma = (\alpha + \tilde{\alpha})/2$ is invariant under the involution and $[\gamma] = [\alpha]$. Note that γ, being invertible modulo $\mathrm{rad}\,\Lambda$, is automatically invertible in Λ.

Second, we prove that any congruence relation can be lifted from $\Lambda/\mathrm{rad}\,\Lambda$ to Λ. Let π be a uniformizing parameter for $\mathcal{O}$. There is a positive integer k such that $\mathrm{rad}\,(\Lambda)^k \subset \pi\Lambda \subset \mathrm{rad}\,(\Lambda)$ [5, Proposition 5.22]), so the topology defined by the radical is equivalent to the π-adic topology, and Λ is complete with respect to its radical. Suppose we have $\alpha, \beta \in \Lambda^+$ and v a unit in Λ such that $\alpha \equiv v\beta\tilde{v} \mod \mathrm{rad}\,\Lambda$. We shall construct a sequence $(v_i)_{i\geq 1}$ of units in Λ with $v_1 = v$ and $\alpha \equiv v_i\beta\tilde{v}_i \mod (\mathrm{rad}\,\Lambda)^i$ for $i \geq 1$; this sequence will converge to a limit $w \in \Lambda^\times$ with $\alpha = w\beta\tilde{w}$, thus completing the proof of the lemma. To construct the $(n+1)$st element in the sequence, we suppose $\alpha \equiv v_n\beta\tilde{v}_n \mod (\mathrm{rad}\,\Lambda)^n$, and let $\delta = v_n\beta\tilde{v}_n - \alpha \in (\mathrm{rad}\,\Lambda)^n$. Since β and v_n are units in A, there is a $\tau \in (\mathrm{rad}\,\Lambda)^n$ such that $v_n\beta\tilde{\tau} = -\delta/2$. We let $v_{n+1} = v_n + \tau$. We then have $v_{n+1}\beta\tilde{v}_{n+1} = v_n\beta\tilde{v}_n + v_n\beta\tilde{\tau} + \tau\beta\tilde{v}_n + \tau\beta\tilde{\tau} = v_n\beta\tilde{v}_n - \delta/2 - \tilde{\delta}/2 + \tau\beta\tilde{\tau} = v_n\beta\tilde{v}_n - \delta + \tau\beta\tilde{\tau} = \alpha + \tau\beta\tilde{\tau}$ with $\tau\beta\tilde{\tau} \in (\mathrm{rad}\,\Lambda)^{2n}$. □

Remark. In Lemma 2.1, and in everything that follows in Sections 1 and 2, one can replace the condition that 2 is invertible in Λ by the weaker condition that Λ contains a central element c with $\tilde{c} + c = 1$. The proof above requires only minor adjustments to include this situation. Note however that for the case of group rings, that will be the focus of our interest in Section 3, the existence of such an element c is in fact equivalent to 2 being invertible in $\mathcal{O}$, as can be easily seen by applying the augmentation map to the identity $\tilde{c} + c = 1$.

Let F be a field, and let $\tilde{}$ be an involution of the first kind on $M_n(F)$, (i.e. $\tilde{}$ is the identity on F). Since transposition is also an involution of the first kind, the Skolem-Noether theorem yields an element $v \in M_n(F)$ such that for all $x \in M_n(F)$, $\tilde{x} = vx^tv^{-1}$. The matrix v is either skew-symmetric ($v^t = -v$), in which case we say that $\tilde{}$ is of *symplectic type*, or symmetric ($v^t = v$), in which case we say that $\tilde{}$ is of *orthogonal type* ([15, Chapter 8, Section 6], [11]).

More generally, if $(B, \tilde{})$ is a central simple F-algebra with involution of the first kind, we say that $(B, \tilde{})$ is orthogonal (respectively, symplectic) if $(B \otimes_F \bar{F}, \tilde{})$ is orthogonal (respectively, symplectic), where $\bar{F}$ is the separable closure of F.

Let S be a semisimple algebra over a finite field F, with involution $\tilde{}$. We can write S as a product of simple algebras, which are all rings of matrices over finite extensions of F

$$S = S_1 \times \cdots \times S_r \ , \text{ where } S_i \simeq M_{n_i}(F_i)\,.$$

When we consider the action of the involution on the simple components, we see that it switches some pairs of components, and stabilizes the others. We denote again by $\tilde{\ }$ the involution induced on the components or pairs of components. On a stable simple factor S_i, the involution is either of the first kind, or it is of the second kind, i.e. it induces a non-trivial involution on the center F_i, in which case F_i is a quadratic extension of the field F_i^+ fixed by the involution.

We will now show that the only non-trivial unimodular hermitian forms of rank one are carried by the simple components on which the involution is of orthogonal type. More precisely :

Lemma 2.2. *Let S be a finitely generated semisimple algebra over a finite field, and let S_{orth} be the product of the simple components on which the involution is of the first kind, of orthogonal type. Then $\mathcal{H}(S) = \mathcal{H}(S_{\mathrm{orth}})$.*

Proof. It is clear that an element of S is invertible and invariant under the involution if and only if its projections on the pairs of simple subalgebras $S_i \times S_j$ switched by $\tilde{\ }$ and on the components stable under $\tilde{\ }$ are invertible and $\tilde{\ }$-invariant, and also that congruence of two elements is determined by congruence of the projections on the stable components or pairs of components.

We first describe $\mathcal{H}(M_{n_i}(F_i) \times M_{n_i}(F_i))$ when $\tilde{\ }$ switches the two components. There is an automorphism θ of order 2 of $M_{n_i}(F_i)$ such that for all x,y in $M_{n_i}(F_i)$, $\widetilde{(x,y)} = (\theta(y), \theta(x))$. So the elements fixed by $\tilde{\ }$ are all of the form $(x, \theta(x))$. But such elements are congruent to $(1,1)$ since $(x, \theta(x)) = (x,1)(1,\theta(x)) = (x,1)(1,1)\widetilde{(x,1)}$. Hence $\mathcal{H}(M_{n_i}(F_i) \times M_{n_i}(F_i)) = \{1\}$.

Secondly, we consider simple components $M_{n_i}(F_i)$ on which the involution is of the second kind, and show that $\mathcal{H}(M_{n_i}(F_i)) = \{1\}$:

Let $\bar{\ }$ denote the involution induced on F_i. The involution which maps a matrix $M = (m_{ij})$ to its transpose conjugate $\bar{M}^t = (\bar{m}_{ji})$ is of the second kind, and the invertible elements fixed by the involution are the non-degenerate hermitian forms of rank n_i over F_i. To show that every such form h is diagonalizable, we show that h represents a non-zero element $\alpha \in F_i$, so we can write $h =<\alpha> \oplus h'$ and proceed by induction on n_i. We have $h(F_i^{n_i}, F_i^{n_i}) = F_i$, and since F_i is a separable extension of F_i^+, the trace map $Tr : F_i \to F_i^+$ is not zero. So there are elements $v, w \in F_i^{n_i}$ such that $Tr(h(v,w)) \neq 0$, and we have $h(v+w, v+w) = h(v,v) + h(w,w) + h(v.w) + \overline{h(v,w)}$ hence $Tr(h(v,w)) = h(v+w,v+w) - h(v,v) - h(w,w)$, so at least one of the three values on the right is non-zero : h represents a non-zero value. Hence every matrix fixed by the involution is congruent to a diagonal matrix, whose entries $\alpha_1, \ldots, \alpha_n$ are in F_i^+. But F_i is a finite field, so every element in F_i^+ is the norm of an element in F_i, say $\alpha_j = \gamma_j\bar{\gamma}_j$, and hence the matrix is congruent to the identity matrix. This shows that for this involution, $\mathcal{H}(M_{n_i}(F_i)) = \{1\}$, but we also know that if $\tilde{\cdot}$ is another involution of the second kind on $M_{n_i}(F_i)$ which induces $\bar{\cdot}$ on F_i, then $\tilde{\cdot}$ is equivalent to $\bar{\cdot}^t$. Indeed, by the Skolem-Noether theorem there is an element $y \in M_{n_i}(F_i)^\times$ such that for all $x \in M_{n_i}(F_i)$, $\tilde{x} = y^{-1}\overline{x}^t y$ ([11]). Moreover, $\tilde{\tilde{x}} = y^{-1}\overline{y}^t x \overline{y}^{t-1} y = x$ implies that $\lambda = y^{-1}\overline{y}^t \in F_i$, and hence

$y = \overline{\overline{y}^t}^t = \overline{\lambda}\overline{y}^t = \overline{\lambda}\lambda y$ so $\overline{\lambda}\lambda = 1$, and Hilbert's theorem 90 yields a $\mu \in F_i^\times$ such that $\lambda = \mu\overline{\mu}^{-1}$. We can replace y by $z = \mu y$ to get $\overline{z}^t = \overline{\mu y}^t = \overline{\mu}\lambda y = \mu y = z$. We showed above that z is congruent to 1, i.e.. that there exists a matrix w such that $z = \overline{w}^t w$. Consider the inner automorphism of $M_{n_i}(F_i)$: $\theta(x) = wxw^{-1}$. We have $\theta(\tilde{x}) = w\tilde{x}w^{-1} = wz^{-1}\overline{x}^t z w^{-1} = ww^{-1}\overline{w}^{t-1}\overline{x}^t\overline{w}^t ww^{-1} = \overline{w}^{t-1}\overline{x}^t\overline{w}^t = \overline{\theta(x)}^t$. So the algebras with involution $(M_{n_i}(F_i), \bar{\ }^t)$ and $(M_{n_i}(F_i), \tilde{\ })$ are isomorphic, and hence for any involution of the second kind on $M_{n_i}(F_i)$, the set of isomorphism classes of rank one unimodular hermitian forms is trivial.

The last case we consider is that of a simple component on which the involution is of symplectic type, say $\tilde{x} = vx^tv^{-1}$ with $v^t = -v$. Suppose $x = \tilde{x}$, then $xv = vx^t$, and $(xv)^t = v^tx^t = -vx^t = -xv$, so xv is skew-symmetric. But all skew-symmetric elements are congruent ([15, Theorem 7.8.1]) so there is a $z \in M_{n_i}(F_i)$ such that $xv = zvz^t$, hence $x = zvz^tv^{-1} = z\tilde{z}$ so again x is congruent to 1 and $\mathcal{H}(M_{n_i}(F_i))$ is trivial.

So we have proved that the only components of S with non-trivial rank-one hermitian forms are the components on which the involution is of orthogonal type, i.e. that $\mathcal{H}(S) = \mathcal{H}(S_{\mathrm{orth}})$. □

3. More general orders

In this section we establish a result that will allow us to extend Theorem 1.1 to a larger class of orders that includes, as we shall see in the next section, group rings for certain types of groups.

Theorem 3.1. *Let Δ be an $\mathcal{O}$-order with involution in a semisimple K-algebra B and let $\Lambda \to \Delta$ be a surjective, involution-preserving homomorphism which induces an isomorphism $(\Lambda/\operatorname{rad}\Lambda)_{\mathrm{orth}} \simeq (\Delta/\operatorname{rad}\Delta)_{\mathrm{orth}}$. If the natural map $\mathcal{H}(\Delta) \to \mathcal{H}(B)$ is injective, then so is the natural map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$.*

Proof. The natural inclusions $\Lambda \hookrightarrow A$ and $\Delta \hookrightarrow B$ induce a diagram of sets

$$\begin{tikzcd}
\mathcal{H}(\Lambda) \arrow[r] \arrow[d] & \mathcal{H}(\Delta) \arrow[d] \\
\mathcal{H}(A) \arrow[r] & \mathcal{H}(B)
\end{tikzcd}$$

with $\mathcal{H}(\Lambda) = \mathcal{H}((\Lambda/\operatorname{rad}\Lambda)_{\mathrm{orth}}) \simeq \mathcal{H}((\Delta/\operatorname{rad}\Delta)_{\mathrm{orth}}) = \mathcal{H}(\Delta)$ by Lemma 2.1 and Lemma 2.2. By hypothesis, the vertical map $\mathcal{H}(\Delta) \to \mathcal{H}(B)$ is injective, so in the diagram the composite maps from $\mathcal{H}(\Lambda)$ to $\mathcal{H}(B)$ are injective, and hence $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective. □

We now show that if $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective, then this property also holds for the endomorphism rings of projective modules over Λ that afford a unimodular hermitian form.

Lemma 3.2. *Let Λ be an $\mathcal{O}$-order with an involution $\tilde{\ }$, and consider $M_n(\Lambda)$ endowed with the involution $\widetilde{(a_{ij})} = (\widetilde{a_{ji}})$. Then the map $\Lambda^\times \to M_n(\Lambda)^\times$ given by $a \mapsto \operatorname{diag}(a, 1, \dots, 1)$ induces a bijection $\mathcal{H}(\Lambda) \simeq \mathcal{H}(M_n(\Lambda))$.*

Proof. Let $\overline{\Lambda} = \Lambda/\mathrm{rad}\,\Lambda$. Then $M_n(\Lambda)/\mathrm{rad}\,M_n(\Lambda) = M_n(\overline{\Lambda})$ (see [5, Proposition 5.14]. It is easy to see that the orthogonal components of $M_n(\overline{\Lambda})$ are of the form $M_n(S)$, where S is an orthogonal component of $\overline{\Lambda}$. By Lemma 2.2, it is enough to see that for these components the map $S \to M_n(S)$ given by $x \mapsto \mathrm{diag}(x, 1, \dots, 1)$ induces a bijection $\mathcal{H}(S) \simeq \mathcal{H}(M_n(S))$. But this is clear, since the elements of $\mathcal{H}(S)$ are classified by their determinant, and $\det \mathrm{diag}(x, 1, \dots, 1) = \det(x)$. □

Theorem 3.3. *Assume that the map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective. Let h_1 and h_2 be unimodular hermitian forms on a projective Λ-module P. If h_1 and h_2 are isometric over A, then they are isometric over Λ.*

Proof. Suppose first that P is free over Λ, say $P = \Lambda^n$. Let $M_n(\Lambda)$ be endowed with the involution $\widetilde{(a_{ij})} = (\widetilde{a_{ji}})$. Consider the following commutative diagram

$$\begin{tikzcd}
\mathcal{H}(\Lambda) \arrow[r] \arrow[d, "\simeq"'] & \mathcal{H}(A) \arrow[d] \\
\mathcal{H}(M_n(\Lambda)) \arrow[r] & \mathcal{H}(M_n(A)),
\end{tikzcd}$$

where the vertical maps are as in Lemma 3.2. The map $\mathcal{H}(A) \to \mathcal{H}(M_n(A))$ is injective since Witt cancellation holds for forms over A [15, Theorem 7.10.9]. Hence, by virtue of the above diagram, if $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective, so is $\mathcal{H}(M_n(\Lambda)) \to \mathcal{H}(M_n(A))$, and we deduce that h_1 and h_2 are isometric over Λ.

Suppose now that P is projective and let Q be a finitely generated projective Λ-module such that $P \oplus Q$ is free. Let $\mathbf{H}(Q) = Q \oplus Q^*$ be the hyperbolic hermitian space on Q and define $(Q', g) = (P, h_1) \perp \mathbf{H}(Q)$. Then $(P, h_1) \perp (Q', g)$ and $(P, h_2) \perp (Q', g)$ are hermitian forms with free underlying Λ-module.

It follows from our hypothesis that $(P, h_1) \perp (Q', g)$ and $(P, h_2) \perp (Q', g)$ are isometric over A. By the above considerations in the free case we conclude that $(P, h_1) \perp (Q', g)$ and $(P, h_2) \perp (Q', g)$ are isometric over Λ. Finally, using Witt cancellation for forms over Λ [15, Theorem 7.10.9], we see that (P, h_1) and (P, h_2) are isometric.

□

Remark. Let P be a projective Λ-module that affords a unimodular hermitian form h. We equip the endomorphism ring $\mathrm{End}_\Lambda(P)$ with the adjoint involution of h, as in (1). An equivalent formulation of Theorem 3.3 is that if the map $\mathcal{H}(\Lambda) \to \mathcal{H}(A)$ is injective, then so is the map $\mathcal{H}(\mathrm{End}_\Lambda(P)) \to \mathcal{H}(\mathrm{End}_A(P \otimes K))$.

In the case where Λ is hereditary, this result also follows directly from Theorem 1.1 and the fact that $\mathrm{End}_\Lambda(P)$ is hereditary as well [14, Theorem 40.21].

4. Group rings and G-forms over local rings

We now study the case of group rings $\mathcal{O}G$, with the involution which sends each element of the finite group G to its inverse, where as before $\mathcal{O}$ is a complete discrete valuation ring. We shall assume throughout this section that $|G|$ is not zero in $\mathcal{O}$.

We recall that for any $\mathcal{O}G$-module M, we can identify canonically the set of hermitian forms on M with the set of G-invariant symmetric $\mathcal{O}$-bilinear forms on M

via the isomorphism $\phi : \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}) \to \mathrm{Hom}_{\mathcal{O}G}(M, \mathcal{O}G)$, functorial in M, given by $\phi(f)(x) = \sum_{g\in G} f(g^{-1}x)g$ (see, for instance, [10]).

Lemma 4.1. *Let G be a finite group and let k be any field. If the order of G is odd, then the only self-dual absolutely simple kG-module is the trivial module k.*

Proof. Suppose first that $\mathrm{char}(k) = 0$. Let χ be an irreducible character of G satisfying the self-duality condition $\chi(g) = \chi(g^{-1})$ for $g \in G$. Let χ_0 be the unit character. To show that $\chi = \chi_0$, it will be enough to show that the inner product $< \chi_0, \chi >$ is nonzero. On the one hand, the sum $\sum_{g\neq 1} \chi(g)$ is divisible by 2, since each term in the sum appears twice by self-duality. On the other hand, it is well-known that $\chi(1)$ divides $|G|$ (see, for instance, [16, Section 6.5, Proposition 17]), which implies in particular that $\chi(1)$ is odd. Hence

$$\begin{aligned} < \chi, \chi_0 > &= \frac{1}{|G|}\sum_{g\in G} \chi(g) \\ &\equiv 1 \pmod 2 . \end{aligned}$$

In particular, $< \chi, \chi_0 > \neq 0$. (See also [16, Section 13.2 Exercise 1]).

Suppose now that $\mathrm{char}(k) = p > 0$. We can assume without loss of generality that k is a finite field. Let K be a local field whose residue field is k. We can also assume that K contains all $|G|$-th roots of unity.

The group C_2 of order 2 acts naturally by duality on the Grothendieck groups $G_0(KG)$ and $G_0(kG)$. One verifies readily that the canonical surjection $d : G_0(KG) \to G_0(kG)$ as well as its canonical section (see [16, Section 18.4] for the definitions) commute with the action of C_2. Hence d induces a surjection

$$d_* : \hat{H}^0(C_2, G_0(KG)) \twoheadrightarrow \hat{H}^0(C_2, G_0(kG)) .$$

Now, by the considerations in characteristic 0, we have $\hat{H}^0(C_2, G_0(KG)) = \mathbb{Z}/2\mathbb{Z}$, with the nontrivial element corresponding to the unit representation K. It is easy to see that k represents a nontrivial element of $\hat{H}^0(C_2, G_0(kG))$, so d_* is an isomorphism, which proves the Lemma. □

Corollary 4.2. *Let k be a field and let G be a group of odd order. Then $(kG/\mathrm{rad}\, kG)_{\mathrm{orth}} = k$.*

Proof. Let S be a simple component of $kG/\mathrm{rad}\, kG \simeq k \times S_1 \times \cdots \times S_r$, with $S \neq k$ and S stable under the involution. We extend the scalars to an algebraic closure $\bar{k}$ of k, and we decompose $S \otimes_k \bar{k} = B_1 \times \cdots \times B_s$ into simple components.

Now we consider the action of the involution on the components B_i. If $\tilde{B}_i = B_i$, we have a non-trivial self-dual simple $\bar{k}G$-module, which contradicts Lemma 4.1. So the components B_i are switched by the involution, and we can write $S \otimes_k \bar{k} = C \times C^{op}$. In particular, $\dim_{\bar{k}}(S \otimes_k \bar{k})^+ = \dim_{\bar{k}}(S \otimes_k \bar{k})^- = \frac{1}{2}\dim_{\bar{k}}(S \otimes_k \bar{k})$ so the involution is of type II on S. □

Proposition 4.3. *Let G be a finite group of odd order. The natural inclusion of group rings $\mathcal{O}G \hookrightarrow KG$ induces an injective map from $\mathcal{H}(\mathcal{O}G)$ to $\mathcal{H}(KG)$.*

Proof. By Corollary 4.2 we have $(\mathcal{O}G/\mathrm{rad}\,\mathcal{O}G)_{\mathrm{orth}} = (kG/\mathrm{rad}\,kG)_{\mathrm{orth}} = k$, so using Theorem 3.1 with $\Delta = \mathcal{O}$ and the augmentation map $\phi : \mathcal{O}G \to \mathcal{O}$ we conclude that the natural map $\mathcal{H}(\mathcal{O}G) \to \mathcal{H}(KG)$ is injective.

□

Proposition 4.4. *Let $p \neq 2$ be the characteristic of k, and let G be a group whose p-Sylow subgroup G_p is normal. Then the map $\mathcal{H}(\mathcal{O}G) \to \mathcal{H}(KG)$ is injective.*

Proof. If p does not divide the order of G, then $\mathcal{O}G$ is a maximal order [5, Proposition 27.1], so Theorem 1.1 applies. Otherwise we can take $\Delta = \mathcal{O}[G/G_p]$ in Theorem 3.1; then $\Delta/\mathrm{rad}\,\Delta = k[G/G_p] = \mathcal{O}G/\mathrm{rad}\,\mathcal{O}G$ since $k[G/G_p]$ is semisimple and $\mathrm{rad}\,\mathcal{O}G$ contains $\pi\mathcal{O}G$, where π denotes a uniformizing parameter for $\mathcal{O}$, and the elements $1 - g$ for $g \in G_p$, which are nilpotent mod π. □

Remark. Note that Proposition 4.4 covers the case of all finite abelian groups G.

Combining Propositions 4.3 and 4.4 with Theorem 3.3 we get the following result, which can be interpreted as a "hermitian" version of [16, Section 16.1, Corollary 2].

Theorem 4.5. *Let G be a finite group either of odd order or such that its p-Sylow subgroup G_p is normal, where p is the characteristic of k. Let (P, g) and (Q, h) be unimodular hermitian forms over OG, where P and Q are projective OG-modules. If $(P \otimes K, g)$ and $(Q \otimes K, h)$ are isometric over KG, then (P, g) and (Q, h) are isometric over OG.*

Proof. We have in particular that $P \otimes K$ and $Q \otimes K$ are KG-isomorphic, so by [16, Section 16.1, Corollary 2], we conclude that $P \simeq Q$ as OG-modules. By Propositions 4.3 and 4.4, the map $\mathcal{H}(\mathcal{O}G) \to \mathcal{H}(KG)$ is injective; hence, by Theorem 3.3, the forms (P, g) and (Q, h) are isometric over OG. □

We now give a Grothendieck group interpretation of Theorem 4.5, which generalizes [2, Theorem 3.5] to a larger class of groups.

For a ring with involution R ($R = \mathcal{O}G$ or $R = KG$ in what follows) we denote by $KU_0(R)$ the Grothendieck group of the category of unimodular hermitian forms on finitely generated projective modules over R. If (M, h) is such a form, we will denote by $[M, h]$ the element of $KU_0(R)$ that it represents.

Theorem 4.6. *With the same hypotheses as in Theorem 4.5, the canonical homomorphism $\iota : KU_0(\mathcal{O}G) \to KU_0(KG)$ induced by extension of scalars is injective.*

Proof. Let ξ be an element of $\ker \iota$. We write ξ as a formal difference $\xi = [P, h] - [Q, g]$. It is known, and easy to see, that the isometry class of a form over KG is completely determined by its class in $KU_0(KG)$, so $(P \otimes K, h) \simeq (Q \otimes K, g)$. Since P and Q are projective modules over $\mathcal{O}G$, we conclude by [16, Section 16.1, Corollary 2], that $P \simeq Q$ as $\mathcal{O}G$-modules. Applying Theorem 4.5, we have $(P, h) \simeq (Q, g)$ as hermitian forms over $\mathcal{O}G$. Hence $\xi = 0$ as claimed. □

Finally, we give an application to the existence of integral orthonormal bases permuted by G. The following statement generalizes Corollary (2.4) in [6] to nonabelian groups:

Corollary 4.7. *Let G be a finite group as in Theorem 4.5. Let $b : \mathcal{O}G \times \mathcal{O}G \to \mathcal{O}$ be the G-invariant symmetric $\mathcal{O}$-bilinear form defined by $b(g,h) = \delta_{g,h}$ for $g, h \in G$. Let $M \subset KG$ be a free $\mathcal{O}G$-lattice self-dual with respect to b. Then M has an orthonormal $\mathcal{O}$-basis permuted by G.*

Proof. There is an element $m \in KG^\times$ such that $M = \mathcal{O}Gm$. Computing the dual of M for the unit form, we get $M^\sharp = \mathcal{O}G\tilde{m}^{-1}$, so since M is self-dual, $\mathcal{O}Gm = \mathcal{O}G\tilde{m}^{-1}$ and hence $\mathcal{O}Gm\tilde{m} = \mathcal{O}G$ so $m\tilde{m} \in \mathcal{O}G^\times$ and in fact $m\tilde{m} \in \mathcal{H}(\mathcal{O}G)$. Now by construction, $m\tilde{m} \sim 1 \in \mathcal{H}(KG)$, and by the injectivity of $\mathcal{H}(\mathcal{O}G) \hookrightarrow \mathcal{H}(KG)$, this means that $m\tilde{m} \sim 1 \in \mathcal{H}(\mathcal{O}G)$, so there is an element $n \in \mathcal{O}G^\times$ such that $n\tilde{n} = m\tilde{m}$. Let $w = n^{-1}m$; then we have $\mathcal{O}Gw = \mathcal{O}Gm$ and $w\tilde{w} = n^{-1}m\tilde{m}\tilde{n}^{-1} = 1$, so right-multiplication by w is an isometry from $(\mathcal{O}G, < 1 >)$ to $(M, < 1 >)$, or equivalently, a G-equivariant isometry of $\mathcal{O}$-modules between $(\mathcal{O}G, b)$ and (M, b). □

As an application, we give a different proof of the the following result found in Erez–Taylor [7, Section 3].

Corollary 4.8 (Erez–Taylor)**.** *Let L/K be a tamely ramified Galois extension of odd degree. Let $A_{L/K} = \mathfrak{D}_{L/K}^{-1/2}$, where $\mathfrak{D}_{L/K}$ is the different of L/K. Then $A_{L/K}$ has a self-dual normal basis over $\mathcal{O}$.*

Proof. It is known that L has a normal basis over K that is self-dual with respect to the trace form (Bayer-Lenstra [4]), that is, $(L, \mathrm{Tr}_{L/K}) \simeq (KG, b)$ as G-forms, where b is as in Corollary 4.7. Moreover, $A_{L/K}$ is self-dual with respect to $\mathrm{Tr}_{L/K}$, and $A_{L/K}$ is a projective $\mathcal{O}G$-module if L/K is tamely ramified, by [17, Proposition 1.3], and hence isomorphic to $\mathcal{O}G$ by [16, Section 16.1, Corollary 2]. So, by Corollary 4.7, $A_{L/K}$ has a self-dual (orthonormal) normal basis.

□

Acknowledgments

The first–named author would like to thank the Laboratoire de mathématiques of the Université de Besançon, where she worked during the preparation of this paper, for its warm hospitality.

References

1. A. Bak, *K-theory of forms*, Princeton University Press, 1981.
2. A. Bak and W. Scharlau, *Grothendieck and Witt groups of orders and finite groups*, Inventiones Math. **23** (1974), 207–240.
3. E. Bayer-Fluckiger and L. Fainsilber, *Non unimodular hermitian forms*, Inventiones Math. **123** (1996), 233–240.
4. E. Bayer-Fluckiger and H.W. Lenstra Jr., *Forms in odd-degree extensions and self-dual normal bases*, Am. J. Math. **112** (1990), 357–373.
5. C.W. Curtis and I Reiner, *Methods of representation theory, with applications to finite groups and orders*, vol. I, Wiley, 1981.
6. B. Erez and J. Morales, *The hermitian structure of rings of integers in odd degree abelian extensions*, J. of Number Theory **40** (1992), 92–104.
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. L. Fainsilber, *Formes hermitiennes sur des algèbres sur des anneaux locaux*, Publications Mathématiques de Besançon (1994).
9. ______, *Formes hermitiennes sur les algèbres p-adiques*, Ph.D. thesis, Université de Franche-Comté, 1994.
10. A. Fröhlich and A.M. McEvett, *Forms over rings with involutions*, J. Algebra **12** (1969), 79–104.
11. M.-A. Knus, A. Merkurev, M. Rost, and J.-P. Tignol, *The book of involutions*, to appear.
12. H.-G. Quebbemann, R. Scharlau, W. Scharlau, and M. Schulte, *Quadratische Formen in additiven Kategorien*, Bull. Soc. Math. France **48** (1976), 93–101.
13. H.-G. Quebbemann, W. Scharlau, and M. Schulte, *Quadratic and hermitian forms in additive and abelian categories*, J. Algebra **59** (1979), 264–289.
14. I. Reiner, *Maximal orders*, Acad. Press, London, 1975.
15. W. Scharlau, *Quadratic and hermitian forms*, Grundlehren der mathematischen Wissenschaften, vol. 270, Springer-Verlag, 1985.
16. J.-P. Serre, *Représentations linéaires des groupes finis*, 3ème édition corrigée ed., Hermann, Paris, 1978.
17. S. Ullom, *Normal bases in Galois extensions of number fields*, Nagoya Math J. **34** (1969), 153–167.

Chalmers tekniska högskola och Göteborgs universitet, Sektionen för matematik, S-412 96, Göteborg, Sweden
E-mail address: laura@math.chalmers.se

Louisiana State University, Department of Mathematics, Baton Rouge, LA, 70808, USA
E-mail address: morales@math.lsu.edu