JOURNAL OF ALGEBRA 168, 314–339 (1994)

Projective Group Representations and Centralizers: Character Theory

L. DELVAUX AND E. NAUWELAERTS

Department of Mathematics, University of Limburg, L.U.C., 3590 Diepenbeek, Belgium

Communicated by Walter Feit

Received July 20, 1992

INTRODUCTION

In [9] we studied the relationship between indecomposable modules over the twisted group rings $R_{*\alpha}G$, $R_{*\alpha}H$ and the centralizer S of $R_{*\alpha}H$ in $R_{*\alpha}G$, where R is a commutative ring (satisfying suitable conditions), G is a finite group with $|G|^{-1} \in R$ and $H < G$. These results are reviewed and sharpened in Section 1 and the corresponding character theory is developed in Section 2. This generalizes results of Karlof [6] and Travis [11]. This work can also be viewed as an extension of Clifford theory (dealing with normal subgroups). In Section 2 we present one of Clifford's theorems for indecomposable modules over twisted group rings.

Furthermore, we derive orthogonality relations for trace functions on S and we express primitive central idempotents of S in terms of trace functions (Section 3). These results are presented in a more general context, namely for Frobenius algebras over rings.

Section 4 deals with indecomposable modules and trace functions for algebras of the form $\varepsilon A\varepsilon$, ε being an idempotent. We also focus on the relation between S and $\varepsilon(R_{*\alpha}G)\varepsilon$, where ε is a primitive idempotent of $R_{*\alpha}H$.

Throughout this paper rings are assumed to have a unit element and modules are unitary. For details on separable algebras we refer the reader to [3].

0021-8693/94 $6.00
Copyright © 1994 by Academic Press, Inc.
All rights of reproduction in any form reserved.

1. Preliminaries; Modules over Centralizers

Throughout this paper R is a commutative ring. A ring is said to be connected if 0 and 1 are the only idempotent elements. We begin with some useful facts about indecomposable modules.

Let A be an R-algebra and suppose that R is connected. We first remark that any left A-module which is finitely generated and projective as R-module is a finite direct sum of indecomposable left A-modules (use rank_R). Now assume that A is finitely generated and projective as an R-module. Then there exist primitive central orthogonal nonzero idempotents $e_1, \ldots, e_s$ in A such that $1 = e_1 + \ldots + e_s$. Moreover, each central nonzero idempotent of A is uniquely a sum of some e_i. If M is an indecomposable left A-module, then there is a unique i such tht $e_iM \neq 0$ and we say that M lies over e_i. In addition, suppose that A is a separable R-algebra. Then a left A-module is projective as an R-module if and only if it is projective as an A-module, cf. [3, p. 48]. Further, if R is semilocal, then any two indecomposable finitely generated projective left A-modules lying over the same primitive central idempotent of A are isomorphic as A-modules; see [4, Theorem 1] and [9, Note 3.4]. In this case, it is easily seen that a left A-module, which is finitely generated and projective over R, is uniquely expressible as a finite direct sum of indecomposable left A-modules (up to isomorphism).

We now assume that R is a *splitting ring* for A (or A is split separable); that is, $A \cong \text{End}_R(M_1) \oplus \ldots \oplus \text{End}_R(M_s)$ as R-algebras, where $M_1, \ldots, M_s$ are finitely generated projective faithful R-modules. Recall that finitely generated projective nonzero modules over connected commutative rings are always faithful, see [3, p. 8]. Note also that the center of A is a free R-module of rank s. Obviously M_i can be viewed as a left A-module by setting $(\varphi_1, \ldots, \varphi_s) \cdot m = \varphi_i(m)$, where $m \in M_i$ and $\varphi_j \in \text{End}_R(M_j)$. Since R is connected, each M_i is an indecomposable left A-module, and they are not isomorphic as such. If finitely generated projective R-modules are free, for example, when R is semilocal or a principal ideal domain, then $M_1, \ldots, M_s$ are, up to isomorphism, all the indecomposable left A-modules which are finitely generated and projective; see [8, Proposition 1.8]. Moreover, in this case, any left A-module which is finitely generated and projective over R is uniquely expressible as a finite direct sum of indecomposable left A-modules.

Furthermore, note that a separable K-algebra E, where K is a field, is semisimple and then indecomposable left E-modules are simple.

We also need the following results.

1.1. *Note.* Let $B \subset A$ be R-algebras with $1_A \in B$. Let V be a left B-module and W a left A-module. Then $\text{Hom}_B(V, W) \cong \text{Hom}_A(A \otimes_B V, W)$ as R-modules.

Indeed, it is easily seen that $\mathrm{Hom}_B(V, W) \to \mathrm{Hom}_A(A \otimes_B V, W)$: $\varphi \mapsto \psi$, with $\psi(a \otimes v) = a\varphi(v)$ for $a \in A$, $v \in V$, is an isomorphism of R-modules.

1.2. PROPOSITION. *Let A be an R-algebra and B a subalgebra of A with $1_A \in B$. Suppose R is connected, R is a splitting ring for B, and finitely generated projective R-modules are free. Let N, resp., M, be an indecomposable left B-module, resp., A-module, which is finitely generated projective over R.*

(1) *Let V be a left B-module which is finitely generated projective over R, and let k be the multiplicity of N in a decomposition of V into indecomposable B-modules. If $k \neq 0$, then* $\mathrm{Hom}_B(N, V)$ *and* $\mathrm{Hom}_B(V, N)$ *are free R-modules of rank k. Otherwise, they are zero.*

(2) *Suppose R is also a splitting ring for A. Then the multiplicity of N in M, viewed as a B-module, is equal to the multiplicity of M in $A \otimes_B N$ (multiplicity in a decomposition into indecomposables).*

Proof. (1) Let $V = L_1 \oplus \ldots \oplus L_n$ be a decomposition into indecomposable left B-modules L_i. Now $\mathrm{Hom}_B(N, V) \cong \oplus_{i=1}^n \mathrm{Hom}_B(N, L_i)$ as R-modules. If L_i is not isomorphic to N in B-mod, then L_i and N lie over distinct primitive central idempotents of B, whence $\mathrm{Hom}_B(N, L_i) = 0$. Moreover, $\mathrm{Hom}_B(N, N) = RI$, see [8, 1.7].

(2) Clearly, $A \otimes_B N$ is projective over A and R. Combine assertion (1) and Note 1.1. ∎

We now recall some elementary facts about twisted group rings. Let G be a group and α a 2-cocycle in $\mathfrak{Z}^2(G, U(R))$, where $U(R)$ is the group of units of R and G acts trivially on R. The corresponding twisted group ring is denoted by $R *_\alpha G$. As R-module, $R *_\alpha G$ is freely generated by symbols $\{u_g \mid g \in G\}$ and multiplication is defined by $(au_x) \cdot (bu_y) = \alpha(x, y)abu_{xy}$ for $a, b \in R$, $x, y \in G$.

Let $H < G$. An element $g \in G$ is said to be *α-H-regular* if $\alpha(g, x) = \alpha(x, g)$ for all $x \in C_H(g)$ (the centralizer). Clearly, an α-H-regular element is β-H-regular for each 2-cocycle β equivalent to α. From [9, 1.1] we retain the following: if $g \in G$ is α-H-regular, then g^{-1} and hgh^{-1}, $h \in H$, are α-H-regular. Moreover, in the case $H \lhd G$, xgx^{-1} is α-H-regular for all $x \in G$.

Furthermore, to α we associate a map f_α: $G \times G \to U(R)$: $(x, g) \mapsto \alpha(x, g)\alpha(xgx^{-1}, x)^{-1}$. Obviously, $u_x u_g (u_x)^{-1} = f_\alpha(x, g) u_{xgx^{-1}}$ for $x, g \in G$. From [9, 1.2 and 1.3] we retain the following.

1.3. LEMMA. *Given $H < G$ and $\alpha \in \mathfrak{Z}^2(G, U(R))$, then*

(1) *there is a 2-cocycle β equivalent to α satisfying $\beta(e, e) = 1$ and $f_\beta(x, g) = 1$ for all β-G-regular $g \in G$ and all $x \in G$, as well as for all β-H-regular $g \in G$ and all $x \in H$.*

(2) *With β as above, we have $\beta(g, g^{-1}) = \beta(xgx^{-1}, xg^{-1}x^{-1})$ for all β-G-regular $g \in G$ and all $x \in G$, as well as for all β-H-regular $g \in G$ and all $x \in H$.*

Next, we consider the centralizer S of $R*_\alpha H$ in $R*_\alpha G$, where $H < G$; i.e., $S = \{a \in R*_\alpha G \mid \forall b \in R*_\alpha H\colon ab = ba\}$. We now assume that G is a finite group and, for any α-H-regular $g \in G$, we put $E_g = \{hgh^{-1} \mid h \in H\}$ and $s_g = \sum_{x \in E_g} u_x$. Further, $|H|^{-1} \in R$ means that $|H|$ is invertible in R. The following is shown in [9, 1.4].

1.4. PROPOSITION. *Assume that $f_\alpha(h, g) = 1$ for all α-H-regular $g \in G$ and all $h \in H$ (see 1.3). Then the α-H-regular subclass sums s_g form an R-basis for S in the following cases:* (i) $\alpha = 1$, (ii) *R is a domain,* (iii) *R is connected and $|G|^{-1} \in R$.*

Note. If $H \lhd G$ and α has been modified as in 1.4, then it is easily verified that $u_x s_g (u_x)^{-1} = f_\alpha(x, g) s_{xgx^{-1}}$ for all α-H-regular $g \in G$ and all $x \in G$.

Recall that in case $|G|^{-1} \in R$, $R*_\alpha G$ is separable over R. In [9, 1.6] we proved the following.

1.5. PROPOSITION. *Let either R be connected or $\alpha = 1$. If $|G|^{-1} \in R$, then S is a separable R-algebra.*

1.6. *Note.* Suppose R is connected and $|G|^{-1} \in R$. Let $m = \exp(G)$ and let η be a primitive mth root of unity. Then $T = R[\eta]$ is a splitting ring for the group ring TG, cf. [10]. Since an extension of a splitting ring is a splitting ring, we can see that T is also a splitting ring for TH, where $H < G$. In [7, 3.1 and 3.3] we constructed a splitting ring L for a twisted group ring. Again, this ring L is a splitting ring for subgroups, see also [9, 2.1]. For centralizers we refer to 1.7.

We now focus on the relationship between indecomposable modules over $R*_\alpha G$, $R*_\alpha H$, and S. However, we present the results in a more general context. Let A be an R-algebra, B a subalgebra of A with $1_A \in B$, and let S be the centralizer of B in A. Suppose R is connected, finitely generated projective R-modules are free, and A and B are split separable over R (i.e., R is a splitting ring for A and B). Let $M_1, \ldots, M_s$, resp., $N_1, \ldots, N_t$, be a basic set of indecomposable left A-modules, resp., B-modules, which are finitely generated projective over R. Let $\{e_1, \ldots, e_s\}$, resp., $\{f_1, \ldots, f_t\}$, be the set of primitive central nonzero idempotents of A, resp., B, and assume that M_j lies over e_j and N_i over f_i. Further, let c_{ij} denote the multiplicity of N_i in a decomposition of $M_j|_B$ into indecomposable left B-modules. In [9, 2.4, 2.6] it is shown that S is a free R-module of rank $\sum_{j=1}^{s} \sum_{i=1}^{t} c_{ij}^2$ (compare with 1.4). Moreover, S is separable over R, see [9, 2.5]. Now put $P_{ij} = \mathrm{Hom}_B(N_i, M_j)$. If $c_{ij} = 0$, then $P_{ij} = 0$; otherwise, P_{ij}

is a free R-module of rank c_{ij}, see Proposition 1.2(1). Further, P_{ij} is a left S-module under the operation $(s \cdot \varphi)(n) = s(\varphi(n))$ for $s \in S$, $\varphi \in P_{ij}$, $n \in N_i$. Note that $N_i \cong B\varepsilon_i$ in B-mod for some primitive idempotents ε_i of B, and $\mathrm{Hom}_B(B\varepsilon_i, M_j) \to \varepsilon_i M_j$: $\varphi \mapsto \varphi(\varepsilon_i)$ is an isomorphism of left S-modules. From [9, 3.5, 3.8, and 3.7] we retain the following.

1.7. THEOREM. (1) *In addition, assume that R is either semilocal or a principal ideal domain. Then each nonzero P_{ij} is an indecomposable left S-module. The nonzero f_ie_j are precisely the distinct primitive central idempotents of S. Furthermore, $P_{ij} \neq 0$ if and only if $f_ie_j \neq 0$, and, in this case, P_{ij} lies over f_ie_j.*

(2) *If R is semilocal, then R is a splitting ring for S.*

1.8. THEOREM. (1) *We have $M_j \cong \oplus_i P_{ij}^{\mathrm{rank}\, N_i}$ as left S-module, where the sum is taken over those i for which $c_{ij} \neq 0$.*

(2) *If R is semilocal and $c_{ij} \neq 0$, then we have $A \otimes_S P_{ij} \cong M_j^{\mathrm{rank}\, N_i}$ and $(A \otimes_B N_i) \otimes_S P_{ij} \cong M_j$ as left A-modules, where $A \otimes_B N_i$ is made into a right S-module by $(a \otimes n)s = as \otimes n$ for $a \in A$, $n \in N_i$, $s \in S$.*

(3) *If R is semilocal and $c_{ij} \neq 0$, then $\mathrm{Hom}_S(P_{ij}, M_j) \cong N_i$ as left B-modules, where $(b \cdot \varphi)(p) = b(\varphi(p))$ for $b \in B$, $\varphi \in \mathrm{Hom}_S(P_{ij}, M_j)$, $p \in P_{ij}$.*

Proof. (1) Let i be such that $c_{ij} \neq 0$. Write f_i as a sum of primitive orthogonal nonzero idempotents of B, say $f_i = \varepsilon_1 + \dots + \varepsilon_k$. By the hypotheses, $N_i \cong B\varepsilon_l$ in B-mod for $l = 1, \dots, k$ and $k = \mathrm{rank}_R(N_i)$. Now $f_iM_j = \varepsilon_1 M_j \oplus \dots \oplus \varepsilon_k M_j$ and $\varepsilon_l M_j \cong P_{ij}$ in S-mod for $l = 1, \dots k$. Moreover, $f_iM_j \neq 0$ if and only if $c_{ij} \neq 0$, and $M_j = \oplus_i f_iM_j$.

(2) The first statement follows from (1) and Proposition 1.2(2) and the second statement is proved in [9, 3.11].

(3) By Proposition 1.2(1), $\mathrm{Hom}_S(P_{ij}, M_j)$ is a free R-module with rank equal to $\mathrm{rank}_R(N_i)$. Moreover, $f_l\mathrm{Hom}_S(P_{ij}, M_j) \neq 0$ if and only if $l = i$, and the assertion follows. ∎

To conclude, we recall some basic facts about trace functions. Let A be an R-algebra and V a left A-module which is finitely generated and projective over R. Let $\{v_1, \dots, v_n\} \subset V$, $\{\varphi_1, \dots, \varphi_n\} \subset \mathrm{Hom}_R(V, R)$ be an R-dual basis for V. The *trace function* (or character) from A to R afforded by V, notation t_V, is defined as follows: $t_V(a) = \sum_{i=1}^n \varphi_i(av_i)$, for all $a \in A$. It is easily seen that t_V does not depend on the choice of the dual basis. Further, $t_V(xy) = t_V(yx)$ for all $x, y \in A$, and if R is connected, then $t_V(1) = \mathrm{rank}_R(V)1_R$; see [8, 2.5].

Now let $A = R_{*\alpha}G$. Adapting the proof of [8, 3.3] (as in [9, 1.4]), we obtain the following result. Let $H < G$ and assume that either R is a domain or $|G|^{-1} \in R$ and R is connected. Then $t_V(u_g) = 0$ for each non-α-H-regular $g \in G$.

2. Clifford Theory for Arbitrary Subgroups

We begin by reviewing Clifford's theorem for normal subgroups. The original version deals with simple modules over group rings; see e.g., [2, p. 259], but here we are concerned with indecomposable modules over twisted group rings. We first require some preliminary remarks. R is a commutative ring throughout.

2.1. *Remarks.* Let G be a group and consider the twisted group ring $R_{*\alpha}G$ with R-basis $\{u_g \mid g \in G\}$. Let $H \lhd G$ and set $B = R_{*\alpha}H$.

1. Let N be a left B-module, $g \in G$, and form $u_g B \otimes_B N = u_g \otimes N$. Clearly any element of this product is uniquely expressible as $u_g \otimes n$, $n \in N$, and $u_g \otimes N \cong N$ as R-modules. Since $H \lhd G$, there is a left B-module structure on $u_g \otimes N$, to be explicit, for any $h \in H$, $n \in N$: $u_h(u_g \otimes n) = u_g \otimes f_\alpha(g, g^{-1}hg)^{-1}u_{g^{-1}hg}n$.
Further, if N is an indecomposable left B-module, then so is $u_g \otimes N$ and conversely. If N is a B-submodule of $M_{|_H}$ for some left $R_{*\alpha}$ G-module M, then $u_g N$ is also a B-submodule of $M_{|_H}$, and $u_g N \to u_g \otimes N : u_g n \mapsto u_g \otimes n$ is an isomorphism of B-modules.

2. Keep the above notation. If N is finitely generated and projective over R with dual basis $\{n_1, \ldots, n_k\} \subset N$, $\{\varphi_1, \ldots, \varphi_k\} \subset \mathrm{Hom}_R(N, R)$, then $\{u_g \otimes n_i\}$, $\{\bar{\varphi}_i\}$, with $\bar{\varphi}_i : u_g \otimes N \to R : u_g \otimes n \mapsto \varphi_i(n)$, is a dual basis for $u_g \otimes N$. Using this, we have $t_{u_g \otimes N}(u_h) = f_\alpha(g, g^{-1}hg)^{-1} t_N(u_{g^{-1}hg})$ for all $h \in H$.

3. Let f be a primitive central idempotent of $R_{*\alpha}H$. Then it is easily verified that, for any $g \in G$, $u_g f(u_g)^{-1}$ is also a primitive central idempotent of $R_{*\alpha}H$.

2.2. Proposition. *Let R be connected, let H be a normal subgroup of a finite group G and M an indecomposable left $R_{*\alpha}$ G-module which is finitely generated and projective as an R-module.*

We may write $M_{|_H} = L_1 \oplus \ldots \oplus L_q$ where each L_i is an indecomposable left $R_{*\alpha}$ H-module. Let f_1 be the primitive central idempotent of $R_{*\alpha}$ H corresponding to L_1, let W_1 denote the direct sum of all L_i lying over f_1, and set $F = \{g \in G \mid u_g W_1 = W_1\}$. Then the following hold:

(1) $M_{|_H} = \oplus_{i=1}^r u_{g_i} W_1$ where $\{g_1, \ldots, g_r\}$ is a set of left coset representatives of F in G.

(2) $M \cong R_{*\alpha}$ $G \otimes_{R_{*\alpha}F} W_1$ as left $R_{*\alpha}$ G-module, and W_1 is an indecomposable left $R_{*\alpha}$ F-module.

Proof. (1) Let $\{f_1, \ldots, f_m\}$ be the set of all primitive central idempotents in $R_{*\alpha}$ H for which $f_j M \neq 0$, and let W_j, $j = 1, \ldots, m$, denote the direct sum of all L_i lying over f_j. Given $g \in G$ and W_j, we show that $u_g W_j = W_k$ for some $k \in \{1, \ldots, m\}$. Clearly $W_j = f_j M$ and thus $u_g W_j =$

$u_g f_j(u_g)^{-1} u_g M = u_g f_j(u_g)^{-1} M$. Now $u_g f_j(u_g)^{-1}$ is a primitive central idempotent of $R*_\alpha H$ which does not annihilate M. Thus $u_g f_j(u_g)^{-1} = f_k$ for some k and $u_g W_j = f_k M = W_k$. In fact, multiplication by u_g defines an action of G on $\{W_1, \ldots, W_m\}$. Consider the distinct G-orbits and let $T_1, \ldots, T_n$ denote the direct sums of their elements. We have $M = W_1 \oplus \ldots \oplus W_m = T_1 \oplus \ldots \oplus T_n$. It is easy to see that each T_j is an $R*_\alpha G$-submodule of M. But M is indecomposable, hence $M = T_1 = \oplus_{i=1}^r u_{g_i} W_1$.

(2) Let $\{g_1, \ldots, g_r\}$ be as in (1). Clearly $R*_\alpha G$ is a free right $R*_\alpha F$-module with basis $\{u_{g_1}, \ldots, u_{g_r}\}$. Therefore any element of $R*_\alpha G \otimes_{R*_\alpha F} W_1$ is uniquely expressible as $\sum_{i=1}^r u_{g_i} \otimes w_i$ with $w_i \in W_1$. Using (1), it then follows that $R*_\alpha G \otimes_{R*_\alpha F} W_1 \to M$: $\sum_{i=1}^r u_{g_i} \otimes w_i \mapsto \sum_{i=1}^r u_{g_i} w_i$ is an isomorphism of left $R*_\alpha G$-modules.

Furthermore, since $R*_\alpha G \otimes_{R*_\alpha F} W_1$ is an indecomposable $R*_\alpha G$-module, W_1 will be an indecomposable left $R*_\alpha F$-module. ∎

2.3. THEOREM. *Keep the notation and hypotheses of Proposition* 2.2. *Assume further that* $|H|^{-1} \in R$ *and that either* R *is semilocal or* R *is a splitting ring for* $R*_\alpha H$ *and finitely generated projective* R*-modules are free. Let* N *be an indecomposable left* $R*_\alpha H$*-module which occurs with nonzero multiplicity* k *in* $M_{|H}$ *(say* $N \cong L_1$ *after rearrangement). Then we have*

$M_{|H} \cong \oplus_{i=1}^r (u_{g_i} \otimes_{R*_\alpha H} N)^k$ *as left* $R*_\alpha H$*-modules, where* $\{g_1, \ldots, g_r\}$ *is a set of left coset representatives of* F *in* G*, and* $F = \{g \in G \mid u_g \otimes N \cong N$ *in* $R*_\alpha H$-mod$\}$.

Proof. By the hypotheses on H and R, $W_1 \cong N^k$ as $R*_\alpha H$-modules and $u_g W_1 = W_1$ if and only if $u_g \otimes N \cong N$ in $R*_\alpha H$-mod (see Section 1). We now apply Proposition 2.2 (1). ∎

2.4. COROLLARY. *We keep the notation and hypotheses of Theorem* 2.3 *and we modify* α *as in Lemma* 1.3. *Then for each* α*-*G*-regular* $h \in H$ *we have*

$$(1) \quad t_M(u_h) = k \sum_{i=1}^{r} t_N(u_{g_i^{-1} h g_i}).$$

$$(2) \quad |F| t_M(u_h) = k \sum_{g \in G} t_N(u_{g^{-1} h g}).$$

Proof. (1) This follows from Theorem 2.3 and Remark 2.1(2).

(2) Let $g \in G$, then there is a unique g_i and an $x \in F$ such that $g = g_i x$. It is easily seen that $u_g \otimes N \cong u_{g_i} \otimes (u_x \otimes N) \cong u_{g_i} \otimes N$ as left $R*_\alpha H$-modules. So, by the choice of α, we have $t_N(u_{g^{-1}hg}) = t_N(u_{g_i^{-1}hg_i})$ for any α-G-regular $h \in H$. ∎

2.5. COROLLARY. *With notation and hypotheses as in Theorem* 2.3, *we have*

$$\operatorname{rank}_R M = k[G\colon F] \operatorname{rank}_R N.$$

Proof. Follows from Theorem 2.3 and the fact that $u_{g_i} \otimes N \cong N$ as R-modules. ∎

2.6. *Note.* Consider a subgroup K of a finite group G. Let N be a left $R*_\alpha K$-module which is finitely generated and projective over R and set $N^G = R*_\alpha G \otimes_{R*_\alpha K} N$. Let $\{g_1, \ldots, g_m\}$ be a set of left coset representatives of K in G.

Obviously $R*_\alpha G$ is a free right $R*_\alpha K$-module with basis $\{u_{g_1}, \ldots, u_{g_m}\}$. Therefore any element of N^G is uniquely expressible as $\sum_{i=1}^m u_{g_i} \otimes n_i$ with $n_i \in N$. So if $\{v_1, \ldots, v_l\} \subset N$, $\{\varphi_1, \ldots, \varphi_l\} \subset \operatorname{Hom}_R(N, R)$ is an R-dual basis for N, then $\{u_{g_i} \otimes v_j\}$, $\{\psi_{ij}\}$, with $\psi_{ij}\colon N^G \to R\colon \sum_{i=1}^m u_{g_i} \otimes n_i \mapsto \varphi_j(n_i)$, is an R-dual basis for N^G.

Define $\tilde{t}_N$ as follows: $\tilde{t}_N(u_g) = t_N(u_g)$ if $g \in K$ and $\tilde{t}_N(u_g) = 0$ if $g \notin K$. Using our dual bases, it is now easily checked that

$$t_{N^G}(u_g) = \sum_{i=1}^{m} f_\alpha(g_i, g_i^{-1} g g_i)^{-1} \tilde{t}_N(u_{g_i^{-1} g g_i}) \quad \text{for any } g \in G.$$

If we modify α as in Lemma 1.3, then we obtain

$$|K| t_{N^G}(u_g) = \sum_{x \in G} \tilde{t}_N(u_{x^{-1} g x}) \qquad \text{for any } \alpha\text{-}G\text{-regular } g \in G.$$

Furthermore, $N^G \cong N^m$ as R-modules. In particular, when R is connected, we have

$$\operatorname{rank}_R(N^G) = [G\colon K] \operatorname{rank}_R(N).$$

We now consider an arbitrary subgroup H of a finite group G. Further, let R be connected, $|G|^{-1} \in R$, and suppose that R is a splitting ring for $R*_\alpha H$ and $R*_\alpha G$ and that finitely generated projective R-modules are free. Let $M_1, \ldots, M_s$, resp., $N_1, \ldots, N_t$, be a basic set of indecomposable left $R*_\alpha G$-modules, resp., $R*_\alpha H$-modules, which are finitely generated projective over R, and let c_{ij} denote the multiplicity of N_i in a decomposition of $M_{j|H}$. Let S denote the centralizer of $R*_\alpha H$ in $R*_\alpha G$ and set $P_{ij} = \operatorname{Hom}_{R*_\alpha H}(N_i, M_j)$.

As pointed out in Section 1, P_{ij} is a left S-module and a free R-module of rank c_{ij} whenever $c_{ij} \neq 0$. Moreover, if $c_{ij} = 0$, then $P_{ij} = 0$. For the indecomposability of P_{ij} and the expression of M_j in terms of N_i and P_{ij} we refer the reader to Section 1, Theorems 1.7 and 1.8. Theorem 1.8 can be viewed as an alternative to Proposition 2.2 and Theorem 2.3. Here we concentrate on the character theory. We use the notation $Z(A)$ for the center of a ring A.

2.7. LEMMA. *With the above hypotheses and $c_{ij} \neq 0$, the following hold*:

(1) $M_j^{c_{ij}} \cong P_{ij}^{\text{rank}\, M_j}$ *as $Z(R*_\alpha G)$-modules.*

(2) $N_i^{c_{ij}} \cong P_{ij}^{\text{rank}\, N_i}$ *as $Z(R*_\alpha H)$-modules.*

Proof. Note that rank stands for rank_R. Let $\{e_1, ..., e_s\}$, resp., $\{f_1, ..., f_t\}$, be the set of primitive central nonzero idempotents of $R*_\alpha G$, resp., $R*_\alpha H$, and assume that M_j lies over e_j and N_i over f_i.

(1) It is clear that $e_k P_{ij} \neq 0$ if and only if $k = j$. So the restriction of P_{ij} to $Z(R*_\alpha G)$ is a finite direct sum of indecomposable $Z(R*_\alpha G)$-modules lying over e_j. By the hypotheses, $Z(R*_\alpha G)e_j = Re_j \cong R$ and $Z(R*_\alpha G)e_j$ is, up to isomorphism, the only indecomposable $Z(R*_\alpha G)$-module which is finitely generated and projective as an R-module and lies over e_j. Therefore $P_{ij} \cong (Z(R*_\alpha G)e_j)^l$ as a $Z(R*_\alpha G)$-module, and comparing ranks with respect to R, we obtain $l = c_{ij}$.

Similarly, we may show that $M_j \cong (Z(R*_\alpha G)e_j)^{\text{rank}\, M_j}$ as $Z(R*_\alpha G)$-modules and assertion (1) follows.

(2) Obviously, $f_k P_{ij} \neq 0$ if and only if $k = i$. We now proceed as in (1). ∎

2.8. *Note.* Let A be an R-algebra, B a subalgebra of A with $1_A \in B$, and S the centralizer of B in A. As above, let R be a connected ring for which finitely generated projective R-modules are free and suppose that R is a splitting ring for A and B. Then Lemma 2.7 remains true (with M_j, N_i, P_{ij}, and c_{ij} as before).

We use the following notation: for any $g \in G$, $E_g = \{hgh^{-1} \mid h \in H\}$, $K_g = \{ygy^{-1} \mid y \in G\}$, $s_g = \sum_{x \in E_g} u_x$, and $v_g = \sum_{x \in K_g} u_x$.

2.9. PROPOSITION. *We keep the above hypotheses and we modify α as in Lemma 1.3. Letting $c_{ij} \neq 0$, we have*

(1) $c_{ij} t_{M_j}(u_g) = |K_g|^{-1} \text{rank}_R M_j \, t_{P_{ij}}(v_g)$ *for any α-G-regular $g \in G$.*

(2) $c_{ij} t_{N_i}(u_h) = |E_h|^{-1} \text{rank}_R N_i \, t_{P_{ij}}(s_h)$ *for any α-H-regular $h \in H$.*

Proof. Apply Lemma 2.7 and use Proposition 1.4. ∎

We next derive a formula which relates t_{M_j}, t_{N_i}, and $t_{P_{ij}}$ and which can be viewed as an extension of Corollary 2.4.

2.10. PROPOSITION. *Keep the above hypotheses, modify* α *as in* 1.3, *and let* $c_{ij} \neq 0$. *Then for each* α-*G-regular* $h \in H$ *we have*

$$c_{ij} t_{M_j}(u_h) = |G|^{-1} \text{rank}_R M_j \left[c_{ij} (\text{rank}_R N_i)^{-1} \sum_{g \in J} t_{N_i}(u_{ghg^{-1}}) + t_{P_{ij}}\Big(\sum_{g \in G \setminus J} u_{ghg^{-1}} \Big) \right],$$

where $J = \{g \in G \mid ghg^{-1} \in H\}$.

Moreover, $t_{P_{ij}}(\sum_{g \in G \setminus J} u_{ghg^{-1}}) = \sum_{g \in G \setminus J} |E_{ghg^{-1}}|^{-1} t_{P_{ij}}(s_{ghg^{-1}})$.

Proof. We first note that $\text{rank}_R(N_i)$ is invertible in R by 3.16(1).

For any $k \in H$, we have $u_k(\sum_{g \in J} u_{ghg^{-1}})(u_k)^{-1} = \sum_{g \in J} u_{kgh(kg)^{-1}}$, because ghg^{-1} is α-G-regular, whence $\sum_{g \in J} u_{ghg^{-1}} \in Z(R*_\alpha H)$. On the other hand, $\sum_{g \in G} u_{ghg^{-1}} \in Z(R*_\alpha G)$ and thus $\sum_{g \in G \setminus J} u_{ghg^{-1}} \in Z(S)$. Now, $t_{M_j}(u_h) = |G|^{-1} t_{M_j}(\sum_{g \in G} u_{ghg^{-1}})$ because h is α-G-regular. Then, applying Lemma 2.7, we obtain

$$\begin{aligned} c_{ij} t_{M_j}(u_h) &= |G|^{-1} \text{rank}_R M_j \, t_{P_{ij}} \Big(\sum_{g \in G} u_{ghg^{-1}} \Big) \\ &= |G|^{-1} \text{rank}_R M_j \left[t_{P_{ij}} \Big(\sum_{g \in J} u_{ghg^{-1}} \Big) + t_{P_{ij}} \Big(\sum_{g \in G \setminus J} u_{ghg^{-1}} \Big) \right] \\ &= |G|^{-1} \text{rank}_R M_j \left[c_{ij} (\text{rank}_R N_i)^{-1} \sum_{g \in J} t_{N_i}(u_{ghg^{-1}}) \right. \\ &\quad \left. + \, t_{P_{ij}} \Big(\sum_{g \in G \setminus J} u_{ghg^{-1}} \Big) \right] \end{aligned}$$

Finally,

$$\sum_{g \in G \setminus J} |E_{ghg^{-1}}|^{-1} s_{ghg^{-1}} = |H|^{-1} \sum_{g \in G \setminus J} \sum_{k \in H} u_{kgh(kg)^{-1}} = \sum_{g \in G \setminus J} u_{ghg^{-1}}. \quad \blacksquare$$

2.11. *Remarks.* 1. If $H \lhd G$, then c_{ij} is invertible in R by Corollary 2.5 and Corollary 3.16(1) below, and we recover Corollary 2.4. The preceding proposition also generalizes results in [6].

2. Note also that $t_{M_j}(x) = \sum_i (\text{rank}_R N_i) t_{P_{ij}}(x)$ for all $x \in S$, where the sum is taken over those i for which $P_{ij} \neq 0$; see Theorem 1.8(1). So $(\text{rank}_R N_i) t_{P_{ij}}(x) = t_{M_j}(x f_i)$ for $x \in S$ and nonzero P_{ij} (with f_i as in 2.7).

3. Theorem 1.8 and Proposition 2.9 may be useful even for normal subgroups, for example when $F = G$ in Theorem 2.3. Compare with [2, Theorem 11.20] (Clifford).

4. Put $A = R*_\alpha G$ and $B = R*_\alpha H$. Under our assumptions, we have $N_i \cong B\varepsilon_i$ in B-mod for some primitive idempotents ε_i in B. Moreover, $\text{Hom}_B(B\varepsilon_i, M_j) \to \varepsilon_i M_j$: $\varphi \mapsto \varphi(\varepsilon_i)$ is an isomorphism of left S-modules.

Let now $\varepsilon_i M_j \neq 0$. Using R-dual bases for M_j and $\varepsilon_i M_j$, we see that $t_{M_j}(x\varepsilon_i) = t_{\varepsilon_i M_j}(x)$ for all $x \in S$, in particular $t_{M_j}(\varepsilon_i) = c_{ij} 1_R$.

On the other hand, $\varepsilon_i M_j$ may be viewed as a unitary left module over the ring $\varepsilon_i A \varepsilon_i \cong \mathrm{End}_A(A\varepsilon_i)^\circ$. If in addition R is semilocal, then $Sf_i \to \varepsilon_i A \varepsilon_i$: $sf_i \mapsto \varepsilon_i s \varepsilon_i$ is an R-algebra isomorphism (f_i as in 2.7); see [9, Corollary 4.9]. Later, in Section 4, we consider indecomposable modules and trace functions for rings of the form $\varepsilon A \varepsilon$ with ε an idempotent.

3. Orthogonality Relations

Our objective is to derive orthogonality relations for characters of the centralizer of $R_{*\alpha} H$ in $R_{*\alpha} G$, where $H < G$. However, we discuss this problem in a more general context. We first collect some results about Frobenius algebras over rings. Throughout, R is a commutative ring and A is a faithful R-algebra which is a finitely generated free R-module. Recall that a bilinear form b on A is associative if $b(xy, z) = b(x, yz)$ for all $x, y, z \in A$. Further, $\mathrm{Hom}_R(A, R)$ is a left A-module under the operation $(a \cdot \varphi)(x) = \varphi(xa)$ for $a, x \in A$, $\varphi \in \mathrm{Hom}_R(A, R)$. We now have the following.

3.1. Lemma. *The following statements are equivalent*:

(1) $A \cong \mathrm{Hom}_R(A, R)$ *as left A-modules.*

(2) *There is an associative bilinear form b: $A \times A \to R$ and there are R-bases $\{a_1, ..., a_n\}$, $\{b_1, ..., b_n\}$ in A such that $b(a_i, b_j)$ form an invertible matrix.*

(3) *There is an associative bilinear form b: $A \times A \to R$ such that for each R-basis $\{a_1, ..., a_n\}$ of A there exists an R-basis $\{b_1, ..., b_n\}$ in A with $b(a_i, b_j) = \delta_{ij}$.*

Proof. It is well known that there is a one-to-one correspondence between associative bilinear forms b: $A \times A \to R$ and (left) A-linear maps β: $A \to \mathrm{Hom}_R(A, R)$, and this correspondence is given by $b(x, y) = \beta(y)(x)$ for all $x, y \in A$. With the above notation we now prove the following.

(1) $\Rightarrow$ (3). Let $\{\varphi_1, ..., \varphi_n\} \subset \mathrm{Hom}_R(A, R)$ be the dual basis of $\{a_1, ..., a_n\}$. If β: $A \to \mathrm{Hom}_R(A, R)$ is an isomorphism, then there is an R-basis $\{b_1, ..., b_n\}$ in A such that $\beta(b_j) = \varphi_j$. So $b(a_i, b_j) = \beta(b_j)(a_i) = \delta_{ij}$.

(3) $\Rightarrow$ (2). This is obvious.

(2) $\Rightarrow$ (1). Again let $\{\varphi_k\}$ be the dual basis of $\{a_k\}$. Since $(b(a_i, b_j))_{ij}$ is the matrix of β with respect to the bases $\{b_k\}$ and $\{\varphi_k\}$, it follows that β is bijective. ∎

If A satisfies any one of the conditions of Lemma 3.1, then we say that A is a *Frobenius algebra*. A bilinear form satisfying the equivalent properties in (2) and (3) is said to be *nonsingular*. Note that $\{a_k\}$ and $\{b_k\}$ in (3) are called *dual bases* with respect to the bilinear form b. Finally, A is a *symmetric algebra* if there exists an associative nonsingular symmetric bilinear form on A.

3.2. *Remarks*. 1. We obtain equivalent conditions by replacing "left" with "right" in (1) or reversing the roles of $\{a_k\}$ and $\{b_k\}$ in (3).

2. A nonsingular bilinear form is nondegenerate. When R is a field, the converse is true.

3. Let b be an associative bilinear form on A and consider the corresponding left A-linear map β: $A \to \mathrm{Hom}_R(A, R)$. Obviously β is completely determined by $\beta(1) = \tau$ and $b(x, y) = \tau(xy)$ for all $x, y \in A$. Further, β is an isomorphism if and only if for all $\varphi \in \mathrm{Hom}_R(A, R)$ there is a unique $u \in A$ such that $\varphi = u \cdot \tau$ (compare with [5, p. 49]).

3.3. Lemma. *Let b and b' be associative bilinear forms on A and suppose that b is nonsingular, then*

(1) *there is a unique $u \in A$ such that $b'(x, y) = b(x, yu)$ for all elements $x, y \in A$.*

(2) *b' is nonsingular if and only if u is invertible in A.*

(3) *If b is symmetric, then b' is symmetric if and only if u is a central element of A.*

Proof. Let β, resp., β', denote the left A-linear maps from A to $\mathrm{Hom}_R(A, R)$ associated to b, resp., b'.

(1) Since b is nonsingular, β is an isomorphism. Therefore, as in Remark 3.2(3), there is a unique $u \in A$ such that $\beta'(1) = u \cdot \beta(1)$ and the assertion in (1) follows.

(2) If b' is nonsingular, then there is also a unique $v \in A$ such that $\beta(1) = v \cdot \beta'(1)$. So $\beta(1) = vu \cdot \beta(1)$, whence $vu = 1$. Similarly, we get $uv = 1$. Conversely, suppose u is invertible in A and let $\{a_k\}$, $\{b_k\}$ be dual bases in A with respect to b. Then it is clear that $\{a_k\}$, $\{b_k u^{-1}\}$ are dual bases with respect to b'.

(3) We have $b'(y, x) = b(y, xu) = b(x, uy)$. Thus b' is symmetric if and only if $b(x, yu) = b(x, uy)$ for all $x, y \in A$. The latter is equivalent to $yu = uy$ for all $y \in A$, because b is nondegenerate. ∎

Let now b be a nonsingular associative bilinear form on A with dual bases $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$ in A.

We put $z = z_b = \sum_{i=1}^{n} a_i b_i$; this element has the following properties.

3.4. LEMMA. *Let t_A denote the trace from A to R afforded by A viewed as left A-module, then $b(x, z) = t_A(x)$ for all $x \in A$.*

Moreover, if b is symmetric, then z is central and in this case we have $z = \sum_{i=1}^n b_i a_i$.

Proof. Let $x \in A$ and write $xa_i = \sum_{j=1}^n r_{ji} a_j$ with $r_{ji} \in R$. Then $b(x, z) = \sum_{i=1}^n b(xa_i, b_i) = \sum_{i=1}^n r_{ii} = t_A(x)$. The remaining statement follows from Lemma 3.3. ∎

3.5. *Note.* In view of the above lemma, z is independent of the choice of the dual bases for b. Let b' be another nonsingular associative bilinear form on A. Then by Lemma 3.3(2) we can find an invertible element $u \in A$ such that $z_b = z_{b'} u$.

Keep the above notation and let $Z(A)$ be the center of A. We consider the $Z(A)$-linear map $\zeta: A \to A: x \mapsto \sum_{i=1}^n b_i x a_i$.

3.6. PROPOSITION. *The set $\zeta(A)$ is an ideal of the center of A. Moreover, $\zeta(A)$ is independent of the choice of the dual bases and independent of the choice of the nonsingular associative bilinear form.*

Proof. For each $y \in A$, we have that

$$a_i y = \sum_{j=1}^n r_{ji} a_j \quad \text{implies} \quad y b_i = \sum_{j=1}^n r_{ij} b_j \qquad r_{ij} \in R. \tag{$*$}$$

Using these relations, we see that $\zeta(A)$ is contained in the center of A. It is also clear that $\zeta(A)$ is an ideal of the center.

Further, $\zeta(A)$ is independent of the choice of the dual bases. So let $\{a_i'\}$, $\{b_i'\}$ be another pair of dual bases with respect to b. If C and D are the matrices expressing $\{a_i'\}$ in terms of $\{a_i\}$ and $\{b_i'\}$ in terms of $\{b_i\}$, respectively, then $C^t D = I_n$. Thus also $DC^t = I_n$ and this yields that $\sum_{i=1}^n b_i' x a_i' = \sum_{i=1}^n b_i x a_i$ for all $x \in A$. Finally, from Lemma 3.3(2) it follows that $\zeta(A)$ is independent of the choice of the bilinear form b. ∎

3.7. PROPOSITION. *If A is a Frobenius R-algebra such that $1 \in \zeta(A)$, then A is a separable R-algebra.*

Proof. Keep the notation of 3.6. By our assumption, there is an element $c \in A$ such that $\sum_{i=1}^n b_i c a_i = 1$. Combining this relation with the relations $(*)$ in Proposition 3.6, we see that $\sum_{i=1}^n b_i c \otimes a_i \in A \otimes_R A^\circ$ is a separability idempotent for A, cf. [3, p. 40]. ∎

3.8. EXAMPLES. 1. Consider a finite group G and the twisted group ring $R *_\alpha G$ with R-basis $\{u_g \mid g \in G\}$. Take the R-linear map $\tau: R *_\alpha G \to R: \sum_{g \in G} r_g u_g \mapsto r_e$. Clearly τ defines a symmetric associative R-bilinear form on $R *_\alpha G$ with dual bases $\{u_g \mid g \in G\}$ and $\{\alpha(g, g^{-1})^{-1} u_{g^{-1}} \mid g \in G\}$.

Note that in this case $z = |G|u_e$. Compare $\zeta(R *_\alpha G)$ with the description of the center in 1.4.

2. Let H be a subgroup of a finite group G such that $|G|^{-1} \in R$ and let S be the centralizer of $R *_\alpha H$ in $R *_\alpha G$. For any α-H-regular element $g \in G$, we set $E_g = \{hgh^{-1} \mid h \in H\}$ and $s_g = \sum_{x \in E_g} u_x$, and we let G_0 denote a set of representatives for the distinct α-H-regular subclasses E_g. If either R is connected and α has been modified as in 1.3 or $\alpha = 1$, then we know that $\{s_g \mid g \in G_0\}$ is an R-basis for S.

Consider now the R-linear map $\tau : S \to R : \sum_{g \in G_0} r_g s_g \mapsto r_e$ $(r_g \in R)$. Using Lemma 1.3(2), we see that τ defines a symmetric associative R-bilinear form on S with dual bases $\{s_g \mid g \in G_0\}$ and $\{|E_g|^{-1}\alpha(g, g^{-1})^{-1}s_{g^{-1}} \mid g \in G_0\}$.

3. If A is a finite-dimensional semisimple R-algebra, R being a field, then A is a symmetric R-algebra; cf. [2, Proposition 9.8].

4. Let $\mathcal{M} = M_{n_1}(R) \oplus \dots \oplus M_{n_q}(R)$ be a direct sum of matrix algebras. We set $E_{ij}^{(k)} = (0, \dots, 0, E_{ij}, 0, \dots, 0) \in \mathcal{M}$ with E_{ij} at the kth place, and the matrix E_{ij} has ij-entry equal to 1 and zeros elsewhere.

Consider the R-linear map tr: $\mathcal{M} \to R : (B_1, \dots, B_q) \mapsto \sum_{i=1}^q \operatorname{trace}(B_i)$. It is clear that tr defines a symmetric associative R-bilinear form on $\mathcal{M}$ with dual bases $\{E_{ij}^{(k)}\}$ and $\{E_{ji}^{(k)}\}$. Note that $z = 0$ is possible, for example when $\mathcal{M} = M_3(\mathbb{Z}_3)$.

More precisely, we have the following.

3.9. LEMMA. *Let $A \cong \operatorname{End}_R(P_1) \oplus \dots \oplus \operatorname{End}_R(P_q)$ as R-algebra, where $P_1, \dots, P_q$ are finitely generated free R-modules. Let b be any nonsingular associative R-bilinear form on A with dual bases $\{a_1, \dots, a_n\}$, $\{b_1, \dots, b_n\}$ in A. Then*

(1) *The center of A coincides with $\{\sum_{i=1}^n b_i x a_i \mid x \in A\}$.*

(2) *$z_b = \sum_{i=1}^n a_i b_i$ is invertible in A if and only if $\operatorname{rank}_R(P_j)$ is invertible in R for each j.*

Proof. We first consider the R-algebra $\mathcal{M}$ from Example 4 and its map tr. If we set $c = \sum_{k=1}^q E_{11}^{(k)}$, then we get $\sum_k \sum_{i,j} E_{ji}^{(k)} c E_{ij}^{(k)} = 1$. Furthermore, we have $z_{\mathrm{tr}} = \sum_k \sum_{i,j} E_{ij}^{(k)} E_{ji}^{(k)} = ((\operatorname{rank}_R P_1)I, \dots, (\operatorname{rank}_R P_q)I)$. Note also that b induces a nonsingular associative R-bilinear form $\bar{b}$ on $\mathcal{M}$. We now prove our statements.

(1) This now follows from Proposition 3.6.

(2) According to Note 3.5, we can find an invertible element $u \in \mathcal{M}$ such that $z_{\bar{b}} = z_{\mathrm{tr}} u$. So $z_{\bar{b}}$ is invertible if and only if z_{tr} is invertible in $\mathcal{M}$ and the assertion follows. ∎

3.10. PROPOSITION. *Let A be a Frobenius R-algebra which is separable over R. Let b be an associative R-bilinear form on A with dual bases $\{a_1, \dots, a_n\}$, $\{b_1, \dots, b_n\}$.*

Then

(1) *$\zeta(A)$ is equal to the center $Z(A)$ of A.*

(2) *If R is a field of characteristic zero, then $z = \sum_{i=1}^{n} a_i b_i$ is invertible in A.*

Proof. Recall that $\zeta(a) = \sum_{i=1}^{n} b_i a a_i$ for any $a \in A$.

(1) *Step* 1. Suppose that $R = K$ is a field. Then the algebraic closure $\overline{K}$ of K is a splitting field for $\overline{K} \otimes_K A$. Obviously, the form b can be extended to an associative $\overline{K}$-bilinear form $\overline{b}$ on $\overline{K} \otimes_K A$ with dual $\overline{K}$-bases $\{1 \otimes a_i\}$, $\{1 \otimes b_i\}$. By Lemma 3.9 there is an element $x \in \overline{K} \otimes_K A$ such that $\sum_{i=1}^{n} (1 \otimes b_i)\, x\, (1 \otimes a_i) = 1$. This gives a system of n linear equations with coefficients in K, having a solution in $\overline{K}^n$. But then these equations must have a solution in K^n and therefore $1 \in \zeta(A)$.

Step 2. Now let R be an arbitrary commutative ring. First note that the separability of A implies that $Z(A)$ is a direct summand of A as R-module; see [3, pp. 51 and 55]. Hence $Z(A)$ is finitely generated as an R-module, and thus $Z(A)$ is integral over R.

We now suppose that $1 \notin \zeta(A)$. Then the ideal $\zeta(A)$ is contained in some maximal ideal M of $Z(A)$. Since $Z(A)$ is integral over R, $m = M \cap R$ is a maximal ideal of R. Now, A/mA is a separable R/m-algebra. For $a \in A$, we set $\bar{a} = a + mA$. The form b defines an associative R/m-bilinear form $\bar{b}$ on A/mA as follows: $\bar{b}(\bar{x}, \bar{y}) = b(x, y) + m$ for all $x, y \in A$. Clearly, $\{\bar{a}_i\}$, $\{\bar{b}_i\}$ are dual R/m-bases with respect to $\bar{b}$. By the first part of the proof, there is an element $x \in A$ such that $1 - \sum_{i=1}^{n} b_i x a_i \in mA$, whence $1 \in AM$. But $AM \cap Z(A) = M$, since A is separable. Consequently, $1 \in M$, a contradiction, and thus $1 \in \zeta(A)$.

(2) As in (1), reduce to the case of an algebraically closed field and apply Lemma 3.9(2). ∎

3.11. *Note.* Keep the hypotheses of 3.10 and suppose that A is commutative. Then z is invertible in A.

3.12. COROLLARY. *Let H be a subgroup of a finite group G with $|G|^{-1} \in R$ and let S be the centralizer of $R*_\alpha H$ in $R*_\alpha G$. Let either R be connected or $\alpha = 1$. Modifying α and keeping the notation of Example 3.8(2), we have*

$$\left\{ \sum_{g \in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})} s_g x s_{g^{-1}} \mid x \in S \right\} \text{ is equal to the center of } S.$$

Proof. By Proposition 1.5, S is a separable R-algebra. Apply Proposition 3.10 to the bilinear form associated to $\tau: S \to R: \sum_{g \in G_0} r_g s_g \mapsto r_e$. ∎

We now derive orthogonality relations for characters and express primitive central idempotents in terms of characters. This generalizes [2, Proposition 9.17].

3.13. THEOREM. *Let A be a Frobenius R-algebra and b a nonsingular associative R-bilinear form on A with dual bases $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$. Put $z = \sum_{i=1}^{n} a_i b_i$. Suppose R is connected and $A \cong \mathrm{End}_R(P_1) \oplus \ldots \oplus \mathrm{End}_R(P_q)$ as R-algebras, $P_1, \ldots, P_q$ being finitely generated projective R-modules. Further, let $\{e_1, \ldots, e_q\}$ be the set of primitive central nonzero idempotents of A and assume P_i lies over e_i. Then*

(1) $\sum_{i=1}^{n} t_{P_j}(a_i)t_{P_k}(b_i) = 0$ *whenever $j \neq k$, and*

$$\mathrm{rank}_R P_j \sum_{i=1}^{n} t_{P_j}(a_i)t_{P_j}(b_i) = t_{P_j}(z).$$

(2) *If b is symmetric, then $t_{P_j}(z)e_j = (\mathrm{rank}_R P_j)^2 \sum_{i=1}^{n} t_{P_j}(a_i)b_i$.*

(3) *If z is invertible in A, then all $\mathrm{rank}_R(P_i)$ are invertible in R. For a symmetric form b, the converse holds and the invertibility of $\mathrm{rank}_R(P_i)$ in R is equivalent to $t_{P_i}(z)$ invertible in R.*

Proof. Recall that P_i is an indecomposable left A-module under the operation: $(\varphi_1, \ldots, \varphi_q) \cdot p = \varphi_i(p)$, $p \in P_i$ and $\varphi_j \in \mathrm{End}_R(P_j)$, and t_{P_i} denotes the trace from A to R afforded by P_i.

(1) We set $c_j = \sum_{i=1}^{n} t_{P_j}(a_i)b_i$. It is easily verified that $b(x, c_j) = t_{P_j}(x)$ for all $x \in A$. As a consequence, we have $c_j \in Ae_j$. Indeed, if $k \neq j$, then $b(x, e_k c_j) = t_{P_j}(xe_k) = 0$ for all $x \in A$, whence $e_k c_j = 0$, because b is nondegenerate.

We now apply t_{P_k}, $k \neq j$, to the above formula for c_j and we obtain $0 = \sum_{i=1}^{n} t_{P_j}(a_i)t_{P_k}(b_i)$.

Next, we show that $t_A = \sum_{i=1}^{n} (\mathrm{rank}_R P_i)t_{P_i}$ on A.

Write P_i^* instead of $\mathrm{Hom}_R(P_i, R)$. Since P_i is a finitely generated projective R-module, we know that $P_i^* \otimes_R P_i \cong \mathrm{End}_R(P_i)$ as left $\mathrm{End}_R(P_i)$-modules, where the left $\mathrm{End}_R(P_i)$-module structure on $P_i^* \otimes_R P_i$ is induced by that on P_i. Clearly, $Ae_i \cong \mathrm{End}_R(P_i)$ as R-algebras and thus $Ae_i \cong P_i^* \otimes_R P_i$ as left A-modules. Moreover, P_i^* is finitely generated and projective over R. This implies that $t_{Ae_i} = t_{P_i^*}(1)t_{P_i} = (\mathrm{rank}_R P_i^*)t_{P_i} = (\mathrm{rank}_R P_i)t_{P_i}$ on A, see [8, Lemmas 2.2 and 2.5]. Using the fact that $t_A = \sum_{i=1}^{q} t_{Ae_i}$ on A, we obtain the desired formula (A and Ae_i viewed as left A-modules).

Now put $w = \sum_{i=1}^{q} (\mathrm{rank}_R P_i)e_i$. We prove that $z = \sum_{i=1}^{q} (\mathrm{rank}_R P_i)c_i = w(\sum_{i=1}^{q} c_i)$.

For any $x \in A$, we have

$$t_A(x) = \sum_{i=1}^{q} (\mathrm{rank}_R P_i)t_{P_i}(x) = \sum_{i=1}^{q} (\mathrm{rank}_R P_i)b(x, c_i)$$

$$= b\left(x, w\left(\sum_{i=1}^{q} c_i\right)\right).$$

But according to Lemma 3.4, $t_A(x) = b(x, z)$ and thus $z = w(\sum_{i=1}^q c_i)$ as claimed. Using this, we get $t_{P_j}(z) = (\text{rank}_R P_j)t_{P_j}(c_j)$ for each j. Then we apply $(\text{rank}_R P_j)t_{P_j}$ to the expression $c_j = \sum_{i=1}^n t_{P_j}(a_i)b_i$ and we obtain the second formula in (1).

(2) Each c_j is central in A, because $t_{P_j}(x) = b(x, c_j)$ for all $x \in A$ with t_{P_j} and b symmetric; see Lemma 3.3. Noting that R is a splitting ring for A, we have $c_j = r_j e_j$ with $r_j \in R$. So $t_{P_j}(c_j) = r_j\,(\text{rank}_R P_j)$ and, as above, $t_{P_j}(z) = (\text{rank}_R P_j)t_{P_j}(c_j)$. Consequently, $t_{P_j}(z)e_j = (\text{rank}_R P_j)^2 c_j$, as desired.

(3) As pointed out in (1), $z = w(\sum_{i=1}^q c_i)$ with $w = \sum_{i=1}^q (\text{rank}_R P_i)e_i$. So the invertibility of z in A implies that all $\text{rank}_R(P_i)$ are invertible in R. Suppose now that b is symmetric. Then z is central and thus $z = \sum_{i=1}^q \lambda_i e_i$ with $\lambda_i \in R$. For each j, we have $t_A(e_j) = b(e_j, z) = \lambda_j b(e_j, e_j)$ and also $t_A(e_j) = \sum_{i=1}^q (\text{rank}_R P_i)t_{P_i}(e_j) = (\text{rank}_R P_j)^2 1_R$. Consequently, if all $\text{rank}_R(P_i)$ are invertible in R, then z is invertible in A. Furthermore, $t_{P_j}(z) = \lambda_j\,\text{rank}_R(P_j)$. From this we deduce that $\text{rank}_R(P_i)$ is invertible in R if and only if $t_{P_i}(z)$ is invertible in R. ∎

3.14. *Remarks*. 1. Using Note 3.5, the result in (3) can be sharpened as follows. Suppose A is a symmetric R-algebra but the form b is not necessarily symmetric and suppose all $\text{rank}_R P_i$ are invertible in R, then z_b is invertible in A. Compare with 3.9.

2. From the proof of Theorem 3.13 we may deduce the following result. Let $Z(A)$ denote the center of A. If $zx = 0$ implies $x = 0$ for all $x \in Z(\mathrm{A})$, then, for each i, $\text{rank}_R(P_i)1_R \neq 0$ and $\text{rank}_R(P_i)1_R$ is not a zero divisor in R. For a symmetric form b, the converse holds and the above property for $\text{rank}_R(P_i)1_R$ is equivalent to the analogous property for $t_{P_i}(z)$. Furthermore, if the modules P_i are free R-modules, then $z \neq 0$ is equivalent to $\text{rank}_R(P_i)1_R \neq 0$ for some i; See proof of 3.9.

3. Using the orthogonality relations, we see that $t_{P_1}, \ldots, t_{P_q}$ are linearly independent over R in case $t_{P_i}(z) \neq 0$ and $t_{P_i}(z)$ is not a zero divisor in R for all i.

4. If we drop in 3.13 the hypothesis that R is a splitting ring for A, then we still obtain the following relation (see the proof of Theorem 3.13(1)). Let M and V be indecomposable left A-modules which are finitely generated projective over R and suppose that M and V lie over distinct primitive central idempotents, then $\sum_{i=1}^n t_M(a_i)t_V(b_i) = 0$.

Next, we show that, under certain conditions, trace functions on a symmetric algebra are determined by their values on the center.

3.15. LEMMA. *Let A be a symmetric R-algebra and let b be a nonsingular symmetric associative R-bilinear form on A with dual bases $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$. Suppose R is connected and R is a splitting ring for the center $Z(A)$ of A. Further, let M be an indecomposable left A-module which is finitely generated projective over R.*

Putting $z = \sum_{i=1}^{n} a_i b_i$, *we then have*

$$t_M(z)t_M(x) = (\mathrm{rank}_R M)t_M\left(\sum_{i=1}^{n} b_i x a_i\right) \qquad \textit{for all } x \in A.$$

Proof. Let $\{e_1, \ldots, e_q\}$ be the set of primitive central nonzero idempotents of A and assume M lies over e_k. By hypothesis, $Z(A) = \mathrm{R}e_1 \oplus \ldots \oplus \mathrm{R}e_q$. Thus $z = \sum_{j=1}^{q} \lambda_j e_j$ with $\lambda_j \in R$. We now have $t_M(\sum_{i=1}^{n} b_i x a_i) = t_M(xz) = \lambda_k t_M(x)$. Since $t_M(z) = (\mathrm{rank}_R M)\lambda_k$, the statement follows. ∎

We now apply these results to twisted group rings and to centralizers in twisted group rings.

3.16. Corollary. *Let R be connected and let G be a finite group with $|G|^{-1} \in R$. Suppose that $R*_\alpha G \cong \mathrm{End}_R(P_1) \oplus \ldots \oplus \mathrm{End}_R(P_q)$ as an R-algebra, $P_1, \ldots, P_q$ being finitely generated projective R-modules. Let $\{e_1, \ldots, e_q\}$ be the set of primitive central nonzero idempotents of $R*_\alpha G$ and assume P_i lies over e_i. Then*

(1) *All* $\mathrm{rank}_R(P_i)$ *are invertible in* R.

(2) $\sum_{g\in G} (1/\alpha(g, g^{-1}))\, t_{P_j}(u_g)t_{P_k}(u_{g^{-1}}) = \delta_{jk}|G|\alpha(e, e)$.

(3) $e_j = (1/|G|\alpha(e, e))\, \mathrm{rank}_R P_j \sum_{g\in G} (1/\alpha(g, g^{-1}))\, t_{P_j}(u_{g^{-1}})u_g$.

Proof. As in Example 3.8(1) we take the bilinear form associated to τ: $R*_\alpha G \to R$: $\sum_{g\in G} r_g u_g \mapsto r_e$. In this case we have $z = |G|u_e$ and $t_{P_j}(z) = |G|\alpha(e, e)\, \mathrm{rank}_R(P_j)$. We now apply Theorem 3.13. ∎

Now let H be a subgroup of a finite group G with $|G|^{-1} \in R$ and let S be the centralizer of $R*_\alpha H$ in $R*_\alpha G$. Suppose that R is a semilocal connected ring and that R is a splitting ring for $R*_\alpha G$ and $R*_\alpha H$. Let $M_1, \ldots, M_s$, resp., $N_1, \ldots, N_t$, be a basic set of indecomposable left $R*_\alpha G$-modules, resp., $R*_\alpha H$-modules, which are finitely generated and projective over R, and let c_{ij} denote the multiplicity of N_i in the restriction to H of M_j. Further, let $\{e_1, \ldots, e_s\}$, resp., $\{f_1, \ldots, f_t\}$, be the set of primitive central nonzero idempotents of $R*_\alpha G$, resp., $R*_\alpha H$, and assume that M_i lies over e_i and N_i over f_i. Finally, put $P_{ij} = \mathrm{Hom}_{R*_\alpha H}(N_i, M_j)$.

We recall from Section 1 that R is a splitting ring for S and that the nonzero P_{ij} are, up to isomorphism, all the indecomposable left S-modules which are finitely generated and projective over R. Moreover, if $c_{ij} = 0$, then $P_{ij} = 0$; otherwise, P_{ij} is a free R-module of rank c_{ij}. The nonzero $f_i e_j$ are precisely the distinct primitive central idempotents of S and P_{ij} lies over $f_i e_j$.

Finally, we modify the cocycle α as in Lemma 1.3 and we keep the notation of 3.8(2).

3.17. Corollary. *Keep the above hypotheses and notation. Put* $z = \sum_{g\in G_0} (1/|E_g|\alpha(g, g^{-1}))\, s_g s_{g^{-1}}$. *Then*

(1) *For nonzero* P_{ij} *and* P_{kl},

$$\sum_{g\in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})}\, t_{P_{ij}}(s_g) t_{P_{kl}}(s_{g^{-1}}) = 0, \qquad \textit{whenever} \quad (i, j) \neq (k, l),$$

$$c_{ij} \sum_{g\in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})}\, t_{P_{ij}}(s_g) t_{P_{ij}}(s_{g^{-1}}) = t_{P_{ij}}(z).$$

(2) *For nonzero* P_{ij},

$$t_{P_{ij}}(z)\, f_i e_j = c_{ij}^2 \sum_{g\in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})}\, t_{P_{ij}}(s_{g^{-1}}) s_g.$$

(3) *z is invertible in S if and only if all nonzero c_{ij} are invertible in R, and for any $c_{ij} \neq 0$, the invertibility of c_{ij} in R is equivalent to the invertibility of $t_{P_{ij}}(z)$ in R.*

Proof. We apply 3.13 to the bilinear form associated to τ: $S \to R$: $\sum_{g\in G_0} r_g s_g \mapsto r_e$. ∎

3.18. *Note.* Keep the above hypotheses and notation. If either $|G|!$ is invertible in R or $H \lhd G$, then all nonzero c_{ij} are invertible in R and thus z is invertible in S. Indeed, in the case $|G|!$ is invertible, this is a direct consequence of $c_{ij} \leq \text{rank}_R(M_j) \leq |G|$. In case $H \lhd G$, the statement follows from Corollaries 2.5 and 3.16(1).

3.19. Corollary. *Let H be a subgroup of a finite group G, S the centralizer of $R{*_\alpha}H$ in $R{*_\alpha}G$, and suppose that either R is connected and α has been modified or $\alpha = 1$. If either $|G|!$* is invertible in R or H $\lhd$ *G and $|G|^{-1} \in R$, then $z = \sum_{g\in G_0} (1/|E_g|\alpha(g, g^{-1}))\, s_g s_{g^{-1}}$ is invertible in S (notation as before).*

Proof. (i) Suppose that R is a field. As in 3.10, we reduce to the case of an algebraically closed field and we apply Note 3.18.

(ii) Now let R be arbitrary. Suppose $1 \notin Z(S)z$, where $Z(S)$ is the center of S, and proceed as in 3.10 in order to obtain a contradiction. For this, we need the following result. Let m be a maximal ideal of R and define $\bar{\alpha}$: $G \times G \to U(R/m)$ by $\bar{\alpha}(x, y) = \alpha(x, y) + m$. Then $g \in G$ is $\bar{\alpha}$-H-regular if and only if g is α-H-regular. To show this, let g be $\bar{\alpha}$-H-regular, $h \in C_H(g)$, and put $a = \alpha(h, g)\, \alpha(g, h)^{-1}$. Thus we have $a - 1 \in m$. We know that $a^k = 1$, where $|G| = k$; see the proof of [9, Proposition 1.4]. So $\varepsilon = k^{-1}(1 + a + \ldots + a^{k-1})$ is an idempotent of R and thus ε is either 0 or

1. If $\varepsilon = 0$, then $a - 1 \in m$ implies that $k1_R \in m$, a contradiction. Therefore $\varepsilon = 1$. But then $k(1 - a) = 1 - a^k = 0$, whence $a = 1$, proving that g is α-H-regular. The converse is obvious. As a consequence, $\bar{\alpha}$ is modified as in Lemma 1.3 and the R/m-algebra S/mS is isomorphic to the centralizer of $R/m *_{\bar{\alpha}} H$ in $R/m *_{\bar{\alpha}} G$. ∎

In the case of centralizers in twisted group rings, say $S = C_{R*_\alpha G}(R*_\alpha H)$ with $H < G$, we give another description of primitive central idempotents of S in terms of characters. But this formula depends not only on S, but also on $R*_\alpha G$ and $R*_\alpha H$.

3.20. LEMMA. *Let G be a finite group and let V be a left $R_*\alpha$ G-module which is finitely generated projective over R. Then for any $a \in R*_\alpha G$ we have*

$$\sum_{g\in G} t_V(au_g^{-1})u_g = \sum_{g\in G} t_V(u_g^{-1})u_g a = \sum_{g\in G} t_V(u_g^{-1})au_g.$$

Proof. Write $a = \sum_{k\in G} r_k u_k$ with $r_k \in R$. Then

$$\begin{aligned}\sum_{g\in G} t_V(au_g^{-1})u_g &= \sum_{k\in G}\sum_{g\in G} r_k t_V(u_k u_g^{-1})u_g u_k^{-1}u_k\\ &= \sum_{k\in G}\sum_{g\in G} r_k t_V((u_{gk^{-1}})^{-1})u_{gk^{-1}}u_k\\ &= \sum_{k\in G}\sum_{x\in G} r_k t_V(u_x^{-1})u_x u_k\\ &= \sum_{x\in G} t_V(u_x^{-1})u_x a.\end{aligned}$$

Furthermore, $t_V(au_g^{-1}) = t_V(u_g^{-1}a)$ and, just as above, we obtain that $\sum_{g\in G} t_V(u_g^{-1}a)u_g = \sum_{g\in G} t_V(u_g^{-1})au_g$. ∎

3.21. THEOREM. *Let H be a subgroup of a finite group G with $|G|^{-1} \in R$ and let S denote the centralizer of $R*_\alpha H$ in $R*_\alpha G$. Suppose R is connected, finitely generated projective R-modules are free, and R is a splitting ring for $R*_\alpha G$ and $R*_\alpha H$. Let $e_j, f_i, M_j, N_i, P_{ij}$, and c_{ij} be as in the discussion preceding Corollary 3.17, and modify α as in Lemma 1.3. Further, for any α-H-regular $g \in G$, put $E_g = \{hgh^{-1} \mid h \in H\}$ and $s_g = \sum_{x\in E_g} u_x$, and let G_0 be a set of representatives for the α-H-regular classes E_g. Then for nonzero P_{ij} and P_{kl},*

$$(1)\quad f_i e_j = |G|^{-1}\operatorname{rank}_R(N_i)\operatorname{rank}_R(M_j)\sum_{g\in G_0}\frac{1}{|E_g|\alpha(g, g^{-1})}\, t_{P_{ij}}(s_{g^{-1}})s_g,$$

(2) $$\sum_{g\in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})} t_{P_{ij}}(s_{g^{-1}})t_{P_{kl}}(s_g)$$
$$= \delta_{ik}\delta_{jl}|G|c_{ij}\,(\mathrm{rank}N_i)^{-1}(\mathrm{rank}M_j)^{-1}1_R.$$

Proof. (1) By 3.16, $e_j = |G|^{-1}\mathrm{rank}_R(M_j)\sum_{g\in G}(1/\alpha(g, g^{-1}))\, t_{M_j}(u_{g^{-1}})u_g$. Applying Lemma 3.20 yields

$$f_ie_j = |G|^{-1}\mathrm{rank}_R(M_j) \sum_{g\in G} \frac{1}{\alpha(g, g^{-1})} t_{M_j}(f_iu_{g^{-1}})u_g.$$

Clearly, if g is not α-H-regular, then the coefficient of u_g in the above decomposition must be zero; see Proposition 1.4. For an α-H-regular g and any $h \in H$, we have $t_{M_j}(f_iu_{g^{-1}}) = t_{M_j}(f_iu_{hg^{-1}h^{-1}})$, and thus $t_{M_j}(f_iu_{g^{-1}}) = (1/|E_g|)\, t_{M_j}(f_is_{g^{-1}})$. So, using 1.3(2), we obtain

$$f_ie_j = |G|^{-1}\mathrm{rank}_R(M_j) \sum_{g\in G_0} \frac{1}{|E_g|\alpha(g, g^{-1})} t_{M_j}(f_is_{g^{-1}})s_g.$$

But $t_{M_j}(f_is_{g^{-1}}) = \mathrm{rank}_R(N_i)t_{P_{ij}}(s_{g^{-1}})$, because of Theorem 1.8(1) and the fact that $t_{P_{kj}}(s_{g^{-1}}f_i) = 0$ whenever $k \neq i$ and $t_{P_{ij}}(s_{g^{-1}}f_i) = t_{P_{ij}}(s_{g^{-1}})$. Assertion (1) follows.

(2) Apply $t_{P_{kl}}$ to the expression for f_ie_j and use 3.16(1). ∎

3.22. *Note.* Keep the above hypotheses and notation and suppose that R is semilocal. Put $z = \sum_{g\in G_0}(1/|E_g|\,\alpha(g, g^{-1}))\, s_gs_g^{-1}$. Comparing Corollary 3.17(1) and Theorem 3.21(2), we obtain for nonzero P_{ij}: $\mathrm{rank}_R(N_i)\mathrm{rank}_R(M_j)t_{P_{ij}}(z) = |G|c_{ij}^2 1_R$.

4. Hecke Algebras

Throughout this section R is a connected commutative ring, A an R-algebra which is finitely generated projective as R-module, and ε a nonzero idempotent of A. We are concerned with the algebra $\varepsilon A\varepsilon$. As is well known, $\varepsilon A\varepsilon \cong (\mathrm{End}_A(A\varepsilon))^\circ \cong \mathrm{End}_A(\varepsilon A)$ as R-algebras. When A is a group ring, this algebra is called a Hecke algebra. It is easily verified that $\varepsilon A\varepsilon$ is also finitely generated projective as an R-module. Further, let $Z(A)$ denote the center of A and let $\{e_1, \ldots, e_s\}$ be the set of primitive central nonzero idempotents of A.

In [9] we investigated indecomposable modules over $\varepsilon A\varepsilon$ and we obtained the following.

4.1. Proposition. *Suppose that A is separable over R, and that either R is semilocal or R is a splitting ring for A and finitely generated projec-*

tive R-modules are free. Let $\{M_1, \ldots, M_s\}$ *be a set of representatives of the classes of indecomposable left A-modules which are finitely generated projective over R, and let* M_j *lie over* e_j. *Then*

(1) *the algebra* $\varepsilon A \varepsilon$ *is separable over R, and if R is a splitting ring for A, then it is also a splitting ring for* $\varepsilon A \varepsilon$.

(2) *The nonzero* εe_j *are precisely the distinct primitive central idempotents of* $\varepsilon A \varepsilon$.

(3) *The nonzero* εM_j *are, up to isomorphism, all the indecomposable left* $\varepsilon A \varepsilon$*-modules which are finitely generated projective and* $\varepsilon M_j \neq 0$ *if and only if* $\varepsilon e_j \neq 0$. *Moreover, for* $\varepsilon M_j \neq 0$, *we have* $M_j \cong A\varepsilon \otimes_{\varepsilon A \varepsilon} \varepsilon M_j$ *in* A-mod.

Proof. See [9, Section 4]. ∎

4.2. *Remarks.* 1. In Proposition 4.1 we do not need the assumptions on R to show that $\varepsilon A \varepsilon$ is separable; see [9, 4.1]. Under the weaker hypothesis that indecomposable finitely generated projective left A-modules lying over the same e_j are isomorphic in A-mod, the statements (2) and (3) in Proposition 4.1 remain true (considering projectivity over A, resp., $\varepsilon A \varepsilon$). This follows from the proofs in [9] and the following remark. Let W be an indecomposable finitely generated projective left $\varepsilon A \varepsilon$-module lying over εe_j. Then $A\varepsilon \otimes_{\varepsilon A \varepsilon} W$ is a finitely generated projective left A-module on which e_j acts as the identity operator, and $\varepsilon(A\varepsilon \otimes_{\varepsilon A \varepsilon} W) \cong W$. So $A\varepsilon \otimes_{\varepsilon A \varepsilon} W \cong M_j$.

2. Note that the map $\mathrm{Hom}_A(A\varepsilon, M_j) \to \varepsilon M_j$: $\varphi \mapsto \varphi(\varepsilon)$ is an R-module isomorphism, which is $\varepsilon A \varepsilon$-linear; see also [9, 4.8]. For the rank, we refer the reader to Proposition 1.2.

3. If E is a semisimple ring and ε an idempotent of E, then it is known that $\varepsilon E \varepsilon$ is semisimple too. In this case, indecomposable modules over E and $\varepsilon E \varepsilon$ are simple modules and the results in Proposition 4.1 remain true (for simple modules).

We now discuss the relationship between trace functions on A and on $\varepsilon A \varepsilon$.

Let M be a left A-module such that $\varepsilon M \neq 0$. If M is finitely generated projective over R, then so is εM. Using R-dual bases for M and εM, we then obtain $t_{\varepsilon M}(\varepsilon x \varepsilon) = t_M(\varepsilon x \varepsilon) = t_M(x\varepsilon)$ for all $x \in A$, in particular $t_M(\varepsilon) = \mathrm{rank}_R(\varepsilon M) 1_R$. Furthermore, we have the following.

4.3. Proposition. *Suppose that R is a splitting ring for Z(A). Let M be an indecomposable left A-module which is finitely generated projective over R and assume* $\varepsilon M \neq 0$. *Then*

$$\mathrm{rank}_R(\varepsilon M) t_M(x) = \mathrm{rank}_R(M) t_{\varepsilon M}(\varepsilon x \varepsilon) \qquad \textit{for all } x \in Z(A).$$

Proof. Assume M lies over e_k. By hypothesis, $Z(A) = Re_1 \oplus \ldots \oplus Re_s$, and thus $x = \sum_{j=1}^{s} r_j e_j$ with $r_j \in R$. We have $t_M(x) = \text{rank}_R(M) r_k$ and $t_M(x\varepsilon) = r_k t_M(\varepsilon)$. From this the assertion follows. ∎

4.4. *Note.* 1. Keep the above hypotheses. In addition, suppose that A is a symmetric R-algebra and let b be a symmetric associative bilinear form on A with dual bases $\{a_1, \ldots, a_n\}$, $\{b_1, \ldots, b_n\}$. Put $z = \sum_{i=1}^{n} a_i b_i$. Combining 3.15 and 4.3, we then obtain

$$\text{rank}_R(\varepsilon M) t_M(z) t_M(x) = (\text{rank}_R M)^2 t_{\varepsilon M}\left(\sum_{i=1}^{n} \varepsilon b_i x a_i \varepsilon\right) \qquad \text{for all } x \in A.$$

2. Suppose e_k acts as the identity operator on M, but M is not necessarily indecomposable, then Proposition 4.3 as well as Lemma 3.15 remain true.

4.5. Corollary. *Let $A = R_{*\alpha} G$ where G is a finite group such that $|G|^{-1} \in R$ and suppose that R is a splitting ring for A. Let M be an indecomposable left A-module which is finitely generated projective over R and assume $\varepsilon M \neq 0$. Further, modify α as in* 1.3, *put $K_g = \{ygy^{-1} \mid y \in G\}$ and $v_g = \sum_{x \in K_g} u_x$ with $g \in G$. Then for any α-G-regular $g \in G$ we have*

$$|K_g| \text{rank}_R(\varepsilon M) t_M(u_g) = \text{rank}_R(M) t_{\varepsilon M}(v_g \varepsilon).$$

Proof. Clearly $t_M(v_g) = |K_g| t_M(u_g)$ and Proposition 4.3 applies. ∎

When A is a twisted group ring we may express primitive central idempotents of $\varepsilon A \varepsilon$ in terms of trace functions as follows.

4.6. Proposition. *Let $A = R_{*\alpha} G$ where G is a finite group such that $|G|^{-1} \in R$. Suppose $R_{*\alpha} G \cong \text{End}_R(M_1) \oplus \ldots \oplus \text{End}_R(M_s)$ as an R-algebra, $M_1, \ldots, M_s$ being finitely generated projective R-modules. Assume that M_i lies over e_i and that $\varepsilon M_i \neq 0$ for $i = 1, \ldots, q$.*

Then for $1 \leq i, j \leq q$ we have

$$(1) \quad \varepsilon e_i = \frac{1}{|G| \alpha(e, e)} \text{rank}_R M_i \sum_{g \in G} \frac{1}{\alpha(g, g^{-1})} t_{\varepsilon M_i}(\varepsilon u_{g^{-1}} \varepsilon) \varepsilon u_g \varepsilon$$

$$(2) \quad \sum_{g \in G} \frac{1}{\alpha(g, g^{-1})} t_{\varepsilon M_i}(\varepsilon u_{g^{-1}} \varepsilon) t_{\varepsilon M_j}(\varepsilon u_g \varepsilon) = \delta_{ij} |G| \text{rank}_R(\varepsilon M_i)(\text{rank}_R M_i)^{-1} \alpha(e, e).$$

Moreover, in the case in which finitely generated projective R-modules are free, we may apply Proposition 4.1.

Proof. Recall that M_i is a left A-module by setting $(\varphi_1, \ldots, \varphi_s) \cdot m = \varphi_i(m)$, $m \in M_i$, and $\varphi_j \in \mathrm{End}_R(M_j)$. According to Corollary 3.16, $e_i = (1/|G|\alpha(e, e)) \operatorname{rank}_R M_i \sum_{g\in G} (1/\alpha(g, g^{-1}))\, t_{M_i}(u_{g^{-1}})u_g$.

Using Lemma 3.20 and the fact that $t_{M_i}(u_{g^{-1}}\varepsilon) = t_{\varepsilon M_i}(\varepsilon u_{g^{-1}}\varepsilon)$, we obtain (1).

The second assertion follows by applying $t_{\varepsilon M_j}$ to the expression for εe_i. ▌

4.7. *Note.* Keep the above hypotheses. As in the proof of 4.6 we derive

$$\varepsilon e_k = \frac{1}{|G|\alpha(e, e)} \operatorname{rank}_R M_k \sum_{g\in G} \frac{1}{\alpha(g, g^{-1})}\, t_{M_k}(u_{g^{-1}}\varepsilon)u_g \qquad \text{for } k = 1, \ldots, s.$$

Note that $\varepsilon M_k \neq 0$ if and only if $\varepsilon e_k \neq 0$. Let now $\varepsilon = \sum_{g\in G} r_g u_g$ with $r_g \in R$. Then it is easily seen that $|G|\alpha(e, e)r_e = \sum_{i=1}^{q} \operatorname{rank}_R(M_i) \operatorname{rank}_R(\varepsilon M_i)1_R$.

We now focus on the case where $\varepsilon \in Z(A)$. This is equivalent to $\varepsilon A\varepsilon$ being an ideal of A, as is easily checked. In this case, ε is uniquely a sum of distinct primitive central idempotents of A, say $\varepsilon = e_{i_1} + \ldots + e_{i_q}$. So $\varepsilon A\varepsilon = Ae_{i_1} \oplus \ldots \oplus Ae_{i_q}$ and $e_{i_1}, \ldots, e_{i_q}$ are precisely the primitive central idempotents of $\varepsilon A\varepsilon$. A left $\varepsilon A\varepsilon$-module W becomes a left A-module by setting $a \cdot w = a\varepsilon w$, $a \in A$, $w \in W$, and we have at once the following.

4.8. Proposition. *Let $\varepsilon \in Z(A)$, then*

(1) *If W is an indecomposable left $\varepsilon A\varepsilon$-module, then it is also an indecomposable left A-module. Conversely, if M is an indecomposable left A-module such that $\varepsilon M \neq 0$, then $\varepsilon m = m$ for all $m \in M$ and M is an indecomposable left $\varepsilon A\varepsilon$-module.*

(2) *Let M be an indecomposable left A-module which is finitely generated projective over R and let $\varepsilon M \neq 0$. Then $t_M(x) = t_M(\varepsilon x\varepsilon)$ for all $x \in A$.*

Proof. Straightforward. ▌

4.9. Proposition. *Suppose that R is a splitting ring for A and that finitely generated projective R-modules are free. Let $M_1, \ldots, M_s$ be a basic set of indecomposable left A-modules which are finitely generated projective over R and let $\varepsilon M_i \neq 0$ for $i = 1, \ldots, q$. For each i, $1 \leq i \leq q$, suppose that either*

(i) $\operatorname{rank}_R(\varepsilon M_i) = \operatorname{rank}_R(M_i)$ *or*

(ii) $t_{M_i}(x) = t_{M_i}(\varepsilon x\varepsilon)$ *for all $x \in A$.*

Then $\varepsilon \in Z(A)$.

Proof. Let $1 \leq i \leq q$ and let M_i lie over e_i. Suppose $(1 - \varepsilon)e_i \neq 0$.

Using ranks, we may write εe_i, resp., $(1 - \varepsilon)e_i$, as a sum of orthogonal primitive nonzero idempotents of A, say $\varepsilon e_i = \eta_1 + \ldots + \eta_l$ and $(1 - \varepsilon)e_i = \mu_1 + \ldots + \mu_k$. Obviously, $e_i = \varepsilon e_i + (1 - \varepsilon)e_i$ and $\eta_t \mu_j = 0$ for $t = 1, \ldots, l$, $j = 1, \ldots, k$.

Case (i). The assumptions on R imply that $(l + k)\text{rank}_R(M_i) = \text{rank}_R(Ae_i) = (\text{rank}_R M_i)^2$, whence $l + k = \text{rank}_R(M_i)$. Clearly, $\eta_1, \ldots, \eta_l$ are also primitive idempotents of $\varepsilon A \varepsilon$ and, using Proposition 4.1, we deduce, just as above, that $l = \text{rank}_R(\varepsilon M_i)$. Consequently, $(1 - \varepsilon)e_i = 0$ or $\varepsilon e_i = e_i$. It follows that $\varepsilon = \sum_{i=1}^{q} \varepsilon e_i \in Z(A)$.

Case (ii). For $j = 1, \ldots, k$, we have $t_{M_i}(\mu_j) = t_{M_i}(\mu_j \varepsilon) = 0$. Now by [8, 1.7], $\mu_j A \mu_j \cong \text{End}_A(A\mu_j)^\circ = RI$ as R-algebra, whence $\mu_j A \mu_j = R\mu_j$. Therefore $t_{M_i}(A\mu_j) = 0$. As $Ae_i \cong M_{n_i}(R)$, we know that the restriction of t_{M_i} to Ae_i is nondegenerate. So $\mu_j = 0$ and thus $(1 - \varepsilon)e_i = 0$. Consequently, $\varepsilon \in Z(A)$. ∎

We conclude this section with some applications. Let G be a finite group, H a subgroup of G with $|H|^{-1} \in R$ and $A = RG$ (with R-basis $\{u_g \mid g \in G\}$). Let $\varepsilon = (1/|H|) \sum_{h \in H} u_h$ and consider $\varepsilon A \varepsilon$.

First note that $H \times H$ acts on G as follows: $((h, k), g) \mapsto hgk^{-1}$, $h, k \in H$, $g \in G$. Therefore for any $g \in G$, $|HgH|$ is invertible in R and it is easily seen that $\varepsilon u_g \varepsilon = (1/|HgH|)\underline{HgH}$, where $\underline{HgH} = \sum_{x \in HgH} u_x$. So the distinct $\underline{HgH}$ form an R-basis for $\varepsilon A \varepsilon$.

In view of this property, $\varepsilon A \varepsilon$ is called a double coset algebra and this algebra has been studied in the special case in which $R = \mathbb{C}$. Note also that $\varepsilon \in Z(A)$ if and only if $H \lhd G$ and, in this case, $\varepsilon A \varepsilon \cong R[G/H]$. We can apply the preceding results, in particular Proposition 4.1, Corollary 4.5, and Note 4.7. Proposition 4.6 now states the following.

4.10. PROPOSITION. *Keep the hypotheses and notation of* 4.6 *and let* $\{g_1, \ldots, g_m\}$ *be a full set of double coset representatives of* H *in* G. *Then*

$$\varepsilon e_i = |G|^{-1}\text{rank}_R(M_i) \sum_{j=1}^{m} \frac{1}{|Hg_jH|} t_{\varepsilon M_i} (\underline{Hg_j^{-1}H})\underline{Hg_jH}.$$

We observe that $\varepsilon A \varepsilon$ is a symmetric R-algebra. So let $g_1, \ldots, g_m$ be as above and $g_1 = e$. Then τ: $\varepsilon A \varepsilon \to R$: $\sum_{j=1}^{m} r_j \underline{Hg_jH} \mapsto r_1$ defines a symmetric associative R-bilinear form on $\varepsilon A \varepsilon$ with dual R-bases $\{a_j = \underline{Hg_jH}\}$ and $\{b_j = (1/|Hg_jH|)\, \underline{Hg_j^{-1}H}\}$. So we may also apply the results in Section 3, in particular Proposition 3.10 and Theorem 3.13.

If $|G|^{-1} \in R$, R is a splitting ring for RG, and finitely generated projective R-modules are free, then, comparing Propositions 4.6(2) and 4.10 and Theorem 3.13(1), we see that $(\text{rank}_R M_i)t_{\varepsilon M_i}(z) = |G|(\text{rank}_R \varepsilon M_i)^2 1_R$, with $z = \sum_{j=1}^{m} a_j b_j$, M_i as in 4.6 and $\varepsilon M_i \neq 0$.

To conclude, let us discuss the relationship between $\varepsilon A \varepsilon$ and the centralizer S of RH in RG. First note that $u_h \varepsilon = \varepsilon = \varepsilon u_h$ for all $h \in H$. So $RH\varepsilon = R\varepsilon$ and thus ε is a primitive idempotent of RH. Moreover, $\varepsilon \in Z(RH)$. It is also clear that $\varepsilon RG \varepsilon \subset S$, hence $\varepsilon RG \varepsilon = \varepsilon S \varepsilon$ and $\varepsilon \in Z(S)$. So we can apply Proposition 4.8.

For the relationship between centralizers and Hecke algebras, see also Remark 2.11(4).

References

1. C. Apostolopoulos, M. Van den Bergh, and F. Van Oystaeyen, On Schur rings of group rings of finite groups, *Comm. Algebra*, to appear.
2. C. W. Curtis and I. Reiner, "Methods of Representation Theory with Applications to Finite Groups and Orders," Vol. I. Wiley-Interscience, New York, 1981.
3. F. DeMeyer and E. Ingraham, "Separable Algebras over Commutative Rings," Lecture Notes in Math., Vol. 181, Springer-Verlag, New York, 1971.
4. F. DeMeyer, Projective modules over central separable algebras, *Canad. J. Math.* **21** (1969), 39–43.
5. W. Feit, "The Representation Theory of Finite Groups," Math. Library, Vol. 25, North-Holland, Amsterdam, 1982.
6. J. Karlof, The subclass algebra associated with a finite group and subgroup, *Trans. Amer. Math. Soc.* **207** (1975), 329–341.
7. E. Nauwelaerts and F. Van Oystaeyen, The Brauer splitting theorem and projective representations of finite groups over rings, *J. Algebra* **112** (1988), 49–57.
8. E. Nauwelaerts and F. Van Oystaeyen, Module characters and projective representations of finite groups, *Proc. London Math. Soc.* **62** (1991), 151–166.
9. E. Nauwelaerts and L. Delvaux, Restriction of projective group representations to subgroups and centralizers, *J. Algebra*, **157**(1993), 63–79.
10. G. Szeto, On the Brauer splitting theorem. *Pacific J. Math.* **31** (1969), 505–512.
11. D. Travis, Spherical functions on finite groups, *J. Algebra* **29** (1974), 65–76.