P. Landrock and O. Manz
Nagoya Math. J.
Vol. 125 (1992), 33–51

SYMMETRIC FORMS, IDEMPOTENTS AND INVOLUTARY ANTIISOMORPHISMS

PETER LANDROCK AND OLAF MANZ

Introduction

Let G be a finite group, F a field and M an irreducible $F[G]$-module. By $\hat{}$ we denote the F-linear involutary antiautomorphism of $F[G]$, induced by inversion on group elements. Suppose that $\mathrm{char}(F) \neq 2$. We then show that M carries a non-singular G-invariant symmetric bilinear form with values in F if and only if there exists a $\hat{}$-invariant idempotent $e \in F[G]$ which generates the projective cover of M. This extends earlier results of W. Willems [Wi]. The assertion is not true if $\mathrm{char}(F) = 2$.

We even consider this question in the class of those finite-dimensional algebras which admit an F-linear involutary antiautomorphism τ and which are symmetric with respect to a τ-invariant symmetric functional. Besides group algebras, also involutary semi-simple F-algebras belong to that class.

In the final part of this paper, we let G be represented irreducibly and orthogonally on a real vector space M. We then show that there is a relationship between G-orbits on the unit sphere of M and idempotents $e \in \mathbb{R}[G]$ such that $M \cong \mathbb{R}[G]e$ and $\hat{e} = e$. This has some connection to a problem in Coding Theory, namely to find G-orbits on the unit sphere whose minimal Euclidian distance is considerably large.

§ 1. Involutary and symmetric algebras

Let A be a finite-dimensional F-algebra over a field F. We set $\overline{A} = A/J(A)$, where $J(A)$ denotes the Jacobson Radical of A. In the following, each A-module should be understood as a finitely generated A-*left*-module.

1.1 LEMMA. *Let $e, f \in A$ be primitive idempotents such that $\overline{ef} \neq 0$. Then the following assertions hold.*

Received July 9, 1990.

(a) *The map* $Ae \to Af$, $ae \mapsto ae\cdot f$, *is an* A*-module isomorphism.*

(b) $fAe \cong fAf$ *(as* F*-vector spaces).*

(c) fAe *is a local algebra isomorphic to* fAf, *via the algebra-isomorphism* $fae \mapsto fae\cdot f$ $(a \in A)$.

Proof. (a) Since $\overline{ef} \neq 0$ and both $\overline{Ae}$ and $\overline{Af}$ are irreducible, the map

$$\overline{Ae} \to \overline{Af}, \quad \overline{ae} \to \overline{ae}\cdot \bar{f},$$

is an isomorphism. Consequently, $Ae \cong Af$ via $ae \mapsto ae\cdot f$ (cf. [HB; VII, 11.6]).

(b) It follows from (a) that

$$fAf \cong \mathrm{Hom}_A(Af, Af) \cong \mathrm{Hom}_A(Af, Ae) \cong fAe \quad (\text{as } F\text{-vector spaces}).$$

(c) By (a), the map $fae \mapsto fae\cdot f$ $(a \in A)$ is a vector space monomorphism between fAe and fAf, and (b) implies that it even is an isomorphism. The assertion now follows from

$$(fae)(fbe)f = (fae)f\cdot(fbe)f \quad (a, b \in A). \qquad \square$$

If A admits an F-linear involutary antiautomorphism τ, we call (A, τ) an *involutary F-algebra.* Observe that τ leaves $J(A)$ invariant and thus τ induces an involutary antiautomorphism on $\bar{A}$. Let V be an A-module over an involutary F-algebra (A, τ). An F-bilinear form

$$\langle\ ,\ \rangle\colon V \times V \to F$$

is called a *τ-form* if it is non-degenerate and if

$$\langle av, w\rangle = \langle v, a^{\tau}w\rangle \qquad \text{for all } a \in A,\ v, w \in V$$

(i.e. the adjoint mapping of a with respect to $\langle\ ,\ \rangle$ is given by a^{τ}).

1.2. LEMMA. *Let* (A, τ) *be an involutary* F*-algebra and* M *an irreducibleA-module.*

(a) *If there exists a primitive idempotent* $f \in A$ *such that* $M \cong \overline{Af}$ *and* $\bar{f}^{\tau}\bar{f} \neq 0$, *then there even exists a primitive idempotent* $e \in A$ *such that* $M \cong \overline{Ae}$ *and* $e^{\tau} = e$. *Moreover,* e *can be chosen an the* 1*-element in* fAf^{τ}.

(b) *Let* M *carry a* τ*-form* $\langle\ ,\ \rangle$. *If* M *contains a non-isotropic vector* x, *then there exists an idempotent* $f \in A$ *which satisfies* $M \cong \overline{Af}$, $\bar{f}^{\tau}\bar{f} \neq 0$ *and* $fx = x$.

Prcof. (a) By Lemma 1.1 (c), the mapping

$$fAf^{\tau} \to fAf, \quad faf^{\tau} \mapsto faf^{\tau}\cdot f,$$

is an algebra-isomorphism. Let $e \in fAf^{\tau}$ be the preimage of $f \in fAf$. Then e is a primitive idempotent and is the 1-element of fAf^{τ}. Since fAf^{τ} is τ-invariant, we also have $e^{\tau} = e$. Finally

$$ae \mapsto ae\cdot f = af \quad (a \in A)$$

yields $Ae \cong Af$, hence $M \cong \overline{Ae}$.

(b) We consider the map $\overline{A} \to M$, $\bar{a} \mapsto ax$. Then there exists a primitive idempotent $f \in A$ such that $\overline{A}(\bar{1} - \bar{f})$ is its kernel. Consequently, $M \cong \overline{Af}$ and $fx = x$. Since

$$0 \neq \langle x, x\rangle = \langle fx, fx\rangle = \langle f^{\tau}fx, x\rangle = \langle \bar{f}^{\tau}\bar{f}x, x\rangle,$$

$\bar{f}^{\tau}\bar{f} \neq 0$ follows. □

We denote by $P(V)$ the projective cover of an A-module V.

1.3 Theorem. *Let (A, τ) be an involutary F-algebra. Suppose that the irreducible A-module M carries a symmetric τ-form $\langle\ ,\ \rangle$. If* $\operatorname{char}(F) \neq 2$, *then there exists a primitive idempotent $e \in A$ such that $e^{\tau} = e$ and $P(M) \cong Ae$.*

Proof. Since $\operatorname{char}(F) \neq 2$, the symmetric form $\langle\ ,\ \rangle$ is not symplectic. Therefore, Lemma 1.2(b) applies and Lemma 1.2(a) yields an idempotent $e \in A$ such that $e^{\tau} = e$ and $M \cong \overline{Ae}$. Hence $P(M) \cong Ae$. □

We shall see in Example 3.1 that the hypothesis $\operatorname{char}(F) \neq 2$ is not superfluous.

It is well-known that an idempotent $\bar{d} = d + J(A)$ can be lifted to an idempotent $e \in A$ which is a polynomial in d with integer coefficients. This observation applies to our question about τ-invariant idempotents as follows.

1.4 Proposition. *Suppose that (A, τ) is an involutary F-algebra. If $\bar{d} = d + J(A)$ is a τ-invariant idempotent in $\overline{A}$, then there exists a τ-invariant idempotent $e \in A$ such that $\bar{e} = \bar{d}$.*

Proof. We may assume that d is τ-invariant. Otherwise namely d can be replaced by dd^{τ}, because $\overline{dd^{\tau}} = \bar{d}\bar{d}^{\tau} = \bar{d}^2 = \bar{d}$. Arguing by induction, we may as well assume that $J(A)^2 = 0$. We set $e = 3d^2 - 2d^3$.

Then $e^2 = e + (d^2 - d)^2(2d+1)(2d-3) = e$, because $d^2 - d \in J(A)$. Since $e^\tau = e$ and $\bar{e} = \bar{d}$, the assertion follows. □

It is clear that in Proposition 1.4, $J(A)$ can be replaced by any τ-invariant nilpotent ideal I.

A finite-dimensional F-algebra is called *symmetric* if there exists a functional $\varphi \in \mathrm{Hom}_F(A, F)$ which satisfies $\varphi(ab) = \varphi(ba)$ for all $a, b \in A$ and which does not contain any non-zero right- (or left-) ideal of A in its kernel. We call φ a *symmetric functional* for A. (Equivalently, A can be characterized by a non-degenerate symmetric associative F-bilinear form $(\ ,\ )\colon A \times A \to F$. Observe that then $(a, b) = \varphi(ab)$. But we prefer to work with the functional φ.)

Let (A, τ) be an involutary F-algebra which is symmetric with respect to $\varphi \in \mathrm{Hom}_F(A, F)$. We call (A, τ, φ) a *symmetric involutary algebra* if

$$\varphi(a^\tau) = \varphi(a) \qquad \text{for all } a \in A.$$

1.5 LEMMA. *Let (A, τ, φ) be a symmetric involutary F-algebra. If $e \in A$ is an idempotent satisfying $e^\tau = e$, then*

$$\langle v, w \rangle = \varphi(vw^\tau), \qquad v, w \in Ae,$$

defines a symmetric τ-form on Ae.

Proof. Suppose that $0 = \langle v_0, w \rangle = \varphi(v_0 w^\tau)$ for all $w = ae \in Ae$. Since $e^\tau = e$, we obtain $0 = \varphi(v_0 e a^\tau) = \varphi(v_0 a^\tau)$ for all $a \in A$, and φ contains the right-ideal $v_0 A$ in its kernel. Thus $v_0 = 0$ and $\langle\ ,\ \rangle$ is non-degenerate.

Since φ is τ-invariant, we have

$$\langle v, w \rangle = \varphi((vw^\tau)^\tau) = \varphi(wv^\tau) = \langle w, v \rangle$$

and $\langle\ ,\ \rangle$ is symmetric. Let $a \in A$. Then

$$\langle av, w \rangle = \varphi(avw^\tau) = \varphi(vw^\tau a) = \varphi(v(a^\tau w)^\tau) = \langle v, a^\tau w \rangle$$

and $\langle\ ,\ \rangle$ is a τ-form. □

The following is inspired by [CR; 9.17], where the element z is defined for semi-simple algebras over a splitting field.

1.6 LEMMA. *Let A be a symmetric algebra with respect to $\varphi \in \mathrm{Hom}_F(A, F)$, and let M be an irreducible A-module with character $\beta \in \mathrm{Hom}_F(A, F)$. For dual bases $\{a_1, \cdots, a_n\}$ and $\{b_1, \cdots, b_n\}$ of A (i.e. $\varphi(a_i b_j) = \delta_{ij}$), we set*

$$z = \sum_{i=1}^{n} \beta(a_i)b_i \in A .$$

We then have:

(a) $\beta(a) = \varphi(za)$ *for all* $a \in A$.

(b) $z \in Z(A) \cap \operatorname{soc}(A)$.

(c) *Let* $e \in A$ *be a primitive idempotent such that* $M \cong \overline{Ae}$. *Then the map* $\overline{Ae} \to \operatorname{soc}(Ae)$, $\overline{ae} \mapsto aez$, *is an* A*-module isomorphism.*

(d) Suppose that (A, τ, φ) is a symmetric involutory F-algebra and assume that β is τ-invariant (i.e. $\beta(a^\tau) = \beta(a)$ for all $a \in A$). Then $z^\tau = z$.

Proof. (a) Observe that $\varphi(za_j) = \sum_{i=1}^{n} \beta(a_i)\varphi(b_i a_j) = \beta(a_j)$ for $j = 1, \cdots, n$. Since $\{a_1, \cdots, a_n\}$ is an F-basis of A, the assertion follows,

(b) Let $c \in J(A)$. By (a), $\varphi(zc) = \beta(c) = 0$ and φ contains the right-ideal $zJ(A)$ in its kernel. Thus $z \in \operatorname{ann}(J(A)) = \operatorname{soc}(A)$. If $a, b \in A$, then again (a) shows $\varphi(a \cdot zb) = \varphi(zb \cdot a) = \beta(ba) = \beta(ab) = \varphi(zab)$. Therefore, $(az - za)A \leq \ker(\varphi)$ and $az = za$ for all $a \in A$.

(c) Let $\varepsilon \in A$ be any lift of the Wedderburn idempotent $\bar{\varepsilon} \in \overline{A}$, corresponding to M. For each $a \in A$, we thus obtain

$$\varphi(za) = \beta(a) = \beta(a\varepsilon) = \varphi(za\varepsilon) = \varphi(\varepsilon za) .$$

This implies that $\varepsilon z = z$ and $ez \neq 0$. Since $\operatorname{soc}(Ae)$ is irreducible and $z \in Z(A) \cap \operatorname{soc}(A)$, the map $\overline{Ae} \to \operatorname{soc}(Ae)$, $\overline{ae} \mapsto aez = aze$, is an isomorphism.

(d) Since φ is τ-invariant, we have $\varphi(a_i^\tau b_j^\tau) = \varphi((a_i b_j)^\tau) = \varphi(a_i b_j) = \delta_{ij}$ and $\{a_1^\tau, \cdots, a_n^\tau\}$, $\{b_1^\tau, \cdots, b_n^\tau\}$ are dual bases of A as well. Since also β is assumed to be τ-invariant, we obtain

$$z^\tau = \sum_{i=1}^{n} \beta(a_i)b_i^\tau = \sum_{i=1}^{n} \beta(a_i^\tau)b_i^\tau .$$

We now apply (a) to both z and z^τ. Consequently, $\varphi(za) = \beta(a) = \varphi(z^\tau a)$ for all $a \in A$, i.e. $z = z^\tau$. □

If (A, τ) is an involutory F-algebra and M an A-module, then $M^* = \operatorname{Hom}_F(M, F)$ becomes an *A-left-module* by

$$(a\alpha)(m) = \alpha(a^\tau m) , \quad a \in A,\ m \in M,\ \alpha \in M^*.$$

The module M^* is called the *dual module* of M (with respect to τ). It is easy to see that M is *self-dual* (i.e. $M^* \cong M$) if and only if M carries a

τ-form (cf. [HB; VII, 8.10]).

Our next aim is to "lift" symmetric τ-forms from $P(M)$ to M.

1.7 PROPOSITION. *Let (A, τ, φ) be a symmetric involutary F-algebra. For a primitive idempotent $e \in A$, suppose that Ae carries a symmetric τ-form $\langle\ ,\ \rangle$. Then $M \cong \overline{Ae} \cong \mathrm{soc}(Ae)$ as well carries a symmetric τ-form.*

Proof. We may assume that Ae is reducible and consider the submodule

$$\mathrm{soc}(Ae)^{\perp} = \{v \in Ae \mid \langle v, w\rangle = 0 \text{ for all } w \in \mathrm{soc}(Ae)\}.$$

Since $\dim(\mathrm{soc}(Ae)^{\perp}) = \dim(Ae) - \dim(\mathrm{soc}(Ae)) = \dim(J(A)e)$, we conclude $\mathrm{soc}(Ae)^{\perp} = J(A)e$.

As Ae is assumed to carry a τ-form, Ae is self-dual and thus $M \cong M^*$. If β denotes the F-character of M, it follows that $\beta(a^{\tau}) = \beta(a)$ for all $a \in A$. For dual bases $\{a_i\}$ and $\{b_j\}$ of A, we consider $z = \sum_i \beta(a_i)b_i$ and define a bilinear form $\langle\ ,\ \rangle'$ on M by

$$\langle \bar{x}, \bar{y}\rangle' = \langle xz, y\rangle, \quad \bar{x}, \bar{y} \in \overline{Ae} \cong M.$$

Since by Lemma 1.6(c), $\bar{x} \mapsto xz$ is an isomorphism from $\overline{Ae}$ onto $\mathrm{soc}(Ae)$, and since $\mathrm{soc}(Ae)^{\perp} = J(A)e$, the form $\langle\ ,\ \rangle'$ is well-defined. Suppose that $0 = \langle \bar{x}, \bar{y}_0\rangle' = \langle xz, y_0\rangle$ for all $\bar{x} \in \overline{Ae}$. Thus xz runs through the whole of $\mathrm{soc}(Ae)$ and $y_0 \in \mathrm{soc}(Ae)^{\perp} = J(A)e$. Therefore, $\bar{y}_0 = 0$ and $\langle\ ,\ \rangle'$ is nondegenerate. Since obviously $\langle a\bar{x}, \bar{y}\rangle' = \langle \bar{x}, a^{\tau}\bar{y}\rangle'$ for all $a \in A$, itrem ains to show that $\langle\ ,\ \rangle'$ is symmetric. By part (b) and (d) of Lemma 1.6, $z^{\tau} = z \in Z(A)$, and therefore

$$\langle \bar{x}, \bar{y}\rangle' = \langle xz, y\rangle = \langle zx, y\rangle = \langle x, z^{\tau}y\rangle = \langle x, zy\rangle = \langle yz, x\rangle = \langle \bar{y}, \bar{x}\rangle'$$

for all $\bar{x}, \bar{y} \in \overline{Ae}$. This completes the proof. □

We are now able to formulate our main result.

1.8 THEOREM. *Let (A, τ, φ) be a symmetric involutary F-algebra, and M an irreducible A-module. If $\mathrm{char}(F) \neq 2$, then the following statements are equivalent.*

(1) *$P(M)$ carries a symmetric τ-form.*
(2) *M carries a symmetric τ-form.*
(3) *There exists an idempotent $e \in A$ such that $M \cong \overline{Ae}$ and $\bar{e}^{\tau} = \bar{e}$.*
(4) *There exists an idempotent $e \in A$ such that $P(M) \cong Ae$ and $e^{\tau} = e$.*

Proof. (1) $\Rightarrow$ (2): Proposition 1.7.
(2) $\Rightarrow$ (3): Theorem 1.3.
(3) $\Rightarrow$ (4): Proposition 1.4.
(4) $\Rightarrow$ (1): Lemma 1.5. □

Recall that the symmetry of A is not needed for (2) $\Rightarrow$ (3) and (3) $\Rightarrow$ (4), and that $\mathrm{char}(F) \neq 2$ is only relevant for (2) $\Rightarrow$ (3).

§ 2. Some applications

As our main application, we consider the group algebra $F[G]$ of a finite group G over the field F. Then

$$a = \sum_{g \in G} a_g g \mapsto \hat{a} = \sum_{g \in G} a_g g^{-1}$$

is an F-linear involutary antiisomorphism of $F[G]$. Moreover, $\lambda_1 \in \mathrm{Hom}_F(F[G], F)$ defined by $\lambda_1(a) = a_1$ is a symmetric functional on $F[G]$. Since $\lambda_1(\hat{a}) = \lambda_1(a)$ for all $a \in F[G]$, $(F[G], \hat{}, \lambda_1)$ is a symmetric involutary F-algebra.

Let V be an $F[G]$-module and $\langle\ ,\ \rangle$ a $\hat{}$-form on V. Then

$$\langle gv, gw \rangle = \langle v, w \rangle \qquad \text{for all } v, w \in V,\ g \in G.$$

Thus the $\hat{}$-forms on V are just the G-invariant non-degenerate F-bilinear forms on V.

2.1. COROLLARY. *Theorem* 1.8 *holds for* $(A, \tau, \varphi) = (F[G], \hat{}, \lambda_1)$.

The Corollary extends earlier results of W. Willems. He showed in his (unpublished) dissertation [Wi; 2.19] that $F[G]e$ (for a primitive idempotent e) carries a symmetric G-invariant non-degenerate F-bilinear form if and only if there exists $d \in F[G]$ such that $\hat{d} = d$ and $F[G]e \cong F[G]d$.

Observe that it is easy to see that $(F[G]e)^* \cong F[G]\hat{e}$ (cf. [OT; Lemma 1]) and hence $\hat{e} = e$ implies the existence of a G-invariant non-degenerate F-bilinear form on $F[G]e$.

We generalize the approach above. Let $H \leq G$ be a subgroup of G such that $\mathrm{char}(F) \nmid |H|$. Then $f = f_H = (1/|H|) \sum_{h \in H} h$ is an idempotent of $F[G]$, and $F[G]f$ is a transitive permutation module. Its endomorphism-ring

$$\mathrm{End}_{F[G]}(F[G]f) \cong_{\mathrm{anti}} fF[G]f =: \mathfrak{h}_F(H, G) = \mathfrak{h}$$

is called *Hecke algebra*. Observe that $H = 1$ implies that $\mathfrak{h} = F[G]$. We choose representatives $x_1 = 1, x_2, \cdots, x_t$ for (H, H)-double cosets in G and set $\operatorname{ind}(x_i) = |H\colon H \cap {}^{x_i}H|$. Then $\mathfrak{B} = \{fx_if \mid i = 1, \cdots, t\}$ is an F-basis for $\mathfrak{h}$.

Let $a = \sum_{i=1}^{t} a_i(fx_if) \in \mathfrak{h}$ $(a_i \in F)$. Then $\mathfrak{h}$ is a symmetric algebra with respect to $\varphi \in \operatorname{Hom}_F(\mathfrak{h}, F)$, defined by $\varphi(a) = a_1$, Also, $\{\operatorname{ind}(x_i)\cdot fx_i^{-1}f \mid i = 1, \cdots, t\}$ is a dual basis of $\mathfrak{B}$, whence $a_j = \varphi(a\cdot\operatorname{ind}(x_j)\cdot fx_j^{-1}f)$, $j = 1, \cdots, t$. (This paragraph is a special case of [CR; 11.30 (i) and (iii)].)

We define τ to be the restriction of $\hat{}$ on $\mathfrak{h}$. Since f is $\hat{}$-invariant, τ is an involutary antiisomorphism on $\mathfrak{h}$. Note that $a^\tau = \sum_{i=1}^{t} a_i(fx_i^{-1}f)$. We now expand a^τ in terms of $\mathfrak{B}$, say $a^\tau = \sum_{i=1}^{t} b_i(fx_if)$, $b_i \in F$. Since $\operatorname{ind}(x_1)\cdot fx_1^{-1}f = f = fx_1f$, it follows from the previous paragraph that $\varphi(a^\tau) = b_1 = \varphi(\sum_i b_i\cdot(fx_if)\cdot f) = \varphi(\sum_i a_i\cdot(fx_i^{-1}f)\cdot f) = a_1 = \varphi(a)$ for $a \in \mathfrak{h}$. Consequently, $(\mathfrak{h}, \tau, \varphi)$ is a symmetric involutary F-algebra.

2.2. Corollary. *Let $\mathfrak{h}$ be a Hecke algebra over F and τ the involutary antiisomorphism induced by* $\hat{}$. *Then Theorem* 1.8 *holds for* $(\mathfrak{h}, \tau, \varphi)$.

Theorem 1.3 clearly can be applied to any involutary F-algebra (A, τ), no matter whether A is symmetric or not. Suppose however that A is symmetric with respect to φ, $\psi \in \operatorname{Hom}_F(A, F)$. It might then happen that (A, τ, φ) is a symmetric involutary F-algebra, but (A, τ, ψ) is not.

2.3. Example. Let q be an odd prime power. Set $A = GF(q^2)$ and consider A as an algebra over $F = GF(q)$. Let τ be the Frobenius automorphism of A over F. Then τ is an F-linear involutary (anti-) isomorphism of A. For $a \in A$, we consider

$$\varphi(a) = \operatorname{tr}_{A/F}(a) = a^\tau + a \quad \text{and} \quad \psi(a) = a^\tau - a\,.$$

Then $\varphi(A) = F$, and $\psi(a) = 0$ if and only if $a \in F$. Thus both φ and ψ are symmetric functionals for A. However $\varphi(a^\tau) = \varphi(a)$, but $\psi(a^\tau) = -\psi(a)$ for all $a \in A$.

The situation of Example 2.3 is typical. Namely let (A, τ) be an involutary F-algebra with center $Z = \mathbf{Z}(A)$. Suppose that Z is a field and consider the subfield K of Z, consisting of all τ-invariant elements. Then $Z\colon K$ is a separable field extension of degree at most 2 (see [Al; X, Thm. 10]). We do not exploit this further on.

If φ is a symmetric functional for A, then it is easy to see that any other symmetric functional ψ is given by

$$\psi(a) = \varphi(za) \qquad \text{for all } a \in A,$$

where z is a central element of A. The following fact as well is easy and will be needed later on.

2.4 LEMMA. *Let A be a symmetric F-algebra with respect to $\varphi \in \mathrm{Hom}_F(A, F)$. If x is an invertible element in $\mathbf{Z}(A)$, then $\varphi_x \in \mathrm{Hom}_F(A, F)$ defined by $\varphi_x(a) = \varphi(xa)$, $a \in A$, as well is a symmetric functional for A.*

Proof. Since $x \in \mathbf{Z}(A)$, we have

$$\varphi_x(ab) = \varphi(xab) = \varphi(bxa) = \varphi(xba) = \varphi_x(ba) \qquad \text{for all } a, b \in A.$$

If φ_x has the right ideal cA in its kernel, then $\varphi(xcA) = 0$, whence $xc = 0$. Since x is invertible, it follows that $c = 0$. □

We now consider a semi-simple algebra S. Recall that S then is symmetric (cf. [CR; 9.8]). By Wedderburn's Theorem,

$$S \cong \bigoplus_{i=1}^{n} \mathrm{Mat}_{m_i}(D_i) \qquad \text{with finite-dimensional skew-fields } D_i.$$

It M is an irreducible S-module, it belongs to a unique Wedderburn component of S. Thus in view of an application of § 1, we may assume that $S = \mathrm{Mat}_m(D)$ is simple.

2.5. PROPOSITION. *Let D be a finite-dimensional skew-field over F and assume that (D, η) is an involutary F-algebra. Then there exists $\chi \in \mathrm{Hom}_F(D, F)$ such that (D, τ, χ) is a symmetric involutary F-algebra.*

Proof. Set $Z = \mathbf{Z}(D)$.

Case 1: Suppose that η induces the identity on Z. We then consider D as a Z-algebra and pick a symmetric functional $\varphi \in \mathrm{Hom}_Z(D, Z)$. Let L be a splitting field for D. Since D is centrally simple over Z, it follows that $L \otimes_Z D = \mathrm{Mat}_n(L)$ for some $n \in \mathbb{N}$. Since both φ and η are Z-linear, we can define $\tilde{\varphi}, \tilde{\eta} \in \mathrm{Hom}_L(\mathrm{Mat}_n(L), L)$ by $\tilde{\varphi} = \mathrm{id}_L \otimes \varphi$ and $\tilde{\eta} = \mathrm{id}_L \otimes \eta$. Then $\tilde{\eta}$ is an involutary antiisomorphism on $\mathrm{Mat}_n(L)$ and $\tilde{\varphi}$ satisfies

$$\tilde{\varphi}((x_{ij})(y_{ij})) = \tilde{\varphi}((y_{ij})(x_{ij})) \qquad \text{for all } (x_{ij}), (y_{ij}) \in \mathrm{Mat}_n(L).$$

It follows that $\tilde{\varphi}$ is (up to some F-scalar factor) the trace on $\mathrm{Mat}_n(L)$. Since $(x_{ij}) \mapsto (x_{ji})^{\tilde{\eta}}$ is an L-algebra automorphism on $\mathrm{Mat}_n(L)$, an elementary version of the Skolem-Noether Theorem implies that there exists an invertible matrix $(c_{kl}) \in \mathrm{Mat}_n(L)$ such that

$$(x_{ij})^{\tilde{\eta}} = (c_{kl})^{-1}(x_{ji})(c_{kl}) \qquad \text{for all } (x_{ij}) \in \mathrm{Mat}_n(L).$$

In particular, $\tilde{\varphi}((x_{ij})^{\tilde{\eta}}) = \tilde{\varphi}((x_{ij}))$ for all $(x_{ij}) \in \mathrm{Mat}_n(L)$. Consequently, we have for all $a \in L$ and $d \in D$

$$a \otimes \varphi(d) = \tilde{\varphi}(a \otimes d) = \tilde{\varphi}((a \otimes d)^{\tilde{\eta}}) = \tilde{\varphi}(a \otimes d^{\eta}) = a \otimes \varphi(d^{\eta}),$$

i.e. $\varphi(d^{\eta}) = \varphi(d)$.

Let $\mu \in \mathrm{Hom}_F(Z, F)$ be any non-zero functional. We set $\chi = \mu\varphi \in \mathrm{Hom}_F(D, F)$. Since $\chi \neq 0$, the skew-field D is a symmetric F-algebra with respect to χ. As $\chi(d^{\eta}) = \chi(d)$ for all $d \in D$, the assertion of the Proposition holds in the first case.

Case 2. Suppose now that η is not the identity on Z. Let $\chi \in \mathrm{Hom}_F(D, F)$ be any symmetric functional on D. If χ is not η-invariant, we consider instead $\varphi \in \mathrm{Hom}_F(D, F)$ defined by $\varphi(d) = \chi(d) + \chi(d^{\eta})$, $d \in D$. Clearly, $\varphi(d^{\eta}) = \varphi(d)$. If $\varphi \neq 0$, then (D, η, φ) is a symmetric involutary F-algebra, and we are done. We may thus assume that $\chi(d^{\eta}) = -\chi(d)$ for all $d \in D$, and also that $\mathrm{char}(F) \neq 2$.

We consider the F-linear map $\eta_Z \in \mathrm{Hom}_F(Z, Z)$. Since $\eta_Z \neq \mathrm{id}_Z$, there exists $0 \neq x \in Z$ such that $x^{\eta} = -x$. By Lemma 2.4, $\chi_x \in \mathrm{Hom}_F(D, F)$ defined by $\chi_x(d) = \chi(xd)$, $d \in D$, is a symmetric functional on D as well. Now $\chi_x(d^{\eta}) = \chi(xd^{\eta}) = \chi(-x^{\eta}d^{\eta}) = -\chi((xd)^{\eta}) = \chi(xd) = \chi_x(d)$ for all $d \in D$, and the proof is complete. $\square$

In order to extend Proposition 2.5 to simple algebras $S = \mathrm{Mat}_m(D)$, we use the fact that any involutary antiisomorphism on S can be written as an involutary antiisomorphism on D followed by transposition and conjugation of matrices.

2.6 Theorem. *Let S be a simple finite-dimensional F-algebra which admits an F-linear involutary antiisomorphism τ. Set $S = \mathrm{Mat}_m(D)$ with a skew-field D, $Z = \mathbf{Z}(S) = \mathbf{Z}(D) \cdot 1_S$ and $K = \{z \in Z \mid z^{\tau} = z\}$.*

(a) [Al; X, Thm. 11] *Then τ induces an involutary antiisomorphism η on D such that $K = \{z \in Z \mid z^{\eta} = z\}$.*

(b) [Al; X, Thm. 10] *There exists a non-singular $(c_{kl}) \in S$ such that $(d_{ij})^{\tau} = (c_{kl})^{-1}(d_{ji}^{\eta})(c_{kl})$ for all $(d_{ij}) \in S = \mathrm{Mat}_m(D)$.*

2.7 Theorem. *Let S be a finite-dimensional simple F-algebra which admits an F-linear involutary antiisomorphism τ. Then there exists $\varphi \in \mathrm{Hom}_F(S, F)$ such that (S, τ, φ) is a symmetric involutary F-algebra.*

Proof. Set $S = \mathrm{Mat}_m(D)$ for a finite-dimensional skew-field D. By

Theorem 2.6, there exist an invertible $(c_{kl}) \in S$ and an F-linear involutory antiisomorphism η on D such that

$$(d_{ij})^\tau = (c_{kl})^{-1}(d_{ji}^\eta)(c_{kl}) \qquad \text{for all } (d_{ij}) \in S.$$

By Proposition 2.5, there exists $\chi \in \mathrm{Hom}_F(D, F)$ such that (D, η, χ) is a symmetric involutory F-algebra. We set $\varphi = \chi \cdot \mathrm{tr} \in \mathrm{Hom}_F(S, F)$. Then φ is a symmetric functional on S, and for $(d_{ij}) \in S$ we have

$$\varphi((d_{ij})^\tau) = \varphi((d_{ij}^\eta)) = \sum_{i=1}^{m} \chi(d_{ii}^\eta) = \sum_{i=1}^{m} \chi(d_{ii}) = \varphi((d_{ij}))\,.$$

This establishes the claim. □

2.8 Corollary. *Let (S, τ) be an involutory F-algebra. If S is semisimple and* $\mathrm{char}(F) \neq 2$, *then the following assertions are equivalent for an irreducible S-module M.*

(1) *M carries a symmetric τ-form.*

(2) *There exists an idempotent $e \in S$ such that $M \cong Se$ and $e^\tau = e$.*

Proof. Let $1 = \varepsilon_1 + \cdots + \varepsilon_t$ be the decomposition of $1 \in S$ into Wedderburn idempotents ε_i. Then τ permutes the ε_i. Observe that under each of the conditions (1) and (2), the idempotent ε_i corresponding to M is fixed. Thus the assertion follows from Theorems 1.8 and 2.7. □

For more examples of involutory algebras we refer to [Al; chap. X].

§ 3. Absolutely irreducible G-modules

3.1 Examples. (a) Let (A, τ) be an involutory F-algebra and M an absolutely irreducible A-module. If M carries a symplectic τ-form $\langle\ ,\ \rangle$, then it is very easy to see that there does not exist an idempotent $e \in A$ such that $\bar{e}^\tau = \bar{e}$ and $M \cong \overline{Ae}$:

Suppose there is such an idempotent e. Since $\langle\ ,\ \rangle$ is non-degenerate, we find $a \in A$ such that $\langle \overline{ae}, \bar{e} \rangle \neq 0$. Since M is absolutely irreducible, $\overline{eae} = \mu\bar{e}$ for some $\mu \in F$. Consequently,

$$0 \neq \langle \overline{ae}, \bar{e} \rangle = \langle \bar{e}^\tau \overline{ae}, \bar{e} \rangle = \langle \overline{eae}, \bar{e} \rangle = \mu \langle \bar{e}, \bar{e} \rangle = 0\,,$$

a contradiction.

(b) Let (A, τ) be an involutory F-algebra, $\mathrm{char}(F) = 2$ and M an absolutely irreducible A-module with symmetric τ-form $\langle\ ,\ \rangle$. If $\dim_F M \geq 2$, counting yields a non-zero isotropic vector in M. Since the isotropic vectors in M form a submodule of M, the form $\langle\ ,\ \rangle$ is symplectic. By (a), there does not exist $e \in A$ such that $\bar{e}^{\tau} = \bar{e}$ and $M \cong \overline{Ae}$. Thus the assertion of Theorem 1.3 is false for $\mathrm{char}(F) = 2$.

(c) Nevertheless, if F is not a splitting field, there might exist such an idempotent. As a trivial example, consider $A = F_2[C_3]$ can let M be its 2-dimensional irreducible module. Clearly, there exists exactly one primitive idempotent $e \in A$ such that $M \cong Ae$. Hence $e^{\tau} = e$, and M carries a symmetric $\hat{}$-form, by Lemma 1.5.

For $\mathrm{char}(F) = 2$, one might have to consider quadratic forms instead of bilineai ones. For more results in this direction, we refer to the (unpublished) dissertation of W. Willems [Wi].

In the following, we restrict ourselves to group algebras $F[G]$ with symmetric functional $\lambda_1 \in \mathrm{Hom}_F(F[G], F)$ and involutary antiisomorphism $\tau = \hat{}$. Since the $\hat{}$-forms are just the G-invariant ones, we shall speak henceforth of G-forms.

We next slightly sharpen the assertion of 3.1(a) in case of group algebras. To do so, we need the following result (see [HB; VII, 8.12]).

3.2 THEOREM. *Let M be an absolutely irreducible self-dual $F[G]$-module. Then to within an F-scalar multiple, there exists only one G-form on M. If char $(F) \neq 2$, this form is either symmetric or symplectic.*

3.3 COROLLARY. *Let M be an absolutely irreducible $F[G]$-module. If* $\mathrm{char}(F) \neq 2$, *then the following asesertions are equivalent.*

(1) *M carries a symplectic G-form.*

(2) *$\overline{\hat{f}f} = 0$ for all idempotents $f \in F[G]$ which satisfy $M \cong \overline{F[G]f}$.*

Proof. (1) $\Rightarrow$ (2): Suppose there exists an f such that $\overline{\hat{f}f} \neq 0$. Then Lemma 1.2(b) implies that there also exists an idempotent $e \in A$ such that $M \cong \overline{F[G]e}$ and $\hat{e} = e$. By Lemma 1.5 and Proposition 1.7, the module M carries a symmetric G-form. Since M is absolutely irreducible, M cannot carry a symplectic G-form, by Theorem 3.2. This contradicts (1).

(2) $\Rightarrow$ (1): Suppose that M carries a symmetric G-form. As $\mathrm{char}(F) \neq 2$, Theorem 1.3 yields an idempotent $e \in F[G]$ such that $M \cong \overline{F[G]e}$ and $\hat{e} = e$. In particular, $\bar{\hat{e}}\bar{e} = \bar{e} \neq 0$, contradicting (2). By Theorem 3.2, M carries a symplectic G-form. □

The next lemma, which we only state under the conditions needed later on, is probably well-known.

3.4 LEMMA. *Let e be an idempotent in $F[G]$, where* $\operatorname{char}(F) \nmid |G|$. *Then* $\lambda_1(e) = (1/|G|) \dim_F(F[G]e)$.

Proof. Let $L \supseteq F$ be an algebraically closed extension field of F. Then

$$\dim_F(F[G]e) = \dim_L(L \otimes_F F[G]e) = \dim_L(L[G]e)\,.$$

Let $e = f_1 + \cdots + f_s$ be a decomposition of e into primitive idempotents f_i in $L[G]$, and $f = f_1$. We denote the character of $L[G]f$ by χ, and the corresponding Wedderburn idempotent by $\varepsilon \in L[G]$. Thus

$$\varepsilon = (\chi(1)/|G|) \sum_{g \in G} \chi(g^{-1})g$$

and $\lambda_1(\varepsilon) = \chi(1)^2/|G|$. Since all primitive idempotents corresponding to ε are conjugate to f, and since $\lambda_1(u^{-1}fu) = \lambda_1(f)$ (for units u in $L[G]$), we conclude $\lambda_1(f) = (1/\chi(1))\lambda_1(\varepsilon) = \chi(1)/|G| = (1/|G|) \dim_L(L[G]f)$. Consequently,

$$\begin{aligned}\lambda_1(e) = \sum_{i=1}^{s} \lambda_1(f_i) = (1/|G|) \sum_{i=1}^{s} \dim_L(L[G]f_i) &= (1/|G|) \dim_L(L[G]e) \\ &= (1/|G|) \dim_F(F[G]e)\,. \qquad \square\end{aligned}$$

As a disadvantage of Theorem 1.3 we recall that its proof does not yield an explicit formula for a τ-invariant idempotent in terms of the given τ-form. Under certain circumstances, we can do better.

Let M be an $F[G]$-module with G-form $\langle\ ,\ \rangle$. For an element $x \in M$, we define

$$c_x = \sum_{g \in G} \langle g^{-1}x, x\rangle g \in F[G]\,.$$

Then c_x has the following properties.

(1) $\lambda_1(c_x a) = \langle ax, x\rangle$ for all $a \in F[G]$.
(Namely just observe that $\lambda_1(c_x h) = \langle hx, x\rangle$ for all $h \in G$.)

(2) If $f \in F[G]$ satisfies $fx = x$, then also $fc_x = c_x$.
(To see this, note that

$\lambda_1(c_x a) = \langle ax, x\rangle = \langle afx, x\rangle = \lambda_1(c_x af) = \lambda_1(fc_x a)$ for all $a \in F[G]$,

and therefore $fc_x - c_x = 0$.)

(3) If $\langle\ ,\ \rangle$ is symmetric, then $c_x = \sum_{g \in G} \langle gx, x\rangle g$ and $\hat{c}_x = c_x$.

3.5 *Remark.* Before we proceed, we recall what Lemma 1.2 says in our present context. Let M be an irreducible $F[G]$-module which carries a G-form and which contains a non-isotropic vector x. Then there exist primitive idempotents $f, e \in F[G]$ with the following properties:

(i) $M \cong \overline{F[G]f} \cong \overline{F[G]e}$.

(ii) $fx = x$.

(iii) $\hat{e} = e$.

(iv) e is the 1-element of $fF[G]\hat{f}$, hence $fF[G]\hat{f} = eF[G]e$.

3.6 PROPOSITION. *Let M be an irreducible $F[G]$-module which carries a symmetric G-form $\langle\ ,\ \rangle$. Suppose that M contains a non-isotropic vector x, and let $\hat{e} = e$ be chosen according to Remark* 3.5. *If*

$$\{v \in eF[G]e \mid \hat{v} = v\} = Fe\,,$$

then $e = \gamma c_x$ for some $\gamma \in F$.

Proof. We choose the idempotent f as in Remark 3.5. By (ii), $fx = x$ implies $fc_x = c_x$. Since $\langle\ ,\ \rangle$ is symmetric, (iv) yields

$$c_x = \hat{c}_x = \hat{c}_x\hat{f} = c_x\hat{f} = fc_x\hat{f} \in fF[G]\hat{f} = eF[G]e\,,$$

and $c_x = \beta e$ for some $\beta \in F$. It remains to show that $c_x \neq 0$. This follows, because $\lambda_1(c_x) = \langle x, x\rangle \neq 0$. □

3.7 THEOREM. *Let $F[G]$ be semi-simple, and suppose that the absolutely irreducible $F[G]$-module M carries a symmetric G-form $\langle\ ,\ \rangle$. Suppose that M contains a non-isotropic vector x (, which holds provided that* $\mathrm{char}(F) \neq 2$). *Then*

$$e = (\dim_F M)/(|G|\cdot\langle x, x\rangle)\cdot c_x = (\dim_F M)/(|G|\cdot\langle x, x\rangle) \sum_{g \in G} \langle gx, x\rangle g$$

is an idempotent such that $M \cong F[G]e$ and $\hat{e} = e$.

Proof. Let $\hat{e} = e$ be chosen as in Remark 3.5. Since $F[G]$ is semi-simple and M is absolutely irreducible, we have $M \cong F[G]e$ and $F \cong \mathrm{End}_{F[G]}(M) \cong_{\mathrm{anti}} eF[G]e$. In particular, $\{v \in eF[G]e \mid \hat{v} = v\} = Fe$, and Proposition 3.6 implies that $e = \gamma c_x$ for some $\gamma \in F$. It remains to determine the scalar γ. By Lemma 3.4,

$$\dim_F M/|G| = \lambda_1(e) = \gamma \cdot \lambda_1(c_x) = \gamma\langle x, x\rangle\,,$$

and the assertion follows. □

3.8 *Remarks.* (a) It should be clear that Theorem 3.7 still holds if we drop the hypothesis "semi-simple" and assume instead that M has defect 0 (i.e. the block ideal of $F[G]$ corresponding to M is simple).

(b) If M has positive defect however, then c_x definitely is no candidate for an idempotent. To see this note that $\lambda_1(c_x j) = \langle jx, x\rangle = 0$ for all $j \in J(F[G])$. Consequently, $c_x \in \operatorname{ann}(J(F[G])) = \operatorname{soc}(F[G])$. Thus $c_x = fc_x\hat{f} \in eF[G]e$ is in the socle and hence in the radical of the block ideal corresponding to M. Therefore, $c_x^2 = 0$.

(c) We do not know how to generally proceed if F is not a splitting field for M. The case $F = \mathbb{R}$ however will be treated in the next section.

§ 4. Real orthogonal representations

Let M be an $\mathbb{R}[G]$-module and fix a symmetric, positive definite bilinear form $(\ ,\ )$ on M. Then $[\ ,\ ]$ defined by

$$[v, w] = \sum_{g\in G} (gv, gw), \qquad v, w \in M,$$

obviously is a symmetric, positive definite G-form. It thus follows from Theorem 1.3.

4.1 Corollary. *Let M be an irreducible $\mathbb{R}[G]$-module. Then there exists an idempotent $e \in \mathbb{R}[G]$ such that $M \cong \mathbb{R}[G]e$ and $\hat{e} = e$.*

4.2 Lemma. *Let e be a primitive idempotent in $\mathbb{R}[G]$ with $\hat{e} = e$. Then*

$$I := \{v \in e\mathbb{R}[G]e \mid \hat{v} = v\} = \mathbb{R}e\,.$$

Proof. By Lemma 1.5, $\langle v, w\rangle = \lambda_1(v\hat{w})$, $v, w \in \mathbb{R}[G]e$, is a symmetric G-form on $\mathbb{R}[G]e$. Moreover, $\langle\ ,\ \rangle$ is positive definite, and it holds that

$$\langle v, wa\rangle = \lambda_1(v\hat{a}\hat{w}) = \langle v\hat{a}, w\rangle \qquad \text{for all } a \in e\mathbb{R}[G]e.$$

Suppose that $\dim_{\mathbb{R}} I \geq 2$ and recall that $e\mathbb{R}[G]e \cong \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$, where $\mathbb{H}$ denotes the quaternion skew-field. If $e\mathbb{R}[G]e \cong \mathbb{C}$, we choose $i \in e\mathbb{R}[G]e$ corresponding to the complex unit in $\mathbb{C}$. It then follows for all $0 \neq v \in \mathbb{R}[G]e$ that

$$0 \leq \langle vi, vi\rangle = \langle vi\hat{i}, v\rangle = \langle vi^2, v\rangle = -\langle v, v\rangle < 0\,,$$

a contradiction.

We may thus assume that $e\mathbb{R}[G]e \cong \mathbb{H}$. If $\dim_{\mathbb{R}} I = 2$, then $I = \operatorname{span}_{\mathbb{R}}\langle e, x\rangle$ for some $x \in e\mathbb{R}[G]e$ and the elements of I pairwise commute. Therefore, I is closed under multiplication and $I \cong \mathbb{C}$. Consequently, if $\dim_{\mathbb{R}} I = 2$ or 4, then I contains an element i such that $i^2 = -e$ and we proceed as in the last paragraph. We still have to consider the case

$\dim_{\mathbb{R}} I = 3$, say $I = \mathrm{span}_{\mathbb{R}}\langle e, x, y\rangle$. Let $\{e, i, j, k\}$ be the canonical $\mathbb{R}$-basis of $e\mathbb{R}[G]e \cong \mathbb{H}$. After a suitable basis transformation we may assume that $x = i + \mu k$ and $y = j + \nu k$ for $\mu, \nu \in \mathbb{R}$. Since $x^2 = -e(1 + \mu^2)$, we obtain for $0 \neq v \in \mathbb{R}[G]e$

$$0 \leq \langle vx, vx\rangle = \langle vx^2, v\rangle = -(1 + \mu^2)\langle v, v\rangle < 0\,,$$

again a contradiction. This completes the proof. □

Let V be an $F[G]$-module (for an arbitrary field F) and $\langle\ ,\ \rangle$ a G-form on V. Then the mapping

$$\alpha \mapsto \langle\ ,\ \rangle_\alpha\,, \qquad \text{where } \langle v, w\rangle_\alpha = \langle v, \alpha w\rangle\,,$$

yields an isomorphism between $\mathrm{End}_{F[G]}(V)$ and the F-space $B_G(V)$ of all G-invariant bilinear forms on V (possibly degenerate).

Assume in addition that $V = F[G]e$ for an idempotent e. The isomorphism $eF[G]e \cong \mathrm{End}_{F[G]}(V)$ is given by $a \mapsto \alpha_a$, where $\alpha_a(v) = va$. Hence

$$a \mapsto \langle\ ,\ \rangle_a\,, \qquad \text{where } \langle v, w\rangle_a = \langle v, wa\rangle,$$

induces a vector space isomorphism between $eF[G]e$ and $B_G(V)$. The following serves as a substitute for Theorem 3.2.

4.3 Proposition. *Let M be an irreducible $\mathbb{R}[G]$-module. Then M has exactly one symmetric G-form (up to $\mathbb{R}$-scalar factors).*

Proof. By Corollary 4.1, we may assume that $M = \mathbb{R}[G]e$ for an idempotent $e = \hat{e}$. Consider the symmetric G-form $\langle\ ,\ \rangle$ on M induced by λ_1 (see Lemma 1.5). Then every other G-invariant bilinear form on M is given by $\langle\ ,\ \rangle_a$ for a unique $a \in e\mathbb{R}[G]e$. Now $\langle\ ,\ \rangle_a$ is symmetric if and only if

$$\langle v, wa\rangle = \langle v, w\rangle_a = \langle w, v\rangle_a = \langle w, va\rangle = \langle w\hat{a}, v\rangle = \langle v, w\hat{a}\rangle$$

for all $v, w \in M$. This happens if and only if $\hat{a} = a$, and Lemma 4.2 implies that $a = \gamma e$ for some $\gamma \in \mathbb{R}$. Consequently, $\langle\ ,\ \rangle_a = \gamma\langle\ ,\ \rangle$, which was to be proved. □

Let M be an irreducible $\mathbb{R}[G]$-module. Using the form $[\ ,\ ]$ and Proposition 4.3, any given symmetric G-form $\langle\ ,\ \rangle$ on M may be assumed to be positive definite. The group G is then said to be *represented orthogonally* on M. It makes sense now to consider the *unit sphere*

$\{x \in M \mid \langle x, x\rangle = 1\}$ on M. Also a distance function $d(\ ,\ )$ can be introduced in the usual way by

$$d(x, y)^2 = \langle x - y, x - y\rangle, \qquad x, y \in M.$$

4.4 THEOREM. *Let G be represented irreducibly and orthogonally on the $\mathbb{R}$-space M with respect to the form $\langle\ ,\ \rangle$.*

a) *Given $x \in M$ with $\langle x, x\rangle = 1$, then*

$$e = (\dim_{\mathbb{R}} M)/|G| \sum_{g \in G} \langle gx, x\rangle g$$

is an idempotent satisfying both $M \cong \mathbb{R}[G]e$ and $e = \hat{e}$. Here, elements of M in the same G-orbit lead to G-conjugate idempotents.

b) *Conversely, given $e = \sum_{g \in G} \alpha_g g$ an idempotent with $M \cong \mathbb{R}[G]e$ and $e = \hat{e}$, there, exists $x \in M$ with $\langle x, x\rangle = 1$ and*

$$\langle gx, x\rangle = |G|\alpha_g/\dim_{\mathbb{R}} M, \qquad g \in G.$$

Proof. a) Consider first $x \in M$ with $\langle x, x\rangle = 1$, and choose the idempotent $e = \hat{e} \in \mathbb{R}[G]$ with $M \cong \mathbb{R}[G]e$ according to Remark 3.5. By Lemma 4.2, $\{v \in e\mathbb{R}[G]e \mid \hat{v} = v\} = \mathbb{R}e$, and Proposition 3.6 yields

$$e = \gamma c_x = \gamma \sum_{g \in G} \langle gx, x\rangle g \qquad \text{for some } \gamma \in \mathbb{R}.$$

The scalar γ again is determined by Lemma 3.4, namely

$$\dim_{\mathbb{R}} M/|G| = \lambda_1(e) = \gamma \cdot \lambda_1(c_x) = \gamma \cdot \langle x, x\rangle = \gamma.$$

Finally observe that replacing x by hx $(h \in G)$ replaces e by heh^{-1}.

b) Assume conversely that $e = \hat{e}$ is given. Then Lemma 1.5 asserts that

$$\langle v, w\rangle' := |G|/\dim_{\mathbb{R}} M \cdot \lambda_1(v\hat{w}), \qquad v, w \in \mathbb{R}[G]e,$$

defines a symmetric G-form $\langle\ ,\ \rangle'$ on $\mathbb{R}[G]e \cong M$. In particular,

$$\langle ge, e\rangle' = \langle g^{-1}e, e\rangle' = |G|/\dim_{\mathbb{R}} M \cdot \lambda_1(g^{-1}e) = |G|\alpha_g/\dim_{\mathbb{R}} M \quad (g \in G),$$

and Lemma 3.4 yields $\langle e, e\rangle' = 1$. By Proposition 4.3, there is a non-zero $\gamma \in \mathbb{R}$ such that $\langle v, w\rangle' = \gamma\langle v, w\rangle$ for all $v, w \in \mathbb{R}[G]e$. Then $1 = \langle e, e\rangle' = \gamma\langle e, e\rangle$, and $\gamma > 0$, since $\langle\ ,\ \rangle$ is positive definite. Hence we may take x to be $\sqrt{\gamma}\, e$. □

For data transmission via a Gaussian channel, it turned out to be successful to consider the codewords as G-orbits on the unit sphere of some Euclidian space $\mathbb{R}^n$. The question about reasonable lower bounds for the minimal Euclidian distance—actually our motivation for this paper—has only got partial answers. The following result was first proved by D. Splpian in 1968. (See [BM; chap. 6] for this result and some background in Coding Theory.)

4.5 COROLLARY (Slepian). *Let G be represented irreducibly and orthogonally, but non-trivially, on the $\mathbb{R}$-space M with respect to the form $\langle\ ,\ \rangle$. Let $x \in M$ with $\langle x, x\rangle = 1$. Then*

a) $\sum_{g\in G} d(gx, x)^2 = 2|G|$.

b) *If $\mathfrak{R}$ denotes any conjugacy class in G and $k \in \mathfrak{R}$, then* $\sum_{g\in\mathfrak{R}} d(gx, x)^2 = 2|\mathfrak{R}|(1 - \chi(k)/\chi(1))$, *where χ is the character of M.*

Proof. By Theorem 4.4, $e = \dim_{\mathbb{R}} M/|G| \sum_{g\in G} \langle gx, x\rangle g$ is an idempotent affording M.

a) Since M is not the trivial module, we have

$$0 = (\sum_{g\in G} \langle gx, x\rangle g)(\sum_{h\in G} h) = \sum_{g\in G} \langle gx, x\rangle(\sum_{h\in G} h),$$

and therefore $\sum_{g\in G} d(gx, x)^2 = \sum_{g\in G} 2(1 - \langle gx, x\rangle) = 2|G|$.

b) Since $d(gx, x)^2 = 2(1 - \langle gx, x\rangle)$, it amounts to show that

$$\sum_{g\in\mathfrak{R}} \langle gx, x\rangle = |\mathfrak{R}|\chi(k)/(1).$$

Put $\bar{\mathfrak{R}} = \sum_{g\in\mathfrak{R}} g$ and observe that $e = \chi(1)/|G| \sum_{g\in G} \langle gx, x\rangle g^{-1}$. Thus $\lambda_1(e\bar{\mathfrak{R}}) = \chi(1)/|G| \sum_{g\in\mathfrak{R}} \langle gx, x\rangle$ and it is therefore sufficient to show that $\lambda_1(e\bar{\mathfrak{R}}) = (|\mathfrak{R}|/|G|)\chi(k)$. Let $d = \dim_{\mathbb{R}} \mathrm{End}_{\mathbb{R}[G]}(M))$. Then $\varepsilon = \chi(1)/(|G|\cdot d) \sum_{g\in G} \chi(g)g^{-1}$ is the Wedderburn idempotent corresponding to M. We decompose $\varepsilon = e_1 + \cdots + e_s$ into primitive idempotents $e_i \in \mathbb{R}[G]$, where $e = e_1$ and $s = \chi(1)/d$. Then $e_i = u_i^{-1}eu_i$ for units $u_i \in \mathbb{R}[G]$. Since

$$\lambda_1(e_i\bar{\mathfrak{R}}) = \lambda_1(u_i^{-1}eu_i\bar{\mathfrak{R}}) = \lambda_1(u_i^{-1}e\bar{\mathfrak{R}}u_i) = \lambda_1(u_iu_i^{-1}e\bar{\mathfrak{R}}) = \lambda_1(e\bar{\mathfrak{R}}),$$

we obtain

$$(\chi(1)/d)\lambda_1(e\bar{\mathfrak{R}}) = \lambda_1(\varepsilon\bar{\mathfrak{R}}) = \chi(1)/(|G|\cdot d) \sum_{g\in\mathfrak{R}} \chi(g) = (\chi(1)/d)(|\mathfrak{R}|/|G|)\chi(k)),$$

which establishes the claim. □

ACKNOWLEDGEMENT. This paper was written when the first author was visiting Mainz and the second autor was visiting Aarhus and Haifa. We thank the *Deutsche Forschungsgemeinschaft* (*DFG*), the *Danish Nat-*

ural Science Research Council and the *Technion* (*Haifa*) for their financial support.

We are also indebted to P. Fleischmann, R. Knörr and A. Juhasz for helpful discussions.

References

[Al] A. Albert, Structure of algebras, AMS Colloquium Publications, 1939.

[BM] I. F. Blake, R. C. Mullin, The mathematical theory of coding, Academic Press, New York, 1975.

[CR] C. Curtis, I. Reiner, Methods of representation theory, John Wiley, New York 1981.

[HB] B. Huppert, N. Blackburn, Finite groups II, Springer-Verlag, Berlin, 1982.

[La] P. Landrock, Finite group algebras and their modules, Cambridge University Press, Cambridge, 1983.

[OT] T. Okuyama, Y. Tsushima, On a conjecture of P. Landrock, J. Algebra **104** (1986), 203–208.

[Wi] W. Willems, Metrische Moduln über Gruppenringen, Dissertation, Mainz, 1976.

Peter Landrock
Department of Mathematics
University of Aarhus
DK-8000 Aarhus
Denmark

Olaf Manz
Department of Mathematics (IWR)
University of Heidelberg
D-6900 Heidelberg
Germany

Current Address:
UCI
Utility Consultants International
D-6000 Frankfurt 71