A NOTE ON SURROGATE FORMS OF CENTRAL SIMPLE ALGEBRAS

By Thomas Unger*
Department of Mathematics, University College Dublin

[Received 26 April 2000. Read 12 October 2000. Published 28 December 2001.]

Abstract

Given a central simple algebra over a field of characteristic not two, the classical invariants of the surrogate form—the quadratic form arising from the quadratic coefficient in the reduced characteristic polynomial of the algebra—are investigated. It is shown that the surrogate form gives the same amount of information as the trace form. Then an involution of the first kind is introduced, and the invariants of the associated involution surrogate form are determined. Finally, the existence of some special subspaces of the algebra is demonstrated.

1. Introduction

The *surrogate form* of a central simple algebra over a field arises from the quadratic coefficient in the reduced characteristic polynomial of that algebra.

More precisely (see e.g. [3, 5]), let A be a central simple algebra of degree n (that is, of dimension n^2) over a field F of $\mathrm{char}(F) \neq 2$. Let Ω denote an algebraic closure of F. Under scalar extension to Ω, A becomes isomorphic to $M_n(\Omega)$. We can therefore fix an F-algebra embedding $A \hookrightarrow M_n(\Omega)$ and view every element $a \in A$ as a matrix in $M_n(\Omega)$. Its characteristic polynomial has coefficients in F and is independent of the embedding of A in $M_n(\Omega)$. We call it the *reduced characteristic polynomial* of a and denote it by

$$\mathrm{Prd}_{A,a}(X) = X^n - s_1(a)X^{n-1} + s_2(a)X^{n-2} - \cdots + (-1)^n s_n(a).$$

The coefficients $s_1(a)$ and $s_n(a)$ are respectively the *reduced trace* and the *reduced norm* of a, denoted

$$\mathrm{Trd}_A(a) = s_1(a) \qquad \text{and} \qquad \mathrm{Nrd}_A(a) = s_n(a).$$

As is well known, the reduced trace gives rise to a quadratic form

$$T_A : A \longrightarrow F, x \longmapsto T_A(x) := \mathrm{Trd}_A(x^2),$$

the *trace form* of A (see e.g. [6]). We call the coefficient $s_2(a)$ the *reduced surrogate* of a, and denote it by $\mathrm{Srd}_A(a)$. One can show (see e.g. [3, xvii]) that

$$s_1(a)^2 - s_1(a^2) = 2s_2(a).$$

* E-mail: thomas.unger@ucd.ie

This allows us to define a quadratic form

$$S_A : A \longrightarrow F, x \longmapsto S_A(x) := 2\,\mathrm{Srd}_A(x) = \mathrm{Trd}_A(x)^2 - \mathrm{Trd}_A(x^2),$$

which we call the *surrogate form* of A.

This form has been studied in the setting of étale algebras L over a field of characteristic two, where it functions as a surrogate for the ordinary trace form in the definition of a discriminant of L (see [1; 12; 15]).

In this note we will determine the classical quadratic form theoretic invariants of the surrogate form of a central simple algebra A of degree n over a field F of $\mathrm{char}(F) \neq 2$. Besides the *dimension* of the form, which is just the dimension of A, i.e. n^2, we mean by classical invariants the *discriminant, signatures* and *Hasse invariant* of the form. The main tool will be the 'comparison argument', which relates the surrogate form to the ordinary trace form of A. We will also determine annihilating polynomials for the surrogate form.

After that we define an *involution surrogate form* for central simple algebras with an involution of the first kind and determine its classical invariants.

We use the notation of [4] and [14] for quadratic forms and of [3] for central simple algebras (with an involution).

In Section 2 we briefly recall the definition of the classical invariants. In Section 3 we investigate the surrogate form. In Section 4 we define the involution surrogate form and investigate its properties. Finally, in Section 5 we show, as applications, the existence of some special subspaces of A.

2. The classical invariants of a quadratic form

Let $q : V \longrightarrow F$ be a non-singular quadratic form on a vector space of finite dimension n over a field F of $\mathrm{char}(F) \neq 2$.

The *discriminant* of q is defined as

$$\mathrm{disc}\, q := (-1)^{\frac{n(n-1)}{2}} \det q \bmod F^{\times 2},$$

where $\det q$ is the determinant of any Gram matrix of q.

Suppose $q \simeq \langle a_1, \dots, a_n\rangle$ (here $\simeq$ denotes isometry of quadratic forms). The *Hasse invariant* of q is defined as

$$s(q) := \prod_{i<j} (a_i, a_j) \in \mathrm{Br}(F),$$

where (a_i, a_j) is the class of the quaternion algebra $(\frac{a_i, a_j}{F})$ in the Brauer group $\mathrm{Br}(F)$ of F. Note that for $a, b \in F^\times$, (a, b) has order two in $\mathrm{Br}(F)$ and that $(1, a)$ is trivial in $\mathrm{Br}(F)$ for any $a \in F^\times$.

If q_1 and q_2 are two quadratic forms over F, then

$$s(q_1 \perp q_2) = s(q_1)s(q_2)(\det q_1, \det q_2). \tag{2.1}$$

If q is a quadratic form over F and $m \geq 1$ an integer, one can show by induction on

m that

$$s(m \times q) = s(q)^m (\det q, \det q)^{\binom{m}{2}}. \tag{2.2}$$

Now suppose that F is an ordered field with ordering $\mathscr{P}$. The *signature* of q at $\mathscr{P}$, $\operatorname{sig}_{\mathscr{P}} q$, is defined to be the number of positive entries minus the number of negative entries in q.

3. The surrogate form

Let A be a central simple algebra of degree n over a field F of characteristic different from two. In this section we will determine the classical invariants of the surrogate form S_A. The main tool will be Proposition 3.1, which relates the surrogate form to the ordinary trace form T_A.

Note that the symmetric bilinear forms associated to T_A and S_A are given by $b_{T_A}(x,y) = \operatorname{Trd}_A(xy)$ and $b_{S_A}(x,y) = \operatorname{Trd}_A(x)\operatorname{Trd}_A(y) - \operatorname{Trd}_A(xy)$ respectively.

Proposition 3.1 ('Comparison argument'). *Let A be a central simple F-algebra of degree $n \geq 1$ and suppose that* $\operatorname{char}(F)$ *does not divide n, then*

$$S_A \perp T_A \simeq \langle 1, n-1 \rangle \perp (n^2 - 1) \times \langle -1, 1 \rangle. \tag{3.1}$$

PROOF. Let $\mathscr{A} = \operatorname{Ker}\operatorname{Trd}_A = \{x \in A \mid \operatorname{Trd}_A(x) = 0\}$. This clearly is a subspace of A of codimension 1. Let us identify F with the $n \times n$ scalar matrices in $M_n(F)$. An easy calculation shows that $\mathscr{A}^{\perp} = F$ for both T_A and S_A. Hence we obtain the following orthogonal decomposition: $A \cong \mathscr{A} \perp F$ for both T_A and S_A. We can therefore decompose both the trace form and the surrogate form on A as follows: $T_A \simeq T_{\mathscr{A}} \perp T_F$ and $S_A \simeq S_{\mathscr{A}} \perp S_F$. From the definition of the surrogate form, we see immediately that $S_{\mathscr{A}} = -T_{\mathscr{A}}$. Also observe that $T_F \simeq \langle n \rangle$ and $S_F \simeq \langle n(n-1) \rangle$. It follows that $T_A \simeq T_{\mathscr{A}} \perp \langle n \rangle$ and $S_A \simeq -T_{\mathscr{A}} \perp \langle n(n-1) \rangle$. Since $T_{\mathscr{A}} \perp -T_{\mathscr{A}}$ is hyperbolic of dimension $2n^2 - 2$, we get $S_A \perp T_A \simeq \langle n, n(n-1) \rangle \perp (n^2-1) \times \langle -1, 1 \rangle$. Hence $S_A \perp T_A \simeq \langle 1, n-1 \rangle \perp (n^2 - 1) \times \langle -1, 1 \rangle$, provided that the characteristic of F does not divide n. ■

Remark 3.2. Note that when $\operatorname{char}(F)$ divides n, we can use the diagonalisation $S_A \perp T_A \simeq \langle n, n(n-1) \rangle \perp (n^2 - 1) \times \langle -1, 1 \rangle$. However, it will follow from Proposition 3.4 that S_A is singular in this case.

It is now clear that the surrogate form of A doesn't give any more information than the trace form of A when $\operatorname{char}(F) \neq 2$.

Corollary 3.3. *Let A and B be two central simple algebras over a field F of* $\operatorname{char}(F) \neq 2$. *Then*

$$T_A \simeq T_B \iff S_A \simeq S_B.$$

Now we can use the comparison argument together with the known invariants of T_A to calculate the invariants of the surrogate form. But first let us recall that, for an ordered field F and any ordering $\mathscr{P}$ of F, the *sign* of A at the ordering $\mathscr{P}$ of F, denoted $\operatorname{sgn}_{\mathscr{P}} A$, is defined as follows:

$$\operatorname{sgn}_{\mathscr{P}} A = \begin{cases} 0 & \text{if } F_{\mathscr{P}} \text{ is a splitting field of } A, \\ 1 & \text{otherwise,} \end{cases}$$

where $F_{\mathscr{P}}$ denotes the real closure of F with respect to $\mathscr{P}$.

Proposition 3.4. *Let A be a central simple F-algebra of degree $n \geq 1$ and suppose that* $\operatorname{char}(F)$ *does not divide n, then*

(i) *if A is split or n is odd,*

$$S_A \simeq \langle n-1 \rangle \perp (n-1) \times \langle -1 \rangle \perp \frac{n(n-1)}{2} \times \langle -1, 1 \rangle;$$

(ii) $\operatorname{disc} S_A = \det S_A = (-1)^{n-1}(n-1) \det T_A = (-1)^{\frac{(n+2)(n-1)}{2}}(n-1) \bmod F^{\times 2}$;

(iii)

$$s(S_A) = s(T_A)(n-1,-1)^{\frac{(n+2)(n-1)}{2}}(-1,-1)^{\frac{(n^2+2)(n-1)}{2}};$$

thus

$$s(S_A) = \begin{cases} (n-1,-1)^{\frac{(n+2)(n-1)}{2}}(-1,-1)^{\frac{(n+2)(n-1)(n^2-n+4)}{8}} & \textit{if } n \textit{ is odd} \\ A^{\frac{n}{2}}(n-1,-1)^{\frac{(n+2)(n-1)}{2}}(-1,-1)^{\frac{(n+2)(n-1)(n^2-n+4)}{8}} & \textit{if } n \textit{ is even} \end{cases};$$

(iv) *if F is an ordered field,* $\operatorname{sig}_{\mathscr{P}} S_A + \operatorname{sig}_{\mathscr{P}} T_A = 2$ *for any ordering $\mathscr{P}$ of F, i.e.*

$$\operatorname{sig}_{\mathscr{P}} S_A = (-1)^{\operatorname{sgn} A+1} \deg A + 2.$$

Proof. (i) Suppose that A is split (i.e. $A \cong M_n(F)$), then the statement follows using the comparison argument, the well-known diagonalisation of the trace form

$$T_{M_n(F)} \simeq n \times \langle 1 \rangle \perp \frac{n(n-1)}{2} \times \langle -1, 1 \rangle$$

and Witt cancellation. Suppose next that $\deg A = n$ is odd. Let $L \subset A$ be a maximal subfield. It is well known that L has degree n over F and that it is a splitting field for A (see e.g. [10, 240–2]). Thus if n is odd, it follows from Springer's Theorem (see e.g. [14, 47]) that T_A is isometric to $T_{M_n(F)}$ and that S_A is isometric to $S_{M_n(F)}$. So the statement follows again.

(ii) This follows from the comparison argument and the fact that $\det T_A = (-1)^{\frac{n(n-1)}{2}} \bmod F^{\times 2}$. Since the surrogate form has dimension n^2, its determinant equals its discriminant.

(iii) Taking Hasse invariants of both sides of (3.1) gives

$$s(S_A) = s(T_A)(\det S_A, \det T_A)(n-1,-1)^{n-1}(-1,-1)^{n-1}.$$

Here we used (2.1), (2.2) and the fact that $n^2-1 \equiv n-1 \equiv \binom{n^2-1}{2}$ (mod 2). Hence

$$s(S_A) = s(T_A)((n-1)(-1)^{k+n-1}, (-1)^k)(n-1,-1)^{n-1}(-1,-1)^{n-1},$$

where $k = \binom{n}{2} = \frac{n(n-1)}{2}$. The first formula of (iii) follows using the fact that $k^2 \equiv k$ (mod 2). The second part comes from combining this with the known computations

$$s(T_A) = \begin{cases} (-1,-1)^{\binom{k}{2}} & \text{if } n \text{ is odd} \\ A^{\frac{n}{2}}(-1,-1)^{\binom{k}{2}} & \text{if } n \text{ is even} \end{cases} \tag{3.2}$$

and the fact that $\binom{k}{2} + \frac{(n^2+2)(n-1)}{2} \equiv \frac{(n+2)(n-1)(n^2-n+4)}{8}$ (mod 2). Note that the odd case in (3.2) follows by direct computation, using the diagonalisation of T_A, while the even case was computed by Lewis and Morales [8, 3].

(iv) This follows directly from (3.1) and the fact that $\operatorname{sig}_{\mathscr{P}} T_A = (-1)^{\operatorname{sgn} A} \deg A$, as shown by Lewis [6, 370]. ■

It is now clear that the surrogate form is non-singular when char(F) does not divide n and $n-1$.

Finally, recall that a polynomial $p(x)$ is said to *annihilate* the quadratic form φ over F if $p(\varphi) = 0$ in the Witt ring $W(F)$ (see e.g. [5]). For example, one can easily show that any n-fold Pfister form is annihilated by $x^2 - 2^n x$.

Proposition 3.5.

(i) *Let A be a central simple F-algebra of degree n; then $p_A(x) := (x-2+n)(x-2-n)(x+n)(x-n)$ annihilates the surrogate form S_A of A. In the following special cases we can do better than this.*

(ii) *Let $M = M_n(F)$; then $p_M(x) := (x-2+n)(x+n)$ annihilates the surrogate form S_M of the full matrix algebra M.*

(iii) *Let $Q = (\frac{a,b}{F})$; then $p_Q(x) := x(x-4)(x+4)$ annihilates the surrogate form S_Q of the quaternion algebra Q.*

PROOF. (i) By the comparison argument, $S_A \perp T_A = \langle 1, n-1\rangle$ in $W(F)$. So $S_A = -T_A \perp \langle 1, n-1\rangle$ in $W(F)$. Since $x^2 - n^2$ annihilates $-T_A$ (see [6, 370]) and since $x^2 - 2x$ annihilates the Pfister form $\langle 1, n-1\rangle$, it follows that S_A is annihilated by $(x-n)(x+n)(x-2-n)(x-2+n)$ by the proposition of [5, §2] with $q_1(x) = x^2 - n^2$ and $q_2(x) = x^2 - 2x$.

(ii) We know that $S_M = \langle n-1\rangle \perp (n-1) \times \langle -1\rangle$ in the Witt ring $W(F)$. So, $S_M \perp (n-1) \times \langle 1\rangle = \langle n-1\rangle$, and hence $(S_M \perp (n-1) \times \langle 1\rangle)^2 = \langle n-1\rangle^2 = \langle 1\rangle$. This implies $(S_M \perp (n-2) \times \langle 1\rangle) \otimes (S_M \perp n \times \langle 1\rangle) = 0$ in $W(F)$.

(iii) A simple calculation shows that $S_Q = \langle 2, -2a, -2b, 2ab\rangle$. In other words, $S_Q = \langle 2\rangle\psi$, where ψ is the 2-fold Pfister form $\langle\langle -a, -b\rangle\rangle$. Therefore $\psi^2 = 4 \times \psi$ and so $S_Q^2 = 4 \times \psi = 4 \times \langle 2\rangle S_Q$. Hence $S_Q^3 = 4 \times \langle 2\rangle S_Q^2 = 16 \times S_Q$. Thus S_Q is annihilated by $x^3 - 16x = x(x-4)(x+4)$. ■

4. The involution surrogate form

Let F be a field of characteristic different from two. Let A be a central simple algebra over F with an involution σ of the first kind (i.e. an anti-automorphism of period two that is the identity map on the centre F of A). We will assume in the rest of this article that char(F) does not divide the degree of A.

In this section we will study the *involution surrogate form* of (A, σ), which is defined to be the quadratic form

$$S_\sigma : A \longrightarrow F, \ x \longmapsto \mathrm{Trd}_A(x)^2 - T_\sigma(x),$$

where T_σ is the *involution trace form*,

$$T_\sigma : A \longrightarrow F, \ x \longmapsto \mathrm{Trd}_A(x\sigma(x)),$$

studied by Lewis [7].

Let $A_+ = \{x \in A \mid \sigma(x) = x\}$ and $A_- = \{x \in A \mid \sigma(x) = -x\}$ be the subspaces of *symmetric* and *skew-symmetric* elements respectively. Let $\deg A = n$ (i.e. A has dimension n^2). The involution σ is said to be *orthogonal* when $\dim A_+ = \frac{n(n+1)}{2}$ and $\dim A_- = \frac{n(n-1)}{2}$, while it is said to be *symplectic* when the dimensions of A_+ and A_- are reversed.

One can easily check that $A_+^\perp = A_-$ for both the involution trace form and the involution surrogate form. Hence we have the orthogonal decomposition $A \cong A_+ \perp A_-$ and can write $T_\sigma = T_\sigma^+ \perp T_\sigma^-$ and $S_\sigma = S_\sigma^+ \perp S_\sigma^-$. Furthermore, the ordinary trace form and surrogate form also decompose orthogonally on $A_+ \perp A_-$, $T_A = T_A^+ \perp T_A^-$ and $S_A = S_A^+ \perp S_A^-$. One can easily verify that $T_A^+ = T_\sigma^+$, while $T_A^- = -T_\sigma^-$. The following lemma compares the involution surrogate and trace forms, analogous to Proposition 3.1.

Lemma 4.1.

(i) $S_\sigma^+ = S_A^+$ *and*

$$S_\sigma^+ \perp T_\sigma^+ \simeq \langle 1, n-1 \rangle \perp (\dim A_+ - 1) \times \langle -1, 1 \rangle.$$

(ii) $S_\sigma^- = -S_A^- = T_A^- = -T_\sigma^-$ *and thus*

$$S_\sigma^- \perp T_\sigma^- \simeq \dim A_- \times \langle -1, 1 \rangle.$$

(iii) $S_\sigma \perp T_\sigma \simeq \langle 1, n-1 \rangle \perp (n^2 - 1) \times \langle -1, 1 \rangle.$

Proof. (i) Since $T_\sigma^+ = T_A^+$, we have $S_\sigma^+ = S_A^+$. For the second part, mimic the proof of Proposition 3.1.

(ii) An easy calculation using the well-known fact that $\mathrm{Trd}_A(\sigma(x)) = \mathrm{Trd}_A(x)$, which implies that $\mathrm{Trd}_A(a) = 0$ for all $a \in A_-$.

(iii) Follows directly from (i) and (ii). ■

As in the previous section, the classical invariants of the involution surrogate form can now be calculated, using the known invariants of the involution trace form and Lemma 4.1. We will therefore omit details in the proofs since they are all simple—but sometimes rather tedious—calculations.

The discriminant of an involution is only defined when the degree of A is even. We will therefore assume for the moment that $\deg A = n = 2m$. We will briefly recall the definition of the determinant and the discriminant of an involution (see [3, 81] for more details). Let σ be an orthogonal involution. One can show that each unit in A_- has the same reduced norm. The *determinant* of σ is the square class of the reduced norm of any skew-symmetric unit:

$$\det \sigma = \mathrm{Nrd}_A(a) \cdot F^{\times 2} \in F^\times / F^{\times 2}$$

for any $a \in A_- \cap A^\times$. When σ is symplectic, we define $\det \sigma = 1$. The *discriminant* of σ (orthogonal or symplectic) is defined to be

$$\operatorname{disc} \sigma = (-1)^m \det \sigma \in F^\times / F^{\times 2}.$$

Proposition 4.2. *Let (A, σ) be a central simple algebra over F of even degree $n = 2m$ with an involution of the first kind. Let S_σ be the involution surrogate form of (A, σ), with orthogonal decomposition $S_\sigma^+ \perp S_\sigma^-$ on $A_+ \perp A_-$.*

(i) *If $n \equiv 0 \pmod 4$, then $\det S_\sigma^- = \operatorname{disc} \sigma$ and $\det S_\sigma^+ = (1-n) \operatorname{disc} \sigma$.*

(ii) *If $n \equiv 2 \pmod 4$, then $\det S_\sigma^- = 2 \operatorname{disc} \sigma$ and $\det S_\sigma^+ = 2(1-n) \operatorname{disc} \sigma$.*

In both cases we have $\det S_\sigma = 1 - n$.

PROOF. In [7], Lewis shows that $\det T_\sigma^+ = \det T_\sigma^-$ and determines the relationship between $\det T_\sigma^+$ and the determinant of σ (which he calls the discriminant). In particular, he shows that

$$\det T_\sigma^+ = \begin{cases} \det \sigma & \text{if } n \equiv 0 \pmod 4, \\ 2 \det \sigma & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

Some calculations, using Lemma 4.1, finish the proof. ■

Proposition 4.3. *Let (A, σ) be a central simple algebra of degree n over F with involution of the first kind. Let S_σ be the involution surrogate form of (A, σ). Then the following relations hold in the Brauer group of F:*

$$s(S_\sigma) = \begin{cases} A^{n/2}(-1, \det \sigma)(-n, 1-n) & \text{if } n \text{ is even and } \sigma \text{ is orthogonal}, \\ A^{n/2}(-1, -1)^{n/2}(-n, 1-n) & \text{if } n \text{ is even and } \sigma \text{ is symplectic}, \\ 1 & \text{if } n \text{ is odd}. \end{cases}$$

PROOF. In [7] Lewis calculates the Hasse invariant of the involution trace form T_σ

and obtains the following relations in the Brauer group of F:

$$s(T_\sigma) = \begin{cases} A^{n/2}(-1, \det\sigma) & \text{if } n \text{ is even and } \sigma \text{ is orthogonal,} \\ A^{n/2}(-1,-1)^{n/2} & \text{if } n \text{ is even and } \sigma \text{ is symplectic,} \\ 1 & \text{if } n \text{ is odd.} \end{cases}$$

Some calculations, using Lemma 4.1, finish the proof. ■

Proposition 4.4. *Let (A, σ) be a central simple algebra of even degree $n = 2m$ over a field F of* $\mathrm{char}(F) \neq 2$ *with involution of the first kind.*

(i) *If* $n \equiv 0 \pmod 4$, *then*

$$s(S_\sigma^-) = \begin{cases} A^{\frac{m(m+1)}{2}}(-1, \det\sigma) & \textit{if } \sigma \textit{ is symplectic,} \\ A^{\frac{m(m-1)}{2}}(-1,-1)^{\frac{m(m+1)}{2}}(2, \det\sigma) & \textit{if } \sigma \textit{ is orthogonal,} \end{cases}$$

and

$$s(S_\sigma^+) = \begin{cases} A^{\frac{m(m-1)}{2}}(1-2m, -\det\sigma) & \textit{if } \sigma \textit{ is symplectic,} \\ A^{\frac{m(m+1)}{2}}(-1,-1)^{\frac{m(m+1)}{2}}(2, \det\sigma) & \\ \qquad (1-2m, -\det\sigma) & \textit{if } \sigma \textit{ is orthogonal.} \end{cases}$$

(ii) *If* $n \equiv 2 \pmod 4$, *then*

$$s(S_\sigma^-) = \begin{cases} A^{\frac{m(m+1)}{2}} & \textit{if } \sigma \textit{ is symplectic,} \\ A^{\frac{m(m-1)}{2}}(-1,-1)^{\frac{m(m-1)}{2}}(-2, \det\sigma) & \textit{if } \sigma \textit{ is orthogonal,} \end{cases}$$

and

$$s(S_\sigma^+) = \begin{cases} A^{\frac{m(m-1)}{2}}(2m-1, 2\det\sigma) & \textit{if } \sigma \textit{ is symplectic,} \\ A^{\frac{m(m+1)}{2}}(-1,-1)^{\frac{m^2-m+2}{2}}(2m-1, 2\det\sigma) & \textit{if } \sigma \textit{ is orthogonal.} \end{cases}$$

Proof. In [11, 307], Quéguiner calculates the Hasse invariant of T_σ^+ and T_σ^- when $\deg A = n = 2m$ is even:

$$s(T_\sigma^+) = \begin{cases} A^{\frac{m(m-1)}{2}}(-1,-1)^{\frac{m(m-1)}{2}} & \text{if } \sigma \text{ is symplectic,} \\ A^{\frac{m(m+1)}{2}}(-2, \det\sigma)^{m-1} & \text{if } \sigma \text{ is orthogonal,} \end{cases}$$

$$s(T_\sigma^-) = \begin{cases} A^{\frac{m(m+1)}{2}}(-1,-1)^{\frac{m(m+1)}{2}} & \text{if } \sigma \text{ is symplectic,} \\ A^{\frac{m(m-1)}{2}}(-2, \det\sigma)^{m-1} & \text{if } \sigma \text{ is orthogonal.} \end{cases}$$

Some calculations, using Lemma 4.1, finish the proof. ■

Let A be a central simple algebra over an ordered field F with ordering $\mathscr{P}$ and let σ be an involution of the first kind on A. In [9] Lewis and Tignol define the notion of a *signature* of an involution of the first kind in terms of the involution trace form T_σ,

$$\operatorname{sig}_{\mathscr{P}} \sigma = \sqrt{\operatorname{sig}_{\mathscr{P}} T_\sigma}.$$

Proposition 4.5. *Let A be a central simple algebra over an ordered field F with ordering $\mathscr{P}$ and let σ be an involution of the first kind on A. Then*

$$\operatorname{sig}_{\mathscr{P}} S_\sigma = 2 - (\operatorname{sig}_{\mathscr{P}} \sigma)^2.$$

PROOF. This follows directly from Lemma 4.1(iii). ■

5. Applications

In this final section, we show the existence of some special subspaces of the algebra A.

Proposition 5.1. *Let A be a central simple algebra of odd degree n over a formally real field F. There exists a subspace $W \subset A$ of dimension $n-2$ for which*

$$\operatorname{Trd}_A(x)^2 < \operatorname{Trd}_A(x^2), \ \forall x \in W, x \neq 0.$$

PROOF. When $\deg A$ is odd, we have that $T_A \simeq T_{M_n(F)}$ and $S_A \simeq S_{M_n(F)}$ by Springer's Theorem as remarked earlier. So,

$$S_A \simeq \langle n-1 \rangle \perp (n-1) \times \langle -1 \rangle \perp \frac{n(n-1)}{2} \times \langle 1, -1 \rangle.$$

Clearly $\langle n-1 \rangle \perp (n-1) \times \langle -1 \rangle$ is isotropic and so contains at least one hyperbolic plane, which we can take to be $\langle n-1, -(n-1) \rangle$. Therefore,

$$\langle n-1 \rangle \perp (n-1) \times \langle -1 \rangle \simeq \mu \perp \langle n-1, -(n-1) \rangle$$

for some quadratic form μ. By Witt cancellation we get

$$(n-1) \times \langle -1 \rangle \simeq \mu \perp \langle -(n-1) \rangle,$$

i.e. μ is a subform of $(n-1) \times \langle -1 \rangle$ and is therefore negative definite. So

$$S_A \simeq \mu \perp \text{hyperbolic part},$$

where μ is negative definite of dimension $n-2$. ■

Proposition 5.2. *Let F be a field of characteristic $\neq 2$ and let A be a central simple F-algebra of odd degree n. There exists a subspace $U \subset A$ of dimension $\geq \frac{n^2-n+2}{2}$ on which Trd_A is multiplicative, i.e.*

$$\operatorname{Trd}_A(xy) = \operatorname{Trd}_A(x)\operatorname{Trd}_A(y), \ \forall x, y \in U.$$

Proof. Again we have

$$S_A \simeq \langle n-1\rangle \perp (n-1)\times\langle -1\rangle \perp \frac{n(n-1)}{2}\times\langle 1,-1\rangle.$$

Clearly $\langle n-1\rangle \perp (n-1)\times\langle -1\rangle$ is isotropic and so contains at least one hyperbolic plane. Therefore the Witt index of S is at least $\frac{n^2-n+2}{2}$ and hence there is a subspace $U \subset A$ of dimension $\geq \frac{n^2-n+2}{2}$ such that

$$S_A(x,y) = \operatorname{Trd}_A(x)\operatorname{Trd}_A(y) - \operatorname{Trd}_A(xy) = 0,\ \forall x,y \in U.$$

(Note: xy need not be in U when x and y are in U.) ■

Remark 5.3. When n is even, the previous proposition is false as the following counterexample shows. Let F be formally real and $A = (\frac{-1,-1}{F})$. Then $S_A = \langle 2,2,2,2\rangle$ and there is no non-trivial subspace of A on which this form vanishes.

Recall that a field extension E/F is called *cyclic* if E/F is Galois and $\operatorname{Gal}(E/F)$ is a cyclic group and that a central simple F-algebra A is *cyclic* if there is a strictly maximal subfield E of A such that E/F is a cyclic extension.

A celebrated theorem of Wedderburn states that if A is a central simple F-algebra of degree 3, then A is cyclic. (For a proof, see [10, 288]. More information about cyclic division algebras can also be found in this monograph.)

Ever since Wedderburn proved this theorem, it has been an open question whether every central simple F-algebra of odd prime degree n is cyclic. A necessary and sufficient condition for this to happen is the existence of an element $a \neq 0$ whose minimal polynomial is $\lambda^n - \det(a)$, i.e. an element a for which

$$\operatorname{Trd}_A(a) = \operatorname{Trd}_A(a^2) = \cdots = \operatorname{Trd}_A(a^{n-1}) = 0.$$

Rowen [13, 767] shows that any central simple algebra of odd degree n contains an element $a \neq 0$ with $\operatorname{Trd}_A(a) = \operatorname{Trd}_A(a^2) = 0$. In particular, when $n = 3$, this yields another proof of Wedderburn's theorem. Rowen's result can be strengthened, as the following proposition shows.

Proposition 5.4. *Let F be a field of characteristic $\neq 2$ and let A be a central simple F-algebra of odd degree n. There exists a subspace $V \subset A$ of dimension $\frac{n(n-1)}{2}$ such that*

$$\operatorname{Trd}_A(x) = 0 = \operatorname{Trd}_A(xy),\ \forall x,y \in V.$$

Proof. Let $\mathscr{A} = \operatorname{Ker}\operatorname{Trd}_A$ and let $V' = \mathscr{A} \cap U$, where U is the subspace occurring in Proposition 5.2. Since $\mathscr{A}$ has codimension 1 in A, V' has codimension at most 1 in U, and thus the dimension of V' is at least $\frac{n^2-n+2}{2} - 1 = \frac{n(n-1)}{2}$. However, if $x \in V'$, then x is in fact an element of the maximal totally isotropic subspace V of the trace from T_A. Since $\dim V = \frac{n(n-1)}{2}$, we thus get $V' = V$. ■

Formanek [2, 342] obtains this result too, using a different method.

ACKNOWLEDGEMENTS

I thank my advisor, David W. Lewis, for suggesting the topic of this paper and for his guidance. I also thank the referee, whose suggestions were very helpful in improving the original version of this article. This research was supported by Enterprise Ireland.

REFERENCES

[1] A.-M. Bergé and J. Martinet, Formes quadratiques et extensions en caractéristique 2, *Annales de l'Institut Fourier (Université de Grenoble)* **35** (2) (1985), 57–77.

[2] E. Formanek, Some remarks about the reduced trace, *Israel Mathematical Conference Proceedings* **1** (1989), 337–43.

[3] M.-A. Knus, A.S. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications 44, American Mathematical Society, Providence, RI, 1988.

[4] T.Y. Lam, *The algebraic theory of quadratic forms*, W.A. Benjamin Inc., Reading, Mass., 1973.

[5] D.W. Lewis, Witt rings as integral rings, *Inventiones Mathematicae* **90** (1987), 631–3.

[6] D.W. Lewis, Trace forms of central simple algebras, *Mathematische Zeitschrift* **215** (1994), 367–75.

[7] D.W. Lewis, A note on trace forms and involutions of the first kind, *Expositiones Mathematicae* **15** (1997), 265–72.

[8] D.W. Lewis and J.F. Morales, The Hasse invariant of the trace form of a central simple algebra, *Publications Mathématiques de la Faculté des Sciences de Besançon, Théorie des nombres, Année 1993–94* (1995), 1–6.

[9] D.W. Lewis and J.-P. Tignol, On the signature of an involution, *Archiv der Mathematik* **60** (1993), 128–35.

[10] R.S. Pierce, *Associative algebras*, Graduate Texts in Mathematics 88, Springer-Verlag, New York, 1982.

[11] A. Quéguiner, Cohomological invariants of algebras with involution, *Journal of Algebra* **194** (1997), 299–330.

[12] P. Revoy, Remarques sur la forme trace, *Linear and Multilinear Algebra* **10** (3) (1981), 223–33.

[13] L.H. Rowen, Brauer factor sets and simple algebras, *Transactions of the American Mathematical Society* **282** (2) (1984), 767–72.

[14] W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften 270, Springer-Verlag, Berlin, 1985.

[15] A.R. Wadsworth, Discriminants in characteristic two, *Linear and Multilinear Algebra* **17** (3–4) (1985), 235–63.