Bull. Aust. Math. Soc. **96** (2017), 412–425
doi:10.1017/S0004972717000466

SYMMETRIC SQUARE-CENTRAL ELEMENTS IN PRODUCTS OF ORTHOGONAL INVOLUTIONS IN CHARACTERISTIC TWO

A.-H. NOKHODKAR

(Received 18 February 2017; accepted 8 April 2017; first published online 17 August 2017)

Abstract

In characteristic two, some criteria are obtained for a symmetric square-central element of a totally decomposable algebra with orthogonal involution, to be contained in an invariant quaternion subalgebra.

2010 *Mathematics subject classification*: primary 16W10; secondary 16K20, 11E39.

Keywords and phrases: central simple algebra, totally decomposable algebra, square-central element, orthogonal involution, quaternion subalgebra.

1. Introduction

A classical question concerning central simple algebras is to identify conditions under which a square-central element lies in a quaternion subalgebra. This question is only solved for certain special cases in the literature. Let A be a central simple algebra of exponent two over a field F. In [2, (3.2)] it was shown that if $\operatorname{char} F \neq 2$ and F is of cohomological dimension less than or equal to 2, then every square-central element of A is contained in a quaternion subalgebra (see also [4, (4.2)]). In [3, (4.1)], it was shown that if $\operatorname{char} F \neq 2$, then an element $x \in A$ with $x^2 = \lambda^2 \in F^{\times 2}$ lies in a (split) quaternion subalgebra if and only if $\dim_F(x - \lambda)A = \frac{1}{2}\dim_F A$. This result was generalised in [14, (3.2)] to an arbitrary characteristic and including $\lambda = 0$. On the other hand, in [18] it was shown that there is an indecomposable algebra of degree 8 and exponent 2, containing a square-central element (see [8, (5.6.10)]). Using similar methods, it was shown in [3] that for $n \geqslant 3$ there exists a tensor product of n quaternion algebras containing a square-central element which does not lie in any quaternion subalgebra.

A similar question for a central simple algebra with involution (A, σ) over F is whether a symmetric or skew-symmetric square-central element of A lies in a σ-invariant quaternion subalgebra. In the case where $\operatorname{char} F \neq 2$, $\deg_F A = 8$ and σ has a trivial discriminant, the index of A is not 2 and one of the components of the Clifford algebra $C(A, \sigma)$ splits, it was shown in [17, (3.14)] that every skew-symmetric square-central element of A lies in a σ-invariant quaternion subalgebra. In [14], some criteria were obtained for symmetric and skew-symmetric elements whose squares lie in F^2 to be contained in a σ-invariant quaternion subalgebra. Also, a sufficient condition was obtained in [12, (6.3)] for symmetric square-central elements in a totally decomposable algebra with orthogonal involution in characteristic two, to be contained in a stable quaternion subalgebra.

In this work we study some properties of symmetric square-central elements in totally decomposable algebras with orthogonal involution in characteristic two. Let (A, σ) be a totally decomposable algebra with orthogonal involution over a field F of characteristic two and let $x \in A \setminus F$ be a symmetric element with $\alpha := x^2 \in F$. Since the case where $\alpha \in F^2$ was investigated in [14], we assume that $\alpha \in F^\times \setminus F^{\times 2}$. First, in Section 3, we study some properties of *inseparable subalgebras*, introduced in [12]. It is shown in Theorem 3.8 that (A, σ) has a unique inseparable subalgebra if and only if either $\deg_F A \leqslant 4$ or σ is anisotropic. In Section 4, we study some isotropy properties of a totally decomposable algebra with orthogonal involution (A, σ). Let $x \in A$ be an alternating element with $x^2 \in F^\times \setminus F^{\times 2}$ and let $C = C_A(x)$. As we shall see in Theorem 4.7, if $(C, \sigma|_C)$ is totally decomposable, then (A, σ) and $(C, \sigma|_C)$ have the same isotropy behaviour. We then study our main problem in Sections 5 and 6. For the case where σ is anisotropic or A has degree 4, it is shown that every symmetric square-central element of A lies in a σ-invariant quaternion subalgebra (see Theorem 5.1 and Proposition 5.2). However, we will see in Proposition 6.3 that if σ is isotropic, $\deg_F A \geqslant 8$ and $(A, \sigma) \not\simeq (M_{2^n}(F), t)$, there always exists a symmetric square-central element of (A, σ) which is not contained in any σ-invariant quaternion subalgebra of A. If A has degree 8 or σ satisfies a certain isotropy condition, it is shown in Proposition 5.7 and Theorem 5.10 that a symmetric square-central element of A lies in a σ-invariant quaternion subalgebra if and only if it is contained in an inseparable subalgebra of (A, σ). Finally, in Example 6.4 we shall see that this criterion cannot be applied to arbitrary involutions.

2. Preliminaries

Throughout this paper, F denotes a field of characteristic two.

Let A be a central simple algebra over F. An *involution* on A is an antiautomorphism $\sigma : A \to A$ of order two. If $\sigma|_F = \mathrm{id}$, we say that σ is of *the first kind*. The sets of *alternating* and *symmetric* elements of (A, σ) are defined as

$$\mathrm{Sym}(A, \sigma) = \{x \in A \mid \sigma(x) = x\} \quad \text{and} \quad \mathrm{Alt}(A, \sigma) = \{\sigma(x) - x \mid x \in A\}.$$

For a field extension K/F we use the notation $A_K = A \otimes K$, $\sigma_K = \sigma \otimes \mathrm{id}$ and $(A, \sigma)_K = (A_K, \sigma_K)$. An extension K/F is called a *splitting field* of A if A_K splits, that is, A_K is isomorphic to the matrix algebra $M_n(K)$, where $n = \deg_F A$ is the degree of A over F. If $(V, \mathfrak{b})$ is a symmetric bilinear space over F, the pair $(\mathrm{End}_F(V), \sigma_\mathfrak{b})$ is denoted by $\mathrm{Ad}(\mathfrak{b})$, where $\sigma_\mathfrak{b}$ is the *adjoint involution* of $\mathrm{End}_F(V)$ with respect to $\mathfrak{b}$

(see [9, page 2]). According to [9, (2.1)], if K is a splitting field of A, then $(A,\sigma)_K$ is adjoint to a symmetric bilinear space $(V,\mathfrak{b})$ over K. We say that σ is *symplectic* if this form is alternating, that is, $\mathfrak{b}(v,v)=0$ for every $v\in V$. Otherwise, σ is called *orthogonal*. By [9, (2.6)], σ is symplectic if and only $1\in \mathrm{Alt}(A,\sigma)$. An involution σ on a central simple algebra A is called *isotropic* if $\sigma(x)x=0$ for some nonzero element $x\in A$. Otherwise, σ is called *anisotropic*. If σ is an orthogonal involution, the *discriminant* of σ is denoted by $\mathrm{disc}\,\sigma$ (see [9, (7.2)]).

A *quaternion algebra* over F is a central simple algebra of degree 2. An algebra with involution (A,σ) over F is called *totally decomposable* if it decomposes into tensor products of quaternion F-algebras with involution. If $(A,\sigma)\simeq\bigotimes_{i=1}^n(Q_i,\sigma_i)$ is a totally decomposable algebra with orthogonal involution over F, then every σ_i is necessarily orthogonal by [9, (2.23)].

Let $(V,\mathfrak{b})$ be a bilinear space over F and let $\alpha\in F$. We say that $\mathfrak{b}$ *represents* α if $\mathfrak{b}(v,v)=\alpha$ for some nonzero vector $v\in V$. The set of elements in F represented by $\mathfrak{b}$ is denoted by $D(\mathfrak{b})$. We also set $Q(\mathfrak{b})=D(\mathfrak{b})\cup\{0\}$. Observe that $Q(\mathfrak{b})$ is an F^2-subspace of F. If K/F is a field extension, the scalar extension of $\mathfrak{b}$ to K is denoted by $\mathfrak{b}_K$. For $\alpha_1,\ldots,\alpha_n\in F^\times$, the diagonal bilinear form $\sum_{i=1}^n\alpha_ix_iy_i$ is denoted by $\langle\alpha_1,\ldots,\alpha_n\rangle$. The form $\langle\langle\alpha_1,\ldots,\alpha_n\rangle\rangle:=\langle 1,\alpha_1\rangle\otimes\cdots\otimes\langle 1,\alpha_n\rangle$ is called a *bilinear (n-fold) Pfister form*. If $\mathfrak{b}$ is a bilinear Pfister form over F, then there exists a bilinear form $\mathfrak{b}'$, called the *pure subform of* $\mathfrak{b}$, such that $\mathfrak{b}\simeq\langle 1\rangle\perp\mathfrak{b}'$. The form $\mathfrak{b}'$ is uniquely determined, up to isometry (see [1, page 906]).

3. The inseparable subalgebra

For an algebra with involution (A,σ) over F, we use the following notation:

$$\begin{aligned}\mathrm{Alt}(A,\sigma)^+&=\{x\in\mathrm{Alt}(A,\sigma)\mid x^2\in F\},\\ \mathrm{Sym}(A,\sigma)^+&=\{x\in\mathrm{Sym}(A,\sigma)\mid x^2\in F\},\\ S(A,\sigma)&=\{x\in A\mid \sigma(x)x\in\mathrm{Alt}(A,\sigma)\oplus F\}.\end{aligned}$$

The set $S(A,\sigma)$ was introduced in [16]. Note that $x\in S(A,\sigma)$ if and only if there exists a unique element $\alpha\in F$ such that $\sigma(x)x+\alpha\in\mathrm{Alt}(A,\sigma)$. As in [16], the element α is denoted by $q_\sigma(x)$. We thus obtain a map $q_\sigma: S(A,\sigma)\to F$ satisfying

$$\sigma(x)x+q_\sigma(x)\in\mathrm{Alt}(A,\sigma)\quad\text{for } x\in S(A,\sigma).$$

According to [16, (3.2) and (3.3)], $S(A,\sigma)$ is an F-subalgebra of A and q_σ is a totally singular quadratic form on $S(A,\sigma)$, that is, $q_\sigma(\lambda x+y)=\lambda^2q_\sigma(x)+q_\sigma(y)$ for $\lambda\in F$ and $x,y\in S(A,\sigma)$. Note that if $x\in S(A,\sigma)$ and $\alpha:=x^2\in F$, then $\sigma(x)x+\alpha=0\in\mathrm{Alt}(A,\sigma)$; hence, $x\in S(A,\sigma)$ and $q_\sigma(x)=\alpha$. In other words, $\mathrm{Sym}(A,\sigma)^+\subseteq S(A,\sigma)$ and the restriction of $q_\sigma(x)$ to $\mathrm{Sym}(A,\sigma)^+$ is the squaring map $x\mapsto x^2$.

Let $(A,\sigma)\simeq\bigotimes_{i=1}^n(Q_i,\sigma_i)$ be a totally decomposable algebra of degree 2^n with orthogonal involution over F. According to [12, (4.6)] there exists a 2^n-dimensional subalgebra $\Phi\subseteq\mathrm{Sym}(A,\sigma)^+$, called an *inseparable subalgebra* of (A,σ), satisfying:

(i) $C_A(\Phi) = \Phi$, where $C_A(\Phi)$ is the centraliser of Φ in A; and
(ii) Φ is generated, as an F-algebra, by n elements.

For every inseparable subalgebra Φ of (A, σ) we have necessarily $\Phi \subseteq \mathrm{Alt}(A, \sigma)^+ \oplus F$. It follows that

$$\Phi \subseteq \mathrm{Alt}(A, \sigma)^+ \oplus F \subseteq \mathrm{Sym}(A, \sigma)^+ \subseteq S(A, \sigma). \tag{3.1}$$

By [12, (5.10)], if Φ_1 and Φ_2 are two inseparable subalgebras of (A, σ), then $\Phi_1 \simeq \Phi_2$ as F-algebras. Note that if $v_i \in \mathrm{Sym}(Q_i, \sigma_i)^+ \setminus F$ is a unit for $i = 1, \dots, n$, then $F[v_1, \dots, v_n]$ is an inseparable subalgebra of (A, σ).

Theorem 3.1. *Let (A, σ) be a totally decomposable algebra with anisotropic orthogonal involution over F and let Φ be an inseparable subalgebra of (A, σ). Then $\Phi = \mathrm{Alt}(A, \sigma)^+ \oplus F = \mathrm{Sym}(A, \sigma)^+ = S(A, \sigma)$ is a maximal subfield of A. In particular, the inseparable subalgebra Φ is uniquely determined.*

Proof. By [16, (4.1)], Φ is a field and $S(A, \sigma) = \Phi$. Hence, the required equalities follow from (3.1). Also, as $\dim_F \Phi = \deg_F A$, Φ is a maximal subfield of A. □

Lemma 3.2. *Let (A, σ) be a central simple F-algebra with orthogonal involution and let $x \in \mathrm{Alt}(A, \sigma)^+$. If $x^2 \notin F^2$, then $\mathrm{Sym}(C_A(x), \sigma|_{C_A(x)})^+ \subseteq \mathrm{Sym}(A, \sigma)^+$.*

Proof. Set $\alpha = x^2 \in F^\times \setminus F^{\times 2}$ and $K = F(x) = F(\sqrt{\alpha})$. Then $C_A(x)$ is a central simple algebra over K. Let $u \in \mathrm{Sym}(C_A(x), \sigma|_{C_A(x)})^+$ and write $u^2 = a + bx$ for some $a, b \in F$. Then $u^2 + a = bx \in \mathrm{Alt}(A, \sigma)$. By [13, (6.4)], $u^4 + au^2 = u(u^2 + a)u \in \mathrm{Alt}(A, \sigma)$. Thus,

$$b^2\alpha = (bx)^2 = (u^2 + a)^2 = u^4 + a^2 = u^4 + au^2 + a(u^2 + a) \in \mathrm{Alt}(A, \sigma).$$

However, $1 \notin \mathrm{Alt}(A, \sigma)$, because σ is orthogonal. Hence, $b = 0$, that is, $u^2 = a \in F$. This implies that $u \in \mathrm{Sym}(A, \sigma)^+$. □

Lemma 3.3. *Let (A, σ) be a central simple algebra of degree 2^n with orthogonal involution over F. Let $x \in \mathrm{Alt}(A, \sigma)^+$ with $x^2 \notin F^2$ and set $C = C_A(x)$. If $(C, \sigma|_C)$ is totally decomposable, then (A, σ) is also totally decomposable. In addition, every inseparable subalgebra of $(C, \sigma|_C)$ is an inseparable subalgebra of (A, σ). In particular, the element x is contained in some inseparable subalgebra of (A, σ).*

Proof. Set $K = F(x)$. Then $(C, \sigma|_C)$ is a totally decomposable algebra of degree 2^{n-1} with orthogonal involution over K. Let Φ be an inseparable subalgebra of $(C, \sigma|_C)$. As $\Phi \subseteq \mathrm{Sym}(C, \sigma|_C)^+$, by Lemma 3.2, $\Phi \subseteq \mathrm{Sym}(A, \sigma)^+$. Write $\Phi = K[v_1, \dots, v_{n-1}]$ for some $v_1, \dots, v_{n-1} \in C$. Since $\dim_F \Phi = 2^n = \deg_F A$ and Φ is generated, as an F-algebra, by $x, v_1, \dots, v_{n-1}$, [12, (3.11)] implies that Φ is a Frobenius subalgebra of A. Hence, $C_A(\Phi) = \Phi$ by [8, (2.2.3)]. It follows from [12, (4.6)] that (A, σ) is totally decomposable and Φ is an inseparable subalgebra of (A, σ). □

Proposition 3.4. *Let (A, σ) be a totally decomposable algebra with orthogonal involution over F. Let $x \in \mathrm{Alt}(A, \sigma)^+$ with $x^2 \notin F^2$ and set $C = C_A(x)$. Then, $(C, \sigma|_C)$ is totally decomposable if and only if x is contained in some inseparable subalgebra of A.*

https://doi.org/10.1017/S0004972717000466 Published online by Cambridge University Press

Proof. The 'if' implication can be found in [12, (6.3 (i))]. The converse follows from Lemma 3.3. □

We recall that every quaternion algebra Q over F has a *quaternion basis*, that is, a basis $(1, u, v, w)$ satisfying $u^2 + u \in F$, $v^2 \in F^\times$ and $w = uv = vu + v$ (see [9, page 25]). In this case, Q is denoted by $[\alpha, \beta)_F$, where $\alpha = u^2 + u \in F$ and $\beta = v^2 \in F^\times$.

Lemma 3.5. *If (Q, σ) is a quaternion algebra with orthogonal involution over F, then there is a quaternion basis $(1, u, v, w)$ of Q such that $u, v \in \mathrm{Sym}(Q, \sigma)$.*

Proof. Let $v \in \mathrm{Alt}(Q, \sigma)$ be a unit. Since $v \notin F$ and $v^2 \in F^\times$, it is easily seen that v extends to a quaternion basis $(1, u, v, w)$ of Q. By [13, (4.5)], $\sigma(u) = u$. □

Lemma 3.6 [13, page 7]. *Let (A, σ) be a totally decomposable algebra with orthogonal involution over F. If σ is isotropic, then $(A, \sigma) \simeq (M_2(F), t) \otimes (B, \tau)$, where t is the transpose involution and (B, τ) is a totally decomposable F-algebra with orthogonal involution.*

Lemma 3.7. *Let (A, σ) be a totally decomposable algebra of degree 8 with orthogonal involution over F. If σ is isotropic, then there are two inseparable subalgebras Φ_1 and Φ_2 of (A, σ) with $\Phi_1 \neq \Phi_2$.*

Proof. By Lemma 3.6, we may identify $(A, \sigma) = (Q_1, \sigma_1) \otimes (Q_2, \sigma_2) \otimes (M_2(F), t)$, where (Q_1, σ_1) and (Q_2, σ_2) are quaternion algebras with orthogonal involution. By Lemma 3.5, there exists a quaternion basis $(1, u_i, v_i, w_i)$ of Q_i over F such that $u_i, v_i \in \mathrm{Sym}(Q_i, \sigma_i)$, $i = 1, 2$. Let $v_3 \in \mathrm{Alt}(M_2(F), t)$ be a unit. By scaling we may assume that $v_3^2 = 1$, because $\operatorname{disc} t$ is trivial (see [9, page 82]). Then,

$$\Phi_1 = F[v_1 \otimes 1 \otimes 1, 1 \otimes v_2 \otimes 1, 1 \otimes 1 \otimes v_3]$$

is an inseparable subalgebra of (A, σ). Set

$$w = v_1 \otimes u_2 \otimes 1 + (v_1 \otimes u_2 + v_1 \otimes 1) \otimes v_3 \in \mathrm{Sym}(A, \sigma).$$

Then, $w^2 = v_1^2 \otimes 1 \otimes 1$; hence, $w^{-1} = \alpha^{-1} w$, where $\alpha = v_1^2 \in F^\times$. Set $\Phi_2 = w \cdot \Phi_1 \cdot w^{-1} \subseteq \mathrm{Sym}(A, \sigma)^+$. Then Φ_2 is an 8-dimensional subalgebra of (A, σ), which is generated, as an F-algebra, by three elements. Also, the equality $C_A(\Phi_1) = \Phi_1$ implies that $C_A(\Phi_2) = \Phi_2$. Hence, Φ_2 is an inseparable subalgebra of (A, σ). On the other hand, computations show that the element $w^{-1}(1 \otimes v_2 \otimes 1) w \in \Phi_2$ does not belong to Φ_1; hence, $\Phi_1 \neq \Phi_2$. □

Theorem 3.8. *A totally decomposable algebra with orthogonal involution (A, σ) over F has a unique inseparable subalgebra if and only if either $\deg_F A \leqslant 4$ or σ is anisotropic.*

Proof. Let Φ be an inseparable subalgebra of (A, σ). If A is a quaternion algebra, then $\Phi = \mathrm{Alt}(A, \sigma) \oplus F$ by dimension count. If $\deg_F A = 4$, then $\Phi = \mathrm{Alt}(A, \sigma)^+ \oplus F$ by [15, (4.4)]. Also, if σ is anisotropic, then Φ is uniquely determined by Theorem 3.1. This proves the 'if' implication. To prove the converse, let $\deg_F A = 2^n$.

Suppose that σ is isotropic and $\deg_F A \geqslant 8$, that is, $n \geqslant 3$. By Lemma 3.6, we may identify $(A,\sigma) = \bigotimes_{i=1}^{n-1}(Q_i,\sigma_i) \otimes (M_2(F),t)$, where every (Q_i,σ_i) is a quaternion algebra with orthogonal involution over F. By Lemma 3.7, the algebra with involution

$$(Q_{n-2},\sigma_{n-2}) \otimes (Q_{n-1},\sigma_{n-1}) \otimes (M_2(F),t),$$

has two inseparable subalgebras Φ_1 and Φ_2 with $\Phi_1 \neq \Phi_2$. Let Φ_3 be an inseparable subalgebra of $\bigotimes_{i=1}^{n-3}(Q_i,\sigma_i)$. Then, $\Phi_3 \otimes \Phi_1$ and $\Phi_3 \otimes \Phi_2$ are two inseparable subalgebras of (A,σ) with $\Phi_3 \otimes \Phi_1 \neq \Phi_3 \otimes \Phi_2$, proving the result. □

4. The isotropy index

Definition 4.1 [5]. Let $(A,\sigma) \simeq \bigotimes_{i=1}^{n}(Q_i,\sigma_i)$ be a totally decomposable algebra with orthogonal involution over F. The *Pfister invariant* of (A,σ) is defined as $\mathfrak{Pf}(A,\sigma) := \langle\langle \alpha_1,\ldots,\alpha_n\rangle\rangle$, where $\alpha_i \in F^\times$ is a representative of the class $\operatorname{disc}\sigma_i \in F^\times/F^{\times 2}$, for $i = 1,\ldots,n$.

According to [5, (7.2)], the isometry class of the Pfister invariant is independent of the decomposition of (A,σ). Moreover, every inseparable subalgebra Φ of (A,σ) may be considered as an underlying vector space of $\mathfrak{Pf}(A,\sigma)$ such that $\mathfrak{Pf}(A,\sigma)(x,x) = x^2$ for $x \in \Phi$ (see [12, (5.5)]).

Lemma 4.2. *Let (A,σ) be a totally decomposable algebra with orthogonal involution over F. If $x \in \operatorname{Sym}(A,\sigma)^+$, then $x^2 \in Q(\mathfrak{Pf}(A,\sigma))$.*

Proof. As already observed, $x \in S(A,\sigma)$ and $q_\sigma(x) = x^2$. The result therefore follows from [16, (4.3)]. □

For a positive integer n, we denote the bilinear n-fold Pfister form $\langle\langle 1,\ldots,1\rangle\rangle$ by $\langle\langle 1\rangle\rangle^n$. We also set $\langle\langle 1\rangle\rangle^0 = \langle 1\rangle$.

Let $\mathfrak{b}$ be a bilinear Pfister form over F. In view of [1, A.5], one can find a nonnegative integer r and an anisotropic bilinear Pfister form $\mathfrak{c}$ such that $\mathfrak{b} \simeq \langle\langle 1\rangle\rangle^r \otimes \mathfrak{c}$. As in [13], we denote the integer r by $\mathfrak{i}(\mathfrak{b})$. If (A,σ) is a totally decomposable F-algebra with orthogonal involution, we simply denote $\mathfrak{i}(\mathfrak{Pf}(A,\sigma))$ by $\mathfrak{i}(A,\sigma)$ and we call it the *isotropy index* of (A,σ). By [5, (5.7)], (A,σ) is anisotropic if and only if $\mathfrak{i}(A,\sigma) = 0$. If $r := \mathfrak{i}(A,\sigma) > 0$, there exists a totally decomposable algebra with anisotropic orthogonal involution (B,ρ) over F such that $(A,\sigma) \simeq (M_{2^r}(F),t) \otimes (B,\rho)$ (see [13, page 7]). In particular, if A is of degree 2^n then $\mathfrak{i}(A,\sigma) = n$ if and only if $(A,\sigma) \simeq (M_{2^n}(F),t)$. Also, if σ is isotropic and Φ is an inseparable subalgebra of (A,σ), then there exists an element $x \in \Phi$ such that $x^2 = 1$.

Proposition 4.3. *Let $\mathfrak{b}$ be a bilinear n-fold Pfister form over F. If $\alpha \in Q(\mathfrak{b}) \setminus F^2$, then $\mathfrak{i}(\mathfrak{b}_{F(\sqrt{\alpha})}) = \mathfrak{i}(\mathfrak{b}) + 1$.*

Proof. Set $K = F(\sqrt{\alpha})$ and $r = \mathfrak{i}(\mathfrak{b})$. As $Q(\langle\langle 1\rangle\rangle^n) = F^2$ and $\alpha \in Q(\mathfrak{b}) \setminus F^2$, it follows that $\mathfrak{b} \not\simeq \langle\langle 1\rangle\rangle^n$, that is, $r < n$. Write $\mathfrak{b} \simeq \langle\langle 1\rangle\rangle^r \otimes \mathfrak{c}$ for some anisotropic bilinear Pfister form $\mathfrak{c}$ over F. Since $Q(\mathfrak{b}) = Q(\mathfrak{c})$, we have $\alpha \in Q(\mathfrak{c})$. Hence, the pure subform of $\mathfrak{c}$

https://doi.org/10.1017/S0004972717000466 Published online by Cambridge University Press

represents $\alpha + \lambda^2$ for some $\lambda \in F$. By [1, A.2], there exist $\alpha_2, \ldots, \alpha_s \in F$ such that $\mathfrak{c} \simeq \langle\langle \alpha + \lambda^2, \alpha_2, \ldots, \alpha_s \rangle\rangle$. Note that $\alpha + \lambda^2 \in K^{\times 2}$; hence, $\mathfrak{c}_K \simeq \langle\langle 1, \alpha_2, \ldots, \alpha_s \rangle\rangle_K$. Since $\mathfrak{c} = \langle\langle \alpha + \lambda^2 \rangle\rangle \otimes \langle\langle \alpha_2, \ldots, \alpha_s \rangle\rangle$ is anisotropic and $K = F(\sqrt{\alpha + \lambda^2})$, by [7, (4.2)] the form $\langle\langle \alpha_2, \ldots, \alpha_s \rangle\rangle_K$ is anisotropic. It follows that $\mathfrak{i}(\mathfrak{c}_K) = 1$; hence, $\mathfrak{i}(\mathfrak{b}_K) = r + 1 = \mathfrak{i}(\mathfrak{b}) + 1$. □

Corollary 4.4. *Let (A, σ) be a totally decomposable algebra with orthogonal involution over F. If $x \in \mathrm{Sym}(A, \sigma)^+$ with $\alpha = x^2 \notin F^2$, then $\mathfrak{i}((A, \sigma)_{F(\sqrt{\alpha})}) = \mathfrak{i}(A, \sigma) + 1$. In particular, $(A, \sigma) \not\simeq (M_{2^n}(F), t)$.*

Proof. By Lemma 4.2, $\alpha \in Q(\mathfrak{Pf}(A, \sigma))$. The result follows from Proposition 4.3. □

Lemma 4.5. *Let (A, σ) be a totally decomposable algebra of degree 2^n with orthogonal involution over F and let $x \in \mathrm{Sym}(A, \sigma)^+$ be a unit. If Φ is an inseparable subalgebra of (A, σ), then for every unit $y \in \Phi$, there exists a positive integer k such that $(xy)^k \in \mathrm{Sym}(A, \sigma)^+$. In addition, for such an integer k, we have $(xy)^k x = x(xy)^k$.*

Proof. Since x and y are units, the element $(xy)^r$ is a unit for every integer r. For $r \geqslant 0$, let $\Phi_r = (xy)^r \cdot \Phi \cdot (xy)^{-r}$. Then Φ_r is a 2^n-dimensional commutative subalgebra of A, which is generated by n elements and satisfies $u^2 \in F$ for every $u \in \Phi_r$. Set $\alpha = x^2 \in F^\times$ and $\beta = y^2 \in F^\times$. Then,

$$(xy)^{-r} = (y^{-1}x^{-1})^r = (\beta^{-1} y \alpha^{-1} x)^r = \alpha^{-r}\beta^{-r}(yx)^r.$$

Hence, $\Phi_r = \alpha^{-r}\beta^{-r}(xy)^r \cdot \Phi \cdot (yx)^r \subseteq \mathrm{Sym}(A, \sigma)$, that is, Φ_r is an inseparable subalgebra of (A, σ). However, there exists a finite number of inseparable subalgebras of (A, σ), so $\Phi_r = \Phi_s$ for some nonnegative integers r, s with $r > s$. It follows that $\Phi_{r-s} = \Phi_0 = \Phi$. In particular, $(xy)^{r-s} y (xy)^{s-r} \in \Phi$ and

$$(xy)^{r-s} y (xy)^{s-r} y = y (xy)^{r-s} y (xy)^{s-r}. \tag{4.1}$$

Set $\lambda = \alpha^{s-r}\beta^{s-r}$, so that $(xy)^{s-r} = \lambda (yx)^{r-s}$. Substituting in (4.1),

$$\lambda (xy)^{r-s} y (yx)^{r-s} y = \lambda y (xy)^{r-s} y (yx)^{r-s}.$$

It follows that $\lambda y^2 (xy)^{2(r-s)} = \lambda y^2 (yx)^{2(r-s)}$, because $y^2 \in F^\times$. Hence, $(xy)^k = (yx)^k$, where $k = 2(r - s)$. Also, $\sigma((xy)^k) = (yx)^k = (xy)^k$ and $((xy)^k)^2 = (xy)^k (yx)^k \in F^\times$; hence, $(xy)^k \in \mathrm{Sym}(A, \sigma)^+$. Finally, $(xy)^k x = x(yx)^k = x(xy)^k$, completing the proof. □

Proposition 4.6. *Let (A, σ) be a totally decomposable algebra with orthogonal involution over F and let $x \in \mathrm{Sym}(A, \sigma)^+$ with $x^2 \notin F^2$. Then, σ is isotropic if and only if $\sigma|_{C_A(x)}$ is isotropic.*

Proof. Since $x^2 \notin F^2$, $C_A(x)$ is a central simple algebra over $F(x) = F(\sqrt{\alpha})$, where $\alpha = x^2 \in F^\times$. If $\sigma|_{C_A(x)}$ is isotropic, then σ is clearly isotropic. To prove the converse, let Φ be an inseparable subalgebra of (A, σ). Since σ is isotopic, there exists $y \in \Phi \setminus F$ with $y^2 = 1$. By Lemma 4.5, there is a positive integer k such that $(xy)^k \in \mathrm{Sym}(A, \sigma)^+$. Let r be the minimum positive integer with $(xy)^r \in \mathrm{Sym}(A, \sigma)^+$; hence, $(xy)^r = (yx)^r$.

We claim that $(xy)^r \neq x^r$. Suppose that $(xy)^r = x^r$. If r is odd, write $r = 2s + 1$ for some nonnegative integer s. The equality $(xy)^r = x^r$ then implies that $(yx)^s y(xy)^s = x^{2s} = \alpha^s$. As $(xy)^s = \alpha^s (yx)^{-s}$, we get $\alpha^s (yx)^s y(yx)^{-s} = \alpha^s$. Hence, $y = 1 \in F$, which contradicts the assumption. If r is even, write $r = 2s$ for some positive integer s, so that $(xy)^r = x^r = \alpha^s$. Multiplying by $(xy)^{-s}$,

$$(xy)^s = \alpha^s (xy)^{-s} = \alpha^s \alpha^{-s} (yx)^s = (yx)^s.$$

It follows that $(xy)^s \in \mathrm{Sym}(A, \sigma)^+$, contradicting the minimality of r. This proves the claim. According to Lemma 4.5, $(xy)^r \in C_A(x)$. Set $z = (xy)^r + x^r \in C_A(x)$. Then $z \neq 0$ and $\sigma(z)z = \alpha^r + \alpha^r = 0$, that is, $\sigma|_{C_A(x)}$ is isotropic. □

Theorem 4.7. *Let (A, σ) be a totally decomposable algebra with orthogonal involution over F. Let $x \in \mathrm{Alt}(A, \sigma)^+$ with $x^2 \notin F^2$ and let $C = C_A(x)$. If $(C, \sigma|_C)$ is totally decomposable, then $\mathfrak{i}(C, \sigma|_C) = \mathfrak{i}(A, \sigma)$.*

Proof. If $\sigma|_C$ is anisotropic, then σ is also anisotropic by Proposition 4.6; hence, $\mathfrak{i}(C, \sigma|_C) = \mathfrak{i}(A, \sigma) = 0$. Suppose that $\sigma|_C$ is isotropic. Set $r = \mathfrak{i}(C, \sigma|_C) > 0$ and $K = F(x)$. Write $(C, \sigma|_C) \simeq (M_{2^r}(K), t) \otimes (B, \tau)$ for some totally decomposable algebra with anisotropic orthogonal involution (B, τ) over K. Note that the algebra B is nontrivial by Corollary 4.4. Since $(M_{2^r}(K), t) \simeq (M_{2^r}(F), t)_K$, we may identify $M_{2^r}(F)$ with a subalgebra of A. Let $D = C_A(M_{2^r}(F))$. Then $x \in D$,

$$(A, \sigma) \simeq (M_{2^r}(F), t) \otimes (D, \sigma|_D), \tag{4.2}$$

and one has a monomorphism of F-algebras with involution $(B, \tau) \hookrightarrow (D, \sigma|_D)$. Considering this map as an inclusion, we see that $B = C_D(x)$. By [11, (3.5)], $x \in \mathrm{Alt}(D, \sigma|_D)$. It follows that $x \in \mathrm{Alt}(D, \sigma|_D)^+$, because $x^2 \in F$. Since (B, τ) is totally decomposable, the pair $(D, \sigma|_D)$ is also totally decomposable by Lemma 3.3. Also, Proposition 4.6 implies that $\sigma|_D$ is anisotropic, because τ is anisotropic. Hence, using (4.2) we obtain $\mathfrak{i}(A, \sigma) = r$, proving the result. □

5. Stable quaternion subalgebras

In this section we study some conditions under which a symmetric square-central element of a totally decomposable algebra with orthogonal involution is contained in a stable quaternion subalgebra. We start with anisotropic involutions.

Theorem 5.1. *Let (A, σ) be a totally decomposable algebra with anisotropic orthogonal involution over F. Then every $x \in \mathrm{Sym}(A, \sigma)^+$ is contained in a σ-invariant quaternion subalgebra of A.*

Proof. Since σ is anisotropic, Theorem 3.1 shows that x is contained in the unique inseparable subalgebra of (A, σ). If $x^2 = \lambda^2$ for some $\lambda \in F$, then $(x + \lambda)^2 = 0$. Hence, $x = \lambda$ by [5, (6.1)] and the result is trivial. Otherwise, $x^2 \notin F^2$ and the conclusion follows from [12, (6.3 (ii))]. □

https://doi.org/10.1017/S0004972717000466 Published online by Cambridge University Press

We next consider algebras of degree 4 and 8.

Proposition 5.2. *Let (A, σ) be a totally decomposable algebra of degree 4 with orthogonal involution over F. If $x \in \mathrm{Sym}(A, \sigma)^+$ with $x^2 \notin F^2$, then x is contained in a σ-invariant quaternion subalgebra of A.*

Proof. By Corollary 4.4, either $\mathfrak{i}(A, \sigma) = 0$ or $\mathfrak{i}(A, \sigma) = 1$. In the first case, the result follows from Theorem 5.1. Suppose $\mathfrak{i}(A, \sigma) = 1$. Set $C = C_A(x)$ and $K = F(x)$. By Proposition 4.6, $(C, \sigma|_C)$ is isotropic. However, $(C, \sigma|_C)$ is a quaternion K-algebra and the isotropy of $\sigma|_C$ implies $\mathfrak{i}(C, \sigma|_C) = 1$, that is, $(C, \sigma|_C) \simeq (M_2(K), t) \simeq (M_2(F), t)_K$. Hence, the algebra $M_2(F)$ may be identified with a subalgebra of $C \subseteq A$. The algebra $Q = C_A(M_2(F))$ is then a σ-invariant quaternion subalgebra of A containing x. □

The next result follows from [7, (4.2)] and the Witt decomposition theorem [6, (1.27)]. Recall that a symmetric bilinear space $(V, \mathfrak{b})$ over F is called *metabolic* if there exists a subspace W of V with $\dim_F W = \frac{1}{2} \dim_F V$ such that $\mathfrak{b}|_{W \times W} = 0$.

Lemma 5.3. *Let $\mathfrak{b}$ be an anisotropic symmetric bilinear form over F and $\alpha \in F^\times \setminus F^{\times 2}$. Then $\mathfrak{b} \otimes \langle\langle \alpha \rangle\rangle$ is metabolic if and only if $\mathfrak{b}_{F(\sqrt{\alpha})}$ is metabolic.*

Recall that two bilinear forms $\mathfrak{b}$ and $\mathfrak{c}$ are called *similar* if $\mathfrak{b} \simeq \lambda \cdot \mathfrak{c}$ for some $\lambda \in F^\times$.

Lemma 5.4. *Let $\mathfrak{b}$ be a 4-dimensional symmetric nonalternating bilinear form over F and let $K = F(\sqrt{\alpha})$ for some $\alpha \in F^\times \setminus F^{\times 2}$. If $\mathfrak{b} \otimes \langle\langle \alpha \rangle\rangle$ is metabolic, then $\mathfrak{b}_K$ is similar to a Pfister form.*

Proof. By the Witt decomposition theorem, one can write $\mathfrak{b} \simeq \mathfrak{b}_1 \perp \mathfrak{b}_2$, where $\mathfrak{b}_1$ is anisotropic and $\mathfrak{b}_2$ is metabolic. The hypothesis implies that the form $\mathfrak{b}_1 \otimes \langle\langle \alpha \rangle\rangle$ is metabolic. By Lemma 5.3, the form $(\mathfrak{b}_1)_K$ (and therefore $\mathfrak{b}_K$) is also metabolic. Since $\mathfrak{b}_K$ is not alternating, by [6, (1.24) and (1.22(3))] either $\mathfrak{b}_K \simeq \langle a, a, b, b \rangle$ or $\mathfrak{b}_K \simeq \langle a, a \rangle \perp \mathbb{H}$, where $a, b \in K^\times$ and $\mathbb{H}$ is the hyperbolic plane. In the first case, $\mathfrak{b}_K$ is similar to $\langle 1, 1, ab, ab \rangle = \langle\langle 1, ab \rangle\rangle$. In the second case, using the isometry $\langle a, a, a \rangle \simeq \langle a \rangle \perp \mathbb{H}$ in [6, (1.16)], we get $\mathfrak{b}_K \simeq \langle a, a, a, a \rangle$. Hence, $\mathfrak{b}_K$ is similar to $\langle\langle 1, 1 \rangle\rangle$. □

Lemma 5.5. *Let (A, σ) be a central simple algebra of degree 4 with orthogonal involution over F and let K/F be a separable quadratic extension. If $(A, \sigma)_K$ is totally decomposable, then (A, σ) is also totally decomposable.*

Proof. By [10, (7.3)], a 4-dimensional orthogonal involution is totally decomposable if and only if its discriminant is trivial. The result therefore follows from the equality $K^{\times 2} \cap F^\times = F^{\times 2}$. □

Lemma 5.6 [14, (5.4)]. *Let (Q, σ) be a quaternion algebra with orthogonal involution over F. If $x \in \mathrm{Sym}(Q, \sigma)^+ \setminus F$ then there exists $\lambda \in F$ such that $x + \lambda \in \mathrm{Alt}(Q, \sigma)^+$.*

Proposition 5.7. *Let (A, σ) be a totally decomposable algebra of degree 8 over F. For an element $x \in \mathrm{Sym}(A, \sigma)^+$ with $x^2 \notin F^2$, the following conditions are equivalent:*

(1) *There exists a σ-invariant quaternion subalgebra of A containing x.*
(2) *There exists an inseparable subalgebra Φ of (A,σ) such that $x \in \Phi$.*

Proof. If $\mathrm{i}(A,\sigma) = 0$, by Theorems 5.1 and 3.1 both conditions are satisfied. Let $\mathrm{i}(A,\sigma) > 0$. Then $(A,\sigma) \simeq (M_2(F),t) \otimes (Q_1,\sigma_1) \otimes (Q_2,\sigma_2)$, where (Q_i,σ_i), $i = 1,2$, is a quaternion algebra with orthogonal involution over F. Suppose first that x is contained in a σ-invariant quaternion subalgebra Q_3 of A. By Lemma 5.6, replacing x with $x+\lambda$ for some $\lambda \in F$, we may assume that $x \in \mathrm{Alt}(A,\sigma)^+$ (note that this replacement does not change the hypothesis $x^2 \notin F^2$ and the conditions (1) and (2)). Set $B = C_A(Q_3)$, $\sigma_3 = \sigma|_{Q_3}$ and $\rho = \sigma|_B$, so that $(A,\sigma) \simeq (Q_3,\sigma_3) \otimes (B,\rho)$. Then

$$(Q_3,\sigma_3) \otimes (B,\rho) \simeq (M_2(F),t) \otimes (Q_1,\sigma_1) \otimes (Q_2,\sigma_2). \tag{5.1}$$

Let $C = C_A(x)$ and $K = F(x) = F(\sqrt{\alpha})$, where $\alpha = x^2 \in F^\times \setminus F^{\times 2}$. Then $(C,\sigma|_C) \simeq (B,\rho)_K$ as K-algebras. We claim that $(B,\rho)_K$ is totally decomposable. The result then follows from Proposition 3.4.

By Lemma 3.5, for $i = 1,2,3$, there exists a quaternion basis $(1,u_i,v_i,w_i)$ of Q_i such that $u_i \in \mathrm{Sym}(Q_i,\sigma_i)$. Let $\beta_i = u_i^2 + u_i \in F$. For $i = 0,1,2,3$, define a field L_i inductively as follows: set $L_0 = F$. For $i \geqslant 1$ set $L_i = L_{i-1}(u_i)$ if $\beta_i \notin \wp(L_{i-1}) := \{y^2 + y \mid y \in L_{i-1}\}$ and $L_i = L_{i-1}$ otherwise. In other words, either $L_i = L_{i-1}$ or L_i/L_{i-1} is a separable quadratic extension. Note that $L_i^{\times 2} \cap F^\times = F^{\times 2}$; hence, either $L_i(\sqrt{\alpha}) = L_{i-1}(\sqrt{\alpha})$ or $L_i(\sqrt{\alpha})/L_{i-1}(\sqrt{\alpha})$ is a separable quadratic extension. We show that $\rho_{L_3(\sqrt{\alpha})}$ is totally decomposable, which implies that $\rho_{L_i(\sqrt{\alpha})}$ is totally decomposable for $i = 0,1,2$ thanks to Lemma 5.5. In particular, $\rho_K = \rho_{F(\sqrt{\alpha})}$ is also totally decomposable, as required.

Set $L = L_3$. Then for $i = 1,2,3$, the algebra Q_{iL} splits. Hence, $(Q_i,\sigma_i)_L \simeq (M_2(L),\tau_i)$, where τ_i is an orthogonal involution on $M_2(L)$. By (5.1),

$$(M_2(L),\tau_3) \otimes (B,\rho)_L \simeq (M_2(L),t) \otimes (M_2(L),\tau_1) \otimes (M_2(L),\tau_2). \tag{5.2}$$

In particular, B_L splits and we may identify $(B,\rho)_L = \mathrm{Ad}(\mathfrak{b})$ for some symmetric bilinear form $\mathfrak{b}$ over L. Since $x \in \mathrm{Alt}(Q_3,\sigma_3)^+$, we have $\operatorname{disc}\sigma_3 = \alpha F^{\times 2}$ and so

$$(M_2(L),\tau_3) \simeq (Q_3,\sigma_3)_L \simeq \mathrm{Ad}(\langle\langle \alpha \rangle\rangle_L), \tag{5.3}$$

by [9, (7.4)]. The right side of (5.2) is the adjoint involution of a metabolic bilinear form over L. Hence, it follows from (5.3) that $\mathfrak{b} \otimes \langle\langle \alpha \rangle\rangle$ is also metabolic. By Lemma 5.4, $\mathfrak{b}_{L(\sqrt{\alpha})}$ is similar to a Pfister form. Hence, $\rho_{L(\sqrt{\alpha})}$ is totally decomposable. This proves that (1) implies (2). The converse follows from [12, (6.3 (ii))]. □

Lemma 5.8 [9, pages 13–14]. *If $\mathfrak{b}$ is an n-dimensional symmetric bilinear form over F, then $\mathrm{Ad}(\mathfrak{b}) \simeq (M_n(F),t)$ if and only if $\mathfrak{b}$ is similar to $n \times \langle 1 \rangle$.*

Lemma 5.9. *Let (A,σ) be a central simple algebra of degree n with orthogonal involution over F. If $(A,\sigma) \otimes (M_m(F),\tau) \simeq (M_{mn}(F),t)$, where m is a nonnegative integer and τ is an orthogonal involution, then $(A,\sigma) \simeq (M_n(F),t)$.*

https://doi.org/10.1017/S0004972717000466 Published online by Cambridge University Press

PROOF. Observe first that A splits; hence, we may identify $(A, \sigma) = \mathrm{Ad}(\mathfrak{b}_1)$ and $(M_m(F), \tau) = \mathrm{Ad}(\mathfrak{b}_2)$ for some symmetric nonalternating bilinear forms $\mathfrak{b}_1$ and $\mathfrak{b}_2$ over F. By Lemma 5.9, $\mathrm{Ad}(\mathfrak{b}_1 \otimes \mathfrak{b}_2) \simeq \mathrm{Ad}(mn \times \langle 1 \rangle)$. Hence, the forms $\mathfrak{b}_1 \otimes \mathfrak{b}_2$ and $mn \times \langle 1 \rangle$ are similar by [9, (4.2)]. As $Q(mn \times \langle 1 \rangle) = F^2$, we obtain $Q(\mathfrak{b}_1) \subseteq \lambda \cdot F^2$ for some $\lambda \in F^\times$. Since $\mathfrak{b}_1$ is nonalternating, it is diagonalisable by [6, (1.17)] and is therefore similar to $n \times \langle 1 \rangle$. By Lemma 5.8, $(A, \sigma) \simeq (M_n(F), t)$. □

THEOREM 5.10. *Let (A, σ) be a totally decomposable algebra of degree 2^n with orthogonal involution over F and let $x \in \mathrm{Sym}(A, \sigma)^+$ with $x^2 \notin F^2$. If $\mathfrak{i}(A, \sigma) = n - 1$, then the following statements are equivalent:*

(1) *There exists a σ-invariant quaternion subalgebra Q of A containing x.*

(2) *There exists an inseparable subalgebra Φ of (A, σ) such that $x \in \Phi$.*

PROOF. The implication (2) ⇒ (1) follows from [12, (6.3 (ii))]. For the converse, observe that by Lemma 5.6, replacing x with $x + \lambda$ for some $\lambda \in F$, we may assume that $x \in \mathrm{Alt}(A, \sigma)^+$. Let $C = C_A(x)$. In view of Proposition 3.4, it suffices to show that $(C, \sigma|_C)$ is totally decomposable. Let $\tau = \sigma|_Q$, $B = C_A(Q)$ and $\rho = \sigma|_B$. Then, $(A, \sigma) \simeq (B, \rho) \otimes (Q, \tau)$. Set $K = F(x)$, so that $(C, \sigma|_C) \simeq_K (B, \rho)_K$. Hence, it is enough to show that $(B, \rho)_K$ is totally decomposable. By Corollary 4.4, $\mathfrak{i}(A, \sigma)_K = n$, so $(A, \sigma)_K \simeq (M_{2^n}(K), t)$. It follows that $(B, \rho)_K \otimes_K (Q, \tau)_K \simeq (M_{2^n}(K), t)$. Since $x \in Q$ and $x^2 \in K^2$, the algebra Q_K splits. Hence, by Lemma 5.9, $(B, \rho)_K \simeq_K (M_{2^{n-1}}(K), t)$. In particular, $(B, \rho)_K$ is totally decomposable, proving the result. □

6. Examples for isotropic involutions

In this section we show that the criteria obtained in Section 5 do not necessarily apply to arbitrary involutions.

LEMMA 6.1. *Let (A, σ) be a totally decomposable algebra of degree 2^n with orthogonal involution over F. If $n \geqslant 2$ and $(A, \sigma) \not\simeq (M_{2^n}(F), t)$, then there exist an element $w \in \mathrm{Sym}(A, \sigma) \setminus (\mathrm{Alt}(A, \sigma) \oplus F)$ and a unit $u \in \mathrm{Alt}(A, \sigma)$ such that $u^2 \in F^\times \setminus F^{\times 2}$ and $uw = wu$.*

PROOF. Let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a decomposition of (A, σ). Since $(A, \sigma) \not\simeq (M_{2^n}(F), t)$, (by re-indexing) we may assume that $(Q_1, \sigma_1) \not\simeq (M_2(F), t)$. Let $u \in \mathrm{Alt}(Q_1, \sigma_1)$ be a unit, so that $u^2 \in F^\times$. If $u^2 \in F^{\times 2}$ then Q_1 splits and $\operatorname{disc} \sigma_1$ is trivial. As $\operatorname{disc} t$ is also trivial (see [9, page 82]), $(Q_1, \sigma_1) \simeq (M_2(F), t)$ by [9, (7.4)], contradicting the assumption. Hence, $u^2 \in F^\times \setminus F^{\times 2}$. By [9, (2.6)], $\dim_F \mathrm{Sym}(Q_2, \sigma_2) = 3$ and $\dim_F \mathrm{Alt}(Q_2, \sigma_2) = 1$. Hence, there exists an element $w \in \mathrm{Sym}(Q_2, \sigma_2) \setminus (\mathrm{Alt}(Q_2, \sigma_2) \oplus F)$. The elements u and w may be identified with elements of A, so that $uw = wu$, $w \in \mathrm{Sym}(A, \sigma)$ and $u \in \mathrm{Alt}(A, \sigma)$. Observe that $\alpha + w \notin \mathrm{Alt}(Q_2, \sigma_2)$ for every $\alpha \in F$. By [11, (3.5)], it follows that $\alpha + w \notin \mathrm{Alt}(A, \sigma)$ for all $\alpha \in F$, that is, $w \in \mathrm{Sym}(A, \sigma) \setminus (\mathrm{Alt}(A, \sigma) \oplus F)$. □

Remark 6.2. Let (B,ρ) be a central simple algebra with involution over F and set $(A,\sigma) = (B,\rho) \otimes (M_2(F),t)$. Then every element $x \in A$ can be written as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where $a,b,c,d \in B$. The involution σ maps x to $\left(\begin{smallmatrix} \rho(a) & \rho(c) \\ \rho(b) & \rho(d) \end{smallmatrix}\right)$. It follows that

$$\mathrm{Alt}(A,\sigma) = \left\{ \begin{pmatrix} a & b \\ \rho(b) & c \end{pmatrix} \,\middle|\, a,c \in \mathrm{Alt}(B,\rho) \text{ and } b \in B \right\},$$

$$\mathrm{Sym}(A,\sigma) = \left\{ \begin{pmatrix} a & b \\ \rho(b) & c \end{pmatrix} \,\middle|\, a,c \in \mathrm{Sym}(B,\rho) \text{ and } b \in B \right\}.$$

The next result shows that Theorem 5.1 does not hold for isotropic involutions of degree $\geqslant 8$ (see also Proposition 5.2).

Proposition 6.3. *Let (A,σ) be a totally decomposable algebra of degree 2^n with isotropic orthogonal involution over F. If $n \geqslant 3$ and $(A,\sigma) \not\simeq (M_{2^n}(F),t)$, then there exists an element $x \in \mathrm{Sym}(A,\sigma)^+$ with $x^2 \notin F^2$ which is not contained in any σ-invariant quaternion subalgebra of A.*

Proof. Since $\mathfrak{i}(A,\sigma) > 0$, we may identify $(A,\sigma) = (B,\rho) \otimes (M_2(F),t)$, where (B,ρ) is a totally decomposable algebra with orthogonal involution over F. The assumptions $n \geqslant 3$ and $(A,\sigma) \not\simeq (M_{2^n}(F),t)$ imply $\deg_F B \geqslant 4$ and $(B,\rho) \not\simeq (M_{2^{n-1}}(F),t)$. By Lemma 6.1, there exists an element $w \in \mathrm{Sym}(B,\rho) \setminus (\mathrm{Alt}(B,\rho) \oplus F)$ and a unit $u \in \mathrm{Alt}(B,\rho)$ for which $u^2 \in F^\times \setminus F^{\times 2}$ and $uw = wu$. Set

$$x = \begin{pmatrix} w & w+u \\ w+u & w \end{pmatrix} \in A.$$

By Remark 6.2, $x \in \mathrm{Sym}(A,\sigma) \setminus (\mathrm{Alt}(A,\sigma) \oplus F)$. Since $u^2 \in F^\times \setminus F^{\times 2}$, we have $x^2 \in F^\times \setminus F^{\times 2}$; hence, $x \in \mathrm{Sym}(A,\sigma)^+$. By Lemma 5.6, x is not contained in any σ-invariant quaternion subalgebra of A, because $x + \alpha \notin \mathrm{Alt}(A,\sigma)$ for every $\alpha \in F$. □

We conclude by showing that the implication (1) ⇒ (2) in Theorem 5.10 and Proposition 5.7 does not hold for arbitrary involutions. We use the ideas of [5, (9.4)]. Recall that the *canonical* involution γ on a quaternion F-algebra Q is defined as $\gamma(x) = \mathrm{Trd}_Q(x) - x$ for $x \in Q$, where $\mathrm{Trd}_Q(x)$ is the reduced trace of x in Q. For a division algebra with involution (D,θ) over F and $\alpha_1,\ldots,\alpha_n \in D^\times \cap \mathrm{Sym}(D,\theta)$, the diagonal hermitian form h on D^n defined by $h(x,y) = \sum_{i=1}^n \theta(x_i)\alpha_i y_i$ is denoted by $\langle \alpha_1,\ldots,\alpha_n\rangle_\theta$.

Example 6.4. Let $F \neq F^2$ and let $K = F(X,Y,Z)$, where X, Y and Z are indeterminates. Let $Q = [X,Y)_K$ and let γ be the canonical involution on Q. By [5, (9.3)], Q is a division algebra over K. Choose an element $s \in \mathrm{Sym}(Q,\gamma)$ with $s^2 = Y$. Let ψ be the diagonal hermitian form $\langle 1,Z,s,s\rangle_\gamma$ over (Q,γ) and set $(B,\rho) = \mathrm{Ad}(\psi)$. By [5, (9.4)], (B,ρ) is not totally decomposable, but $(B,\rho)_L$ is totally decomposable for every splitting field L of A.

Now, choose $\alpha \in F^\times \setminus F^{\times 2}$ and let $Q' = [X,\alpha)_K$ with a quaternion basis $(1,u,v,w)$. Let τ be the involution on Q' induced by $\tau(u) = u$ and $\tau(v) = v$. Then, τ is an orthogonal involution and $v = \tau(uv) - uv \in \mathrm{Alt}(Q', \tau)$. Set $(A, \sigma) = (B, \rho) \otimes_K (Q', \tau)$. Then, (A, σ) is a central simple algebra with orthogonal involution over K. We claim that (A, σ) is totally decomposable. Let $L = K(u) \subseteq Q'$ and set $C = C_A(1 \otimes u)$. Then, L/K is a separable quadratic extension and

$$(C, \sigma|_C) \simeq_L (B, \rho)_L \tag{6.1}$$

is a central simple L-algebra with orthogonal involution. Since $u^2 + u = X$, it follows that $Q_L \simeq [X, Y)_L$ splits, which implies that B_L is also split. Thus $(B, \rho)_L$ is totally decomposable, that is, $(C, \sigma|_C)$ is totally decomposable by (6.1). Using [13, (7.3)] and the isomorphism (6.1), one can find a totally decomposable algebra with orthogonal involution (C', σ') over K such that $(C, \sigma|_C) \simeq (C', \sigma')_L$. As $C \subseteq A$, the algebra C' may be identified with a subalgebra of A. Let $Q'' = C_A(C')$. Then, Q'' is a quaternion K-subalgebra of A and $(A, \sigma) \simeq_K (C', \sigma') \otimes_K (Q'', \sigma|_{Q''})$ is totally decomposable, proving the claim.

The element $1 \otimes v \in \mathrm{Alt}(A, \sigma)^+$ is contained in the copy of Q' in A, which is a σ-invariant quaternion subalgebra of A. Note that $(C_A(1 \otimes v), \sigma|_{C_A(1\otimes v)}) \simeq (B, \rho)_{K(v)}$ as $K(v)$-algebras. We show that $(B, \rho)_{K(v)}$ is not totally decomposable, which implies that $1 \otimes v$ is not contained in any inseparable subalgebra of (A, σ), by [12, (6.3(i))]. Since $v^2 = \alpha \in F^\times \setminus F^{\times 2}$, we have $K(v) \simeq F(\sqrt{\alpha})(X, Y, Z)$. Hence, $Q_{K(v)}$ is still a division algebra by [5, (9.3)]. By [5, (9.4)], $(B, \rho)_{K(v)}$ is not totally decomposable.

References

[1] J. Arason and R. Baeza, 'Relations in I^n and $I^n W_q$ in characteristic 2', *J. Algebra* **314**(2) (2007), 895–911.

[2] D. Barry, 'Decomposable and indecomposable algebras of degree 8 and exponent 2 (with an appendix by A. S. Merkurjev)', *Math. Z.* **276**(3–4) (2014), 1113–1132.

[3] D. Barry, 'Power-central elements in tensor products of symbol algebras', *Comm. Algebra* **44**(9) (2016), 3767–3787.

[4] D. Barry and A. Chapman, 'Square-central and Artin–Schreier elements in division algebras', *Arch. Math. (Basel)* **104**(6) (2015), 513–521.

[5] A. Dolphin, 'Orthogonal Pfister involutions in characteristic two', *J. Pure Appl. Algebra* **218**(10) (2014), 1900–1915.

[6] R. Elman, N. Karpenko and A. Merkurjev, *The Algebraic and Geometric Theory of Quadratic Forms*, American Mathematical Society Colloquium Publications, 56 (American Mathematical Society, Providence, RI, 2008).

[7] D. Hoffmann, 'Witt kernels of bilinear forms for algebraic extensions in characteristic 2', *Proc. Amer. Math. Soc.* **134**(3) (2006), 645–652.

[8] N. Jacobson, *Finite-dimensional Division Algebras Over Fields* (Springer, Berlin, 1996).

[9] 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, 1998).

[10] M.-A. Knus, R. Parimala and R. Sridharan, 'Involutions on rank 16 central simple algebras', *J. Indian Math. Soc. (N.S.)* **57**(1–4) (1991), 143–151.

[11] M. G. Mahmoudi and A.-H. Nokhodkar, 'On split products of quaternion algebras with involution in characteristic two', *J. Pure Appl. Algebra* **218**(4) (2014), 731–734.

[12] M. G. Mahmoudi and A.-H. Nokhodkar, 'On totally decomposable algebras with involution in characteristic two', *J. Algebra* **451** (2016), 208–231.

[13] A.-H. Nokhodkar, 'Quadratic descent of totally decomposable orthogonal involutions in characteristic two', *J. Pure Appl. Algebra* **221**(4) (2017), 948–959.

[14] A.-H. Nokhodkar, 'On the decomposition of metabolic involutions', *J. Algebra Appl.*, doi:10.1142/S0219498817501298.

[15] A.-H. Nokhodkar, 'On decomposable biquaternion algebras with involution of orthogonal type', 2016, arXiv:1508.02018.

[16] A.-H. Nokhodkar, 'Orthogonal involutions and totally singular quadratic forms in characteristic two', *Manuscripta Math.* (2017), doi:10.1007/s00229-017-0922-y.

[17] A. Quéguiner-Mathieu and J.-P. Tignol, 'Discriminant and Clifford algebras', *Math. Z.* **240**(2) (2002), 345–384.

[18] L. H. Rowen, 'Central simple algebras', *Israel J. Math.* **29** (1978), 285–301.

A.-H. NOKHODKAR, Department of Pure Mathematics,
Faculty of Science, University of Kashan, PO Box 87317-51167,
Kashan, Iran
e-mail: a.nokhodkar@kashanu.ac.ir

https://doi.org/10.1017/S0004972717000466 Published online by Cambridge University Press