INVOLUTIONS AND STABLE SUBALGEBRAS

KARIM JOHANNES BECHER, NICOLAS GRENIER-BOLEY,
AND JEAN-PIERRE TIGNOL

Abstract. Given a central simple algebra with involution over an arbitrary field, étale subalgebras contained in the space of symmetric elements are investigated. The method emphasizes the similarities between the various types of involutions and privileges a unified treatment for all characteristics whenever possible. As a consequence a conceptual proof of a theorem of Rowen is obtained, which asserts that every division algebra of exponent two and degree eight contains a maximal subfield that is a triquadratic extension of the centre.

Keywords: Central simple algebra, involution, Double Centraliser Theorem, étale subalgebra, capacity, Jordan algebra, crossed products, characteristic two,

Classification (MSC 2010): 16H05, 16R50, 16W10

1. Introduction

We investigate étale algebras in the space of symmetric elements of a central simple algebra with involution over an arbitrary field, emphasizing the similarities between the various types of involutions and avoiding restrictions on the characteristic. In Section 2 and Section 3 we recall the terminology and some crucial techniques for algebras with involution. We enhance this terminology in a way that allows us to avoid unnecessary case distinctions in the sequel, according to the different types of involution and to the characteristic. To this end the notion of *capacity* of an algebra with involution is defined in Section 3 to be the degree of the algebra if the involution is orthogonal or unitary, and half the degree if the involution is symplectic. In Section 5 we isolate a notion of *neat* subalgebra, which captures the features of separable field extensions of the centre consisting of symmetric elements while avoiding the pathologies that may arise with arbitrary étale algebras. We prove their existence and determine their maximal dimension to be equal to the capacity (Theorem 4.1 and Proposition 5.3). In Section 6, given a neat quadratic algebra K, we establish the existence of a neat algebra L linearly disjoint from K and centralising K, such that the composite KL is a neat algebra of maximal dimension (Theorem 6.10). This result is applied in Section 7 to construct neat biquadratic algebras in the space of symmetric elements of central simple algebras of degree 4 with orthogonal or unitary involutions, and of central simple algebras of degree 8 with symplectic involutions (Theorem 7.4). As

Date: 20 October, 2016.

a consequence, we obtain a conceptual proof of a theorem of Rowen, which asserts that division algebras of exponent 2 and degree 8 are elementary abelian crossed products, i.e., they contain a maximal subfield which is a triquadratic separable extension of the centre (Corollary 7.7). We obtain this result through a refined version, which says that any symplectic involution on a central simple algebra of degree 8 stabilizes some triquadratic étale extension of the centre (Theorem 7.6). This was proven in [7, Lemma 6.1] for division algebras in characteristic different from two, but there the proof uses Rowen's Theorem, which we obtain here as a consequence. This illustrates the usefulness of involutions in the investigation of central simple algebras of exponent two.

The results of this paper will be used in [4], which proposes a common approach to the definition of the first cohomological invariant (discriminant) of the involutions of capacity four of various types through Pfister forms in arbitrary characteristic.

2. Algebras

In this preliminary section we introduce and recall some definitions and facts from the theory of finite-dimensional simple and semisimple algebras. As a general reference we refer to [11] and [8].

Let F be an arbitrary field. For a commutative F-algebra K we set $[K : F] = \dim_F K$. Recall that an F-algebra is *étale* if it is isomorphic to a finite product of finite separable field extensions. An étale F-algebra is said to be *split* if it is F-isomorphic to F^n for some $n \in \mathbb{N}$.

2.1. **Lemma.** *Let L be a split étale F-algebra with $|F| > [L : F]$. Then $L = F[a]$ for an element $a \in L^\times$ separable over F.*

Proof. In F^n any element $a = (a_1, \dots, a_n)$ with distinct $a_1, \dots, a_n \in F^\times$ is invertible and has minimal polynomial $\prod_{i=1}^n (X - a_i)$ over F, which is separable of degree n, whereby $L = F[a]$. □

Let A be an F-algebra. We denote by $Z(A)$ the centre of A and by A^{op} the opposite algebra of A.

2.2. **Lemma.** *Let $K = Z(A)$ and assume that K is an étale F-algebra. Let L be a commutative semisimple F-subalgebra of A which is F-linearly disjoint from K. Then A is free as a left (resp. right) L-module if and only if A is free as a left (resp. right) KL-module.*

Proof. We prove the statement for left modules, the proof for right modules is analogous. Note that the commutative L-algebra KL is isomorphic to $K \otimes_F L$, which is free as an L-module. Hence, if A is free as a left KL-module, then it is free as a left L-module.

Suppose conversely that A is free as a left L-module. Then $K \otimes_F A$ is free as a left KL-module. On the other hand, $K \otimes_F A$ is isomorphic as a left KL-module to $A^{[K:F]}$. Since K is étale and F-linearly disjoint from L, it follows from [5, Chap. V, §6, N° 7] that $KL \simeq K_1 \times \cdots \times K_r$ for some fields $K_1, \ldots, K_r$. Consider a finitely generated module M over $K_1 \times \cdots \times K_r$. Then M is of the form $M_1 \times \cdots \times M_r$ where M_i is a K_i-vector space for $i = 1, \ldots, r$. Furthermore M is free if and only if the dimensions $\dim_{K_i} M_i$ for $i = 1, \ldots, r$ are all the same. In particular, for M^n is free for an arbitrary positive integer n if and only if M is free. As $A^{[K:F]}$ is free as a left KL-module, we conclude that the same holds for A. □

We call the F-algebra A *central simple* if $\dim_F A < \infty$, $Z(A) = F$ and A is simple as a ring. Let A be a finite-dimensional simple F-algebra. Then $K = Z(A)$ is a field and A is a central simple K-algebra. By Wedderburn's Theorem (cf. [8, Theorem 2.1.3]) we have $\dim_K A = n^2$ for some positive integer n, which is called the *degree of* A and denoted by $\deg A$. Moreover, A is Brauer equivalent to a central division K-algebra D, which is is unique up to K-isomorphism. The degree of D is called the *index of* A and denoted by $\operatorname{ind} A$. If $\operatorname{ind} A = 1$ then A is K-isomorphic to $\mathbb{M}_n(K)$ for $n = \deg A$, and in this case we say that A is *split*. We further set $\operatorname{coind} A = \frac{\deg A}{\operatorname{ind} A}$ and call this the *coindex of* A. Hence, for any finite-dimensional division F-algebra D and any positive integer n we have $\operatorname{coind} \mathbb{M}_n(D) = n$.

Let A be an F-algebra. For any F-subalgebra B of A we obtain an F-subalgebra

$$C_A(B) = \{x \in A \mid xb = bx \text{ for all } b \in B\}$$

which is called the *centraliser of* B *in* A. Given two subalgebras L_1 and L_2 of A, we say that L_1 *centralises* L_2 if $L_1 \subseteq C_A(L_2)$, or equivalently, $L_2 \subseteq C_A(L_1)$.

An element $e \in A$ is called an *idempotent* if $e^2 = e$. For any nonzero idempotent $e \in A$ the ring eAe with unity e becomes an F-algebra by identifying F with eF. Moreover, if A is a central simple F-algebra, then also the F-algebra eAe is central simple, and it is Brauer equivalent to A.

2.3. **Proposition.** *Let A be a finite-dimensional simple F-algebra. Assume that $Z(A)$ is separable over F. Let L be a commutative semisimple F-subalgebra of A that is F-linearly disjoint from $Z(A)$. Then $C_A(L)$ is a semisimple F-algebra with centre L and*

$$[L : F] \cdot \dim_F C_A(L) \geqslant \dim_F A.$$

Moreover, the following conditions are equivalent:

(*a*) $[L : F] \cdot \dim_F C_A(L) = \dim_F A$;
(*b*) *all the simple components of $C_A(L)$ have the same degree;*
(*c*) *A is free as a left L-module;*
(*d*) *A is free as a right L-module.*

They hold in particular whenever L is a field or $[L : F] = \deg A$.

Proof. Let $K = Z(A)$. Note that $[KL : K] = [L : F]$, $C_A(KL) = C_A(L)$ and further that $\dim_F C_A(L) = [K : F]\cdot\dim_K C_A(KL)$ and $\dim_F A = [K : F]\cdot\dim_K A$. Hence, in view of the statements and by Lemma 2.2 we may replace K by F and assume that A is central simple as an F-algebra.

Note first that, if L is a field, then (a) holds by the Double Centraliser Theorem and furthermore conditions (b)–(d) are trivially satisfied.

In the general case let $e_1, \ldots, e_r$ be the primitive idempotents of L. For $i = 1, \ldots, r$ we set $A_i = e_iAe_i$ and $L_i = e_iL$. Thus, identifying F with $e_iF \subseteq L_i$, each L_i is a finite field extension of F contained in the central simple F-algebra A_i, and in the decomposition $A = \bigoplus_{i,j=1}^r e_iAe_j$ we have

$$C_A(L) = C_{A_1}(L_1) \oplus \cdots \oplus C_{A_r}(L_r).$$

Each $C_{A_i}(L_i)$ is a simple F-algebra with centre L_i, whereby $C_A(L)$ is a semisimple algebra with centre L. For $i = 1, \ldots, r$ we set $\ell_i = [L_i : F]$ and $d_i = \deg C_{A_i}(L_i)$ and obtain that $[L_i : F] \cdot \dim_F C_{A_i}(L_i) = \dim_F A_i = (\deg A_i)^2$ by the Double Centraliser Theorem, whereby $\deg A_i = \ell_i d_i$. Hence $\deg A = \sum_{i=1}^r \ell_i d_i$ and it follows that

$$\dim_F C_A(L) = \sum_{i=1}^r \dim_F C_{A_i}(L_i) = \sum_{i=1}^r \ell_i d_i^2.$$

As $[L : F] = \sum_{i=1}^r \ell_i$ it follows that

$$\begin{aligned}
[L : F] \cdot \dim_F C_A(L) &= \Big(\sum_{i=1}^r \ell_i\Big) \cdot \Big(\sum_{i=1}^r \ell_i d_i^2\Big) \\
&= \Big(\sum_{i=1}^r \ell_i d_i\Big)^2 + \sum_{i<j} \ell_i\ell_j(d_i - d_j)^2 \\
&= (\deg A)^2 + \sum_{i<j} \ell_i\ell_j(d_i - d_j)^2.
\end{aligned}$$

This proves the inequality in the statement as well as the equivalence of (a) and (b) because the last term on the right hand side vanishes if and only if $d_1 = \cdots = d_r$. To prove the equivalence of (b) with (c), note that by using [9, (1.9) and (1.10)] we have for $i = 1, \ldots, r$ that

$$\dim_F e_iA = \deg A_i \cdot \deg A = \ell_i d_i \deg A$$

and therefore $\dim_{L_i} e_iA = d_i \deg A$. Hence Condition (b) holds if and only if $\dim_{L_1} e_1A = \cdots = \dim_{L_r} e_rA$, which is Condition (c). The proof of the equivalence of (b) with (d) is completely analogous.

Since $[L : F] = \sum_{i=1}^r \ell_i$ and $\deg A = \sum_{i=1}^r \ell_i d_i$, the equality $[L : F] = \deg A$ requires that $d_1 = \cdots = d_r = 1$, which implies Condition (b). □

Let K be a quadratic étale F-subalgebra of A and let γ denote its nontrivial F-automorphism. We denote

$$C'_A(K) = \{x \in A \mid xk = \gamma(k)x \text{ for all } k \in K\}.$$

If A is a finite-dimensional semisimple F-algebra then for an element $a \in A$ we denote by

$$\operatorname{Prd}_{A,a}(X) \in F[X]$$

its reduced characteristic polynomial (see [12, §9]).

2.4. **Proposition.** *Assume that A is a central simple F-algebra. Let K be an F-subalgebra of A isomorphic to $F \times F$. Let e_1 and e_2 be the primitive idempotents of K and $A_i = e_i A e_i$ for $i = 1, 2$. Suppose that $\deg A_1 = \deg A_2$. Let $a \in C'_A(K)$, $u = e_1 a e_2$ and $v = e_2 a e_1$. Then $a = u + v$ and*

$$\operatorname{Prd}_{A,a}(X) = \operatorname{Prd}_{A_1,uv}(X^2) = \operatorname{Prd}_{A_2,vu}(X^2) \in F[X].$$

Proof. For $a \in C'_A(K)$, we have $ae_1 = e_2 a$ and $ae_2 = e_1 a$, hence $e_1 a = e_1 a e_2 = u$ and $e_2 a = e_2 a e_1 = v$, and therefore $a = e_1 a + e_2 a = u + v$. Then

$$uv = e_1 a e_2 a e_1 = e_1 a^2 e_1 \in A_1 \quad \text{and} \quad vu = e_2 a e_1 a e_2 = e_2 a^2 e_2 \in A_2.$$

To prove the equalities we may extend scalars to a splitting field of A. Thus we assume that A is split and identify A with a matrix algebra in such a way that $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $e_2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $a = \left(\begin{smallmatrix} 0 & u \\ v & 0 \end{smallmatrix}\right)$, where u and v are matrices. We have to show that the characteristic polynomials Pc_a, Pc_{uv}, Pc_{vu} are related by

$$\operatorname{Pc}_a(X) = \operatorname{Pc}_{uv}(X^2) = \operatorname{Pc}_{vu}(X^2).$$

Since the coefficients of the characteristic polynomials are polynomial functions of the entries, it suffices to prove these equalities in the case where u and v are generic matrices over $\mathbb{Z}$, for the general case then follows by specialization. Since we have $\operatorname{Tr}(a^{2k}) = 2\operatorname{Tr}\big((uv)^k\big) = 2\operatorname{Tr}\big((vu)^k\big)$ and $\operatorname{Tr}(a^{2k+1}) = 0$ for any $k \in \mathbb{N}$, we obtain the result by applying Newton's Identities relating the coefficients of the characteristic polynomial of a matrix to the traces of its powers. □

2.5. **Corollary.** *Assume that A is a central simple F-algebra. Let K be an étale quadratic F-subalgebra of A such that $\dim_F C_A(K) = \frac{1}{2}\dim_F A$. Then*

$$\operatorname{Prd}_{A,a}(X) = \operatorname{Prd}_{C_A(K),a^2}(X^2) \in F[X] \text{ for any } a \in C'_A(K).$$

Proof. To prove the equality we may extend scalars. Hence we may assume that K is split. Then the equation follows from Proposition 2.4. □

3. Capacity

In this section we recall some basic facts and objects associated with involutions on central simple algebras. We recall the distinction of involutions into two kinds and further into three different types. We further introduce some notation that will allow us to study involutions of different types and over fields of arbitrary characteristic in a unified way. Our main reference for involutions is [9].

Let A be an F-algebra. By an *F-involution on A* we mean an F-linear anti-automorphism $\sigma : A \to A$ such that $\sigma \circ \sigma = \mathsf{id}_A$. Given an F-involution on A we set

$$\begin{aligned} \operatorname{Sym}(\sigma) &= \{x \in A \mid \sigma(x) = x\}, \\ \operatorname{Skew}(\sigma) &= \{x \in A \mid \sigma(x) = -x\}, \\ \operatorname{Symd}(\sigma) &= \{x + \sigma(x) \mid x \in A\}. \end{aligned}$$

By an *F-algebra with involution* we mean a pair (A, σ) of a finite-dimensional F-algebra A and an F-involution σ on A with $F = Z(A) \cap \operatorname{Sym}(\sigma)$ and such that A has no non-trivial two-sided ideal I with $\sigma(I) = I$.

In the sequel let (A, σ) denote an F-algebra with involution. Then either $Z(A) = F$ or $Z(A)$ is a quadratic étale extension of F with non-trivial automorphism $\sigma|_{Z(A)}$. One says that (A, σ), or the involution σ, is of the *first kind* or of the *second kind*, respectively, according to whether $[Z(A) : F]$ equals 1 or 2.

As long as $Z(A)$ is a field it follows that A is central simple as a $Z(A)$-algebra. However, if (A, σ) is of the second kind, we may also have that $Z(A) \simeq F \times F$: in this case $(A, \sigma) \simeq (A_0 \times A_0^{\mathsf{op}}, \mathsf{sw})$ for a central simple F-algebra A_0 and where sw is the so-called *switch-involution* given by $\mathsf{sw}(a_1, a_2^{\mathsf{op}}) = (a_2, a_1^{\mathsf{op}})$ (see [9, (2.14)]).

If σ is an involution of the first kind, then we say that σ is *symplectic* if $\dim_F \operatorname{Symd}(\sigma) < \dim_F \operatorname{Skew}(\sigma)$ and $1 \in \operatorname{Symd}(\sigma)$, otherwise we say that σ is *orthogonal*. Considering the F-linear map $x \mapsto x + \sigma(x)$ one sees that

$$\dim_F \operatorname{Skew}(\sigma) + \dim_F \operatorname{Symd}(\sigma) = \dim_F A,$$

hence $\dim_F \operatorname{Symd}(\sigma) < \dim_F \operatorname{Skew}(\sigma)$ is equivalent to $\dim_F \operatorname{Symd}(\sigma) < \frac{1}{2} \dim_F A$.

If σ is of the second kind then we also say that σ is *unitary*. We say that (A, σ) is *unitary of inner type* when $Z(A) \simeq F \times F$. (The term is motivated by a corresponding notion for algebraic groups.)

The property of the involution σ to be *orthogonal*, *symplectic* or *unitary* is called its *type*. Notions for properties of an involution (such as its kind and its type) shall also be employed for the algebra with involution as a pair.

Whenever $Z(A)$ is a field we denote by $\deg A$, $\operatorname{ind} A$, $\operatorname{coind} A$ the degree, index or coindex of A, respectively, as a central simple $Z(A)$-algebra. In the case where $Z(A) \simeq F \times F$, we define the same terms with reference to (any of) the two simple components of A. We say that the algebra with involution (A, σ) is *split* if $\operatorname{ind} A = 1$.

Note that $\operatorname{Symd}(\sigma) \subseteq \operatorname{Sym}(\sigma)$ and that this is an equality unless $\operatorname{char} F = 2$ and (A, σ) is of the first kind. (See [9, (2.17)] for $\operatorname{char} F = 2$ and σ unitary.) To avoid case distinctions in our statements and arguments, we set

$$\operatorname{Sym}^*(\sigma) = \begin{cases} \operatorname{Sym}(\sigma) & \text{if } \sigma \text{ is orthogonal or unitary,} \\ \operatorname{Symd}(\sigma) & \text{if } \sigma \text{ is symplectic.} \end{cases}$$

Note that $\operatorname{Sym}^*(\sigma) = \operatorname{Symd}(\sigma)$ except when $\operatorname{char} F = 2$ and σ is orthogonal.

Dealing with orthogonal involutions in characteristic two requires additional care, as one may see in the following statement.

3.1. **Proposition.** *Let e be a nonzero idempotent in* $\mathrm{Sym}(\sigma)$ *and* $\sigma_e = \sigma|_{eAe}$. *Then* (eAe, σ_e) *is an F-algebra with involution of the same kind as* (A, σ). *Moreover,* (eAe, σ_e) *is of the same type as* (A, σ) *except when* $\operatorname{char} F = 2$, σ *is orthogonal and* $e \in \mathrm{Symd}(\sigma)$, *in which case* σ_e *is symplectic.*

Proof. Obviously the F-algebra eAe is stable under the F-involution σ_e and $Z(eAe) = eZ(A)e$. Hence (eAe, σ_e) is an F-algebra with involution of the same kind as (A, σ). To compare the types of the involutions, we only need to consider the case where (A, σ) is of the first kind.

If $a \in A$ is such that $a + \sigma(a)$ equals 1 or e, then $eae + \sigma(eae) = e$. Hence, if $1 \in \mathrm{Symd}(\sigma)$ or $e \in \mathrm{Symd}(\sigma)$, then $e \in \mathrm{Symd}(\sigma_e)$. It remains to consider the dimensions of $\mathrm{Symd}(\sigma)$ and $\mathrm{Symd}(\sigma_e)$.

Let $f = 1 - e$, and let $n = \deg A$, $r = \deg eAe$, and $s = \deg fAf$, so that $n = r + s$. The decomposition

$$A = eAe \oplus (eAf \oplus fAe) \oplus fAf$$

is stable under σ, hence

$$\mathrm{Symd}(\sigma) = \big(eAe \cap \mathrm{Symd}(\sigma)\big) \oplus \big((eAf \oplus fAe) \cap \mathrm{Symd}(\sigma)\big) \oplus \big(fAf \cap \mathrm{Symd}(\sigma)\big).$$

If $a \in A$ satisfies $a + \sigma(a) \in eAe$, then $a + \sigma(a) = eae + \sigma(eae)$. This shows that

$$eAe \cap \mathrm{Symd}(\sigma) = \mathrm{Symd}(\sigma_e),$$

and it follows that $\dim_F\big(eAe \cap \mathrm{Symd}(\sigma)\big) = \frac{1}{2}r(r + \varepsilon_e)$ with $\varepsilon_e = \pm 1$. Likewise, $\dim_F\big(fAf \cap \mathrm{Symd}(\sigma)\big) = \frac{1}{2}s(s + \varepsilon_f)$ with $\varepsilon_f = \pm 1$. Now, if $a \in A$ is such that $a + \sigma(a) = ebf + fce$ for some b, $c \in A$, then

$$ebf + fce = \sigma(ebf + fce) = e\sigma(c)f + f\sigma(b)e,$$

hence $fce = f\sigma(b)e = \sigma(ebf)$ and $a + \sigma(a) = ebf + \sigma(ebf)$. Therefore

$$(eAf \oplus fAe) \cap \mathrm{Symd}(\sigma) = \{x + \sigma(x) \mid x \in eAf\},$$

and it follows that $\dim_F(eAf \oplus fAe) \cap \mathrm{Symd}(\sigma) = \dim_F eAf = rs$. Therefore the above decomposition of $\mathrm{Symd}(\sigma)$ yields

$$\dim_F \mathrm{Symd}(\sigma) = \tfrac{1}{2}r(r + \varepsilon_e) + rs + \tfrac{1}{2}s(s + \varepsilon_f) = \tfrac{1}{2}(n^2 + r\varepsilon_e + s\varepsilon_f).$$

As $\dim_F \mathrm{Symd}(\sigma) = \frac{1}{2}n(n + \varepsilon)$ for $\varepsilon = \pm 1$, we conclude that $\varepsilon = \varepsilon_e = \varepsilon_f$. Hence, $\dim_F \mathrm{Symd}(\sigma) < \frac{1}{2}\dim_F A$ if and only if $\dim_F \mathrm{Symd}(\sigma_e) < \frac{1}{2}\dim_F eAe$. □

We give an example for the exceptional case in the statement of Proposition 3.1.

3.2. **Example.** Suppose that $\operatorname{char} F = 2$. Write t for the transpose involution on $\mathbb{M}_4(F)$. Consider the matrices

$$m = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad e = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

in $\mathbb{M}_4(F)$. The involution $\sigma = \operatorname{Int}(m) \circ t$ is orthogonal because m is not alternating. It is easy to see that $e \in \operatorname{Symd}(\sigma)$. Hence, σ restricts to a symplectic involution on $e\mathbb{M}_4(F)e$.

We define

$$\operatorname{cap}(A, \sigma) = \begin{cases} \deg A & \text{if } \sigma \text{ is orthogonal or unitary,} \\ \frac{1}{2} \deg A & \text{if } \sigma \text{ is symplectic,} \end{cases}$$

and call this integer the *capacity of* (A, σ). This terminology is inspired by the theory of Jordan algebras: when the characteristic is different from 2 and the algebra A is split, then $\operatorname{Sym}(\sigma)$ is a Jordan algebra of capacity equal to $\operatorname{cap}(A, \sigma)$; see [10, § I.5.1]. Note that with this definition, there exist F-algebras with involution of any given type and any positive integer as capacity.

3.3. **Proposition.** *Let L be an F-subalgebra of A contained in $\operatorname{Sym}(\sigma)$ and such that L/F is a separable field extension. Set $C = C_A(L)$ and $\sigma_C = \sigma|_C$. Then (C, σ_C) is an L-algebra with involution of the same type as (A, σ) and such that*

$$\operatorname{cap}(A, \sigma) = [L : F] \cdot \operatorname{cap}(C, \sigma_C) .$$

Proof. With $\sigma(L) = L$ we also have that $\sigma(C) = C$. Let $K = Z(A)$. Then $[LK : L] = [K : F]$ and $[LK : K] = [L : F]$. The Double Centraliser Theorem yields that $C_A(C) = KL$ and $\deg A = [L : F] \cdot \deg C$. As obviously $KL \subseteq Z(C) \subseteq C_A(C)$ we conclude that $Z(C) = KL$. Hence, (C, σ_C) is an L-algebra with involution, and σ_C is unitary if and only if σ is unitary. Using [9, (4.12)] in the other cases, we conclude that the L-algebra with involution (C, σ_C) has the same type as the F-algebra with involution (A, σ). Since $\deg A = [L : F] \cdot \deg C$ we conclude the analogous equality for the capacity. □

We are going to show in Theorem 4.1 that the capacity of (A, σ) is equal to the maximal value for $[L : F]$ where L is an étale F-algebra contained in $\operatorname{Sym}^*(\sigma)$. To this end we first consider the case where A is split, in which case we will even find a split étale subalgebra in $\operatorname{Sym}^*(\sigma)$ of degree equal to $\operatorname{cap}(A, \sigma)$.

3.4. **Proposition.** *Assume that (A, σ) is split. Then $\operatorname{Sym}^*(\sigma)$ contains a split étale F-subalgebra L of A with $[L : F] = \operatorname{cap}(A, \sigma)$.*

Proof. Set $n = \operatorname{cap}(A, \sigma)$. If $Z(A)$ is not a field, then (A, σ) can be identified with $(\mathbb{M}_n(F) \times \mathbb{M}_n(F)^{\mathsf{op}}, \mathsf{sw})$, and letting $L_0 \subseteq \mathbb{M}_n(F)$ be the algebra of diagonal matrices and $L = \{(x, x) \mid x \in L_0\}$, we obtain that $L \subseteq \operatorname{Sym}^*(\sigma)$ and $L \simeq F^n$.

We may thus assume that $K = Z(A)$ is a field. We identify A with $\operatorname{End}_K V$ for some K-vector space V. Then σ is the adjoint involution of some nondegenerate F-bilinear form $b : V \times V \to K$, which is symmetric nonalternating if σ is orthogonal, alternating if σ is symplectic, and hermitian with respect to the nontrivial F-automorphism of K if σ is unitary. If σ is orthogonal or unitary (resp. symplectic), we may decompose V into an orthogonal sum of 1-dimensional (resp. 2-dimensional) K-subspaces

$$V = V_1 \perp \ldots \perp V_n$$

where $n = \operatorname{cap}(\sigma)$. For $i = 1, \ldots, n$, let $e_i \colon V \to V_i$ be the orthogonal projection corresponding to this decomposition, viewed as an K-endomorphism of V. Since for all $x, y \in V$ we have

$$b\big(x, e_i(y)\big) = b\big(e_i(x), e_i(y)\big) = b(e_i(x), y),$$

we have that $e_i \in \operatorname{Sym}(\sigma)$ and conclude by Proposition 3.1 that $e_i \in \operatorname{Sym}^*(\sigma)$. Hence $L = Fe_1 \oplus \cdots \oplus Fe_n$ is an F-subalgebra of A contained in $\operatorname{Sym}^*(\sigma)$ with $L \simeq F^n$. □

4. Forms on the space of symmetrized elements

Certain existence statements for elements or subalgebras with special properties in an algebra with involution can be proven by reducing to the situation where the base field is algebraically closed. This requires a geometric description of the property in question. Here we are interested in elements and subalgebras contained in $\operatorname{Sym}^*(\sigma)$. To obtain a geometric formulation we introduce a polynomial $\chi_a \in F[X]$ associated to an arbitrary element $a \in \operatorname{Sym}^*(\sigma)$, whose degree is $\operatorname{cap}(A, \sigma)$ and which has a as a root. It is defined as either the reduced characteristic polynomial $\operatorname{Prd}_{A,a}$ or the Pfaffian characteristic polynomial $\operatorname{Prp}_{\sigma,a}$ (see [9, (2.10)]):

$$\chi_a = \begin{cases} \operatorname{Prd}_{A,a} & \text{if } \sigma \text{ is orthogonal or unitary,} \\ \operatorname{Prp}_{\sigma,a} & \text{if } \sigma \text{ is symplectic.} \end{cases}$$

For the unitary case, note that, even though the coefficients of the reduced characteristic polynomial of any $a \in A$ lie in $Z(A)$, yet when $\sigma(a) = a$ the coefficients of $\operatorname{Prd}_{A,a}$ lie in F (see [9, (2.16)]). (When $(A, \sigma) = (A_0 \times A_0^{\mathsf{op}}, \mathsf{sw})$, then $a = (a_0, a_0^{\mathsf{op}})$ for some $a_0 \in A_0$, and $\chi_a = \operatorname{Prd}_{A_0, a_0}$.) Thus we have $\chi_a \in F[X]$ in all cases. Note that χ_a is a multiple of the minimal polynomial of a over F and that the two polynomials have the same irreducible factors. Therefore, if χ_a is separable then χ_a is the minimal polynomial of a over F.

4.1. **Theorem.** *Any étale F-subalgebra of A contained in* $\operatorname{Sym}(\sigma)$ *is contained in* $\operatorname{Sym}^*(\sigma)$. *Furthermore*

$$\operatorname{cap}(A, \sigma) = \max\{[L : F] \mid L \text{ étale } F\text{-algebra with } L \subseteq \operatorname{Sym}(\sigma)\}.$$

Proof. Let $L \subseteq \mathrm{Sym}(\sigma)$ be an étale F-algebra. To show that $L \subseteq \mathrm{Sym}^*(\sigma)$ and $[L : F] \leqslant \mathrm{cap}(\sigma)$, we may extend scalars and assume that F is algebraically closed. Then L and $Z(A)$ are split. Let $r = [L : F]$ and let $e_1, \dots, e_r \in L$ be the primitive idempotents in L. Then $e_i e_j = \delta_{ij}$ for $i, j \in \{1, \dots r\}$ and $\sum_{i=1}^r e_i = 1$. It follows that

$$\deg A = \sum_{i=1}^{r} \deg(e_i A e_i).$$

If σ is orthogonal or unitary, then we have $\mathrm{Sym}^*(\sigma) = \mathrm{Sym}(\sigma)$ and $\mathrm{cap}(A, \sigma) = \deg(A) \geqslant r$, because $\deg(e_i A e_i) \geqslant 1$ for $i = 1, \dots, r$. Assume now that σ is symplectic. Then Proposition 3.1 shows for $i = 1, \dots, r$ that σ restricts on $e_i A e_i$ to a symplectic involution, whereby $\deg(e_i A e_i) \geqslant 2$ and $e_i \in \mathrm{Symd}(\sigma)$. We conclude that $L \subseteq \mathrm{Symd}(\sigma)$ and $\mathrm{cap}(\sigma) = \frac{1}{2} \deg A = \sum_{i=1}^r \frac{1}{2} \deg e_i A e_i \geqslant r$. This shows that $L \subseteq \mathrm{Sym}^*(\sigma)$ and $[L : F] = r \leqslant \mathrm{cap}(A, \sigma)$ in any case.

Back in the situation where F is an arbitrary field, it remains to show that $\mathrm{Sym}^*(\sigma)$ contains an étale F-algebra L with $[L : F] = \mathrm{cap}(\sigma)$. This follows from Proposition 3.4 if (A, σ) is split. In particular, we may assume that F is infinite. Let $\overline{F}$ denote an algebraic closure of F. Then $\mathrm{Sym}^*(\sigma)$ is Zariski-dense in $\overline{\mathrm{Sym}^*(\sigma)} = \mathrm{Sym}^*(\sigma) \otimes_F \overline{F}$. An element $a \in \overline{\mathrm{Sym}^*(\sigma)}$ is separable over $\overline{F}$ if and only if the discriminant of χ_a is nonzero. Since this is a polynomial condition, the elements of $\overline{\mathrm{Sym}^*(\sigma)}$ which are separable over $\overline{F}$ form an open subset of $\overline{\mathrm{Sym}^*(\sigma)}$, and by Proposition 3.4 and Lemma 2.1 this subset is not empty. Since $\mathrm{Sym}^*(\sigma)$ is dense in $\overline{\mathrm{Sym}^*(\sigma)}$, we conclude that there exists an element $a \in \mathrm{Sym}^*(\sigma)$ which is separable over $\overline{F}$, and thus separable over F. Hence χ_a is equal to the minimal polynomial of a over F. We conclude that $F[a]$ is an étale F-algebra and $[F[a] : F] = \deg(\chi_a) = \mathrm{cap}(A, \sigma)$. □

The F-vector space $\mathrm{Sym}^*(\sigma)$ may contain (non-étale) commutative F-algebras L with $[L : F] > \mathrm{cap}(A, \sigma)$.

4.2. **Example.** Let L_0 be the F-subalgebra of $\mathbb{M}_4(F)$ consisting of the matrices

$$\begin{pmatrix} a & 0 & b & c \\ 0 & a & d & e \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix}$$

with $a, b, c, d, e \in F$. Then $L = \{(x, x) \mid x \in L_0\}$ is a 5-dimensional commutative F-subalgebra of $A = \mathbb{M}_4(F) \times \mathbb{M}_4(F)^{\mathsf{op}}$. For the involution $\sigma = \mathsf{sw}$ on A we have that $\mathrm{cap}(A, \sigma) = 4$ and $L \subseteq \mathrm{Sym}(\sigma) = \mathrm{Sym}^*(\sigma)$.

4.3. **Proposition.** *Let $\Psi : (A, \sigma) \to (B, \tau)$ be a homomorphism of F-algebras with involution with $\mathrm{cap}(A, \sigma) = \mathrm{cap}(B, \tau)$. Then $\chi_{\Psi(a)} = \chi_a$ holds for every $a \in \mathrm{Sym}^*(\sigma)$. Furthermore, if (A, σ) and (B, τ) are of the same type, then Ψ is an isomorphism.*

Proof. The characteristic polynomial is invariant under algebra isomorphisms and under scalar extension. Hence, the first part of the statement is obtained by extending scalars to an algebraically closure, where it is easy to verify. Finally, if (A,σ) and (B,τ) are of the same type then $\dim_F A = \dim_F B$ and since Ψ is injective, it follows that it is an isomorphism of algebras with involution. □

We give some examples of split algebras with involution and embeddings between them. For a matrix α with coefficients in a ring we denote by α^t the transpose matrix of α. If m is a positive integer and α and β are two $m \times m$ matrices over a ring, then we denote by $\alpha \times \beta$ the $2m \times 2m$ matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

4.4. **Proposition.** *Let m be a positive integer.*

(*a*) *The map $u : \mathbb{M}_m(F)^2 \to \mathbb{M}_m(F)^2, (\alpha,\beta) \longmapsto (\beta^t, \alpha^t)$ turns $(\mathbb{M}_m(F)^2, u)$ into an F-algebra with unitary involution of capacity m.*

(*b*) *The map*

$$s : \mathbb{M}_{2m}(F) \to \mathbb{M}_{2m}(F), \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \delta^t & -\beta^t \\ -\gamma^t & \alpha^t \end{pmatrix}$$

turns $(\mathbb{M}_{2m}(F), s)$ into an F-algebra with symplectic involution of capacity m.

(*c*) *The map $\Phi : (\mathbb{M}_m(F), t) \to (\mathbb{M}_{2m}(F), s), \alpha \mapsto \alpha \times \alpha^t$ is a homomorphism of F-algebras with involution.*

(*d*) *The map $\Psi : (\mathbb{M}_m(F) \times \mathbb{M}_m(F), u) \to (\mathbb{M}_{2m}(F), s), (\alpha,\beta) \mapsto \alpha \times \beta$ is a homomorphism of F-algebras with involution.*

(*e*) *We have $\Phi(\mathbb{M}_m(F)) = \Psi(\mathrm{Sym}(u))$.*

Proof. This is obvious. □

We consider the case $m = 2$.

4.5. **Example.** Let

$$\mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{M}_2(F) \text{ and } J = \begin{pmatrix} 0 & \mathbb{I}_2 \\ -\mathbb{I}_2 & 0 \end{pmatrix} \in \mathbb{M}_4(F).$$

The involution $s : \mathbb{M}_4(F) \to \mathbb{M}_4(F)$ of Proposition 4.4 is given by $\mathrm{Int}(J) \circ t$, where t is the transposition involution. The F-space $\mathrm{Symd}(s)$ consists of the matrices

$$\begin{pmatrix} a & b & 0 & e \\ c & d & -e & 0 \\ 0 & f & a & c \\ -f & 0 & b & d \end{pmatrix}$$

with $a,b,c,d,e,f \in F$. For later use we note that the determinant of such a matrix is equal to $(ad - bc + ef)^2$.

For $a \in \mathrm{Sym}^*(\sigma)$ we write

$$\chi_a = X^d - c_1(a)X^{d-1} + c_2(a)X^{d-2} - \cdots + (-1)^d c_d(a)$$

and observe that this defines a form $c_i\colon \mathrm{Sym}^*(\sigma) \to F$ of degree i for $i = 1, \ldots, d$.

We recall some quadratic form terminology from [6, (7.17)]. Let $q : V \to F$ be a quadratic form over F, defined on a finite-dimensional F-vector space V. We denote by b_q the *polar form of* q given by

$$V \times V \to F, (x, y) \mapsto q(x + y) - q(x) - q(y)\,.$$

We further set

$$\begin{aligned} \mathrm{rad}(b_q) &= \{x \in V \mid b_q(x, y) = 0 \text{ for all } y \in V\} \\ \mathrm{rad}(q) &= \{x \in \mathrm{rad}(b_q) \mid q(x) = 0\} \end{aligned}$$

and observe that these are F-subspaces of V with $\mathrm{rad}(q) \subseteq \mathrm{rad}(b_q)$. Moreover, if $\mathrm{char}\, F \neq 2$ then $q(x) = \frac{1}{2}b_q(x, x)$ for all $x \in V$ and thus $\mathrm{rad}(q) = \mathrm{rad}(b_q)$. We call the quadratic form q *regular* if $\mathrm{rad}(q) = \{0\}$ and *nondegenerate* if q is regular and $\dim_F \mathrm{rad}(b_q) \leqslant 1$.

4.6. **Proposition.** *Assume that* $\mathrm{cap}(A, \sigma) = 2$ *and set* $V = \mathrm{Sym}^*(\sigma)$. *Then*

$$\dim_F V = \begin{cases} 3 & \text{if } \sigma \text{ is orthogonal,} \\ 4 & \text{if } \sigma \text{ is unitary,} \\ 6 & \text{if } \sigma \text{ is symplectic} \end{cases}$$

and $c_2|_V : V \to F$ *is a nondegenerate quadratic form over* F, *also given by the rule* $x \mapsto x\overline{x}$ *where* $\overline{x} = c_1(x) - x$ *for* $x \in V$.

Proof. By the definitions of the capacity and of V the value of $\dim_F V$ follows from [9, (2.6)]. For $x \in V$ we have $c_2(x) = c_2(x) - \chi_x(x) = -x^2 + c_1(x)x = x\overline{x}$.

To show that the quadratic form c_2 is nondegenerate we may extend scalars and assume that F is algebraically closed. Note that (A, σ) is isomorphic to any F-algebra with involution of same type and of capacity 2. It thus suffices to prove that c_2 is nondegenerate for a convenient choice of (A, σ).

Consider the F-linear map

$$\Gamma : F^6 \to \mathbb{M}_4(F)\,, (a, b, c, d, e, f) \longmapsto \begin{pmatrix} a & b & 0 & e \\ c & d & -e & 0 \\ 0 & f & a & c \\ -f & 0 & b & d \end{pmatrix}.$$

The characteristic polynomial of $\Gamma(a, b, c, d, e, f)$ is $(T^2-(a+d)T+(ad-bc+ef))^2$, hence its Pfaffian polynomial is $T^2 - (a + d)T + (ad - bc + ef)$. In particular, $c_2(\Gamma(a, b, c, d, e, f)) = ad - bc + ef$.

Suppose that σ is symplectic. Then (A, σ) is identified with $(\mathbb{M}_4(F), s)$, whereby $V = \Gamma(F^6)$. Hence the form c_2 is given by the polynomial $X_1X_4 - X_2X_3 + X_5X_6$, whence it is hyperbolic. and in particular nondegenerate.

Suppose that σ is unitary. Then (A,σ) is identified with the image of Ψ, thus $V = \{\Gamma(a,b,c,d,0,0) \mid a,b,c,d \in F\}$. Hence, c_2 is given by the polynomial $X_1X_4 - X_2X_3$, whence it is hyperbolic and in particular nondegenerate.

Suppose that σ is orthogonal. Then (A,σ) is identified with the image of Φ. Thus we have $V = \{\Gamma(a,b,c,a,0,0) \mid a,b,c \in F\}$. Hence, c_2 is given by the polynomial $X_1^2 - X_2X_3$, whence it is nondegenerate. □

5. Neat subalgebras

Let (A,σ) be an F-algebra with involution. An F-subalgebra L of A is called *neat in* (A,σ) or a *neat subalgebra of* (A,σ) if L is étale, $L \subseteq \mathrm{Sym}(\sigma)$, A is free as a left L-module and, for all primitive idempotents e of L the F-algebras with involution $(eAe, \sigma|_{eAe})$ have the same degree and the same type; this type then coincides with the type of σ. Note that the condition on the type of $\sigma|_{eAe}$ is only relevant when $\operatorname{char} F = 2$ and σ is orthogonal, otherwise it holds by Proposition 3.1.

5.1. **Proposition.** *Let L be a neat F-subalgebra of (A,σ) and let K be an F-subalgebra of L. Then K is neat in (A,σ) if and only if L is free as a K-module.*

Proof. Both conditions are invariant under scalar extensions, so we suppose that the étale F-algebra L is split. Then K is split as well. Let $n = [L:F]$ and let $e_1,\dots,e_n$ denote the primitive idempotents of L. Since L is neat in (A,σ) we have $\deg e_iAe_i = \frac{1}{n}\deg A$ for $i = 1,\dots,n$.

Let $r = [K:F]$ and let $f_1,\dots,f_r$ denote the primitive idempotents of K. Then there is a partition $I_1,\dots,I_r$ of $\{1,\dots,n\}$ such that, for $j = 1,\dots,r$, we have that $f_j = \sum_{i\in I_j} e_i$ and thus $|I_j| \cdot \deg f_jAf_j = \frac{1}{n}\deg A$. Therefore, the equality $\deg f_1Af_1 = \dots = \deg f_rAf_r$ is equivalent to the equality $|I_1| = \dots = |I_r|$, which holds if and only if L is free as a K-module. Since the conditions for neatness related to the involution are inherited from L to K, the statement follows. □

We first consider neat subalgebras in algebras with unitary involution of inner type.

5.2. **Proposition.** *Assume that $(A,\sigma) = (A_0 \times A_0^{\mathsf{op}}, \mathsf{sw})$ for a central simple F-algebra A_0. Any étale F-subalgebra L_0 of A_0 gives rise to an étale F-subalgebra $L = \{(x, x^{\mathsf{op}}) \mid x \in L_0\}$ of A contained in $\mathrm{Sym}(\sigma)$ and isomorphic to L_0. Conversely, any étale F-subalgebra L of A contained in $\mathrm{Sym}(\sigma)$ is obtained in this way. Furthermore, L is neat in (A,σ) if and only if A_0 is free as an L_0-left module.*

Proof. This is obvious. □

We show next that an étale F-subalgebra of A contained in $\mathrm{Sym}(\sigma)$ of maximal possible degree is automatically neat in (A,σ).

5.3. **Proposition.** *Let L be an étale F-subalgebra of A with $L \subseteq \mathrm{Sym}(\sigma)$ and $[L:F] = \mathrm{cap}(\sigma)$. Then L is neat in (A,σ).*

Proof. If $(A,\sigma) = (A_0 \times A_0^{\mathsf{op}}, \mathsf{sw})$ for some central simple F-algebra A_0 then the statement follows from Proposition 5.2 and Proposition 2.3. Hence we may assume that A is simple.

Let $e_1, \dots, e_r$ be the primitive idempotents of L. For $i = 1, \dots, r$, set $L_i = e_i L$, $A_i = e_i A e_i$, $\ell_i = [L_i : F]$, $d_i = \deg C_{A_i}(L_i)$ and $\sigma_i = \sigma|_{A_i}$, whereby (A_i, σ_i) is an F-algebra with involution with $Z(A_i) = e_i Z(A) e_i$ and $L_i \subseteq \mathrm{Sym}^*(\sigma_i)$, according to Theorem 4.1.

As in the proof of Proposition 2.3 we obtain that $[L : F] = \sum_{i=1}^r \ell_i$ and $\deg(A) = \sum_{i=1}^r \ell_i d_i$ and further that $\deg(A_i) = \ell_i d_i$ for $i = 1, \dots, r$. Hence the hypothesis $[L:F] = \mathrm{cap}(\sigma)$ yields that

$$d \cdot \sum_{i=1}^r \ell_i = \sum_{i=1}^r \ell_i d_i$$

where $d = 2$ if σ is symplectic and $d = 1$ otherwise. In the case where σ is symplectic, we obtain for $i = 1, \dots, r$ that σ_i is symplectic and $L_i \subseteq \mathrm{Symd}(\sigma_i)$, so that σ_i restricts to a symplectic involution on $C_{A_i}(L_i)$, which implies that d_i is even. In any case we conclude from the above equality that $d_1 = \cdots = d_r = d$. Note further that if σ is orthogonal, then for $i = 1, \dots, r$ we have that $A_i = L_i$ and $\sigma_i = \mathsf{id}_{L_i}$, which is an orthogonal involution.

This together with Proposition 3.1 implies that σ restricts in every case to an involution of the same type on eAe for every primitive idempotent e of L. Hence, L is neat in (A,σ). □

If $\mathrm{char}\, F = 2$ and σ is orthogonal then there may exist étale F-subalgebras L of A that are maximal in $\mathrm{Sym}^*(\sigma)$ and with $[L:F] < \mathrm{cap}(A,\sigma)$, as the following example illustrates. In any other case one can actually show that étale F-subalgebras of A contained in $\mathrm{Sym}^*(\sigma)$ and maximal for these properties are of degree equal to $\mathrm{cap}(A,\sigma)$.

5.4. **Example.** We enhance Example 3.2, where $\mathrm{char}\, F = 2$ and where in the F-algebra $A = \mathbb{M}_4(F)$ we considered two matrices m and e and the orthogonal involution $\sigma = \mathrm{Int}(m) \circ t$ whose restriction to eAe is symplectic. Set

$$e_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in A.$$

The F-subalgebra $L = Fe_1 \oplus Fe_2 \oplus Fe$ of A is split étale and maximal with respect to inclusion among the étale subalgebras of $\mathrm{Sym}(\sigma) = \mathrm{Sym}^*(\sigma)$, and yet we have $\dim_F L = 3 < 4 = \mathrm{cap}(\sigma)$. The F-subalgebra L is not neat in (A,σ) because the restriction of σ to eAe is symplectic, but also because the conditions

of Proposition 2.3 do not hold, since $[L : F]$ does not divide $[\mathbb{M}_4(F) : F]$. Likewise, the F-algebra $L' = Fe_1 \oplus F(e_2 + e)$ is split étale and contained in $\mathrm{Sym}^*(\sigma)$, but even though the restrictions of σ to e_1Ae_1 and $(e_2 + e)A(e_2 + e)$ are orthogonal, L' is not neat in (A, σ) because the simple components of its centraliser do not have the same dimension.

In the rest of this section, we investigate neat subalgebras of (A, σ) that are split. We start with the following observation on split étale subalgebras of central simple algebras.

5.5. **Proposition.** *Let D be a finite-dimensional division F-algebra, V a finite-dimensional right D-vector space and $A = \mathrm{End}_D V$. Let $e_1, \dots, e_r \in A \setminus \{0\}$. The following are equivalent:*

(*a*) $V = e_1V \oplus \cdots \oplus e_rV$.
(*b*) $1 = e_1 + \cdots + e_r$ *and* $e_ie_j = \delta_{ij}e_i$ *for* $1 \leqslant i, j \leqslant r$.
(*c*) $L = F[e_1, \dots, e_r]$ *is a split étale F-subalgebra of A with* $[L : F] = r$.

Proof. This is obvious. □

We refer to [9, §4] for the terminology and basic facts on hermitian forms. An orthogonal decomposition of a hermitian form yields a split étale subalgebra contained in the space of symmetric elements of the adjoint algebra with involution.

5.6. **Proposition.** *Let D be a finite-dimensional division F-algebra, V a finite-dimensional right D-vector space and $A = \mathrm{End}_D V$. Let τ be an F-involution on D for which (D, τ) is an F-algebra with involution. Let $h : V \times V \to D$ be a hermitian or skew-hermitian form with respect to τ and let σ be the F-involution on $A = \mathrm{End}_D V$ adjoint to h. Let $V_1, \dots, V_r$ be D-subspaces of V such that*

$$V = V_1 \oplus \cdots \oplus V_r\,.$$

Let $e_1, \dots, e_r \in A$ denote the projections corresponding to this decomposition and $L = F[e_1, \dots, e_r]$. Then the following hold:

(*i*) *L is a split F-étale subalgebra of A with $[L : F] = r$.*
(*ii*) *(A, σ) is an F-algebra with involution of the same kind as (D, τ).*
(*iii*) *$L \subseteq \mathrm{Sym}(\sigma)$ if and only if the decomposition $V = V_1 \oplus \cdots \oplus V_r$ is orthogonal with respect to h.*
(*iv*) *If $L \subseteq \mathrm{Sym}(\sigma)$, then L is neat in (A, σ) if and only if for $i = 1, \dots, r$ we have $\dim_D V_i = \frac{1}{r} \dim_D V$ and h restricts to a non-alternating form on V_i in the case where h is non-alternating.*

Proof. By Proposition 5.5 we have (*i*). Part (*ii*) is [9, (4.2)]. By the definition of L we have $L \subseteq \mathrm{Sym}(\sigma)$ if and only if

$$h\big(x, e_i(y)\big) = h\big(e_i(x), e_i(y)\big) = h(e_i(x), y)$$

holds for all $i = 1, \dots, m$ and $x, y \in V$, which is if and only if the decomposition of V is orthogonal with respect to h. This shows (iii).

We have

$$C_A(L) = e_1 A e_1 \oplus \cdots \oplus e_r A e_r = (\operatorname{End}_D V_1) \oplus \cdots \oplus (\operatorname{End}_D V_r)$$

and $\dim_D V_i = \deg \operatorname{End}_D V_i$ for $i = 1, \dots, r$. Hence, all simple components of $C_A(L)$ have the same degree if and only if $\dim_D V_i = \frac{1}{r} \dim_D V$ for $i = 1, \dots, r$. Assuming that $L \subseteq \operatorname{Sym}(\sigma)$, it is clear that for $i = 1, \dots, r$ the involution σ restricts to an involution of the same type on $e_i A e_i$ except if σ is orthogonal and $\operatorname{char} F = 2$, and in that case the condition holds if and only if the restriction of h on V_i is non-alternating. This shows (iv). □

5.7. **Corollary.** *Let r be a positive integer. There exists a split neat F-subalgebra of (A, σ) of degree r if and only if r divides* $\operatorname{coind} A$ *and* $\operatorname{cap}(A, \sigma)$.

Proof. Note that if (A, σ) is not split symplectic then $\operatorname{coind} A$ divides $\operatorname{cap}(A, \sigma)$.

A central simple algebra A_0 contains an F-subalgebra L_0 isomorphic to F^r and such that A_0 is free as a left L_0-module if and only if r divides $\operatorname{coind} A_0$. This together with Proposition 5.2 shows the statement in the case where (A, σ) is unitary of inner type.

We may thus assume that A is simple. We identify A with $\operatorname{End}_D(V)$ where D is a division F-algebra and V is a finite-dimensional right D-vector space. Then $\dim_D V = \operatorname{coind} A$. If (A, σ) is split symplectic, then $D = F$ and we set $\tau = \mathsf{id}_F$. In any other case we may fix an F-involution τ on D of the same type as σ. Then σ is adjoint to a τ-sesquilinear form $h : V \times V \to D$ which is alternating if (A, σ) is split symplectic and hermitian otherwise. It is clear that an orthogonal decomposition of (V, h) in r subspaces of equal dimension does exist if and only if r divides $\dim_D V$ and further $\frac{1}{2} \dim_F V$ in the case where (A, σ) is split symplectic. Hence the statement follows from Proposition 5.6. □

5.8. **Corollary.** *Assume (A, σ) is split. Any split neat F-subalgebra K of (A, σ) is contained in a split neat F-subalgebra L of (A, σ) with $[L : F] = \operatorname{cap}(A, \sigma)$.*

Proof. Set $r = [K : F]$ and $m = \operatorname{cap}(A, \sigma)$. Assume first $Z(A)$ is a field. We may identify A with $\operatorname{End}_{Z(A)} V$ for a free $Z(A)$-vector space V with $\dim_{Z(A)} V = \deg A$. Then σ is adjoint to an F-bilinear form $h : V \times V \to Z(A)$ which is symmetric, alternating or $Z(A)/F$-hermitian, according to its type. By Proposition 5.5 and Proposition 5.6 any split neat F-subalgebra K of (A, σ) with $[K : F] = r$ is given by an orthogonal decomposition of (V, h) into r equidimensional subspaces. By Corollary 5.7 then r divides m. Hence this decomposition of (V, h) can be refined to an orthogonal decomposition of m equidimensional subspaces, which by Corollary 5.7 corresponds to a split neat F-subalgebra L of (A, σ) with the desired properties.

Assume now that (A, σ) is split unitary of inner type. Hence we may identify (A, σ) with $(A_0 \times A_0^{\mathsf{op}}, \mathsf{sw})$ for $A_0 = \operatorname{End}_F(V)$ where V is an F-vector space with

$\dim_F V = \deg A_0 = m$. Then $K = \{(x, x^{\mathsf{op}}) \mid x \in K_0\}$ for a split étale F-subalgebra K_0 of A_0 with $[K_0 : F] = r$. By Proposition 5.5 then K_0 corresponds to a decomposition of V into a direct sum of r subspaces. Since A is free as a left K-module, we conclude by Lemma 2.2 that A_0 is free as a left K_0-module. In particular r divides $\dim_F V$ and K_0 is given by a decomposition of V into a direct sum of r equidimensional subspaces. Hence this direct decomposition of V can be refined into a direct decomposition of m one-dimensional subspaces, which corresponds to an embedding of K_0 into a split étale F-subalgebra L_0 of A_0 with $[L_0 : F] = \dim_F V = m$. Then $L = \{(x, x^{\mathsf{op}}) \mid x \in L_0\}$ has the desired properties. □

6. Neat quadratic subalgebras

Throughout this section let (A, σ) be an F-algebra with involution and let K be a neat quadratic F-subalgebra of (A, σ). We shall prove that there exists a maximal neat subalgebra of (A, σ) of the form KL for a neat F-subalgebra L of (A, σ) which is F-linearly disjoint from K. This result will be crucial for our main results in the final section.

Set $C = C_A(K)$ and $C' = C'_A(K) = \{x \in A \mid xk = \gamma(k)x \text{ for all } k \in K\}$ where γ denotes the nontrivial F-automorphism of K.

6.1. **Proposition.** *We have $A = C \oplus C'$ and the F-vector spaces C and C' are stable under σ and satisfy*

$$C \cap \operatorname{Symd}(\sigma) = \operatorname{Symd}(\sigma|_C) \quad \text{and} \quad C' \cap \operatorname{Sym}(\sigma) = C' \cap \operatorname{Symd}(\sigma)\,.$$

Moreover, $\dim_F C' = \dim_F C = \frac{1}{2}\dim_F A$ *and* $\dim_F\big(C' \cap \operatorname{Sym}(\sigma)\big) = \frac{1}{4}\dim_F A$.

Proof. We fix $u \in K \setminus F$ with $u^2 - u \in F$ and set $c = u^2 - u$. Hence $\gamma(u) = 1 - u$ and we have $4c + 1 \neq 0$ because the roots of the polynomial $X^2 - X - c$ are simple. We obtain that $C' = \{x \in A \mid xu + ux = x\}$. Since $\sigma(u) = u$ we have $\sigma(C') = C'$.

Consider the F-linear map

$$\varphi\colon A \to A, \quad x \mapsto \tfrac{1}{4c+1}\big((2c+1)x - ux - xu + 2uxu\big).$$

Computation shows that $\varphi(x) \in C$ and $x - \varphi(x) \in C'$ for any $x \in A$, and moreover $\varphi(x) = x$ for $x \in C$ and $\varphi(x) = 0$ for $x \in C'$. Therefore

$$A = C \oplus C'\,.$$

Since K is neat in (A, σ) and $[K : F] = 2$, it follows from Proposition 2.3 that $\dim_F C = \frac{1}{2}\dim_F A$, whereby $\dim_F C' = \frac{1}{2}\dim_F A$.

Now, consider the F-linear map $f\colon C' \to C', x \mapsto x + \sigma(x)$ and set $W = \ker(f)$ and $U = f(C')$. Hence $W = C' \cap \operatorname{Skew}(\sigma)$ and $\dim_F C' = \dim_F W + \dim_F U$. For $x \in C' \cap \operatorname{Sym}(\sigma)$ we have $x = xu + ux = xu + \sigma(xu) \in U \subseteq C' \cap \operatorname{Symd}(\sigma)$, whereby

$$U = C' \cap \operatorname{Sym}(\sigma) = C' \cap \operatorname{Symd}(\sigma)\,.$$

As $(1-2u)^2 = 1+4c \in F^\times$, multiplication from the left by $1-2u$ yields F-isomorphisms between U and W. Hence $\dim_F U = \dim_F W = \frac{1}{2}\dim_F C'$.

Clearly we have $\mathrm{Symd}(\sigma|_C) \subseteq C \cap \mathrm{Symd}(\sigma)$. To show the converse inclusion, we may obviously assume that $\mathrm{char}\, F = 2$, whereby $u^2+u = c \in F$. Consider $z \in C \cap \mathrm{Symd}(\sigma)$. Let $x \in A$ be such that $z = \sigma(x)+x$. As $u \in K \subseteq C$ we have $zu = uz$ and obtain that $\sigma(xu+ux) = (z+x)u + u(z+x) = ux+xu$ and thus

$$z = \sigma(xu+ux+x) + xu + ux + x\,.$$

Since $u(ux+xu+x) = (u^2+u)x + uxu = x(u^2+u) + uxu = (ux+xu+x)u$ we further have $ux+xu+x \in C_A(u) = C$ and conclude that $z \in \mathrm{Symd}(\sigma|_C)$. □

6.2. **Remark.** The definition of φ in the proof comes from the observation that $\frac{1}{4c+1}(2c+1-u\otimes 1 - 1\otimes u + 2u\otimes u)$ is the separability idempotent of K.

Let us consider in more detail the case where K is a field. We then consider C as a K-algebra and denote by σ_C the K-involution on C obtained by restricting σ.

6.3. **Proposition.** *Assume that K is a field. For $a \in C' \cap \mathrm{Sym}(\sigma)$ we have*

$$a^2 \in \mathrm{Sym}^*(\sigma_C) \text{ and } \chi_{A,a}(X) = \chi_{C,a^2}(X^2) \in F[X^2]\,.$$

Proof. As $a \in C' \cap \mathrm{Sym}(\sigma)$ we have that $a^2 \in C \cap \mathrm{Sym}(\sigma)$. If σ is symplectic then σ_C is symplectic by Proposition 3.3 and for $\ell \in C$ satisfying $\ell + \sigma(\ell) = 1$ we obtain that $a^2 = a\ell a + \sigma(a\ell a)$. This shows that $a^2 \in \mathrm{Sym}^*(\sigma_C)$.

From Corollary 2.5 we obtain the equality

$$\mathrm{Prd}_{A,a}(X) = \mathrm{Prd}_{C,a^2}(X^2)\,.$$

We conclude that $\chi_{C,a^2}(X^2) = \chi_{A,a}(X) \in F[X^2]$. □

Back in the more general situation where K is a neat quadratic F-algebra, but not necessarily a field, we conclude the following.

6.4. **Corollary.** *For $a \in C' \cap \mathrm{Sym}(\sigma)$ we have $\chi_a(X) \in F[X^2]$.*

Proof. If $K \simeq F \times F$ then the statement follows from Proposition 2.4. Otherwise K is a field, so that the statement follows from Proposition 6.3. □

6.5. **Proposition.** *Assume that* $\mathrm{cap}(A,\sigma) = 2$. *Then*

$$\mathrm{Sym}^*(\sigma) = K \oplus (C' \cap \mathrm{Sym}(\sigma))$$

and this decomposition is orthogonal for the quadratic form $c_2 : \mathrm{Sym}^*(\sigma) \to F$. Furthermore $c_2|_K : K \to F$ is the norm form of K and $c_2(x) = -x^2 \in F$ for all $x \in C' \cap \mathrm{Sym}(\sigma)$.

Proof. Set $V = \mathrm{Sym}^*(\sigma)$ and $W = C' \cap \mathrm{Sym}(\sigma)$. It follows from Proposition 6.1 and by comparing dimensions that $V = K \oplus W$. Writing $\overline{x} = c_1(x) - x$ for $x \in V$ defines an F-linear map $V \to F, x \mapsto \overline{x}$. By Proposition 4.6 we have $c_2(x) = x\overline{x}$ for any $x \in V$.

For $x \in F$ we have $\chi_x = (X - x)^2$, whereby $c_1(x) = 2x$ and $c_2(x) = x^2$. For $x \in V \setminus F$ we have that χ_x is the minimal polynomial of x over F. From this we conclude that $\overline{x} = \gamma(x)$ for $x \in K$ and that $c_2|_K$ is the norm form of K.

For $w \in W$ we have $w^2 \in C \cap \mathrm{Symd}(\sigma) \cap C_A(w) = F$, whence $\chi_w = X^2 - w^2$ and $w + \overline{w} = c_1(w) = 0$. For $v \in K$ and $w \in W$, using that $vw = w\gamma(v) = w\overline{v}$ and $w + \overline{w} = 0$ we obtain that

$$c_2(v + w) - c_2(v) - c_2(w) = v\overline{w} + w\overline{v} = v(w + \overline{w}) = 0\,.$$

This shows that K is orthogonal to W with respect to c_2 and that $\overline{x} = -x$ and $c_2(x) = -x^2$ for $x \in W$. □

6.6. **Corollary.** *If* $\mathrm{cap}(A, \sigma) = 2$*, then* K *is contained in a* σ*-stable quaternion* F*-subalgebra of* A*.*

Proof. Let $W = C' \cap \mathrm{Sym}(\sigma)$. It follows from Proposition 4.6 and Proposition 6.5 that the quadratic form $c_2|_W : W \to F, x \mapsto -x^2$ is nondegenerate. As $W \neq \{0\}$ it follows that there exists $x \in W$ with $x^2 \in F^\times$. Since $Kx \subseteq C'$ we conclude that $K \oplus Kx$ is a σ-stable quaternion F-subalgebra. □

For $a \in C' \cap \mathrm{Sym}(\sigma)$, by Corollary 6.4 there is a unique polynomial $f \in F[X]$ with $\chi_a(X) = f(X^2)$, and we call the element *a square separable* if f is separable.

6.7. **Proposition.** *Assume that* F *is algebraically closed. In* A *the set*

$$\{a \in C' \cap \mathrm{Sym}(\sigma) \mid a \text{ is square separable}\} \cap A^\times$$

is open in $C' \cap \mathrm{Sym}(\sigma)$ *with respect to the Zariski topology.*

Proof. A polynomial in $F[X]$ is inseparable if and only if its discriminant vanishes. Hence, for $a \in C' \cap \mathrm{Sym}(\sigma)$ being square separable is characterised by the nonvanishing of a polynomial in the coefficients of $\chi_a(X)$, which in turn are polynomials in the coefficients of a with respect to any fixed F-basis of $C' \cap \mathrm{Sym}(\sigma)$. Therefore in $C' \cap \mathrm{Sym}(\sigma)$ the square separable elements form an open subset with respect to the Zariski topology. On the other hand, in A the invertible elements are characterised by the nonvanishing of the reduced norm, whereby $A^\times$ is open in A. The statement follows from these two observations by basic topology. □

6.8. **Proposition.** *If* $|F| > \frac{1}{2}\mathrm{cap}(A, \sigma)$ *then* $C' \cap \mathrm{Sym}(\sigma) \cap A^\times$ *contains a square separable element.*

Proof. Suppose first that F is finite or algebraically closed. Then (A, σ) is split. Set $r = \frac{1}{2}\mathrm{cap}(A, \sigma)$. If K is a field then (C, σ_C) is a split K-algebra with involution of the same type as (A, σ) and with $\mathrm{cap}(C, \sigma_C) = r$, so that by Corollary 5.7 there exists a split neat K-subalgebra L of (C, σ_C) with $[L : K] = r$. If $K \simeq F \times F$ then by Corollary 5.8 K is contained in a split neat F-subalgebra L of (A, σ) with $[L : F] = 2r$. In either of these two cases we have that $L \simeq K^r$ as F-algebras. Let $e_1, \ldots, e_r \in L$ be the corresponding idempotents in L satisfying $K \simeq Ke_i$ for $i = 1, \ldots, r$. If $K \simeq F \times F$, then we fix a primitive idempotent $f \in K$ and

obtain that $e_1f, \dots, e_rf, e_1(1-f), \dots, e_r(1-f)$ are the primitive idempotents in L. For $i = 1, \dots, r$, we set $A_i = e_iAe_i$ and $\sigma_i = \sigma|_{A_i}$ and obtain by identifying F with $Fe_i \subseteq A_i$ that (A_i, σ_i) is a split F-algebra with involution of the same type as (A, σ) and with $\operatorname{cap}(A_i, \sigma_i) = \frac{1}{r}\operatorname{cap}(A, \sigma) = 2$.

By the hypothesis there exist pairwise distinct elements $c_1, \dots, c_r \in F^\times$. Consider $i \in \{1, \dots, r\}$. By Corollary 6.6 the neat quadratic F-subalgebra Ke_i of A_i is contained in a σ_i-stable quaternion F-subalgebra Q_i of A_i. By the assumption on F, Q_i is split, and since $Ke_i \subseteq \operatorname{Sym}(\sigma_i)$ we have that σ_i is orthogonal. It follows that there exists $g_i \in Q_i \cap \operatorname{Sym}(\sigma_i)$ with $g_i^2 = e_ic_i$ and such that $\operatorname{Int}_{Q_i}(g_i)$ restricts to the nontrivial F-automorphism on Ke_i. Then $F[g_1, \dots, g_r]$ is a split neat F-subalgebra of (A, σ). For $g = g_1 + \dots + g_r \in C' \cap \operatorname{Sym}(\sigma)$ it easily follows that $\operatorname{Prd}_{A,a} = \prod_{i=1}^r (X^2 - c_i)$, whereby g is invertible and square separable.

We turn to the general case, where we may assume that F is an infinite field. We choose an algebraic closure $\overline{F}$ of F. By the above the set of square separable invertible elements of $\overline{C' \cap \operatorname{Sym}(\sigma)}$ is nonempty and by Corollary 6.4 it is open in $(C' \cap \operatorname{Sym}(\sigma)) \otimes_F \overline{F}$. As $C' \cap \operatorname{Sym}(\sigma)$ is dense in $(C' \cap \operatorname{Sym}(\sigma)) \otimes_F \overline{F}$ with respect to the Zariski topology, we conclude that there exists a square separable invertible element in $C' \cap \operatorname{Sym}(\sigma)$. □

6.9. **Proposition.** *Let $a \in C' \cap \operatorname{Sym}(\sigma) \cap A^\times$ be square separable. Then $F[a^2]$ and $K[a^2]$ are neat F-subalgebras of (A, σ) such that $F[a^2]$ is F-linearly disjoint from K and $[K[a^2] : F] = [F[a] : F] = \operatorname{cap}(A, \sigma)$.*

Proof. By the hypothesis $\chi_a(X) = f(X^2)$ for a separable polynomial $f \in F[X]$. In particular $\deg f = \frac{1}{2}\deg \chi_a = \frac{1}{2}\operatorname{cap}(A, \sigma)$. As f is separable and $f(a^2) = 0$, the F-algebra $F[a^2]$ is étale and $[F[a^2] : F] = \deg f = \frac{1}{2}\operatorname{cap}(A, \sigma)$. Since $a \in C'$ we have that $a^2 \in C$, whereby $F[a^2] \subseteq C$ and $aF[a^2] \subseteq C'$, which shows that $F[a] = F[a^2] \oplus aF[a^2]$. Since $a \in A^\times$ it follows that

$$[F[a] : F] = 2 \cdot [F[a^2] : F] = \operatorname{cap}(A, \sigma)\,.$$

As $a^2 \in C$ the F-algebra $K[a^2]$ is commutative. Conjugation by a restricts to a nontrivial F-automorphism of order two on $K[a^2]$ which fixes $F[a^2]$. It follows that K is F-linearly disjoint from $F[a^2]$ and that $[K[a^2] : F[a^2]] = 2$. Hence, $[K[a^2] : F] = \operatorname{cap}(A, \sigma)$ and $K[a^2]$ is neat in (A, σ), by Proposition 5.3. Since $K[a^2]$ is free as an $F[a^2]$-module, it follows by Proposition 5.1 that $F[a^2]$ is neat in (A, σ). □

6.10. **Theorem.** *There exists a neat subalgebra L of (A, σ) that centralizes K and is F-linearly disjoint from K and such that KL is a neat subalgebra of (A, σ) with $[KL : F] = \operatorname{cap}(\sigma)$.*

Proof. Assume that (A, σ) is split. If $K \simeq F \times F$, then the statement follows immediately from Corollary 5.8. Suppose now that K is a field. Set $C = C_A(K)$ and $\sigma_C = \sigma|_C$. By Proposition 3.3 we obtain that (C, σ_C) is a split K-algebra with involution such that $\operatorname{cap}(\sigma_C) = \frac{1}{2}\operatorname{cap}(\sigma)$. It follows by Proposition 3.4 that

$\mathrm{Sym}^*(\sigma_C)$ contains a split étale K-algebra M of A such that $[M:K] = \mathrm{cap}(\sigma_C)$. By Proposition 5.3 we have that M is neat in (A,σ). Let L be the F-subalgebra of M generated by the idempotent elements in M. Then L is F-linearly disjoint from K and $KL = M$, thus $[KL:F] = [M:K]\cdot[K:F] = \mathrm{cap}(\sigma)$. Furthermore, M is free as an L-module, whence L is neat in (A,σ) by Proposition 5.1.

Hence the statement holds when A is split. In particular it holds when F is finite. Assume now that F is infinite. By Proposition 6.8 there exists an element $a \in C' \cap \mathrm{Sym}(\sigma) \cap A^\times$ which is square separable. Then Proposition 6.9 shows that $L = F[a^2]$ has the desired property. □

6.11. **Remark.** If $\mathrm{char}\, F \neq 2$ then instead of the set in Proposition 6.7 one may consider the set $\{a \in C' \cap \mathrm{Sym}(\sigma) \cap A^\times \mid \chi_a \text{ separable}\}$. To see that this set is Zariski-open in $C' \cap \mathrm{Sym}(\sigma)$ when F is algebraically closed is easier, as it does not involve Proposition 2.4, Corollary 2.5 and Proposition 6.3. Note however that this set is empty if $\mathrm{char}\, F = 2$.

7. Capacity four

In this section we consider in more detail algebras with involution of capacity four and show the existence of biquadratic neat subalgebras (Theorem 7.4). We shall in particular be interested in the case of symplectic involutions on algebras of degree eight. In this case we will conclude the existence of a triquadratic étale extension of the centre which is stable under the involution (Theorem 7.6). In particular, we obtain a new proof to Rowen's Theorem stating that every degree eight algebra of exponent two contains a triquadratic étale subalgebra (Corollary 7.7).

We need the following two preparatory results, which are well-known.

7.1. **Proposition.** *Assume that A is a central simple F-algebra. There exist $r \in \mathbb{N}$ and a sequence of separable quadratic field extensions $(F_i/F_{i-1})_{i=1}^r$ with $F_0 = F$ such that $\mathrm{ind}\, A_{F_r}$ is odd.*

Proof. Primary decomposition (cf. [8, Proposition 4.5.16]) yields that $A \simeq B \otimes C$ for two central simple F-algebras B and C such that $\deg B$ is odd and $\deg C = 2^m$ for some $m \geqslant 1$. Then C represents an element of order dividing 2^m in the Brauer group of F. By [2, Theorem] there exist $r \in \mathbb{N}$ and a sequence of separable quadratic field extensions $(F_i/F_{i-1})_{i=1}^r$ with $F_0 = F$ and such that C_{F_r} is split. (Alternatively, this can be derived from Merkurjev's Theorem [8, Theorem 1.5.8].) It follows that $\mathrm{ind}\, A_{F_r}$ divides $\deg B$. □

7.2. **Proposition** (Springer)**.** *A cubic form over F has a nontrivial zero if and only if it has a nontrivial zero in a quadratic field extension of F.*

Proof. Consider a cubic form f in n variables over F. To prove the nontrivial implication we suppose that f has a nontrivial zero in $F[X]/(p)$ for some irreducible quadratic polynomial $p \in F[X]$. Hence there exist $b_1, c_1, \ldots, b_n, c_n \in F$,

not all zero, and $h \in F[X]$ such that

$$f(b_1 + c_1X, \dots, b_n + c_nX) = p(X) \cdot h(X)\,.$$

Suppose first that $h \in F$. Comparing coefficients in degree 3 we obtain that $f(c_1, \dots, c_n) = 0$. Moreover, if $c_1 = \cdots = c_n = 0$ then we obtain further that $f(b_1, \dots, b_n) = 0$. As b_1, c_1, …, b_n, $c_n \in F$ are not all zero, it follows that f has a nontrivial zero in F.

Suppose now that $h \notin F$. As $\deg(f(b_1+c_1X, \dots, b_n+c_nX)) \leqslant \deg(f) = 3$ and $\deg(p) = [K : F] = 2$, we conclude that $\deg(h) = 1$. Hence there exists $a \in F$ such that $h(a) = 0$. Then $f(b_1 + c_1a, \dots, b_n + c_na) = 0$. Moreover, if $b_i + c_ia = 0$ for $i = 1, \dots, n$, then $0 = f(c_1(X - a), \dots, c_n(X - a)) = (X - a)^3 f(c_1, \dots, c_n)$ and thus $f(c_1, \dots, c_n) = 0$. Hence f has a nontrivial zero in F. □

Now let (A, σ) be an F-algebra with involution. Recall that for $d = \operatorname{cap}(\sigma)$ and $a \in \operatorname{Sym}^*(\sigma)$ we have $\chi_a = X^d - c_1(a)X^{d-1} + c_2X^{d-2} + \cdots + (-1)^d c_d(a) \in F[X]$.

7.3. **Lemma.** *Assume that* $\operatorname{cap}(\sigma)$ *is a multiple of* 4. *There exists* $a \in \operatorname{Sym}^*(\sigma) \setminus F$ *such that* $c_1(a) = c_3(a) = 0$.

Proof. Let $d = \operatorname{cap}(\sigma)$. We first consider the situation where $\operatorname{coind}(A)$ is even. Then by Corollary 5.7 there exists a split neat F-subalgebra L of (A, σ) with $[L : F] = 2$. If $\operatorname{char} F \neq 2$ we choose an element $a \in L \setminus F$ with $a^2 = 1$ and obtain that $\chi_a(X) = (X^2 - 1)^{d/2}$. If $\operatorname{char} F = 2$ then we choose $a \in L \setminus F$ with $a^2 = a$ and obtain that $\chi_a(X) = X^d + X^{d/2}$. In either case we have that $a \in \operatorname{Sym}^*(\sigma) \setminus F$ and $\chi_a(X) \in F[X^2]$. Hence a has the desired properties.

In the general case, by Proposition 7.1 there exists $r \in \mathbb{N}$ and a sequence of quadratic field extensions $(F_i/F_{i-1})_{i=1}^r$ with $F_0 = F$ such that $\operatorname{ind} A_{F_r}$ is odd. In particular, $\operatorname{coind} A_{F_r}$ is even.

Let $W = \ker(c_1) \subseteq \operatorname{Sym}^*(\sigma)$. If $\operatorname{char} F \neq 2$, then $F \cap W = 0$, and we consider the cubic form $f = c_3$ on W. If $\operatorname{char} F = 2$, then we have $c_3(x + a) = c_3(x)$ for every $x \in W$ and every $a \in F$, for $\chi_{x+a}(X) = \chi_x(X - a)$. In this case we consider the cubic form $f\colon W/F \to F, x + F \mapsto c_3(x)$. In each case the validity of the statement is equivalent to the existence of a nontrivial zero of the cubic form f. By the special case considered above, f has a nontrivial zero in F_r. Since f is a cubic form and F_i/F_{i-1} is a quadratic extension for $i = 1, \dots, r$, we conclude by Proposition 7.2 that f has a nontrivial zero over F. □

An étale F-algebra K is called *biquadratic* (resp. *triquadratic*) if it is isomorphic to the tensor product of two (resp. three) quadratic étale F-algebras.

The following result extends [7, Corollary 6.2 and Theorem 9.1 (1)].

7.4. **Theorem.** *Let* (A, σ) *be an* F*-algebra with involution with* $\operatorname{cap}(\sigma) = 4$. *Then* (A, σ) *contains a neat biquadratic* F*-subalgebra.*

Proof. By Theorem 6.10 it suffices to show that (A, σ) contains a quadratic neat F-subalgebra. If A has zero-divisors, then we may conclude this by applying Corollary 5.7 with $r = 2$. Hence we assume that A is a division F-algebra.

By Lemma 7.3 there exists an element $a \in \mathrm{Sym}^*(\sigma) \setminus F$ with $c_1(a) = c_3(a) = 0$, whereby $\chi_a(X) = X^4 + c_2(a)X^2 + c_4(a) \in F[X^2]$. In particular $[F(a^2) : F] \leqslant 2$. We set $E = F[a]$ if $a^2 \in F$ and $E = F[a^2]$ otherwise. Then E is a quadratic field extension of F contained in $\mathrm{Sym}(\sigma)$.

If E is separable over F, then E is a neat subalgebra of (A, σ) and we may take $K = E$. Suppose now that the quadratic extension E is inseparable. In particular $\mathrm{char}\, F = 2$. We consider $C = C_A(E)$ and write σ_C for the restriction of σ to C. If we can find $y \in \mathrm{Sym}(\sigma_C) \setminus E$ such that $y^2 + y \in E$, we obtain for $u = y^2$ that $u \in \mathrm{Sym}(\sigma_C) \setminus E \subseteq \mathrm{Sym}(\sigma) \setminus F$ and $u^2 + u = (y^2 + y)^2 \in F$, whereby $F[u]$ is a separable quadratic extension of F contained in $\mathrm{Sym}(\sigma)$, so that we may take $K = F[u]$. It therefore suffices to show the existence of such an element y.

Note that (C, σ_C) is an E-algebra with involution and $\deg(C) = \frac{1}{2}\deg(A)$. If $\mathrm{cap}(\sigma_C) = 2$, then the existence of $y \in \mathrm{Sym}(\sigma_C) \setminus E$ with $y^2 + y \in E$ follows by Theorem 4.1. The only possibility to have $\mathrm{cap}(\sigma_C) \neq 2$ is that (A, σ) is symplectic of degree 8 and (C, σ_C) is orthogonal of degree 4.

In particular, the statement holds in the case where σ is orthogonal. Applying this to (C, σ_C) when σ_C is orthogonal and $\deg(C) = 4$, we obtain a separable quadratic extension of E inside $\mathrm{Sym}(\sigma_C)$ and thus an element $y \in \mathrm{Sym}(\sigma_C) \setminus E$ with $y^2 + y \in E$, as desired. □

The proof of our next result uses a corestriction argument on central simple algebras. Consider a separable quadratic field extension K/F and a central simple K-algebra B. We refer to [9, §3.B] for the definition and the basic properties of the central simple F-algebra $\mathrm{Cor}_{K/F}(B)$, the corestriction (or norm) of B from K to F (which is denoted $N_{K/F}(B)$ in [9]).

7.5. **Lemma.** *Assume that B is a K-quaternion algebra. Then B contains a quadratic étale F-algebra linearly disjoint from K if and only if $\mathrm{Cor}_{K/F}(B)$ is not a division algebra.*

Proof. If $\mathrm{char}\, F \neq 2$, a proof is given in [9, (16.28)]. We refer to [3] for a proof in arbitrary characteristic. □

The following result extends [7, Lemma 6.1].

7.6. **Theorem.** *Assume that (A, σ) is symplectic of degree 8. Then A contains a σ-stable triquadratic étale F-subalgebra. Moreover, any neat biquadratic F-subalgebra of (A, σ) is contained in a σ-stable triquadratic étale F-subalgebra of A.*

Proof. In view of Theorem 7.4 it suffices to prove the second part of the statement. Thus let L be a neat biquadratic F-subalgebra of (A, σ).

Assume first that L is split. Let $e_1, \dots, e_4$ be the primitive idempotents of L. For $i = 1, \dots, 4$ by identifying F with Fe_i we obtain that e_iAe_i is a quaternion F-algebra Brauer equivalent to A and $\sigma|_{e_iAe_i}$ is its canonical involution. As $\deg A = 8$ and A contains a split biquadratic étale F-subalgebra, we have $\mathrm{ind}\, A \leqslant 2$. If $\mathrm{ind}\, A = 2$ then we fix $a \in F$ with $4a \neq -1$ such that $F[X]/(X^2 - X - a)$

is a splitting field of A, otherwise we set $a = 0$. In either case, we obtain for $i = 1, \dots, 4$ an element $f_i \in e_i A e_i \backslash F e_i$ with $f_i^2 = f_i + a e_i$. Then $f = f_1 + f_2 + f_3 + f_4$ is such that $f + \sigma(f) = 1$ and $f^2 = f + a$. Hence $L[f]$ is a σ-stable triquadratic F-subalgebra of A.

Assume now that L is not split. Then L contains a quadratic field extension K of F. With the notation of Section 6 we obtain an F-algebra with involution (C, σ_C). By Proposition 3.3 the involution σ_C is symplectic and $\operatorname{cap}(C, \sigma_C) = 2$. Since $[L : K] = 2 = \operatorname{cap}(C, \sigma_C)$, by Proposition 5.3 the étale K-algebra L is neat in (C, σ_C). By Corollary 6.6 it follows that L is contained in a σ_C-stable quaternion K-subalgebra Q of C. We set $Q' = C_C(Q)$ and observe that Q' is a σ_C-stable quaternion K-subalgebra of C. We set $\sigma_Q = \sigma|_Q$ and $\sigma_{Q'} = \sigma|_{Q'}$ and obtain that (Q, σ_Q) and $(Q', \sigma_{Q'})$ are quaternion K-algebras with involution such that

$$(C, \sigma_C) \simeq (Q, \sigma_Q) \otimes (Q', \sigma_{Q'}) .$$

Since $L \subseteq \operatorname{Sym}(\sigma_Q)$ it follows from Proposition 5.3 that σ_Q is orthogonal. As σ_C is symplectic, it follows by [9, (2.23)] that $\sigma_{Q'}$ is symplectic. Hence $\sigma_{Q'}$ is the canonical involution of Q'.

The central simple K-algebra C is Brauer equivalent to A_K. Since A carries an F-linear involution, $A \otimes_F A$ is split. This implies that $\operatorname{Cor}_{K/F}(C)$ is split, hence $\operatorname{Cor}_{K/F}(Q) \simeq \operatorname{Cor}_{K/F}(Q')$. Since L is biquadratic, we have $L \simeq K \otimes_F M$ for some quadratic étale F-algebra M. As $M \subseteq Q$, Lemma 7.5 shows that $\operatorname{Cor}_{K/F}(Q)$ is not a division algebra. Therefore $\operatorname{Cor}_{K/F}(Q')$ is not a division algebra. Hence, by Lemma 7.5 there exists a quadratic étale F-algebra $K' \subseteq Q'$ linearly disjoint from K. Note that K' is σ-stable, for $\sigma|_{Q'}$ is the canonical involution of Q'. Note further that $K' \subseteq Q' = C_C(Q) \subseteq C_A(L)$. Hence LK' is a σ-stable triquadratic étale F-subalgebra of A. □

It is known that every central division algebra of exponent two and degree at most eight has a maximal subfield that is a separable multiquadratic extension of the centre. This was shown by Albert [1, Theorem 11.9] for degree four and by Rowen [13, Theorem 1] for degree eight. We obtain a new proof of this statement.

7.7. **Corollary** (Albert, Rowen)**.** *Let A be a central simple F-algebra such that* $\deg(A)$ *divides* 8 *and $A \otimes_F A$ is split. Then A contains a maximal commutative subalgebra that is an étale multiquadratic F-algebra.*

Proof. Let $n \in \mathbb{N}$ be such that $\deg(A) = 2^n$. If $n \leqslant 1$ then the statement is obvious. If $n = 2$ then we choose an orthogonal involution σ on A and conclude by Theorem 7.4. If $n = 3$ then we choose a symplectic involution σ on A and apply Theorem 7.6. □

Acknowledgments. It is a pleasure to thank Holger Petersson for his comments on Jordan algebraic aspects.

This work was supported by the FWO Odysseus Programme (project *Explicit Methods in Quadratic Form Theory*), funded by the Fonds Wetenschappelijk

Onderzoek – Vlaanderen. The third author acknowledges support from the Fonds de la Recherche Scientifique–FNRS under grant n° J.0014.15. Work on this paper was initiated in 2011 while the first and the third author where, respectively, Fellow and Senior Fellow of the Zukunftskolleg, whose hospitality is gratefully acknowledged.

References

[1] A.A. Albert, Structure of Algebras. AMS Coll. Pub. 24, Providence, RI, 1961.
[2] K.J. Becher. Splitting fields of central simple algebras of exponent two. *J. Pure Appl. Algebra* **220** (2016): 3450–3453.
[3] K.J. Becher, N. Grenier-Boley, J.-P. Tignol. Transfer of quadratic forms and of quaternion algebras over quadratic field extensions *Preprint arXiv 1610.06096* (2016).
[4] K.J. Becher, N. Grenier-Boley, J.-P. Tignol. Involutions with Pfister forms characterizing decomposability, in preparation.
[5] N. Bourbaki. *Algèbre, Chapitres 4–7*. Springer-Verlag, Berlin-Heidelberg, 2007.
[6] R. Elman, N. Karpenko, A. Merkurjev. *The algebraic and geometric theory of quadratic forms*. American Mathematical Society Colloquium Publications, **56**, Amer. Math. Soc., Providence, RI, 2008.
[7] S. Garibaldi, R. Parimala, J.-P. Tignol. Discriminant of symplectic involutions. *Pure Appl. Math. Q.* **5** (2009): 349–374.
[8] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*. Cambridge University Press, 2006.
[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] K. McCrimmon, *A taste of Jordan algebras*, Universitext, Springer, New York, 2004.
[11] R. Pierce. *Associative Algebras*. Graduate texts in mathematics. Springer-Verlag, 1982.
[12] I. Reiner. *Maximal orders*. London Mathematical Society Monographs **5**. Academic Press, London–New York, 1975.
[13] L.H. Rowen. Division algebras of exponent 2 and characteristic 2, *J. Algebra* **90** (1984): 71–83.

Universität Konstanz, Zukunftskolleg/FB Mathematik und Statistik, D-78457 Konstanz, Germany.

Universiteit Antwerpen, Departement Wiskunde en Informatica, Middelheimlaan 1, B-2020 Antwerpen, Belgium
E-mail address: KarimJohannes.Becher@uantwerpen.be

Université de Rouen Normandie, Laboratoire de Didactique André Revuz (LDAR-EA 4434), F-76130 Mont-Saint-Aignan, France.
E-mail address: nicolas.grenier-boley@univ-rouen.fr

Université catholique de Louvain, ICTEAM Institute, Avenue G. Lemaître 4, Box L4.05.01, B-1348 Louvain-La-Neuve, Belgium.
E-mail address: jean-pierre.tignol@uclouvain.be