16-DIMENSIONAL ALGEBRAS WITH INVOLUTION

Adrian R. Wadsworth

June 1990

These notes gives a simplified account of some of the very nice results in [KPS] — simplified because we consider algebras over a field instead of Azumaya algebras over an arbitrary commutative ring.

Let F be a field, and let E be a central simple F-algebra, with $\dim_F E = n^2$. Until further notice, we assume $\mathrm{char}(F) \neq 2$. Set E° = group of units of E, and likewise $F^\circ = F \setminus \{0\}$. Let $*\colon E \to E$, $a \mapsto a^*$ be an involution. All the involutions we work with are assumed to be of the first kind (i.e., $\alpha^* = \alpha$ for all $\alpha \in F$). A good reference for the basic facts on central simple algebras with involution is Scharlau's book [S]. Given the involution $*$ on E, we write $S_* = \{s \in E \mid s^* = s\}$ and $A_* = \{a \in E \mid a^* = -a\}$. So, $E = S_* \oplus A_*$ as F-vector spaces (as $\mathrm{char}(F) \neq 2$). If $*$ is of orthogonal type, then $\dim_F S_* = \frac{n(n+1)}{2}$ and $\dim_F A_* = \frac{n(n-1)}{2}$, while if $*$ is of symplectic type, then $\dim_F S_* = \frac{n(n-1)}{2}$ and $\dim_F A_* = \frac{n(n+1)}{2}$.

Now let us fix two quaternion algebra $Q_i = \left(\frac{\alpha_i, \beta_i}{F}\right)$ over F, $i = 1, 2$. So, Q_1 has its standard base $1, i_1, j_1, k_1$ satisfying

$$i_1^2 = \alpha_1,\ j_1^2 = A_1,\ k_1 = i_1 j_1 = -j_1 i_1, \quad \text{with} \quad \alpha_1, \beta_1 \in F^\circ .$$

Let $-_1$ be the standard involution on Q_1 (given by $1 \mapsto 1$, $i_1 \mapsto -i_1$, $j_1 \mapsto -j_1$), $k_1 \mapsto -k_1$) which is the unique involution of symplectic type on Q_1. Then $A_{-_1} = F$-span $\{i_1, j_1, k_1\}$, the "pure part" of Q_1. Likewise, by replacing the subscript 1 by 2, we have corresponding objects for Q_2.

Let $E = Q_1 \otimes_F Q_2$. We will be looking at structures associated with orthogonal type involutions on E. The basic such involution, which we'll work from, is chosen to be $-_1 \otimes -_2$, call this $-$ (so $\overline{a \otimes b} = a^{-_1} \otimes b^{-_2}$). Set $A = A_-$ and $S = S_-$. Clearly $A = A_{-1} \oplus A_{-_2} = F$-span $\{i_1, j_1, k_1, i_2, j_2 k_2\}$ (we are identifying elements of the Q_i with their images in E) and $S = F \cdot 1 \oplus A_{-_1} \otimes A_{-_2}$ ($\dim S = 10$). Define $V_1 = F$-span $\{i_1, j_1, k_1\} \subseteq E$ and $V_2 = F$-span $\{i_2, j_2, k_2\}$, so that $A = V_1 \oplus V_2$.

Lemma 1. *For any $a = v_1 + v_2 \in A$ with $v_i \in V_i$, we have $v_i^2 \in F$ and*

$$\mathrm{Nrd}(a) = (v_1^2 - v_2^2)^2 \in F^2 .$$

Retypeset February 1995.

Proof. Since $v_1 \in A_{-_1} \subseteq Q_1$, $v_1^2 = -\mathrm{Nrd}_{Q_1}(v_1) \in F$; likewise $v_2^2 \in F$. Let K be the F-subalgebra of E generated by v_1 and v_2. Assume, for simplicity, that $v_1 \neq 0$, $v_2 \neq 0$. Since $v_1 v_2 = v_2 v_1$ and $v_1^2, v_2^2 \in F$, it is easy to see that $K = F$-span $\{1, v_1, v_2, v_1 v_2\}$, $\dim_F K = 4$, and K is a commutative Galois extension of F. The Galois group of K over F is evidently $\mathbb{Z}_2 \times \mathbb{Z}_2$ with generators $-_1 \otimes id$ and $id \otimes -_2$ restricted to K. The orbit of a under the Galois action is $\{v_1 + v_2, v_1 - v_2, -v_1 + v_2, -v_1 - v_2\}$. The reduced norm of E on K is just the norm from K to F, so

$$\mathrm{Nrd}(a) = N_{K/F}(a) = (v_1 + v_2)(v_1 - v_2)(-v_1 + v_2)(-v_1 - v_2) = (v_1^2 - v_2^2)^2 \in F^2 .$$

(This computation is valid even if K is not a field, since it is still a maximal separable subalgebra of E.) It's easy to check that the formula for $\mathrm{Nrd}(a)$ is still valid if $v_1 = 0$ or $v_2 = 0$. $\square$

Define an F-linear function $p\colon A \to A$ by $p(v_1 + v_2) = v_1 - v_2$ for $v_i \in V_i$. Clearly for $a = v_1 + v_2 \in A$, $ap(a) = p(a)a = v_1^2 - v_2^2 \in F$ (as v_1 and v_2 commute). So, setting $q(a) = ap(a)$, we have a quadratic form $q : A \to F$. Since we just showed $\mathrm{Nrd}(a) = q(a)^2$, $q(a)$ is called in[KPS] the *Pfaffian* of a, and $p(a)$ is called the *Pfaffian adjoint* of a. Note that, relative to the orthogonal base $\{i_1, j_1, k_1, i_2, j_2, k_2\}$, q is the diagonal quadratic form $\langle \alpha_1, \beta_1, -\alpha_1\beta_1, -\alpha_2, -\beta_2, \alpha_2\beta_2 \rangle$ which, up to sign, is the "Albert form" of $Q_1 \otimes_F Q_2$ (so called because Albert proved that E is a division algebra if and only if this form is anisotropic). It is important to know that the function p is unique up to scalar multiple:

Lemma 2. (cf. [KPS, Prop. 3.1]) *If $p'\colon A \to A$ is an F-linear function such that $ap'(a) \in F$ for all $a \in A$ (or $p'(a)a \in F$, all $a \in A$), then $p' = \lambda p$ for some $\lambda \in F$.*

Proof. (For simplicity we'll assume $|F| > 3$; the result is easily checked also when $|F| = 3$.) Take any $v_i \in V_i$ with $v_i^2 \neq 0$, $i = 1, 2$. Then $p'(v_i) \in F v_i^{-1} = F p(v_i)$; so $p'(v_i) = \lambda_i p(v_i)$ for some $\lambda_i \in F$. Since $|F| > 3$ there exists $\mu \in F^\circ$ with $(\mu v_2)^2 \neq v_1^2$. Then $v_1 + \mu v_2 \in E^\circ$ since by Lemma 1, $\mathrm{Nrd}(v_1 + \mu v_2) = (v_1^2 - (\mu v_2)^2)^2 \in F^\circ$. Hence, as with the v_i, $p'(v_1 + \mu v_2) = \delta p(v_1 + \mu v_2)$ for some $\delta \in F$. That is, $\lambda_1 p(v_1) + \mu\lambda_2 p(v_2) = \delta p(v_1) + \delta\mu p(v_2)$. Since $p(v_1)$ $(\in V_1)$ and $p(v_2)$ $(\in V_2)$ are linearly independent over F, $\lambda_1 = \delta$ and $\mu\lambda_2 = \mu\delta$, so $\lambda_2 = \delta = \lambda_1$, as $\mu \neq 0$. Since V_1 and V_2 each have a base consisting of units, this shows p' of each base vector is the same scalar multiple (say λ) of p of that vector. So $p' = \lambda p$. $\square$

Lemma 3. *For every $c \in E$ and $a \in A$,* $q(ca\bar{c}) = \mathrm{Nrd}(c)q(a)$.

Proof. (Note that $ca\bar{c} \in A$, as $a \in A$.) We have, by Lemma 1, $q(ca\bar{c})^2 = \mathrm{Nrd}(ca\bar{c}) = \mathrm{Nrd}(c)^2\mathrm{Nrd}(a) = (\mathrm{Nrd}(c)q(a))^2$. So $q(ca\bar{c}) = \pm\mathrm{Nrd}(c)q(a)$. To see that the sign is always $+$, we use a homotopy argument. We may assume $a \in E^\circ$, since otherwise $q(a) = 0$. Let $d = cx + (1-x) \in E(x) = E \otimes_F F(x)$ where x is an indeterminate. The function $q\colon A \to F$ induces by scalar extension $q' : A \otimes_F F(x) \to F(x)$, where $A \otimes_F F(x) = A_{-'}$, where $-' = - \otimes id$ is the extension of $-$ to $E(x)$. The observations just made for q apply likewise to q', showing $q'(da\bar{d}')^2 = (\mathrm{Nrd}(d)q(a))^2$. This is an equation in $F[x]$; so, for $\varepsilon = \pm 1$, $q'(da\bar{d}') = \varepsilon\mathrm{Nrd}(d)q(a)$. By specializing $x \to 0$ we find $d \to 1$, so $q(a) = \varepsilon\mathrm{Nrd}(1)q(a)$; hence, $\varepsilon = 1$ as $q(a) \in F^\circ$. Now by specializing $x \to 1$, as $d \to c$ we obtain $q(ca\bar{c}) = \varepsilon\mathrm{Nrd}(c)q(a) = \mathrm{Nrd}(c)q(a)$. $\square$

Now suppose $*$ is any involution of orthogonal type on E. By Skolem-Noether there is $s \in E^\circ$ with $r^* = s\bar{r}s^{-1}$ for all $r \in E$. Fix this s, (s is uniquely determined up to a scalar multiple by $*$.) Since $*$ is an involution, $s \in S \cup A$, and since $*$ has orthogonal type, $s \in S$. For any $r \in E$, we have $(sr)^* = s(\bar{r}\bar{s})s^{-1} = s\bar{r}$; likewise $(rs^{-1})^* = \bar{r}s^{-1}$. Thus, for the skew-symmetric set with respect to $*$, A_*, we have

$$A_* = sA = As^{-1}\,.$$

We use the functions p and q on A to define analogous functions $p_* \colon A_* \to A_*$ which is F-linear and $q_* : A_* \to F$, which is a quadratic form, as follows: for $b \in A_*$ (so $bs \in A$) set

$$p_*(b) = sp(bs) \quad \text{and} \quad q_*(b) = bp_*(b) = q(bs)\,.$$

From the properties of p we obtain corresponding properties of p_*, i.e., p_* is an F-linear isomorphism of A_*; for all $b \in A_*$, $bp_*(b) = p_*(b)b = q_*(b) \in F$; and p_* is uniquely determined up to a scalar multiple in the same way that p is in Lemma 2. (For, given a p'_* on A_*, we obtain p' on A by $p'(a) = s^{-1}p'_*(as^{-1})$.) Note that the map $b \to bs$ is an isometry between the quadratic form q_* on A_* and q on A. So, q_* is also the Albert form for $Q_1 \otimes_F Q_2$. Observe that for all $b \in A_*$,

$$\begin{aligned} \mathrm{Nrd}(b) &= \mathrm{Nrd}(bs)\mathrm{Nrd}(s^{-1}) = q(bs)^2\mathrm{Nrd}(s^{-1}) \\ &= q_*(b)^2\mathrm{Nrd}(s^{-1})\,. \end{aligned} \tag{1}$$

Thus, for every unit $b \in A_*$, $\mathrm{Nrd}(b)$ maps to the same coset in $F^\circ/F^{\circ 2}$, namely $\mathrm{Nrd}(s)F^{\circ 2}$. Thus, $\mathrm{Nrd}(s)F^{\circ 2}$ is an invariant of $*$ (independent of the choice of s to describe $*$, and also independent of the initial choice of involution $-$ on E). This square class $\mathrm{Nrd}(s)F^{\circ 2}$ is called the *Pfaffian discriminant* of the involution $*$, written *pfd* $(*)$.

Lemma 4. *For all $b \in A_*$, $p_*(p_*(b)) = \mathrm{Nrd}(s) \cdot b$.*

Proof. We compute

$$\begin{aligned} p_*(p_*(b)) \cdot p_*(b) &= q_*(p_*(b)) = q(p_*(b)s) = q(sp(bs)s) \\ &= \mathrm{Nrd}(s)q(p(bs)) \qquad \text{(by Lemma 3)} \\ &= \mathrm{Nrd}(s)bsp(bs) = \mathrm{Nrd}(s)b \cdot p_*(b)\,. \end{aligned}$$

Whenever b is a unit, so is $p_*(b)$, and we can cancel $p_*(b)$ in the formula above to obtain the desired equality. Because A_* is spanned by units and $p_* \circ p_*$ is F-linear, the equality holds for all $b \in A_*$. $\square$

Lemma 5. *Suppose $*_i$ is an involution of orthogonal type on Q_i and $* = *_1 \otimes *_2$. Then* *pfd* $(*) = 1 \cdot F^{\circ 2}$.

Proof. Since $*_i$ is of orthogonal type there is a unit $t_i \in A_{-_i}$ (the pure part of Q_i) such that $r^{*_i} = t_i r^{-_i} t_i^{-i}$ for all $r \in Q_i$. Then conjugation by $s = t_1 \otimes t_2$ induces $* = *_1 \otimes *_2$ from $- = -_1 \otimes -_2$. Let $K = F(t_1 \otimes 1, 1 \otimes t_2)$, a 4-dimensional commutative Galois extension of F in E. As in the proof of Lemma 1,

$$\mathrm{Nrd}(s) = N_{K/F}(s) = (t_1 \otimes t_2)(-t_1 \otimes t_2)(t_1 \otimes -t_2)(-t_1 \otimes -t_2) = t_1^4 \otimes t_2^4 = (t_1^2 \cdot t_2^2)^2 \in F^{\circ 2}\,.$$

Hence, *pfd* $(*) = 1 \cdot F^{\circ 2}$. $\square$

Theorem 1. (cf. [KPS, Cor. 5.5]) *For the orthogonal type involution $*$ on E, the following are equivalent:*

(i) *There is an F-central quaternion algebra Q in E with $Q^* = Q$.*

(ii) *There are F-central quaternion subalgebras Q_1' and Q_2' of E with $Q_i'^* = Q_i$, $i = 1, 2$, and $E = Q_1' \otimes_F Q_2'$.*

(iii) *$pfd\,(*) = 1 \cdot F^{\circ 2}$ (i.e., $\mathrm{Nrd}(s) \in F^{\circ 2}$).*

Proof. (i) $\Rightarrow$ (ii) This is immediate from the double centralizer theorem.

(ii) $\Rightarrow$ (i) Clear.

(ii) $\Rightarrow$ (iii) Let $*_i$ be the restriction of $*$ to Q_i', $i = 1, 2$. Since $* = *_1 \otimes *_2$ and $*$ has orthogonal type, $*_1$ and $*_2$ must be of the same type. If the $*_i$ are of symplectic type, then $*_i$ is the standard involution on Q_i'; then as $* = *_1 \otimes *_2$, Lemma 1 applied to $(E, *)$ instead of $(E, -)$ shows $\mathrm{Nrd}(b) \in F^2$ for all $b \in A_*$. Hence, $pfd\,(*) = 1 \cdot F^{\circ 2}$. If the $*_i$ are of orthogonal type Lemma 5 applied with respect to the decomposition $E = Q_1' \otimes_F Q_2'$ (instead of $Q_1 \otimes_F Q_2$) shows again $\mathrm{Nrd}(b) \in F^2$ for all $b \in A_*$; hence again $pfd\,(*) = 1 \cdot F^{\circ 2}$.

(iii) $\Rightarrow$ (ii) Suppose $pfd\,(*) = 1 \cdot F^{\circ 2}$. Then $\mathrm{Nrd}(s) = \lambda^2$ for some $\lambda \in F^\circ$. By Lemma 4, $p_* \circ p_* = \lambda^2 \cdot id$. Hence, the only possible eigenvalues of p_* are λ and $-\lambda$. Let $Y_{\varepsilon\lambda} = \{b \in A_* \mid p_*(b) = \varepsilon\lambda b\}$ for $\varepsilon = \pm 1$. Since p_* is a diagonalizable linear transformation (as its minimal polynomial, dividing $x^2 - \lambda^2$, has no repeated roots) $A_* = Y_\lambda \oplus Y_{-\lambda}$. Let $Q_1' = F \cdot 1 \oplus Y_\lambda$ and $Q_2' = F \cdot 1 \oplus Y_{-\lambda}$. Clearly $Q_i'^* = Q_i'$, $i = 1, 2$.

It remains to show that the Q_i are quaternion algebras over F which centralize each other. For this we use the quadratic form $q_*(b) = bp_*(b) = p_*(b)b$. (For the last equality note that as $q_*(b) \in F$, $q_*(b) = sq_*(b)s^{-1} = s[q(bs)]s^{-1} = s[p(bs)bs]s^{-1} = sp(bs)b = p_*(b)b$. The associated bilinear form B_* for q_* is given by $B_*(b, d) = \frac{1}{2}[q_*(b + d) - q_*(b) - q_*(d)]$, so

$$B_*(b, d) = \frac{1}{2}[bp_*(d) + dp_*(b)] = \frac{1}{2}[p_*(b)d + p_*(d)b]\,. \tag{2}$$

If $b \in Y_\lambda$ and $d \in Y_{-\lambda}$, this yields $B_*(b, d) = \frac{\lambda}{2}[-bd + db] = \frac{\lambda}{2}[bd - db]$; since $B_*(b, d) = -B_*(b, d)$, this yields $B_*(b, d) = 0$ and $bd = db$. So, $Y_{-\lambda}$ centralizes Y_λ and $Y_\lambda \perp Y_{-\lambda}$ with respect to q_*.

Because $\dim Y_\lambda + \dim Y_{-\lambda} = 6$, we may assume $\dim Y_\lambda \geq 3$. (Otherwise, interchange λ and $-\lambda$.) Since q_* is a nondegenerate quadratic form on A_* (as q is nondegenerate on A) and $Y_\lambda \perp Y_{-\lambda}$, q_* must be nondegenerate on Y_λ and on $Y_{-\lambda}$. Therefore, we can choose two specific elements b, $c \in Y_\lambda$ with $q_*(b) \neq 0$, $q_*(c) \neq 0$ (i.e., b and c are units) and $B_*(b, c) = 0$ (i.e., from (2), $bc = -cb$). We have $b^2 = \lambda^{-1}bp_*(b) = \lambda^{-1}q_*(b) \in F^\circ$ and likewise $c^2 \in F^\circ$. So, $F(b, c)$ is a quaternion algebra over F. Now, $(bc)^* = c^*b^* = (-c)(-b) = cb = -bc$; so $bc \in A_*$. Further, as $bcp_*(bc) = q_*(bc) \in F$ and $bcbc = -b^2c^2 \in F^\circ$, we see $p_*(bc) = \mu bc$ for $\mu \in F$. That is, bc is an eigenvector for p_*. But $bc \notin Y_{-\lambda}$ since bc anticommutes with b, while elements of $Y_{-\lambda}$ commute with those of Y_λ. So, $bc \in Y_\lambda$. Hence, the 3-dimensional space F-span $\{b, c, bc\}$ lies in Y_λ. Since $q_*|_{Y_\lambda}$ is nondegenerate, if $\dim Y_\lambda > 3$ we could find $y \in Y_\lambda$ with $q_*(y) \neq 0$ and $0 = B_*(b, y) = B_*(c, y) = B_*(bc, y)$. By (2) this implies y anticommutes with $b, c,$ *and* bc, forcing $y = 0$, which contradicts $q_*(y) \neq 0$. Thus, $Y_\lambda = F$-span $\{b, c, bc\}$, $\dim Y_\lambda = 3$, and $F(b, c) = Q_1'$, showing Q_1' is indeed a quaternion algebra. Since $\dim Y_{-\lambda} = 6 - \dim Y_\lambda = 3$, the same argument shows Q_2' is also a quaternion algebra. Since $Y_{-\lambda}$ centralizes Y_λ, Q_2' centralizes Q_1', completing the proof. $\square$

Remark. There is another way to prove that the Q_i' in (iii) $\Rightarrow$ (ii) are quaternion algebras centralizing each other. Suppose first that $*$ and $-$ are isomorphic involutions on E, i.e., suppose there is an F-algebra isomorphism $f: E \to E$ such that $f(\mu^*) = \overline{f(\mu)}$, for all $r \in E$. Then $f(A_*) = A$; let $p' = f \circ p_* \circ f^{-1}: A \to A$. Because $bp_*(b) \in F$ for all $b \in A_*$, $ap'(a) \in F$ for all $a \in A$. By Lemma 2, $p' = \mu \cdot p$ for some $\mu \in F$. In fact, $\mu^2 = \lambda^2$ since $p' \circ p' = \lambda^2 \cdot id$ (as $p_* \circ p_* = \lambda^2 id$) while $p \circ p = id$. So, we may assume $\mu = \lambda$. Then λ-eigenspace of $p' =$ 1-eigenspace of $p = F$-span $\{i_1, j_1, k_1\}$. So, $f^{-1}(Q_1) = f^{-1}(F \cdot 1 \oplus \lambda$-eigenspace of $p') = F \cdot 1 + \lambda$-eigenspace of $p_* = Q_1'$. Because f is an algebra isomorphism, it follows that Q_1' is a quaternion algebra over F. Likewise, $Q_2' = f^{-1}(Q_2)$ is a quaternion algebra, and Q_2' centralizes Q_1' since Q_2 centralizes Q_1.

This completes the argument in case $(E, *) \cong (E, -)$. The condition for $(E, *) \cong (E, -)$ is easily checked to be that there exists $y \in E^\circ$ with $ys\bar{y} \in F^\circ$ (cf. [S, Th. 7.4(iv), p. 302]). While this need not hold, it will hold after extending scalars to the separable closure of F.* Hence, there is a finite degree Galois extension K of F such that $(E \otimes_F K, * \otimes id) \cong (E \otimes_F K, - \otimes id)$. The argument just given, applied to $E \otimes_F K$, shows that $Q_1' \otimes_F K$ and $Q_2' \otimes_F K$ are quaternion algebras over K centralizing each other. Since Q_1' is the set of fixed elements of Q_1' under the action of the Galois group $\mathcal{G}(K/F)$ ($\sigma \in \mathcal{G}(K/F)$ acts via $id \otimes \sigma: Q_1' \otimes_F K \to Q_1' \otimes_F K$, a ring automorphism), Q_1' is closed under multiplication. The ring Q_1' is a 4-dimensional central simple F-algebra since $Q_1' \otimes_F K$ is a 4-dimensional central simple K-algebra. So Q_1' is a quaternion algebra over F, as likewise is Q_2'; finally, Q_2' centralizes Q_1' since $Q_2' \otimes_F K$ centralizes $Q_1' \otimes_F K$.

By an old theorem of Albert, every 16-dimensional central simple F-algebra E with involution is a tensor product of quaternion algebras. The first example of such an E with an involution $*$ which does not admit a $*$-*compatible* decomposition into quaternion algebras (in the sense of (ii) of Theorem 1) was given in [ART]. Theorem 1 shows that "almost every" E has an involution which does not admit a compatible quaternionic decomposition. It suffices to find a symmetric element s with respect to any orthogonal type involution on E such that $\mathrm{Nrd}(s) \notin F^2$. In fact, the unusual case is to have an E such that *every* orthogonal type involution admits a compatible quaternionic decomposition. Of course this occurs if F is quadratically closed ($F = F^2$); but then, $E \cong M_4(F)$. Here is an example of such an E which is a division algebra.

Example. Let F be a field with Henselian valuation v, with residue field $\bar{F}$, $\mathrm{char}(\bar{F}) \neq 2$, and let E be a 16-dimensional F-central division algebra with involution. Suppose E is totally ramified over F with respect to the unique extension of v to a valuation of E. Then $\mathrm{Nrd}(r) \in F^2$ for each $r \in E$. Hence, every orthogonal type involution on E admits a compatible quaternionic decomposition. (For an explicit example of this, let F_0 be any field ($\mathrm{char} F_0 \neq 2$), let F be the iterated Laurent power series field $F = F_0((x_1))((x_2))((x_3))((x_4))$, and let $E = \left(\frac{x_1, x_2}{F}\right) \otimes_F \left(\frac{x_3, x_4}{F}\right)$.)

Proof. See [TW] for more on totally ramified valuations. In particular, if Γ_E (resp. Γ_F) is

*Suppose L is a separably closed field and $*$ is any orthogonal type involution on the matrix algebra $M_4(L)$. Since $*$ is of the same type as the transposed involution t there is a $z \in M_4(L)^\circ$ with $z^t = z$ and $r^* = zr^tz^{-1}$ for all $\mu \in M_4(L)$. The condition for $(M_4(L), *) \cong (M_4(L), t)$ is that for some unity y, $y = y^t =$ some $\delta \in L$. That is, the symmetric bilinear form associated to z is isometric to the diagonal form $\langle \delta, \delta, \ldots, \delta \rangle$. By Gram-Schmidt, the form is diagonalizable; as L is separably closed, it can be diagonalized to $\langle 1, 1, \ldots, 1 \rangle$. So, $(M_4(L), *) \cong (M_4(L), t)$.

the value group of the valuation on E (resp. F), then the order of E in the Brauer group of F equals the exponent of the factor group Γ_E/Γ_F. Hence, for $r \in E$, $v(r^2) = 2v(a) \in \Gamma_F$. So, $r^2 = a\lambda$ with $\lambda \in F$ and $u \in E$ with $v(u) = 0$. E has the same residue field as F since E is totally ramified over F; so, we may modify λ and u so that the residue of u is 1. Write $u = 1+m$ with $v(m) > 0$. Because the valuation on the field $F(r)$ extending v on F is Henselian, $1+m \in F(r)^2$, say $1+m = (1+n)^2$ with $n \in F(r)$ and $v(n) > 0$. So, $r = cd$ where $c = r(1+u)^{-1}$ and $\alpha = 1+n \in F(r)$. Since $c^2 = \lambda \in F$, $\operatorname{Nrd}(c) = c^4 \in F^2$. Because the Henselian valuation v extends uniquely to $F(r)$, $N_{N(r)/F}(d) = 1 + \mu$ with $v(u) > 0$; but $1 + u \in F^2$ is v is Henselian. Since $\operatorname{Nrd}(d)$ is a power of $N_{N(r)/F}(d)$ $\operatorname{Nrd}(d) \in F^2$. Thus $\operatorname{Nrd}(r) = \operatorname{Nrd}(c)\operatorname{Nrd}(d) \in F^2$. The rest follows by Theorem 1. $\square$

So far, we have considered only orthogonal type involutions on $E = Q_1 \otimes_F Q_2$. But the approach given above can be adapted with few modifications for symplectic type involutions, as we now describe. The main point is that Theorem 1 still holds, but further, condition (iii) of the Theorem (hence also (i) and (ii)) is true for *every* symplectic type involution on E.

With $-$ still denoting our specified (orthogonal type) involution $-_1 \otimes -_2$ on $E = Q_1 \otimes_F Q_2$, let $\star$ be any symplectic type involution on E. Fix a unit $z \in A = A_-$ with $\mu^\star = z\bar{\mu}z^{-1}$ for all $r \in E$. The appropriate 6-dimensional subspace to work with here is the symmetric set $S_\star$. We have $S_\star = zA = Az^{-1}$. So we obtain $p_i\colon S_\star \to S_\star$ and $q_\star\colon S_\star \to F$ from p and q on A as before: for $b \in S_\star$, set $p_\star(b) = zp(bz)$ and $q_\star(b) = bp_\star(b) = q(bz)$. As before, $p_\star$ has the same uniqueness property as p in Lemma 2; as in (1) on p. 3, $\operatorname{Nrd}(b) = q_\star(b)^2\operatorname{Nrd}(z)^{-1}$ for all $b \in S_\star$, and the analogue to Lemma 4 holds, with the same proof. So, we again get a well-defined Pfaffian discriminant $pfd\,(\star) = \operatorname{Nrd}(z)F^{\circ 2} \in F^\circ/F^{\circ 2}$. But Lemma 1 shows $\operatorname{Nrd}(z) \in F^{\circ 2}$. So, $pfd\,(\star) = 1{\cdot}F^{\circ 2}$ for every symplectic type involution on E.

In proving Theorem 1 for the symplectic $\star$, (ii) $\Rightarrow$ (iii) is trivial since we have just seen that (iii) alway holds. For (iii) $\Rightarrow$ (ii) we must change the way of getting Q_1' and Q_2' because of the different eigenspace structure of $p_\star$ (see below). We still have $p_\star^2 = \operatorname{Nrd}(z){\cdot}id = \lambda^2{\cdot}id$, so $S_\star$ has the eigenspace decomposition $S_\star = Y_\lambda \oplus Y_{-\lambda}$. The analogue to (2) on p. 4 for $B_\star$ shows that $Y_\lambda \perp Y_{-\lambda}$ with respect to $q_\star$, so $q_\star|_{Y_{\pm\lambda}}$ is nondegenerate. With λ chosen (from $\pm\lambda$) so that $\dim Y_\lambda \geq 3$, we pick b, $c \in Y_\lambda$ such that $q_\star(b), q_\star(c) \neq 0$ (so b^2, $c^2 \in F^\circ$) and $B_\star(b,c) = 0$ (so by (2) $bc = -cb$). Let $Q_1' = F(b,c)$, which is clearly a quaternion algebra over F; furthermore, ${Q_1'}^\star = Q_1'$ such that $b^\star = b$ and $c^\star = c$. Then let Q_2' be the centralizer of Q_1' in E; then Q_2' is a $\star$-invariant quaternion algebra with $E = Q_1' \otimes_F Q_2'$, as desired.

In the orthogonal case there was a canonical choice of the Q_i' for (ii) of Theorem 1 coming from the eigenspaces of p_*. But in the symplectic case there is no such canonical choice. To see why, let us make a specific choice $z = i_1$, so $r^\star = i_1\bar{r}i_1^{-1}$. Then, easy calculations show: $S_\star = F\text{-span}\ \{1, j_1, k_1, i_1i_2, i_1j_2, i_1k_2\}$, $p_\star$ has eigenvalues $\pm\alpha_1$ with eigenspaces $Y_{\alpha_1} = F\text{-span}\ \{1\}$ and $Y_{-\alpha_1} = F\text{-span}\ \{j_1, k_1, i_1i_2, i_1j_2, i_1k_2\}$. The eigenspaces have dimension 1 and 5, not 3 and 3! By a scalar extension argument like the one in the remark on p. 5, we can see that for *any* symplectic type involution $\star$ on E, $p_\star$ will have eigenspaces of dimension 1 and 5. In fact, the Pfaffian arises again for any unit z of A; if $\star$ is the symplectic type involution $r \mapsto z\bar{r}z^{-1}$, then $p_i^2 = \operatorname{Nrd}(z)\cdot id = q(z)^2\cdot id$, so the eigenvalues of p_i are $\pm q(z)$. The 1-dimensional eigenspace is that of $q(z)$, and the 5-dimensional eigenspace is that of $-q(z)$.

There is also a nice proof in [KPS] of Jacobson's theorem [J, Th. 3.12] relating 16 dimensional algebras with involution and their Albert forms, which we turn to now.

Lemma 6. (cf. [KPS, Prop. 3.3]) *With $E = Q_1 \otimes_F Q_2$ and $- = -_1 \otimes -_2$ as above, let $q(a) = ap(a) \colon A \to F$ be the Albert form (= Pfaffian form) on $A = A_-$, as above. For any $\lambda \in F^\circ$, let $C(\lambda q)$ be the Clifford algebra of λq. Then, $C(\lambda q) \cong M_2(E)$.*

Proof. Define $h \colon A \to M_2(E)$ by $a \mapsto \begin{pmatrix} 0 & a \\ \lambda p(a) & 0 \end{pmatrix}$. Then $h(a)^2 = \lambda ap(a) \cdot 1 = \lambda q(a)$. From the universal mapping property for Clifford algebras, h induces an F-algebra homomorphism $f \colon C(\lambda q) \to M_2(E)$. This f is injective, as $C(\lambda q)$ is simple, so an isomorphism by dimension count. $\square$

Theorem 2. (Jacobson) (cf. [KPS, Th. 3.4]). *Let $E = Q_1 \otimes_F Q_2$ and $\widetilde{E} = \widetilde{Q_1} \otimes_F \widetilde{Q_2}$, where $Q_1, Q_2, \widetilde{Q_1}, \widetilde{Q_2}$ are quaternion algebras over F. Then $E \cong \widetilde{E}$ if and only if the Albert forms q and $\tilde{q}$ are similar (i.e., $\tilde{q}$ is isometric to λq for some $\lambda \in F^\circ$).*

Proof. Suppose $\tilde{q}$ is isometric to λq. Then, by Lemma 6, $M_w(\widetilde{E}) \cong C(\tilde{q}) \cong C(\lambda q) \cong M_2(E)$. Hence, $\widetilde{E} \cong E$. Conversely, suppose there is an isomorphism $f : \widetilde{E} \to E$. The standard involution $\sim$ on $\widetilde{E}$ (relative to the decomposition $\widetilde{E} = \widetilde{Q_1} \otimes_F \widetilde{Q_2}$) induces an involution $*$ of orthogonal type on E, given by $r^* = f\left(\widetilde{f^{-1}(r)}\right)$. Then $f(A_\sim) = A_*$, and the Pfaffian adjoint $\tilde{p}$ on $A_\sim$ induces a function p' on A_* ($p' = f \circ \tilde{p} \circ f^{-1}$) such that $bp'(b) = bf(\tilde{q}(f^{-1}(b))) \in F$, for all $b \in A_*$. Hence, by the uniqueness Lemma 2, $p' = \lambda p_*$. Then for $s \in S_-$ such that $r^* = s\bar{r}s^{-1}$ all $r \in E$ for any $b \in A_*$, $f(\tilde{q}(f^{-1}(b))) = bp'(b) = \lambda bp_*(b) = \lambda q(bs)$. So, $a \mapsto f(a)s$ gives an isometry between $\tilde{q}$ and λq. $\square$

We turn finally to characteristic 2. In [KPS] the Pfaffian adjoint is defined for any Azumaya algebra of rank 16 with involution over any commutative ring. We show how it plays out when the ring is a field F and $\mathrm{char}(F) = 2$. Because $\mathrm{char}(F) = 2$, every involution $*$ on E is of orthogonal type in that $\dim S_* = 10$ where $S_* = \{s \in E \mid s^* = s\}$. Since $* \circ * = id$ the linear map $* \colon E \to E$ satisfies the equation $0 = x^2 - 1 = (x-1)^2$. So, 1 is the only possible eigenvalue of $*$, but $*$ is not diagonalizable since its minimal polynomial had a repeated root. So, E doesn't decompose as an orthogonal sum of eigenspaces of $*$. By dimension count (since the 1-eigenspace of $*$ has dimension 10), the Jordan canonical form of $*$ must consist of 6 2×2 blocks $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ together with 4 $|x|$ blocks (1). To get a 6-dimensional subspace, we define $A_* = \{b - b^* \mid b \in E\}$. Since rank $(id - *) = 6$ from the Jordan form, $\dim A_* = 6$. So, $A_* \subseteq S_*$, instead of A_* and S_* being complementary subspaces.

Suppose $Q = \left[\frac{\alpha,\beta}{F}\right)$ is a quaternion algebra over our char 2 field F, i.e., Q is the F-algebra with F-base $\{1, i, j, k\}$ with relations

$$i^2 + i = \alpha \in F, \quad j^2 = \beta \in F^\circ, \quad k = ij = ji + j\,.$$

Note the further relations

$$ik = ki + k \quad \text{and} \quad jk = kj + \beta \quad \text{and} \quad k^2 = \alpha\beta\,.$$

The standard involution $-$ on Q is given by $\bar{1} = 1$, $\bar{i} = i + 1$, $\bar{j} = j$, $\bar{k} = k$. So the symmetric set $S_- = F$-span $\{1, j, k\}$ while the A-set $A_- = F$-span $\{1\}$. For $x = \mu + \nu i + \sigma j + \tau k$, we have

$$\operatorname{Nrd}(x) = x\bar{x} = \bar{x}x = \mu^2 + \mu\nu + \alpha\nu^2 + \beta\sigma^2 + \beta\sigma^2 + \beta\sigma\tau + \beta\alpha\tau^2\,.$$

Thus, $\operatorname{Nrd}(x) = x^2$ whenever $x = \bar{x}$, i.e., $x \in S_- = F$-span $\{1, j, k\}$. Note also that the reduced norm quadratic form is $[1, \alpha] \perp \beta[1, \alpha]$, where $[1, \alpha]$ denotes the nondegenerate 2-dimensional quadratic form $1 \cdot \mu^2 + 1 \cdot \mu\nu + \alpha \cdot \nu^2$.

Now suppose $E = Q_1 \otimes_F Q_2$ where $Q_1 = \left[\frac{\alpha_1, \beta_1}{F}\right)$ $\left(\text{resp. } Q_2 = \left[\frac{\alpha_2, \beta_2}{F}\right)\right)$, and 1,i_1,j_1,k_1 (resp. 1,i_2,j_2,k_2) is the standard base of Q_1 (resp. Q_2) and $-_1$ (resp. $-_2$) is its standard involution. Write 1 for $1 \otimes 1$ and $i_1, \ldots, k_2$ for $i_1 \otimes 1, \ldots, 1 \otimes k_2$ in E. Let $A = A_-$. Clearly $S_{-_1} \otimes 1$ and $1 \otimes S_{-_2}$ lie in A_-, but they don't span it. An added generator of A_- is given by $i_1 + i_2$ since $i_1(i_2 + 1) - \overline{i_1(i_2 + 1)} = i_1(i_2 + 1) - (i_2)(i_1 + 1) = i_1 + i_2$. Thus, an F-base of A_- is $\{1, j_1, k_1, j_2, k_2, i_1 + i_2\}$. The analogue of Lemma 1 above is:

Lemma 7. *For $x = \mu \cdot 1 + r + s + \nu \cdot (i_1 + i_2) \in A$, where $r \in F$-span $\{j_1, k_1\}$, $s \in F$-span $\{j_2, k_2\}$, and $\mu, \nu \in F$, we have*

$$x^2 + \nu x \in F \quad \textit{and} \quad \operatorname{Nrd}(x) = (x^2 + \nu x)^2 \in F^2\,.$$

Proof. Let $z = i_1 + i_2$. Easy calculations show $z^2 = z + (\alpha_1 + \alpha_2)$, $zr + rz = r$, and $zs + sz = s$. Thus, as $rs = sr$ and r^2, $s^2 \in F$,

$$\begin{aligned} x^2 + \nu x &= [\mu^2 + \mu^2 + s^2 + \nu^2 z^2 + \nu[rz + zr] + \nu[sz + zs]] + \nu[\mu + r + s + \nu z] \\ &= \mu^2 + r^2 + s^2 + \mu\nu + \nu^2(\alpha_1 + \alpha_2) \in F\,. \end{aligned}$$

The equations $z^2 + z = \alpha_1 + \alpha_2$, $(r + s)z = z(r + s) + (r + s)$, and $(r + s)^2$ $(= r^2 + s^2) \in F$ show that z and $(r + s)$ generate a quaternion algebra Q' isomorphic to $\left[\frac{\alpha_1 + \alpha_2, r^2 + s^2}{F}\right)$ inside E.* Thus, $\operatorname{Nrd}_E(x)$ (reduced norm relative to E) is the square of $\operatorname{Nrd}_{Q'}(x)$. Since $x + v$ is the image of x under the standard involution on Q', $\operatorname{Nrd}_{Q'}(x) = x(x + v)$, and $\operatorname{Nrd}_E(x) = \operatorname{Nrd}_{Q'}(x)^2 = [x(x + v)]^2 \in F^2$. $\square$

From this lemma it is clear we can take the Pfaffian adjoint $p\colon A \to A$ to be $p(x) = x + v \cdot 1$ for $x = \mu \cdot 1 + r + s + v \cdot z$ as above. As in Lemma 2, the function p is unique to a scalar multiple, and the Pfaffian quadratic form $q\colon A \to F$ is $q(x) = xp(x) = p(x)x = \mu^2 + \mu\nu + \nu^2(\alpha_1 + \alpha_2) + r^2 + s^2$. Here, r^2 gives the quadratic form $\beta_1[1, \alpha_1]$ and s^2 gives

*There is a technical difficulty with this if $r^2 = s^2$. For then Q' is not a quaternion algebra (not even semisimple). But the lemma is still valid, as can be seen by first working over the rational function field $K = F(X_1, X_2)$ with the algebra $\left[\frac{\alpha_1, x_1}{K}\right) \otimes_K \left[\frac{\alpha_2, x_2}{K}\right)$, where the argument is valid (except if $r - s = 0$, which is easily treated separately) then specializing $x_1 \mapsto \beta_1$, $x_2 \mapsto \beta_2$.

$\beta_2[1,\alpha_2]$. So, the form q is isometric to $[1,\alpha_1+\alpha_2] \perp \beta_1[1,\alpha_1] \perp \beta_2[1,\alpha_2]$. This is the form called in [MS] the Albert form associated to $E = Q_1 \otimes_F Q_2$. Mammone and Shapiro proved the analogue to Jacobson's theorem, Theorem 2 above, for $\mathrm{char}(F)=2$ using this Albert form. Notice that $p \circ p = id$, but p is not diagonalizable on A, as the only eigenvalue of p is 1, and the 1-eigenspace is F-span $\{1, j_1, k_1, j_2, k_2\}$, of dimension 5. Observe that the analogue to Lemma 3 holds here, and the proof is easier since there is no sign ambiguity about the square root.

Now, take any unit $s \in S_-$, and form a new involution $*$ on E by $r^* = s\bar{r}s^{-1}$. From the equations $(sr)^* = s\bar{r}$ and $sr - (sr)^* = s(r-\bar{r})$, we see $S_* = sS_- = S_-s^{-1}$ and $A_* = sA = As^{-1}$. Thus, we may again define a Pfaffian adjoint $p_* : A_* \to A_*$ by $p_*(b) = sp(bs)$, and define $q_* : A_* \to F$ by $q_*(b) = bp_*(b) = q(bs)$. So q_* is a quadratic form on A_* isometric to q on A. Then p_* has the same type of uniqueness as p in Lemma 2. Since Lemma 6 clearly still holds, it follows that the proof of Theorem 2 works also in characteristic 2, yielding the Mammone-Shapiro version of Jacobson's theorem. (Of course, this is still just another case of [KPS, Th. 3.4], which is valid for rank 16 Azumaya algebras over any commutative ring.)

Formula (1) above holds also when $\mathrm{char}(F)=2$: for all $b \in A_*$,

$$\mathrm{Nrd}(b) = q_*(b)^2 \mathrm{Nrd}(s)^{-1}\,.$$

Hence, again there is a Pfaffian discriminant for $*$, $\mathit{pfd}\,(*) = \mathrm{Nrd}(s)F^{\circ 2} \in F^\circ/F^{\circ 2}$. One can ask about Theorem 1 for $\mathrm{char}(F)=2$, and the answer seems not completely settled. One can see, as in Lemma 5 that for any involution $*$ on E arising as $*_1 \otimes *_2$ where $*_i$ is an involution on Q_i, $\mathit{pfd}\,(*) = 1 \cdot F^{\circ 2}$. Thus, the argument for (ii) $\Rightarrow$ (iii) of Theorem 1 works when $\mathrm{char}(F)=2$. This allows us to construct examples of E with an involution $*$ admitting no $*$-invariant quaternionic decomposition. Now, Lemma 4 also holds in characteristic 2 (with the same proof), so for any involution $*$ on E, if $\mathit{pfd}\,(*) = 1 \cdot F^{\circ 2}$, then p_* has a (unique) eigenvalue in F°. If the eigenspace Y for p_* is 5-dimensional, then one can always find a 2-dimensional subspace of Y on which q_* is nondegenerate, and this can be used to build a $*$-invariant quaternion subalgebra of E; so then we have (iii) $\Rightarrow$ (ii) of Theorem 1. But, I think $\mathit{pfd}\,(*) = 1$ and $\dim(Y) = 5$ if and only if $s \in A$. However, it can also occur that $\dim(Y) = 3$ and the associated bilinear form B_* of q_* (given by $(b,c) \mapsto q_*(b+c) - q_*(b) - q_*(c)$) vanishes identically on $Y \times Y_\circ$. (I think this occurs whenever $s \in S_-$ but $s \notin A$ (and $\mathrm{Nrd}(s) \in F^{\circ 2}$).) But it is not clear in this case whether one can always construct a $*$-invariant quaternion subalgebra of E.

References

[ART] S. A. Amitsur, L. H. Rowen, and J.-P. Tignol, *Division algebras of degree 4 and 8 with involution*, Israel J. Math. **33** (1979), 133–148.

[J] N. Jacobson, *Some applications of Jordan norms to involutorial simple associative algebras*, Adv. in Math. **48** (1983), 149–165.

[KPS] M.-A. Knus, R. Parimala, and R. Sridharan, *Pfaffians, central simple algebras, and similitudes*, Math. Z. **206** (1991), 589–604.

[MS] P. Mammone and D. B. Shapiro, *The Albert quadratic form for an algera of degree 4*, Proc. Amer. Math. Soc. **105** (1989), 525–530.

[S] W. Scharlau, *Quadratic and Hermitian forms*, Springer, 1985.

[TW] J.-P. Tignol and A. R. Wadsworth, *Totally ramified valuations on finite-dimensional division algebras*, Trans. Amer. Math. Soc. **302** (1987), 223–250.

9500 Gilman Dr., Dept. of Mathematics, La Jolla, CA 92093-0112
E-mail address: arwadsworth@ucsd.edu