Involutions and Trace Forms on Exterior Powers of a Central Simple Algebra

R. Skip Garibaldi, Anne Quéguiner-Mathieu,
Jean-Pierre Tignol

Received: February 2, 2001
Revised: April 25, 2001

Communicated by Ulf Rehmann

Abstract. For A a central simple algebra of degree $2n$, the nth exterior power algebra $\lambda^n A$ is endowed with an involution which provides an interesting invariant of A. In the case where A is isomorphic to $Q \otimes B$ for some quaternion algebra Q, we describe this involution quite explicitly in terms of the norm form for Q and the corresponding involution for B.

1991 Mathematics Subject Classification: 16K20 (11E81 20G05)
Keywords and Phrases: Trace forms, involutions, central simple algebras

The classification of irreducible representations of a split semisimple simply connected algebraic group G over an arbitrary field F is well-known: they are in one-to-one correspondence with the cone of dominant weights of G. Furthermore, one can tell whether or not an irreducible representation is orthogonal or symplectic (= supports a G-invariant bilinear form which is respectively symmetric or skew-symmetric) by inspecting the corresponding dominant weight [11, §3.11]. (Throughout this paper, we only consider fields of characteristic $\neq 2$, cf. 1.8.) A G-invariant bilinear form on an irreducible representation is necessarily unique up to a scalar multiple.

If the assumption that G is split is dropped, then the Galois group Γ of a separable closure F_s of F over F acts on the cone of dominant weights (via the so-called "$*$-action"), and this action may be nontrivial. Those irreducible representations corresponding to dominant weights which are not fixed by Γ are not defined over F. Although an irreducible representation ρ whose dominant weight is fixed by Γ may not be F-defined, there is always some central simple

F-algebra A and a map $G \to SL_1(A)$ defined over F which is an appropriate descent of ρ, see [14] or [12, p. 230, Prop. 1] for details. The algebra A is uniquely determined up to F-isomorphism. If ρ is orthogonal or symplectic over F_s, then it is easy to show that A supports a unique G-invariant involution γ of the first kind which is adjoint to the G-invariant bilinear form over every extension of F where A is split and hence ρ is defined.

It is of interest to determine γ. For example, invariants of γ in turn provide invariants of G. All involutions γ have been implicitly determined for $F = \mathbb{Q}_p$ and $F = \mathbb{R}$ in [4] and [5], but over an arbitrary field the problem is much more difficult since involutions are no longer classified by their classical invariants [2]. We restrict our attention to simply connected groups of type ${}^1A_{2n-1}$; that is, to the case $G = SL_1(A)$ for A a central simple F-algebra of degree $2n$. Moreover, we will focus on the fundamental irreducible representation corresponding to the middle vertex of the Dynkin diagram of G, which supports a G-invariant involution γ.

For any nonnegative integer $k \leq 2n$, there is a central simple F-algebra $\lambda^k A$ attached to A called the *kth exterior power of* A, and the appropriate analogues of the fundamental representations of $SL_1(A)$ are the natural maps $SL_1(A) \to SL_1(\lambda^k A)$ for $1 \leq k < 2n$. The representation we will study, which corresponds to the middle vertex of the Dynkin diagram, is the $k = n$ case. In general, $\lambda^k A$ is of degree $\binom{2n}{k}$ and is Brauer-equivalent to $A^{\otimes k}$, see [7, 10.A]. It is defined so that when A is the split algebra $A = \operatorname{End}_F(W)$, this $\lambda^k \operatorname{End}_F(W)$ is naturally isomorphic to $\operatorname{End}_F(\wedge^k W)$.

The nth exterior power $\lambda^n A$ is endowed with a canonical involution γ such that when A is split, γ is adjoint to the bilinear form θ defined on $\wedge^n W$ by the equation $\theta(x_1 \wedge \ldots \wedge x_n, y_1 \wedge \ldots \wedge y_n)e = x_1 \wedge \ldots \wedge x_n \wedge y_1 \wedge \ldots \wedge y_n$, where e is any basis of the 1-dimensional vector space $\wedge^{2n} W$. This involution is preserved by the image of G in $SL_1(\lambda^n A)$ and is the one we wish to describe. If n is even and $A^{\otimes n}$ is split, then γ is orthogonal and $\lambda^n A$ is split, so our fundamental representation of G is defined over F and orthogonal. For example, for A a biquaternion algebra over an arbitrary field F, γ is adjoint to an Albert form of A [3, 6.2]. In this paper, we provide a complete description of γ for G of type ${}^1A_{2n-1}$ when n is odd (see 1.1) or when n is even and A is isomorphic to $B \otimes Q$ where Q is a quaternion algebra (in 1.4 and 1.5). In particular, until now a description of γ has not been known for any algebra A of index ≥ 8. If A is a tensor product of quaternion algebras, we provide (in 1.6 below) a formula that gives γ in terms of the norm forms of the quaternion algebras.

Describing this particular involution γ is also interesting from the point of view of groups of type ${}^1D_{2n}$. Such a group is isogenous to $G = \operatorname{Spin}(E, \sigma)$ for E a central simple algebra of degree $4n$ and σ an orthogonal involution with trivial discriminant. If σ is hyperbolic, then E is isomorphic to $M_2(A)$ for some algebra A of degree $2n$. The analogue of the direct sum of the two half-spin representations for $\operatorname{Spin}(M_2(A), \sigma)$ over F is the map $G \to SL_1(C(M_2(A), \sigma))$ where $C(M_2(A), \sigma)$ denotes the even Clifford algebra of $(M_2(A), \sigma)$. This algebra is endowed with a canonical involution $\underline{\sigma}$ which is G-invariant; it is mostly hyperbolic but contains a nontrivial piece which is isomorphic to $(\lambda^n A, \gamma)$. Please see [3] for a precise statement and [10] for a rational proof.

This relationship between representations of D_{2n} and A_{2n-1} as well as the results in this paper hint at a general theory of orthogonal representations of semisimple algebraic groups over arbitrary fields. We hope to study this in the future.

1 STATEMENT OF THE MAIN RESULTS

We will always assume that our base field F has characteristic $\neq 2$ and that A is a central simple F-algebra of degree $2n$. (See 1.8 for a discussion of the characteristic 2 case.) We assume moreover that A is isomorphic to a tensor product $A = Q \otimes B$, where Q is a quaternion algebra over F, and B is a central simple F-algebra, necessarily of degree n. Note that this is always the case when n is odd. We write γ_Q for the canonical symplectic involution on Q and n_Q for the norm form.

If n is odd, the main result is the following, proven in Section 4:

THEOREM 1.1. *If n is odd, the algebra with involution $(\lambda^n(Q \otimes B), \gamma)$ is Witt-equivalent to $(Q, \gamma_Q)^{\otimes n}$.*

Witt-equivalence for central simple algebras is the natural generalization of Witt-equivalence for quadratic forms, see [1] for a definition.

Assume now that n is even, $n = 2m$. Then $\lambda^n A$ is split and the involution γ is orthogonal. We fix some quadratic form q_A to which γ is adjoint. It is only defined up to similarity.

The algebra $\lambda^m B$ is endowed with a canonical involution which we denote by γ_m. For $k = 0, \ldots, n$, we let $t_k : \lambda^k B \to F$ be the reduced trace quadratic form defined by

$$t_k(x) = \operatorname{Trd}_{\lambda^k B}(x^2). \tag{1.2}$$

This form also has a natural description from the representation-theoretic viewpoint: The group $SL_1(B)$ acts on the vector space $\lambda^k B$, and when B is split $\lambda^k B$ is isomorphic to a tensor product of an irreducible representation with its dual, see Section 2. Consequently, there is a canonical $SL_1(B)$-invariant quadratic form on $\lambda^k B$; it is t_k.

We let t_m^+ and t_m^- denote the restrictions of t_m to the subspaces $\operatorname{Sym}(\lambda^m B, \gamma_m)$ and $\operatorname{Skew}(\lambda^m B, \gamma_m)$ of elements of $\lambda^m B$ which are respectively symmetric and skew-symmetric under γ_m, so that $t_m = t_m^+ \oplus t_m^-$. The forms thus defined are related by the following equation, proven in 5.5:

THEOREM 1.3. *In the Witt ring of F, the following equality holds:*

$$\langle 2 \rangle \cdot \sum_{k=0}^{m-1} (-1)^k t_k = \begin{cases} -t_m^- & \text{if } m \text{ is even,} \\ t_m^+ & \text{if } m \text{ is odd.} \end{cases}$$

The similarity class of q_A is determined by the following theorem, proven in 5.7:

Theorem 1.4. *If n is even, $n = 2m$, the similarity class of q_A contains the quadratic form:*

$$t_m^+ - t_m^- + n_Q \cdot \Bigl(t_m^- + \sum\nolimits_{\substack{0\leq k<m \\ k \text{ even}}} \langle 2\rangle t_k\Bigr) \qquad \text{if } m \text{ is even,}$$

$$t_m^- - t_m^+ + n_Q \cdot \Bigl(\sum\nolimits_{\substack{0\leq k<m \\ k \text{ even}}} \langle 2\rangle t_k\Bigr) \qquad \text{if } m \text{ is odd.}$$

The Witt class of this quadratic form can be described more precisely under some additional assumptions (see Proposition 6.1 for precise statements). We just mention here a particular case in which the formula reduces to be quite nice.

Assume that m is even and B is of exponent at most 2. Then $\lambda^m B$ is split, and its canonical involution is adjoint to a quadratic form q_B. Even though this form is only defined up to a scalar factor, its square is actually defined up to isometry. We then have the following, proven in 5.8:

Corollary 1.5. *If m is even (i.e., $\deg B \equiv 0 \mod 4$) and B is of exponent at most 2, then the similarity class of q_A contains a form whose Witt class is $q_B^2 + n_Q\bigl(2^{n-2} - \frac{1}{2}\binom{n}{m} - \wedge^2 q_B\bigr)$.*

Some of the notation needs an explanation. For a quadratic form q on a vector space W with associated symmetric bilinear form b so that $q(w) = b(w, w)$, we have an induced quadratic form on $\wedge^2 W$ which we denote by $\wedge^2 q$. For $x_1, x_2, y_1, y_2 \in W$, its associated symmetric bilinear form $\wedge^2 b$ is defined by

$$(\wedge^2 b)(x_1 \wedge x_2, y_1 \wedge y_2) = b(x_1, y_1)b(x_2, y_2) - b(x_1, y_2)b(x_2, y_1).$$

Thus if $q = \langle \alpha_1, \dots, \alpha_n\rangle$, we have

$$\wedge^2 q \simeq \oplus_{1\leq i<j\leq n}\langle \alpha_i\alpha_j\rangle.$$

From this, one sees that even if q is just defined up to similarity, $\wedge^2 q$ is well-defined up to isometry. (The form $\wedge^2 q$ also admits a representation-theoretic description: It is isomorphic to a scalar multiple of the Killing form on the Lie algebra $\mathfrak{o}(q)$, where the scalar factor depends only on the dimension of q.)

From Corollary 1.5, we also get the following, which is proven in 6.3:

Corollary 1.6. *Let $A_r = Q_1 \otimes \dots \otimes Q_r$ be a tensor product of r quaternion F-algebras, where $r \geq 3$, and let T_{A_r} be the reduced trace quadratic form on A_r. The similarity class of q_{A_r} contains a quadratic form whose Witt class is*

$$2^{n-1} - \frac{2^{n-2}}{n}\langle 2^r\rangle \cdot T_{A_r} = 2^{f(r)}\bigl(2^r - (2 - n_{Q_1})\cdots(2 - n_{Q_r})\bigr),$$

where $n = 2^{r-1} = \frac{1}{2}\deg A$ and $f(r) = 2^{r-1} - r - 1$.

In particular, for $r = 3$, we get the quadratic form

$$4(n_{Q_1} + n_{Q_2} + n_{Q_3}) - 2(n_{Q_1}n_{Q_2} + n_{Q_1}n_{Q_3} + n_{Q_2}n_{Q_3}) + n_{Q_1}n_{Q_2}n_{Q_3}.$$

Adrian Wadsworth had casually conjectured a description of q_{A_3} in [3, 6.8], and we now see that his conjecture was not quite correct in that it omitted the $n_{Q_1}n_{Q_2}n_{Q_3}$ term.

As a consequence of Corollary 1.6, we can show that the form q_A lies in the nth power of the fundamental ideal of the Witt ring WF for many central simple algebras A of degree $2n$; the following result is proven in 6.4:

Corollary 1.7. *Suppose that A is a central simple algebra of degree $2n \equiv 0 \mod 4$ which is isomorphic to matrices over a tensor product of quaternion algebras. Then the form q_A lies in I^nF.*

The first author conjectured [3, 6.6] that q_A lies in I^nF for *all* central simple F-algebras A of degree $2n \equiv 0 \mod 4$ and such that $A^{\otimes 2}$ is split. Corollary 1.7 fails to prove the full conjecture because for every integer $r \geq 3$ there exists a division algebra A of degree 2^r and exponent 2 such that A doesn't decompose as $A' \otimes A''$ for any nontrivial division algebras A' and A'' [6, 3.3], so such an A doesn't satisfy the hypotheses of Corollary 1.7.

If A is a tensor product of two quaternion algebras, the form q_A is an Albert form of A, and the Witt index of q_A determines the Schur index of A, as Albert has shown (see for instance [7, (16.5)]). Corollary 1.6 shows that one cannot expect nice results relating the Witt index of q_{A_r} and the Schur index of A_r for $r \geq 3$. As pointed out to us by Jan van Geel, the difficulty is that Merkurjev has constructed in [9, §3] algebras of the form A_r for $r \geq 3$ (i.e., tensor products of at least 3 quaternion algebras) which are skew fields but whose center, F, has $I^3F = 0$. By Corollary 1.7, the forms q_{A_r} are then hyperbolic.

Remark 1.8 (characteristic 2). One might hope that results concerning representations of algebraic groups would not involve the restriction that the characteristic is not 2. However, removing this restriction for the results in this paper would necessarily dramatically change their nature. For example, the trace forms t_k occurring here are degenerate in characteristic 2. Also, our methods require the ability to take tensor products of quadratic forms and to scale by a factor of $\langle 2 \rangle$, neither of which are available in characteristic 2. These restrictions may be avoidable, but we have chosen not to attempt to do so because such an attempt would almost certainly make this paper so technical that it would be nearly unreadable.

2 Description of $\lambda^n M_2(B)$

In order to prove these results, we have to describe the algebra with involution $(\lambda^n(Q \otimes B), \gamma)$, which we will do by Galois descent. Hence we first give a description of $\lambda^n M_2(B)$, see Theorem 2.5 below.

Assume $B = \mathrm{End}_F(V)$ for some n-dimensional vector space V. For $0 \leq k \leq n$, we have $\lambda^k B = \mathrm{End}_F(\wedge^k V)$. We identify $M_2(B) \simeq \mathrm{End}_F(V \oplus V)$ by mapping $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(B)$ to the endomorphism

$$(x, y) \mapsto \big(a(x) + b(y), c(x) + d(y)\big).$$

The distinguished choice of embedding of B in $M_2(B)$ corresponds with the obvious choice of direct sum decomposition of $V \oplus V$. (There are many others.) This gives an identification $\lambda^n M_2(B) = \mathrm{End}_F(\wedge^n(V \oplus V))$. For all integers k, ℓ, this decomposition determines $\wedge^k V \otimes \wedge^\ell V$ as a vector subspace of $\wedge^{k+\ell}(V \oplus V)$ by mapping $(x_1 \wedge \cdots \wedge x_k) \otimes (y_1 \wedge \cdots \wedge y_\ell)$ to

$$(x_1, 0) \wedge \cdots \wedge (x_k, 0) \wedge (0, y_1) \wedge \cdots \wedge (0, y_\ell) \in \wedge^{k+\ell}(V \oplus V).$$

In particular, we have

$$\wedge^n (V \oplus V) = \oplus_{k=0}^n \left(\wedge^k V \otimes \wedge^{n-k} V\right). \tag{2.1}$$

For each k, the space $\wedge^k V \otimes \wedge^{n-k} V$ can be identified to $\mathrm{End}_F(\wedge^k V)$ as follows. Fix a nonzero element (hence a basis) e of $\wedge^n V$ and define a bilinear form

$$\theta_k \colon \ \wedge^k V \times \wedge^{n-k} V \to F$$

by the equation

$$\theta_k(x_k, x_{n-k})\, e = x_k \wedge x_{n-k} \text{ for } x_\ell \in \wedge^\ell V.$$

This form is nonsingular, so it provides the identification mentioned above

$$\wedge^k V \otimes \wedge^{n-k} V = \mathrm{End}_F(\wedge^k V) \tag{2.2}$$

by sending $x_k \otimes x_{n-k}$ to the map $y \mapsto x_k \theta_{n-k}(x_{n-k}, y)$. The product in $\mathrm{End}_F(\wedge^k V)$ then corresponds in $\wedge^k V \otimes \wedge^{n-k} V$ to

$$(x_k \otimes x_{n-k})(y_k \otimes y_{n-k}) = \theta_{n-k}(x_{n-k}, y_k)\, x_k \otimes y_{n-k}.$$

From (2.1) and (2.2), we deduce an identification of the corresponding endomorphism rings

$$\lambda^n M_2(B) = \mathrm{End}_F(\oplus_{k=0}^n \lambda^k B). \tag{2.3}$$

This remains true in the case when B is non split, as we will prove by Galois descent. First, we must introduce some maps on $\oplus_{k=0}^n \lambda^k B$.
Since the bilinear form θ_k is nonsingular, for any $f \in \mathrm{End}_F(\wedge^k V)$, we have a unique element $\gamma_k(f) \in \mathrm{End}_F(\wedge^{n-k} V)$ such that

$$\theta_k\left(f(x), y\right) = \theta_k\left(x, \gamma_k(f)(y)\right),$$

for every $x \in \wedge^k V$ and $y \in \wedge^{n-k} V$. This defines a canonical anti-isomorphism (not depending on the choice of e)

$$\gamma_k \colon \operatorname{End}_F(\wedge^k V) \to \operatorname{End}_F(\wedge^{n-k} V)$$

such that

$$\gamma_k(x \otimes y) = (-1)^{k(n-k)} y \otimes x \tag{2.4}$$

for x and y as before. One may easily verify that $\gamma_{n-k} \circ \gamma_k = \operatorname{Id}_{\operatorname{End}_F(\wedge^k V)}$ for all $k = 0, \dots, n$. By Galois descent, the maps γ_k are defined even when B is nonsplit, i.e., we have anti-isomorphisms $\gamma_k \colon \lambda^k B \to \lambda^{n-k} B$ such that $\gamma_k \circ \gamma_{n-k} = \operatorname{Id}_{\lambda^k B}$ (see [7, Exercise 12, p. 147] for a rational definition). In the particular case where n is even, by definition of the bilinear form $\theta_{n/2}$, the map $\gamma_{n/2}$ is actually the canonical involution on $\lambda^{n/2} B$.

Theorem 2.5. *Whether or not B is split, there is a canonical isomorphism*

$$\Phi \colon \lambda^n M_2(B) \to \operatorname{End}_F(\lambda^0 B \oplus \cdots \oplus \lambda^n B)$$

which in the split case is the identification (2.3) *above. The canonical involution γ on $\lambda^n M_2(B)$ induces via Φ an involution on $\operatorname{End}_F(\oplus_{k=0}^n \lambda^k B)$ which is adjoint to the bilinear form T defined on $\lambda^0 B \oplus \cdots \oplus \lambda^n B$ by*

$$T(u,v) = \begin{cases} (-1)^\ell \operatorname{Trd}_{\lambda^k B}\left(u \gamma_\ell(v)\right) & \text{if } k + \ell = n, \\ 0 & \text{if } k + \ell \neq n, \end{cases}$$

for any $u \in \lambda^k B$ and $v \in \lambda^\ell B$.

Proof. We prove this by Galois descent. Fix a separable closure F_s of F and let $\Gamma := \operatorname{Gal}(F_s/F)$ be the absolute Galois group. We fix a vector space V over F such that $\dim_F V = \deg B = n$ and let $V_s = V \otimes_F F_s$. We fix also an F_s-algebra isomorphism $\varphi \colon B \otimes_F F_s \xrightarrow{\sim} \operatorname{End}_F(V) \otimes_F F_s$. Every $\sigma \in \Gamma$ acts canonically on V_s and $\operatorname{End}_{F_s}(V_s) = \operatorname{End}_F(V) \otimes_F F_s$; we denote again by σ these canonical actions, so that $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$ for $f \in \operatorname{End}_{F_s}(V_s)$. On the other hand, the canonical action of Γ on $B \otimes_F F_s$ corresponds under φ to some twisted action $*$ on $\operatorname{End}_{F_s}(V_s)$. Since every F_s-linear automorphism of $\operatorname{End}_{F_s}(V_s)$ is inner, we may find $g_\sigma \in \operatorname{GL}(V_s)$ such that

$$\sigma * f = g_\sigma \circ \sigma(f) \circ g_\sigma^{-1} = \operatorname{Int}(g_\sigma) \circ \sigma(f) \qquad \text{for all } f \in \operatorname{End}_{F_s}(V_s).$$

Then φ induces an F-algebra isomorphism from B onto the F-subalgebra

$$\left\{ f \in \operatorname{End}_{F_s}(V_s) \mid g_\sigma \circ \sigma(f) \circ g_\sigma^{-1} = f \text{ for all } \sigma \in \Gamma \right\}.$$

The $*$-action of Γ on $\operatorname{End}_{F_s}(V_s)$ induces twisted actions on $\operatorname{End}_{F_s}\bigl(\wedge^n(V_s \oplus V_s)\bigr)$ and on $\operatorname{End}_{F_s}\bigl(\oplus_{k=0}^n \operatorname{End}_{F_s}(\wedge^k V_s)\bigr)$ such that the F-algebras of Γ-invariant elements are $\lambda^n\bigl(M_2(B)\bigr)$ and $\operatorname{End}_F(\oplus_{k=0}^n\lambda^k B)$ respectively. To prove the first assertion of the theorem, we will show that these actions correspond to each other under the isomorphism

$$\operatorname{End}_{F_s}\bigl(\wedge^n(V_s\oplus V_s)\bigr)\xrightarrow{\sim}\operatorname{End}_{F_s}\bigl(\oplus_{k=0}^n\operatorname{End}_{F_s}(\wedge^k V_s)\bigr)$$

derived from (2.1) and (2.2).

For $\sigma\in\Gamma$ and $k=0,\dots,n$, define $\wedge^k g_\sigma\in\operatorname{GL}(\wedge^k V_s)$ by

$$\wedge^k g_\sigma(x_1\wedge\ldots\wedge x_k)=g_\sigma(x_1)\wedge\ldots\wedge g_\sigma(x_k).$$

Then φ induces an F-algebra isomorphism from $\lambda^k B$ onto the F-subalgebra

$$\bigl\{f\in\operatorname{End}_{F_s}(\wedge^k V_s)\mid \wedge^k g_\sigma\circ\sigma(f)\circ(\wedge^k g_\sigma)^{-1}=f\text{ for all }\sigma\in\Gamma\bigr\},$$

hence also from $\operatorname{End}_F(\oplus_{k=0}^n\lambda^k B)$ to

$$\Bigl\{f\in\operatorname{End}_{F_s}\bigl(\oplus_{k=0}^n\operatorname{End}_{F_s}(\wedge^k V_s)\bigr)\mid \bigl(\oplus_k\operatorname{Int}(\wedge^k g_\sigma)\bigr)\circ\sigma(f)=f\circ\bigl(\oplus_k\operatorname{Int}(\wedge^k g_\sigma)\bigr)\text{ for all }\sigma\in\Gamma\Bigr\}.$$

Similarly, define $\wedge^n(g_\sigma\oplus g_\sigma)\in\operatorname{GL}\bigl(\wedge^n(V_s\oplus V_s)\bigr)$ by

$$\wedge^n\,(g_\sigma\oplus g_\sigma)\bigl((x_1,y_1)\wedge\ldots\wedge(x_n,y_n)\bigr)=\bigl(g_\sigma(x_1),g_\sigma(y_1)\bigr)\wedge\ldots\wedge\bigl(g_\sigma(x_n),g_\sigma(y_n)\bigr),$$

so that $\lambda^n\bigl(M_2(B)\bigr)$ can be identified through φ with

$$\Bigl\{f\in\operatorname{End}_{F_s}\bigl(\wedge^n(V_s\oplus V_s)\bigr)\mid \wedge^n\,(g_\sigma\oplus g_\sigma)\circ\sigma(f)=f\circ\wedge^n(g_\sigma\oplus g_\sigma)\text{ for all }\sigma\in\Gamma\Bigr\}.$$

Certainly, $\wedge^n(g_\sigma\oplus g_\sigma)=\oplus_{k=0}^n(\wedge^k g_\sigma\otimes\wedge^{n-k}g_\sigma)$ under (2.1), and computation shows that $\wedge^k g_\sigma\otimes\wedge^{n-k}g_\sigma=(\det g_\sigma)\operatorname{Int}(\wedge^k g_\sigma)$ under (2.2). Therefore, (2.1) and (2.2) induce an isomorphism of F-algebras

$$\Phi\colon\ \lambda^n\bigl(M_2(B)\bigr)\xrightarrow{\sim}\operatorname{End}_F(\oplus_{k=0}^n\lambda^k B).$$

To complete the proof of the theorem, we show that the canonical involution γ on $\lambda^n\bigl(M_2(B)\bigr)$ corresponds to the adjoint involution with respect to T under Φ. In order to do so, we view $\lambda^n\bigl(M_2(B)\bigr)$ and $\operatorname{End}_F(\oplus_{k=0}^n\lambda^k B)$ as the fixed subalgebras of $\operatorname{End}_{F_s}\bigl(\wedge^n(V_s\oplus V_s)\bigr)$ and $\operatorname{End}_{F_s}\bigl(\oplus_{k=0}^n\operatorname{End}_{F_s}(\wedge^k V_s)\bigr)$, and show that the canonical involution γ on $\operatorname{End}_{F_s}\bigl(\wedge^n(V_s\oplus V_s)\bigr)$ corresponds to the adjoint involution with respect to T (extended to F_s) under the isomorphism induced by (2.1) and (2.2).

Taking any nonzero element $e \in \wedge^n V_s$, the identification $\wedge^{2n}(V_s \oplus V_s) = \wedge^n V_s \otimes \wedge^n V_s$ allows us to write $e \otimes e$ for a nonzero element of $\wedge^{2n}(V_s \otimes V_s)$. Then γ is adjoint to the bilinear form

$$\Theta\colon\ \wedge^n (V_s \oplus V_s) \times \wedge^n (V_s \oplus V_s) \to F_s$$

given by

$$\Theta(x,y)\, e \otimes e = x \wedge y \text{ for } x, y \in \wedge^n (V_s \oplus V_s)$$

as was mentioned in the introduction. Using the identification of $\wedge^k V_s \otimes \wedge^{n-k} V_s$ as a subspace of $\wedge^n(V_s \oplus V_s)$, we have that for $x_i, y_i \in \wedge^i V_s$,

$$\Theta(x_k \otimes x_{n-k}, y_\ell \otimes y_{n-\ell}) = \\ \begin{cases} (-1)^\ell \theta_k(x_k, y_\ell)\theta_{n-k}(x_{n-k}, y_{n-\ell}) & \text{if } k + \ell = n, \\ 0 & \text{if } k + \ell \neq n. \end{cases}$$

We translate this into terms involving B, using the isomorphism φ to identify $\lambda^k B_s := (\lambda^k B) \otimes_F F_s$ with $\operatorname{End}_{F_s}(\wedge^k V_s)$. In particular, we know that

$$\operatorname{Trd}_{\lambda^k B_s}(x_k \otimes x_{n-k}) = \theta_{n-k}(x_{n-k}, x_k)$$

for Trd the reduced trace, and that

$$\theta_k(x_k, x_{n-k}) = (-1)^{k(n-k)} \theta_{n-k}(x_{n-k}, x_k).$$

So for $x = x_k \otimes x_{n-k} \in \lambda^k B_s$ and $y = y_\ell \otimes y_{n-\ell} \in \lambda^\ell B_s$,

$$\Theta(x,y) = \begin{cases} (-1)^\ell \operatorname{Trd}_{\lambda^k B_s}(\gamma_\ell(y)x) & \text{if } k + \ell = n, \\ 0 & \text{if } k + \ell \neq n. \end{cases}$$

Of course, in the $k + \ell = n$ case we could just as easily have taken

$$\Theta(x,y) = (-1)^\ell \operatorname{Trd}_{\lambda^\ell B_s}(\gamma_k(x)y).$$

So, the vector space isomorphism derived from (2.1) and (2.2) is an isometry of Θ and T, and it follows that the canonical involution γ adjoint to Θ corresponds to the adjoint involution to T under Φ. $\square$

For later use, we prove a little bit more about this isomorphism Φ. Let us consider the elements $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $e_2 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in M_2(B)$, and let t be an indeterminate over F. We write λ^n for the map $M_2(B) \to \lambda^n M_2(B)$ defined in [7, 14.3], which is a homogeneous polynomial map of degree n. In the split case where $M_2(B)$ is identified with $\operatorname{End}_F(V \oplus V)$ and $\lambda^n M_2(B)$ with $\operatorname{End}_F\big(\wedge^n(V \oplus V)\big)$, the map is given by

$$(\lambda^n f)(w_1 \wedge \cdots \wedge w_n) = f(w_1) \wedge \cdots \wedge f(w_n)$$

for $f \in \operatorname{End}_F(V \oplus V)$ and $w_1, \ldots, w_n \in V \oplus V$. Whether or not B is split, there exist $\ell_0, \ldots, \ell_n \in \lambda^n M_2(B)$ such that

$$\lambda^n(e_1 + te_2) = t^n \ell_0 + t^{n-1}\ell_1 + \cdots + t\ell_{n-1} + \ell_n.$$

We then have

Lemma 2.6. *For $k = 0, \dots, n$, the image of ℓ_k under Φ is the projection on $\lambda^k B$. Moreover, we have $\gamma(\ell_k) = \ell_{n-k}$.*

Proof. It is enough to prove it in the split case. Hence, we may assume $B = \mathrm{End}_F(V)$, and use identification (2.2) of the previous section. An element of $\lambda^k B = \mathrm{End}_F(\wedge^k V)$ can be written as $(x_1 \wedge \dots \wedge x_k) \otimes (y_1 \wedge \dots \wedge y_{n-k})$, where $x_1, \dots, x_k, y_1, \dots, y_{n-k} \in V$. The endomorphism $\lambda^n(e_1 + te_2)$ acts on this element as follows:

$$\begin{aligned}\lambda^n(e_1 + te_2)\,&((x_1 \wedge \dots \wedge x_k) \otimes (y_1 \wedge \dots \wedge y_{n-k}))\\ &= \quad (x_1, 0) \wedge \dots \wedge (x_k, 0) \wedge (0, ty_1) \wedge \dots \wedge (0, ty_{n-k})\\ &= \quad t^{n-k}(x_1 \wedge \dots \wedge x_k) \otimes (y_1 \wedge \dots \wedge y_{n-k}).\end{aligned}$$

Hence, the image under ℓ_i of this element is itself if $i = k$ and 0 otherwise. This proves the first assertion of the lemma. By Theorem 2.5, to prove the second one, one has to check that for any $u, v \in \lambda^0 B \oplus \dots \oplus \lambda^n B$, we have $T(\ell_i(u), v) = T(u, \ell_{n-i}(v))$, which follows easily from the description of T given in that theorem. ☐

Remark 2.7. By the previous lemma, the elements $\ell_0, \dots, \ell_n \in \lambda^n M_2(B)$ are orthogonal idempotents. Hence, the fact that $\gamma(\ell_k) = \ell_{n-k}$ for all $k = 0, \dots, n$ implies that the involution γ is hyperbolic if n is odd and Witt-equivalent to its restriction to $\ell_m \lambda^n M_2(B) \ell_m$ if $n = 2m$.

We will also use the following:

Lemma 2.8. *For any $b \in F^\times$, consider $g_0 := \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right) \in M_2(B)$, and set $g := \lambda^n(g_0)$. We have:*

1. *for any $u \in \lambda^k B$, $\Phi(g)(u) = b^{n-k}\gamma_k(u) \in \lambda^{n-k} B$;*
2. *$g^2 = b^n$ and $\gamma(g) = (-1)^n g$;*
3. *For any $k = 0, \dots, n$, $g\ell_k = \ell_{n-k} g$.*

Proof. Again, it is enough to prove it in the split case. A direct computation then shows that for any $x \otimes y \in \wedge^k V \otimes \wedge^{n-k} V = \lambda^k B$, we have

$$g(x \otimes y) = (-1)^{k(n-k)} b^{n-k} (y \otimes x),$$

which combined with (2.4) gives (1), which in turn easily implies (3). The first part of (2) is because λ^n restricts to be a group homomorphism on $M_2(B)^*$ [7, 14.3], and the second part then follows since $\gamma(g)g = \mathrm{Nrd}_{\lambda^n M_2(B)}(g) = (-b)^n$ by [7, 14.4]. ☐

3 Description of $\lambda^n(Q \otimes B)$

We suppose that $Q = (a,b)_F$ is a quaternion F-algebra and B is an arbitrary central simple F-algebra of degree n. We will describe $\lambda^n(Q \otimes B)$ by Galois descent from $K = F(\alpha)$, where $\alpha \in F_s$ is a fixed square root of a. More precisely, let us identify Q with the F-subalgebra of $M_2(K)$ generated by $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)$ and $g_0 = \left(\begin{smallmatrix} 0 & b \\ 1 & 0 \end{smallmatrix}\right)$, i.e.,

$$Q = \{x \in M_2(K) \mid g_0 \bar{x} g_0^{-1} = x\},$$

where $\bar{\ }$ denotes the non-trivial automorphism of K/F. We also have

$$Q \otimes B = \{x \in M_2(B_K) \mid g_0 \bar{x} g_0^{-1} = x\},$$

where $B_K = B \otimes_F K$, and g_0 is now viewed as an element of $M_2(B_K)$.
The canonical map $\lambda^n \colon A \to \lambda^n A$ restricts to be a group homomorphism on A^* [7, 14.3]. Moreover, when $\deg A = 2n$, for $a \in A^*$, $\operatorname{Int}(\lambda^n(a))$ preserves the canonical involution γ on $\lambda^n A$ [7, 14.4], and so we get a map

$$\lambda^n \colon \operatorname{Aut}(A) \to \operatorname{Aut}(\lambda^n A, \gamma).$$

In particular this holds for $A = M_2(B_K)$. This induces a map on Galois cohomology

$$H^1(K/F, \operatorname{Aut}(M_2(B_K))) \xrightarrow{H^1(\lambda^n)} H^1(K/F, \operatorname{Aut}(\lambda^n M_2(B_K), \gamma)).$$

The image under this map of the 1-cocycle $\bar{\ } \mapsto \operatorname{Int}(g_0)$ is the 1-cocycle $\bar{\ } \mapsto \operatorname{Int}(\lambda^n g_0)$, as in the preceding section. Since the former 1-cocycle corresponds to $Q \otimes B$, the latter corresponds to $\lambda^n(Q \otimes B)$, so

$$\lambda^n(Q \otimes B) = \{x \in \lambda^n M_2(B_K) \mid g \bar{x} g^{-1} = x\} \tag{3.1}$$

for $g := \lambda^n(g_0)$. We fix this definition of g for the rest of the paper.

4 The n odd case

This section is essentially the proof of Theorem 1.1.
We set $\lambda^{\text{even}} B := \oplus_{\substack{0 \le k < n \\ k \text{ even}}} \lambda^k B$. For $0 \le k \le n$, we let t_k be the reduced trace quadratic form on $\lambda^k B$ as in (1.2). We then have the following:

Lemma 4.1. *When $n = \deg B$ is odd, the algebra with involution $(\lambda^n(Q \otimes B), \gamma)$ is isomorphic to $(Q, \gamma_Q) \otimes (C, \sigma)$, where (C, σ) is isomorphic to $\operatorname{End}_F(\lambda^{\text{even}} B)$ endowed with the adjoint involution with respect to $\sum_{\substack{0 \le k < n \\ k \text{ even}}} t_k$.*

Proof. If $i, j \in Q$ satisfy $i^2 = a$, $j^2 = b$ and $ij = -ji$, then since λ^n restricts to be a group homomorphism on $(Q \otimes B)^*$, $\lambda^n(i \otimes 1)$ and $\lambda^n(j \otimes 1) \in \lambda^n(Q \otimes B)$ anticommute and satisfy

$$\begin{aligned} \lambda^n(i \otimes 1)^2 &= a^n, & \lambda^n(j \otimes 1)^2 &= b^n, \\ \gamma(\lambda^n(i \otimes 1)) &= -\lambda^n(i \otimes 1), & \gamma(\lambda^n(j \otimes 1)) &= -\lambda^n(j \otimes 1). \end{aligned}$$

(For the bottom two equations, see [7, (14.4)].) Hence, these two elements generate a copy of Q in $\lambda^n(Q\otimes B)$ on which γ restricts to be γ_Q and we have $(\lambda^n(Q\otimes B),\gamma)\simeq(Q,\gamma_Q)\otimes(C,\sigma)$, where C is the centralizer of Q in $\lambda^n(Q\otimes B)$ and σ denotes the restriction of γ to C [7, 1.5].

To describe C, we take $i=\alpha(e_1-e_2)$ and $j=g_0$, as in the beginning of the previous section, so that $\lambda^n(j\otimes 1)=g$ and

$$\lambda^n(i\otimes 1)=\alpha^n((-1)^n\ell_0+(-1)^{n-1}\ell_1+\cdots+\ell_n)=-\alpha^n(\ell_{\mathrm{even}}-\ell_{\mathrm{odd}}),$$

where $\ell_{\mathrm{even}}=\sum_{\substack{0\le k\le n\\ k\text{ even}}}\ell_k$ and $\ell_{\mathrm{odd}}=\sum_{\substack{0\le k\le n\\ k\text{ odd}}}\ell_k$.

Let us consider the map $\Psi\colon \ell_{\mathrm{even}}\lambda^n(M_2(B))\ell_{\mathrm{even}}\to\lambda^n(M_2(B_K))$ defined by $\Psi(x)=x+gxg^{-1}$. A direct computation shows that Ψ is an F-algebra homomorphism, amazingly. Clearly, $\overline{\Psi(x)}=\Psi(x)$ and since $g^2=b^n$ is central (see Lemma 2.8), $g\Psi(x)=\Psi(x)g$ for all x. Hence, the image of Ψ is contained in $\lambda^n(Q\otimes B)$ and is centralized by g. Moreover,

$$\lambda^n(i\otimes 1)\Psi(x)=-\alpha^n(x-gxg^{-1})=\Psi(x)\lambda^n(i\otimes 1).$$

Hence, the image of Ψ also centralizes $\lambda^n(i\otimes 1)$, and is therefore contained in C. Now, since ℓ_{even} is an idempotent of $\lambda^n(M_2(B))$, the algebra $\ell_{\mathrm{even}}\lambda^n(M_2(B))\ell_{\mathrm{even}}$ is simple, hence Ψ is injective. By dimension count it follows that its image is exactly C.

Since $\gamma(\Psi(x))=\Psi(g^{-1}\gamma(x)g)$, the involution σ on C corresponds via Ψ to $\mathrm{Int}(g^{-1})\circ\gamma$ on $\ell_{\mathrm{even}}\lambda^n(M_2(B))\ell_{\mathrm{even}}$. Note that if $x\in\ell_{\mathrm{even}}\lambda^n(M_2(B))\ell_{\mathrm{even}}$, then $\gamma(x)\in\ell_{\mathrm{odd}}\lambda^n(M_2(B))\ell_{\mathrm{odd}}$ and $g^{-1}\gamma(x)g\in\ell_{\mathrm{even}}\lambda^n(M_2(B))\ell_{\mathrm{even}}$. By Theorem 2.5, we get that (C,σ) is isomorphic to $\mathrm{End}_F(\lambda^{\mathrm{even}}B)$ endowed with the involution adjoint to the quadratic form T' defined by $T'(u,v)=T(u,\Phi(g)(v))$. Using the description of T given in Theorem 2.5 and Lemma 2.8(1), it is easy to check that the λ^kB are pairwise orthogonal for T' and that T' restricts to be $\langle(-b)^{n-k}\rangle t_k$ on λ^kB. Thus T' is similar to $\sum_{\substack{0\le k<n\\ k\text{ even}}}t_k$. ☐

Let us now prove Theorem 1.1. If $n=2m+1$, then the algebra with involution $(Q,\gamma_Q)^{\otimes n}$ is isomorphic to $(Q,\gamma_Q)\otimes(\mathrm{End}_F(Q),\mathrm{ad}_{n_Q})^{\otimes m}$, where ad_{n_Q} denotes the adjoint involution with respect to the quadratic form n_Q. Indeed, one may easily check that $(Q\otimes Q,\gamma_Q\otimes\gamma_Q)$ is isomorphic to $\big(\mathrm{End}_F(Q),\mathrm{ad}_{T_{(Q,\gamma_Q)}}\big)$, where $T_{(Q,\gamma_Q)}$ is the quadratic form defined by $T_{(Q,\gamma_Q)}(x)=\mathrm{Trd}_Q(x\gamma_Q(x))$. Since for any $x\in Q$, we have $x\gamma_Q(x)=n_Q(x)\in F$, $T_{(Q,\gamma_Q)}=\langle 2\rangle n_Q$, and $(Q^{\otimes 2},\gamma_Q^{\otimes 2})\simeq(\mathrm{End}_F(Q),\mathrm{ad}_{n_Q})$. Therefore, to prove Theorem 1.1, it suffices to show that the algebras with involution $(Q,\gamma_Q)\otimes(C,\sigma)$ and $(Q,\gamma_Q)\otimes(\mathrm{End}_F(Q),\mathrm{ad}_{n_Q})^{\otimes m}$ are Witt-equivalent. We will use the following lemma:

Lemma 4.2. *Let (U,q) and (U',q') be two quadratic spaces over F. There exists an isomorphism*

$$(Q,\gamma_Q)\otimes(\mathrm{End}_F(U),\mathrm{ad}_q)\simeq(Q,\gamma_Q)\otimes(\mathrm{End}_F(U'),\mathrm{ad}_{q'})$$

if and only if the quadratic forms $n_Q\otimes q$ and $n_Q\otimes q'$ are similar.

Proof. Consider the right Q-vector space $U_Q = U \otimes_F Q$. The quadratic form q on U induces a hermitian form $h\colon U_Q \times U_Q \to Q$ (with respect to γ_Q) such that

$$h(u \otimes x, u' \otimes x') = \frac{1}{2}\big(q(u+u') - q(u) - q(u')\big)\gamma_Q(x)x'$$

for u, $u' \in U$ and x, $x' \in Q$. The adjoint involution ad_h satisfies

$$(\mathrm{End}_Q(U_Q), \mathrm{ad}_h) = (\mathrm{End}_F(U), \mathrm{ad}_q) \otimes (Q, \gamma_Q). \tag{4.3}$$

The trace form of h, which is by definition the quadratic form

$$U \otimes_F Q \to F,\ x \mapsto h(x,x),$$

is $q \otimes n_Q$. Similarly, we denote by h' the hermitian form induced by q'. By a theorem of Jacobson [13, 10.1.7], the hermitian modules (U_Q, h) and (U'_Q, h') are isomorphic if and only if their trace forms are isometric. Hence, if the quadratic forms $q \otimes n_Q$ and $q' \otimes n_Q$ are similar, i.e., $q \otimes n_Q \simeq \langle \mu \rangle q' \otimes n_Q$ for some $\mu \in F^*$, then the hermitian forms h and $\langle\mu\rangle h'$ are isomorphic, which proves that

$$(Q, \gamma_Q) \otimes (\mathrm{End}_F(U), \mathrm{ad}_q) \simeq (Q, \gamma_Q) \otimes (\mathrm{End}_F(U'), \mathrm{ad}_{q'}).$$

Conversely, if there is such an isomorphism, then equation (4.3) shows that the hermitian forms h and h' are similar, hence their trace forms $q \otimes n_Q$ and $q' \otimes n_Q$ also are similar. □

These two lemmas reduce the proof of Theorem 1.1 to showing that the quadratic forms $n_Q \otimes \sum_{\substack{0 \le k < n \\ k \text{ even}}} t_k$ and $n_Q^{\otimes(m+1)}$ are Witt-equivalent, up to a scalar factor.
On the one hand, we have $n_Q^{\otimes(m+1)} = 4^m n_Q$, since $n_Q^{\otimes 2} = 4 n_Q$. On the other hand, since the algebra B is split by an odd-degree field extension, Springer's Theorem [8, VII.2.3] shows that t_k is isometric to the trace form of

$$\lambda^k(M_n(F)) = M_{\binom{n}{k}}(F)$$

which is Witt-equivalent to $\binom{n}{k}\langle 1 \rangle$. Hence the Witt class of $n_Q \otimes \sum_{\substack{0 \le k < n \\ k \text{ even}}} t_k$ is

$$\sum_{\substack{0 \le k < n \\ k \text{ even}}} \binom{n}{k} n_Q = 2^{n-1} n_Q = 4^m n_Q,$$

which completes the proof of Theorem 1.1.

5 THE n EVEN CASE

In this section, we prove Theorems 1.3, 1.4, and Corollary 1.5.

Assume from now on that n is even and write $n = 2m$. Consider the element of $\lambda^n(M_2(B_K))$

$$h = \alpha(1 - b^{-m}g)(\ell_0 + \cdots + \ell_{m-1} + \tfrac{1}{2}\ell_m) + (1 + b^{-m}g)(\tfrac{1}{2}\ell_m + \ell_{m+1} + \cdots + \ell_n).$$

One can check that

$$h^{-1} = \tfrac{1}{2}\left((\alpha^{-1} + b^{-m}g)(\ell_0 + \cdots + \ell_m) + (1 - b^{-m}g\alpha^{-1})(\ell_m + \cdots + \ell_n)\right)$$

and $g = b^m \, h\overline{h}^{-1}$.
Therefore, it follows from (3.1) that

$$\lambda^n(Q \otimes B) = h\lambda^n M_2(B)h^{-1} \subset \lambda^n M_2(B)_K.$$

Using the isomorphism Φ of Theorem 2.5 as an identification, we then have

$$\lambda^n(Q \otimes B) = \operatorname{End}_F\left(h(\lambda^0 B) \oplus \cdots \oplus h(\lambda^n B)\right),$$

and the canonical involution on $\lambda^n(Q \otimes B)$ is adjoint to the restriction of the bilinear form T_K to the F-subspace $h(\lambda^0 B) \oplus \cdots \oplus h(\lambda^n B)$. This restriction is given by the following formula:

Lemma 5.1. *The F-subspaces $h(\lambda^k B)$ are pairwise orthogonal. Moreover, for u, $v \in \lambda^k B$ we have*

$$T_K\left(h(u), h(v)\right) = \begin{cases} -2a(-1)^k b^{m-k} \operatorname{Trd}_{\lambda^k B}(uv) & \textit{if } k < m, \\ (-1)^m \Big(\frac{1+a}{2} \operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)v\big) + \frac{1-a}{2} \operatorname{Trd}_{\lambda^m B}(uv)\Big) & \textit{if } k = m, \\ 2(-1)^k b^{m-k} \operatorname{Trd}_{\lambda^k B}(uv) & \textit{if } k > m. \end{cases}$$

Proof. Using Lemmas 2.6 and 2.8(1), one may easily check that for any $u \in \lambda^k B$, we have

$$h(u) = \begin{cases} \alpha(u - b^{m-k}\gamma_k(u)) & \text{if } k < m, \\ \frac{1}{2}\big[(1+\alpha)u + (1-\alpha)\gamma_k(u)\big] & \text{if } k = m, \\ u + b^{m-k}\gamma_k(u) & \text{if } k > m. \end{cases}$$

The claim then follows from the description of T given in Theorem 2.5 and Lemma 2.8(1) by some direct computations. For instance, if $u, v \in \lambda^m B$, we get

$$T_K\big(h(u), h(v)\big) = (-1)^m \operatorname{Trd}_{\lambda^m B_K}\big[h(u)\gamma_m\big(h(v)\big)\big] \tag{5.2}$$

by Theorem 2.5, and

$$\begin{aligned} &h(u)\gamma_m\big(h(v)\big) = \\ &\tfrac{1}{4}\big[(1+\alpha)^2 u\gamma_m(v) + (1-a)\big(uv + \gamma_m(u)\gamma_m(v)\big) + (1-\alpha)^2\gamma_m(u)v\big]. \end{aligned} \tag{5.3}$$

Since $\operatorname{Trd}_{\lambda^m B}\big(u\gamma_m(v)\big) = \operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)v\big)$ and $\operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)\gamma_m(v)\big) = \operatorname{Trd}_{\lambda^m B}(uv)$, it follows that

$$\operatorname{Trd}_{\lambda^m B_K}\big[(1+\alpha)^2 u\gamma_m(v) + (1-\alpha)^2\gamma_m(u)v\big] = 2(1+a)\operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)v\big)$$

and

$$\operatorname{Trd}_{\lambda^m B_K}\big[(1-a)(uv+\gamma_m(u)\gamma_m(v))\big] = 2(1-a)\operatorname{Trd}_{\lambda^m B}(uv).$$

Therefore, (5.2) and (5.3) yield

$$T_K\big(h(u),h(v)\big) = (-1)^m\frac{1+a}{2}\operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)v\big) + (-1)^m\frac{1-a}{2}\operatorname{Trd}_{\lambda^m B}(uv).$$

□

This lemma provides a first description of the similarity class of q_A:

Proposition 5.4. *If n is even, the similarity class of q_A contains the quadratic form:*

$$\big(\oplus_{0\leq k<m}\langle 2(-1)^k b^{m-k}\rangle\langle 1,-a\rangle t_k\big)\oplus\langle(-1)^m\rangle(t_m^+\oplus\langle -a\rangle t_m^-).$$

Proof. Since the anti-isomorphism γ_k defines an isometry $t_k \simeq t_{n-k}$, the restriction of T_K to $h(\lambda^k B\oplus\lambda^{n-k}B)$, for all $k<m$, is

$$\langle 2(-1)^k b^{m-k}\rangle\langle 1,-a\rangle t_k.$$

Moreover, we have

$$\frac{1+a}{2}\operatorname{Trd}_{\lambda^m B}\big(\gamma_m(u)v\big) + \frac{1-a}{2}\operatorname{Trd}_{\lambda^m B}(uv) = \begin{cases}\operatorname{Trd}_{\lambda^m B}(uv) & \text{if } u\in\operatorname{Sym}(\lambda^m B,\gamma_m),\\ -a\operatorname{Trd}_{\lambda^m B}(uv) & \text{if } u\in\operatorname{Skew}(\lambda^m B,\gamma_m).\end{cases}$$

Hence, the proposition clearly follows from the lemma. □

5.5. Proof of Theorem 1.3.

Theorem 1.3 is a consequence of the preceding results in the special case where $Q=(a,b)_F$ is split. In that case, we may take $b=1$ so that the matrix $g_0=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ then decomposes as $g_0=f_0\bar f_0^{-1}$, where $f_0=\left(\begin{smallmatrix}1&-\alpha\\1&\alpha\end{smallmatrix}\right)$. Hence, if we let $f=\lambda^n f_0$, we have $g=f\bar f^{-1}$. On the other hand, we also have $g=h\bar h^{-1}$, for h as in the preceding section, hence $f^{-1}h=\overline{f^{-1}h}$, which means that $f^{-1}h\in\lambda^n\big(M_2(B)\big)$. Considering the isomorphism Φ of Theorem 2.5 as an identification as we did in the preceding section, we get that $f^{-1}h\in\operatorname{End}_F(\lambda^0 B\oplus\cdots\oplus\lambda^n B)$, hence

$$h(\lambda^0 B\oplus\cdots\oplus\lambda^n B) = f(\lambda^0 B\oplus\cdots\oplus\lambda^n B).$$

To prove Theorem 1.3, we compute the restriction of T_K to this F-subspace in two different ways. First, we use [7, (14.4)], which says that f is a similarity for T_K with similarity factor $\operatorname{Nrd}_{M_2(B_K)}(f_0) = (-2\alpha)^n = 2^n a^m$. Hence, for any $u, v \in \lambda^0 B \oplus \cdots \oplus \lambda^n B$, we have

$$T_K(f(u), f(v)) = 2^n a^m T(u, v).$$

By Remark 2.7 and Theorem 2.5, the form T is Witt-equivalent to its restriction to $\lambda^m B$, which is isometric to $\langle(-1)^m\rangle(t_m^+ \oplus \langle -1\rangle t_m^-)$.
Second, the restriction of T_K to $h(\lambda^0 B \oplus \cdots \oplus \lambda^n B)$ has been computed in Lemma 5.1 and the proof of Proposition 5.4. Comparing the results, we get that the quadratic forms

$$\big(\oplus_{0\le k<m}\langle 2(-1)^k\rangle\langle 1, -a\rangle t_k\big) \oplus \langle(-1)^m\rangle(t_m^+ \oplus \langle -a\rangle t_m^-)$$

and

$$\langle 2^n a^m\rangle\langle(-1)^m\rangle(t_m^+ \oplus \langle -1\rangle t_m^-)$$

are Witt-equivalent. If m is even, we get that the following equality holds in the Witt ring:

$$\Big(\sum\nolimits_{0\le k<m}\langle 2(-1)^k\rangle\langle 1, -a\rangle t_k\Big) + t_m^+ + \langle -a\rangle t_m^- = t_m^+ - t_m^-,$$

from which we deduce

$$\langle 1, -a\rangle \left(\Big(\sum\nolimits_{0\le k<m} \langle 2(-1)^k\rangle t_k\Big) + t_m^-\right) = 0.$$

To finish the proof, we may assume a is an indeterminate over the base field F. The previous equality then implies that the quadratic form

$$\Big(\bigoplus\nolimits_{0\le k<m} \langle 2(-1)^k\rangle t_k\Big) \oplus t_m^-$$

is hyperbolic, which proves the theorem in this case. A similar argument finishes the proof for the m odd case.

Remark 5.6. Let $t_{(\lambda^m B,\gamma_m)}\colon \lambda^m B \to F$ be the quadratic form

$$t_{(\lambda^m B,\gamma_m)}(x) = \operatorname{Trd}_{\lambda^m B}(\gamma_m(x)x).$$

Using Theorem 1.3, together with the facts that $t_{n-k} = t_k$, $t_{(\lambda^m B,\gamma_m)} = t_m^+ - t_m^-$, and that $2q \simeq 2\langle 2\rangle q$ for an arbitrary quadratic form q since $2\langle 2\rangle = 2\langle 1\rangle$, we obtain the following memorable formula:

$$\sum_{k=0}^{n}(-1)^k t_k = t_{(\lambda^m B,\gamma_m)} \qquad \text{in } WF.$$

5.7. PROOF OF THEOREM 1.4. Consider first the case where m is even. In that case, Theorem 1.3 yields

$$\sum\nolimits_{\substack{0\leq k<m\\ k\text{ even}}}\langle 2\rangle t_k + t_m^- = \sum\nolimits_{\substack{0\leq k<m\\ k\text{ odd}}}\langle 2\rangle t_k.$$

Substituting in the formula given in Proposition 5.4, we get that the similarity class of q_A contains a quadratic form whose Witt class is

$$\begin{aligned}\sum\nolimits_{\substack{0\leq k<m\\ k\text{ even}}}\langle 2,-2a\rangle t_k + \sum\nolimits_{\substack{0\leq k<m\\ k\text{ even}}}\langle -2b,2ab\rangle t_k + \langle -a,-b,ab\rangle t_m^- + t_m^+ \\ = \sum\nolimits_{\substack{0\leq k<m\\ k\text{ even}}}\langle 2\rangle n_Q t_k + t_m^+ - t_m^- + n_Q t_m^-.\end{aligned}$$

Now, suppose m is odd. Multiplying by $\langle a\rangle$ the quadratic form given in Proposition 5.4 does not change its similarity class, and shows that the similarity class of q_A contains a quadratic form whose Witt class is

$$\langle 1,-a\rangle\cdot\Bigl(t_m^+ + \sum\nolimits_{0\leq k<m}\langle 2(-b)^{k+1}\rangle t_k\Bigr) + t_m^- - t_m^+.$$

Substituting for t_m^+ the formula of Theorem 1.3 simplifies the expression in brackets to $\langle 1,-b\rangle\cdot\Bigl(\sum_{\substack{0\leq k<m\\ k\text{ even}}}\langle 2\rangle t_k\Bigr)$ and completes the proof.

5.8. PROOF OF COROLLARY 1.5. Let us assume that B is of exponent at most 2. Then, for any even k, the algebra $\lambda^k B$ is split. Hence, its trace form t_k is Witt-equivalent to $\binom{n}{k}$. Since m is even, $\lambda^m B$ is also split, and its canonical involution γ_m is adjoint to a quadratic form q_B. This form is only defined up to a scalar factor, but its square is defined up to isometry. Now [7, 11.4] gives relationships between q_B and the forms t_m^+ and t_m^-:

$$t_m^+ - t_m^- \simeq q_B^2 \qquad\text{and}\qquad -t_m^- \simeq \langle 1/2\rangle \wedge^2 q_B.$$

Hence, by Theorem 1.4, the similarity class of q_A contains a form whose Witt class is

$$q_B^2 + n_Q\Bigl(\langle -2\rangle(\wedge^2 q_B) + \sum\nolimits_{\substack{0\leq k<m\\ k\text{ even}}}\tbinom{n}{k}\langle 2\rangle\Bigr).$$

One may easily check that, since $\langle 2,2\rangle \simeq \langle 1,1\rangle$ and q_B is even-dimensional, $q_B^2 \simeq \langle 2\rangle q_B^2$. Since we are concerned only with the similarity class of q_A, we may therefore forget the factors $\langle 2\rangle$ throughout. Moreover, since m is even, $\sum_{\substack{0\leq k<m\\ k\text{ even}}}\binom{n}{k} = 2^{n-2} - \frac{1}{2}\binom{n}{m}$, and Corollary 1.5 follows.

6 ANOTHER APPROACH TO THE n EVEN CASE

Let us decompose $B = B_0\otimes B_1$, where $\deg B_0 = 2m_0$ is a power of 2 and $\deg B_1 = m_1$ is odd. We have $m = m_0 m_1$, and m is even if and only if $m_0 > 1$.

We write T_0 for the trace form of B_0. Under the assumption that $B_0^{\otimes 2}$ is split (which is automatic if m is odd), we will give a different characterization of q_A for $A = Q \otimes B$ than the one in Theorem 1.4. Corollaries 1.6 and 1.7 will follow from this.

Proposition 6.1. *Suppose that $B_0^{\otimes 2}$ is split. Then the similarity class of q_A contains a form whose Witt class is*

$$2^{n-1} + \frac{2^{n-3}}{m_0} T_0 (n_Q - 2) \text{ if } m \text{ is even}$$

and

$$2^{n-2}(n_Q - n_{B_0}) \text{ if } m \text{ is odd.}$$

(Note that B_0 is a quaternion algebra if m is odd.)

This result is already known for m odd: If A is a biquaternion algebra (i.e., $m = 1$) it is [3, 6.2], and in general it follows from [3, 6.4] by a straightforward computation, using the fact that for any integer $k \geq 1$, one has $n_Q^k = 2^{2(k-1)} n_Q$. However, the results from [3] make use of Clifford algebras, which seems a long way to go. So we include a direct proof.
We start with a lemma.

Lemma 6.2. *Suppose that $B_0^{\otimes 2}$ is split. Then the quadratic form t_k is Witt-equivalent to $\binom{n}{k}$ if k is even and $\frac{1}{2m_0}\binom{n}{k} T_0$ if k is odd. Moreover, we have:*

$$t_m^- = \frac{2^{n-3}}{m_0} \langle 2 \rangle T_0 - \Big(2^{n-2} - \tfrac{1}{2}\tbinom{n}{m}\Big)\langle 2 \rangle \text{ if } m \text{ is even,}$$

and

$$t_m^+ = 2^{n-2}\langle 2 \rangle - \Big(2^{n-3} - \tfrac{1}{4}\tbinom{n}{m}\Big)\langle 2 \rangle T_0 \quad \text{if } m \text{ is odd.}$$

This lemma actually specifies t_m^+ and t_m^- whatever the parity of m since in both cases $t_m = t_m^+ + t_m^-$, and t_m is known.

Proof. Since B_1 is split by an odd-degree field extension, Springer's Theorem shows that t_k is isometric to the trace form of $\lambda^k\big(B_0 \otimes M_{m_1}(F)\big)$. If k is even, this algebra is split, and the result is clear. If k is odd, the algebra is Brauer-equivalent to B_0, hence isomorphic to $M_p(F) \otimes B_0$, where $p = \frac{1}{2m_0}\binom{n}{k}$. The form of t_k for k odd then follows from the fact that the trace form of a tensor product of central simple algebras is isometric to the product of the trace forms of each factor.
We have $m = m_0 m_1$, and m is odd if and only if $m_0 = 1$. Recall that

$$\sum_{\substack{0 \leq k < m \\ k \text{ even}}} \binom{n}{k} = \begin{cases} 2^{n-2} & \text{if } m \text{ is odd,} \\ 2^{n-2} - \frac{1}{2}\binom{n}{m} & \text{if } m \text{ is even,} \end{cases}$$

and

$$\sum_{\substack{0\leq k<m\\ k \text{ odd}}}\binom{n}{k}=\begin{cases}2^{n-2}-\frac{1}{2}\binom{n}{m} & \text{if } m \text{ is odd,}\\ 2^{n-2} & \text{if } m \text{ is even.}\end{cases}$$

The second part of the lemma then follows from Theorem 1.3 by a direct computation. □

Let us now prove Proposition 6.1. Assume first that m is even. The preceding lemma yields

$$t_m^- + \sum_{\substack{0\leq k<m\\ k \text{ even}}}\langle 2\rangle t_k = \frac{2^{n-3}}{m_0}\langle 2\rangle T_0$$

and

$$t_m^+ - t_m^- = \binom{n}{m} - 2t_m^- = 2^{n-1}\langle 2\rangle - \frac{2^{n-2}}{m_0}\langle 2\rangle T_0 + \binom{n}{m}\langle 1,-2\rangle.$$

Since $\binom{n}{m}$ is even, the last term on the right side vanishes, hence the quadratic form given by Theorem 1.4 is

$$\langle 2\rangle\Big(2^{n-1} - \frac{2^{n-2}}{m_0}T_0 + \frac{2^{n-3}}{m_0}n_Q T_0\Big).$$

This finishes the m even case.

Assume now that m is odd. Then, B_0 is a quaternion algebra, and $T_0 = \langle 2\rangle(2 - n_{B_0})$. The preceding lemma yields

$$\sum_{\substack{0\leq k<m\\ k \text{ even}}}\langle 2\rangle t_k = 2^{n-2}\langle 2\rangle$$

and

$$t_m^- - t_m^+ = \tfrac{1}{2}\binom{n}{m}T_0 - 2t_m^+ = \tfrac{1}{2}\binom{n}{m}T_0 - 2^{n-1}\langle 2\rangle + \Big(2^{n-2} - \tfrac{1}{2}\binom{n}{m}\Big)\langle 2\rangle T_0.$$

If $m = 1$, then this reduces to $t_m^- - t_m^+ = -\langle 2\rangle n_{B_0}$, and Theorem 1.4 gives the desired result. Otherwise, since m is odd and $m \geq 3$, the integer $2^{n-2} - \frac{1}{2}\binom{n}{m}$ is even, by [7, (10.29)], hence $\big(2^{n-2} - \frac{1}{2}\binom{n}{m}\big)\langle 2\rangle = 2^{n-2} - \frac{1}{2}\binom{n}{m}$ and the right side of the last displayed equation simplifies to yield

$$t_m^- - t_m^+ = -2^{n-2}\langle 2\rangle n_{B_0}.$$

Therefore, the quadratic form given by Theorem 1.4 is $2^{n-2}\langle 2\rangle(n_Q - n_{B_0})$, which is isometric to $2^{n-2}(n_Q - n_{B_0})$ since $2^{n-2}\langle 2\rangle = 2^{n-2}$, and the proof of Proposition 6.1 is complete.

6.3. PROOF OF COROLLARY 1.6. Corollary 1.6 can be proved by induction, using the formula given in Corollary 1.5, but it can also be directly deduced from Proposition 6.1. Indeed, let us assume $A = A_r = Q_1 \otimes \cdots \otimes Q_r$ is a product of $r \geq 3$ quaternion algebras. We let $B = Q_2 \otimes \cdots \otimes Q_r$. Its degree $n = 2^{r-1}$ is a power of 2, and since $r \geq 3$, $m = 2^{r-2}$ is even. In the notation from earlier in this previous section, we have $B_0 = B$ and $B_0^{\otimes 2}$ is split. Hence, we may apply Proposition 6.1. The form T_0 is the trace form of B, that is the tensor product of the trace forms of the quaternion algebras Q_i for $i = 2, \ldots, r$. Hence, we have $T_0 = \langle 2^{r-1}\rangle(2 - n_{Q_2}) \cdots (2 - n_{Q_r})$, and Proposition 6.1 tells us that the similarity class of q_A contains a form whose Witt class is

$$\begin{aligned} 2^{n-1} + \frac{2^{n-3}}{2^{r-2}}\langle 2^{r-1}\rangle(n_{Q_1} - 2)(2 - n_{Q_2}) \cdots (2 - n_{Q_r}) = \\ = 2^{n-1}\langle 2^{r-1}\rangle - 2^{n-r-1}\langle 2^{r-1}\rangle(2 - n_{Q_1})(2 - n_{Q_2}) \cdots (2 - n_{Q_r}) \\ = \langle 2^{r-1}\rangle 2^{n-r-1}\big(2^r - (2 - n_{Q_1}) \cdots (2 - n_{Q_r})\big), \end{aligned}$$

which proves the corollary.

6.4. Proof of Corollary 1.7. Let us now consider a central simple algebra A as in the statement of Corollary 1.7. Then A is isomorphic to $M_k(A_r)$, where $A_r = Q_1 \otimes \cdots \otimes Q_r$ is a product of r quaternion algebras. If A is split then q_A is hyperbolic and the result is clear, so we may assume that $r \neq 0$. Because $\deg A \equiv 0 \mod 4$ by hypothesis, we may further assume that $r \neq 1$ (so that $r \geq 2$), with perhaps some of the Q_i being split.

We first treat the $k = 1$ case. If $r = 2$, then A is biquaternion algebra and q_A is an Albert form, which lies in I^2F. If $r \geq 3$, then by Corollary 1.6 we have to prove that

$$2^{n-1} - 2^{n-r-1}(2 - n_{Q_1}) \cdots (2 - n_{Q_r})$$

lies in I^nF. When we expand this product, the terms of the form 2^{n-1} cancel, and we are left with a sum of terms of the form $\pm 2^{n-\ell-1} n_{Q_{i_1}} \cdots n_{Q_{i_\ell}}$, where $\ell \geq 1$. Since for any i the form n_{Q_i} lies in I^2F, $2^{n-\ell-1} n_{Q_{i_1}} \cdots n_{Q_{i_\ell}}$ belongs to $I^{n-\ell-1+2\ell}F = I^{n+\ell-1}F$, and hence to I^nF.

Now suppose that $k \geq 2$. Since $r \geq 2$, we have $\deg(A_r) \equiv 0 \mod 4$ and we can apply [3, 6.3(1)]. Hence, the similarity class of q_A contains a form which is Witt-equivalent to $q_{A_r}^{\otimes k}$. Since the result holds for A_r by the $k = 1$ case, we are done.

Acknowledgments

The first author would like to thank ETH Zürich for its hospitality while some of the research for this paper was conducted. The second and third authors are partially supported by the European Commission under the TMR contract ERB-FMRX-CT97-0107. The third author is partially supported by the National Fund for Scientific Research (Belgium).

References

[1] I. Dejaiffe, D. Lewis, and J.-P. Tignol, *Witt equivalence of central simple algebras with involution*, Rend. Circ. Mat. Palermo, Ser. II 49 (2000), 325–342.

[2] R. Elman, T.-Y. Lam, *Classification theorems for quadratic forms over fields*, Comment. Math. Helv. 49 (1974), 373–381.

[3] R.S. Garibaldi, *Clifford algebras of hyperbolic involutions*, Math. Zeit. 236 (2001), 321–349 [DOI `10.1007/s002090000180`].

[4] F. Grosshans, *Orthogonal representations of algebraic groups*, Trans. Amer. Math. Soc. 137 (1969), 519–532. Corrected in Trans. Amer. Math. Soc. 144 (1969), 571.

[5] ______, *Real orthogonal representations of algebraic groups*, Trans. Amer. Math. Soc. 160 (1971), 343–352.

[6] B. Jacob, *Indecomposable division algebras of prime exponent*, J. Reine Angew. Math. 413 (1991), 181–197.

[7] M.-A. Knus, A.S. Merkurjev, M. Rost, and J.-P. Tignol, *The book of involutions*, Colloquium Publications, vol. 44, AMS, Providence, RI, 1998.

[8] T.Y. Lam, *The algebraic theory of quadratic forms*, Benjamin, Reading, MA, 1973.

[9] A.S. Merkurjev, *Simple algebras and quadratic forms*, Math. USSR Izv. 38 (1992), no. 1, 215–221.

[10] A. Quéguiner and J.-P. Tignol, *Clifford and discriminant algebras*, preprint, 2001.

[11] H. Samelson, *Notes on Lie algebras*, second edition, Springer-Verlag, New York, 1990.

[12] I. Satake, *Symplectic representations of algebraic groups satisfying a certain analyticity condition*, Acta Math. 117 (1967), 215–279.

[13] W. Scharlau, *Quadratic and hermitian forms*, Grund. math. Wiss., vol. 270, Springer, Berlin-New York, 1985.

[14] J. Tits, *Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque*, J. Reine Angew. Math. 247 (1971), 196–220.

R. Skip Garibaldi
UCLA, Dept. of Mathematics,
Los Angeles, CA 90095-1555,
USA
skip@member.ams.org
http://www.math.ucla.edu/~skip/

Anne Quéguiner-Mathieu
UMR CNRS 7539,
Département de Mathématiques,
Université Paris 13,
F-93430 Villetaneuse,
France
queguin@math.univ-paris13.fr

Jean-Pierre Tignol
Départment de Mathématiques,
Université Catholique de Louvain,
B-1348 Louvain-la-Neuve,
Belgium
tignol@agel.ucl.ac.be
http://www.math.ucl.ac.be/tignol/