THE ASYMMETRY OF AN ANTI-AUTOMORPHISM

ANNE CORTELLA AND JEAN-PIERRE TIGNOL

Abstract. The asymmetry of a nonsingular pairing on a vector space is an endomorphism of the space on which the classification of arbitrary pairings (not necessarily symmetric or skew-symmetric) is based. A general notion of asymmetry is defined for arbitrary anti-automorphisms on a central simple algebra, and conditions are given to characterize the elements which are the asymmetries of some anti-automorphism. The asymmetry is used to define the determinant of an anti-automorphism.

Introduction

The asymmetry of an arbitrary nonsingular pairing (not necessarily symmetric or skew-symmetric) on a finite-dimensional vector space V is an invertible endomorphism of V which is an important invariant of the pairing. It is 1 if and only if the pairing is symmetric and -1 if and only if it is skew-symmetric. This invariant was first considered by Williamson [9], and more recently by Riehm [6].

In the present paper, we determine under which conditions a linear map $a \in \mathrm{GL}(V)$ is the asymmetry of some nonsingular pairing on V: the map a must be conjugate to its inverse and satisfy some conditions on the generalized eigenspaces of eigenvalues $+1$ and -1, see Theorem 1. As pointed out by Ranicki, the property that a is an asymmetry could be rephrased by saying that a certain asymmetric Poincaré complex of dimension 1 is round simple null-cobordant. (See [5, Ch. 20] for background information on Poincaré complexes.)

In section 2, we define the asymmetry of an anti-automorphism σ on a central simple algebra A: it is an element $a_\sigma \in A^\times$ which is mapped, under scalar extension to a splitting field of A, to the asymmetry of any nonsingular pairing to which σ is adjoint. It is defined up to sign by the properties that $\sigma^2(x) = a_\sigma x a_\sigma^{-1}$ for all $x \in A$ and that $\sigma(a_\sigma) = a_\sigma^{-1}$. This element was incidentally used by Saltman [7, Lemma 3.3, Theorem 4.4] to show that if an Azumaya algebra A carries an anti-automorphism, then the ring of 2×2 matrices $M_2(A)$ carries an involution, and that Azumaya algebras over connected semilocal rings which are isomorphic to their opposite have an involution. We show that in a central simple algebra of exponent 2, an invertible element is the asymmetry of some anti-automorphism if and only if it is conjugate to its inverse (Theorem 2). Albert's theorem that every central simple algebra of exponent 2 has an involution is an immediate consequence, since involutions are the anti-automorphisms of asymmetry ± 1. In the final section, the asymmetry is used to define the determinant of an anti-automorphism.

Date: July 1, 2000.

The authors warmly thank Andrew Ranicki for his comments on an earlier version of this paper. They gratefully acknowledge support from the FNRS–CNRS cooperation agreement and from the TMR network "K-theory and linear algebraic groups" (contract ERB FMRX CT 97-0107). The second author is partially supported by the National Fund for Scientific Research (Belgium).

1. The asymmetry of a nonsingular pairing

Throughout this section, V denotes a finite-dimensional vector space over an arbitrary field F. We define the asymmetry and the adjoint anti-automorphism of a nonsingular pairing on V, and determine which linear transformations of V are asymmetries.

1.1. **Definitions.** Let $V^* = \mathrm{Hom}_F(V,F)$ be the dual of V. Every pairing (or bilinear form) $b\colon V\times V\to F$ induces a linear map $\hat{b}\colon V\to V^*$ which carries $x\in V$ to $b(x,\bullet)\in V^*$. The transpose map $\hat{b}^t\colon V=V^{**}\to V^*$ carries $x\in V$ to $b(\bullet,x)\in V^*$.

Proposition 1. *For a pairing b on V, the following conditions are equivalent:*

(a) *if $x\in V$ is such that $b(x,y)=0$ for all $y\in V$, then $x=0$;*
(b) *if $y\in V$ is such that $b(x,y)=0$ for all $x\in V$, then $y=0$;*
(c) *the map $\hat{b}$ is bijective.*

If these conditions hold, the pairing b is called *nonsingular*.

Proof. Condition (a) is equivalent to injectivity of $\hat{b}$, and (b) to injectivity of $\hat{b}^t$, hence also to surjectivity of $\hat{b}$. Since $\dim V=\dim V^*$, each of these conditions implies that $\hat{b}$ is bijective. □

All the pairings considered in the sequel are nonsingular. To every nonsingular pairing b on V we attach an anti-automorphism σ_b of $\mathrm{End}_F V$ and a linear transformation $a_b\in\mathrm{GL}(V)$ as follows:

Proposition 2. *Let b be a nonsingular pairing on V. There is a unique map $\sigma_b\colon \mathrm{End}_F V\to\mathrm{End}_F V$ and a unique map $a_b\colon V\to V$ such that*

$$b\big(f(x),y\big)=b\big(x,\sigma_b(f)(y)\big)\qquad \text{for all } x,\ y\in V,\ f\in\mathrm{End}_F V \tag{1}$$

and

$$b(x,y)=b\big(y,a_b(x)\big)\qquad\text{for all } x,\ y\in V. \tag{2}$$

The map σ_b is an F-linear anti-automorphism of $\mathrm{End}_F V$ and the map a_b is linear and invertible. These maps satisfy the following properties:

(i) *$\sigma_b^2(f)=a_b\circ f\circ a_b^{-1}$ for all $f\in\mathrm{End}_F V$;*
(ii) *$\sigma_b(a_b)=a_b^{-1}$.*

Proof. For $f\in\mathrm{End}_F V$, let $\sigma_b(f)=(\hat{b}\circ f\circ\hat{b}^{-1})^t$. Equality (1) is easily checked, and the fact that σ_b is an F-linear anti-automorphism of $\mathrm{End}_F V$ follows. Uniqueness of σ_b follows from the hypothesis that b is nonsingular.

On the other hand, let $a_b=(\hat{b}^t)^{-1}\circ\hat{b}$. This map is clearly linear and invertible, and it satisfies (2). Uniqueness of a_b is clear. To check the additional properties, observe that for $f\in\mathrm{End}_F V$

$$\sigma_b^2(f)=\big(\hat{b}\circ(\hat{b}\circ f\circ\hat{b}^{-1})^t\circ\hat{b}^{-1}\big)^t=\big((\hat{b}^t)^{-1}\circ\hat{b}\big)\circ f\circ\big((\hat{b}^t)^{-1}\circ\hat{b}\big)^{-1}$$

and

$$\sigma_b\big((\hat{b}^t)^{-1}\circ\hat{b}\big)=\big(\hat{b}\circ\big((\hat{b}^t)^{-1}\circ\hat{b}\big)\circ\hat{b}^{-1}\big)^t=\big((\hat{b}^t)^{-1}\circ\hat{b}\big)^{-1}.$$

□

We call σ_b the anti-automorphism *adjoint* to b. Using the Skolem-Noether theorem, it is easily seen that every F-linear anti-automorphism of $\operatorname{End}_F V$ is adjoint to some nonsingular pairing, see [4, p. 1]. The map a_b is called the *asymmetry* of b. From the definition, it is clear that the adjoint anti-automorphism and the asymmetry of any scalar multiple of b are the same as those of b. Moreover, the map a_b is determined up to sign by properties (i) and (ii).

We combine a_b and σ_b into a linear involution of $\operatorname{End}_F V$ as follows:

Proposition 3. *Let b be a nonsingular pairing on V. There is a unique linear map $\gamma_b\colon \operatorname{End}_F V \to \operatorname{End}_F V$ such that*

$$b\big(x, f(y)\big) = b\big(y, \gamma_b(f)(x)\big) \qquad \text{for all } x,\ y \in V,\ f \in \operatorname{End}_F V. \tag{3}$$

This map satisfies the following additional properties:

(i) $\gamma_b\big(f\circ g\circ h\big) = \sigma_b(h)\circ\gamma_b(g)\circ\sigma_b^{-1}(f)$ *for $f,\ g,\ h \in \operatorname{End}_F V$;*
(ii) $\gamma_b^2 = \operatorname{Id}_{\operatorname{End} V}$*;*
(iii) $\gamma_b(\operatorname{Id}_V) = a_b$*.*

Proof. Set $\gamma_b(f) = \sigma_b(f)\circ a_b$ $(= a_b\circ\sigma_b^{-1}(f))$ for $f \in \operatorname{End}_F V$; then (iii) is clear and (3), (i), (ii) follow from the properties of σ_b and a_b. □

We call γ_b the *linear involution* of $\operatorname{End}_F V$ associated to b. As for the adjoint anti-automorphism σ_b and the asymmetry a_b, it is clear that γ_b is also the linear involution associated to any scalar multiple of b.

Remark. There are corresponding notions for pairings on faithfully projective modules with values in invertible modules (over an arbitrary commutative ring R): see [3, Chap. III, (8.2)].

1.2. **Characterization of asymmetries.** The goal of this subsection is to answer the following question: Under which conditions on a map $a \in \operatorname{GL}(V)$ does there exist a nonsingular pairing b on V whose asymmetry is a, i.e., such that $a_b = a$? Identifying $\operatorname{End}_F V$ with a matrix algebra $M_n(F)$ through the choice of a basis of V, this amounts to asking for which invertible matrices $a \in \operatorname{GL}_n(F)$ the equation $a = (x^t)^{-1}x$ has a solution $x \in \operatorname{GL}_n(F)$, in view of the definition of a in terms of $\hat{b}$ in the proof of Proposition 2.

The conditions involve the following vector spaces: for an arbitrary integer $m \geq 1$ and $\varepsilon = \pm 1$, we let

$$V_m^{\varepsilon} = \frac{\ker(a-\varepsilon\operatorname{Id}_V)^m}{\ker(a-\varepsilon\operatorname{Id}_V)^{m-1} + (a-\varepsilon\operatorname{Id}_V)\big(\ker(a-\varepsilon\operatorname{Id}_V)^{m+1}\big)}.$$

Theorem 1. *Suppose* $\operatorname{char} F \neq 2$. *A map $a \in \operatorname{GL}(V)$ is the asymmetry of some nonsingular pairing on V if and only if the following conditions hold:*

(1) *a is conjugate to a^{-1} in* $\operatorname{GL}(V)$*;*
(2) *for every even integer m,* $\dim V_m^{+1}$ *is even;*
(3) *for every odd integer m,* $\dim V_m^{-1}$ *is even.*

If $\operatorname{char} F = 2$*, a map $a \in \operatorname{GL}(V)$ is the asymmetry of some nonsingular pairing on V if and only if conditions* (1) *and* (2) *hold.*

Proof. We first show that the conditions are necessary. Suppose b is a nonsingular pairing on V such that $a_b = a$. Proposition 2 shows that $\sigma_b(a) = a^{-1}$. To see how this equality implies condition (1), we argue in terms of matrices. Using a basis of V, we identify $\operatorname{End}_F V$ with the matrix algebra $M_n(F)$. Since the transpose map t is an anti-automorphism, $\sigma_b \circ t$ is a linear automorphism of $M_n(F)$, hence the Skolem-Noether theorem yields an invertible matrix u such that $\sigma_b \circ t$ is the conjugation by u. Then $\sigma_b(x) = ux^t u^{-1}$ for all $x \in M_n(F)$. In particular, since $\sigma_b(a) = a^{-1}$ it follows that a^{-1} is conjugate to a^t. But it is well-known that every matrix is conjugate to its transpose, hence condition (1) is proved.

To show that conditions (2) and (3) are necessary if $\operatorname{char} F \neq 2$, we show that the nonsingular pairing b induces a nonsingular skew-symmetric pairing on V_m^{+1} if m is even and on V_m^{-1} if m is odd. Conditions (2) and (3) follow because only even-dimensional vector spaces carry nonsingular skew-symmetric pairings if the characteristic of the base field is different from 2.

Fix some integer m and $\varepsilon = \pm 1$. For the convenience of notation, we let

$$U_m^\varepsilon = \ker(a - \varepsilon \operatorname{Id}_V)^m,$$

so $V_m^\varepsilon = U_m^\varepsilon / \big(U_{m-1}^\varepsilon + (a - \varepsilon \operatorname{Id}_V)(U_{m+1}^\varepsilon)\big)$. For $x, y \in U_m^\varepsilon$, define

$$b_m^\varepsilon(x,y) = b\big(x, (a - \varepsilon \operatorname{Id}_V)^{m-1}(y)\big).$$

Since $y \in U_m^\varepsilon$, we have

$$a \circ (a - \varepsilon \operatorname{Id}_V)^{m-1}(y) = \varepsilon (a - \varepsilon \operatorname{Id}_V)^{m-1}(y), \tag{4}$$

hence

$$\begin{aligned} b\big(y, (a - \varepsilon \operatorname{Id}_V)^{m-1}(x)\big) &= \varepsilon b\big(y, a \circ (a - \varepsilon \operatorname{Id}_V)^{m-1}(x)\big) \\ &= \varepsilon b\big((a - \varepsilon \operatorname{Id}_V)^{m-1}(x), y\big). \end{aligned} \tag{5}$$

On the other hand, equality (4) yields

$$(a - \varepsilon \operatorname{Id}_V)^{m-1}(y) = (\varepsilon a^{-1})^{m-1}(a - \varepsilon \operatorname{Id}_V)^{m-1}(y) = (-1)^{m-1}\sigma_b(a - \varepsilon \operatorname{Id}_V)^{m-1}(y),$$

hence

$$b\big((a - \varepsilon \operatorname{Id}_V)^{m-1}(x), y\big) = (-1)^{m-1} b\big(x, (a - \varepsilon \operatorname{Id}_V)^{m-1}(y)\big). \tag{6}$$

Comparing (5) and (6), we obtain

$$b_m^\varepsilon(y,x) = (-1)^{m-1}\varepsilon b_m^\varepsilon(x,y).$$

Therefore, b_m^ε is a skew-symmetric bilinear form on U_m^ε if $\varepsilon = +1$ and m is even, and also if $\varepsilon = -1$ and m is odd.

To see that b_m^ε induces a nonsingular pairing on V_m^ε, we consider the radical of b_m^ε, which is

$$\operatorname{rad} b_m^\varepsilon = \big\{ x \in U_m^\varepsilon \mid b(x,z) = 0 \text{ for all } z \in (a - \varepsilon \operatorname{Id}_V)^{m-1}(U_m^\varepsilon) \big\}.$$

Thus, $\operatorname{rad} b_m^\varepsilon$ is the intersection of U_m^ε with the orthogonal[1] complement for the form b of

$$(a - \varepsilon \operatorname{Id}_V)^{m-1}(U_m^\varepsilon) = \operatorname{im}(a - \varepsilon \operatorname{Id}_V)^{m-1} \cap \ker(a - \varepsilon \operatorname{Id}_V),$$

which is $\ker \sigma_b(a - \varepsilon \operatorname{Id}_V)^{m-1} + \operatorname{im} \sigma_b(a - \varepsilon \operatorname{Id}_V)$. Since $\sigma_b(a) = a^{-1}$, we have $\ker \sigma_b(a - \varepsilon \operatorname{Id}_V)^{m-1} = \ker(a - \varepsilon \operatorname{Id}_V)^{m-1}$ and $\operatorname{im} \sigma_b(a - \varepsilon \operatorname{Id}_V) = \operatorname{im}(a - \varepsilon \operatorname{Id}_V)$,

[1] If b is not symmetric nor skew-symmetric, one has to distinguish orthogonality on the left and on the right; the orthogonal complements of a-invariant subspaces coincide, however.

hence

$$\begin{aligned}\operatorname{rad} b_m^\varepsilon &= \big(U_{m-1}^\varepsilon + \operatorname{im}(a-\varepsilon\operatorname{Id}_V)\big)\cap U_m^\varepsilon\\ &= U_{m-1}^\varepsilon + \big(\operatorname{im}(a-\varepsilon\operatorname{Id}_V)\cap U_m^\varepsilon\big)\\ &= U_{m-1}^\varepsilon + (a-\varepsilon\operatorname{Id}_V)(U_{m+1}^\varepsilon).\end{aligned}$$

Therefore, b_m^ε induces a nonsingular pairing on $U_m^\varepsilon/\big(U_{m-1}^\varepsilon + (a-\varepsilon\operatorname{Id}_V)(U_{m+1}^\varepsilon)\big) = V_m^\varepsilon$.

Suppose now $\operatorname{char} F = 2$. The arguments above still show that b_m^ε induces a nonsingular bilinear pairing on V_m^ε, but in characteristic 2 skew-symmetric pairings are symmetric, hence we cannot conclude that $\dim V_m^\varepsilon$ is even. To show that $\dim V_m^{+1}$ is even if m is even, we show that b_m^{+1} is in fact alternating if m is even. For $x\in U_m^{+1}$ we have

$$(a-\operatorname{Id}_V)^{m-2}(x)\in\ker(a-\operatorname{Id}_V)^2 = \ker(a^2-\operatorname{Id}_V),$$

hence $a^2\circ(a-\operatorname{Id}_V)^{m-2}(x) = (a-\operatorname{Id}_V)^{m-2}(x)$. Since m is even, we obtain by induction

$$a^{m-2}\circ(a-\operatorname{Id}_V)^{m-2}(x) = (a-\operatorname{Id}_V)^{m-2}(x),$$

hence

$$(a-\operatorname{Id}_V)^{m-2}(x) = a^{2-m}\circ(a-\operatorname{Id}_V)^{m-2}(x) = \sigma(a-\operatorname{Id}_V)^{m-2}(x).$$

Therefore,

$$b\big(x,(a-\operatorname{Id}_V)^{m-2}(x)\big) = b\big((a-\operatorname{Id}_V)^{m-2}(x),x\big) = b\big(x,a\circ(a-\operatorname{Id}_V)^{m-2}(x)\big).$$

It follows that $b\big(x,(a-\operatorname{Id}_V)^{m-1}(x)\big)=0$, hence b_m^{+1} is alternating. This completes the proof that the conditions are necessary.

To prove that the conditions are sufficient, we shall make V into a module over the ring $F[X,X^{-1}]$ of Laurent polynomials in one indeterminate X. As a preparation, we make some observations on the prime ideals of this principal ideal domain.

Let J be the automorphism of $F[X,X^{-1}]$ which maps X to X^{-1}. We also denote by J the extension of this automorphism to the field of fractions $F(X)$ and to the factor module $E = F(X)/F[X,X^{-1}]$. Every prime ideal $P\subset F[X,X^{-1}]$ is generated by an irreducible polynomial of the form

$$\pi = a_0 + a_1X + \cdots + a_dX^d \in F[X]$$

such that a_0, $a_d\neq 0$. If $P^J = P$, the Laurent polynomials π, π^J differ by a factor which is invertible in $F[X,X^{-1}]$, hence $\pi = \alpha X^d\pi^J$ for some $\alpha\in F^\times$. Comparing coefficients, we have

$$a_i = \alpha a_{d-i} \qquad \text{for } i = 0,\dots,d,$$

hence $a_d = \alpha a_0 = \alpha^2 a_d$ and therefore $\alpha = \pm 1$. If d is odd, then

$$\pi = \sum_{i=0}^{(d-1)/2} a_i(X^i + \alpha X^{d-i}),$$

hence π is divisible by $1+\alpha X$. As π is irreducible, we may then choose $\pi = X+1$ if $\alpha = 1$, and $\pi = X-1$ if $\alpha=-1$. Suppose next d is even. If $\alpha=-1$ and $\operatorname{char} F\neq 2$, then $a_{d/2} = -a_{d/2}$ implies $a_{d/2} = 0$. In that case, we have

$$\pi = \sum_{i=0}^{d/2-1} a_i(X^i - X^{d-i}),$$

hence π is divisible by $1 - X$. This is a contradiction, since π is assumed to be irreducible. Therefore, $\alpha = 1$ and $(X^{d/2}\pi^{-1})^J = X^{d/2}\pi^{-1}$. We may then choose π of the form

$$\pi = 1 + a_1X + a_2X^2 + \cdots + a_2X^{d-2} + a_1X^{d-1} + X^d.$$

Let $\mathcal{R}_1$ be the set of irreducible polynomials of this form.

For each pair of prime ideals $\{P, P^J\}$ with $P^J \neq P$, we arbitrarily choose a generator $\pi \in F[X]$ of one of P, P^J and denote by $\mathcal{R}_2$ the set of irreducible polynomials thus chosen. Thus, the set of prime ideals of $F[X, X^{-1}]$ is $\{\pi F[X, X^{-1}]\}$ where π runs over the set $\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_2^J \cup \{X - 1, X + 1\}$, and we have $\pi^J F[X, X^{-1}] \neq \pi F[X, X^{-1}]$ if and only if $\pi \in \mathcal{R}_2 \cup \mathcal{R}_2^J$.

Returning to the proof of Theorem 1, we define a structure of $F[X, X^{-1}]$-module on V by letting

$$X \cdot v = a(v) \qquad \text{for all } v \in V.$$

Since $F[X, X^{-1}]$ is a principal ideal domain, the $F[X, X^{-1}]$-module V decomposes as a (finite) direct sum of quotients of $F[X, X^{-1}]$, as follows:

$$V \simeq \bigoplus_{\pi,m} \big(F[X, X^{-1}]/\pi^m\big)^{\mu(\pi,m)}$$

for some integers $\mu(\pi, m)$ which all vanish except a finite number, where π runs over $\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_2^J \cup \{X - 1, X + 1\}$, and m over the positive integers.

Condition (1) shows that the elementary divisors of a are the same as those of a^{-1}, hence

$$V \simeq \bigoplus_{\pi,m} \big(F[X, X^{-1}]/(\pi^J)^m\big)^{\mu(\pi,m)}.$$

Therefore, we have $\mu(\pi, m) = \mu(\pi^J, m)$ for all m if $\pi \in \mathcal{R}_2$.

For all integers m and for $\varepsilon = \pm 1$ we have

$$\dim V_m^{\varepsilon} = \mu(X - \varepsilon, m).$$

Therefore, condition (2) says that $\mu(X - 1, m)$ is even for all m even, and condition (3) says that $\mu(X + 1, m)$ is even for all m odd. Assuming $\operatorname{char} F \neq 2$ and conditions (1), (2) and (3) hold, we may decompose V into a direct sum of six $F[X, X^{-1}]$-submodules

$$V = V_1 \oplus V_2 \oplus V_3 \oplus V_4 \oplus V_5 \oplus V_6$$

where

$$V_1 \simeq \bigoplus_{\pi\in\mathcal{R}_1} \bigoplus_m \big(F[X,X^{-1}]/\pi^m\big)^{\mu(\pi,m)},$$
$$V_2 \simeq \bigoplus_{\pi\in\mathcal{R}_2} \bigoplus_m \big(F[X,X^{-1}]/\pi^m \oplus F[X,X^{-1}]/(\pi^J)^m\big)^{\mu(\pi,m)},$$
$$V_3 \simeq \bigoplus_{m \text{ odd}} \big(F[X,X^{-1}]/(X-1)^m\big)^{\mu(X-1,m)},$$
$$V_4 \simeq \bigoplus_{m \text{ even}} \big(F[X,X^{-1}]/(X-1)^m \oplus F[X,X^{-1}]/(X-1)^m\big)^{\mu(X-1,m)/2},$$
$$V_5 \simeq \bigoplus_{m \text{ even}} \big(F[X,X^{-1}]/(X+1)^m\big)^{\mu(X+1,m)},$$
$$V_6 \simeq \bigoplus_{m \text{ odd}} \big(F[X,X^{-1}]/(X+1)^m \oplus F[X,X^{-1}]/(X+1)^m\big)^{\mu(X+1,m)/2}.$$

If $\operatorname{char} F = 2$ and conditions (1), (2) hold, there is a similar decomposition

$$V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$$

where $V_1, \dots, V_4$ are as above. We shall show below (see Lemma 1) that there are nonsingular $(-X)$-hermitian forms with values in E (with respect to J) on

$$(7)\qquad \begin{array}{cl} F[X,X^{-1}]/\pi^m & \text{if } \pi\in\mathcal{R}_1,\\ F[X,X^{-1}]/\pi^m \oplus F[X,X^{-1}]/(\pi^J)^m & \text{if } \pi\in\mathcal{R}_2,\\ F[X,X^{-1}]/(X-1)^m & \text{if } m \text{ is odd},\\ \big(F[X,X^{-1}]/(X-1)^m\big)^2 & \text{if } m \text{ is even},\\ F[X,X^{-1}]/(X+1)^m & \text{if } m \text{ is even and } \operatorname{char} F\neq 2,\\ \big(F[X,X^{-1}]/(X+1)^m\big)^2 & \text{if } m \text{ is odd and } \operatorname{char} F\neq 2. \end{array}$$

The orthogonal sum of these forms yields a nonsingular $(-X)$-hermitian form

$$h\colon V\times V \to E$$

with respect to J. As Ischebeck-Scharlau [2] or Waterhouse [8], define an F-linear map $T\colon E\to F$ by observing that every element in E is represented by a unique rational fraction f which has a zero at ∞ and does not have a pole at 0, and letting

$$T\big(f + F[X,X^{-1}]\big) = f(0).$$

It is easily verified that $T(r^J) = -T(r)$ for all $r\in E$. Moreover, for every nonzero $r\in E$ there exists an integer k such that $T(X^{-k}r)\neq 0$, hence T does not vanish on any nonzero $F[X,X^{-1}]$-submodule of E.

Let $T_*(h)\colon V\times V\to F$ be the transfer bilinear map, defined by

$$T_*(h)(x,y) = T\big(h(x,y)\big) \qquad \text{for } x,\ y\in V.$$

If $x\in V$ is such that $T_*(h)(x,y) = 0$ for all $y\in V$, then T vanishes on the $F[X,X^{-1}]$-submodule $h(x,V)$, hence $h(x,V)=\{0\}$ and therefore $x=0$ since h is nonsingular. This shows that $T_*(h)$ is nonsingular.

Moreover, since h is $(-X)$-hermitian we have

$$T_*(h)(y,x) = T\big((-X)h(x,y)^J\big) = -T\big(Xh(x,y)^J\big) = \\ = T\big(X^J h(x,y)\big) = T\big(h(x,Xy)\big) = T_*(h)\big(x,a(y)\big)$$

for all x, $y\in V$. Therefore, a is the asymmetry of $T_*(h)$.

To complete the proof, we prove the existence of nonsingular $(-X)$-hermitian forms as asserted above.

Lemma 1. *There are nonsingular $(-X)$-hermitian forms with values in E (with respect to J) on the modules listed in* (7).

Proof. Suppose first $\pi \in \mathcal{R}_1$, hence $(X^{d/2}\pi^{-1})^J = X^{d/2}\pi^{-1}$, where d is the degree of π. For $u, v \in F[X, X^{-1}]$, let

$$h(u,v) = (X-1)(X^{d/2}\pi^{-1})^m u^J v + F[X, X^{-1}] \in E.$$

This map induces a sesquilinear form on $F[X, X^{-1}]/\pi^m$. The induced form is $(-X)$-hermitian since $(X-1)^J = -X^{-1}(X-1)$; it is nonsingular since $h(1,v) = 0$ implies π^m divides $(X-1)v$ in $F[X, X^{-1}]$, hence $v = 0$ in $F[X, X^{-1}]/\pi^m$ since π is prime to $X - 1$.

Next, suppose $\pi \in \mathcal{R}_2$. For u_1, u_2, v_1, $v_2 \in F[X, X^{-1}]$, we let

$$h\big((u_1, u_2), (v_1, v_2)\big) = \pi^{-m} u_1^J v_2 - X(\pi^J)^{-m} u_2^J v_1 + F[X, X^{-1}] \in E.$$

Computation shows that this map induces a nonsingular $(-X)$-hermitian form on $\big(F[X, X^{-1}]/\pi^m\big) \times \big(F[X, X^{-1}]/(\pi^J)^m\big)$.

Similarly, the following maps induce nonsingular $(-X)$-hermitian forms on the corresponding modules (where e is an arbitrary non-negative integer):

$$h(u,v) = X^{e-1}(X-1)^{-2e-1}u^J v + F[X, X^{-1}] \in E \quad \text{on } F[X, X^{-1}]/(X-1)^{2e+1};$$

$$h\big((u_1, u_2), (v_1, v_2)\big) = X^e (X-1)^{-2e}(u_1^J v_2 - X u_2^J v_1) + F[X, X^{-1}] \in E \quad \text{on } \big(F[X, X^{-1}]/(X-1)^{2e}\big)^2;$$

and if $\operatorname{char} F \neq 2$,

$$h(u,v) = (X-1)X^e(X+1)^{-2e}u^J v + F[X, X^{-1}] \in E \quad \text{on } F[X, X^{-1}]/(X+1)^{2e};$$

$$h\big((u_1, u_2), (v_1, v_2)\big) = (X-1)^{2e+1}(X+1)^{-2e-1}(u_1^J v_2 + X u_2^J v_1) + F[X, X^{-1}] \in E \quad \text{on } \big(F[X, X^{-1}]/(X+1)^{2e+1}\big)^2.$$

We omit the straightforward verifications. □

Remark. The theory of hermitian forms over principal ideal domains can also be used to show that the conditions in Theorem 1 are necessary.

2. The asymmetry of an anti-automorphism

2.1. **Definition.** Let A be a (finite-dimensional) central simple algebra over an arbitrary field F, and let $\sigma\colon A \to A$ be an F-linear anti-automorphism of A. Our goal is to attach to σ a unit $a_\sigma \in A^\times$ which plays the same rôle as the asymmetry a_b of a nonsingular pairing b with respect to the adjoint anti-automorphism σ_b. The key to the definition is an analogue of the linear involution γ_b, which we now define.

Proposition 4. *There is a unique linear map $\gamma_\sigma\colon A \to A$ which satisfies the following property: for any splitting field K of A, any isomorphism*

$$\theta\colon A_K = A \otimes_F K \to \operatorname{End}_K V$$

and any nonsingular pairing b on V such that $\sigma_b = \theta \circ (\sigma \otimes \mathrm{Id}_K) \circ \theta^{-1}$,

$$\theta \circ (\gamma_\sigma \otimes \mathrm{Id}_K) \circ \theta^{-1} = \gamma_b.$$

This map satisfies the following additional properties:

(i) $\gamma_\sigma\big(xyz\big) = \sigma(z)\gamma_\sigma(y)\sigma^{-1}(x)$ *for* $x,\ y,\ z \in A$*;*
(ii) $\gamma_\sigma^2 = \mathrm{Id}_A$.

Proof. It suffices to prove the existence of γ_σ. Uniqueness is then clear, and the additional properties follow from those of γ_b in Proposition 3.

Let $T_\sigma\colon A \times A \to F$ be the nonsingular pairing defined by

$$T_\sigma(x, y) = \mathrm{Trd}_A\big(\sigma(x)y\big) \qquad \text{for } x,\ y \in A,$$

where Trd_A is the reduced trace. Let $(e_i)_{i\in I}$ be a basis of A and let $(e_i^\sharp)_{i\in I}$ be the dual basis with respect to the pairing T_σ, so that

$$T_\sigma(e_i^\sharp, e_j) = \delta_{ij} \qquad \text{for } i,\ j \in I.$$

We let

$$\gamma_\sigma(x) = \sum_{i\in I} e_i x e_i^\sharp \qquad \text{for } x \in A.$$

In other words, γ_σ is the image of $\sum_{i\in I} e_i \otimes e_i^\sharp \in A \otimes_F A$ under the "sandwich" map $\mathrm{Sand}\colon A \otimes_F A \to \mathrm{End}_F A$ defined by $\mathrm{Sand}(x \otimes y)(z) = xzy$. Observe that γ_σ does not depend on the choice of the basis $(e_i)_{i\in I}$ since $\sum_{i\in I} e_i \otimes e_i^\sharp$ is the element which corresponds to Id_A under the bijection $\mathrm{Id}_A \otimes \hat{T}_\sigma\colon A \otimes_F A \to A \otimes_F A^* = \mathrm{End}_F A$.

As a consequence, for every field extension K/F, the map $\gamma_{\sigma\otimes\mathrm{Id}_K}\colon A \otimes K \to A \otimes K$ satisfies

$$\gamma_{\sigma\otimes\mathrm{Id}_K} = \gamma_\sigma \otimes \mathrm{Id}_K$$

since for $x \in A \otimes K$,

$$\gamma_{\sigma\otimes\mathrm{Id}_K}(x) = \sum_{i\in I} (e_i \otimes 1)x(e_i^\sharp \otimes 1) = (\gamma_\sigma \otimes \mathrm{Id}_K)(x).$$

To show that γ_σ is as required, assume that A is split: let $A = \mathrm{End}_F V$ and let b be a nonsingular pairing on V such that $\sigma = \sigma_b$. We have to show that $\gamma_\sigma = \gamma_b$. To prove this equality, we use the identification $V \otimes_F V = \mathrm{End}_F V$ defined by the linear isomorphism $\mathrm{Id}_V \otimes \hat{b}\colon V \otimes_F V \to V \otimes_F V^* = \mathrm{End}_F V$. Then $(v \otimes w)(x) = vb(w, x)$ for $v,\ w,\ x \in V$ and moreover

$$f \circ (v \otimes w) = f(v) \otimes w, \quad \sigma(v \otimes w) = a_b(w) \otimes v \quad \text{and} \quad \mathrm{Trd}(v \otimes w) = b(w, v)$$

for $v,\ w \in V$ and $f \in \mathrm{End}_F V$. Let $(v_i)_{1\le i\le n}$ be a basis of V and let $(v_i')_{1\le i\le n}$ be the dual basis for the pairing b, so that

$$b(v_i', v_j) = \delta_{ij} \qquad \text{for } i,\ j = 1, \dots, n. \tag{8}$$

Then $(v_i \otimes v_j)_{1\le i,j\le n}$ is a basis of $\mathrm{End}_F V$, and the dual basis with respect to T_σ is given by

$$(v_i \otimes v_j)^\sharp = v_i' \otimes v_j'.$$

Therefore, we have for $f \in \operatorname{End}_F V$

$$\begin{aligned}\gamma_\sigma(f) &= \sum_{i,j=1}^{n} (v_i \otimes v_j) \circ f \circ (v_i' \otimes v_j') \\ &= \sum_{i,j=1}^{n} v_i \otimes v_j'\, b\big(v_j, f(v_i')\big) \\ &= \sum_{i,j=1}^{n} v_i \otimes v_j'\, b\big(v_i', \gamma_b(f)(v_j)\big).\end{aligned}$$

For all $x \in V$ we have $x = \sum_{i=1}^n v_i b(v_i', x)$, hence $\sum_{i=1}^n v_i\, b\big(v_i', \gamma_b(f)(v_j)\big) = \gamma_b(f)(v_j)$ for all j, and the last equality above simplifies to

$$\gamma_\sigma(f) = \sum_{j=1}^{n} \gamma_b(f)(v_j) \otimes v_j' = \gamma_b(f) \circ \Big(\sum_{j=1}^{n} v_j \otimes v_j'\Big).$$

Since $\sum_{j=1}^n v_j \otimes v_j' = \operatorname{Id}_V$, it follows that $\gamma_\sigma(f) = \gamma_b(f)$. □

In view of property (i), we have

$$\gamma_\sigma(x) = \sigma(x)\gamma_\sigma(1) = \gamma_\sigma(1)\sigma^{-1}(x) \qquad \text{for all } x \in A. \tag{9}$$

Therefore, γ_σ is completely determined by the element $\gamma_\sigma(1) \in A^\times$.

Definition. The *asymmetry* of the anti-automorphism σ is the element $a_\sigma = \gamma_\sigma(1) \in A^\times$, where γ_σ is the linear involution defined in Proposition 4.

If $A = \operatorname{End}_F V$ and $\sigma = \sigma_b$ is the anti-automorphism adjoint to some nonsingular pairing b on V, it follows from Proposition 4 and property (iii) of Proposition 3 that a_σ is the asymmetry of the nonsingular form b, i.e.,

$$a_\sigma = a_b.$$

In the general case, equation (9) shows that

$$\sigma^2(x) = a_\sigma x a_\sigma^{-1} \qquad \text{for all } x \in A. \tag{10}$$

Moreover, since $\gamma_\sigma^2 = \operatorname{Id}_A$ we have

$$1 = \gamma_\sigma(a_\sigma) = \sigma(a_\sigma)a_\sigma. \tag{11}$$

The element a_σ is uniquely determined up to sign by (10) and (11).

Recall that an anti-automorphism σ is called an *involution* if $\sigma^2 = \operatorname{Id}_A$.

Proposition 5. *A linear anti-automorphism is an involution if and only if its asymmetry is* $+1$ *or* -1.

Proof. If $a_\sigma = \pm 1$, equation (10) shows that $\sigma^2 = \operatorname{Id}_A$. Conversely, if σ is an involution, (10) shows that $a_\sigma \in F^\times$. It then follows from (11) that $a_\sigma^2 = 1$, hence $a_\sigma = \pm 1$. □

If $\operatorname{char} F \neq 2$, a linear involution σ is called *orthogonal* (resp. *symplectic*) if after scalar extension to a splitting field it is adjoint to a symmetric (resp. skew-symmetric) bilinear pairing. Therefore, orthogonal involutions are exactly the linear anti-automorphisms with asymmetry $+1$, and symplectic involutions are those with asymmetry -1. Therefore, equations (10) and (11) are not sufficient to determine the type of the involution. This observation suggests that the sign of a_σ is meaningful for arbitrary anti-automorphisms.

The following proposition yields an alternative definition of the asymmetry a_σ, without reference to the linear involution γ_σ and without scalar extension to a splitting field.

Let $\sigma_*\colon A\otimes_F A\to \operatorname{End}_F A$ be the F-algebra homomorphism defined by

$$\sigma_*(a\otimes b)(x)=ax\sigma(b)\qquad\text{for } a,\,b,\,x\in A,$$

and recall (from [4, (3.5)], for instance) the *Goldman element* of A: this is the element $g\in A\otimes_F A$ such that $\operatorname{Sand}(g)(x)=\operatorname{Trd}_A(x)$ for all $x\in A$. Thus, there is a well-defined linear endomorphism $\sigma_*(g)\colon A\to A$.

Proposition 6. *The asymmetry of σ is the unique element $a_\sigma\in A^\times$ such that*

$$\sigma\big(\sigma_*(g)(f)\big)=a_\sigma f$$

for all $f\in A$.

Proof. It suffices to prove that a_σ satisfies the property above, since uniqueness is clear. To do this, we may extend scalars to a splitting field. Therefore, we may assume $A=\operatorname{End}_F V$ for some F-vector space V, and $\sigma=\sigma_b$ is the anti-automorphism adjoint to some nonsingular pairing b on V.

For all $f\in A$ and all $x,\,y\in V$ we have

$$b\big(f(x),y\big)=b\big(y,a_\sigma\circ f(x)\big),$$

by definition of the asymmetry (see (2)), hence we have to show

$$b\big(f(x),y\big)=b\big(y,\sigma\big(\sigma_*(g)(f)\big)(x)\big)$$

or, equivalently (by definition of $\sigma=\sigma_b$),

$$b\big(f(x),y\big)=b\big(\sigma_*(g)(f)(y),x\big)\tag{12}$$

for all $f\in A$ and all $x,\,y\in V$.

In order to compute the right-hand side, we identify $A=\operatorname{End}_F V$ to $V\otimes_F V$ via the linear isomorphism $\operatorname{Id}_V\otimes\hat b\colon V\otimes_F V\to V\otimes_F V^*=\operatorname{End}_F V$, as in the proof of Proposition 4. If $(v_i)_{1\le i\le n}$ is a basis of V and $(v_i')_{1\le i\le n}$ is the dual basis for the pairing b (see (8)), then the Goldman element is

$$g=\sum_{i,j}(v_i\otimes v_j')\otimes(v_j\otimes v_i')$$

since it is easily computed that for all $u,\,w\in V$

$$\begin{aligned}\operatorname{Sand}(g)(u\otimes w)&=\sum_{i,j}(v_i\otimes v_j')\circ(u\otimes w)\circ(v_j\otimes v_i')=\\&=\Big(\sum_i v_i\otimes v_i'\Big)\Big(\sum_j b(v_j',u)b(w,v_j)\Big)=b(w,u)\sum_i v_i\otimes v_i'=\operatorname{Trd}(u\otimes w)\operatorname{Id}_V.\end{aligned}$$

Now, for $u,\,w\in V$,

$$\sigma_*(g)(u\otimes w)=\sum_{i,j}(v_i\otimes v_j')\circ(u\otimes w)\circ\sigma(v_j\otimes v_i').$$

Since $(u\otimes w)\circ\sigma(f)=u\otimes f(w)$ for $f\in\operatorname{End}_F V$, the right-hand side of the last equality simplifies to

$$\sum_{i,j}\big((v_i\otimes v_j'(u)\big)\otimes\big((v_j\otimes v_i')(w)\big)=\sum_{i,j}v_i\otimes v_j b(v_j',u)b(v_i',w),$$

hence

$$\sigma_*(g)(u\otimes w) = w\otimes u.$$

Therefore, for u, w, x, $y\in V$,

$$b\big(\sigma_*(g)(u\otimes w)(y),x\big) = b\big((w\otimes u)(y),x\big) = b(w,x)b(u,y).$$

Since we also have $b\big((u\otimes w)(x),y\big) = b(u,y)b(w,x)$, equation (12) holds for $f = u\otimes w$. Since $\operatorname{End}_F V = V\otimes_F V$, it follows that (12) holds for all $f\in A$, and the proof is complete. □

Remark. Asymmetries can be defined on the same model for anti-automorphisms of Azumaya algebras; one may avoid the use of a basis of A in Proposition 4 by defining $\gamma_\sigma = \operatorname{Sand}(\xi_\sigma)$ where $\xi_\sigma\in A\otimes A$ is the element mapped to Id_A by $\operatorname{Id}_A\otimes\hat{T}_\sigma$. Alternatively, we may set $\xi_\sigma = (\operatorname{Id}_A\otimes\sigma^{-1})(g)$ where $g\in A\otimes A$ is the Goldman element. This is the approach taken by Saltman in [7] (see also [3, Chap. III, §8]).

2.2. **Characterization of asymmetries.** In this subsection, we show that in a central simple algebra of exponent 2, every unit which is conjugate to its inverse is the asymmetry of some anti-automorphism.

We first compare the asymmetries of two anti-automorphisms σ, τ on a central simple algebra A. The Skolem-Noether theorem shows that the automorphism $\tau\circ\sigma^{-1}$ is the conjugation by some unit $u\in A^\times$, i.e.,

$$\tau(x) = u\sigma(x)u^{-1}\qquad\text{for all } x\in A. \tag{13}$$

Proposition 7. *Let σ, τ be anti-automorphisms of a central simple algebra A, and let $u\in A^\times$ be such that* (13) *holds. The asymmetries a_σ, a_τ of σ and τ are related by*

$$a_\tau = u\sigma(u)^{-1}a_\sigma.$$

Proof. We use the definition of asymmetry provided by Proposition 6. For a, b, $x\in A$, we have

$$\tau_*(a\otimes b)(x) = ax\tau(b) = axu\sigma(b)u^{-1}$$

hence

$$\tau_*(a\otimes b)(x) = \sigma_*(a\otimes b)(xu)u^{-1}.$$

Therefore, denoting by $r_u\colon A\to A$ the linear map of multiplication on the right by u, we have

$$\tau_*(a\otimes b) = (r_u)^{-1}\circ\sigma_*(a\otimes b)\circ r_u$$

for all a, $b\in A$, hence also

$$\tau_*(g) = (r_u)^{-1}\circ\sigma_*(g)\circ r_u$$

for g the Goldman element of A. It follows that for all $f\in A$,

$$\tau_*(g)(f) = \sigma_*(fu)u^{-1}. \tag{14}$$

By Proposition 6, the asymmetry a_τ satisfies

$$a_\tau f = \tau\big(\tau_*(g)(f)\big)\qquad\text{for all } f\in A.$$

Using (14), we obtain

$$a_\tau f = \tau\big(\sigma_*(g)(fu)u^{-1}\big) = u\sigma\big(\sigma_*(g)(fu)u^{-1}\big)u^{-1} = u\sigma(u)^{-1}\sigma\big(\sigma_*(g)(fu)\big)u^{-1}.$$

Proposition 6 also yields $\sigma\big(\sigma_*(g)(fu)\big) = a_\sigma fu$, hence

$$a_\tau f = u\sigma(u)^{-1}a_\sigma f \qquad \text{for all } f \in A.$$

The proposition follows. ☐

Theorem 2. *Let A be a central simple algebra of exponent 2 over an arbitrary field F. A unit is the asymmetry of some anti-automorphism of A if and only if it is conjugate to its inverse.*

Proof. Suppose $a \in A^\times$ is the asymmetry of some anti-automorphism σ. We have to show that the F-vector space

$$U = \{x \in A \mid xa = a^{-1}x\}$$

contains an invertible element. This amounts to proving that the restriction of the reduced norm polynomial Nrd_A does not vanish on U. Theorem 1 shows that this polynomial does not vanish on $U \otimes K$, for any splitting field K of A, since a is the asymmetry of $\sigma \otimes \operatorname{Id}_K$. Therefore, the reduced norm does not vanish on U, since F is an infinite field. (Note that every central simple algebra over a finite field is split, hence of exponent 1.)

For the converse, suppose $a \in A^\times$ is conjugate to a^{-1}. Let K be a splitting field of A; identify $A \otimes K = \operatorname{End}_K V$ for some K-vector space V. We first show, by using Theorem 1, that a $(= a \otimes 1)$ is the asymmetry of some anti-automorphism of $\operatorname{End}_K V$. With the same notation as in Theorem 1, we have to prove that $\dim_K V_m^{+1}$ is even if m is even, and moreover that $\dim_K V_m^{-1}$ is even if m is odd and $\operatorname{char} F \neq 2$. For every integer $m \geq 1$ and $\varepsilon = \pm 1$, we have an exact sequence of K-vector spaces

$$0 \to \frac{\ker(a - \varepsilon \operatorname{Id}_V)^{m+1}}{\ker(a - \varepsilon \operatorname{Id}_V)^m} \xrightarrow{a - \varepsilon \operatorname{Id}_V} \frac{\ker(a - \varepsilon \operatorname{Id}_V)^m}{\ker(a - \varepsilon \operatorname{Id}_V)^{m-1}} \to V_m^\varepsilon \to 0,$$

hence

$$\dim V_m^\varepsilon = \operatorname{rk}(a - \varepsilon \operatorname{Id}_V)^{m-1} - 2\operatorname{rk}(a - \varepsilon \operatorname{Id}_V)^m + \operatorname{rk}(a - \varepsilon \operatorname{Id}_V)^{m+1}, \tag{15}$$

where rk denotes the rank.

For all $b \in A$ we have

$$\operatorname{rk} b = \frac{\dim_K b(A \otimes K)}{\deg(A \otimes K)} = \frac{\dim_F bA}{\deg A},$$

hence $\operatorname{rk} b$ is divisible by the Schur index $\operatorname{ind} A$ (see [4, (1.9)]). Since A has exponent 2, $\operatorname{ind} A$ is even, by [1, Theorem 5.17]. Therefore, $\operatorname{rk} b$ is even for all $b \in A$, and equation (15) shows that $\dim V_m^\varepsilon$ is even for every integer m and for $\varepsilon = \pm 1$. By Theorem 1, it follows that a is the asymmetry of some anti-automorphism θ of $A \otimes K$.

Now, fix some anti-automorphism σ of A. Let a_σ be its asymmetry and consider the F-vector space

$$W = \{x \in A \mid xa = \sigma(x)a_\sigma\}.$$

If $u \in (A \otimes K)^\times$ is such that $\theta(x) = u(\sigma \otimes \operatorname{Id}_K)(x)u^{-1}$ for all $x \in A \otimes K$, then $u^{-1} \in W \otimes K$, by Proposition 7. Therefore, the same arguments as in the first part of the proof show that W contains an invertible element w. Using Proposition 7 again, we see that a is the asymmetry of the anti-automorphism $x \mapsto w^{-1}\sigma(x)w$. ☐

Corollary 1 (Albert)**.** *Every central simple algebra of exponent* 2 *carries an involution. Moreover, if the characteristic of the base field is different from* 2*, every central simple algebra of exponent* 2 *carries involutions of both orthogonal and symplectic types.*

Proof. It readily follows from Theorem 2 that $+1$ and -1 are asymmetries of some anti-automorphisms. These anti-automorphisms are involutions, by Proposition 5. □

2.3. **The determinant of an anti-automorphism.** Let σ be a linear anti-automorphism of a central simple algebra A over an arbitrary field F. Let $a_\sigma \in A^\times$ be the asymmetry of A and γ_σ the linear involution of Proposition 4. Consider the vector spaces

$$\operatorname{Alt}(A,\sigma) = \{x - \sigma(x)a_\sigma \mid x \in A\} = \{x - \gamma_\sigma(x) \mid x \in A\}$$

and

$$\operatorname{Sk}(A,\sigma) = \{x \in A \mid \sigma(x) + xa_\sigma^{-1} = 0\} = \{x \in A \mid \gamma_\sigma(x) = -x\}.$$

From equations (10) and (11), it follows that $\operatorname{Alt}(A,\sigma) \subset \operatorname{Sk}(A,\sigma)$. Moreover, we have $x - \gamma_\sigma(x) = 2x$ for all $x \in \operatorname{Sk}(A,\sigma)$, hence $\operatorname{Alt}(A,\sigma) = \operatorname{Sk}(A,\sigma)$ if $\operatorname{char} F \neq 2$.

Lemma 2. *Suppose σ, τ are anti-automorphisms of A, and let $u \in A^\times$ be such that*

$$\tau(x) = u\sigma(x)u^{-1} \qquad \text{for all } x \in A.$$

Then

$$\operatorname{Alt}(A,\tau) = u \operatorname{Alt}(A,\sigma) \quad \text{and} \quad \operatorname{Sk}(A,\tau) = u \operatorname{Sk}(A,\sigma).$$

Proof. Proposition 7 yields $a_\tau = u\sigma(u)^{-1}a_\sigma$ and $a_\sigma = u^{-1}\tau(u)a_\tau$. Therefore, for all $x \in A$ we have

$$x - \tau(x)a_\tau = u\big(u^{-1}x - \sigma(u^{-1}x)a_\sigma\big) \quad \text{and} \quad u\big(x - \sigma(x)a_\sigma\big) = ux - \tau(ux)a_\tau,$$

proving that $\operatorname{Alt}(A,\tau) = u \operatorname{Alt}(A,\sigma)$. The proof that $\operatorname{Sk}(A,\tau) = u \operatorname{Sk}(A,\sigma)$ is along the same lines. □

Lemma 3. *If* $\deg A$ *is even,* $\operatorname{Alt}(A,\sigma)$ *contains invertible elements. Moreover, the square class* $\operatorname{Nrd}_A(x) \cdot F^{\times 2} \in F^\times/F^{\times 2}$ *does not depend on the choice of* $x \in A^\times \cap \operatorname{Alt}(A,\sigma)$.

Proof. Let τ be an anti-automorphism of A with asymmetry $+1$ and let $u \in A^\times$ be such that

$$\tau(x) = u\sigma(x)u^{-1} \qquad \text{for all } x \in A.$$

By Lemma 2, we have

$$\operatorname{Alt}(A,\sigma) = u^{-1} \operatorname{Alt}(A,\tau). \tag{16}$$

Since τ is an involution, Corollary (2.8) of [4] shows that $\operatorname{Alt}(A,\tau)$ contains invertible elements if $\deg A$ is even, hence $\operatorname{Alt}(A,\sigma)$ also contains invertible elements. Moreover, from [4, (7.1)], it follows that all the invertible elements have the same reduced norm up to a square of F; therefore, if $v \in A^\times \cap \operatorname{Alt}(A,\tau)$ it follows from (16) that $\operatorname{Nrd}_A(x) \in \operatorname{Nrd}_A(u^{-1}v) \cdot F^{\times 2}$ for all $x \in A^\times \cap \operatorname{Alt}(A,\sigma)$. □

This last lemma allows us to define the *determinant* of an anti-automorphism σ of a central simple algebra A of even degree, as follows:

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

for any $x\in A^\times\cap\operatorname{Alt}(A,\sigma)$.

This definition is consistent with [4, (7.2)], where the determinant of an orthogonal involution is defined.

Example 1. Since clearly $1-a_\sigma\in\operatorname{Alt}(A,\sigma)$, we have

$$\det\sigma = \operatorname{Nrd}_A(1-a_\sigma)\cdot F^{\times 2}$$

if $1-a_\sigma$ is invertible. Therefore, the determinant of σ is entirely determined by its asymmetry in this particular case.

Example 2. The transpose involution on a matrix algebra $M_n(F)$ (with n even) has trivial determinant. Indeed, the matrix

$$\begin{pmatrix} m_1 & & 0\\ & \ddots & \\ 0 & & m_{n/2}\end{pmatrix} \qquad \text{where } m_1=\cdots=m_{n/2}=\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$$

is in $\operatorname{Alt}\bigl(M_n(F),t\bigr)$ and has determinant 1.

Proposition 8. *Let σ, τ be anti-automorphisms of a central simple algebra A of even degree, and let $u\in A^\times$ be such that*

$$\tau(x)=u\sigma(x)u^{-1}\qquad \text{for all } x\in A.$$

Then

$$\det\tau=\operatorname{Nrd}_A(u)\det\sigma.$$

Proof. This readily follows from Lemma 2. □

Proposition 9. *Let V be an even-dimensional vector space over an arbitrary field F and let b be a nonsingular pairing on V. For every basis $(v_i)_{1\le i\le n}$ of V,*

$$\det\sigma_b=\det\bigl(b(v_i,v_j)\bigr)_{1\le i,j\le n}\cdot F^{\times 2}.$$

Proof. Identify $\operatorname{End}_F V$ with the matrix algebra $M_n(F)$ by means of the basis $(v_i)_{1\le i\le n}$. The anti-automorphism σ_b is then given by

$$\sigma_b(m)=u^{-1}m^tu\qquad\text{for all } m\in M_n(F),$$

where $u=\bigl(b(v_i,v_j)\bigr)_{1\le i,j\le n}\in M_n(F)$. Therefore, Proposition 8 yields

$$\det\sigma_b=\det u^{-1}\det t.$$

Since it was observed in Example 2 above that $\det t$ is trivial, the proposition follows. □

References

[1] A.A. Albert, *Structure of Algebras,* Coll. Pub. **24**, Amer. Math. Soc., Providence, RI, 1939.

[2] F. Ischebeck, W. Scharlau, *Hermitesche und orthogonale Operatoren über kommutativen Ringen,* Math. Ann. **200** (1973), 327–334.

[3] M.-A. Knus, *Quadratic and Hermitian Forms over Rings,* Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991.

[4] M.-A. Knus, A.S. Merkurjev, M. Rost and J.-P. Tignol, *The Book of Involutions,* Coll. Pub. **44**, Amer. Math. Soc., Providence, RI, 1998.

[5] A. Ranicki, *High-dimensional Knot Theory,* Springer Monographs in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 1998.

[6] C. Riehm, *The equivalence of bilinear forms,* J. Algebra **31** (1974), 45–66.

[7] D.J. Saltman, *Azumaya algebras with involution,* J. Algebra **52** (1978), 526–539.

[8] W.C. Waterhouse, *A nonsymmetric Hasse-Minkowski theorem,* Amer. J. Math. **99** (1977), 755–759.

[9] J. Williamson, *On the algebraic problem concerning the normal form of linear dynamical systems,* Amer. J. Math. **58** (1936), 141–163.

Anne Cortella
e-mail: cortella@math.univ-fcomte.fr
UMR CNRS 6623
Laboratoire de Mathématiques de Besançon
Université de Franche-Comté
16, route de Gray
F-25030 Besançon Cedex
France

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