CENTRAL SIMPLE ALGEBRAS, INVOLUTIONS AND QUADRATIC FORMS

Lectures at the National Taiwan University, April 1993

Jean-Pierre Tignol

Université Catholique de Louvain
B-1348 Louvain-la-Neuve, Belgium

These notes are based on a series of lectures given at the National Taiwan University in April 1993. Their aim is to provide an introduction to the theory of central simple algebras with involution, viewed as a theory of twisted quadratic (or alternating) forms. The first chapter explains the viewpoint and gives the basic results concerning involutions on central simple algebras. The second chapter focuses on the construction of the Clifford algebra for an algebra with orthogonal involution, and the third discusses groups of similarities and isometries, introducing twisted versions of the special Clifford groups and spin groups.

The material in Chapters 2 and 3 is mostly new (at least in the way it is presented); it has been obtained in joint work with Max Knus, Alexandr Merkurjev and Markus Rost. It is my hope that these notes will be expanded, improved and incorporated into a joint book on involutions, Clifford algebras and triality.

It is my great pleasure to acknowledge support from the National Research Council of China and to express my warmest thanks to the National Taiwan University, and particularly to Professor Ming chang Kang, for their hospitality. I am also very grateful to Professor Eng Tjioe Tan, from the National Chengchi University, who did not measure his efforts to make my stay in Taiwan a most pleasant experience, and to my audience at the National Taiwan University, who took heavy doses of involutions with unfailing patience and good humor.

J.-P. Tignol
June 1993

Contents

Chapter 1.

Involutions and hermitian forms

In these notes, we will be working in the perspective that involutions on central simple algebras are twisted forms of quadratic or alternating forms up to a scalar factor. To motivate this point of view, we consider the basic, classical situation of linear algebra.

Let V be a finite-dimensional vector space over a field F of characteristic different from 2. A bilinear form $b : V \times V \to F$ is called *nonsingular* if the induced map

$$\hat{b} : V \to V^* = \mathrm{Hom}_F(V, F)$$

defined by

$$\hat{b}(x)(y) = b(x, y) \qquad \text{for all } x, y \in V$$

is an isomorphism of vector spaces. For any $f \in \mathrm{End}_F(V)$ we may then define $\sigma_b(f) \in \mathrm{End}_F(V)$ by:

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

where $f^t \in \mathrm{End}_F(V^*)$ is the transpose of f. Alternatively, $\sigma_b(f)$ may be defined by the following property:

$$b(x, f(y)) = b(\sigma_b(f)(x), y) \qquad \text{for all } x, y \in V. \tag{1.1}$$

The map $\sigma_b : \mathrm{End}_F(V) \to \mathrm{End}_F(V)$ is then an anti-automorphism of $\mathrm{End}_F(V)$, which is known as the *adjoint anti-automorphism* with respect to the nonsingular bilinear form b. The map σ_b is clearly F-linear.

We denote by $\mathrm{Ant}_F(\mathrm{End}_F(V))$ the set of linear anti-automorphisms of $\mathrm{End}_F(V)$. Anti-automorphisms σ such that $\sigma^2 = \mathrm{Id}$ are called *involutions*. We also denote by $\mathrm{Bil}(V)$ the F-vector space of bilinear forms on V and by $\mathrm{Bil}^0(V)$ the subset of nonsingular bilinear forms. The multiplicative group $F^\times$ acts naturally on $\mathrm{Bil}(V)$ and $\mathrm{Bil}^0(V)$ (by multiplication). Bilinear forms which are in the same orbit are called *similar*.

The basic result which motivates our approach and which will be generalized in subsequent sections (see §1.4) is the following:

(0.1) Theorem. *The map which associates to each nonsingular bilinear form b on V its adjoint anti-automorphism σ_b induces a one-to-one correspondence*

$$\mathrm{Bil}^0(V)/F^\times \xrightarrow{\sim} \mathrm{Ant}_F(\mathrm{End}_F(V)).$$

Under this correspondence, F-linear involutions on $\mathrm{End}_F(V)$ correspond to nonsingular bilinear forms which are either symmetric or skew-symmetric.

Proof: From relation (1.1) it follows that for $\alpha \in F^\times$ the adjoint anti-automorphism $\sigma_{\alpha b}$ with respect to the multiple αb of b is the same as the adjoint anti-automorphism σ_b. Therefore, the map $b \mapsto \sigma_b$ induces a well-defined map from the set of nonsingular bilinear forms on V up to similarity to the set of F-linear anti-automorphisms of $\mathrm{End}(V)$.

To show that this map is one-to-one, note that if $b, b' \in \mathrm{Bil}^0(V)$ are nonsingular bilinear forms on V, then the map $v = \hat{b}^{-1} \circ \hat{b'} \in \mathrm{GL}(V)$ is such that

$$b'(x,y) = b(v(x),y) \qquad \text{for all } x, y \in V.$$

From this relation, it follows that the adjoint anti-automorphisms σ_b, $\sigma_{b'}$ are related by:

$$\sigma_b(f) = v \circ \sigma_{b'}(f) \circ v^{-1} \qquad \text{for all } f \in \mathrm{End}_F(V),$$

or equivalently

$$\sigma_b = \mathrm{Int}(v) \circ \sigma_{b'},$$

where $\mathrm{Int}(v)$ is the inner automorphism of $\mathrm{End}_F(V)$ induced by v:

$$\mathrm{Int}(v)(f) = v \circ f \circ v^{-1} \qquad \text{for } f \in \mathrm{End}_F(V).$$

Therefore, if $\sigma_b = \sigma_{b'}$, then $v \in F^\times$ and b, b' are scalar multiples of each other.

Moreover, if b is a fixed nonsingular bilinear form on V with adjoint anti-automorphism σ_b, then for $\sigma' \in \mathrm{Ant}_F(\mathrm{End}_F(V))$ the compositum $\sigma_b \circ \sigma'^{-1}$ is an F-linear automorphism of $\mathrm{End}_F(V)$. Since these automorphisms are inner, by the Skolem-Noether theorem (see [18, Theorem 8.4.2]), there exists $u \in \mathrm{GL}(V)$ such that $\sigma_b \circ \sigma'^{-1} = \mathrm{Int}(u)$. Then σ' is the adjoint anti-automorphism with respect to the bilinear form b' defined by:

$$b'(x,y) = b(u(x),y).$$

Thus, the first part of the Theorem is proved.

Observe also that if b is a nonsingular bilinear form on V with adjoint anti-automorphism σ_b, then the bilinear form b' defined by

$$b'(x,y) = b(y,x) \qquad \text{for all } x, y \in V$$

has adjoint anti-automorphism $\sigma_{b'} = \sigma_b^{-1}$. Therefore, $\sigma_b^2 = \mathrm{Id}$ if and only if b and b' are scalar multiples of each other; since the scalar factor ε such that $b' = \varepsilon b$ clearly satisfies $\varepsilon^2 = 1$, this condition is equivalent to: b is symmetric or skew-symmetric.

This shows that F-linear involutions correspond to symmetric or skew-symmetric bilinear forms under the bijection above. ∎

Our aim in this first chapter is to give an analogous interpretation of involutions on arbitrary central simple algebras in terms of hermitian forms on vector spaces over skew fields. We first review basic notions concerning central simple algebras.

§1. Central simple algebras

Unless otherwise mentioned, all the algebras we consider in this work are finite-dimensional with 1. When we consider algebras with involutions, the base field F will be assumed to have characteristic different from 2, but this assumption is not needed in this first section. As a general rule, we will use the convention that homomorphisms of modules will be written on the side opposite to scalars. Thus, we will use the usual functional notation for homomorphisms of right modules, but for *left* modules we will write homomorphisms on the *right* of the arguments and use the right-hand rule for mapping composition[1].

For any algebra A over a field F and any field extension K/F, we denote by A_K the K-algebra obtained from A by extending scalars to K:

$$A_K = A \otimes_F K.$$

We also define the *opposite algebra* A^{op} by:

$$A^{\mathrm{op}} = \{a^{\mathrm{op}} \mid a \in A\},$$

with the operations defined as follows:

$$a^{\mathrm{op}} + b^{\mathrm{op}} = (a+b)^{\mathrm{op}} \quad a^{\mathrm{op}}.b^{\mathrm{op}} = (ba)^{\mathrm{op}} \quad \alpha.a^{\mathrm{op}} = (\alpha a)^{\mathrm{op}} \quad \text{for } a, b \in A \text{ and } \alpha \in F.$$

A *central simple algebra* over a field F is a (finite-dimensional) algebra $A \neq \{0\}$ with center F $(= F.1)$ which has no two-sided ideal except $\{0\}$ and A. For instance, the algebra $M_n(F)$ of $n \times n$ matrices over a field F is a central simple algebra. An algebra $A \neq \{0\}$ is a *division algebra* (or a *skew field*) if every non-zero element in A is invertible.

1.1. Wedderburn's theorem

The structure of central simple algebras is determined by a well-known theorem of Wedderburn:

(1.1) Theorem. (Wedderburn) *For an algebra A over a field F, the following conditions are equivalent:*

[1] Among the funny consequences of this convention, note that if V is a right vector space over a division ring D, then its dual V^* is a left vector space over D and if f, g are endomorphisms of V, then their transpose obey the rule: $(f \circ g)^t = f^t \circ g^t$.

1. *A is central simple.*
2. *The canonical map $A \otimes_F A^{\mathrm{op}} \to \mathrm{End}_F(A)$ which associates to $a \otimes b^{\mathrm{op}}$ the linear map $x \mapsto axb$ is an isomorphism.*
3. *There is a field K containing F such that A_K is isomorphic to a matrix algebra over K:*
$$A_K \simeq M_n(K) \quad \text{for some } n.$$
4. *If Ω is an algebraically closed field containing F,*
$$A_\Omega \simeq M_n(\Omega) \quad \text{for some } n.$$
5. *There is a finite-dimensional central division algebra D over F and an integer r such that $A \simeq M_r(D)$.*

Moreover, if these conditions hold, the division algebra D is uniquely determined up to an algebra isomorphism as $D = \mathrm{End}_A(M)$ for any simple left A-module M.

For the proof, we refer to [18, Chapter 8] or [6, §3].

The fields K for which condition *(3)* holds are called *splitting fields* of A. Accordingly, the algebra A is called *split* if it is isomorphic to a matrix algebra $M_n(F)$ (or to $\mathrm{End}_F(V)$ for some vector space V over F).

Since the dimension of an algebra does not change under an extension of scalars, it follows from the above theorem that the dimension of every central simple algebra is a square: $\dim_F A = n^2$ if $A_K \simeq M_n(K)$ for some extension K/F. The integer n is called the *degree* of A and denoted by $\deg A$. The degree of the division algebra D in condition *(5)* is called the *index* of A (or sometimes the *Schur index* of A) and denoted by $\mathrm{ind}\, A$. Alternatively, the index of A can be defined by the relation:

$$\deg A . \mathrm{ind}\, A = \dim_F M$$

where M is a simple left module over A. This relation readily follows from the fact that if $A \simeq M_r(D)$, then D^r is a simple left module over A.

In view of the uniqueness of the division algebra D in the preceding theorem, we introduce the following definition:

(1.2) Definition. Let A, B be finite-dimensional central simple algebras over a field F. Let $A \simeq M_r(D)$ and $B \simeq M_s(E)$ for some division algebras D, E over F. The algebras A, B are called *Brauer-equivalent* if $D \simeq E$. It then follows that $M_s(A) \simeq M_r(B)$. Conversely, if $M_t(A) \simeq M_m(B)$ for some integers t, m, then $M_{rt}(D) \simeq M_{sm}(E)$, hence Wedderburn's theorem shows $D \simeq E$. The preceding definition may therefore be rephrased as follows: A and B are Brauer-equivalent if and only if $M_t(A) \simeq M_m(B)$ for some integers t, m.

Clearly, every central simple algebra is Brauer-equivalent to one and only one division algebra (up to isomorphism). If A and B are Brauer-equivalent central simple algebras, then $\operatorname{ind} A = \operatorname{ind} B$ and $A \simeq B$ if and only if $\deg A = \deg B$.

The tensor product endows the set of Brauer equivalence classes of central simple algebras over F with the structure of an abelian group, denoted $\operatorname{Br}(F)$ and called the *Brauer group* of F. The unit element in this group is the class of F, which is also the class of all the matrix algebras over F. The inverse of the class of a central simple algebra A is the class of the opposite algebra A^{op}, as part *(2)* of Wedderburn's theorem shows.

1.2. One-sided ideals in central simple algebras

A fundamental result of the Wedderburn theory of central simple algebras is that all the finitely generated left (resp. right) modules over a central simple algebra A over a field F decompose into direct sums of simple left (resp. right) modules, and that the simple left (resp. right) modules are all isomorphic. If $A = M_r(D)$ for some integer r and some central division algebra D, then D^r is a simple left A-module (with the matrix multiplication, writing the elements of D^r as column vectors). Therefore, every finitely generated left A-module M is isomorphic to a direct sum of copies of D^r:

$$M \simeq (D^r)^t,$$

hence

$$\dim_F M = rt \dim_F D = t \deg A \operatorname{ind} A.$$

(1.3) Definition. The *rank* of the left A-module M is defined by:

$$\operatorname{rk} M = \frac{\dim_F M}{\deg A}.$$

Observe from the preceding relation that the rank of a finitely generated left A-module is always a multiple of $\operatorname{ind} A$.

Since D^r is a simple left A-module, we have $D \simeq \operatorname{End}_A(D^r)$; therefore, if $M \simeq (D^r)^t$, then

$$\operatorname{End}_A(M) \simeq M_t(\operatorname{End}_A(D^r)) \simeq M_t(D).$$

This shows that $\operatorname{End}_A(M)$ is a central simple algebra Brauer-equivalent to A of degree $\operatorname{rk} M$.

The preceding discussion of course applies also to right A-modules; writing the elements of D^r as row vectors, matrix multiplication also endows D^r with a right A-module structure, and D^r is then a simple right A-module.

Ideals and subspaces

Suppose now $A = \mathrm{End}_D(V)$ for some central division algebra D over F and some finite-dimensional vector space V over D. We aim to get an explicit description of the one-sided ideals in A in terms of subspaces of V.

Let $U \subset V$ be a subspace. Composing every linear map from V to U with the inclusion $U \hookrightarrow V$, we identify $\mathrm{Hom}_D(V, U)$ to a subspace of $A = \mathrm{End}_D(V)$:

$$\mathrm{Hom}_D(V, U) = \{f \in \mathrm{End}_D(V) \mid \mathrm{im}\, f \subset U\}.$$

This space is clearly a right ideal in A, of rank

$$\mathrm{rk}\, \mathrm{Hom}_D(V, U) = \dim_D U . \deg D.$$

Similarly, composing every linear map from the quotient space V/U to V with the canonical map $V \to V/U$, we may identify $\mathrm{Hom}_D(V/U, V)$ to a subspace of $A = \mathrm{End}_D(V)$:

$$\mathrm{Hom}_D(V/U, V) = \{f \in \mathrm{End}_D(V) \mid \ker f \supset U\}.$$

This space is clearly a left ideal in A of rank

$$\mathrm{rk}\, \mathrm{Hom}_D(V/U, V) = \dim_D(V/U) . \deg D.$$

(1.4) Proposition. *The map $U \mapsto \mathrm{Hom}_D(V, U)$ defines a one-to-one correspondence between subspaces in V and right ideals in $A = \mathrm{End}_D(V)$. Similarly, the map $U \mapsto \mathrm{Hom}_D(V/U, V)$ defines a one-to-one correspondence between subspaces in V and left ideals in A. Moreover, there are canonical isomorphisms of F-algebras:*

$$\mathrm{End}_A(\mathrm{Hom}_D(V, U)) \simeq \mathrm{End}_D(U) \quad \textit{and} \quad \mathrm{End}_A(\mathrm{Hom}_D(V/U, V)) \simeq \mathrm{End}_D(V/U).$$

Proof: The last statement is clear: multiplication on the left (resp. right) defines an F-algebra homomorphism $\mathrm{End}_D(U) \hookrightarrow \mathrm{End}_A(\mathrm{Hom}_D(V, U))$ (resp. $\mathrm{End}_D(V/U) \hookrightarrow \mathrm{End}_A(\mathrm{Hom}_D(V/U, V))$). Since $\mathrm{rk}(\mathrm{Hom}_D(V, U)) = \dim_D U . \deg D$, we have

$$\deg \mathrm{End}_A(\mathrm{Hom}_D(V, U)) = \dim_D U . \deg D = \deg \mathrm{End}_D(U),$$

so the homomorphism $\mathrm{End}_D(U) \hookrightarrow \mathrm{End}_A(\mathrm{Hom}_D(V, U))$ is an isomorphism. Similarly, the homomorphism $\mathrm{End}_D(V/U) \hookrightarrow \mathrm{End}_A(\mathrm{Hom}_D(V/U, V))$ is an isomorphism by dimension count.

For the first part, it suffices to show that every right (resp. left) ideal in A has the form $\mathrm{Hom}_D(V, U)$ (resp. $\mathrm{Hom}_D(V/U, V)$) for some subspace $U \subset V$. We first consider a special case:

(1.5) Lemma. *For $f \in A = \mathrm{End}_D(V)$,*

$$fA = \mathrm{Hom}_D(V, \mathrm{im}\, f) \quad \textit{and} \quad Af = \mathrm{Hom}_D(V/\ker f, V).$$

Proof: The inclusions $fA \subset \mathrm{Hom}_D(V, \mathrm{im}\, f)$ and $Af \subset \mathrm{Hom}_D(V/\ker f, V)$ are obvious. To prove the converse inclusions, choose sections s and t of the epimorphism $f : V \to \mathrm{im}\, f$ and of the monomorphism $\overline{f} : V/\ker f \to V$ induced by f. Thus, s and t are linear maps:

$$s : \mathrm{im}\, f \to V \qquad t : V \to V/\ker f$$

such that $f \circ s = \mathrm{Id}_{\mathrm{im}\, f}$ and $t \circ \overline{f} = \mathrm{Id}_{V/\ker f}$, i.e. $t \circ f(x) = x + \ker f$ for all $x \in V$. For all $g \in \mathrm{Hom}_D(V, \mathrm{im}\, f)$ we have $g = f \circ s \circ g \in fA$, so $\mathrm{Hom}_D(V, \mathrm{im}\, f) \subset fA$. Similarly, for $g \in \mathrm{Hom}_D(V/\ker f, V)$ we have $g = g \circ t \circ f \in Af$, so $\mathrm{Hom}_D(V/\ker f, V) \subset Af$. ∎

End of the proof of Proposition 1.4: Let $I \subset A$ be a right ideal. Let $U = \sum_{f \in I} \mathrm{im}\, f \subset V$. Clearly, $I \subset \mathrm{Hom}_D(V, U)$. To prove the converse inclusion, pick $f \in I$ for which $\mathrm{im}\, f$ is maximal. If we show $\mathrm{im}\, f = U$, then we are done since the Lemma yields

$$\mathrm{Hom}_D(V, U) = fA \subset I.$$

Suppose $\mathrm{im}\, f$ is properly contained in U. Then there exists $g \in I$ such that $\mathrm{im}\, g \not\subset \mathrm{im}\, f$. Let $u \in (\mathrm{im}\, g) \setminus (\mathrm{im}\, f)$ and choose a complementary subspace V' to $\mathrm{im}\, f \oplus uD$:

$$V = \mathrm{im}\, f \oplus uD \oplus V'.$$

If π is the projection on $\mathrm{im}\, f$ parallel to $uD \oplus V'$, then $\mathrm{im}\, \pi = \mathrm{im}\, f$ hence the Lemma shows $\pi \in fA \subset I$. Similarly, if π' is the projection on uD parallel to $\mathrm{im}\, f \oplus V'$, then $\mathrm{im}\, \pi' \subset \mathrm{im}\, g$ hence $\pi' \in gA \subset I$. Therefore, $\pi + \pi' \in I$; but $\pi + \pi'$ is the projection on $\mathrm{im}\, f \oplus uD$ parallel to V', so $\mathrm{im}(\pi + \pi') = \mathrm{im}\, f \oplus uD$ properly contains $\mathrm{im}\, f$. It follows that $\mathrm{im}\, f$ is not maximal if $\mathrm{im}\, f \neq U$. This completes the proof that every right ideal in A has the form $\mathrm{Hom}_D(V, U)$ for some subspace U in V.

Similarly, if I is a left ideal in A, we set $U = \bigcap_{f \in I} \ker f$ and we clearly have $I \subset \mathrm{Hom}_D(V/U, V)$. Let $f \in I$ be such that $\ker f$ is minimal. If we show $U = \ker f$, then the Lemma yields $\mathrm{Hom}_D(V/U, V) = Af \subset I$, and we are done.

Suppose U is properly contained in $\ker f$. Then there exists $g \in I$ such that $\ker f \cap \ker g \subsetneq \ker f$. Let V_1 (resp. V_2) be a complementary subspace of $\ker f \cap \ker g$ in $\ker f$ (resp. in $\ker g$) and let W be a complementary subspace of $\ker f + \ker g$ in V, so that

$$\ker f = (\ker f \cap \ker g) \oplus V_1, \quad \ker g = (\ker f \cap \ker g) \oplus V_2$$

and

$$V = (\ker f \cap \ker g) \oplus V_1 \oplus V_2 \oplus W.$$

Let π be the projection on $V_2 \oplus W$ parallel to $\ker f$ and π' be the projection on V_1 parallel to $(\ker f \cap \ker g) \oplus V_2 \oplus W$. We have $\pi(\ker f) = 0$, hence $\pi \in \mathrm{Hom}_D(V/\ker f, V) = Af \subset I$. Similarly, $\pi'(\ker g) = 0$ hence $\pi' \in \mathrm{Hom}_D(V/\ker g, V) = Ag \subset I$. Therefore, $\pi + \pi' \in I$; but $\pi + \pi'$ is the projection on $V_1 \oplus V_2 \oplus W$ parallel to $\ker f \cap \ker g$ so $\ker(\pi + \pi') \subsetneq \ker f$, contradicting the minimality of $\ker f$. ∎

(1.6) Corollary. *For every left (resp. right) ideal $I \subset A$ there exists an idempotent $e \in A$ such that $I = Ae$ (resp. $I = eA$). Then* $\mathrm{End}_A(I) = eAe$.

Proof: If $I = \mathrm{Hom}_D(V/U, V)$ (resp. $\mathrm{Hom}_D(V, U)$), choose a complementary subspace U' in V, so that $V = U \oplus U'$, and take for e the projection on U' parallel to U (resp. the projection on U parallel to U'). We then have $I = Ae$ (resp. $I = eA$), by Lemma 1.5.

To prove the last part, observe that for $a \in A$, multiplication on the right (resp. left) by eae defines an endomorphism of left A-modules $r_{eae} : Ae \to Ae$ (resp. an endomorphism of right A-modules $\ell_{eae} : eA \to eA$):

$$(xe)r_{eae} = xeae \qquad \ell_{eae}(ex) = eaex.$$

If this endomorphism is zero, then $(e)r_{eae} = eae = 0$ (resp. $\ell_{eae}(e) = eae = 0$). Therefore, the map $r : eAe \to \mathrm{End}_A(Ae)$ (resp. $\ell_{eae} : eAe \to \mathrm{End}_A(eA)$) is an injective F-algebra homomorphism.

For any endomorphism $f : Ae \to Ae$ (resp. $g : eA \to eA$) of left (resp. right) A-modules we have

$$\begin{aligned} (xe)f &= xe.(e)f && \text{(resp. } g(ex) = g(e).ex\text{)} \\ (e)f &= e.(e)f \in eAe && \text{(resp. } g(e) = g(e).e \in eAe\text{).} \end{aligned}$$

This shows that $r : eAe \to \mathrm{End}_A(Ae)$ (resp. $\ell : eAe \to \mathrm{End}_A(eA)$) is an isomorphism. ∎

Annihilators

For every left ideal I in a central simple algebra A over a field F, the *annihilator* I^0 is defined by:

$$I^0 = \{x \in A \mid I.x = \{0\}\}.$$

This set is clearly a right ideal. Similarly, for every right ideal I, the annihilator I^0 is defined by:

$$I^0 = \{x \in A \mid x.I = \{0\}\};$$

it is a left ideal in A.

(1.7) Proposition. *For every left or right ideal $I \subset A$,*

$$\mathrm{rk}\, I + \mathrm{rk}\, I^0 = \deg A$$

and $I^{00} = I$.

Proof: Let $A = \mathrm{End}_D(V)$. For any subspace $U \subset V$ it follows from the definition of the annihilator that

$$\mathrm{Hom}_D(V, U)^0 = \mathrm{Hom}_D(V/U, V) \quad \text{and} \quad \mathrm{Hom}_D(V/U, V)^0 = \mathrm{Hom}_D(V, U).$$

Since every left (resp. right) ideal $I \subset A$ has the form $I = \mathrm{Hom}_D(V/U, V)$ (resp. $I = \mathrm{Hom}_D(V, U)$), the Proposition follows. ∎

§2. Involutions

In this section, the characteristic of the base field F is always assumed different from 2, although this hypothesis is not necessary for the basic definitions and observations.

2.1. Kinds and types

An *involution* on a central simple algebra A over a field F is a map $\sigma : A \to A$ subject to the following conditions:

1. $\sigma(x+y) = \sigma(x) + \sigma(y)$ for $x, y \in A$.
2. $\sigma(xy) = \sigma(y)\sigma(x)$ for $x, y \in A$.
3. $\sigma^2(x) = x$ for $x \in A$.

Note that the map σ is *not* required to be F-linear. However, applying σ to both sides of the relation $1\sigma(1) = \sigma(1)$ yields $\sigma(1) = 1$. Therefore, the center F $(= F.1)$ is preserved under σ, and the restriction of σ to F is either the identity or an automorphism of period 2.

The involution σ is called *of the first kind* if σ is the identity on F (i.e. σ is F-linear); otherwise it is said to be *of the second kind.* In the latter case, the subfield $F_0 \subset F$ elementwise invariant under σ is of codimension 2.

Occasionally[2], we will be in a situation where the base field is the subfield F_0 rather than the field F. Under scalar extension to an algebraic closure of F_0, the field F, hence also the algebra A, decomposes into a direct product of two factors. It is therefore convenient to extend our discussion of involutions of the second kind to semi-simple F_0-algebras of the form $A \times B$ where A, B are central simple F_0-algebras. An involution of the second kind is then an F_0-linear anti-automorphism $\sigma : A \times B \to A \times B$ of period 2 whose restriction to $F_0 \times F_0$ is the twist: $\sigma(f, g) = (g, f)$. In particular, σ maps $A \times \{0\} = (A \times B) \cdot (1, 0)$ to $\{0\} \times B = (A \times B) \cdot (0, 1)$.

If K is any extension of F, every involution of the first kind σ on A extends to an involution of the first kind $\sigma_K = \sigma \otimes \mathrm{Id}_K$ on $A_K = A \otimes_F K$. In particular, if K is a splitting field of A, we may identify $A_K = \mathrm{End}_K(V)$ for some vector space V over K of dimension $n = \deg A$. The discussion in the introduction to this chapter shows that σ_K is then the adjoint involution with respect to some nonsingular bilinear form b on V, which is either symmetric or skew-symmetric. The involution σ is said to be *of orthogonal type* (or simply *orthogonal*) or *of type* $+1$ if σ_K is the adjoint involution with respect to a symmetric bilinear form; otherwise it is called *of symplectic type* (or simply *symplectic*) or *of type* -1.

To show that this definition does not depend on the choice of the splitting field K, we give an alternative characterization of orthogonal and symplectic involutions in terms of symmetric and skew-symmetric elements.

[2]Notably in the case of (even) Clifford algebras: see Theorem 2.6 of Chapter 2.

For any involution σ on a central simple algebra A, we denote by $(A,\sigma)_+$ and $(A,\sigma)_-$ the sets of symmetric and skew-symmetric elements respectively:

$$(A,\sigma)_+ = \{a \in A \mid \sigma(a) = a\} \qquad (A,\sigma)_- = \{a \in A \mid \sigma(a) = -a\}.$$

If σ is of the first kind, then $(A,\sigma)_+$ and $(A,\sigma)_-$ are vector spaces over the base field F. If σ is of the second kind, then they are vector spaces over the subfield $F_0 \subset F$ of invariant elements under σ. In both cases,

$$A = (A,\sigma)_+ \oplus (A,\sigma)_-$$

since every element $a \in A$ can be decomposed as $a = \frac{1}{2}(a + \sigma(a)) + \frac{1}{2}(a - \sigma(a))$.

(2.1) Proposition. *Let A be a central simple algebra of degree n over F and let σ be an involution on A.*

1. *If σ is of the first kind and orthogonal type, then*

$$\dim_F(A,\sigma)_+ = \frac{n(n+1)}{2} \quad \text{and} \quad \dim_F(A,\sigma)_- = \frac{n(n-1)}{2}.$$

2. *If σ is of the first kind and symplectic type, then*

$$\dim_F(A,\sigma)_+ = \frac{n(n-1)}{2} \quad \text{and} \quad \dim_F(A,\sigma)_- = \frac{n(n+1)}{2}.$$

   Moreover, in this case n is necessarily even.

3. *If σ is of the second kind, let $F_0 \subset F$ be the subfield of invariant elements under σ; then*

$$\dim_{F_0}(A,\sigma)_+ = \dim_{F_0}(A,\sigma)_- = n^2.$$

Proof: Suppose first that σ is of the first kind. Since dimensions do not change under scalar extension, we may extend scalars to a splitting field of A. Therefore, there is no loss of generality if we assume $A = M_n(F) = \mathrm{End}_F(F^n)$.

Suppose σ is the adjoint involution with respect to some nonsingular bilinear form b on F^n and let $u \in \mathrm{GL}_n(F)$ denote the Gram matrix of this form, so that

$$b(x,y) = x^t.u.y \qquad \text{for all } x,y \in F^n,$$

and

$$u^t = \pm u.$$

More precisely, we have $u^t = u$ if b is symmetric (i.e. σ is orthogonal) and $u^t = -u$ if b is skew-symmetric (i.e. σ is symplectic). If n is odd, then every skew-symmetric matrix is singular, so the case $u^t = -u$ arises only when n is even.

Using the above expression for b, the relation $b(x,a(y)) = b(\sigma(a)(x),y)$ for all $x,y \in F^n$ yields

$$\sigma(a) = u^{-1}a^t u \qquad \text{for all } a \in M_n(F).$$

Therefore, $(A,\sigma)_+ = u^{-1}(M_n(F),t)_+$ if $u^t = u$ (i.e. σ is orthogonal) and $(A,\sigma)_+ = u^{-1}(M_n(F),t)_-$ if $u^t = -u$ (i.e. σ is symplectic). Since $\dim_F(M_n(F),t)_+ = \frac{n(n+1)}{2}$, parts *1* and *2* are proved.

Suppose then that σ is of the second kind and let $z \in F^\times$ be such that $\sigma(z) = -z$. Then

$$(A,\sigma)_+ = z(A,\sigma)_- \quad \text{and} \quad (A,\sigma)_- = z(A,\sigma)_+,$$

so that $\dim_{F_0}(A,\sigma)_+ = \dim_{F_0}(A,\sigma)_-$. Since $A = (A,\sigma)_+ \oplus (A,\sigma)_-$, the proof is complete. ∎

2.2. Examples

Given an involution on a central simple algebra A, all the other involutions on A can be obtained by the following Proposition:

(2.2) Proposition. *Let A be a central simple algebra over a field F and let σ be an involution on A.*

a) If σ is of the first kind of type ε $(= \pm 1)$ then for all unit $u \in A^\times$ such that $\sigma(u) = \lambda u$ with $\lambda = \pm 1$, the map $\mathrm{Int}(u)\circ\sigma$ is an involution of the first kind on A of type $\varepsilon\lambda$. Moreover, for every involution σ' of the first kind of type ε' $(= \pm 1)$ there exists a unit $u \in A^\times$ such that $\sigma(u) = \varepsilon\varepsilon'$ and $\sigma' = \mathrm{Int}(u)\circ\sigma$. If $\varepsilon = \varepsilon'$, then

$$(A,\sigma')_+ = u\cdot(A,\sigma)_+ = (A,\sigma)_+\cdot u^{-1} \quad \text{and} \quad (A,\sigma')_- = u\cdot(A,\sigma)_- = (A,\sigma)_-\cdot u^{-1}.$$

If $\varepsilon' = -\varepsilon$, then

$$(A,\sigma')_+ = u\cdot(A,\sigma)_- = (A,\sigma)_-\cdot u^{-1} \quad \text{and} \quad (A,\sigma')_- = u\cdot(A,\sigma)_+ = (A,\sigma)_+\cdot u^{-1}.$$

b) If σ is of the second kind and F_0 denotes the subfield of F elementwise invariant under σ, then for all unit $u \in A^\times$ such that $\sigma(u) = \lambda u$ with $\lambda \in F$ and $\lambda\sigma(\lambda) = 1$, the map $\mathrm{Int}(u)\circ\sigma$ is an involution of the second kind on A which leaves F_0 elementwise invariant. Conversely, for every involution σ' of the second kind leaving F_0 elementwise invariant, there exists a unit $u \in A^\times$ such that $\sigma(u) = u$ and $\sigma' = \mathrm{Int}(u)\circ\sigma$. Then

$$(A,\sigma')_+ = u\cdot(A,\sigma)_+ = (A,\sigma)_+\cdot u^{-1} \quad \text{and} \quad (A,\sigma)_- = u\cdot(A,\sigma)_- = (A,\sigma)_-\cdot u^{-1}.$$

Proof: If $\sigma' = \mathrm{Int}(u)\circ\sigma$ with $\sigma(u) = \pm u$, then a straightforward verification shows that σ' is an involution, and that

$$\begin{aligned} (A,\sigma')_+ &= u\cdot(A,\sigma)_+ = (A,\sigma)_+\cdot u^{-1} && \text{if } \sigma(u) = u \\ (A,\sigma')_+ &= u\cdot(A,\sigma)_- = (A,\sigma)_-\cdot u^{-1} && \text{if } \sigma(u) = -u \end{aligned}$$

If σ is of the first kind, Proposition 2.1 then allows us to compare the types of σ and σ'. On the other hand, if σ' is an involution on A which has the same restriction to F

as σ, then $\sigma' \circ \sigma$ is an automorphism of A which leaves F elementwise invariant. The Skolem-Noether theorem (see for instance [18, Theorem 8.4.2]) then yields an element $u \in A^\times$ such that $\sigma' \circ \sigma = \mathrm{Int}(u)$, i.e.

$$\sigma' = \mathrm{Int}(u) \circ \sigma.$$

It follows that $\sigma'^2 = \mathrm{Int}(u\sigma(u)^{-1})$, hence the relation $\sigma'^2 = I$ yields $\sigma(u) = \lambda u$ for some $\lambda \in F^\times$. Applying σ to both sides of this relation and substituting λu for $\sigma(u)$ in the resulting equation, we get $u = \lambda\sigma(\lambda)u$, hence

$$\lambda\sigma(\lambda) = 1.$$

If σ is of the first kind, it follows that $\lambda^2 = 1$, hence $\sigma(u) = \pm u$. If σ is of the second kind, we get $N_{F/F_0}(\lambda) = 1$, hence Hilbert's theorem 90 yields $\lambda_0 \in F^\times$ such that $\lambda = \lambda_0\sigma(\lambda_0)^{-1}$. Substituting $\lambda_0 u$ for u, we may then assume $\sigma(u) = u$. ∎

(2.3) Example: Quaternion algebras. A *quaternion algebra* over a field F is a central simple F-algebra of dimension 4. Since we assume that the characteristic of F is different from 2, it can be shown (see [18, §8.11]) that every quaternion algebra Q has a basis $1, i, j, k$ subject to the relations:

$$i^2 \in F^\times, \quad j^2 \in F^\times, \quad ij = k = -ji.$$

Such a basis is called a *quaternion basis*; if $i^2 = a$ and $j^2 = b$, the quaternion algebra Q is denoted:

$$Q = (a, b)_F.$$

Conversely, for any $a, b \in F^\times$ the 4-dimensional F-algebra Q with basis $1, i, j, k$ where multiplication is defined through the relations $i^2 = a$, $j^2 = b$, $ij = k = -ji$ is central simple and is therefore a quaternion algebra $(a, b)_F$.

For every quaternion algebra Q, an F-linear map $\gamma : Q \to Q$ can be defined by:

$$\gamma(x) = \mathrm{Trd}_Q(x) - x \qquad \text{for all } x \in Q$$

where Trd_Q is the reduced trace in Q (see for instance [18, §11.5] for the definition of the reduced trace on a central simple algebra). Explicitly,

$$\mathrm{Trd}_Q(x_0 + x_1 i + x_2 j + x_3 k) = 2x_0 \qquad \text{for } x_0, x_1, x_2, x_3 \in F,$$

hence

$$\gamma(x_0 + x_1 i + x_2 j + x_3 k) = x_0 - x_1 i - x_2 j - x_3 k.$$

Direct computations show that γ is an involution, called the *quaternion conjugation* or the *canonical involution* and often denoted by $^-$: $x \mapsto \overline{x} = \gamma(x)$. Clearly, $(Q, \gamma)_+ = F$ and $(Q, \gamma)_-$ has dimension 3, so γ is a symplectic involution. The elements in $(Q, \gamma)_-$ are called *pure quaternions.*

From Proposition 2.2, it follows that every involution of the first kind σ on Q has the form $\sigma = \mathrm{Int}(u) \circ \gamma$ where u is a unit such that $\gamma(u) = \pm u$. If σ is symplectic, then $\gamma(u) = u$, hence $u \in F^\times$ and $\sigma = \gamma$.

In conclusion, every quaternion algebra Q has a unique symplectic involution, namely the canonical involution γ, and orthogonal involutions which are of the form $\mathrm{Int}(u) \circ \gamma$ where u is an invertible pure quaternion.

Involutions of the second kind on quaternion algebras also have a very particular type:

(2.4) Proposition. (Albert) *Let σ be an involution of the second kind on a quaternion algebra Q over a field F and let F_0 be the subfield of F elementwise invariant under σ. There exists a unique F_0-subalgebra $Q_0 \subset Q$ such that*

$$Q = Q_0 \otimes_{F_0} F$$

and

$$\sigma = \gamma_0 \otimes \alpha$$

where γ_0 is the canonical involution on Q_0 and $\alpha = \sigma|_F$ is the non-trivial automorphism of F over F_0. Moreover, the algebra Q_0 is uniquely determined by these conditions.

Proof: Let γ be the canonical involution on Q. Then $\sigma \circ \gamma \circ \sigma$ is an involution of the first kind and symplectic type on Q, so $\sigma \circ \gamma \circ \sigma = \gamma$ since we have observed above that the canonical involution is the unique involution of symplectic type on Q. From this last relation, it follows that $\sigma \circ \gamma$ is an α-semilinear automorphism of period 2 of Q. The F_0-subalgebra Q_0 of invariant elements then satisfies the required conditions. ∎

(The original proof of Albert is in [1, Theorem 10.21]).

Tensor products yield further examples of algebras with involution:

(2.5) Proposition. *Let $A_1, \ldots, A_n$ be central simple algebras with involutions $\sigma_1, \ldots, \sigma_n$ over a field F.*

a) If for all $i = 1, \ldots, n$ the involution σ_i is of the first kind and of type ε_i $(= \pm 1)$, then $\sigma_1 \otimes \cdots \otimes \sigma_n$ is an involution of the first kind on $A_1 \otimes_F \cdots \otimes_F A_n$, of type $\varepsilon_1 \ldots \varepsilon_n$.

b) If all the involutions σ_i are of the second kind and leave elementwise invariant the same subfield F_0 of codimension 2 in F, then $\sigma_1 \otimes \cdots \otimes \sigma_n$ is an involution of the second kind on $A_1 \otimes_F \cdots \otimes_F A_n$ which leaves F_0 invariant.

The proof, by induction on n, is straightforward.

Tensor products of quaternion algebras thus yield examples of central simple algebras with involution. Merkurjev's theorem [14] shows that every central simple algebra with involution is Brauer-equivalent to a tensor product of quaternion algebras. However, there are examples of division algebras with involution of degree 8 which do not decompose into tensor products of quaternion algebras, and there are examples of involutions σ on tensor products of two quaternion algebras which are not of the form $\sigma_1 \otimes \sigma_2$ [2]. A necessary and sufficient decomposability condition for an involution on a tensor product of two quaternion algebras has been given by Knus-Parimala-Sridharan [13].

§3. Existence of involutions

The aim of this section is to give a proof of the following Brauer-group characterization of central simple algebras with involution:

(3.1) Theorem. *Let A be a central simple algebra over a field F.*

a) There is an involution of the first kind on A if and only if $A \otimes_F A$ splits.

b) Suppose F is a quadratic extension of some subfield F_0. There is an involution of the second kind on A which leaves F_0 elementwise invariant if and only if the norm[3] $N_{F/F_0}(A)$ splits.

In particular, if A has an involution, then every central simple algebra Brauer-equivalent to A has an involution of the same type.

The first part is due to Albert [1, Theorem 10.19]. Albert also proved part *(b)* in the case where A is a special kind of crossed product [1, Theorem 10.16]. Part *(b)* was stated in full generality by Riehm [15] and proved by Scharlau [17](see also [18, §8.9]).

Each part requires a separate treatment. We shall follow an approach based on ideas of Tamagawa (oral tradition — see [5, §2]), starting with the case of involutions of the first kind.

3.1. Existence of involutions of the first kind

The fact that $A \otimes_F A$ splits when A has an involution of the first kind is easy to see:

(3.2) Proposition. *Every involution of the first kind σ on a central simple algebra A induces an isomorphism of F-algebras $\sigma_* : A \otimes_F A \to \mathrm{End}_F(A)$ by:*

$$(x)\sigma_*(a \otimes b) = \sigma(a)xb.$$

(Here, A is considered as a left F-vector space, so that endomorphisms are written on the right of the arguments).

Proof: It is straightforward to check that σ_* is an F-algebra homomorphism. It is injective since $A \otimes_F A$ is simple and therefore also surjective by dimension count. ∎

To prove the converse, we will need a special element in $A \otimes_F A$, called the *Goldman element* (after Knus and Ojanguren [10, p. 112]).

[3] see (3.7) below for the definition of the norm of a central simple algebra.

Goldman element

For any central simple algebra A over a field F we may consider the F-linear map

$$\mathrm{Sand} : A \otimes_F A \to \mathrm{End}_F(A)$$

defined by:

$$\mathrm{Sand}(a \otimes b)(x) = axb.$$

(3.3) Lemma. *The map* Sand *is an isomorphism of F-vector spaces.*

Proof: Sand is the composite of the isomorphism $A \otimes_F A \simeq A \otimes_F A^{\mathrm{op}}$ which maps $a \otimes b$ to $a \otimes b^{\mathrm{op}}$ and of the canonical F-algebra isomorphism $A \otimes_F A^{\mathrm{op}} \simeq \mathrm{End}_F(A)$ of Wedderburn's theorem (1.1). ∎

Consider the reduced trace $\mathrm{Trd}_A : A \to F$. Composing this map with the inclusion $F \hookrightarrow A$, we may view Trd_A as an element in $\mathrm{End}_F(A)$.

(3.4) Definition. The *Goldman element* in $A \otimes_F A$ is the unique element $g \in A \otimes_F A$ such that

$$\mathrm{Sand}(g) = \mathrm{Trd}_A .$$

(3.5) Proposition. *The Goldman element $g \in A \otimes_F A$ satisfies the following properties:*

1. $g^2 = 1$.
2. $g.(a \otimes b) = (b \otimes a).g$ *for all* $a, b \in A$.
3. *If A is split: $A = \mathrm{End}_F(V)$, then under the canonical identification $A \otimes_F A = \mathrm{End}_F(V \otimes_F V)$ the element g is defined by:*

$$g(v_1 \otimes v_2) = v_2 \otimes v_1 \qquad \text{for } v_1, v_2 \in V.$$

Proof: We first check *(3)* by using the canonical isomorphism $\mathrm{End}_F(V) = V \otimes_F V^*$. If $(e_i)_{1 \le i \le n}$ is a basis of V and $(e_i^*)_{1 \le i \le n}$ is the dual basis, consider the element

$$g = \sum_{i,j} e_i \otimes e_j^* \otimes e_j \otimes e_i^* \in V \otimes V^* \otimes V \otimes V^* = \mathrm{End}_F(V) \otimes_F \mathrm{End}_F(V).$$

For all $f \in \mathrm{End}_F(V)$, we have

$$\mathrm{Sand}(g)(f) = \sum_{i,j} (e_i \otimes e_j^*) \circ f \circ (e_j \otimes e_i^*) = \sum_{i,j} e_i \otimes e_i^* . e_j^*(f(e_j)).$$

Since $\sum_i e_i \otimes e_i^* = \mathrm{Id}_V$ and $\sum_j e_j^*(f(e_j)) = \mathrm{tr}(f)$, the preceding equation shows that

$$\mathrm{Sand}(g)(f) = \mathrm{tr}(f) \qquad \text{for all } f \in \mathrm{End}_F(V),$$

hence g is the Goldman element in $\mathrm{End}_F(V) \otimes \mathrm{End}_F(V)$. On the other hand, for $v_1, v_2 \in V$ we have

$$\begin{aligned} g(v_1 \otimes v_2) &= \sum_{i,j} (e_i \otimes e_j^*)(v_1) \otimes (e_j \otimes e_i^*)(v_2) \\ &= \left(\sum_i e_i . e_i^*(v_2)\right) \otimes \left(\sum_j e_j . e_j^*(v_1)\right) \\ &= v_2 \otimes v_1. \end{aligned}$$

This completes the proof of *(3)*.

In view of *(3)*, parts *(1)* and *(2)* are easy to check in the split case $A = \mathrm{End}_F(V)$, hence they hold in the general case also: indeed, for any splitting field K of A the Goldman element g in $A \otimes_F A$ is also the Goldman element in $A_K \otimes_K A_K$ since the sandwich map and the reduced trace map commute to scalar extensions. Since A_K is split we have $g^2 = 1$ in $A_K \otimes_K A_K$, and $g.(a \otimes b) = (b \otimes a).g$ for all $a, b \in A_K$, hence also for all $a, b \in A$. ∎

Involutions of the first kind and one-sided ideals

For any involution of the first kind σ on a central simple algebra A, we define a map

$$\sigma' : A \otimes_F A \to A$$

by

$$\sigma'(a \otimes b) = \sigma(a)b.$$

This map is a homomorphism of right $A \otimes A$-modules, if A is endowed with the right $A \otimes A$-module structure defined by: $x.(a \otimes b) = \sigma(a)xb$. (Compare Proposition 3.2). The kernel $\ker \sigma'$ is therefore a right ideal in $A \otimes_F A$. Clearly, no non-zero element of the form $a \otimes 1$ or $1 \otimes a$ is in the kernel of σ'. Dimension count then shows that

$$(A \otimes 1) \oplus \ker \sigma' = A \otimes_F A = \ker \sigma' \oplus (1 \otimes A).$$

If the algebra A is split, let $A = \mathrm{End}(V)$ and let b be a nonsingular (symmetric or skew-symmetric) form on V such that σ is the adjoint involution with respect to b. We may consider b as a linear map $b : V \otimes V \to F$ and identify $A \otimes A = \mathrm{End}(V \otimes V)$. We claim that the map σ' is then defined by the relation:

$$b \circ f = b \circ (\mathrm{Id}_V \otimes \sigma'(f)) \qquad \text{for all } f \in \mathrm{End}(V \otimes V).$$

Since both sides are linear in f, it suffices to verify this relation for $f = f_1 \otimes f_2$, where $f_1, f_2 \in \mathrm{End}(V)$. Then $\sigma'(f) = \sigma(f_1)f_2$, hence for $x, y \in V$ we have

$$b \circ (\mathrm{Id}_V \otimes \sigma'(f))(x \otimes y) = b(x, \sigma(f_1) \circ f_2(y)) = b(f_1(x), f_2(y)) = b \circ f(x \otimes y).$$

This proves the claim.

This observation shows that in the split case

$$\ker \sigma' = \{f \in \mathrm{End}(V \otimes V) \mid b \circ f = 0\}.$$

In particular, if g denotes, as above, the Goldman element: $g(v_1 \otimes v_2) = v_2 \otimes v_1$ for $v_1, v_2 \in V$, it follows that $1 - g \in \ker \sigma'$ if b is symmetric and $1 + g \in \ker \sigma'$ if b is alternating. The same property therefore holds in the general case: $1 - g \in \ker \sigma'$ if σ is orthogonal and $1 + g \in \ker \sigma'$ if σ is symplectic.

(3.6) Theorem. *Let A be a central simple algebra over a field F and let $g \in A \otimes A$ denote its Goldman element. The map $\sigma \mapsto \ker \sigma'$ defines a one-to-one correspondence between the involutions of the first kind on A and right ideals $I \subset A \otimes_F A$ satisfying the following conditions:*

1. $(A \otimes 1) \oplus I = A \otimes_F A = I \oplus (1 \otimes A)$.
2. $I \ni 1 \pm g$.

Under this correspondence, involutions of orthogonal (resp. symplectic) type correspond to ideals containing $1 - g$ (resp. $1 + g$).

Note that, for right ideals $I \subset A \otimes_F A$ satisfying condition *(2)*, any one of the equalities in *(1)* implies the other one. Indeed, condition *(2)* implies that $(1 \pm g)(a \otimes 1)g \in I$ for all $a \in A$; now, Proposition 3.5 shows that $g(a \otimes 1)g = 1 \otimes a$, hence

$$(1 \pm g)(a \otimes 1)g = (a \otimes 1)g \pm (1 \otimes a).$$

Therefore, if I contains $a \otimes 1$ for some $a \in A$, it also contains $1 \otimes a$. Similarly, if it contains $1 \otimes a$, it also contains $a \otimes 1$.

Proof of Theorem 3.6: It was shown above that for each involution σ, the right ideal $\ker \sigma'$ satisfies conditions *(1)* and *(2)*. To prove that the map $\sigma \mapsto \ker \sigma'$ is bijective, we define an inverse map. Suppose I is a right ideal in $A \otimes_F A$ satisfying conditions *(1)* and *(2)*. For every element $a \in A$, we have

$$a \otimes 1 \in A \otimes_F A = I \oplus (1 \otimes A).$$

Therefore, there exists a unique element $\sigma_I(a) \in A$ such that

$$a \otimes 1 - 1 \otimes \sigma_I(a) \in I.$$

The map σ_I is clearly F-linear. We claim that σ_I is an involution on A. For $a, b \in A$, we have

$$(a \otimes 1 - 1 \otimes \sigma_I(a)).(b \otimes 1) \in I \quad \text{and} \quad (b \otimes 1 - 1 \otimes \sigma_I(b)).(1 \otimes \sigma_I(a)) \in I$$

since I is a right ideal. Adding these two relations, we get

$$ab \otimes 1 - 1 \otimes \sigma_I(b)\sigma_I(a) \in I,$$

which shows that $\sigma_I(ab) = \sigma_I(b)\sigma_I(a)$. On the other hand, from condition *(2)* it follows that for every $u \in I$,

$$(1 \pm g).u - u \in I,$$

hence $gu \in I$. Therefore, for all $a \in A$ we have $g(a \otimes 1 - 1 \otimes \sigma_I(a))g \in I$, hence

$$\sigma_I(a) \otimes 1 - 1 \otimes a \in I.$$

This shows $\sigma_I^2(a) = a$ and completes the proof of the claim that σ_I is an involution of the first kind on A.

Let $\sigma_I' : A \otimes_F A \to A$ be the corresponding map, defined by $\sigma_I'(a \otimes b) = \sigma_I(a)b$. Let $u = \sum u_i' \otimes u_i'' \in A \otimes A$. If $u \in \ker \sigma_I'$, then $\sum \sigma_I(u_i')u_i'' = 0$, hence

$$u = \sum_i (u_i' \otimes u_i'' - 1 \otimes \sigma_I(u_i')u_i'') = \sum_i (u_i' \otimes 1 - 1 \otimes \sigma_I(u_i')).(1 \otimes u_i'').$$

This shows that $\ker \sigma_i'$ is generated as a right ideal in $\otimes A$ by elements of the form $a \otimes 1 - 1 \otimes \sigma_I(a)$. Since these elements are all in I, by definition of σ_I, it follows that $\ker \sigma_I' \subset I$; but these ideals have the same dimension, hence $\ker \sigma_I' = I$.

Conversely, if σ is any involution of the first kind on A, then

$$a \otimes 1 - 1 \otimes \sigma(a) \in \ker \sigma' \qquad \text{for all } a \in A,$$

hence $\sigma_{\ker \sigma'} = \sigma$. Therefore, the maps $\sigma \mapsto \ker \sigma'$ and $I \mapsto \sigma_I$ are inverse bijections between the set of involutions of the first kind on A and the set of right ideals in $A \otimes_F A$ satisfying conditions *(1)* and *(2)*. ∎

We can now complete the proof of Albert's theorem (case *(a)* of Theorem 3.1). According to Wedderburn's theorem (see 1.1), we may find a central division algebra D over F such that

$$A \simeq M_r(D) \qquad \text{for some integer } r.$$

The condition that $A \otimes_F A$ is split implies that $D \otimes_F D$ is also split, hence minimal right ideals in $D \otimes_F D$ have dimension $\deg(D \otimes_F D) = \dim_F D$, and maximal right ideals have dimension $(\dim_F D)^2 - \dim_F D$. Let I be a maximal right ideal containing $1 - g$. Since D is a division algebra, $D \otimes 1$ and $1 \otimes D$ intersect I trivially; therefore, dimension count shows that

$$(D \otimes 1) \oplus I = D \otimes_F D = I \oplus (1 \otimes D).$$

It then follows from Theorem 3.6 that D has an (orthogonal) involution of the first kind, which we denote by $\bar{}$. An involution of the first kind σ is then defined on $M_r(D)$ by

$$\sigma((a_{ij})_{1 \le i,j \le r}) = (\overline{a_{ji}})_{1 \le i,j \le r}$$

and transported to A by the isomorphism $A \simeq M_r(D)$.

3.2. Existence of involutions of the second kind

Before discussing involutions of the second kind, we recall the construction of the norm of a central simple algebra, in the particular case of interest in this section.

The norm (or corestriction) of central simple algebras

Let K/L be a finite separable extension of fields. For every central simple K-algebra A, there is a central simple L-algebra $N_{K/L}(A)$ of degree $(\deg A)^{[K:L]}$, called the *norm* of A, defined so as to induce a homomorphism of Brauer groups

$$N_{K/L} : \mathrm{Br}(K) \to \mathrm{Br}(L)$$

which corresponds to the corestriction map in Galois cohomology.

In view of Theorem 3.1, we shall only discuss here the case where K/L is a quadratic extension, referring to [6, §8] (and [21]) for a more general treatment along similar lines.

The case of quadratic extensions is particularly simple in view of the fact that separable quadratic extensions are Galois. Let K/L be such an extension, and let

$$\mathrm{Gal}(K/L) = \{\mathrm{Id}_K, \alpha\}$$

denote its Galois group. For any K-algebra A, we define the conjugate algebra

$${}^{\alpha}A = \{{}^{\alpha}a \mid a \in A\}$$

with the following operations:

$${}^{\alpha}a + {}^{\alpha}b = {}^{\alpha}(a+b) \qquad {}^{\alpha}a.{}^{\alpha}b = {}^{\alpha}(ab) \qquad {}^{\alpha}(ka) = \alpha(k){}^{\alpha}a$$

for $a, b \in A$ and $k \in K$. The switch map

$$s : {}^{\alpha}A \otimes_K A \to {}^{\alpha}A \otimes_K A$$

defined by

$$s({}^{\alpha}a \otimes b) = {}^{\alpha}b \otimes a$$

is α-semilinear over K and is an L-algebra automorphism.

(3.7) Definition. The *norm* $N_{K/L}(A)$ of the K-algebra A is the L-subalgebra of ${}^{\alpha}A \otimes_K A$ elementwise invariant under the switch map:

$$N_{K/L}(A) = \{u \in {}^{\alpha}A \otimes_K A \mid s(u) = u\}.$$

Of course, the same construction can be used to define the norm $N_{K/L}(V)$ of any K-vector space V.

(3.8) Proposition. *1. For any K-algebra A,*

$$N_{K/L}(A)_K = {}^{\alpha}A \otimes_K A.$$

2. *For any K-algebras A, B,*

$$N_{K/L}(A \otimes_K B) = N_{K/L}(A) \otimes_L N_{K/L}(B).$$

3. *For any finite-dimensional K-vector space V,*

$$N_{K/L}(\mathrm{End}_K(V)) = \mathrm{End}_L(N_{K/L}(V)).$$

4. *If A is a central simple K-algebra, the norm $N_{K/L}(A)$ is a central simple L-algebra of degree*

$$\deg N_{K/L}(A) = (\deg A)^2.$$

Moreover, the norm induces a group homomorphism

$$N_{K/L} : \mathrm{Br}(K) \to \mathrm{Br}(L).$$

5. *For any central simple L-algebra A,*

$$N_{K/L}(A_K) \simeq A \otimes_L A.$$

Proof: (1): Since $N_{K/L}(A)$ is an L-subalgebra of ${}^{\alpha}A \otimes_K A$, there is a natural map $N_{K/L}(A) \otimes_L K \to {}^{\alpha}A \otimes_K A$ induced by multiplication in ${}^{\alpha}A \otimes_K A$. This map is a homomorphism of K-algebras; it is bijective since if $K = L(\sqrt{d})$ every element $a \in {}^{\alpha}A \otimes_K A$ can be written in a unique way as[4] $a = a_1 + a_2\sqrt{d}$ with a_1, a_2 invariant under the switch map s:

$$a = \left[\tfrac{1}{2}(a + s(a))\right] + \left[\tfrac{1}{2}(a - s(a))(\sqrt{d})^{-1}\right]\sqrt{d}.$$

(2) is straightforward (see [6, p. 55] or [18, Lemma 8.9.7]). The canonical map $N_{K/L}(A) \otimes_L N_{K/L}(B) \to N_{K/L}(A \otimes_K B)$ corresponds, after extending scalars to K, to the map

$$({}^{\alpha}A \otimes_K A) \otimes_K ({}^{\alpha}B \otimes_K B) \to {}^{\alpha}(A \otimes_K B) \otimes_K (A \otimes_K B)$$

which carries ${}^{\alpha}a_1 \otimes a_2 \otimes {}^{\alpha}b_1 \otimes b_2$ to ${}^{\alpha}(a_1 \otimes b_1) \otimes (a_2 \otimes b_2)$.

(3): There is a natural isomorphism:

$${}^{\alpha}\mathrm{End}_K(V) = \mathrm{End}_K({}^{\alpha}V)$$

which identifies ${}^{\alpha}f$ for $f \in \mathrm{End}_K(V)$ to the endomorphism of ${}^{\alpha}V$ mapping ${}^{\alpha}v$ to ${}^{\alpha}(f(v))$. We may therefore identify:

$${}^{\alpha}\mathrm{End}_K(V) \otimes_K \mathrm{End}_K(V) = \mathrm{End}_K({}^{\alpha}V \otimes_K V),$$

[4] To get a proof valid in all characteristics, choose $a_1 = (s(a)k - a\alpha(k))(k - \alpha(k))^{-1}$ and $a_2 = (a - s(a))(k - \alpha(k))^{-1}$ for any $k \in K \setminus L$.

and check that the switch map s is then identified to conjugation by s_V, where $s_V : {}^{\alpha}V \otimes_K V \to {}^{\alpha}V \otimes_K V$ is the α-linear map defined through:

$$s_V({}^{\alpha}v \otimes w) = {}^{\alpha}w \otimes v \quad \text{for } v, w \in V.$$

The L-algebra $N_{K/L}(\mathrm{End}_K(V))$ of fixed elements under s is then identified to the L-algebra of endomorphisms of the L-subspace elemntwise invariant under s_V, i.e. to $\mathrm{End}_L(N_{K/L}V)$.

(4): If A is a central simple K-algebra, then ${}^{\alpha}A \otimes_K A$ also is central simple over K, hence $N_{K/L}(A)$ is central simple over L, by the first part of this Proposition. If A' is Brauer-equivalent to A, then we may find vector spaces V, V' over K such that

$$A \otimes_K \mathrm{End}_K(V) \simeq A' \otimes_K \mathrm{End}_K(V').$$

It then follows from parts *(2)* and *(3)* above that

$$N_{K/L}(A) \otimes_L \mathrm{End}_L(N_{K/L}V) \simeq N_{K/L}(A') \otimes_L \mathrm{End}_L(N_{K/L}V'),$$

hence $N_{K/L}(A)$ and $N_{K/L}(A')$ are Brauer-equivalent. Part *(2)* above moreover shows that the Brauer-group map induced by $N_{K/L}$ is a homomorphism.

To prove *(5)*, we first note that if A is an L-algebra, then ${}^{\alpha}(A_K) = A_K$ under the identification ${}^{\alpha}(a \otimes k) = a \otimes \alpha(k)$. Therefore,

$${}^{\alpha}(A_K) \otimes_K A_K \simeq A \otimes_L A \otimes_L K$$

and $N_{K/L}(A)$ can be identified to the L-algebra elementwise invariant under the L-algebra automorphism s' of $A \otimes_L A \otimes_L K$ defined through:

$$s'(a_1 \otimes a_2 \otimes k) = a_2 \otimes a_1 \otimes \alpha(k).$$

On the other hand, $A \otimes_L A$ can be identified to the algebra of fixed points under the automorphism s'' defined through:

$$s''(a_1 \otimes a_2 \otimes k) = a_1 \otimes a_2 \otimes \alpha(k).$$

We aim to show that these F-algebras are isomorphic when A is central simple.

Let $g \in A \otimes_L A$ be the Goldman element (see (3.4)). By Proposition 3.5, we have

$$g^2 = 1 \quad \text{and} \quad g(a_1 \otimes a_2) = (a_2 \otimes a_1)g \quad \text{for all } a_1, a_2 \in A,$$

hence for all $x \in A \otimes_L A$, $s'(x \otimes 1) = gxg^{-1} \otimes 1$. In particular:

$$s'(g \otimes 1) = g \otimes 1,$$

and moreover

$$s''(y) = (g \otimes 1).s'(y).(g \otimes 1)^{-1} \quad \text{for all } y \in A \otimes_L A \otimes_L K.$$

Let $k \in K$ be such that $\alpha(k) \neq \pm k$ and let

$$u = k + (g \otimes 1)\sigma(k) \in A \otimes_L A \otimes_L K.$$

This element is invertible, since $u.(k - (g \otimes 1)\alpha(k)) = k^2 - \alpha(k)^2 \in K^\times$; moreover,

$$s'(u) = \alpha(k) + (g \otimes 1)k = u.(g \otimes 1).$$

Therefore, for all $x \in A \otimes_L A \otimes_L K$,

$$s'(uxu^{-1}) = u(g \otimes 1)\alpha'(x)(g \otimes 1)^{-1}u^{-1} = u\,s''(x)u^{-1}.$$

This equation shows that conjugation by u induces an isomorphism from the L-algebra of invariant elements under s'' onto the L-algebra of invariant elements under s', hence

$$A \otimes_L A \simeq N_{K/L}(A_K).$$

■

Remarks:

1. Property *(5)* in the Proposition above does not hold for arbitrary L-algebras. For instance, one may check as an exercise that $N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}_\mathbb{C}) \simeq \mathbb{R} \times \mathbb{R} \times \mathbb{C}$, whereas $\mathbb{C} \otimes_\mathbb{R} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$.

2. The proof of property *(5)* above in [6, p. 55] is flawed: see the correction in [21].

We now come back to the proof of Theorem 3.1. As in the case of involutions of the first kind, the necessary condition for the existence of an involution of the second kind is easy to prove:

(3.9) Proposition. *Let σ be an involution of the second kind on a central simple F-algebra A and let F_0 denote the subfield of F elementwise invariant under σ. There is a natural isomorphism of F_0-algebras:*

$$\sigma_* : N_{F/F_0}(A) \xrightarrow{\sim} \mathrm{End}_{F_0}((A,\sigma)_+).$$

Proof: Let α denote the non-trivial element of the Galois group of F over F_0. The map

$$\sigma_* : {}^\alpha A \otimes_F A \to \mathrm{End}_F(A)$$

defined by

$$(x)\sigma_*({}^\alpha a \otimes b) = \sigma(a)xb$$

is an isomorphism of F-algebras since ${}^\alpha A \otimes_F A$ and $\mathrm{End}_F(A)$ have the same dimension and ${}^\alpha A \otimes_F A$ is simple. We have

$$(\sigma(x))\sigma_*({}^\alpha b \otimes a) = \sigma(\sigma_*({}^\alpha a \otimes b)(x)),$$

so if $u \in {}^\alpha A \otimes_F A$ is invariant under the switch map $s : {}^\alpha A \otimes_F A \to {}^\alpha A \otimes_F A$, then $\sigma_*(u)$ maps $(A,\sigma)_+$ to itself. Therefore, σ_* restricts to an injective homomorphism of F_0-algebras $\sigma_* : N_{F/F_0}(A) \to \mathrm{End}_{F_0}((A,\sigma)_+)$. Dimension count shows that this homomorphism is an isomorphism. ■

Involutions of the second kind and one-sided ideals

As above, let σ be an involution of the second kind on a central simple F-algebra A and denote by F_0 the subfield of F elementwise invariant under σ. The natural isomorphism σ_* of the preceding Proposition endows $(A,\sigma)_+$ with a right $N_{F/F_0}(A)$-module structure.

Let $\sigma' : N_{F/F_0}(A) \to (A,\sigma)_+$ be defined by:

$$\sigma'(u) = 1.u \ (= (1)\sigma_*(u)).$$

Since $\sigma_*(N_{F/F_0}(A)) = \mathrm{End}_{F_0}((A,\sigma)_+)$, it is clear that the map σ' is surjective, hence $\ker\sigma'$ is a right ideal of dimension $n^4 - n^2$, where $n = \deg A$. Extending scalars to F, we have $N_{F/F_0}(A)_F = {}^{\alpha}A \otimes_F A$ and the map $\sigma'_F : {}^{\alpha}A \otimes_F A \to A$ induced by σ' is:

$$\sigma'_F({}^{\alpha}a \otimes b) = \sigma(a)b.$$

Therefore, $({}^{\alpha}a \otimes 1) \cap \ker\sigma'_F = \{0\} = \ker\sigma' \cap (1 \otimes A)$, hence

$$({}^{\alpha}A \otimes 1) \oplus \ker\sigma'_F = {}^{\alpha}A \otimes_F A = \ker\sigma'_F \oplus (1 \otimes A).$$

(3.10) Theorem. *Let A be a central simple algebra over a field F. Suppose $F_0 \subset F$ is a field of codimension 2. The map $\sigma \mapsto \ker\sigma'$ defines a one-to-one correspondence between involutions of the second kind on A leaving F_0 elementwise invariant and right ideals $I \subset N_{F/F_0}(A)$ such that*

$$({}^{\alpha}A \otimes 1) \oplus I_F = {}^{\alpha}A \otimes_F A = I_F \oplus (1 \otimes A).$$

Proof: We have already checked that for each involution σ the ideal $\ker\sigma'$ satisfies the condition above. Conversely, suppose I is a right ideal such that ${}^{\alpha}A \otimes_F A = I_F \oplus (1 \otimes A)$; For each $a \in A$, there is a unique element $\sigma_I(a) \in A$ such that

$${}^{\alpha}a \otimes 1 - 1 \otimes \sigma_I(a) \in I_F. \tag{1.2}$$

The map $\sigma_I : A \to A$ is α-semilinear and the same arguments as in the proof of Theorem 3.6 show that it is an anti-automorphism on A.

In order to check that $\sigma_I^2(a) = a$ for all $a \in A$, we use the fact that the ideal I_F is preserved under the switch map $s : {}^{\alpha}A \otimes_F A \to {}^{\alpha}A \otimes_F A$, since it is extended from an ideal I in $N_{F/F_0}(A)$. Therefore, applying s to relation (1.2) we get

$$1 \otimes a - {}^{\alpha}\sigma_I(a) \otimes 1 \in I_F,$$

hence $\sigma_I^2(a) = a$.

Let $\ker\sigma'_I$ be the ideal in $N_{F/F_0}(A)$ corresponding to the involution σ_I. Arguing as in Theorem 3.6, we see that $(\ker\sigma'_I)_F = I_F$, and conclude that $\ker\sigma'_I = I$, since I (resp. $\ker\sigma'_I$) is the subset of invariant elements in I_F (resp. $(\ker\sigma'_I)_F$) under the switch map.

On the other hand, for any given involution σ on A we have

$${}^{\alpha}a \otimes 1 - 1 \otimes \sigma(a) \in \ker\sigma'_F \qquad \text{for all } a \in A,$$

hence $\sigma_{\ker\sigma'} = \sigma$. ∎

We may now complete the proof of Theorem 3.1. Suppose $A \simeq M_r(D)$ for some central division algebra D over F and some integer r. Since the norm map N_{F/F_0} is defined on the Brauer group of F, the condition that $N_{F/F_0}(A)$ splits implies that $N_{F/F_0}(D)$ also splits. Let I be a maximal right ideal in $N_{F/F_0}(D)$. We have $\dim_{F_0} I = \dim_{F_0} N_{F/F_0}(D) - \deg N_{F/F_0}(D) = (\dim_F D)^2 - \dim_F D$. Moreover, since D is a division algebra, it is clear that $({}^{\alpha}D \otimes 1) \cap I_F = \{0\} = I_F \cap (1 \otimes D)$, hence

$$({}^{\alpha}D \otimes 1) \oplus I_F = {}^{\alpha}D \otimes_F D = I_F \oplus (1 \otimes D),$$

by dimension count. The preceding Theorem then shows that D has an involution of the second kind $^-$ leaving F_0 elementwise invariant. An involution σ of the same kind can then be defined on $M_r(D)$ by

$$\sigma((a_{ij})_{1 \le i,j \le r}) = (\overline{a_{ji}})_{1 \le i,j \le r}$$

and transported to A by the isomorphism $A \simeq M_r(D)$. ∎

Part *(b)* of Theorem 3.1 can easily be extended to cover also the case of semi-simple F_0-algebras $A \times B$ with A, B central simple over F_0. The norm $N_{F_0 \times F_0/F_0}$ is defined as follows:

$$N_{F_0 \times F_0/F_0}(A \times B) = A \otimes_{F_0} B.$$

This definition is consistent with Definition 3.7, and it is easy to check that Proposition 3.8 extends to the case where $F = F_0 \times F_0$.

If $\sigma : A \times B \to A \times B$ is an involution of the second kind, then the restriction of σ to A $(= A \times \{0\})$ is an anti-isomorphism $\sigma_A : A \to B$. Therefore, $A \otimes_{F_0} B$ splits.

Conversely, if $A \otimes_{F_0} B$ splits, then A and B are anti-isomorphic. Let $\sigma_A : A \to B$ be an anti-isomorphism. We may then define an involution of the second kind σ on $A \times B$ by:

$$\sigma(x, y) = (\sigma_A^{-1}(y), \sigma_A(x)).$$

§4. Hermitian forms

In this section, we set up a one-to-one correspondence between involutions on central simple algebras and hermitian forms on vector spaces over division algebras.

If A is a central simple algebra over a field F and V is a simple left A-module, then according to Theorem 1.1 the algebra $D = \mathrm{End}_A(V)$ is a division algebra, V is a right vector space over D and A may be identified to the algebra of D-endomorphisms of V:

$$A = \mathrm{End}_D(V).$$

Since D is Brauer-equivalent to A, Theorem 3.1 shows that A has an involution if and only if D has an involution. Therefore, in this section we will work from the point of view that central simple algebras with involution are algebras of endomorphisms of vector spaces over division algebras with involution.

4.1. Adjoint involutions

Let D be a central division algebra over a field F and let V be a finite-dimensional right vector space over D. Suppose $^-: D \to D$ is an involution on D and $\lambda \in F$ is such that $\lambda\overline{\lambda} = 1$. (In particular, $\lambda = \pm 1$ if $^-$ is of the first kind). A *λ-hermitian form* on V (with respect to the involution $^-$ on D) is a bi-additive map

$$h : V \times V \to D$$

such that, for $x, y \in V$ and $d \in D$,

$$h(x, yd) = h(x, y)d \qquad h(xd, y) = \overline{d}h(x, y)$$

and

$$h(y, x) = \lambda\overline{h(x, y)}.$$

Every λ-hermitian form h induces a map

$$\hat{h} : V \to V^* = \mathrm{Hom}_D(V, D)$$

defined by $\hat{h}(x)(y) = h(x, y)$ for $x, y \in V$. This map is D-linear if V^* is endowed with the right D-vector space structure defined by

$$\psi.d = \overline{d}\psi \qquad \text{for } \psi \in V^* \text{ and } d \in D,$$

i.e. $(\psi.d)(x) = \overline{d}\psi(x)$ for $x \in V$.

The λ-hermitian form h is called *nonsingular* if $\hat{h}$ is bijective, which amounts to the following condition: if $x \in V$ is such that $h(x, y) = 0$ for all $y \in V$, then $x = 0$. If this condition holds, then a map $\sigma_h : \mathrm{End}_D(V) \to \mathrm{End}_D(V)$ may be defined by:

$$\sigma_h(f) = \hat{h}^{-1} \circ f^t \circ \hat{h}.$$

Equivalently, $\sigma_h(f)$ is defined by the following condition:

$$h(x, f(y)) = h(\sigma_h(f)(x), y) \qquad \text{for all } x, y \in V.$$

Direct verifications show that σ_h is an involution on $\mathrm{End}_D(V)$ such that $\sigma_h(x) = \overline{x}$ for all $x \in F$. It is called the *adjoint involution* with respect to the λ-hermitian form h.

The following Theorem is the expected generalization of the result proven in the introduction to this chapter:

(4.1) Theorem. *The map $h \mapsto \sigma_h$ defines a one-to-one correspondence between nonsingular λ-hermitian forms on V (with respect to the involution $^-$ on D) up to a factor in $F^\times$ and involutions σ on $\mathrm{End}_D(V)$ such that $\sigma(x) = \overline{x}$ for all $x \in F$.*

If $^-$ is of the first kind and type ε $(= \pm 1)$, the adjoint involution with respect to a λ-hermitian form is of type $\varepsilon\lambda$.

Proof: If h and h' are nonsingular λ-hermitian forms on V, then the map $v = \hat{h}^{-1} \circ \hat{h}' \in \mathrm{GL}_D(V)$ is such that

$$h'(x,y) = h(v(x),y) \qquad \text{for all } x,y \in V.$$

Therefore, the adjoint involutions $\sigma_h, \sigma_{h'}$ are related by:

$$\sigma_h = \mathrm{Int}(v) \circ \sigma_{h'}.$$

Therefore, if $\sigma_h = \sigma_{h'}$, then $v \in F^\times$ and the forms h, h' differ by a factor in $F^\times$.

On the other hand, if h is a nonsingular λ-hermitian form on V with adjoint involution σ_h and if σ' is an arbitrary involution on $\mathrm{End}_D(V)$ such that $\sigma'(x) = \overline{x}$ $(= \sigma_h(x))$ for all $x \in F$, then $\sigma_h \circ \sigma'^{-1}$ is an inner automorphism of $\mathrm{End}_D(V)$, by the Skolem-Noether theorem. Let

$$\sigma_h \circ \sigma'^{-1} = \mathrm{Int}(u) \qquad \text{for some } u \in \mathrm{GL}_D(V).$$

Then σ' is the adjoint involution with respect to the λ-hermitian form h' defined by

$$h'(x,y) = h(u(x),y) \qquad \text{for } x,y \in V.$$

This shows that the correspondence between nonsingular λ-hermitian forms on V up to a factor in $F^\times$ and involutions on $\mathrm{End}_D(V)$ is bijective.

Suppose now that the involution $^-$ on D is of the first kind and type ε $(= \pm 1)$. If $\dim_D V = r$, we identify V to D^r, hence also $\mathrm{End}_D(V)$ to $M_r(D)$, by means of a basis $(e_i)_{1 \le i \le r}$ of V. Let τ be the involution on $M_r(D)$ defined by

$$\tau((d_{ij})_{1 \le i,j \le r}) = (\overline{d_{ji}})_{1 \le i,j \le r}.$$

Symmetric matrices under τ have arbitrary entries d_{ij} for $i < j$ and diagonal entries which are symmetric under $^-$; therefore,

$$\dim_F(M_r(D),\tau)_+ = \frac{r(r-1)}{2} \dim_F D + r \dim_F(D,^-)_+.$$

It then follows from Proposition 2.1 that τ is of type ε.

Let now h be a nonsingular λ-hermitian form on V with respect to the involution $^-$ on D (so $\lambda = \pm 1$, since $^-$ is of the first kind), and let h_e denote the matrix of h with respect to the basis $(e_i)_{1 \le i \le r}$:

$$h_e = (h(e_i,e_j))_{1 \le i,j \le r}.$$

The condition $h(e_i,e_j) = \lambda \overline{h(e_j,e_i)}$ yields $h_e = \lambda \tau(h_e)$. Moreover, for $x,y \in D^r$ $(= V)$ we have

$$h(x,y) = \overline{x}^t . h_e . y,$$

and the adjoint involution σ_h on $M_r(D)$ $(= \mathrm{End}_D(V))$ is therefore given by

$$\sigma_h(f) = \tau(h_e f h_e^{-1}) = h_e^{-1} \tau(f) h_e,$$

or, equivalently,

$$\sigma_h = \mathrm{Int}(h_e^{-1}) \circ \tau.$$

By Proposition 2.2*(a)*, it follows that σ_h is of type $\varepsilon\lambda$, since $\tau(h_e^{-1}) = \lambda h_e^{-1}$. ∎

4.2. The Witt index

Using the correspondence set up in the preceding Theorem, we can transfer to involutions various notions defined for hermitian forms, provided they are invariant under the similarity relation. As a first case, we consider here the Witt index. The following results are taken from [4].

If h is a nonsingular λ-hermitian form on a vector space V over a central division F-algebra D, then for every subspace W the orthogonal subspace $W^\perp$ is defined by

$$\begin{aligned} W^\perp &= \{x \in V \mid h(x,y) = 0 \text{ for all } y \in W\} \\ &= \{x \in V \mid h(y,x) = 0 \text{ for all } y \in W\}. \end{aligned}$$

A vector $v \in V$ is called *isotropic* if $h(v,v) = 0$; a subspace $W \subset V$ is called *totally isotropic* if $W \subset W^\perp$ or, equivalently, if every vector in W is isotropic. The *Witt index* $w(V,h)$ is the maximum of the dimensions of totally isotropic subspaces in V (or the dimension of a maximal totally isotropic subspace in V, since they all have the same dimension).

Using the correspondence between subspaces of V and right ideals in $\mathrm{End}_D(V)$, we may define corresponding notions for central simple algebras with involution:

(4.2) Definition. For every right ideal I in an algebra with involution (A,σ), the orthogonal $I^\perp$ is defined by:

$$I^\perp = \{x \in A \mid \sigma(x)y = 0 \text{ for all } y \in I\}.$$

Equivalently, $I^\perp$ can be defined as the annihilator of the left ideal $\sigma(I)$:

$$I^\perp = \sigma(I)^0;$$

therefore, $I^\perp$ is a right ideal.

(4.3) Proposition. *For every right ideal $I \subset A$,*

$$\mathrm{rk}\, I + \mathrm{rk}\, I^\perp = \deg A$$

and $I^{\perp\perp} = I$. Moreover, if $(A,\sigma) = (\mathrm{End}_D(V), \sigma_h)$ and $I = \mathrm{Hom}_D(V,W)$ for some subspace $W \subset V$, then

$$I^\perp = \mathrm{Hom}_D(V, W^\perp).$$

Proof: Since $\mathrm{rk}\,\sigma(I) = \mathrm{rk}\, I$, the first relation follows from the corresponding statement for annihilators (Proposition 1.7). This first relation implies that $\mathrm{rk}\, I^{\perp\perp} = \mathrm{rk}\, I$. Since the inclusion $I \subset I^{\perp\perp}$ is obvious, we get $I = I^{\perp\perp}$. Finally, suppose $I = \mathrm{Hom}_D(V,W)$ for some subspace $W \subset V$. For every $f \in \mathrm{End}_D(V)$, $g \in I$ we have

$$g(y) \in W \qquad \text{and} \qquad h(f(x), g(y)) = h(x, \sigma(f) \circ g(y)) \quad \text{for all } x,y \in V.$$

Therefore, $\sigma(f) \circ g = 0$ if and only if $f(x) \in W^\perp$, hence

$$I^\perp = \mathrm{Hom}_D(V, W^\perp).$$

■

In view of the Proposition above, the following definitions are natural:

(4.4) Definitions. An ideal I in a central simple algebra with involution (A, σ) is called *isotropic* if $I \subset I^\perp$. The *Witt index* of the algebra with involution (A, σ) (or simply of the involution σ) is defined by:

$$w(A, \sigma) = \max\{\operatorname{rk} I \mid I \subset I^\perp\}.$$

If I is an isotropic ideal, then $\operatorname{rk} I \leq \operatorname{rk} I^\perp$, hence by the preceding Proposition $\operatorname{rk} I \leq \frac{1}{2} \deg A$. Moreover, the (Schur) index $\operatorname{ind} A$ divides $\operatorname{rk} I$ for every right ideal I (see § 1.2), hence

$$\operatorname{ind} A \text{ divides } w(A, \sigma) \quad \text{and} \quad w(A, \sigma) \leq \frac{\deg A}{2}.$$

In particular, if $w(A, \sigma)$ is small (but non-zero!), then $\operatorname{ind} A$ is also small.

The algebra with involution (A, σ) is called *isotropic* if $w(A, \sigma) > 0$ or, equivalently, if there exists a non-zero element $x \in A$ such that $\sigma(x)x = 0$. (The right ideal xA is then isotropic). It is called *hyperbolic* if $w(A, \sigma) = \frac{1}{2} \deg A$. Of course, if A is a division algebra, then necessarily $w(A, \sigma) = 0$, i.e. (A, σ) is anisotropic.

Exercises for Chapter 1.

1. Let (A, σ) be a central simple F-algebra with involution of the first kind and let $K \subset A$ be a subfield containing F. Suppose K consists of symmetric elements, so that the restriction $\sigma' = \sigma|_{C_A K}$ of σ to the centralizer of K is of the first kind. Show that σ and σ' are of the same type.

2. Let (A, σ) be a central simple algebra with involution and let e be a symmetric idempotent in A. Show that the restriction of σ to eAe is of the same kind and of the same type as σ.

3. Let (A, σ) be a central simple F-algebra with involution of the first kind. Under the isomorphism $\sigma_* : A \otimes_F A \to \mathrm{End}_F(A)$, the involution $\sigma \otimes \sigma$ is transported to the adjoint involution σ_b with respect to some nonsingular bilinear form b on A. Find b.

4. (Rowen - Saltman [16]) Let V be a vector space of dimension n over a field F and let σ be an involution of the first kind on $\mathrm{End}(V)$. Prove that σ is orthogonal if and only if there exist n symmetric orthogonal[5] idempotents in $\mathrm{End}(V)$. Prove that σ is symplectic if and only if there exist $n = 2m$ skew-symmetric elements $e_i, f_i \in \mathrm{End}(V)$ (where $i = 1, \ldots, m$) subject to:

$$e_i e_j = f_i f_j = 0 \qquad \text{for all } i, j;$$

$$e_i f_j = f_j e_i = 0 \qquad \text{for all } i \neq j;$$

$$e_i f_i \text{ and } f_i e_i \text{ are idempotents such that } \sum_{i=1}^{n} (e_i f_i + f_i e_i) = \mathrm{Id}_V .$$

5. Let K/L be a quadratic extension of fields of characteristic different from 2, and let $a \in L$, $b \in K$. Prove the "projection formula" for the norm of the quaternion algebra $(a, b)_K$:

$$N_{K/L}(a, b)_K \simeq (a, N_{K/L}(b))_L.$$

6. (Notation as in the preceding exercise). Show that if $(a, N_{K/L}(b))_L$ is split, then there exists an element $b' \in F^\times$ such that $(a, b)_K \simeq (a, b')_L \otimes_L K$.

7. Let (A, σ) be a central simple algebra with involution and let I, J be right ideals in A. Prove: $(I + J)^\perp = I^\perp \cap J^\perp$ and $(I \cap J)^\perp = I^\perp + J^\perp$.

8. Use the preceding exercise to show that all the maximal isotropic right ideals in a central simple algebra with involution have the same rank.

   [Hint: If J is an isotropic ideal and I is an arbitrary right ideal, show that $\mathrm{rk}\, J - \mathrm{rk}(I^\perp \cap J) \leq \mathrm{rk}\, I - \mathrm{rk}(I \cap J)$. If I is also isotropic and $\mathrm{rk}\, I < \mathrm{rk}\, J$, use this relation to show $I^\perp \cap J \not\subset I$, and conclude that $I + (I^\perp \cap J)$ is an isotropic ideal which strictly contains I.]

[5] Two idempotents e, f are called orthogonal if $ef = fe = 0$.

9. (Bayer-Fluckiger - Shapiro - Tignol [4]) Let I be a right ideal in a central simple algebra A with an involution σ. Prove that the following conditions are equivalent:

   (a) $I \cap I^{\perp} = \{0\}$.

   (b) $I = eA$ for some symmetric idempotent $e \in A$.

   Moreover, if these conditions hold, the symmetric idempotent e such that $I = eA$ is unique and satisfies: $(1-e)A = I^{\perp}$.

10. (Bayer-Fluckiger - Shapiro - Tignol [4]) Let (A, σ) be a central simple F-algebra with orthogonal involution. Prove that the following conditions are equivalent:

    (a) σ is hyperbolic.

    (b) There exists an idempotent $e \in A$ such that $\sigma(e) = 1 - e$.

    (c) A contains a split subalgebra A_0 of degree 2 (i.e. $A_0 \simeq M_2(F)$), stable under σ and such that the restriction of σ to A_0 is the adjoint involution with respect to a hyperbolic 2-dimensional quadratic form.

    Prove corresponding statements for symplectic involutions and for involutions of the second kind.

11. Let (A, σ), (B, τ) and (C, ν) be central simple F-algebras with involutions of the first kind. If $(A, \sigma) \otimes_F (B, \tau) \simeq (A, \sigma) \otimes_F (C, \nu)$ (as algebras with involution), does it follow that $(B, \tau) \simeq (C, \nu)$? [Hint: Use the preceding exercise].

Chapter 2.

Clifford theory

In this chapter, we develop two invariants of orthogonal involutions on central simple algebras: the discriminant and the (even) Clifford algebra. Our method of investigation is mostly based on scalar extension: after setting the definitions, the main properties are proved by extending scalars to a splitting field of the central simple algebra. The given orthogonal involution is then the adjoint involution with respect to some nonsingular bilinear symmetric form, and one may then use known properties of the Clifford algebra of quadratic forms. Occasionally, we will need to use a splitting field which is not too "disruptive", in the sense that the group of square classes of the base field injects into the group of square classes of the splitting field:

Fact: *For every central simple algebra A over a field F, there exists a splitting field K in which F is algebraically closed. In particular, the natural homomorphism $F^\times/F^{\times 2} \to K^\times/K^{\times 2}$ is injective.*

One may for instance take for K the function field of the Severi-Brauer variety of A.

§1. The discriminant

The notion of discriminant of an orthogonal involution goes back to Jacobson's work on Clifford algebras [8]. The definition we present here is more direct; it is due to Knus-Parimala-Sridharan [12].

Let (A, σ) be a central simple algebra with involution of the first kind over a field F (of characteristic different from 2). It will be convenient to use the following definition:

(1.1) Definition.

$$\mathrm{Alt}(\sigma) = \begin{cases} (A,\sigma)_+ & \text{if } \sigma \text{ is symplectic.} \\ (A,\sigma)_- & \text{if } \sigma \text{ is orthogonal.} \end{cases}$$

The elements in $\mathrm{Alt}(\sigma)$ are called *alternating*[1] (even though they are actually symmetric

[1] In a characteristic-free approach, it would be more convenient to define $\mathrm{Alt}(\sigma) = \{x - \varepsilon\sigma(x) \mid x \in A\}$ where $\varepsilon = \pm 1$ is the type of σ, following [11].

if σ is symplectic). We also let $\mathrm{Alt}(\sigma)^\times$ denote the set of invertible elements in $\mathrm{Alt}(\sigma)$:

$$\mathrm{Alt}(\sigma)^\times = \mathrm{Alt}(\sigma) \cap A^\times.$$

A direct application of Proposition 2.2 yields:

$$\mathrm{Alt}(\mathrm{Int}(u) \circ \sigma) = u \cdot \mathrm{Alt}(\sigma) = \mathrm{Alt}(\sigma) \cdot u^{-1} \qquad \text{for all } u \in A^\times \text{ such that } \sigma(u) = \pm u.$$

This formula displays the advantage of the definition above: in contrast to Proposition 2.2, it is not necessary here to consider separately the cases $\sigma(u) = +u$ and $\sigma(u) = -u$.

The definition of the discriminant of an (orthogonal) involution is based on the following crucial result:

(1.2) Proposition. *If* $\deg A$ *is even, then* $\mathrm{Alt}(\sigma)^\times \neq \varnothing$. *Moreover, for any* $a, b \in \mathrm{Alt}(\sigma)^\times$,

$$\mathrm{Nrd}_A(a) \equiv \mathrm{Nrd}_A(b) \mod F^{\times 2}.$$

In particular, if σ *is symplectic, then* $\mathrm{Nrd}_A(a) \in F^{\times 2}$ *for all* $a \in \mathrm{Alt}(\sigma)^\times$.

Proof: The invertible elements form a Zariski-open subset in $\mathrm{Alt}(\sigma)$ (defined by the relation $\mathrm{Nrd}_A(X) \neq 0$). If $\deg A$ is even, then scalar extension to a splitting field shows that this subset is non-empty, hence $\mathrm{Alt}(\sigma)^\times$ is a dense open subset in $\mathrm{Alt}(\sigma)$.

Let K be a splitting field of A in which F is algebraically closed. Fix an isomorphism:

$$f : A_K \xrightarrow{\sim} M_n(K)$$

and let $\sigma' = f \circ (\sigma \otimes \mathrm{Id}_K) \circ f^{-1}$ be the transport to $M_n(K)$ of the involution σ. We have

$$\sigma' = \mathrm{Int}(u) \circ t$$

(where t is the transposition involution) for some $u \in \mathrm{GL}_n(K)$ such that $u^t = \pm u$. If $a, b \in \mathrm{Alt}(\sigma)$, then $f(a \otimes 1), f(b \otimes 1) \in \mathrm{Alt}(\sigma') = u \cdot \mathrm{Alt}(t)$. Let

$$f(a \otimes 1) = ua' \qquad f(b \otimes 1) = ub'$$

for some $a', b' \in \mathrm{Alt}(t)^t$. Since the determinant of every skew-symmetric matrix of even order is a square (namely, the square of the pfaffian: see [3, Theorem 3.27]), we have $\det a', \det b' \in K^{\times 2}$ and therefore

$$\det(f(a \otimes 1)) \equiv \det u \equiv \det(f(b \otimes 1)) \mod K^{\times 2}.$$

Since $\mathrm{Nrd}_A(a) = \det(f(a \otimes 1))$ (and similarly for b), it follows that

$$\mathrm{Nrd}_A(ab^{-1}) \in F^\times \cap K^{\times 2},$$

hence $\mathrm{Nrd}_A(ab^{-1}) \in F^{\times 2}$ since F is algebraically closed in K. This completes the proof, since we may take $b = 1$ when σ is symplectic. ∎

The Proposition above makes it possible to set the following definition:

(1.3) Definition. (Knus-Parimala-Sridharan) Let σ be an involution of the first kind on a central simple algebra A of *even* degree over a field F. The *discriminant* of σ is the square class of the reduced norm of any invertible element:

$$\operatorname{disc}\sigma = \operatorname{Nrd}_A(a) \cdot F^{\times 2} \in F^\times/F^{\times 2} \quad \text{for any } a \in \operatorname{Alt}(\sigma)^\times.$$

If σ is symplectic, then necessarily $\operatorname{disc}\sigma = 1$ since we may take $a = 1$ in the definition above. Therefore, the discriminant is a meaningful invariant only for orthogonal involutions. It is however useful to define it for arbitrary involutions, so as to avoid exceptions in the following list of properties:

(1.4) Proposition. *Let (A,σ) be a central simple algebra of even degree with involution of the first kind over a field F.*

1. *For all $u \in A^\times$ such that $\sigma(u) = \pm u$,*

$$\operatorname{disc}(\operatorname{Int}(u) \circ \sigma) = \operatorname{Nrd}_A(u) \cdot \operatorname{disc}\sigma.$$

2. *If A is split: $A = \operatorname{End}_F(V)$ and $\sigma = \sigma_b$ is the adjoint involution with respect to some nonsingular bilinear form b on V, then*

$$\operatorname{disc}\sigma_b = \operatorname{disc} b.$$

3. *If (B,τ) is another central simple F-algebra with involution of the first kind, then*

$$\operatorname{disc}(\sigma \otimes \tau) = \begin{cases} \operatorname{disc}\sigma & \text{if } \deg B \text{ is odd.} \\ 1 & \text{if } \deg B \text{ is even.} \end{cases}$$

Proof: (1) follows from the fact that $\operatorname{Alt}(\operatorname{Int}(u) \circ \sigma) = u \cdot \operatorname{Alt}(\sigma)$.

(2): Let $n = \dim V$ and identify A to $M_n(F)$ by means of a basis e of V. Let also $b_e \in \operatorname{GL}_n(F)$ denote the Gram matrix of the bilinear form b with respect to the chosen basis e. The involution σ_e is then given by:

$$\sigma_b = \operatorname{Int}(b_e^{-1}) \circ t,$$

where t is the transposition involution. It is easily seen that $\operatorname{disc} t = 1$, hence the first part of the Proposition yields:

$$\operatorname{disc}\sigma_b = \det(b_e^{-1}) \cdot F^{\times 2} = \operatorname{disc}(b).$$

(3): If $a \in \operatorname{Alt}(\sigma)^\times$, then $a \otimes 1 \in \operatorname{Alt}(\sigma \otimes \tau)^\times$ if τ is orthogonal. Since

$$\operatorname{Nrd}_{A\otimes B}(a \otimes 1) = \operatorname{Nrd}_A(a)^{\deg B} \tag{2.1}$$

we get the required relation in the case where τ is orthogonal. If τ is symplectic (which implies that $\deg B$ is even, by Proposition 2.1 of Chapter 1), let $a \in A^\times$ be such that $\sigma(a) = \varepsilon a$, where ε is the type of σ. (The existence of such an element can be proved by the same argument as in Proposition 1.2). Then $a \otimes 1 \in \operatorname{Alt}(\sigma \otimes \tau)$, hence $\operatorname{disc}(\sigma \otimes \tau) = \operatorname{Nrd}_{A\otimes B}(a \otimes 1) \cdot F^{\times 2}$ and equation (2.1) yields $\operatorname{disc}(\sigma \otimes \tau) = 1$. ∎

§2. The Clifford algebra

Since the Clifford algebra of a quadratic form is not invariant when the quadratic form is multiplied by a scalar, it is not possible to define a corresponding notion for involutions. However, the *even* Clifford algebra is indeed an invariant for quadratic forms up to similarity, and our aim in this section is to generalize its construction to algebras with orthogonal involutions. The first definition of the (generalized, even) Clifford algebra of an algebra with orthogonal involution was given by Jacobson [8], using Galois descent. Our approach is based on Tits' "rational" definition [22], with some simplifications due to the fact that we exclude fields of characteristic different from 2.

Since our main tool will be scalar extension to a splitting field, we first discuss the case of a quadratic space.

2.1. The split case

Let (V, q) be a nonsingular quadratic space over a field F of characteristic different from 2. We denote by b_q the symmetric bilinear form

$$b_q(x, y) = \tfrac{1}{2}(q(x+y) - q(x) - q(y)),$$

which we call the *polar* of q, by $\hat{b}_q : V \xrightarrow{\sim} V^* = \mathrm{Hom}_F(V, F)$ the *adjoint* of b_q, defined by:

$$\hat{b}_q(x)(y) = b_q(x, y)$$

and by σ_q the *adjoint involution* on $\mathrm{End}_F(V)$ with respect to b_q (see Chapter 1). Using $\hat{b}_q$, we may identify $\mathrm{End}_F(V) = V \otimes_F V^*$ with $V \otimes_F V$:

$$\mathrm{Id}_V \otimes \hat{b}_q : \mathrm{End}_F(V) = V \otimes V^* \xrightarrow{\sim} V \otimes V.$$

Under this identification, $v \otimes w \in V \otimes V$ is identified to the linear map:

$$v \otimes w : x \mapsto v\, b_q(w, x).$$

Moreover, it is straightforward to check that the involution σ_q is given by the twist:

$$\sigma_q(v \otimes w) = w \otimes v,$$

the trace $\mathrm{Tr} : \mathrm{End}_F(V) \to F$ by the polar of q:

$$\mathrm{Tr}(v \otimes w) = b_q(v, w)$$

and the multiplication by:

$$(v \otimes w) \circ (v' \otimes w') = v\, b_q(w, v') \otimes w'.$$

Note that every orthogonal involution on a split central simple algebra is the adjoint involution with respect to some nonsingular quadratic form (see the introduction of Chapter 1). Henceforth, we will often consider split central simple algebras with orthogonal involutions

$$(A, \sigma) = (\mathrm{End}_F(V), \sigma_q)$$

as $A = V \otimes V$ with the involution, multiplication and (reduced) trace defined above. We call this identification $A = V \otimes V$ the *standard identification* (even if it is not completely canonical, since the quadratic form q, hence also b_q and $\hat{b}_q$, is determined by the involution σ_q only up to a scalar factor).

Let $C(V,q) = C_0(V,q) \oplus C_1(V,q)$ denote the Clifford algebra of (V,q). We denote by τ the *canonical involution* of $C(V,q)$, which is the identity on V, as well as its restriction to $C_0(V,q)$. If not explicitly mentioned, we shall always view $C(V,q)$ and $C_0(V,q)$ as algebras with involution, taking τ as the natural involution. Our first result is a description of the even Clifford algebra $C_0(V,q)$ "by generators and relations" (compare [22, p. 32]):

(2.1) Lemma. *In the tensor algebra $T(V \otimes V)$, consider the following 2-sided ideals:*

- *$I_1(q)$ is the ideal generated by all the elements of the form*

$$v \otimes v - q(v), \quad \text{for } v \in V.$$

- *$I_2(q)$ is the ideal generated by all the elements of the form*

$$u \otimes v \otimes v \otimes w - q(v)u \otimes w, \quad \text{for } u, v, w \in V.$$

Then

$$C_0(V,q) = \frac{T(V \otimes V)}{I_1(q) + I_2(q)}$$

and the canonical involution τ on $C_0(V,q)$ is induced by the twist: $v \otimes w \mapsto w \otimes v$.

Proof: There is a canonical epimorphism

$$\frac{T(V \otimes V)}{I_1(q) + I_2(q)} \to C_0(V,q).$$

Calculations with an orthogonal basis of V easily show

$$\dim_F \left(\frac{T(V \otimes V)}{I_1(q) + I_2(q)} \right) \leq \dim_F C_0(V,q).$$

Therefore, the canonical epimorphism is injective. ∎

We also recall the following structure theorem for even Clifford algebras:

(2.2) Theorem. *Let (V,q) be a nonsingular quadratic space.*

1. *If $\dim V$ is odd: $\dim V = 2m+1$, then $C_0(V,q)$ is central simple F-algebra of degree 2^m. The canonical involution τ on $C_0(V,q)$ is of the first kind; it is orthogonal if $m \equiv 0$ or $3 \bmod 4$ and symplectic if $m \equiv 1$ or $2 \bmod 4$.*
2. *If $\dim V$ is even: $\dim V = 2m$, the center of $C_0(V,q)$ is an étale quadratic F-algebra Δ isomorphic to $F[X]/(X^2 - \delta(q))$ where $\delta(q) \in F^\times$ is such that*

$$\operatorname{disc} q = (-1)^m \delta(q) \cdot F^{\times 2}.$$

Moreover,

(a) If Δ is a field (i.e. if $\operatorname{disc} q \neq 1$), then $C_0(V,q)$ is a central simple Δ-algebra of degree 2^{m-1}.

(b) If $\Delta \simeq F \times F$ (i.e. if $\operatorname{disc} q = 1$), then $C_0(V,q)$ is a direct product of two central simple F-algebras of degree 2^{m-1}.

The canonical involution τ on $C_0(V,q)$ is of the first kind if m is even and of the second kind if m is odd; it is of orthogonal type if $m \equiv 0 \bmod 4$ and of symplectic type if $m \equiv 2 \bmod 4$. (In the case where $\operatorname{disc} q = 1$, this means that τ is orthogonal or symplectic on each factor of $C_0(V,q)$).

The proof can be found for instance in [18, Theorem 9.2.10].

2.2. Definition of the Clifford algebra

Let (A,σ) be a central simple algebra with orthogonal involution over a field F of characteristic different from 2. Our goal is to define an algebra $C(A,\sigma)$ in such a way that in the split case $C(\operatorname{End}_F(V),\sigma_q)$ reduces to the even Clifford algebra $C_0(V,q)$.

Let $\underline{A}$ denote A viewed as an F-vector space. The canonical map $A \to \underline{A}$ is denoted by $a \mapsto \underline{a}$. We recall the "sandwich" isomorphism:

$$\operatorname{Sand} : \underline{A} \otimes \underline{A} \xrightarrow{\sim} \operatorname{End}_F(\underline{A})$$

such that $\operatorname{Sand}(\underline{a} \otimes \underline{b})(\underline{x}) = \underline{axb}$ for $a,b,x \in A$ (see Lemma 3.3 in Chapter 1). We use this isomorphism to define a map

$$\sigma_2 : \underline{A} \otimes \underline{A} \to \underline{A} \otimes \underline{A}$$

as follows: for fixed $u \in \underline{A} \otimes \underline{A}$ the map $\underline{A} \to \underline{A}$ defined by: $\underline{x} \mapsto \operatorname{Sand}(u)(\underline{\sigma(x)})$ is linear and therefore of the form $\operatorname{Sand}(\sigma_2(u))$ for a certain $\sigma_2(u) \in \underline{A}$. In other words, the map σ_2 is defined by the condition:

$$\operatorname{Sand}(\sigma_2(u))(\underline{a}) = \operatorname{Sand}(u)(\underline{\sigma(a)}) \qquad \text{for all } u \in \underline{A} \otimes \underline{A} \text{ and } a \in A.$$

(2.3) Lemma. *If A is split: $(A,\sigma) = (\mathrm{End}_F V, \sigma_q)$, then under the standard identification $A = V \otimes V$, we have*

$$\sigma_2(x_1 \otimes x_2 \otimes x_3 \otimes x_4) = x_1 \otimes x_3 \otimes x_2 \otimes x_4 \qquad \text{for } x_1, x_2, x_3, x_4 \in V.$$

Proof: It suffices to see that, for $x_1, x_2, x_3, x_4, v, w \in V$,

$$\mathrm{Sand}(x_1 \otimes x_3 \otimes x_2 \otimes x_4)(v \otimes w) = \mathrm{Sand}(x_1 \otimes x_2 \otimes x_3 \otimes x_4)(w \otimes v).$$

This follows from a straightforward computation:

$$\begin{aligned} \mathrm{Sand}(x_1 \otimes x_3 \otimes x_2 \otimes x_4)(v \otimes w) &= x_1 \otimes x_3 \circ v \otimes w \circ x_2 \otimes x_4 \\ &= x_1 \otimes x_4 . b(x_3, v) b(w, x_2) \\ \mathrm{Sand}(x_1 \otimes x_2 \otimes x_3 \otimes x_4)(w \otimes v) &= x_1 \otimes x_2 \circ w \otimes v \circ x_3 \otimes x_4 \\ &= x_1 \otimes x_4 . b(x_2, w) b(v, x_3). \end{aligned}$$

■

We denote by $\mu : \underline{A} \otimes \underline{A} \to \underline{A}$ the multiplication map:

$$\mu(\underline{a} \otimes \underline{b}) = \underline{ab},$$

so that in the split case $(A,\sigma) = (\mathrm{End}_F V, \sigma_q)$ we have under the standard identification $A = V \otimes V$:

$$\mu(x_1 \otimes x_2 \otimes x_3 \otimes x_4) = x_1 \otimes x_4 . b_q(x_2, x_3).$$

(2.4) Definition. For any central simple F-algebra with orthogonal involution (A,σ), the *Clifford algebra* $C(A,\sigma)$ is defined as a quotient of the tensor algebra $T(\underline{A})$:

$$C(A,\sigma) = \frac{T(\underline{A})}{J_1(\sigma) + J_2(\sigma)}$$

where

- $J_1(\sigma)$ is the ideal generated by the elements of the form $\underline{s} - \mathrm{Trd}_A(s)$, for all $s \in A$ such that $\sigma(s) = s$.
- $J_2(\sigma)$ is the ideal generated by the elements of the form $u - \mu(u)$, for all $u \in \underline{A} \otimes \underline{A}$ such that $\sigma_2(u) = u$.

Note that we have in particular $\underline{1} \equiv (\deg A).1 \bmod J_1(\sigma)$; therefore

$$\underline{1} \neq 1 \qquad \text{in } C(A,\sigma).$$

Let $\underline{\sigma} : T(\underline{A}) \to T(\underline{A})$ denote the involution on the (infinite-dimensional) F-algebra $T(\underline{A})$ induced by the involution σ on A; namely,

$$\underline{\sigma}(\underline{a_1} \otimes \cdots \otimes \underline{a_r}) = \underline{\sigma(a_r)} \otimes \cdots \otimes \underline{\sigma(a_1)}.$$

Direct computations show that the ideals $J_1(\sigma)$ and $J_2(\sigma)$ are preserved under the involution $\underline{\sigma}$. Therefore, this involution induces an involution on the quotient algebra $C(A,\sigma)$, which we also denote by $\underline{\sigma}$.

(2.5) Proposition. *If $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$ is a split algebra, then the standard identification $\mathrm{Id}_V \otimes \hat{b}_q : V \otimes_F V \to V \otimes_F V^* = \mathrm{End}_F(V)$ induces a "standard identification" of Clifford algebras*

$$\eta_q : (C_0(V,q),\tau) \xrightarrow{\sim} (C(\mathrm{End}_F(V),\sigma_q),\underline{\sigma}).$$

Proof: The map induced by $\mathrm{Id}_V \otimes \hat{b}_q$ on tensor algebras maps the ideals $I_1(q)$ and $I_2(q)$ of Lemma 2.1 into $J_1(\sigma_q)$ and $J_2(\sigma_q)$ respectively. Calculations with an orthogonal basis of V show that $J_1(\sigma_q)$ and $J_2(\sigma_q)$ are actually the images of $I_1(q)$ and $I_2(q)$, and the Proposition follows. ∎

Although the degree of A is arbitrary in the discussion above, the case where $\deg A$ is odd does not yield anything beyond the even Clifford algebras of quadratic spaces, since central simple algebras of odd degree with involutions of the first kind are split (see [6, §9, Corollary 7]). Therefore, we shall henceforth assume that A is a central simple algebra of even degree $n = 2m$.

Using scalar extension to a splitting field, we obtain the following structure theorem for Clifford algebras:

(2.6) Theorem. *Let A be a central simple F-algebra of even degree $n = 2m$ with an orthogonal involution σ and let $C(A,\sigma)$ be its Clifford algebra, with canonical involution $\underline{\sigma}$.*

1. *The center of $C(A,\sigma)$ is an étale quadratic F-algebra Δ which is isomorphic to $F[X]/(X^2 - \delta(\sigma))$, where $\delta(\sigma) \in F^\times$ is such that*
$$\mathrm{disc}\,\sigma = (-1)^m \delta(\sigma) \cdot F^{\times 2}.$$
2. *If Δ is a field (i.e. if $\mathrm{disc}\,\sigma \neq 1$), then $C(A,\sigma)$ is a central simple Δ-algebra of degree 2^{m-1}; if $\Delta \simeq F \times F$ (i.e. $\mathrm{disc}\,\sigma = 1$), then $C(A,\sigma)$ is a direct product of two central simple F-algebras of degree 2^{m-1}. So, in both cases $C(A,\sigma)$ is an Azumaya algebra over Δ.*
3. *The involution $\underline{\sigma}$ on $C(A,\sigma)$ is of the first kind if m is even and is of the second kind if m is odd; it is of orthogonal type if $m \equiv 0 \bmod 4$ and of symplectic type if $m \equiv 2 \bmod 4$. (If $\Delta \simeq F \times F$, this means that the involution is of orthogonal or symplectic type on both factors of $C(A,\sigma)$).*

Proof: Let K be a splitting field of A in which F is algebraically closed. We have $(A \otimes_F K, \sigma \otimes \mathrm{Id}_K) \simeq (\mathrm{End}_K(V),\sigma_q)$ for some quadratic space (V,q) over K, of dimension $n = \deg A$ and discriminant $\mathrm{disc}\,q = \mathrm{disc}(\sigma \otimes \mathrm{Id}_K)$, by Proposition 1.4. If $\delta(\sigma)$ is a representative in $F^\times$ of $\mathrm{disc}\,\sigma$, we then have $\mathrm{disc}\,q = \delta(\sigma) \cdot K^{\times 2} \in K^\times/K^{\times 2}$. It is clear from the definition that the construction of the Clifford algebra commutes with scalar extension:

$$C(A,\sigma) \otimes_F K = C(A \otimes_F K, \sigma \otimes \mathrm{Id}_K) \simeq C_0(V,q).$$

In particular, it follows that the center Δ of $C(A,\sigma)$ is a quadratic étale extension which becomes isomorphic over K to $K[X]/(X^2 - \delta(\sigma))$. Since F is algebraically closed in K, it follows that $\Delta \simeq F[X]/(X^2 - \delta(\sigma))$. The other statements also follow from the structure theorem for even Clifford algebras of quadratic spaces: see Theorem 2.2. ∎

2.3. Lie algebra structures

We continue with the same notation as in the preceding section; in particular, (A,σ) is a central simple F-algebra with orthogonal involution and $C(A,\sigma)$ is its Clifford algebra.

Since $C(A,\sigma)$ is defined as a quotient of the tensor algebra $T(\underline{A})$, the canonical map $A \to \underline{A} \to T(\underline{A})$ yields a canonical map

$$c\colon A \to C(A,\sigma)$$

which is F-linear but not injective (since $c(s) = \mathrm{Trd}_A(s)$ for all $s \in (A,\sigma)_+$) and does not map $1 \in A$ to $1 \in C(A,\sigma)$:

$$c(1) = \deg A.$$

We aim to show that this map has nice properties anyway, with respect to Lie algebra structures.

Let $\mathfrak{L}(A)$ be A viewed as a Lie-algebra with the bracket operation $[x,y] = xy - yx$. The vector space $(A,\sigma)_- = \mathrm{Alt}(\sigma)$ of skew-symmetric elements is stable under the bracket operation and may therefore be viewed as a Lie subalgebra of $\mathfrak{L}(A)$.

In the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$, we have

$$\mathrm{Alt}(\sigma) = \{f \in \mathrm{End}_F(V) \mid b_q(fx,y) + b_q(x,fy) = 0 \quad \text{for all } x,y \in V\}.$$

This is the *Lie algebra* of the orthogonal group $O(V,q)$. We denote it simply by $\mathfrak{L}(V,q)$. It turns out that this Lie algebra can be identified to a (Lie-)subalgebra of the Clifford algebra $C(V,q)$, as we now show. (Compare [9, pp. 231–232]).

(2.7) Lemma. *For $x,y,z \in V$ we have in $C(V,q)$:*

$$[[x,y],z] = 4(x\,b_q(y,z) - y\,b_q(x,z)) \in V.$$

Proof: This is a direct computation based on the fact that for $v,w \in V$,

$$b_q(v,w) = \tfrac{1}{2}(v\cdot w + w\cdot v) \quad \text{in } C(V,q).$$

For $x,y,z \in V$, we compute:

$$\begin{aligned}[[x,y],z] &= (x\cdot y\cdot z + x\cdot z\cdot y + y\cdot z\cdot x + z\cdot y\cdot x)\\ &\quad -(y\cdot x\cdot z + y\cdot z\cdot x + x\cdot z\cdot y + z\cdot x\cdot y)\\ &= 4(x\,b_q(y,z) - y\,b_q(x,z)) \in V.\end{aligned}$$

■

Let $[V,V] \subset C(V,q)$ be the subspace spanned by the brackets $[x,y] = x \cdot y - y \cdot x$ for $x, y \in V$. In view of the Lemma, we may define a linear map

$$\rho : [V,V] \to \mathrm{End}_F(V)$$

by: $\rho(\xi)(z) = \frac{1}{4}[\xi, z]$ for $\xi \in [V,V]$ and $z \in V$. The Lemma above yields:

$$\rho([x,y]) = x \otimes \hat{b}_q(y) - y \otimes \hat{b}_q(x) \qquad \text{for } x, y \in V. \tag{2.2}$$

(2.8) Lemma. *a) The following diagram is commutative:*

$$\begin{array}{ccc} [V,V] & \hookrightarrow & C_0(V,q) \\ \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \eta_q} \\ \mathrm{End}(V) & \xrightarrow{c} & C(\mathrm{End}(V), \sigma_q) \end{array}$$

where c is the canonical map and η_q is the canonical identification of Proposition 2.5.

b) The subspace $[V,V]$ is a Lie subalgebra of $\mathfrak{L}(C_0(V,q))$, and ρ induces an isomorphism of Lie algebras:

$$\rho : [V,V] \xrightarrow{\sim} \mathfrak{L}(V,q).$$

c) The restriction of the canonical map c to $\mathfrak{L}(V,q)$ is an injective Lie-algebra homomorphism:

$$c : \mathfrak{L}(V,q) \hookrightarrow \mathfrak{L}(C(\mathrm{End}(V), \sigma_q)).$$

Proof: (a) follows from equation (2.2) and from the definitions of c and η_q.

(b): Jacobi's identity yields, for $x, y, u, v \in V$:

$$[[u,v],[x,y]] = [[[x,y],v],u] - [[[x,y],u],v].$$

Since Lemma (2.7) shows that $[[x,y],z] \in V$ for all $x, y, z \in V$, it follows that $[[u,v],[x,y]] \in [V,V]$. Therefore, $[V,V]$ is a Lie subalgebra of $\mathfrak{L}(C(V,q))$ (or $\mathfrak{L}(C_0(V,q))$). Jacobi's identity also yields:

$$\rho([\xi,\eta]) = [\rho(\xi), \rho(\eta)] \qquad \text{for } \xi, \eta \in [V,V],$$

hence ρ is a Lie-algebra homomorphism. From equation (2.2), we get for $x, y, u, v \in V$:

$$\begin{aligned} b_q(\rho([x,y])(u), v) &= (b_q(x,v)b_q(y,u) - b_q(y,v)b_q(x,u)) \\ &= -b_q(u, \rho([x,y])(v)), \end{aligned}$$

hence $\rho([x,y]) \in \mathfrak{L}(V,q)$. Therefore, we may consider ρ as a map:

$$\rho : [V,V] \to \mathfrak{L}(V,q).$$

It only remains to prove that this map is bijective. Let $n = \dim V$. Using an orthogonal basis of V, it is easily verified that $\dim[V,V] = n(n-1)/2 = \dim \mathfrak{L}(V,q)$. On the other hand, since η_q is an isomorphism, *(a)* shows that ρ is injective; it is therefore also surjective.

(c): Using η_q to identify $[V,V]$ to a Lie subalgebra of $C(\mathrm{End}(V),\sigma_q)$, we derive from *(a)* and *(b)* that the restriction of c to $\mathfrak{L}(V,q)$ is the inverse of ρ. Therefore, c is injective on $\mathfrak{L}(V,q)$ and is a Lie-algebra homomorphism. ∎

(2.9) Proposition. *Let (A,σ) be a central simple algebra with orthogonal involution and let*

$$c\colon A \to C(A,\sigma)$$

denote the canonical map. Let also $\underline{\sigma}$ be the canonical involution on $C(A,\sigma)$.

a) The restriction of c to $\mathrm{Alt}(\sigma)$ is an injective Lie-algebra homomorphism

$$c\colon \mathrm{Alt}(\sigma) \hookrightarrow (C(A,\sigma),\underline{\sigma})_-.$$

b) $c(A) = F\cdot 1 \oplus c(\mathrm{Alt}(\sigma))$.

c) $c(\mathrm{Alt}(\sigma))$ *generates $C(A,\sigma)$ as an (associative) F-algebra.*

Proof: (a): By definition of $\underline{\sigma}$, we have $\underline{\sigma}(c(a)) = c(\sigma(a))$ for $a \in A$, so $c(\mathrm{Alt}(\sigma)) \subset (C(A,\sigma),\underline{\sigma})_-$. The rest follows by descent from part *(c)* of the Lemma.

To prove *(b)* we first observe that the sum of $F\cdot 1$ and $c(\mathrm{Alt}(\sigma))$ is direct, since the image of $\mathrm{Alt}(\sigma)$ consists of skew-symmetric elements. Since $A = (A,\sigma)_+ \oplus \mathrm{Alt}(\sigma)$ and $c(s) = \mathrm{Trd}_A(s)\cdot 1$ for all $s \in (A,\sigma)_+$, we get *(b)*. Finally, *(c)* follows from *(b)* since the definition of $C(A,\sigma)$ shows that this algebra is generated by $c(A)$. ∎

In relation with *(c)* of the Proposition above, note that $\mathrm{Alt}(\sigma)$ generates A as an (associative) F-algebra if $\deg A > 2$. This is easily seen by descent: extending the scalars, we may assume σ is the transposition involution on $A = M_n(F)$. Denoting by e_{ij} the usual matrix units, we have

$$e_{ii} = (e_{ij} - e_{ji})^2(e_{ik} - e_{ki})^2 \quad \text{if } i,j,k \text{ are pairwise distinct}$$

and

$$e_{ij} = e_{ii}(e_{ij} - e_{ji}).$$

(Compare [9, p.304]; an alternative proof without descent can be found in [7, Theorem 2.2, p. 28]).

(2.10) Example. Let $A = Q_1 \otimes Q_2$, where Q_1 and Q_2 are quaternion algebras over F, and let $\sigma = \gamma_1 \otimes \gamma_2$, the tensor product of the canonical involutions on Q_1 and Q_2. By Proposition 1.4, we have $\mathrm{disc}\,\sigma = 1$, hence Theorem 2.6 shows that $C(A,\sigma) = C_1 \times C_2$ for some quaternion algebras C_1, C_2. Moreover, the canonical involution $\underline{\sigma}$ is symplectic, hence it is the quaternion conjugation on C_1 and C_2. We claim that C_1 and C_2 are isomorphic to Q_1 and Q_2.

Let $Q_1' = (Q_1, \gamma_1)_-$ denote the Lie algebra of pure quaternions in Q_1, and define similarly Q_2', C_1' and C_2'. A direct computation yields

$$\mathrm{Alt}(\sigma) = (Q_1' \otimes 1) \oplus (1 \otimes Q_2') \simeq Q_1' \times Q_2'.$$

On the other hand, by Proposition 2.9, there is an injective Lie-algebra homomorphism induced by the canonical map c:

$$c\colon Q_1' \times Q_2' \hookrightarrow C_1' \times C_2',$$

which is readily seen to be an isomorphism, by dimension count. Since Lie algebras of pure quaternions are easily seen to be simple and since the decomposition of a semi-simple Lie algebra into a direct product of simple Lie algebras is unique, it follows that Q_1' and Q_2' are isomorphic to C_1' and C_2'. Since the Lie algebra of pure quaternions uniquely determines the quaternion algebra (see exercise ???), it follows that Q_1 and Q_2 are isomorphic to C_1 and C_2 (as associative algebras). In conclusion, we have shown:

$$C(Q_1 \otimes Q_2, \gamma_1 \otimes \gamma_2) \simeq Q_1 \times Q_2.$$

§3. The Clifford bimodule

Although the odd part $C_1(V,q)$ of the Clifford algebra of a quadratic space (V,q) is not invariant under similarities, it turns out that the tensor product $V \otimes C_1(V,q)$ is invariant, and therefore an analogue can be defined for a central simple algebra with orthogonal involution (A,σ). This will be the aim of this section. This construction will be used at the end of this section to obtain fundamental relations between the Clifford algebra $C(A,\sigma)$ and the algebra A (see Theorem 3.11); it will also be an indispensable tool in the definition of spin groups in the next Chapter.

We first review the basic properties of the vector space $V \otimes C_1(V,q)$ that we want to generalize.

3.1. The split case

Let (V,q) be a quadratic space over a field F (of characteristic different from 2). Let $C_1(V,q)$ be the odd part of the Clifford algebra $C(V,q)$. Multiplication in $C(V,q)$ endows $C_1(V,q)$ with a $C_0(V,q)$-bimodule structure. Since V is in a natural way a left $\mathrm{End}(V)$-module, the tensor product $V \otimes C_1(V,q)$ is at the same time a left $\mathrm{End}(V)$-module and a $C_0(V,q)$-bimodule: for $f \in \mathrm{End}(V)$, $v \in V$, $c_0 \in C_0(V,q)$ and $c_1 \in C_1(V,q)$ we set

$$f \cdot (v \otimes c_1) = f(v) \otimes c_1 \qquad c_0 * (v \otimes c_1) = v \otimes c_0 c_1 \qquad (v \otimes c_1) \cdot c_0 = v \otimes c_1 c_0.$$

The various actions clearly commute.

Henceforth, we assume that the dimension of V is even:

$$\dim V = n = 2m.$$

This is the main case of interest for generalization to central simple algebras with involution, since central simple algebras of odd degree with involution of the first kind are split: see [6, §9, Corollary 7]. In this case the center of $C_0(V,q)$ is an étale quadratic extension of F:

$$\Delta = F(\sqrt{(-1)^m \operatorname{disc} q}).$$

(This is a slight abuse of notation, since $\operatorname{disc} q \in F^\times/F^{\times 2}$). Let ι denote the non-trivial automorphism of Δ/F. In the Clifford algebra $C(V,q)$ we have

$$z \cdot v = v \cdot \iota(z) \qquad \text{for } v \in V \text{ and } z \in \Delta,$$

hence

$$z * (v \otimes c_1) = (v \otimes c_1) \cdot \iota(z) \qquad \text{for } v \in V,\ c_1 \in C_1(V,q) \text{ and } z \in \Delta. \tag{2.3}$$

We summarize the basic properties of $V \otimes C_1(V,q)$ in the following Proposition:

(3.1) Proposition. *Let* $\dim V = n = 2m$.

1. *The vector space* $V \otimes C_1(V,q)$ *carries natural structures of left* $\operatorname{End}(V)$*-module and* $C_0(V,q)$*-bimodule. Moreover, the various actions commute, so that* $V \otimes C_1(V,q)$ *is a left* $\operatorname{End}(V) \otimes_F C_0(V,q) \otimes_F C_0(V,q)^{\mathrm{op}}$*- module. In view of equation (2.3), it is also a left* $\operatorname{End}(V) \otimes_F C_0(V,q) \otimes_\Delta {}^{\iota}C_0(V,q)^{\mathrm{op}}$*-module.*
2. *The standard identification* $\operatorname{End}(V) = V \otimes V$ *induced by the quadratic form* q *and the embedding* $V \hookrightarrow C_1(V,q)$ *define a canonical map* $d : \operatorname{End}(V) \to V \otimes C_1(V,q)$ *which is an injective homomorphism of left* $\operatorname{End}(V)$*-modules.*
3. $\dim_F(V \otimes C_1(V,q)) = n\,2^{n-1}$.

The proof follows from straightforward verifications.

Let us consider $V \otimes C_1(V,q)$ as a right Δ-module through the right action of $C_0(V,q)$:

$$(v \otimes c_1) \cdot z = v \otimes c_1 z \qquad \text{for } v \in V,\ c_1 \in C_1(V,q) \text{ and } z \in \Delta.$$

We want to define on $V \otimes C_1(V,q)$ a canonical hermitian form with values in Δ, in order to obtain an involution on $\operatorname{End}_\Delta(V \otimes C_1(V,q))$. The definition involves the involution τ on $C(V,q)$ which is the identity on V. Recall the restriction of τ to Δ (see Theorem 2.2):

$$\tau|_\Delta = \begin{cases} \mathrm{Id}_\Delta & \text{if } m \text{ is even} \\ \iota & \text{if } m \text{ is odd.} \end{cases}$$

(3.2) Lemma. *The form on* $C_1(V,q)$

$$(c_1, c_2) \mapsto \mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2) \in \Delta$$

is hermitian relatively to the involution of Δ *given by the restriction of* τ *to* Δ*, and is nonsingular. Moreover,*

$$\mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2) = \iota\left(\mathrm{Trd}_{C_0(V,q)}(c_2\tau(c_1))\right) \quad \textit{for all } c_1, c_2 \in C_1(V,q).$$

Proof: The first claim is obvious. We now check nonsingularity. Let $v \in V$ be such that $q(v) \neq 0$. Multiplication on the left by v in $C(V,q)$ defines an F-linear isomorphism between $C_0(V,q)$ and $C_1(V,q)$, hence every element $c \in C_1(V,q)$ is of the form vc' for some $c' \in C_0(V,q)$. For all $c_1', c_2' \in C_0(V,q)$ we have

$$\mathrm{Trd}_{C_0(V,q)}(\tau(vc_1') \cdot vc_2') = q(v) \cdot \mathrm{Trd}_{C_0(V,q)}(\tau(c_1')c_2'). \tag{2.4}$$

Therefore, if vc_1' is in the radical of the form $\mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2)$, then

$$\mathrm{Trd}_{C_0(V,q)}(\tau(c_1')c_2') = 0$$

for all $c_2' \in C_0(V,q)$. Since $C_0(V,q)$ is an Azumaya algebra over Δ, the quadratic form $\mathrm{Trd}_{C_0(V,q)}(x^2)$ is nonsingular on $C_0(V,q)$, hence the preceding relation forces $\tau(c_1') = 0$, hence $vc_1' = 0$. This shows that the hermitian form $\mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2)$ is nonsingular on $C_1(V,q)$.

To complete the proof, observe that, for $c_1', c_2' \in C_0(V,q)$:

$$vc_2' \cdot \tau(vc_1') = vc_2'\tau(c_1')v = vc_2'\tau(c_1')v^{-1} \cdot q(v).$$

Since the restriction of the inner automorphism $\mathrm{Int}(v)$ to $C_0(V,q)$ is ι-semilinear, we have:

$$\mathrm{Trd}_{C_0(V,q)}(vc_2'\tau(c_1')v^{-1}) = \iota\left(\mathrm{Trd}_{C_0(V,q)}(c_2'\tau(c_1'))\right).$$

Since $\mathrm{Trd}_{C_0(V,q)}(\tau(c_1')c_2') = \mathrm{Trd}_{C_0(V,q)}(c_2'\tau(c_1'))$ for $c_1', c_2' \in C_0(V,q)$, it follows that

$$\mathrm{Trd}_{C_0(V,q)}(vc_2' \cdot \tau(vc_1')) = q(v) \cdot \iota\left(\mathrm{Trd}_{C_0(V,q)}(\tau(c_1')c_2')\right).$$

Comparing with equation (2.4), we get the required relation. ∎

We then define a nonsingular hermitian form on $V \otimes C_1(V,q)$ (relatively to the involution $\tau|_\Delta$ on Δ) by:

$$H(v_1 \otimes c_1, v_2 \otimes c_2) = b_q(v_1, v_2)\ \mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2) \qquad \text{for } v_1, v_2 \in V \text{ and } c_1, c_2 \in C_1(V,q).$$

(3.3) Proposition. *For* $\xi_1, \xi_2 \in V \otimes C_1(V,q)$*,* $f \in \mathrm{End}(V)$ *and* $u_1, u_2 \in C_0(V,q)$*,*

$$H(\xi_1, f \cdot [u_1 * \xi_2 \cdot u_2]) = H(\sigma_q(f) \cdot [\tau(u_1) * \xi_1 \cdot \tau(u_2)], \xi_2).$$

Proof: The Proposition follows from a direct computation. It suffices to consider the case where $\xi_1 = v_1 \otimes c_1$, $\xi_2 = v_2 \otimes c_2$. Then $f \cdot [u_1 * \xi_2 \cdot u_2] = f(v_2) \otimes u_1c_2u_2$, hence

$$H(\xi_1, f \cdot [u_1 * \xi_2 \cdot u_2]) = b_q(v_1, f(v_2))\ \mathrm{Trd}_{C_0(V,q)}(\tau(c_1)u_1c_2u_2).$$

Similarly,

$$H(\sigma_q(f) \cdot [\tau(u_1) * \xi_1 \cdot \tau(u_2)], \xi_2) = b_q(\sigma_q(f)(v_1), v_2)\ \mathrm{Trd}_{C_0(V,q)}(u_2\tau(c_1)u_1c_2).$$

∎

3.2. Definition of the Clifford bimodule

In order to define an analogue of $V \otimes C_1(V,q)$ for a central simple algebra with orthogonal involution (A,σ), we first define a canonical representation of the symmetric group S_{2n} on $A^{\times n}$.

Representation of the symmetric group

As above, we denote by $\underline{A}$ the underlying vector space of the F-algebra A. For any integer $n \geq 2$, we define a generalized sandwich map

$$\mathrm{Sand}_n : \underline{A}^{\otimes n} \to \mathrm{Hom}_F(\underline{A}^{\otimes n-1}, \underline{A})$$

by the condition:

$$\mathrm{Sand}_n(\underline{a_1} \otimes \cdots \otimes \underline{a_n})(\underline{b_1} \otimes \cdots \otimes \underline{b_{n-1}}) = \underline{a_1 b_1 a_2 b_2 \ldots b_{n-1} a_n}.$$

(So, Sand_2 is the map denoted simply Sand in section 3.1 of Chapter 1).

(3.4) Lemma. *For any central simple F-algebra A, the map* Sand_n *is an isomorphism of vector spaces.*

Proof: The case $n = 2$ was proved before: see Lemma 3.3. For $n \geq 3$, we use bijectivity of Sand_2. First, we observe that it suffices to prove surjectivity of Sand_n, since $\underline{A}^{\otimes n}$ and $\mathrm{Hom}_F(\underline{A}^{\otimes n-1}, \underline{A})$ have the same dimension over F. Let $a_1, \ldots, a_m$ be a basis of A. We construct a basis of $\mathrm{Hom}_F(\underline{A}^{\otimes n-1}, \underline{A})$ as follows: for any sequence $\mathbf{i} = (i_1, \ldots, i_n)$ of indices with $1 \leq i_k \leq m$, let $f_{\mathbf{i}} : \underline{A}^{\otimes n-1} \to \underline{A}$ be the linear map such that

$$f_{\mathbf{i}}(\underline{a_{j_1}} \otimes \cdots \otimes \underline{a_{j_{n-1}}}) = \begin{cases} 0 & \text{if } (j_1, \ldots, j_{n-1}) \neq (i_1, \ldots, i_{n-1}) \\ \underline{a_{i_n}} & \text{if } (j_1, \ldots, j_{n-1}) = (i_1, \ldots, i_{n-1}). \end{cases}$$

The maps $f_{\mathbf{i}}$ thus defined form a basis of $\mathrm{Hom}_F(\underline{A}^{\otimes n-1}, \underline{A})$, when $\mathbf{i}$ runs over the set of all sequences $(i_1, \ldots, i_n)$. Therefore, it suffices to show that each of the maps $f_{\mathbf{i}}$ is in the image of Sand_n.

For any fixed sequence $\mathbf{i} = (i_1, \ldots, i_n)$ and any $\ell = 1, \ldots, n-1$, we may find $c_\ell \in \underline{A}^{\otimes 2}$ such that

$$\mathrm{Sand}_2(c_\ell)(\underline{a_{j_\ell}}) = \begin{cases} 0 & \text{if } j_\ell \neq i_\ell \\ 1 & \text{if } j_\ell = i_\ell, \end{cases}$$

because Sand_2 is surjective. Let $c_\ell = \sum_{k \in I_\ell} \underline{u_{\ell,k}} \otimes \underline{v_{\ell,k}}$. Then

$$\sum_{k_1 \in I_1, \ldots, k_{n-1} \in I_{n-1}} (u_{1,k_1} a_{j_1} v_{1,k_1})(u_{2,k_2} a_{j_2} v_{2,k_2}) \ldots (u_{n-1,k_{n-1}} a_{j_{n-1}} v_{n-1,k_{n-1}}) =$$

$$= \begin{cases} 0 \text{ if } (j_1, \ldots, j_{n-1}) \neq (i_1, \ldots, i_{n-1}) \\ 1 \text{ if } (j_1, \ldots, j_{n-1}) = (i_1, \ldots, i_{n-1}) \end{cases}$$

hence

$$\mathrm{Sand}_n\left(\sum_{k_1 \in I_1, \ldots, k_{n-1} \in I_{n-1}} \underline{a_{i_n} u_{1,k_1}} \otimes \underline{v_{1,k_1} u_{2,k_2}} \otimes \cdots \otimes \underline{v_{n-2,k_{n-2}} u_{n-1,k_{n-1}}} \otimes \underline{v_{n-1,k_{n-1}}} \right) = f_{\mathbf{i}}.$$

∎

(3.5) Proposition. *Let (A,σ) be a central simple F-algebra with involution of orthogonal type. For all $n \geq 1$ there is a canonical representation $\rho_n : S_{2n} \to \mathrm{GL}(\underline{A}^{\otimes n})$ of the symmetric group S_{2n}, such that in the split case $A = V \otimes V$,*

$$\rho_n(\pi)(v_1 \otimes \cdots \otimes v_{2n}) = v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(2n)} \qquad \text{for all } \pi \in S_{2n} \text{ and } v_1, \ldots, v_{2n} \in V.$$

Proof: We first define the image of the transpositions $\tau(i) = (i, i+1)$ for $i = 1, \ldots, 2n-1$.

If i is odd, $i = 2\ell + 1$, let

$$\rho_n(\tau(i)) = I_{\underline{A}} \otimes \cdots \otimes I_{\underline{A}} \otimes \underline{\sigma} \otimes I_{\underline{A}} \otimes \cdots \otimes I_{\underline{A}},$$

where $\underline{\sigma}$ is in $\ell + 1$-st position. In the split case, σ corresponds to the twist under the standard identification $A = V \otimes V$; therefore

$$\rho_n(\tau(2\ell+1))(v_1 \otimes \cdots \otimes v_{2\ell+1} \otimes v_{2\ell+2} \otimes \cdots \otimes v_{2n}) = v_1 \otimes \cdots \otimes v_{2\ell+2} \otimes v_{2\ell+1} \otimes \cdots \otimes v_{2n}.$$

If i is even, $i = 2\ell$, we define $\rho_n(\tau(i))$ by the condition:

$$\begin{aligned} \mathrm{Sand}_n(\tau(i)(u))(x) \;=\; & \mathrm{Sand}_n(u)(I_{\underline{A}} \otimes \cdots \otimes I_{\underline{A}} \otimes \underline{\sigma} \otimes I_{\underline{A}} \otimes \cdots \otimes I_{\underline{A}}(x)) \\ & \text{for } u \in \underline{A}^{\times n} \text{ and } x \in \underline{A}^{\times n-1} \end{aligned}$$

where $\underline{\sigma}$ is in ℓ-th position. The same computation as in Lemma 2.3 shows that in the split case

$$\rho_n(\tau(2\ell))(v_1 \otimes \cdots \otimes v_{2\ell} \otimes v_{2\ell} \otimes \cdots \otimes v_{2n}) = v_1 \otimes \cdots \otimes v_{2\ell+1} \otimes v_{2\ell} \otimes \cdots \otimes v_{2n},$$

as required.

In order to define $\rho_n(\pi)$ for arbitrary $\pi \in S_{2n}$, we use the fact that $\tau(1), \ldots, \tau(2n-1)$ generate S_{2n}: we fix some factorization

$$\pi = \tau_1 \circ \cdots \circ \tau_s \qquad \text{where } \tau_1, \ldots, \tau_s \in \{\tau(1), \ldots, \tau(2n-1)\}$$

and define $\rho_n(\pi) = \rho_n(\tau_1) \circ \cdots \circ \rho_n(\tau_s)$. Then, in the split case $A = V \otimes V$,

$$\rho_n(\pi)(v_1 \otimes \cdots \otimes v_{2n}) = v_{\pi^{-1}(1)} \otimes \cdots \otimes v_{\pi^{-1}(2n)} \qquad \text{for all } \pi \in S_{2n} \text{ and } v_1, \ldots, v_{2n} \in V,$$

hence ρ_n is a homomorphism in the split case. Extending scalars to a splitting field, we see that ρ_n also is a homomorphism in the general case. Therefore, the definition of $\rho_n(\pi)$ does not actually depend on the factorization of π. ∎

The definition

As above, let (A,σ) be a central simple F-algebra with orthogonal involution. For all $n \geq 1$, let $\gamma_n = \rho_n((1,2,\ldots,2n)^{-1}) \in GL(\underline{A}^{\otimes n})$, where ρ_n is as in Proposition 3.5, and let $\gamma = \oplus\gamma_n : T(\underline{A}) \to T(\underline{A})$ be the induced linear map. Thus, in the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$, we have, under the identification $A = V \otimes V$ induced by $\hat{b}_q$:

$$\gamma(v_1 \otimes \cdots \otimes v_{2n}) = \gamma_n(v_1 \otimes \cdots \otimes v_{2n}) = v_2 \otimes \cdots \otimes v_{2n} \otimes v_1.$$

Let also $T_+(\underline{A}) = \oplus_{n\geq 1}\underline{A}^{\otimes n}$. The vector space $T_+(\underline{A})$ carries a natural structure of left and right module over the tensor algebra $T(\underline{A})$. We define a new left module structure $*$ as follows: for $u \in T(\underline{A})$ and $v \in T_+(\underline{A})$ we set

$$u * v = \gamma^{-1}(u \otimes \gamma(v)).$$

Thus, in the split case $A = V \otimes V$, $\sigma = \sigma_q$, the product $*$ avoids the first factor:

$$(u_1 \otimes \cdots \otimes u_{2i}) * (v_1 \otimes \cdots \otimes v_{2j}) = v_1 \otimes u_1 \otimes \cdots \otimes u_{2i} \otimes v_2 \otimes \cdots \otimes v_{2j}.$$

(Compare the definition of $*$ in section 3.1).

(3.6) Definition. The *canonical Clifford bimodule* of (A,σ) is defined as:

$$D(A,\sigma) = \frac{T_+(\underline{A})}{[J_1(\sigma) * T_+(\underline{A})] + [T_+(\underline{A}) \cdot J_1(\sigma)]}$$

where $J_1(\sigma)$ is the 2-sided ideal of $T(\underline{A})$ which is involved in the definition of the Clifford algebra $C(A,\sigma)$. (See definition 2.4).

The map $a \mapsto \underline{a} \in T_+(\underline{A})$ induces a canonical F-linear map

$$d\colon A \to D(A,\sigma).$$

(3.7) Theorem. *Let (A,σ) be a central simple F-algebra with an orthogonal involution.*

1. *The F-vector space $D(A,\sigma)$ carries a natural $C(A,\sigma)$-bimodule structure, where action on the left is through $*$, and a natural left A-module structure. Moreover, the various actions commute, so that $D(A,\sigma)$ is a left $A\otimes_F C(A,\sigma)\otimes_F C(A,\sigma)^{\mathrm{op}}$-module.*
2. *In the split case $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$, the standard identification $\mathrm{Id}_V \otimes \hat{b}_q : V \otimes V \xrightarrow{\sim} \mathrm{End}_F(V) = V \otimes V^*$ induces a standard identification of Clifford bimodules $V \otimes_F C_1(V,q) \xrightarrow{\sim} D(A,\sigma)$, with the obvious $C_0(V,q)$-bimodule and left $\mathrm{End}_F(V)$-module operations.*
3. *The canonical map $d : A \to D(A,\sigma)$ is an injective homomorphism of left A-modules.*
4. $\dim_F D(A,\sigma) = (\deg A).2^{(\deg A)-1}$.

Proof: Extending scalars to split A, it is easy to verify that

$$J_2(\sigma) * T_+(\underline{A}) \subseteq T_+(\underline{A}) \cdot J_1(\sigma) \quad \text{and} \quad T_+(\underline{A}) \cdot J_2(\sigma) \subseteq J_1(\sigma) * T_+(\underline{A}).$$

Therefore, the actions of $T(\underline{A})$ on $T_+(\underline{A})$ on the left through $*$ and on the right through the usual product induce a $C(A,\sigma)$-bimodule structure on $D(A,\sigma)$.

We define on $T_+(\underline{A})$ a left A-module structure by using the multiplication map $\mu : \underline{A}^{\otimes 2} \to \underline{A}$ which carries $\underline{a} \otimes \underline{b}$ to $\underline{ab}$. Explicitly, for $a \in A$ and $u = \underline{u_1} \otimes \cdots \underline{u_i} \in \underline{A}^{\otimes i}$, we set

$$a \cdot u = \underline{au_1} \otimes \underline{u_2} \otimes \cdots \otimes \underline{u_i}.$$

Thus, in the split case $(A, \sigma) = (\mathrm{End}_F(V), \sigma_q)$, we have, under the standard identification $A = V \otimes V$:

$$a \cdot (v_1 \otimes \cdots \otimes v_{2i}) = a(v_1) \otimes v_2 \otimes \cdots \otimes v_{2i}.$$

It is then clear that the left action of A on $T_+(\underline{A})$ commutes with the left and right actions of $T(\underline{A})$. Therefore, the subspace $[J_1(\sigma) * T_+(\underline{A})] + [T_+(\underline{A}) \cdot J_1(\sigma)]$ is preserved under the action of A, and it follows that $D(A, \sigma)$ inherits this action from $T_+(\underline{A})$.

In the split case, the map $\mathrm{Id}_V \otimes \hat{b}_q^{-1} : A = V \otimes V^* \to V \otimes V$ induces a linear map from $D(A, \sigma)$ onto $V \otimes C_1(V, q)$. Using an orthogonal basis of (V, q), one can show that

$$\dim_F D(A, \sigma) \leq \dim_F V . \dim_F C_1(V, q).$$

Therefore, the induced map is an isomorphism. This proves *(1)* and *(2)*, and *(4)* follows by counting dimensions. Now, *(3)* is clear in the split case (see Proposition 3.1), and the Theorem follows. ∎

The canonical involution

We now use the involution σ on A to define an involutorial F-linear operator ω on $D(A, \sigma)$. As above, $\underline{\sigma}$ denotes the involution of $C(A, \sigma)$ induced by σ and τ is the involution on $C(V, q)$ which is the identity on V.

(3.8) Lemma. *There exists an involutorial F-linear operator ω on $D(A, \sigma)$ such that for $a \in A$, $c_1, c_2 \in C(A, \sigma)$ and $x \in D(A, \sigma)$,*

$$\omega(c_1 * x \cdot c_2) = \underline{\sigma}(c_2) * \omega(x) \cdot \underline{\sigma}(c_1), \quad \omega(a \cdot x) = a \cdot \omega(x) \quad \textit{and} \quad \omega(d(a)) = d(a).$$

Moreover, in the split case $(A, \sigma) = (\mathrm{End}_F(V), \sigma_q)$ we have $\omega = \mathrm{Id}_V \otimes \tau$ under the standard identifications $A = V \otimes V$, $D(A, \sigma) = V \otimes C_1(V, q)$.

Proof: Let $\tilde{\omega} = \gamma^{-1} \circ \underline{\sigma} : T_+(\underline{A}) \to T_+(\underline{A})$, where $\underline{\sigma}$ is the involution on $T(\underline{A})$ induced by σ. Thus, in the split case $A = V \otimes V$, $\sigma = \sigma_q$:

$$\tilde{\omega}(v_1 \otimes \cdots \otimes v_{2n}) = v_1 \otimes v_{2n} \otimes v_{2n-1} \otimes \cdots \otimes v_3 \otimes v_2.$$

Extending scalars to a splitting field of A, it is easy to check that for $a \in A$, $u_1, u_2 \in T(\underline{A})$ and $v \in T_+(\underline{A})$,

$$\tilde{\omega}(u_1 * v \cdot u_2) = \underline{\sigma}(u_2) * \tilde{\omega}(v) \cdot \underline{\sigma}(u_1), \quad \tilde{\omega}(a \cdot v) = a \cdot \tilde{\omega}(v) \quad \text{and} \quad \tilde{\omega}(\underline{a}) = \underline{a}.$$

It follows from the first relation that

$$\tilde{\omega}(J_1(\sigma) * T_+(\underline{A})) = T_+(\underline{A}) \cdot \underline{\sigma}(J_1(\sigma)) \subseteq T_+(\underline{A} \cdot J_1(\sigma))$$

and

$$\tilde{\omega}(T_+(\underline{A}) \cdot J_1(\sigma)) = \underline{\sigma}(J_1(\sigma)) * T_+(\underline{A}) \subseteq J_1(\sigma) * T_+(\underline{A}),$$

hence $\tilde{\omega}$ induces an involutorial F-linear operator ω on $D(A,\sigma)$ which satisfies the required conditions. ∎

The canonical hermitian form

For the next Proposition, observe that multiplication in A and $C(A,\sigma)$ endow the tensor product $A \otimes_F C(A,\sigma)$ with natural structures of A- and $C(A,\sigma)$-bimodules: for $a_1, a_2, x \in A$ and $c_1, c_2, y \in C(A,\sigma)$, we set:

$$a_1 \cdot (x \otimes y) \cdot a_2 = a_1 x a_2 \otimes y \quad \text{and} \quad c_1 \cdot (x \otimes y) \cdot c_2 = x \otimes c_1 y c_2.$$

(3.9) Proposition. *There exists an isomorphism of $C(A,\sigma)$-bimodules*

$$\psi : D(A,\sigma) \otimes_{C(A,\sigma)} D(A,\sigma) \xrightarrow{\sim} A \otimes_F C(A,\sigma)$$

such that in the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$ we have

$$\psi((v_1 \otimes c_1) \otimes (v_2 \otimes c_2)) = (v_1 \otimes v_2) \otimes c_1 c_2$$

through the standard identifications $A = V \otimes V$ and $D(A,\sigma) = V \otimes C_1(V,q)$. Moreover ψ satisfies

$$\psi((a_1 \cdot x_1) \otimes (a_2 \cdot x_2)) = a_1 \cdot \psi(x_1 \otimes x_2) \cdot \sigma(a_2)$$

and

$$\psi(\omega(x_1) \otimes \omega(x_2)) = (\sigma \otimes \underline{\sigma}) \circ \psi(x_2 \otimes x_1)$$

for $a_1, a_2 \in A$ and $x_1, x_2 \in D(A,\sigma)$.

Proof: We define a map $\tilde{\psi} : T_+(\underline{A}) \times T_+(\underline{A}) \to \underline{A} \otimes T(\underline{A})$ by:

$$\tilde{\psi}(u,v) = (\rho_{i+j}((1,2)) \circ \gamma_{i+j}^{-1})(u \otimes \gamma_j(v)) = \rho_{i+j}((1,2))(u * v) \quad \text{for } u \in \underline{A}^{\otimes i} \text{ and } v \in \underline{A}^{\otimes j}.$$

Straightforward verifications show that the map $\tilde{\psi}$ induces an isomorphism ψ with the required properties. (Note that it suffices to prove the additional properties of ψ when A is split.) ∎

We now use the isomorphism ψ to define a canonical hermitian form H on $D(A,\sigma)$.

As observed before, there is no significant loss if we restrict our attention to the case where the degree of A is even, since A is split if its degree is odd. Henceforth, we shall assume $\deg A = n = 2m$. According to Theorem 2.6, the center Δ of $C(A,\sigma)$ is then a quadratic étale F-algebra. We let ι denote the non-trivial automorphism of Δ/F. The restriction of $\underline{\sigma}$ to Δ is determined in *(3)* of Theorem 2.6:

$$\underline{\sigma}|_\Delta = \begin{cases} \mathrm{Id}_\Delta & \text{if } m \text{ is even} \\ \iota & \text{if } m \text{ is odd.} \end{cases}$$

Restricting to Δ the actions of $C(A,\sigma)$ on $D(A,\sigma)$, we may consider $D(A,\sigma)$ as a left and right module over Δ. Inspection of the split case (see equation 2.3) shows that

$$z * x = x \cdot \iota(z) \quad \text{for } z \in \Delta \text{ and } x \in D(A,\sigma). \tag{2.5}$$

Consider the Δ-linear form

$$t = \mathrm{Trd}_A \otimes \mathrm{Trd}_{C(A,\sigma)} : A \otimes_F C(A,\sigma) \to \Delta$$

(when $\Delta = F \times F$ and $C(A,\sigma) = C_1 \times C_2$, then $\mathrm{Trd}_{C(A,\sigma)} = \mathrm{Trd}_{C_1} \times \mathrm{Trd}_{C_2}$, i.e. $\mathrm{Trd}_{C(A,\sigma)}$ is the reduced trace of $C(A,\sigma)$ as an Azumaya algebra over Δ) and define $H : D(A,\sigma) \times D(A,\sigma) \to \Delta$ by:

$$H(x,y) = t \circ \psi(\omega(x) \otimes y).$$

(3.10) Proposition. *The map H is a nonsingular hermitian form on $D(A,\sigma)$, viewed as a right Δ-module, relative to the restriction $\underline{\sigma}|_\Delta$ of $\underline{\sigma}$ to Δ. (It is therefore a symmetric bilinear form if $\underline{\sigma}|_\Delta = I$, i.e. if m is even). In the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$ we have, under the standard identifications $A = V \otimes V$ and $D(A,\sigma) = V \otimes C_1(V,q)$:*

$$H(v_1 \otimes c_1, v_2 \otimes c_2) = b_q(v_1,v_2) \cdot \mathrm{Trd}_{C_0(V,q)}(\tau(c_1)c_2) \quad \text{for } v_1, v_2 \in V \text{ and } c_1, c_2 \in C_1(V,q). \tag{2.6}$$

Moreover H satisfies:

$$H(x, a \cdot [u * y \cdot v]) = H(\sigma(a) \cdot [\underline{\sigma}(u) * x \cdot \underline{\sigma}(v)], y)$$
$$\text{for } x, y \in D(A,\sigma),\ u, v \in C(A,\sigma) \text{ and } a \in A,$$

$$H(\omega(x), \omega(y)) = \underline{\sigma} \circ \iota(H(x,y)) \qquad \text{for } x, y \in D(A,\sigma) \tag{2.7}$$

and, if $\deg A = 2m \geq 4$,

$$H(d(a_1), d(a_2)) = 2^{m-1} \mathrm{Trd}_A(\sigma(a_1)a_2) \qquad \text{for } a_1, a_2 \in A, \tag{2.8}$$

where $d : A \to D(A,\sigma)$ is the canonical map.

Proof: Proposition 3.9 shows that

$$\psi(\omega(y) \otimes x) = (\sigma \otimes \underline{\sigma}) \circ \psi(\omega(x) \otimes y),$$

hence

$$H(y,x) = \underline{\sigma}(H(x,y)) \quad \text{for all } x,y \in D(A,\sigma).$$

Moreover, since ψ is an isomorphism of $C(A,\sigma)$-bimodules, we have for all $z \in \Delta$:

$$H(x,yz) = H(x,y)z.$$

Therefore, H is a hermitian form on $D(A,\sigma)$.

In the split case $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$ we have, under the identifications $A = V \otimes_F V$ induced by $\hat{b}_q$:

$$\mathrm{Trd}_A(v_1 \otimes v_2) = b_q(v_1,v_2).$$

Therefore, the definition of t and the description of ψ in the split case (Proposition 3.9) yield relation (2.6), which shows that the form H is the same as the form H of §3.1.

In order to prove that H is nonsingular and to verify the additional properties of H, it suffices to consider the split case. In this case, nonsingularity was proven in Lemma 3.2 and relation (2.7) in Proposition 3.3. In order to prove relation (2.7), we let $x_i = v_i \otimes c_i$ with $v_i \in V$ and $c_i \in C_1(V,q)$ for $i = 1,2$. Then

$$H(\omega(x_1),\omega(x_2)) = b_q(v_1,v_2) \cdot \mathrm{Trd}_{C_0(V,q)}(c_1\tau(c_2))$$

whereas

$$H(x_2,x_1) = b_q(v_2,v_1) \cdot \mathrm{Trd}_{C_0(V,q)}(\tau(c_2)c_1).$$

The preceding Lemma then yields

$$H(\omega(x_1),\omega(x_2)) = \iota(H(x_2,x_1)),$$

and the proof of relation (2.7) is complete since H is hermitian relative to $\underline{\sigma}$.

In order to prove relation (2.8) when $\deg A (= \dim V) \geq 4$, we pick an orthogonal basis $(e_1,\ldots,e_n)$ of (V,q). Since both sides of the relation we want to prove are bilinear over F, it suffices to prove it when a_1, a_2 run over the basis $(e_i \otimes e_j)_{1\leq i,j\leq n}$ of A. We have

$$\begin{aligned} H(d(e_i \otimes e_j), d(e_k \otimes e_\ell)) &= t((e_i \otimes e_k) \otimes e_j e_\ell) \\ &= b_q(e_i,e_k) \cdot \mathrm{Trd}_{C_0(V,q)}(e_j e_\ell) \end{aligned}$$

whereas

$$\begin{aligned} \mathrm{Trd}_A(\sigma(e_i \otimes e_j) \cdot e_k \otimes e_\ell) &= \mathrm{Trd}_A(b_q(e_i,e_k) \cdot e_j \otimes e_\ell) \\ &= b_q(e_i,e_k) \cdot b_q(e_j,e_\ell). \end{aligned}$$

Therefore, it suffices to show:

$$\mathrm{Trd}_{C_0(V,q)}(e_j e_\ell) = 2^{m-1} b_q(e_j,e_\ell) \quad \text{for } j,\ell = 1,\ldots,n.$$

This is clear if $j = \ell$, since then $e_j e_\ell = b_q(e_j,e_\ell)$. If $j \neq \ell$, pick a basis element e_r distinct from e_j and e_ℓ. The element $e_j e_r \in C_0(V,q)$ is invertible and anticommutes with $e_j e_\ell$, hence

$$\mathrm{Trd}_{C_0(V,q)}(e_j e_\ell) = 0 = b_q(e_j,e_\ell).$$

■

3.3. The fundamental relations

In this section, (A,σ) denotes a central simple F-algebra of even degree $n = 2m$ with orthogonal involution. Letting the Clifford algebra $C(A,\sigma)$ act on itself and on the canonical bimodule $D(A,\sigma)$, we will prove the following fundamental relations:

(3.11) Theorem. *Let* $\Delta = F(\sqrt{(-1)^m \operatorname{disc}\sigma})$ *be the center of the Clifford algebra* $C(A,\sigma)$.

1. *If* $\deg A \equiv 0 \bmod 4$ *(i.e. if* m *is even), then*

$$[C(A,\sigma)]^2 = 0 \quad \text{in } \operatorname{Br}(\Delta). \tag{2.9}$$

$$N_{\Delta/F}[C(A,\sigma)] = [A] \quad \text{in } \operatorname{Br}(F). \tag{2.10}$$

2. *If* $\deg A \equiv 2 \bmod 4$ *(i.e. if* m *is odd), then*

$$[C(A,\sigma)]^2 = [A_\Delta] \quad \text{in } \operatorname{Br}(\Delta). \tag{2.11}$$

$$N_{\Delta/F}[C(A,\sigma)] = 0 \quad \text{in } \operatorname{Br}(F). \tag{2.12}$$

(If $\Delta = F \times F$, *the norm* $N_{\Delta/F}$ *is defined as at the end of §3.2 of Chapter 1:* $N_{F\times F/F}(C_1 \times C_2) = C_1 \otimes_F C_2$.*)*

Relations (2.9) and (2.12) follow, by Theorem 3.1, from the fact that the canonical involution $\underline{\sigma}$ on $C(A,\sigma)$ is of the first kind when $\deg A \equiv 0 \bmod 4$ and of the second kind when $\deg A \equiv 2 \bmod 4$. More explicitly, the proof of Theorem 3.1 shows that these relations follow from the isomorphism

$$\underline{\sigma}_* : C(A,\sigma) \otimes_\Delta C(A,\sigma) \to \operatorname{End}_\Delta(C(A,\sigma)).$$

Relation (2.10) was first proved by Jacobson [8, Theorem 4] in the case where $\Delta = F \times F$. In the same special case, proofs of (2.10) and (2.11) have been given by Tits [22, Proposition 7], [23, 6.2]. In the general case, these relations have been established by Tamagawa [19] and by Tao [20].

The proof we present below derives from the action of $C(A,\sigma)$ on $D(A,\sigma)$; we will in fact prove a more precise result, taking the various involutions into account.

In order to describe the more precise result, we let $E(A,\sigma) = D(A,\sigma)^\omega$ denote the F-subspace of ω-invariant elements in $D(A,\sigma)$. If $\deg A \equiv 0 \bmod 4$, then $\sigma|_\Delta = \mathrm{Id}_\Delta$, hence Lemma 3.8 and relation (2.5) show that

$$\omega(xz) = \omega(x)\iota(z) \qquad \text{for } x \in D(A,\sigma) \text{ and } z \in \Delta.$$

Therefore, the mltiplication map $E(A,\sigma) \otimes_F \Delta \to D(A,\sigma)$ is an isomorphism of Δ-modules. Moreover, relation (2.7) shows that $H(e_1,e_2) \in F$ for all $e_1,e_2 \in E(A,\sigma)$, hence H restricts to a symmetric bilinear form B on $E(A,\sigma)$, and

$$(E(A,\sigma),B) \otimes_F \Delta = (D(A,\sigma),H).$$

In particular the form B is nonsingular.

(3.12) Theorem. *The $A \otimes_F C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)^{\mathrm{op}}$-module structure on $D(A,\sigma)$ induces the following canonical isomorphisms of algebras with involution:*

- *If* $\deg A \equiv 0 \bmod 4$*:*

$$(A,\sigma) \otimes_F N_{\Delta/F}(C(A,\sigma),\underline{\sigma}) \simeq (\mathrm{End}_F(E(A,\sigma)),\sigma_B).$$

- *If* $\deg A \equiv 2 \bmod 4$*:*

$$(A,\sigma) \otimes_F (C(A,\sigma),\underline{\sigma}) \otimes_\Delta (C(A,\sigma),\underline{\sigma}) \simeq ({}^{\iota}\mathrm{End}_\Delta(D(A,\sigma)),\sigma_H).$$

Proof: Suppose first that m is even. We define a left $C(A,\sigma) \otimes_F {}^{\iota}C(A,\sigma)$-module structure on $D(A,\sigma)$ by:

$$(c_1 \otimes {}^{\iota}c_2) \cdot x = c_1 * x \cdot \underline{\sigma}(c_2) \quad \text{for } c_1, c_2 \in C(A,\sigma) \text{ and } x \in D(A,\sigma).$$

In particular, since $\underline{\sigma}|_\Delta = I$, we have for $z \in \Delta$ and $x \in D(A,\sigma)$:

$$(z \otimes {}^{\iota}1) \cdot x = z * x \quad \text{and} \quad [1 \otimes (z \cdot {}^{\iota}1)] \cdot x = [1 \otimes {}^{\iota}(\iota(z)] \cdot x = x \cdot \iota(z).$$

Relation (2.5) then shows

$$(z \otimes {}^{\iota}1) \cdot x = [1 \otimes (z \cdot {}^{\iota}1)] \cdot x,$$

hence $D(A,\sigma)$ carries an induced structure of left module over $C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)$. From Lemma 3.8, we derive:

$$\omega((c_2 \otimes {}^{\iota}c_1) \cdot x) = c_1 * \omega(x) \cdot \underline{\sigma}(c_2) = (c_1 \otimes {}^{\iota}c_2) \cdot \omega(x),$$

for $c_1, c_2 \in C(A,\sigma)$ and $x \in D(A,\sigma)$. Therefore, the F-subspace $E(A,\sigma)$ of ω-invariant elements carries a structure of left module over $N_{\Delta/F}(C(A,\sigma))$.

On the other hand, the left action of A on $D(A,\sigma)$ induces an action on $E(A,\sigma)$, hence $E(A,\sigma)$ is a left module over $A \otimes_F N_{\Delta/F}(C(A,\sigma))$. This left module structure yields a homomorphism of F-algebras:

$$A \otimes_F N_{\Delta/F}(C(A,\sigma)) \to \mathrm{End}_F(E(A,\sigma)).$$

Since

$$\dim_F E(A,\sigma) = \tfrac{1}{2} \dim_F D(A,\sigma) = m \cdot 2^{2m-1}$$

and

$$\deg(A \otimes_F N_{\Delta/F}(C(A,\sigma))) = \deg A \cdot \deg C(A,\sigma) = 2m \cdot 2^{2m-2},$$

this homomorphism is an isomorphism. It only remains to check that this isomorphism transports the involution $\sigma \otimes N_{\Delta/F}(\underline{\sigma})$ to the adjoint involution with respect to B. This follows from relation (2.7) in Proposition 3.10.

Suppose then that m is odd. We define a left $C(A,\sigma) \otimes_F C(A,\sigma)$-module structure on $D(A,\sigma)$ by:

$$(c_1 \otimes c_2) \cdot x = c_1 * x \cdot \underline{\sigma}(c_2) \quad \text{for } c_1, c_2 \in C(A,\sigma) \text{ and } x \in D(A,\sigma).$$

Since $\underline{\sigma}|_\Delta = \iota$, relation (2.5) yields:

$$(z \otimes 1) \cdot x = x \cdot \iota(z) = (1 \otimes z) \cdot x \quad \text{for } z \in \Delta \text{ and } x \in D(A,\sigma). \tag{2.13}$$

Therefore, there is an induced $C(A,\sigma) \otimes_\Delta C(A,\sigma)$-module structure on $D(A,\sigma)$. Since the left action of A on $D(A,\sigma)$ commutes with the action of $C(A,\sigma) \otimes_\Delta C(A,\sigma)$, we get an F-algebra homomorphism:

$$A \otimes_F C(A,\sigma) \otimes_\Delta C(A,\sigma) \to \mathrm{End}_Z(D(A,\sigma)).$$

Counting dimensions over F, we see that this homomorphism is an isomorphism.

Note that, by relation (2.13), this isomorphism is not linear over Δ but ι-semilinear. Therefore, it yields an isomorphism of Δ-algebras:

$$A \otimes_F C(A,\sigma) \otimes_\Delta C(A,\sigma) \to {}^{\iota}\mathrm{End}_Z(D(A,\sigma)).$$

To complete the proof, it suffices to check that this isomorphism transports the involution $\sigma \otimes \underline{\sigma} \otimes \underline{\sigma}$ to the adjoint involution with respect to the bilinear form H; this follows from relation (2.7) in Proposition 3.10. ∎

Exercises for Chapter 2

1. Let (A, σ) be a central simple F-algebra with involution of the first kind and let $K \subset A$ be a subfield containing F. Suppose K consists of symmetric elements, so that the restriction $\sigma' = \sigma|_{C_A K}$ of σ to the centralizer of K in A is an involution of the first kind. Prove:
$$\operatorname{disc} \sigma = N_{K/F}(\operatorname{disc} \sigma').$$

2. Let Q be a quaternion algebra with canonical involution γ and let $Q' = (Q, \gamma)_-$ denote the space of pure quaternions. Show that Q' is a simple Lie subalgebra of $\mathfrak{L}(Q)$.

3. (Notations as in the previous exercise). Let Q_1 and Q_2 be two quaternion algebras over a field F. Show that the Lie algebras Q_1', Q_2' of pure quaternions are isomorphic if and only if the associative algebras Q_1 and Q_2 are isomorphic.

Chapter 3.

Similarities

In this chapter, we investigate the groups of similarities for algebras with involution. The quotient of such a group by its center is the group of automorphism of the algebra with involution, and is a twisted form of the projective orthogonal, symplectic or unitary group. Our study is more detailed (or rather, less incomplete) in the orthogonal case, where relations with the Clifford algebra can be obtained and an analogue of the special Clifford group can be defined.

§1. Definitions

To motivate our definition of a similarity for an algebra with involution, we first consider the case of a quadratic space (V, q) over a field F (of characteristic different from 2). A similarity in this case is a linear map $f : V \to V$ for which there exists a constant $\lambda \in F^\times$ such that

$$q(f(v)) = \lambda\, q(v) \qquad \text{for all } v \in V.$$

This condition can be linearized to:

$$b_q(f(v), f(w)) = \lambda\, b_q(v, w) \qquad \text{for all } v, w \in V$$

and can be rephrased as follows, using the adjoint involution σ_q:

$$b_q(\sigma_q(f) \circ f(v), w) = b_q(\lambda v, w) \qquad \text{for all } v, w \in V.$$

Therefore, a similarity is an element $f \in \mathrm{End}_F(V)$ for which there exists $\lambda \in F^\times$ such that $\sigma_q(f) \circ f = \lambda$.

(1.1) Definition. Let (A, σ) be a central simple F-algebra with involution. A *similarity* of (A, σ) is an element $a \in A$ such that

$$\sigma(a)a \in F^\times.$$

The scalar $\sigma(a)a$ is called the *similarity factor* of a and denoted by $\mu(a)$. The set of all similarities of (A,σ) is a subgroup of $A^\times$ which we denote by $\mathrm{Sim}(A,\sigma)$, and the map μ is a group homomorphism

$$\mu : \mathrm{Sim}(A,\sigma) \to F^\times.$$

We will also use more specific notations for the group $\mathrm{Sim}(A,\sigma)$ according to the kind and type of σ:

$$\mathrm{Sim}(A,\sigma) = \begin{cases} \mathrm{GO}(A,\sigma) & \text{if } \sigma \text{ is of orthogonal type.} \\ \mathrm{GSp}(A,\sigma) & \text{if } \sigma \text{ is of symplectic type.} \\ \mathrm{GU}(A,\sigma) & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

Similarities with similarity factor 1 are called *isometries* and denoted

$$\ker\mu = \begin{cases} \mathrm{O}(A,\sigma) & \text{if } \sigma \text{ is of orthogonal type.} \\ \mathrm{Sp}(A,\sigma) & \text{if } \sigma \text{ is of symplectic type.} \\ \mathrm{U}(A,\sigma) & \text{if } \sigma \text{ is of the second kind.} \end{cases}$$

The above definitions extend in a straightforward way to the case of involutions of the second kind on semi-simple algebras with center $F \times F$.

Similarities can also be characterized in terms of automorphisms of the algebra with involution: an automorphism of (A,σ) is an F-algebra automorphism which commutes with σ:

$$\mathrm{Aut}_F(A,\sigma) = \{\alpha \in \mathrm{Aut}_F(A) \mid \sigma \circ \alpha = \alpha \circ \sigma\}.$$

(1.2) Theorem. $\mathrm{Aut}_F(A,\sigma) = \{\mathrm{Int}(a) \mid a \in \mathrm{Sim}(A,\sigma)\}$. *There is therefore an exact sequence:*

$$1 \to F^\times \to \mathrm{Sim}(A,\sigma) \xrightarrow{\mathrm{Int}} \mathrm{Aut}_F(A,\sigma) \to 1.$$

Proof: By the Skolem-Noether theorem, every automorphism of A over F has the form $\mathrm{Int}(a)$ for some $a \in A^\times$. Since

$$\sigma \circ \mathrm{Int}(a) = \mathrm{Int}(\sigma(a)^{-1}) \circ \sigma,$$

the automorphism $\mathrm{Int}(a)$ commutes with σ if and only if $\sigma(a)^{-1} \equiv a \bmod F^\times$, i.e. $\sigma(a)a \in F^\times$. ∎

(1.3) Examples. 1. For every quadratic space (V,q), the discussion before definition 1.1 shows that

$$\mathrm{GO}(\mathrm{End}_F(V),\sigma_q) = \mathrm{GO}(V,q).$$

Similarly, if b is a nonsingular skew-symmetric form on a vector space V, then

$$\mathrm{GSp}(\mathrm{End}_F(V),\sigma_b) = \mathrm{GSp}(V,b).$$

2. Let A be a quaternion algebra with canonical involution γ. Since $\gamma(a)a \in F$ for all $a \in A$, we have

$$\mathrm{Sim}(A,\gamma)\ (= \mathrm{GSp}(A,\gamma)) = A^\times.$$

Let σ be an orthogonal involution on A; by example 2.3 we have

$$\sigma = \mathrm{Int}(q) \circ \gamma$$

for some invertible pure quaternion q. Since γ is canonical, it commutes with all automorphisms of A. Therefore, an inner automorphism $\mathrm{Int}(a)$ commutes with σ if and only if it commutes with $\mathrm{Int}(q)$, i.e. $aq \equiv qa \bmod F^\times$. If $\lambda \in F^\times$ is such that $aq = \lambda qa$, then taking the reduced norm of both sides of this equation we get $\lambda^2 = 1$, hence $aq = \pm qa$. The group of similarities of (A,σ) therefore consists of the invertible elements which commute or anticommute with q. If h is any invertible element which anticommutes with q, we thus have:

$$\mathrm{GO}(A,\sigma) = F(q)^\times \cup F(q)^\times \cdot h.$$

3. Let $A = Q_1 \otimes_F Q_2$ be a tensor product of two quaternion algebras and $\sigma = \gamma_1 \otimes \gamma_2$, the tensor product of the canonical involutions. As observed in example 2.10 of Chapter 2, the Lie algebra $\mathrm{Alt}(\sigma)$ decomposes in a unique way as a direct sum of the (Lie-) algebras of pure quaternions in Q_1 and Q_2:

$$\mathrm{Alt}(\sigma) = (Q_1' \otimes 1) \oplus (1 \otimes Q_2').$$

Therefore, every automorphism $\alpha \in \mathrm{Aut}_F(A,\sigma)$ must preserve the pair of subalgebras $\{Q_1, Q_2\}$. If $Q_1 \neq Q_2$, then α restricts to automorphisms of Q_1 and of Q_2. Let $q_1 \in Q_1'$, $q_2 \in Q_2'$ be such that

$$\alpha|_{Q_1} = \mathrm{Int}(q_1) \qquad \alpha|_{Q_2} = \mathrm{Int}(q_2).$$

Then $\alpha = \mathrm{Int}(q_1 \otimes q_2)$; so

$$\mathrm{GO}(A,\sigma) = \{q_1 \otimes q_2 \mid q_1 \in Q_1', q_2 \in Q_2'\}.$$

If $Q_1 \simeq Q_2$, then we may assume for the convenience of notations that $A = Q \otimes_F Q$, where Q is a quaternion algebra isomorphic to Q_1 and Q_2. Under the isomorphism $\gamma_* : A \to \mathrm{End}_F(Q)$ such that $\gamma_*(q_1 \otimes q_2)(x) = q_1 x \gamma(q_2)$ for $q_1, q_2, x \in Q$, the involution $\sigma = \gamma \otimes \gamma$ is transported to the adjoint involution with respect to the reduced norm quadratic form; therefore

$$\mathrm{GO}(A,\sigma) = \mathrm{GO}(Q, \mathrm{Nrd}_Q).$$

Odd degree case

If (A,σ) is a central simple F-algebra of odd degree with involution of the first kind, then A is split: $A = \mathrm{End}_F(V)$ and $\sigma = \sigma_q$ for some quadratic space (V,q). If $f \in A$ is a similarity of (V,q) with similarity factor $\lambda \in F^\times$, then taking the determinant of both sides of the relation

$$\lambda \cdot q \simeq q$$

we get $\lambda \in F^{\times 2}$. If $\lambda = \lambda_1^2$, then $\lambda_1^{-1} f$ is an isometry. Therefore,

$$\mathrm{GO}(A,\sigma) = \mathrm{GO}(V,q) = \mathrm{O}(V,q) \cdot F^\times \simeq \mathrm{O}(V,q) \times F^\times.$$

Direct similarities

Suppose (A,σ) is a central simple F-algebra of even degree with involution of the first kind:

$$\deg A = n = 2m.$$

Taking the reduced norm of both sides in the equality

$$\sigma(a)a = \mu(a) \in F^\times \qquad \text{for } a \in \mathrm{Sim}(A,\sigma),$$

we get

$$\mathrm{Nrd}_A(a)^2 = \mu(a)^{2m},$$

hence

$$\mathrm{Nrd}_A(a) = \pm\mu(a)^m.$$

The element $a \in \mathrm{Sim}(A,\sigma)$ is called a *direct* (resp. *indirect*) similarity if $\mathrm{Nrd}_A(a) = +\mu(a)^m$ (resp. $\mathrm{Nrd}_A(a) = -\mu(a)^m$).

(1.4) Proposition. *If σ is symplectic, all the similarities of (A,σ) are direct.*

Proof: Since direct and indirect similarities are preserved under scalar extension, we may assume that the algebra A is split: let $A = M_n(F)$ and $\sigma = \mathrm{Int}\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} \circ t$ where t is the transpose involution and I_m is the unit matrix of order m. The condition for $a \in A^\times = \mathrm{GL}_n(F)$ to be a similarity with similarity factor $\mu(a) = \lambda \in F^\times$ is then:

$$\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} a^t \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} a = \lambda,$$

or

$$a^t \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} a = \lambda \begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix}.$$

Taking the pfaffian of both sides we get, by known formulas for pfaffians (see [3, Theorem 3.28]):

$$(\det a)\,\mathrm{pf}\begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix} = \lambda^m\,\mathrm{pf}\begin{pmatrix} 0 & -I_m \\ I_m & 0 \end{pmatrix},$$

hence $\det a = \lambda^m$. ∎

In the case of orthogonal involutions, it is clear that direct similarities form a subgroup of index at most 2 in the group of all similarities; we denote this subgroup by $\mathrm{GO}_+(A,\sigma)$, and we denote by $\mathrm{GO}_-(A,\sigma)$ the coset of indirect similarities, which may be empty[1]. We also denote:

$$\mathrm{O}_+(A,\sigma) = \mathrm{GO}_+(A,\sigma) \cap \mathrm{O}(A,\sigma) = \{a \in A \mid \sigma(a)a = \mathrm{Nrd}_A(a) = 1\}$$

and

$$\mathrm{O}_-(A,\sigma) = \mathrm{GO}_-(A,\sigma) \cap \mathrm{O}(A,\sigma) = \{a \in A \mid \sigma(a)a = 1 = -\mathrm{Nrd}_A(a)\}.$$

The elements in $\mathrm{O}_+(A,\sigma)$ are the *direct isometries*.

(1.5) Examples. 1. Hyperplane reflections in a quadratic space (V,q) are indirect similarities (in fact, indirect isometries). Therefore, $\mathrm{GO}_+(V,q)$ is a subgroup of index 2 in $\mathrm{GO}(V,q)$ and $\mathrm{O}_+(V,q)$ is a subgroup of index 2 in $\mathrm{O}(V,q)$.

2. Let A be a quaternion algebra with canonical involution γ and let $\sigma = \mathrm{Int}(q) \circ \gamma$ for some invertible pure quaternion q. Let also $h \in A$ be an invertible pure quaternion which anticommutes with q. The group $\mathrm{GO}(A,\sigma)$ has been determined in example 1.3 (2); straightforward norm computations show that

$$\mathrm{GO}_+(A,\sigma) = F(q)^\times \qquad \text{and} \qquad \mathrm{GO}_-(A,\sigma) = F(q)^\times \cdot h.$$

However, no element in $F(q)^\times \cdot h$ has norm 1 unless A is split, so

$$\mathrm{O}_+(A,\sigma) = \mathrm{O}(A,\sigma) = \{z \in F(q) \mid N_{F(q)/F}(z) = 1\} \quad \text{if } A \text{ is not split.}$$

3. Let $A = Q_1 \otimes_F Q_2$, a tensor product of two quaternion algebras, and $\sigma = \gamma_1 \otimes \gamma_2$ where γ_1, γ_2 are the canonical involutions on Q_1 and Q_2.
If $Q_1 \not\simeq Q_2$, then we know from example 1.3 (3) that all the similarities of (A,σ) are of the form $q_1 \otimes q_2$ for some $q_1 \in Q_1^\times$, $q_2 \in Q_2^\times$. We have

$$\mu(q_1 \otimes q_2) = \gamma_1(q_1)q_1 \otimes \gamma_2(q_2)q_2 = \mathrm{Nrd}_{Q_1}(q_1) \cdot \mathrm{Nrd}_{Q_2}(q_2)$$

and

$$\mathrm{Nrd}_A(q_1 \otimes q_2) = \mathrm{Nrd}_{Q_1}(q_1)^{\deg Q_2} \cdot \mathrm{Nrd}_{Q_2}(q_2)^{\deg Q_1} = \mu(q_1 \otimes q_2)^2,$$

so all the similarities are direct:

$$\mathrm{GO}(A,\sigma) = \mathrm{GO}_+(A,\sigma) \qquad \text{and} \qquad \mathrm{O}(A,\sigma) = \mathrm{O}_+(A,\sigma).$$

On the other hand, if $Q_1 \simeq Q_2$, then the algebra A is split and the first example above shows that $\mathrm{GO}_+(A,\sigma)$ is a subgroup of index 2 in $\mathrm{GO}(A,\sigma)$.

[1] From the viewpoint of linear algebraic groups, one would rather say that this coset may have no rational point. Over a splitting field of A however, we get $\mathrm{GO}_-(A,\sigma) = \mathrm{GO}_-(V,q) \neq \varnothing$. The subgroup $\mathrm{GO}_+(A,\sigma)$ is the connected component of the identity in $\mathrm{GO}(A,\sigma)$.

§2. Relation with the Clifford algebra

In this section, (A,σ) denotes a central simple F-algebra of even degree with orthogonal involution:

$$\deg A = n = 2m.$$

Since the Clifford algebra $C(A,\sigma)$ is canonically associated to (A,σ), every automorphism $\alpha \in \mathrm{Aut}_F(A,\sigma)$ induces an automorphism

$$C(\alpha) \in \mathrm{Aut}_F(C(A,\sigma),\underline{\sigma}).$$

Explicitly, $C(\alpha)$ can be defined as the unique automorphism of $C(A,\sigma)$ such that

$$C(\alpha)(c(a)) = c(\alpha(a)) \qquad \text{for } a \in A,$$

where $c: A \to C(A,\sigma)$ is the canonical map. The map

$$C: \mathrm{Aut}_F(A,\sigma) \to \mathrm{Aut}_F(C(A,\sigma),\underline{\sigma})$$

is a group homomorphism. Slightly abusing notations, we also denote by C the homomorphism

$$C: \mathrm{GO}(A,\sigma) \to \mathrm{Aut}_F(C(A,\sigma),\underline{\sigma})$$

obtained by composing the preceding map with the epimorphism Int : $\mathrm{GO}(A,\sigma) \to \mathrm{Aut}_F(A,\sigma)$ of Theorem 1.2. Thus, for $g \in \mathrm{GO}(A,\sigma)$ and $a \in A$,

$$C(g)(c(a)) = c(gag^{-1}).$$

(2.1) Proposition. *Suppose A is split: $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$ for some quadratic space (V,q). Then, under the standard identifications $\mathrm{GO}(A,\sigma) = \mathrm{GO}(V,q)$ and $C(A,\sigma) = C_0(V,q)$, the canonical map*

$$C: \mathrm{GO}(V,q) \to C_0(V,q)$$

is defined by

$$C(g)(v_1 \cdot \cdots \cdot v_{2r}) = \mu(g)^{-r}\, g(v_1) \cdot \cdots \cdot g(v_{2r})$$

for $g \in \mathrm{GO}(V,q)$ and $v_1,\dots,v_{2r} \in V$.

Proof: It suffices to check the formula above on generators $v \cdot w$ of $C_0(V,q)$. For $v,w \in V$, the product $v \cdot w$ in $C(V,q)$ is the image of $v \otimes w$ under the canonical map c:

$$v \cdot w = c(v \otimes w),$$

hence

$$C(g)(v \cdot w) = c(g \circ (v \otimes w) \circ g^{-1}).$$

Let $\lambda = \mu(g)$; then $\sigma(g)^{-1} = \lambda^{-1} g$ hence, for $x \in V$,

$$(g \circ (v \otimes w) \circ g^{-1})(x) = g(v)\, b_q(w, g^{-1}(x)) = g(v)\, b_q(\lambda^{-1} g(w), x).$$

Therefore, $(g \circ (v \otimes w) \circ g^{-1})(x) = (\lambda^{-1} g(v) \otimes g(w))(x)$, which shows:

$$g \circ (v \otimes w) \circ g^{-1} = \lambda^{-1} g(v) \otimes g(w),$$

hence $c(g \circ (v \otimes w) \circ g^{-1}) = \lambda^{-1} g(v) \cdot g(w)$. ∎

Note that, for $g \in \mathrm{GO}(A,\sigma)$, the automorphism $C(g)$ of $C(A,\sigma)$ is F-linear but does not necessarily leave the center Δ of $C(A,\sigma)$ elementwise invariant. This condition in fact characterizes the direct similarities:

(2.2) Proposition. *A similarity $g \in \mathrm{GO}(A,\sigma)$ is direct if and only if $C(g)$ leaves the center Δ of $C(A,\sigma)$ elementwise invariant.*

Proof: It suffices to check the split case: $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$. We then use the standard identifications and the Proposition above. Let $(e_1,\dots,e_{2m})$ be an orthogonal basis of (V,q). For $g \in \mathrm{GO}(A,\sigma) = \mathrm{GO}(V,q)$, we have

$$C(g)(e_1 \cdot \cdots \cdot e_{2m}) = \mu(g)^{-m} g(e_1) \cdot \cdots \cdot g(e_{2m}).$$

On the other hand, calculations in the Clifford algebra show:

$$g(e_1) \cdot \cdots \cdot g(e_{2m}) = \det(g)\, e_1 \cdot \cdots \cdot e_{2m};$$

hence $e_1 \cdot \cdots \cdot e_{2m}$ is invariant under $C(g)$ if and only if $\det(g) = \mu(g)^m$. ∎

The image of the canonical map C has been determined by Wonenburger:

(2.3) Proposition. *If $\deg A > 2$, the canonical homomorphism $C : \mathrm{Aut}_F(A,\sigma) \to \mathrm{Aut}_F(C(A,\sigma),\underline{\sigma})$ is injective; its image consists of the automorphisms of $(C(A,\sigma),\underline{\sigma})$ which preserve the image $c(A)$ of A under the canonical map $c : A \to C(A,\sigma)$.*

Proof: From the definition of $C(\alpha)$ for $\alpha \in \mathrm{Aut}_F(A,\sigma)$, it is clear that this automorphism preserves the image $c(A)$ of A. Conversely, suppose $\beta \in \mathrm{Aut}_F(C(A,\sigma),\underline{\sigma})$ preserves $c(A)$. By Proposition 2.9 of Chapter 2, c is injective on $\mathrm{Alt}(\sigma)$, hence β induces a bijective linear map[2]

$$\beta' : \mathrm{Alt}(\sigma) \to \mathrm{Alt}(\sigma).$$

Since $\mathrm{Alt}(\sigma)$ generates A as an associative algebra (see the comments following Proposition 2.9 of Chapter 2), β' extends to at most one automorphism β'' of A; if it exists, this automorphism β'' then has the property that $C(\beta'') = \beta$. If $\beta = \mathrm{Id}$, then $\beta' = \mathrm{Id}$ and therefore $\beta'' = \mathrm{Id}$; this shows that C is injective. To show the existence of β'' in the general case, we may extend scalars to a splitting field of A; the property then follows from [24, Theorem 4]. ∎

Remarks:

1. The preceding Proposition also holds for central simple algebras of odd degree with orthogonal involution: see [24, Theorem 4].

2. If $\mathrm{char}\, F = 0$ and $\deg A \geq 10$, Lie algebra techniques can be used to prove that the Lie-algebra automorphism β' extends to an associative algebra automorphism β'': see [9, p. 307].

[2] In fact, a Lie-algebra automorphism of $\mathrm{Alt}(\sigma)$.

§3. The special Clifford group

Recall that for a quadratic space (V,q), the special Clifford group $\Gamma_+(V,q)$ is defined by:

$$\Gamma_+(V,q) = \{c \in C_0(V,q)^\times \mid c \cdot V \cdot c^{-1} \subset V\}$$

where the product $c \cdot V \cdot c^{-1}$ is computed in the Clifford algebra $C(V,q)$ (see for instance [18, §9.3][3]). Conjugation by $c \in \Gamma_+(V,q)$ induces a direct isometry of V, denoted $\chi(c)$:

$$\chi(c)(v) = c \cdot v \cdot c^{-1} \in V \qquad \text{for } v \in V,$$

and there is an exact sequence:

$$1 \to F^\times \to \Gamma_+(V,q) \xrightarrow{\chi} \mathrm{O}_+(V,q) \to 1 \tag{3.1}$$

(see [18, Theorem 3.3]).

Although there is no analogue of the (full) Clifford algebra for an algebra with involution, we show in this section that the canonical Clifford bimodule may be used to define an analogue of the special Clifford group.

As in the preceding section, (A,σ) denotes a central simple F-algebra of even degree with an orthogonal involution:

$$\deg A = n = 2m.$$

As the Clifford algebra $C(A,\sigma)$, the bimodule $D(A,\sigma)$ also is canonically associated to (A,σ). Therefore, every automorphism $\alpha \in \mathrm{Aut}_F(A,\sigma)$ induces a bijective linear map

$$D(\alpha) : D(A,\sigma) \to D(A,\sigma)$$

such that

$$D(\alpha)(d(a)) = d(\alpha(a)) \qquad \text{for } a \in A$$

and

$$D(\alpha)(a \cdot [c_1 * x \cdot c_2]) = \alpha(a) \cdot [C(\alpha)(c_1) * D(\alpha)(x) \cdot C(\alpha)(c_2)]$$

for $a \in A$, $c_1, c_2 \in C(A,\sigma)$ and $x \in D(A,\sigma)$. (Explicitly, $D(\alpha)$ is induced by the map $\underline{\alpha} : T_+(\underline{A}) \to T_+(\underline{A})$ such that

$$\underline{\alpha}(\underline{a_1} \otimes \cdots \otimes \underline{a_r}) = \underline{\alpha(a_1)} \otimes \cdots \otimes \underline{\alpha(a_r)}.)$$

As in the preceding section, we extend this definition to the group $\mathrm{GO}(A,\sigma)$, by letting $D(g) = D(\mathrm{Int}(g))$ for $g \in \mathrm{GO}(A,\sigma)$.

For $g \in \mathrm{GO}(A,\sigma)$, we also define a map

$$\delta_g : D(A,\sigma) \to D(A,\sigma)$$

[3] In [18], the group $\Gamma_+(V,q)$ is denoted $\mathrm{S}\Gamma(V,q)$ and $\mathrm{O}_+(V,q)$ is denoted $\mathrm{SO}(V,q)$.

by

$$\delta_g(x) = g^{-1} \cdot D(g)(x) \qquad \text{for } x \in D(A,\sigma).$$

The map δ_g is a homomorphism of left A-modules, since for $a \in A$ and $x \in D(A,\sigma)$,

$$\delta_g(a \cdot x) = g^{-1} \cdot (gag^{-1}) \cdot D(g)(x) = a \cdot \delta_g(x).$$

In the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$, the same arguments as in Proposition 2.1 show that, under the standard identifications $\mathrm{GO}(A,\sigma) = \mathrm{GO}(V,q)$, $D(A,\sigma) = V \otimes C_1(V,q)$,

$$D(g)(v \otimes w_1 \cdot \cdots \cdot w_{2r-1}) = \mu(g)^{-r}\, g(v) \otimes g(w_1) \cdot \cdots \cdot g(w_{2r-1})$$

and

$$\delta_g(v \otimes w_1 \cdot \cdots \cdot w_{2r-1}) = \mu(g)^{-r}\, v \otimes g(w_1) \cdot \cdots \cdot g(w_{2r-1})$$

for $g \in \mathrm{GO}(A,\sigma)$ and $v, w_1, \ldots, w_{2r-1} \in V$.

(3.1) Theorem. *For all $g \in \mathrm{O}_+(A,\sigma)$, there exists $c \in C(A,\sigma)^\times$ such that*

$$\delta_g(x) = c * x \cdot c^{-1} \qquad \textit{for all } x \in D(A,\sigma).$$

Proof: We first check the split case $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$. By (3.1), for all $g \in \mathrm{O}_+(V,q)$ we can find $c \in C_0(V,q)^\times$ such that $\chi(c) = g$. Then, for $v, w_1, \ldots, w_{2r-1} \in V$,

$$\begin{aligned} c * (v \otimes w_1 \cdot \cdots \cdot w_{2r-1}) \cdot c^{-1} &= v \otimes c \cdot w_1 \cdot \cdots \cdot w_{2r-1} \cdot c^{-1} \\ &= v \otimes (c \cdot w_1 \cdot c^{-1}) \cdot \cdots \cdot (c \cdot w_{2r-1} \cdot c^{-1}). \end{aligned}$$

Since $c \cdot w \cdot c^{-1} = \chi(c)(w) = g(w)$ for $w \in V$, and since $\mu(g) = 1$, we get:

$$c * (v \otimes w_1 \cdot \cdots \cdot w_{2r-1}) \cdot c^{-1} = \delta_g(v \otimes w_1 \cdot \cdots \cdot w_{2r-1}).$$

This proves the claim in the split case.

In the general case, recall the homomorphism

$$A \otimes_F C(A,\sigma) \otimes_F {}^{\iota}C(A,\sigma)^{\mathrm{op}} \to \mathrm{End}_F(D(A,\sigma))$$

induced by the $C(A,\sigma)$-bimodule and left A-module structure on $D(A,\sigma)$. Let Δ denote the center of $C(A,\sigma)$; considering $D(A,\sigma)$ as a left Δ-module, the homomorphism above yields an isomorphism

$$\Phi : C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_{A \otimes \Delta}(D(A,\sigma))$$

such that $\Phi(c_1 \otimes {}^{\iota}c_2^{\mathrm{op}})(x) = c_1 * x \cdot c_2$ for $c_1, c_2 \in C(A,\sigma)$ and $x \in D(A,\sigma)$.

For $g \in \mathrm{O}_+(A,\sigma)$, Proposition 2.2 shows that $C(g)$ leaves Δ elementwise invariant, hence δ_g is an $A \otimes \Delta$-endomorphism of $D(A,\sigma)$. By the isomorphism above, there exists a unique element $\xi \in C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)^{\mathrm{op}}$ such that $\Phi(\xi) = \delta_g$.

The beginning of the proof shows that over a splitting field of A the element ξ takes the form $c \otimes {}^{\iota}(c^{-1})^{\mathrm{op}}$, where $c \in C_0(V,q)$ is such that $\chi(c) = g$. Since the minimal

number of terms in a decomposition of an element of a tensor product is invariant under scalar extension, it follows that $\xi = c_1 \otimes {}^{\iota}c_2^{\mathrm{op}}$ for some $c_1, c_2 \in C(A,\sigma)$. Moreover, if $s : C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)^{\mathrm{op}} \to C(A,\sigma) \otimes_\Delta {}^{\iota}C(A,\sigma)^{\mathrm{op}}$ denotes the switch map, defined by

$$s(c \otimes {}^{\iota}c'^{\mathrm{op}}) = c' \otimes {}^{\iota}c^{\mathrm{op}} \qquad \text{for } c, c' \in C(A,\sigma),$$

then $s(\xi)\xi = 1$, since $\xi = c \otimes {}^{\iota}(c^{-1})^{\mathrm{op}}$ over a splitting field. Therefore, the elements $c_1, c_2 \in C(A,\sigma)^\times$ are subject to:

$$c_1 c_2 = \lambda \in \Delta \qquad \text{with } N_{\Delta/F}(\lambda) = 1.$$

By Hilbert's Theorem 90, there exists $\lambda_1 \in \Delta$ such that $\lambda = \lambda_1 \iota(\lambda_1)^{-1}$. Then $\xi = c_3 \otimes {}^{\iota}(c_3^{-1})^{\mathrm{op}}$ for $c_3 = \lambda_1^{-1} c_1$, hence

$$\delta_g(x) = c_3 * x \cdot c_3^{-1} \qquad \text{for } x \in D(A,\sigma).$$

■

(3.2) Definition. The *Clifford group* $\Gamma(A,\sigma)$ is defined by

$$\Gamma(A,\sigma) = \{c \in C(A,\sigma)^\times \mid c * d(A) \cdot c^{-1} \subset d(A)\}.$$

Since the $C(A,\sigma)$-bimodule actions on $D(A,\sigma)$ commute with the left A-module action and since the canonical map $d : A \to D(A,\sigma)$ is a homomorphism of left A-modules, the condition defining the Clifford group is equivalent to:

$$c * d(1) \cdot c^{-1} \in d(A).$$

For $c \in \Gamma(A,\sigma)$, define $\chi(c) \in A$ by the relation:

$$c * d(1) \cdot c^{-1} = d(\sigma(\chi(c))).$$

(The element $\chi(c)$ is uniquely determined by this relation, since the canonical map d is injective: see Theorem 3.7).

(3.3) Proposition. *In the split case* $(A,\sigma) = (\mathrm{End}_F(V), \sigma_q)$, *the standard identifications* $C(A,\sigma) = C_0(V,q)$, $D(A,\sigma) = V \otimes C_1(V,q)$ *induce an identification* $\Gamma(A,\sigma) = \Gamma_+(V,q)$, *and the map* χ *defined above is the same as the map* χ *of (3.1). In particular,* $\chi(c) \in \mathrm{O}_+(A,\sigma)$ *for all* $c \in \Gamma(A,\sigma)$.

Proof: Under the standard identifications, we have $A = V \otimes V$ and $d(A) = V \otimes V \subset V \otimes C_1(V,q)$. Moreover, for $c \in C(A,\sigma) = C_0(V,q)$ and $v, w \in V$,

$$c * d(v \otimes w) \cdot c^{-1} = v \otimes c \cdot w \cdot c^{-1}. \tag{3.2}$$

Therefore, the condition $c * d(A) \cdot c^{-1} \subset d(A)$ amounts to:

$$v \otimes c \cdot w \cdot c^{-1} \in V \otimes V \qquad \text{for all } v, w \in V,$$

or $c \cdot V \cdot c^{-1} \subset V$. This proves the first claim.

Suppose now $c * d(1) \cdot c^{-1} = d(\sigma(g))$. Since d is a homomorphism of left A-modules, we then get for all $v, w \in V$:

$$\begin{aligned} c * d(v \otimes w) \cdot c^{-1} &= (v \otimes w) \cdot (c * d(1) \cdot c^{-1}) \\ &= d((v \otimes w) \circ \sigma(g)). \end{aligned}$$

Now, for $x \in V$,

$$\begin{aligned} (v \otimes w) \circ \sigma(g)(x) &= v\, b_q(w, \sigma(g)(x)) \\ &= v\, b_q(g(w), x) \\ &= (v \otimes g(w))(x), \end{aligned}$$

hence $(v \otimes w) \circ \sigma(g) = v \otimes g(w)$ and

$$c * d(v \otimes w) \cdot c^{-1} = d(v \otimes g(w)).$$

In view of equation (3.2), this shows: $g(w) = c \cdot w \cdot c^{-1}$. ∎

(3.4) Proposition. *The following sequence is exact:*

$$1 \to F^\times \to \Gamma(A, \sigma) \xrightarrow{\chi} O_+(A, \sigma) \to 1.$$

Proof: The fact that $\ker \chi = F^\times$ follows by scalar extension to a splitting field from exact sequence (3.1). Surjectivity of χ follows from Theorem 3.1. ∎

We conclude by mentioning two extra properties of the group $\Gamma(A, \sigma)$. The second one will allow us to define the spin group $\mathrm{Spin}(A, \sigma)$.

(3.5) Proposition. *The triangle*

$$\begin{array}{ccc} \Gamma(A,\sigma) & \xrightarrow{\quad\chi\quad} & O_+(A,\sigma) \\ & {\scriptstyle \mathrm{Int}} \searrow \quad \swarrow {\scriptstyle C} & \\ & \mathrm{Aut}_F(C(A,\sigma)) & \end{array}$$

commutes.

Proof: It suffices to check the split case. If $c \in \Gamma_+(V, q)$ and $\chi(c) = g$, then for $v, w \in V$,

$$\begin{aligned} C(g)(v \cdot w) &= g(v) \cdot g(w) \\ &= (c \cdot v \cdot c^{-1}) \cdot (c \cdot w \cdot c^{-1}) \\ &= c \cdot (v \cdot w) \cdot c^{-1}. \end{aligned}$$

∎

(3.6) Proposition. $\Gamma(A,\sigma) \subset \mathrm{Sim}(C(A,\sigma),\underline{\sigma})$; *more precisely, for* $c \in \Gamma(A,\sigma)$,

$$\mu(c) = \underline{\sigma}(c)c \in F^\times.$$

Proof: This may be seen by extending scalars to a splitting field of A. Alternatively, one may argue "rationally" as follows: since $c * d(1) \cdot c^{-1} \in d(A)$, this element is invariant under the involution ω on $D(A,\sigma)$:

$$\omega(c * d(1) \cdot c^{-1}) = c * d(1) \cdot c^{-1}.$$

By Lemma 3.8 of Chapter 2, we have

$$\omega(c * d(1) \cdot c^{-1}) = \underline{\sigma}(c)^{-1} * d(1) \cdot \underline{\sigma}(c).$$

Combining these two relations, we get:

$$(\underline{\sigma}(c)c) * d(1) \cdot (\underline{\sigma}(c)c)^{-1} = d(1),$$

hence $\underline{\sigma}(c)c \in \ker\chi = F^\times$. ∎

(3.7) Definition. The *spin group* $\mathrm{Spin}(A,\sigma)$ is the group of elements in $\Gamma(A,\sigma)$ with similarity factor 1:

$$\mathrm{Spin}(A,\sigma) = \{c \in \Gamma(A,\sigma) \mid \underline{\sigma}(c)c = 1\}.$$

In the split case $(A,\sigma) = (\mathrm{End}_F(V),\sigma_q)$ the standard identifications yield $\mathrm{Spin}(A,\sigma) = \mathrm{Spin}(V,q)$.

Using the last Proposition above, we may also define a spinor norm for direct isometries:

(3.8) Definition. The spinor norm $\mathrm{NS} : \mathrm{O}_+(A,\sigma) \to F^\times/F^{\times 2}$ is the map which completes the following commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & F^\times & \longrightarrow & \Gamma(A,\sigma) & \xrightarrow{\chi} & \mathrm{O}_+(A,\sigma) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle 2} & & \downarrow{\scriptstyle \mu} & & \vdots{\scriptstyle \mathrm{NS}} & & \\
1 & \longrightarrow & F^{\times 2} & \longrightarrow & F^\times & \longrightarrow & F^\times/F^{\times 2} & \longrightarrow & 1
\end{array}$$

Exercises for Chapter 3.

1. Let Q be a quaternion F-algebra with canonical involution γ, and let $A = Q \otimes_F Q$ with involution $\sigma = \gamma \otimes \gamma$. Prove that $\mathrm{GO}_+(A,\sigma) = \{q_1 \otimes q_2 \mid q_1, q_2 \in Q^\times\}$ and determine the group of similarity factors $\mu(\mathrm{GO}_+(A,\sigma))$.

2. Let (A,σ) be a central simple F-algebra with involution of the first kind and let $\alpha \in \mathrm{Aut}_F(A)$. Prove that the following statements are equivalent:

   (a) $\alpha \in \mathrm{Aut}_F(A,\sigma)$.

   (b) $\alpha[(A,\sigma)_+] = (A,\sigma)_+$.

   (c) $\alpha[(A,\sigma)_-] = (A,\sigma)_-$.

3. Let (A,σ) be a central simple F-algebra with orthogonal involution and degree a power of 2, and let $B \subset A$ be a proper subalgebra with center F. Prove that every similarity $f \in \mathrm{GO}(A,\sigma)$ such that $fBf^{-1} = B$ is direct.

4. Let B be a central simple F-algebra and let $A = B \times B^{\mathrm{op}}$, with the involution σ (of the second kind) defined by:

$$\sigma(b_1, b_2^{\mathrm{op}}) = (b_2, b_1^{\mathrm{op}}).$$

   Describe the group of similarities $\mathrm{GU}(A,\sigma)$.

Bibliography

[1] A.A. Albert. *Structure of Algebras.* Coll. Pub. 24, Amer. Math. Soc., Providence, R.I., 1961.

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

[3] E. Artin. *Geometric Algebra.* Interscience Pub., New York, N.Y., 1957.

[4] E. Bayer-Fluckiger, D.B. Shapiro, J.-P. Tignol. Hyperbolic Involutions. Preprint, 1992.

[5] A. Berele, D. Saltman. The centers of generic division algebras with involution. *Israel J. Math.* **63** (1988) 98–118.

[6] P. Draxl. *Skew Fields.* London Math. Soc. Lecture Notes Series 81, Cambridge Univ. Press, Cambridge, 1983.

[7] I.N. Herstein. *Topics in Ring Theory.* Chicago Lectures in Math., Univ. Chicago Press, Chicago, 1969.

[8] N. Jacobson. Clifford algebras for algebras with involution of type D, *J. Algebra* **1** (1964) 288–300. (pp. 516–528 in: *Collected Mathematical Papers, vol. 2,* Birkhäuser, Boston, 1989).

[9] N. Jacobson. *Lie Algebras.* Dover Publications, Inc. New York, 1979.

[10] M.-A. Knus, M. Ojanguren. *Théorie de la descente et algèbres d'Azumaya.* Lecture Notes in Math. 389, Springer-Verlag, Berlin, 1974.

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

[12] M.-A. Knus, R. Parimala, R. Sridharan. On the discriminant of an involution. *Bull. Soc. Math. Belgique, Sér. A* **43** (1991) 89-98.

[13] M.-A. Knus, R. Parimala, R. Sridharan. Involutions on rank 16 central simple algebras, *J. Indian Math. Soc.* **57** (1991) 143–151.

[14] A.S. Merkurjev. On the norm residue homomorphism of degree 2. *Dokl. Akad. Nauk SSSR* **261** (1981) 542–547. (English translation: *Soviet Math. Dokl.***24** (1981) 546–551.

[15] C. Riehm. The corestriction of algebraic structures. *Invent. Math.* **11** (1970) 73–98.

[16] L.H. Rowen, D.J. Saltman. The discrimination of an involution. Secret paper, 1990?

[17] W. Scharlau. Zur Existenz von Involutionen auf einfachen Algebren. *Math. Z.* **145** (1975) 29–32.

[18] W. Scharlau. *Quadratic and Hermitian Forms.* Grundlehren math. Wiss. 270. Springer-Verlag, Berlin, 1985.

[19] T. Tamagawa. On Clifford algebra. Secret paper, 1971?

[20] D. Tao. The generalized even Clifford algebra. Preprint, 1992.

[21] J.-P. Tignol. On the corestriction of central simple algebras. *Math. Z.* **194** (1987) 267–274.

[22] J. Tits. Formes quadratiques, groupes orthogonaux et algèbres de Clifford. *Invent. Math.* **5** (1968) 19–41.

[23] J. Tits. Représentations linéaires irréductibles d'un groupe réductif sur un corps quelconque. *J. reine angew. Math.* **247** (1971) 196–220.

[24] M.J. Wonenburger. The Clifford algebra and the group of similitudes. *Canadian J. Math.* **14** (1961) 60–68.