Max-Albert Knus

Quadratic Forms,
Clifford Algebras and Spinors

IMECC-UNICAMP

1988

Max-Albert Knus

ETH
Mathematik
Rämistr. 101
CH–8092 Zürich
Switzerland

AMS Subject Classification (1985 Revision): 11E04, 11E16, 11E20, 11E39, 11E57, 11E81, 11E88, 15A63, 15A66, 15A90, 20G15, 20G45

Foreword

These notes grew out of a course given at UNICAMP for two months between August and October 1987. One aim of the course was to present the basic theory of quadratic forms and Clifford algebras over a field in a characteristic free way. In even dimension we restrict attention to nonsingular forms. In odd dimension nonsingularity implies that the characteristic must be different from 2. An elegant way to avoid this restriction is to work with $\frac{1}{2}$–regular forms. Such a form is the orthogonal sum of a 1–dimensional form and of a nonsingular form of even dimension. The $\frac{1}{2}$–regular forms behave almost as nicely as nonsingular forms and they are also defined in characteristic 2. A typical example in dimension 3 is given by the elements of reduced trace zero in a quaternion algebra. The notion of $\frac{1}{2}$–regularity is due to Kneser (see his Göttingen lecture notes mentioned in the bibliography at the end of these notes).

Another purpose of the lectures was to give a detailled study of forms of low dimension, low meaning ≤ 6. The Clifford algebra gives much information for these forms. In particular the Clifford algebra can be used to describe quite explicitly the spin group, the Lie algebra of the orthogonal group and the group of special similitudes of a form. In dimensions 4, 5, and 6 we have applied methods developed in joint papers with Parimala and Sridharan. These methods also give a different approach to results of Dieudonné (Acta Math. 87, 1952). Moreover they do not depend on the characteristic of the field. The main tool is a reduced pfaffian, introduced independently by Fröhlich, Jacobson and Tamagawa. Its role is very similar to the role of the reduced norm of a quaternion algebra in the study of forms of dimension 3 and 4. A general theory of the pfaffian and applications to quadratic forms of rank 6 over commutative rings can be found in the papers with Parimala and Sridharan mentioned above. This theory of forms of rank 6 is related to the theory of central simple algebras of dimension 16. In particular it yields new proofs of some theorems of Albert.

These notes have two appendices. In the first one we summarize, in a chart, all the proven results on the structure of Clifford algebras in low dimensions. The second gives some concrete applications. We introduce spinors, following Chevalley, and compute explicitly the spinor representations of four Clifford algebras occuring in physics: the Pauli algebra, the Minkowski algebra, the Majorana algebra and the Dirac algebra.

Even if this course deals with forms over fields, it was sometimes convenient (and even necessary) to consider forms over commutative rings. Moreover readers, familiar with the techniques of commutative algebra, will observe that the argument, used many times, to prove a result by passing to some field extension, comes from descent theory.

We make the following conventions. The ground field is denoted by K. Vector spaces are always finite dimensional. Algebras are associative with 1 (if not explicitly mentioned) and K is identified with $K \cdot 1$. Unadorned tensor products are taken over K. The group of units of an algebra is denoted by $A^{\bullet}$. Maps are written on the left, like functions. We use a unique numbering in each chapter for Examples, Lemmas, Propositions, Theorems and Corollaries. The bibliography only contains books and papers mentioned in the notes. We did not try systematically to give credits for the results or the proofs used.

I am very grateful to A. Paques, UNICAMP, who made my visit to Campinas possible. He attended my course with patience, read the notes very carefully and made many suggestions (and corrections). I also would like to thank P. Hänsli, who helped me a lot in correcting the final version, R. Parimala and R. Sridharan, who read a preliminary version and Elda Mortari for her excellent script with LaTeX. Of course I am still responsible for any mistakes remaining. My visit to UNICAMP was financed by grants from FINEP and FAPESP. I thank these institutions and UNICAMP for their support.

Contents

Contents

Chapter 1

Quadratic Forms

This chapter gives basic facts about quadratic forms which hold over fields independently of the characteristic. The proof of Theorem 10 (Witt cancellation) follows Wagner (see also the notes of Micali–Revoy). Useful references are the books of Bourbaki, Chevalley, Lam, Scharlau, Baeza, Demazure–Gabriel and Micali–Revoy, as well as the paper of Bass on Clifford algebras.

Let K be a field. A *quadratic form* is a pair (V, q), where V is a finite dimensional vector space over K and q is a map $q : V \to K$ such that

1) $q(\lambda x) = \lambda^2 q(x),\ \ \lambda \in K,\ x \in V$;

2) the map $b_q : V \times V \to K$ defined by $b_q(x, y) = q(x + y) - q(x) - q(y)$ is bilinear.

We call b_q the *polar* of q.

Let $b : V \times V \to K$ be a symmetric bilinear form on V. The map

$$h : V \to V^* = \mathrm{Hom}_K(V, K), \quad h(x) = b(x,\ -),\ \ x \in V,$$

is called the *adjoint* of b. If we identify V with V^{**} through the map $x \mapsto x^{**},\ x^{**}(f) = f(x),\ f \in V^*$, we have $h^*(x) = b(-, x)$, where $h^* : V^{**} \to V^*$ is the transpose of h, i.e. $h^*(x^{**})(y) = x^{**}(h(y)) = h(y)(x)$. Hence $h^* = h$, since b is symmetric. We say that b is *nonsingular* and that the pair (V, b) is a *symmetric bilinear space* if h is an isomorphism. A quadratic form $q : V \to K$ is called *nonsingular* and the pair (V, q) is called a *quadratic space* if the polar b_q is nonsingular. We denote its adjoint by h_q. If the characteristic of K is not equal to 2, the polar b_q determines q, since

$$q(x) = \tfrac{1}{2} b_q(x, x), \qquad x \in V,$$

and the theory of quadratic spaces is identical with the theory of symmetric bilinear spaces. The two theories are quite different in characteristic 2. In these notes we shall restrict to quadratic spaces.

A *morphism of quadratic forms*

$$\varphi : (V, q) \to (V', q')$$

is a K–linear map $\varphi : V \to V'$ such that $q'(\varphi(x)) = q(x)$ for all $x \in V$. Similarly a *morphism of bilinear forms*

$$\varphi : (V, b) \to (V', b')$$

is a K–linear map $\varphi : V \to V'$ such that $b'(\varphi(x), \varphi(y)) = b(x, y)$ for all $x, y \in V$. A morphism $\varphi : (V, b) \to (V', b')$ (resp. $(V, q) \to (V', q')$) must be injective if b (resp. q) is nonsingular. Morphisms, which are isomorphisms, are called *isometries.* The group of isometries of (V, b) (resp. (V, q)) is denoted by $O(V, b)$ (resp. $O(V, q)$) and is called the *orthogonal group* of (V, b) (resp. (V, q)). An isometry of quadratic forms induces an isometry of the associated polar forms but not conversely (if char $K = 2$), see Example 2.

Let $q : V \to K$ be a quadratic form and $K \subset L$ a field extension. We can extend the form q to a form $q_L : L \otimes V \to L$ by putting

$$q_L(\sum_i \lambda_i \otimes v_i) = \sum_i \lambda_i^2 q(v_i) + \sum_{i<j} \lambda_i \lambda_j b_q(v_i, v_j).$$

The polar of q_L is $1 \otimes b_q$ and its adjoint is $1 \otimes h_q : L \otimes V \to L \otimes V^* = (L \otimes V)^*$. It is usual to denote q_L by $1 \otimes q$ and $(L \otimes V,\ 1 \otimes q)$ by $L \otimes (V, q)$. Obviously $L \otimes (V, q)$ is nonsingular if, and only if, (V, q) is nonsingular.

Let $\{e_1, \dots e_n\}$ be a basis of V and let

$$a_i = q(e_i), \quad a_{ij} = b_q(e_i, e_j), \quad 1 \le i, \quad j \le n.$$

The form q is determined by the a_i and a_{ij}, since

$$q(x) = \sum_i a_i x_i^2 + \sum_{i<j} a_{ij} x_i x_j \quad \text{for} \quad x = \sum_i x_i e_i.$$

In matrix notation, we have $q(x) = \xi^t\alpha\xi$, ξ^t denoting the transpose of ξ, where

$$\xi = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \qquad \text{and} \qquad \alpha = \begin{pmatrix} a_1 & a_{12} & \cdots & a_{1n} \\ 0 & a_2 & \cdots & a_{2n} \\ \vdots & 0 & \ddots & \vdots \\ 0 & \cdots & 0 & a_n \end{pmatrix}.$$

Conversely, for any $(n \times n)$-matrix ρ, we can define a quadratic form q on V by putting $q(x) = \xi^t\rho\xi$ for $x = \sum_i x_i e_i$ and $\xi = (x_1, \dots x_n)^t$.The matrix ρ is not uniquely determined by q. We have

$$\xi^t\rho\xi = \xi^t\rho'\xi, \quad \forall \xi \in K^n \Leftrightarrow \rho = \rho' + \gamma, \quad \gamma \text{ alternating.}$$

We recall that an *alternating* matrix is a matrix of the form

$$\gamma = \begin{pmatrix} 0 & c_{12} & \cdots & c_{1n} \\ -c_{12} & 0 & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -c_{1n} & -c_{2n} & \cdots & 0 \end{pmatrix}$$

i.e. γ is antisymmetric and has zeroes on the diagonal. A matrix γ is alternating if and only if $\gamma = \delta - \delta^t$ for some matrix δ. Thus, a basis $\{e_1, \dots e_n\}$ of V being fixed, q is determined by the class $[\rho]$ of ρ modulo alternating matrices and each such class corresponds to a quadratic form. Moreover in each class $[\rho]$ there is a triangular matrix. We say that ρ and ρ' are equivalent if $[\rho] = [\rho']$ i.e. if $\rho - \rho'$ is alternating. If α is as above, the matrix $\beta = (b_q(e_i, e_j))$ of the polar is

$$\beta = \begin{pmatrix} 2a_1 & a_{12} & \cdots & a_{1n} \\ a_{12} & 2a_2 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & 2a_n \end{pmatrix} = \alpha + \alpha^t$$

and $b_q(x, y) = \xi^t\beta\eta$ with $\xi = (x_1, \dots, x_n)^t$, $\eta = (y_1, \dots, y_n)^t$ if $x = \sum x_i e_i$ and $y = \sum y_i e_i$. Obviously β depends only on the class $[\alpha]$ of α. Let $\{e_1^*, \dots, e_n^*\}$ be the dual basis of V^*, i.e. $e_i^*(e_j) = \delta_{ij}$. We get

$$h_q(e_j) = \sum_i a_{ij} e_i^*$$

so that (V, q) is nonsingular if and only if $\det\beta \neq 0$. We call $\det\beta$ the *discriminant of q with respect to the basis* $\{e_1, \dots, e_n\}$ and denote it by $d(e_1, \dots, e_n)$. Let $\{e'_1, \dots, e'_n\}$ be another basis of V and let

$$e_j = \sum_i u_{ij} e'_i.$$

Let ν be the matrix (u_{ij}) and let $\beta' = (b_q(e'_i, e'_j))$. We have

$$\beta = \nu^t \beta' \nu.$$

Let $K^{\bullet 2}$ be the set of squares in $K^\bullet$. The class of $d(e_1, \ldots, e_n)$ modulo $K^{\bullet 2}$ does not depend on the choice of the basis $\{e_1, \ldots, e_n\}$. We denote this class by $\operatorname{disc}(q)$ and call it the *discriminant* of q. Similarly, if $\varphi : (V, q) \to (V', q')$ is an isometry and

$$\varphi(e_j) = \sum_i u_{ij} e'_i$$

for bases $\{e_1, \ldots, e_n\}$ of V, resp. $\{e'_1, \ldots, e'_n\}$ of V', we have $\beta = \nu^t \beta' \nu$, putting $\beta = (b_q(e_i, e_j))$, $\beta' = (b_{q'}(e'_i, e'_j))$ and $\nu = (u_{ij})$. The condition $\beta = \nu^t \beta' \nu$ is necessary and sufficient for the existence of an isometry of the bilinear spaces (V, b_q), (V', b'_q) but is not sufficient for an isometry of the quadratic spaces (V, q) and (V', q'). If $y = \varphi(x)$, $x \in V$, let $y = \sum_i y_i e'_i$, $x = \sum_i x_i e_i$, $\eta = (y_1, \ldots, y_n)^t$ and $\xi = (x_1, \ldots, x_n)^t$, so that $\eta = \nu \xi$. Assume that $q(x) = \xi^t \alpha \xi$ and $q'(y) = \eta^t \alpha' \eta$ for matrices α, resp. α'. We have

$$\xi^t \alpha \xi = \eta^t \alpha' \eta = \xi^t \nu^t \alpha' \nu \xi \quad \text{for all} \quad \xi \in K^n.$$

Therefore $\nu \in GL_n(K)$ defines an isometry if and only if $[\alpha] = [\nu^t \alpha' \nu]$. It follows that isometry classes of quadratic spaces are in $1-1$–correspondence with equivalence classes $[\alpha]$ of matrices $\alpha \in M_n(K)$ such that $\alpha + \alpha^t$ is nonsingular.

Remark 1. The interpretation of a quadratic space as the class $[\alpha]$ of a matrix α modulo alternating matrices was already applied in Klingenberg–Witt. This interpretation has led to important generalizations of the notion of a quadratic space (see the papers or books by Bak, Bass, Tits, Wall and Scharlau). We shall try to give an idea of these generalizations by some examples. Let R be a ring with an *involution* $r \mapsto \overline{r}$, i.e. an automorphism of the additive group of R such that $\overline{1} = 1$, $\overline{rs} = \overline{s}\,\overline{r}$ and $\overline{\overline{r}} = r$ for all $r, s \in R$. Further let $\varepsilon = \pm 1$ and let Λ be an additive subgroup of R such that

(1) $\{r - \varepsilon \overline{r},\ r \in R\} \subset \Lambda \subset \{r \in R \mid \overline{r} = -\varepsilon r\}$,

(2) for all $r \in R$, $\overline{r} \Lambda r \subset \Lambda$.

Further, let

$$\Lambda_n^\varepsilon = \{\alpha \in M_n(R) \mid \alpha = \begin{pmatrix} \lambda_1 & a_{12} & \cdots & a_{1n} \\ -\varepsilon a_{12} & \lambda_2 & & \\ & & \ddots & \\ -\varepsilon a_{1n} & & & \lambda_n \end{pmatrix}, \quad a_{ij} \in R,\ \lambda_i \in \Lambda\}.$$

For any matrix $\alpha = (a_{ij})$, we put $\alpha^* = (\overline{a}_{ij})^t$. It follows from the properties (1) and (2) of Λ that

$$\gamma \in \Lambda_n^\varepsilon \Rightarrow \alpha^*\gamma\alpha \in \Lambda_n^\varepsilon \quad \text{for all} \quad \alpha \in M_n(R).$$

We define now an equivalence relation $\alpha \sim \alpha'$ on $M_n(R)$ by

$$\alpha \sim \alpha' \Leftrightarrow \alpha - \alpha' \in \Lambda_n^\varepsilon$$

and denote the equivalence class by $[\alpha]$. We say that $[\alpha]$ is an (ε, Λ)–*quadratic form* on R^n and that $[\alpha]$ is *nonsingular* if $\beta = \alpha + \varepsilon\alpha^*$ is invertible (observe that β depends only on the class $[\alpha]$ of α). An *isometry* $[\alpha] \to [\alpha']$ is by definition a matrix $\nu \in GL_n(R)$ such that $[\alpha] = [\nu^*\alpha'\nu]$. We remark that an (ε, Λ)–quadratic form on R^n is not, as in the classical theory, a quadratic map $R^n \to R$. But we can associate to $[\alpha]$ a map

$$q : R^n \to R/\Lambda, \quad q(\xi) = \text{class of} \quad \xi^*\alpha\xi \quad \text{mod } \Lambda.$$

We now consider different special cases of (ε, Λ)–quadratic forms. Let $\Lambda_{\text{min}} = \{r - \varepsilon\,\overline{r},\ r \in R\}$ and $\Lambda_{\text{max}} = \{r \in R \mid \overline{r} = -\varepsilon\, r\}$.

1) R a field with trivial involution, $\varepsilon = 1$ and $\Lambda = \Lambda_{\text{min}}$: quadratic forms, $\Lambda = \Lambda_{\text{max}}$: symmetric bilinear forms.

2) R a field with trivial involution, $\varepsilon = -1$ and $\Lambda = \Lambda_{\text{min}}$: alternating forms, $\Lambda = \Lambda_{\text{max}}$: antisymmetric bilinear forms.

3) R a skew field with a nontrivial involution, $\varepsilon = 1$ $\Lambda = \Lambda_{\text{min}}$: even hermitian forms, $\Lambda = \Lambda_{\text{max}}$: hermitian forms.

More exotic cases are possible. We give two examples (without claiming that the corresponding theories have applications!)

4) R a field of characteristic 2 with trivial involution, $\varepsilon = 1$ (!) and $\Lambda = (R^2, +)$, the additive group of squares in R.

5) R a commutative ring with trivial involution, $\varepsilon = -1$ and Λ an ideal of R

such that $2R \subset \Lambda$.

We now give an important example of a quadratic space:

Example 2. Let V be a 2–dimensional vector space over K with a basis $\{e, f\}$. We define a quadratic form on V by

$$q(xe + yf) = xy \quad \text{or} \quad q(\xi) = \xi^t \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \xi \ \text{ for } \ \xi = \begin{pmatrix} x \\ y \end{pmatrix}.$$

The polar b_q has matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, hence (V, q) is nonsingular. We observe that $(V, q) \simeq (V, \lambda q)$ for any $\lambda \in K^\bullet$, since

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ 0 & 0 \end{pmatrix}.$$

The quadratic space (V, q) is called the *hyperbolic plane* and is denoted by $H(K)$. We have

$$O(V, b_q) = \left\{ \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in GL_2(K) \mid \begin{pmatrix} x & y \\ u & v \end{pmatrix}^t \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ u & v \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$$= \left\{ \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in GL_2(K) \mid 2xu = 2vy = 0, \ uy + xv = 1 \right\}$$

so that

$$O(V, b_q) = SL_2(K) = \left\{ \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in GL_2(K) \mid \det \begin{pmatrix} x & y \\ u & v \end{pmatrix} = 1 \right\}$$

if char $K = 2$. On the other hand

$$O(V, q) = \left\{ \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in GL_2(K) \ \mid \ xu = vy = 0, \ \ uy + xv = 1 \right\}.$$

Thus $O(V, q)$ is strictly contained in $O(V, b_q)$ in characteristic 2.

Let (V_1, q_1), (V_2, q_2) be quadratic forms. We define the *orthogonal sum*

$$(V, q) = (V_1 \perp V_2, q_1 \perp q_2)$$

as $V = V_1 \oplus V_2$ and $q(x) = q_1(x_1) + q_2(x_2)$ for $x = (x_1, x_2) \in V$, $x_i \in V_i$. We have obviously

$$\operatorname{disc}(q_1 \perp q_2) = \operatorname{disc}(q_1) \cdot \operatorname{disc}(q_2).$$

In particular $q_1 \perp q_2$ is nonsingular if, and only if, q_1, q_2 are nonsingular. Let (V, q) be a quadratic form (not necessarily nonsingular) and let $U \subset V$ be a subspace. We denote the restriction of q to U by $q|_U$ and we set

$$U^\perp = \{x \in V \mid b_q(x, y) = 0, \quad \forall y \in U\}.$$

Lemma 3. Let (V, q) be a quadratic form and let $U \subset V$ be a subspace such that $(U, q|_U)$ is nonsingular. Then

$$(V, q) = (U, q|_U) \perp (U^\perp, q|_{U^\perp}).$$

Proof. It clearly suffices to show that $V = U \oplus U^\perp$. Let $h : V \to V^*$ be the adjoint of q and let $h|_U : U \to U^*$ be its restriction to U. By hypothesis it is an isomorphism. Let now $v \in V$. The restriction of $h(v) \in V^*$ to U^* is in the image of $h|_U$ since $h|_U$ is an isomorphism. Thus there exists $u \in U$ such that $b(x, u) = b(x, v)$ for all $x \in U$. This means that $v - u$ is an element of $U^\perp$ or that $V = U + U^\perp$. The fact that $U \cap U^\perp = \{0\}$ follows from the fact that $q|_U$ is nonsingular.

Important examples of quadratic spaces are hyperbolic spaces. The hyperbolic plane $H(K)$ was defined in Example 2. A quadratic space isometric to the orthogonal sum of n hyperbolic planes is called a *hyperbolic space* of dimension $2n$ and is denoted by $H(K^n)$. The space $H(K^n)$ is given by the class $[\begin{pmatrix} 0 & 1_n \\ 0 & 0 \end{pmatrix}]$, where 1_n is the $n \times n$–identity matrix. There is another, more intrinsic, way to define hyperbolic spaces. Let V be a vector space of dimension n over K. We define a quadratic form on

$$H(V) = V \oplus V^*$$

by

$$q(x, f) = f(x), \qquad x \in V, \qquad f \in V^*.$$

Choosing a basis $\{e_1, \dots, e_n\}$ of V and taking the dual basis in V^*, it is easy to see that $H(V)$ is isometric to the hyperbolic space $H(K^n)$. Any K–linear isomorphism $\varphi : V \tilde{\to} V'$ induces an isometry

$$H(\varphi) = (\varphi, \varphi^{*-1}) : H(V) \tilde{\to} H(V').$$

Further, we have canonical isometries $H(V \oplus W) \simeq H(V) \perp H(W)$.

Let (V, q) be a quadratic space. Then $(V, -q)$ is also a quadratic space. We have

Proposition 4. $(V, q) \perp (V, -q) \simeq H(V)$.

Proof. If (V, q) is given by the class $[\alpha]$, then $q \perp -q$ is given by the class $[\left(\begin{smallmatrix} \alpha & 0 \\ 0 & -\alpha \end{smallmatrix}\right)]$. We have to find an invertible $(2n \times 2n)$–matrix ν such that

$$\left[\nu^t \begin{pmatrix} \alpha & 0 \\ 0 & -\alpha \end{pmatrix} \nu\right] = \left[\begin{pmatrix} 0 & 1_n \\ 0 & 0 \end{pmatrix}\right].$$

Such a matrix is given by

$$\nu = \begin{pmatrix} 1 & -1 \\ \alpha & \alpha^t \end{pmatrix}^{-1}$$

(use that $\left(\begin{smallmatrix} 0 & \alpha^t \\ -\alpha & 0 \end{smallmatrix}\right)$ is alternating and that $[\alpha] = [\alpha^t]$).

Corollary 5. Any quadratic space is an orthogonal summand in a hyperbolic space.

Let (V, q) be a quadratic space. An element $e \neq 0 \in V$ is called *isotropic* if $q(e) = 0$ and a subspace U of V is called *totally isotropic* if $q|_U$ is identically zero. For example the subspace V of the hyperbolic space $H(V)$ is totally isotropic. Conversely, we have

Proposition 6. Let U be a totally isotropic subspace of a quadratic space (V, q). There exists a morphism $\varphi : H(U) \to (V, q)$ whose restriction to U is the identity. In particular (V, q) contains an orthogonal summand isometric to $H(U)$.

Proof. The embedding $U \to V$ induces a surjective map $V^* \to U^*$. Composing with the isomorphism $h_q : V \tilde{\to} V^*$ we obtain a surjective map $t : V \to U^*$ given by $v \mapsto b_q(v, -)|_U$. Its kernel is $U^\perp$, i.e. the sequence

$$0 \to U^\perp \to V \xrightarrow{t} U^* \to 0$$

is exact. Let W be a direct summand of $U^\perp$ in V such that $t|_W$ is an isomorphism $W \tilde{\to} U^*$. It follows that the dual map $U \to W^*$, which is given by $u \mapsto b_q(u, -)|_W$ is also an isomorphism. Since $U \subset U^\perp$, $U \cap W = \{0\}$ and U, W generate a subspace of V which is a direct sum $U \oplus W$. The restriction of b_q to $U \oplus W$ is given by a bloc matrix

$$\beta = \begin{pmatrix} 0 & \alpha_1^t \\ \alpha_1 & \delta \end{pmatrix}$$

if we choose a basis $\{e_1, \dots, e_{2n}\}$ of $U \oplus W$ such that $\{e_1, \dots, e_n\}$ is a basis of U and $\{e_{n+1}, \dots, e_{2n}\}$ is a basis of W. Since β is of the form $\alpha + \alpha^t$, δ is of the form $\xi + \xi^t$ and we can choose for α the matrix

$$\alpha = \begin{pmatrix} 0 & 0 \\ \alpha_1 & \xi \end{pmatrix}.$$

If we make a change of basis in $U \oplus W$ given by a bloc matrix $\nu = \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$, we get

$$\alpha' = \begin{pmatrix} 0 & 0 \\ \alpha_1 & \alpha_1 x + \xi \end{pmatrix}$$

for the new matrix. This does not change the basis of U. Since α_1 is invertible, we may choose $x = -\alpha_1^{-1}\xi$. Therefore we can assume that $\xi = 0$ or $\alpha = \left(\begin{smallmatrix} 0 & 0 \\ \alpha_1 & 0 \end{smallmatrix}\right)$. We now replace α by $\left(\begin{smallmatrix} 0 & \alpha_1^t \\ 0 & 0 \end{smallmatrix}\right)$, which differs from α by the alternating matrix $\left(\begin{smallmatrix} 0 & \alpha_1^t \\ -\alpha_1 & 0 \end{smallmatrix}\right)$. We recall that α_1^t is the matrix of $t|_W : W \tilde{\to} U^*$. Thus $\left(\begin{smallmatrix} 1 & 0 \\ 0 & (\alpha_1^t)^{-1} \end{smallmatrix}\right)$ defines an isomorphism $\varphi : U \oplus U^* \tilde{\to} U \oplus W \subset V$. Since

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha_1^{-1} \end{pmatrix} \begin{pmatrix} 0 & \alpha_1^t \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (\alpha_1^t)^{-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

φ is a morphism $H(U) \to V$ of quadratic spaces and $\varphi|_U$ is the identity.

Corollary 7. Let (V, q) be a quadratic space of dimension $2m$. If $U \subset V$ is a totally isotropic subspace of dimension m, then $(V, q) \simeq H(U)$.

Corollary 8. Let (V, q) be a quadratic space and let $e \in V$ be an isotropic element. There exists an isotropic element $f \in V$ such that $b_q(e, f) = 1$. In particular V contains a hyperbolic plane as an orthogonal summand.

A pair $\{e, f\}$ of elements of V is called a *hyperbolic pair* if e, f are isotropic and $b_q(e, f) = 1$.

Let (V, q) be a quadratic form. We say that $x \neq 0 \in V$ is *anisotropic* if $q(x) \neq 0$ and that (V, q) is *anisotropic* if all $x \neq 0 \in V$ are anisotropic.

Corollary 9. Let (V,q) be a quadratic space. There exists a decomposition

$$(V,q) = (V_0, q_0) \perp H(K^n)$$

with (V_0, q_0) anisotropic.

The decomposition is unique up to isometry, in view of the following Witt cancellation theorem and we call n the *Witt index* of (V,q).

Theorem 10 (Witt cancellation).. Let (V_1,q_1), (V_2,q_2) and (V',q') be quadratic spaces such that $(V_1,q_1) \perp (V',q') \simeq (V_2,q_2) \perp (V',q')$. Then $(V_1,q_1) \simeq (V_2,q_2)$.

Before proving Theorem 10, we remark that Witt cancellation does not hold for bilinear spaces in characteristic 2. We have

$$\beta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}^t \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

so that 1_3 and β define isometric bilinear spaces over $\mathbb{F}_2$. But $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ are not isometric.

Proof of Theorem 10. By Corollary 5 and induction, we may assume that we have two orthogonal decompositions

$$(V_1,q_1) \perp H_1 = (V,q) = (V_2,q_2) \perp H_2$$

of a quadratic space (V,q) with H_1, H_2 hyperbolic planes. Let $\{e_1, f_1\}$ be a hyperbolic pair in H_1 and $\{e_2, f_2\}$ a hyperbolic pair in H_2. In view of the next proposition there is an isometry φ of (V,q) such that $\varphi(e_1) = e_2$, $\varphi(f_1) = f_2$. Since $(V_1,q_1) = H_1^\perp$ and $(V_2,q_2) = H_2^\perp$, φ is an isometry $(V_1,q_1) \tilde{\to} (V_2,q_2)$.

Proposition 11. Let (V,q) be a quadratic space and $\{e_1, f_1\}$, $\{e_2, f_2\}$ be hyperbolic pairs in V. There exists an isometry φ of (V,q) such that $\varphi(e_1) = e_2$, $\varphi(f_1) = f_2$.

We give some definitions before proving Proposition 11. We say that two hyperbolic planes H_1, H_2 in (V,q) are *adjacent* if there exists a hyperbolic pair $\{e_1, f_1\}$

in H_1 and a hyperbolic pair $\{e_2, f_2\}$ in H_2 with a common element. We say that H_1 and H_2 are *related* if there is a finite chain of adjacent hyperbolic planes connecting H_1 and H_2.

Lemma 12. Two hyperbolic planes $H_1,\ H_2$ in a quadratic space (V, q) are always related.

Proof. Let $\{e_1, f_1\},\ \{e_2, f_2\}$ be hyperbolic pairs in $H_1,\ H_2$. If one of the 4 elements $b_q(e_1, e_2),\ b_q(e_1, f_2),\ b_q(f_1, e_2),\ b_q(f_1, f_2)$ is not zero, say $b_q(e_1, e_2)$, we replace the pair $\{e_2, f_2\}$ of H_2 by the pair $\{e_3, f_3\}$, $e_3 = e_2 b_q(e_1, e_2)^{-1}$, $f_3 = f_2 b_q(e_1, e_2)$. Then $H_1,\ H_2$ are adjacent to the hyperbolic plane generated by the hyperbolic pair $\{e_1, e_3\}$. If all of the above 4 elements are equal to zero, then $\{e_1,\ f_1 + e_2\},\ \{f_2, f_1 + e_2\}$ are hyperbolic pairs generating hyperbolic planes H_3 and H_4. The chain H_1, H_3, H_4, H_2 shows that H_1 and H_2 are related.

Proof of Proposition 11. In view of Lemma 12, we may assume that $e_1 = e_2$. Let $f = f_2 - f_1$ and let $U = Kf$. If $b_q(f, f_1) \neq 0$, then $V = Kf_1 \oplus U^{\perp}$. The map $\varphi : V \to V$ given by $\varphi(\lambda f_1 + w) = \lambda(f_1 + f_2) + w$ is an isometry such that $\varphi(f_1) = f_2$ and $\varphi(e_1) = e_1$. If $b_q(f, f_1) = 0$, then $q(f) = 0$ and $f \in H_1^{\perp}$. Let $v \in H_1^{\perp}$ such that $\{f, v\}$ is a hyperbolic pair in $H_1^{\perp}$ and let H_3 be the hyperbolic plane generated by $\{f, v\}$. The linear map $u_1 : H_1 \perp H_3 \to H_1 \perp H_3$ given by $e_1 \mapsto e_1,\ f_1 \mapsto f_1 + f,\ f \mapsto f$ and $v \mapsto v - e_1$ has the matrix

$$\nu = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

with respect to the basis $\{v, f, f_1, e_1\}$. Since

$$\nu^t \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \nu = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

we see that u_1 is an isometry of $H_1 \perp H_3$ such that $u_1(e_1) = e_1$ and $u_1(f_1) = f_2$. Since

$$(V, q) \simeq H_1 \perp H_3 \perp (H_1 \perp H_3)^{\perp},$$

u_1 can be extended to an isometry $u = u_1 \perp 1$ with the wanted property.

If the characteristic of K is not equal to 2, there is a much simpler proof of the Witt cancellation theorem. We need the notion of a diagonalizable form. Let $V = K^n$ with the canonical basis $\{e_1, \ldots, e_n\}$ and let $a_1, \ldots, a_n$ be elements of K. We denote by $\langle a_1, \ldots, a_n \rangle$ the quadratic form $q : V \to K$ given by

$$q(e_i) = a_i, \qquad i = 1, \ldots, n, \qquad b_q(e_i, e_j) = 0, \qquad i \neq j.$$

A quadratic form (V', q') is called *diagonalizable* if $(V', q') \simeq \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in K$. Obviously

$$\langle a_1, \ldots, a_n \rangle \simeq \langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle.$$

Lemma 13. If char $K \neq 2$, any quadratic form is diagonalizable.

Proof. This is clear if $q(v) = 0$ for all $v \in V$. Assume that $q(v_1) = a_1 \neq 0$ and let $U = Kv_1$. Since char $K \neq 2$, $(U, q|_U)$ is nonsingular and the claim follows from Lemma 3 and induction on the dimension.

Thus to prove Witt cancellation for quadratic spaces over a field of characteristic not equal to 2, it suffices to show that

$$(V_1, q_1) \perp \langle a \rangle \simeq (V_2, q_2) \perp \langle a \rangle \Rightarrow (V_1, q_1) \simeq (V_2, q_2).$$

This, in turn, is a consequence of

Proposition 14. Let (V, q) be a quadratic space over a field K of characteristic not equal to 2 and let $x,\ y$ be elements of V such that $q(x) = q(y) \neq 0$. There exists an isometry φ of V such that $\varphi(x) = y$.

To prove Proposition 14 we need the notion of a reflection. Let u be an anisotropic element in a quadratic space (V, q) (over any field K). The map $\tau_u : V \to V$ defined by

$$\tau_u(x) = x - \frac{b_q(x, u)}{q(u)}\, u$$

is called a *reflection*. Obviously $\tau_u(u) = -u$ and $\tau_u = 1$ on $(Ku)^\perp$. We let it as an exercise to check that τ_u is an isometry of (V, q) and that $\tau_u^2 = 1$.

Proof of Proposition 14. If $q(x) = q(y)$ we have the equality

$$b_q(x + y,\ x + y) + b_q(x - y,\ x - y) = 4b_q(x, x).$$

So either $x - y$ or $x + y$ is anisotropic. If $x - y$ is anisotropic, then $\tau_{x-y}(x) = y$. If $x + y$ is anisotropic, then $\tau_{x+y}\tau_x(x) = y$.

Corollary 15. $O(V, q)$ is generated by reflections if char $K \neq 2$.

Proof. Since (V, q) is a quadratic space over a field K with char $K \neq 2$, there exists $x \in V$ anisotropic. Let $\varphi \in O(V, q)$ and let $y = \varphi(x)$. By Proposition 14, there exists a product of reflections τ such that $\tau(y) = x$, so $(\tau\varphi)(x) = x$. Let $U = (Kx)^\perp$. We have $V = U \perp Kx$, since x is anisotropic (and char $K \neq 2$!) and $\tau\varphi|_U$ is an isometry of U. By induction on the dimension, $\tau\varphi|_U$ is a product of reflections in U. These reflections can be extended to reflections on V (by taking the identity on x). This proves the claim.

Remark 16. Corollary 15 is a weak form of the theorem of Cartan–Dieudonné. The corollary holds also in characteristic 2, except for $(V, q) = H(\mathbb{F}_2) \perp H(\mathbb{F}_2)$, where the switch of the 2 hyperbolic planes is not a product of reflections. The proof in the general case is quite complicated (see Dieudonné, Sur les groupes classiques).

If the characteristic of K is not equal to 2, any quadratic space is the orthogonal sum of 1–dimensional spaces. In general, we have the weaker (and best possible) result that a quadratic space of even dimension is an orthogonal sum of 2–dimensional subspaces. For $a,\ b \in K$, let $[a, b]$ denote the quadratic form (K^2, q) with

$$q(e_1) = a, \quad q(e_2) = b \quad \text{and} \quad b_q(e_1, e_2) = 1,$$

where $\{e_1, e_2\}$ is the canonical basis of K^2. The form $[a, b]$ is nonsingular if, and only if, $1 - 4ab \neq 0$.

Lemma 17. Any quadratic space (V,q) of even dimension $2m$ is isometric to an orthogonal sum of m spaces $[a_i,b_i]$ with $1-4a_ib_i\neq 0,\ \ i=1,\dots,m$.

Proof. Assume first that char $K=2$. Since (V,q) is nonsingular, there exist $x,\ y\in V$ such that $b_q(x,y)=\lambda\neq 0$. Replacing y by $\frac{1}{\lambda}y$, we have $b_q(x,y)=1$. Let $a_1=q(x),\ \ b_1=q(y)$. Since $d(x,y)=4a_1b_1-1=1$, we see that: (1) $x,\ y$ are linearly independent; (2) the restriction of q to $Kx\oplus Ky$ is nonsingular. The claim then follows by Lemma 3 and induction on the dimension. If char $K\neq 2$, it suffices to show that a 2–dimensional diagonal space $\langle a,b\rangle,\ a\cdot b\neq 0$, is isometric to a space $[a_1,b_1]$ with $1-4a_1b_1\neq 0$. Let $x_1,x_2\in V$ with $q(x_1)=a,\ q(x_2)=b$ and $b_q(x_1,x_2)=0$. Let $x_3=x_2+\frac{1}{2a}\,x_1$. We get

$$b_q(x_1,x_3)=1,\quad q(x_3)=b+\tfrac{1}{4a}\quad\text{and}\quad 1-4a(b+\tfrac{1}{4a})=-4ab\neq 0$$

so that $\langle a,b\rangle\simeq[a,b+\frac{1}{4a}]$.

In characteristic 2 a quadratic space cannot have odd dimension, since the matrix of its polar form is alternating and an $(n\times n)$–alternating matrix has zero determinant if n is odd. To overcome this difficulty (and since there exist interesting forms in odd dimensions also in characteristic 2 !), we introduce the notion of $\frac{1}{2}$–regular forms (see the notes of Kneser). We first define the $\frac{1}{2}$–discriminant. For this we need the following

Lemma 18. Let n be an odd integer and let $a_i,\ 1\leq i\leq n$, and $a_{ij},\ 1\leq i<j\leq n$, be indeterminates. There exists a polynomial $p(a_i,a_{ij})\in\mathbb{Z}[a_i,a_{ij}]$ such that

$$\det\begin{pmatrix}2a_1 & a_{12} & \cdots & a_{1n}\\ a_{12} & 2a_2 & \cdots & a_{2n}\\ \vdots & \vdots & & \vdots\\ a_{1n} & a_{2n} & \cdots & 2a_n\end{pmatrix}=2p(a_i,a_{ij}).$$

Proof. Since n is odd the determinant on the left hand side is zero modulo 2.

For example, we have

$$\det\begin{pmatrix}2a_1 & a_{12} & a_{13}\\ a_{12} & 2a_2 & a_{23}\\ a_{13} & a_{23} & 2a_3\end{pmatrix}=2(4a_1a_2a_3+a_{12}a_{23}a_{13}-a_1a_{23}^2-a_2a_{13}^2-a_3a_{12}^2).$$

Let now (V, q) be a quadratic form over K with $\mathrm{Dim}_K V = n$ odd. Let $\{e_1, \ldots, e_n\}$ be a basis of V and let $a_i = q(e_i)$, $a_{ij} = b_q(e_i, e_j)$, $i < j$. We call the element $p(a_i, a_{ij})$, where p is as in Lemma 18, the $\frac{1}{2}$–*discriminant* of q with respect to the basis $\{e_1, \ldots, e_n\}$ and denote it by $d_0(e_1, \ldots e_n)$. As for the discriminant, the class of $d_0(e_1, \ldots e_n)$ modulo $K^{\bullet 2}$ is independent of the choice of the basis and we denote it by $\frac{1}{2}\mathrm{disc}(q)$. If (V_1, q_1) is of odd dimension and (V_2, q_2) of even dimension, we have

$$\tfrac{1}{2}\mathrm{disc}(q_1 \perp q_1) = \tfrac{1}{2}\mathrm{disc}(q_1) \cdot \mathrm{disc}(q_2).$$

We say that (V, q) is $\frac{1}{2}$–*regular* if $\frac{1}{2}\mathrm{disc}(q) \neq 0$. A 1–dimensional form $\langle a \rangle$ is $\frac{1}{2}$–regular if $a \neq 0$ and $q_1 \perp q_2$ is $\frac{1}{2}$–regular if q_1 is $\frac{1}{2}$–regular of odd dimension and q_2 is nonsingular of even dimension.

We have the following decomposition theorem for $\frac{1}{2}$–regular forms:

Lemma 19. Let (V, q) be $\frac{1}{2}$–regular of dimension $2m + 1$. There exist elements $a_0,\ a_1,\ b_1, \ldots, a_m,\ b_m \in K$ with a_0 and $1 - 4a_ib_i$, $i = 1, \ldots, m$, not zero, such that

$$(V, q) \simeq \langle a_0 \rangle \perp [a_1, b_1] \perp \cdots \perp [a_m, b_m].$$

Proof. If char $K \neq 2$, the claim follows from Lemma 17 and Lemma 13. Assume that char $K = 2$ and that $\mathrm{Dim}_K V \geq 3$. Since (V, q) is $\frac{1}{2}$–regular, b_q is not identically zero and there exists $x_1,\ y_1 \in V$ with $b_q(x_1, y_1) = 1$. Then $x_1,\ y_1$ are linearly independent and q restricted to $Kx_1 \oplus Ky_1$ is nonsingular. The claim now follows by Lemma 3 and induction.

We observe that the notion of $\frac{1}{2}$–regular quadratic forms is also important in the theory of forms over commutative rings R such that $\frac{1}{2} \notin R$ but not necessarily $2 = 0$ in R. A recent application can be found in the paper of Swan mentioned in the bibliography.

Remark 20. The decomposition $(V, q) = \langle a_0 \rangle \perp \langle V', q' \rangle$ with (V', q') nonsingular, given by Lemma 19, is in fact unique in characteristic 2. The 1–dimensional space $\langle a_0 \rangle$ is the radical of q, i.e.

$$\langle a_0 \rangle = \{x \in V \mid b_q(x, y) = 0, \quad \forall y \in V\}$$

and (V', q') is the nonsingular part, i.e. V' is generated by all $x \in V$ with $b_q(x, z) \neq 0$ for some $z \in V$.

Chapter 2

Central Simple Algebras

This chapter presents basic results about finite dimensional algebras. References are the books of Cohn, Herstein, Jacobson (see the bibliography) or any advanced algebra textbook. A reference for this chapter as well as for the next two chapters is the book of Scharlau. Many proofs in this chapter are copied from Scharlau's book.

Let R be a ring. A left or right R–module M is called *simple* if $M \neq 0$ and M has no submodules other than M and 0. The ring R is called *simple* if it has no two–sided ideals other than 0 and R. By Schur's lemma the endomorphism ring $A = \mathrm{End}_R(M)$ of a simple module is a skew field (i.e. a ring such that any non-zero element has an inverse). We define the *centre* $Z(R)$ of a ring as

$$Z(R) = \{x \in R \mid ax = xa, \quad \forall a \in R\}.$$

Obviously R is a $Z(R)$–algebra. For any ring R we denote the ring of all $(n \times n)$–matrices with entries in R by $M_n(R)$. We define the *opposite ring* R^{op} of R as $R^{op} = R$ as additive group while the product in R^{op} is defined as $a^o \cdot b^o = (ba)^o$, where a^o is a viewed as an element of R^{op}.

Lemma 1. Let D be a skew field with centre K. The ring $M_n(D)$ is simple. Its centre is $K \cdot 1_n$, where 1_n is the $(n \times n)$–unit matrix.

Proof. Let E_{ij} be the matrix with entry 1 in place (i,j) and entries zero otherwise. Then $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$, where δ_{jk} is the symbol of Kronecker. If α is a matrix with a non-zero entry a_{ij}, then $a_{ij}^{-1}E_{ki}\alpha E_{jk} = E_{kk}$. Therefore the two–sided ideal generated by α contains the unit matrix $1_n = E_{11} + \cdots + E_{nn}$. This proves that $M_n(D)$ is simple.

If $\alpha = (a_{ij}) \in Z(M_n(D))$, the equation $E_{ij}\alpha = \alpha E_{ij}$ implies that $a_{ii} = a_{jj}$ for all i and j and $a_{ij} = 0$ for all $i \neq j$. Thus $\alpha \in K \cdot 1_n$. This shows that $Z(M_n(D)) = K \cdot 1_n$.

We have the following converse:

Lemma 2. Let K be a field and A a finite dimensional simple K–algebra. There exists a skew field D such that $A \simeq M_n(D)$.

Proof. Let M be a non-zero minimal left ideal of A. Such exist since A is a finite dimensional vector space over K. Then M is a simple A–module and $\mathrm{End}_A(M)$ is a skew field by Schur's lemma. Let $D = \mathrm{End}_A(M)^{op}$. We view M as a right D–module putting $m \cdot d = d^0(m)$. For any $a \in A$, let $\ell_a : M \to M$ be given by left multiplication with a. Since $\ell_a \in \mathrm{End}_D(M)$, we have a ring homomorphism

$$i : A \to \mathrm{End}_D(M), \quad a \mapsto \ell_a,$$

which is injective, since A simple. We check that i is surjective. Let $x,\ y \in M$. The map $\rho_y : x \mapsto xy$ is an element of D, thus $f(xy) = f(x)y$ for $x,\ y \in M$ and $f \in \mathrm{End}_D(M)$. We claim that $i(M)$ is a left ideal in $\mathrm{End}_D(M)$. We have $f \cdot i(x)(y) = f(xy) = f(x)y = i(f(x))(y)$, hence $f \cdot i(x) = i(f(x)) \in i(M)$ for $f \in \mathrm{End}_D(M)$ as claimed. Since A is simple, we have $A = MA$, so $i(A) = i(M)i(A$. Therefore $i(A)$ is a left ideal of $\mathrm{End}_D(M)$. Since $1 \in i(A)$, i is surjective. Finally, we have $\mathrm{End}_D(M) \simeq M_n(D)$ for some n since M is a finite dimensional vector space over D.

Lemma 3. Let D be a skew field and $A = M_n(D)$. Then

1) The ideals L_i of column matrices:

$$L_i = \begin{pmatrix} 0 & * & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & 0 \\ & i - th\ column & & \end{pmatrix}, \qquad i = 1, 2, \ldots n$$

are minimal left ideals of A and $M_n(D) \simeq L_1 \oplus \cdots \oplus L_n$.

2) All simple A–modules, in particular all minimal ideals of A, are isomorphic.

3) Every A–module $M \neq 0$ which is finite dimensional as a D–vector space, is

a direct sum of simple A–modules.

Proof. 1) Let $\alpha = \sum_j E_{ji}a_j \in L_i$ and $a_k \neq 0$, then $(a_k^{-1}E_{kk})\alpha = E_{ki} \in L_i$. Hence the left ideal generated by any non zero element α of L_i is L_i, so L_i is minimal.

2) Obviously all L_i are isomorphic as left A–modules. Let N be a simple A–module. Since $A = \sum_i L_i$ and $AN = N$, there is i such that $L_iN \neq 0$. The map $L_i \to N$, $\alpha \mapsto \alpha x$, is not the zero map for some $x \in N$. Since L_i and N are simple this map is an isomorphism.

3) Let N be a maximal submodule of M such that $N \subset M$ and $N \neq M$ and let $x \in M \backslash N$. Since M/N is simple, $M = N + Ax = N + \sum_i L_i x$. Here $L_i x$ is either 0 or a simple module. There is i such that $L_i x \overset{\subset}{\neq} N$. Since $L_i x$ is simple and N is a maximal submodule of M, $M = N \oplus L_i x$. The claim follows by induction on $\mathrm{Dim}_D M$.

Lemma 4. If $D,\ D'$ are skew fields such that $M_n(D) \simeq M_{n'}(D')$, then $D \simeq D'$ and $n = n'$.

Proof. To show that $D \simeq D'$ it suffices to show that for any simple $M_n(D)$–module N, there exists an isomorphism $D^{op} \simeq \mathrm{End}_{M_n(D)}(N)$. Since two simple $M_n(D)$–modules are isomorphic, we can take for N the column D^n. Since D^n is also a right D–module, we get a map

$$\varphi : D^{op} \to \mathrm{End}_{M_n(D)}(D^n),\quad \varphi(d) = r_d,$$

where r_d is right multiplication with d. Obviously, φ is a ring homomorphism. Since D is a skew field, φ is injective. We let it as an exercise to check that φ is surjective.

The next result follows from Lemma 2 and Lemma 4.

Theorem 5 (Wedderburn). Let A be a finite dimensional simple K–algebra. Then $A \simeq M_n(D)$, for a suitable skew field D. The integer n is uniquely determined by A and D is determined up to an isomorphism.

Let A be a K–algebra. For any subset $B \subset A$, we define the *centralizer* of B

in A to be

$$Z_A(B) = \{a \in A \mid ab = ba, \qquad \forall b \in B\}.$$

In particular $Z_A(A)$ is the centre of A. Obviously $K \subset Z_A(A) = Z(A)$ and we say that A is *central* if $K = Z(A)$. We shall use the abbreviation "*c.s.* algebra" for a finite dimensional central simple K–algebra.

Lemma 6. 1) If A, B are finite dimensional K–algebras and $A' \subset A$, $B' \subset B$ are subalgebras, then $Z_{A\otimes B}(A' \otimes B') = Z_A(A') \otimes Z_B(B')$. In particular we have $Z(A \otimes B) = Z(A) \otimes Z(B)$.

2) If A is a *c.s.* algebra and B is a simple algebra, then $A \otimes B$ is simple.

3) $A \otimes B$ is a *c.s.* algebra if and only if A and B are *c.s.* algebras.

Proof. 1) The inclusion $\supset$ is obvious. Let $\{b_1, \ldots, b_n\}$ be a basis of B and let

$$x = \sum_{i=1}^{n} x_i \otimes b_i \in Z_{A\otimes B}(A' \otimes B').$$

We have

$$(ax_1) \otimes b_1 + \cdots = (x_1 a) \otimes b_1 + \cdots \qquad \text{for all} \quad a \in A'$$

hence $x_i \in Z_A(A')$. Let $\{c_1, \ldots, c_k\}$ be a basis of $Z_A(A')$. Then $x = \sum_{i=1}^k c_i \otimes y_i$, $y_i \in B$. The same argument shows that $y_i \in Z_B(B')$.

2) Let $I \neq 0$ be a two–sided ideal of $A \otimes B$. We have to show that $I = A \otimes B$. Assume first that I contains an element $a \otimes b \neq 0$. We have $AaA = A$, hence there exist $a_i, a_i' \in A$, $1 \le i \le t$, such that $1 = \sum_{i=1}^t a_i a a_i'$. Therefore $\sum_{i=1}^t (a_i \otimes 1)(a \otimes b)(a_i' \otimes 1) = 1 \otimes b$. The same argument applied to b shows that $1 \otimes 1 \in I$. Let now $x = \sum_{i=1}^k a_i \otimes b_i$, $a_i \in A$, $b_i \in B$ be an element of I with k minimal. Suppose that $k > 1$. By the above argument we can assume that $a_k = 1$. By the minimality of k, a_{k-1} and a_k are linearly independent. Since A is central $a_{k-1} \notin Z(A)$. Let $a \in A$ such that $aa_{k-1} - a_{k-1}a \neq 0$ and let y be the element

$$(a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1 a) \otimes b_1 + \cdots + (aa_{k-1} - a_{k-1}a) \otimes b_{k-1}.$$

The b_i are linearly independent by the minimality of k and the last summand is not zero, hence $y \in I$ is not zero and has a smaller k. Therefore $k = 1$ and we are in the case considered above.

3) One direction is an immediate consequence of 1) and 2) and the other is obvious: if A is not central, $A \otimes B$ is not central. If A is not simple, $A \otimes B$ is not simple.

An algebra A is *c.s.* if and only if the opposite algebra A^{op} is *c.s.* We have

Lemma 7. Let A be a *c.s.* algebra. The homomorphism of algebras

$$\varphi : A \otimes A^{op} \to \mathrm{End}_K(A), \quad \varphi(a \otimes b^o)(x) = axb$$

is an isomorphism.

Lemma 7 is an immediate consequence of Lemma 6 and of the following (obvious) result

Lemma 8. Let $\varphi : A \to B$ be a homomorphism of finite dimensional K–algebras. If $\mathrm{Dim}_K A = \mathrm{Dim}_K B$ and A is simple, then φ is an isomorphism.

Let A, B be *c.s.* algebras over K. We say that A and B are *Brauer equivalent* if there exist integers k and ℓ such that

$$A \otimes M_k(K) \simeq B \otimes M_\ell(K).$$

Let $A = M_r(D)$ and $B = M_s(D')$. Then A and B are Brauer equivalent if, and only if, $D \simeq D'$. Let $[A]$ be the equivalence class of A. We get a well-defined multiplication by putting $[A] \cdot [B] = [A \otimes B]$. The multiplication is commutative, associative, has $[K] = [M_n(K)]$ as element 1 and each element has an inverse, since $[A][A^{op}] = 1$. Thus the equivalence classes of *c.s.* algebras form a group. It is called the *Brauer group* of K and is denoted by $Br(K)$.

Example 9. We have $Br(K) = \{1\}$ for any algebraically closed field. In fact, let D be a central division algebra over K, i.e. a skew field D with centre $Z(D) = K$ and which is finite–dimensional over K. If $K \subset D$ and $K \neq D$, let $d \in D \backslash K$. We get a field extension $K \subset K(d) \subset D$ which is finite over K, so d is algebraic over K and $d \in K$. Contradiction.

If $K = \mathbb{R}$, a classical result of Frobenius says that $\mathbb{R}$, $\mathbb{C}$ and the quaternions $\mathbb{H}$

are the only finite dimensional division algebras over $\mathbb{R}$. Since $\mathbb{C}$ is commutative, any *c.s.* algebra over $\mathbb{R}$ is of the form $M_n(D)$ with $D = \mathbb{R}$ or $\mathbb{H}$. Hence $Br(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

If A is a K–algebra and a is a unit of A, i.e. an invertible element, then

$$i_a(x) = axa^{-1}, \quad x \in A,$$

is an automorphism of A. Such automorphisms are called *inner*. We now prove a very useful classical result.

Theorem 10 (Skolem-Noether).. Let A be a *c.s.* algebra over K and B a finite dimensional simple K–algebra. Let $\beta, \gamma : B \to A$ be two algebra homomorphisms. There exists an inner automorphism i_a of A such that $\gamma = i_a \circ \beta$.

Proof. Let first $A = \mathrm{End}_K(V)$, V a vector space over K. We can view V as a left B–module in two different ways, putting $b \cdot v = \beta(b)(v)$ or $b \cdot v = \gamma(b)(v)$. By Lemma 3 these two B–modules are isomorphic so there exists a K–linear isomorphism $f : V \to V$ such that

$$f(\beta(b)(v)) = \gamma(b)f(v) \quad \text{for all} \quad v \in V$$

hence $\gamma(b) = f\beta(b)f^{-1}$. For the general case, we consider the maps

$$\beta \otimes 1, \quad \gamma \otimes 1 : B \otimes A^{op} \to A \otimes A^{op} = \mathrm{End}_K(A).$$

The algebra $B \otimes A^{op}$ is simple by Lemma 6. It then follows from the case $A = \mathrm{End}_K(V)$ that there exists $f \in A \otimes A^{op}$ such that

$$\gamma(b) \otimes a^o = f(\beta(b) \otimes a^o)f^{-1}$$

for all $b \in B$, $a^o \in A^{op}$. Setting $b = 1$, we see that $f \in Z_{A \otimes A^{op}}(1 \otimes A^{op}) = A \otimes 1$ (by Lemma 6). Therefore we get $f = a \otimes 1$. The claim finally is a consequence of $\gamma(b) \otimes 1 = (a \otimes 1)(\beta(b) \otimes 1)(a \otimes 1)^{-1}$.

Corollary 11. Let A be a *c.s.* algebra. Every homomorphism $A \to A$ is an inner automorphism.

Remark 12. Let A be a *c.s.* algebra over K and let S be a finite dimensional commutative K–algebra. We claim that S–automorphisms of $B = S \otimes A$ are inner. This generalization of Corollary 11 will be used later. Let $\mathrm{Rad}(S)$ be the *Jacobson radical* of S i.e. the set of nilpotent elements of S. The quotient $S/\mathrm{Rad}(S)$ is a product of field extensions of K. Let now φ be an automorphism of B and let $\overline{\varphi}$ be the induced automorphism of $\overline{B} = (S/\mathrm{Rad}(S)) \otimes A$. By an obvious generalization of Corollary 11, $\overline{\varphi}$ is inner, $\overline{\varphi} = i_{\overline{v}}$, $\overline{v} \in \overline{B}^{\bullet}$. Let

$$J_\varphi = \{x \in B \mid \varphi(b)x = xb, \qquad \forall b \in B\}.$$

The automorphism φ is inner if, and only if, there exists $u \in J_\varphi$ which is a unit of B. We get

$$\begin{aligned} \overline{J}_\varphi &= (S/\mathrm{Rad}(S)) \otimes J_\varphi = J_{\overline{\varphi}} \\ &= \{\overline{x} \in \overline{B} \mid \overline{\varphi}(\overline{b})\overline{x} = \overline{x}\overline{b}, \qquad \forall \overline{b} \in \overline{B}\} \end{aligned}$$

and

$$J_{\overline{\varphi}} = \overline{S}\overline{v} \qquad \text{since} \qquad \overline{\varphi} = i_{\overline{v}}.$$

Let $v \in B$ be such that its image in $\overline{B}$ is $\overline{v}$. By Nakayama's Lemma (see any of the algebra textbooks in the bibliography or Scharlau's book), v is a unit of B and $J_\varphi = Sv$. This shows the claim.

Corollary 13. Let A, B, C be *c.s.* algebras. Then $A \otimes B \simeq A \otimes C$ implies that $B \simeq C$.

Proof. Let $E = A \otimes C$ and let α be an isomorphism $A \otimes B \tilde{\to} A \otimes C$. We have

$$C = \{x \in E \mid x(a \otimes 1) = (a \otimes 1)x, \qquad \forall a \in A\} = Z_E(A \otimes 1)$$

$$\alpha(B) = \{y \in E \mid y\alpha(a \otimes 1) = \alpha(a \otimes 1)y, \qquad \forall a \in A\} = Z_E(\alpha(A \otimes 1)).$$

Let now $\psi : A \to E$ be given by $\psi(a) = a \otimes 1$ and $\varphi : A \to E$ by $\varphi(a) = \alpha(a \otimes 1)$. By Theorem 10 there exists $u \in E$ such that $\psi = i_u \circ \varphi$. It follows that i_u induces an isomorphism $\alpha(B) \tilde{\to} C$.

Lemma 14. 1) Let $K \subset L$ be a field extension and let A be a K–algebra. Then A is a *c.s.* K–algebra if and only if $L \otimes A$ is a *c.s.* L–algebra. In particular $K \subset L$

induces a group homomorphism $Br(K) \to Br(L)$.

2) Let A be a *c.s.* K–algebra. There exists a finite field extension $K \subset L$ such that $L \otimes A \simeq M_n(L)$. In particular $\mathrm{Dim}_K A$ is always a square.

Proof. 1) follows from Lemma 6 (at least one direction of 1) !).

2) Let $\overline{K}$ be the algebraic closure of K. By Example 9, we get that $\overline{K} \otimes A \simeq M_n(\overline{K})$. Let α be such an isomorphism. Let $\{x_1, \ldots x_r\}$ be a basis of A over K, then

$$\alpha(1 \otimes x_\ell) = \sum_{i,j} \lambda_{ij\ell} E_{ij}, \quad \lambda_{ij\ell} \in \overline{K},$$

where $\{E_{ij} \mid 1 \leq i,\ j \leq n\}$, is the canonical basis of $M_n(K)$. Let L be the subfield of $\overline{K}$ generated by K and the $\lambda_{ij\ell}$. Since the $\lambda_{ij\ell}$ are algebraic over K, L is a finite extension of K and α can be viewed as an isomorphism $L \otimes A \tilde{\to} M_n(L)$.

We call a pair (L, α), $\alpha : L \otimes A \tilde{\to} M_n(L)$, a *splitting* of A. The following result is a nontrivial sharpening of Lemma 14. We refer to any of the books mentioned at the beginning of this chapter for a proof (for example Herstein or Scharlau).

Theorem 15. For any *c.s.* K–algebra A, there exists a splitting (L, α) with $K \subset L$ a finite Galois extension.

We now use the existence of Galois splittings to construct the characteristic polynomial of a *c.s.* algebra. Let (L, α) be a Galois splitting of A. If $L[X]$ is the polynomial ring in one variable X over L, we extend K–automorphisms of L to $K[X]$-automorphisms of $L[X]$ by putting $g(X) = X$ for all $g \in G = \mathrm{Gal}(L/K)$. As for fields, we have

$$K[X] = \{p(X) \in L[X] \mid g(p(X)) = p(X), \quad \forall g \in G\}.$$

Further, we can extend the isomorphism $\alpha : L \otimes A \tilde{\to} M_n(L)$ to an isomorphism

$$\alpha : L[X] \otimes A \tilde{\to} M_n(L[X])$$

by putting $\alpha(X \otimes 1) = X \cdot 1_n$. For $a \in A$, we define the *reduced characteristic polynomial* of a by

$$\chi(X, a) = \det(\alpha(X \otimes 1 - 1 \otimes a)).$$

Let $\chi(X, a) = X^n + \lambda_{n-1}X^{n-1} + \cdots + \lambda_0$. The coefficient $(-1)^n\lambda_0$ is called the *reduced norm* of a. We denote it by $n(a)$ or $n_A(a)$. The coefficient $-\lambda_{n-1}$ is the *reduced trace* and it is denoted by $tr(a)$ or $tr_A(a)$.

Lemma 16. The polynomial $\chi(X, a)$ is independent of the choice of the Galois splitting (L, α) and has coefficients in K. In particular $n(a) \in K$ and $tr(a) \in K$ for $a \in A$.

Proof. Let $\alpha : L \otimes A \tilde{\to} M_n(L)$ and $\alpha' : L' \otimes A \tilde{\to} M_n(L')$ be two Galois splittings. Replacing L and L' by a Galois extension L'' which contains L and L', we see that we may assume $L = L'$. In view of Corollary 11, we have $\alpha' = i_u \circ \alpha$ for some $u \in GL_n(L)$ so that

$$\begin{aligned} \det(\alpha'(X \otimes 1 - 1 \otimes a)) &= \det(u(\alpha(X \otimes 1 - 1 \otimes a))u^{-1}) \\ &= \det(\alpha(X \otimes 1 - 1 \otimes a)). \end{aligned}$$

We finally show that $\chi(X, a) \in K[X]$. For any $g \in \mathrm{Gal}(L/K)$, let $\overline{g}$ be the K–automorphism of $M_n(L[X])$ given by

$$\overline{g}(a_{ij}) = (g(a_{ij})).$$

The automorphism $\alpha(g \otimes 1)\alpha^{-1}\overline{g}^{-1}$ of $M_n(L[X])$ is L–linear, hence there is $u \in GL_n(L)$ such that $\alpha(g \otimes 1)\alpha^{-1}\overline{g}^{-1} = i_u$. Then we get

$$\alpha(1 \otimes a) = u\overline{g}(\alpha(1 \otimes a))u^{-1}.$$

Since $\det(\overline{g}(a_{ij})) = g(\det(a_{ij}))$, it follows that $\chi(X, a) = g(\chi(X, a))$ for all $g \in G$. Therefore $\chi(X, a) \in K[X]$, as claimed.

The reduced norm and trace satisfy the following formulas

$$\begin{array}{rl} n(ab) = n(a)n(b) & tr(a+b) = tr(a) + tr(b) \\ n(\lambda a) = \lambda^n n(a) & tr(\lambda a) = \lambda tr(a) \\ & tr(ab) = tr(ba) \end{array}$$

for a, $b \in A$ and $\lambda \in K$. Further $a \in A$ is invertible if and only if $n(a) \neq 0$. These properties follow from the corresponding properties of the determinant and the trace for matrices. Further $\chi(a, a) = 0$ for all $a \in A$, i.e. the Cayley–Hamilton theorem holds for the characteristic polynomial.

Chapter 3

Involutions on Central Simple Algebras

Let R be a ring. As already mentioned in Chapter 1, Remark 1, an *involution* on R is a map $\sigma : x \mapsto \overline{x}$ of R to itself such that

$$1)\quad \overline{a+b} = \overline{a} + \overline{b} \qquad 2)\quad \overline{ab} = \overline{b}\,\overline{a}, \qquad 3)\quad \overline{\overline{a}} = a.$$

for all $a,\ b \in R$. A homomorphism $\varphi : (R, \sigma) \to (R', \sigma')$ of rings-with-involution is a homomorphism $\varphi : R \to R'$ such that $\varphi \circ \sigma = \sigma' \circ \varphi$.

Let now A be a K–algebra, K a field. If σ is an involution of A, the restriction of σ to K is an involution σ_0 of K. If σ_0 is the identity, we say that σ is an *involution of the first kind.* Hence involutions of the first kind are K–linear. If σ_0 is not the identity, let K_0 be the fixed field of σ_0, $K_0 = \{x \in K \mid \sigma_0(x) = x\}$. The extension $K_0 \subset K$ is a quadratic Galois extension with Galois group $\mathrm{Gal}(K/K_0) = \{1, \sigma_0\} \simeq \mathbb{Z}/2\mathbb{Z}$. If this case occurs we say that σ is an *involution of the second kind.*

We now study involutions of the first kind on *c.s.* algebras and begin with the algebra $A = M_n(K)$. For any matrix x, the map $x \mapsto x^t$ is an involution of $M_n(K)$ of the first kind. If σ is another such involution, the map $x \mapsto \sigma(x^t)$ is an automorphism of $M_n(K)$. Therefore, by the Skolem–Noether theorem, there is $u \in GL_n(K)$ such that

$$\sigma(x^t) = uxu^{-1} \quad \text{or} \quad \sigma(x) = ux^tu^{-1}, \quad x \in M_n(K).$$

The fact that $\sigma^2 = 1$ implies $u^t = \varepsilon u$, where $\varepsilon = \pm 1$. We denote the involution $x \mapsto ux^tu^{-1}$ by σ_u and call ε the *type* of σ_u. This is well defined, since $\sigma_u = \sigma_v$ implies $u = \lambda v$ for $0 \neq \lambda \in K$. Involutions of type 1 are usually called of *orthogonal type* and involutions of type – 1 of *symplectic type.* If char $K = 2$ there are no differences between the two types. In this case it is useful to consider a more special class of involutions. We say that σ_u is of *even* ε*−type* if u is of the fom $v + \varepsilon v^t$. In particular σ_u is of *even symplectic* type if u is an alternating matrix

$$u = \begin{pmatrix} 0 & u_{12} & \dots & u_{1n} \\ -u_{12} & 0 & & \\ \vdots & & \ddots & \\ -u_{1n} & & & 0 \end{pmatrix},$$

not just a skew–symmetric matrix. We observe that involutions of even symplectic type can only occur if n is even. This is clear if $\mathrm{char} K \neq 2$. If $\mathrm{char} K = 2$, an alternating matrix is the matrix of the polar of a quadratic form. Its determinant is a multiple of 2 if n is odd (Lemma 18 of Chapter 1) hence is zero in characteristic 2. Thus an $(n \times n)$–alternating matrix, n odd, is never invertible. Let

$$\mathrm{Alt}_n(K) = \{y \in M_n(K) \mid y \quad \text{is alternating}\} = \{x - x^t \mid x \in M_n(K)\}.$$

The vector space $\mathrm{Alt}_n(K)$ is of dimension $\frac{n(n-1)}{2}$ over K. Let now $\sigma = \sigma_u$ be an involution of $M_n(K)$ of type ε. We call

$$\mathrm{Alt}_n^\sigma(K) = \{x - \varepsilon\sigma(x) \mid x \in M_n(K)\}.$$

the space of *alternating elements* of σ. We have for $y \in \mathrm{Alt}_n^\sigma(K)$,

$$\begin{aligned} y &= x - \varepsilon\sigma(x) = x - \varepsilon u x^t u^{-1} = (xu - \varepsilon u x^t)u^{-1} \\ &= (xu - (xu)^t)u^{-1} \end{aligned}$$

and similarly $y = u(u^{-1}x - (u^{-1}x)^t)$. Thus

Lemma 1. We have $\mathrm{Alt}_n^\sigma(K) = \mathrm{Alt}_n(K) \cdot u^{-1} = u \cdot \mathrm{Alt}_n(K)$ if $\sigma = \sigma_u$. In particular $\mathrm{Dim}_K \mathrm{Alt}_n^\sigma(K) = \frac{n(n-1)}{2}$.

Let σ_u, σ_v be two involutions on $M_n(K)$ and let

$$\varphi : (M_n(K), \sigma_u) \tilde{\to} (M_n(K), \sigma_v)$$

be an isomorphism of K–algebras–with–involution. By Corollary 11 of Chapter 2, $\varphi = i_c$, $c \in GL_n(K)$, and $c\sigma_u(x)c^{-1} = \sigma_v(cxc^{-1})$ for $x \in M_n(K)$. A computation shows that $v^{-1}cuc^t$ is in the centre of $M_n(K)$. Hence there exists $\lambda \in K^\bullet$ such that

$$\lambda v = cuc^t.$$

In particular the type of the involution σ_u is an invariant of the isomorphism class of $(M_n(K),\sigma_u)$. Another consequence is the following

Lemma 2. Let s_m be the $2m$–alternating matrix with m blocs $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$ on the diagonal and let v be any invertible alternating matrix. There exists $c \in GL_{2m}(K)$ such that $v = cs_mc^t$. In particular $(M_{2m}(K),\sigma_v) \simeq (M_{2m}(K),\sigma_{s_m})$.

Proof. Let $V = K^{2m}$ and let $b : V \times V \to K$ be the alternating bilinear form defined by $b(\xi,\eta) = \xi^t v\eta$, $\xi = (x_1,\dots,x_{2m})^t$ and $\eta = (y_1,\dots,y_{2m})^t$. Since v is invertible, there exist $\xi_1,\ \xi_2 \in V$ such that $b(\xi_1,\xi_2) \neq 0$ and we can even assume that $b(\xi_1,\xi_2) = 1$. The two vectors ξ_1 and ξ_2 are linearly independent. Let now

$$V_1 = K\xi_1 \oplus K\xi_2 \quad \text{and} \quad V_2 = \{\xi \in V \mid b(\xi_i,\xi) = 0, \quad i = 1,2\}.$$

We have $V = V_1 \oplus V_2$. Let $\{\xi_3,\dots,\xi_{2m}\}$ be a basis of V_2 and let $d = (d_{ij})$ be the matrix of the change of basis, i.e., $\xi_j = \sum d_{ij}e_i$, where $\{e_1,\dots,e_{2m}\}$ is the canonical basis of K^{2m}. Putting $v' = (b(\xi_i,\xi_j))$, we have

$$v' = \begin{pmatrix} s_1 & 0 \\ 0 & v'' \end{pmatrix} \quad \text{and} \quad v' = d^t v d.$$

The matrix v'' is alternating and the claim then follows by induction on the dimension of V.

We now discuss involutions of the first kind on *c.s.* algebras. Let A be such an algebra, with involution $\sigma : a \mapsto \overline{a}$, and let (L,α) be a splitting of A. Then $\alpha(1\otimes\sigma)\alpha^{-1}$ is an involution of $M_n(L)$, hence of the form σ_u, $u \in GL_n(L)$. Let ε be the type of σ_u. Using that ε depends only on the isomorphism class of $(M_n(L),\sigma_u)$ it is easy to check that ε is independent of the choice of the splitting (L,α). We call ε the *type* of the involution σ. Again, ε depends only on the isomorphism class of (A,σ). In the next Lemma we collect some results whose proofs are straightforward.

Lemma 3. Let $A_1,\ A_2$ be K–algebras with involutions σ_1(resp. σ_2).

1) Then $\sigma_1 \otimes \sigma_2$ is an involution of $A_1 \otimes A_2$ of the first kind if σ_1,σ_2 are of the first kind and of second kind if σ_1,σ_2 are of the second kind.

2) If σ_1 has type ε_1 and σ_2 type ε_2, then $\sigma_1 \otimes \sigma_2$ has type $\varepsilon_1\varepsilon_2$.

3) If u is a unit of A_1 such that $\sigma_1(u) = \eta u,\ \eta = \pm 1$ and if σ_1 is of type ε_1, then $i_u \circ \sigma_1$ is an involution of type $\varepsilon_1 \eta$. Conversely if $i_u \circ \sigma_1$ is an involution for some unit u of A_1, then $\sigma_1(u) = \pm u$.

Let A be a $c.s.$ algebra of dimension n^2 with an involution σ of type ε. We call the set

$$\mathrm{Alt}^\sigma(A) = \{x - \varepsilon\, \sigma(x) \mid x \in A\}$$

the set of *alternating elements* of A. Let $\alpha : L \otimes A \tilde{\to} M_n(L)$ be a splitting of A such that $\alpha(1 \otimes \sigma)\alpha^{-1} = \sigma_u$. By Lemma 1, we have $\alpha(\mathrm{Alt}^\sigma(A)) = u \cdot \mathrm{Alt}_n(L)$, thus $\mathrm{Alt}^\sigma(A)$ is a vector space of dimension $\frac{n(n-1)}{2}$ over K.

We say that σ is of *even ε–type* if there is a splitting (L, α) such that $\alpha(1 \otimes \sigma)\alpha^{-1} = \sigma_u$ with $u = v + \varepsilon v^t \in GL_n(L)$. This definition is in fact independent of the splitting. If (L', α') is another splitting, we may assume that $L' = L$ and $\alpha' = i_c \circ \alpha$, for some $c \in GL_n(L)$. If $\alpha'(1 \otimes \sigma)\alpha'^{-1} = \sigma_{u'}$, with $u' \in GL_n(L)$, we have $i_c \circ \sigma_u \circ i_c^{-1} = \sigma_{u'}$, hence $\lambda u' = cuc^t$ for some unit λ of L. We have $\lambda u' = v' + \varepsilon v'^t$, where $v' = cvc^t$. If $\varepsilon = -1$, we say that the involution is of *even symplectic type* and if $\varepsilon = 1$, we say that the involution is of *even orthogonal type*. In fact, if the involution is of even symplectic type, by Lemma 2, we can even choose the splitting (L, α) such that $\alpha(1 \otimes \sigma)\alpha^{-1} = \sigma_{s_m}$ with $s_m = \mathrm{diag}((\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}), \ldots, (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}))$, where $4m^2 = \mathrm{Dim}_K A$. We further observe that $1 \in \mathrm{Alt}^\sigma(A)$ if σ is of even symplectic type. Going over to a splitting of A as above, it suffices to remark that $s_m^{-1} \cdot 1 \in \mathrm{Alt}_{2m}(K)$.

In the following examples, we now discuss two important classes of K–algebras with K–linear involutions, the quadratic algebras and the central simple algebras of dimension 4.

Example 4. Quadratic Algebras. We say that a K–algebra S is *quadratic* if $\mathrm{Dim}_K S = 2$. Let $\{1, v\}$ be a basis of S. We have

$$v^2 = av + b$$

for some $a,\ b \in K$. Hence

$$S \simeq K[X]/(X^2 - aX - b).$$

It follows, in particular, that a quadratic algebra is always commutative. We define a K–linear map $\sigma : x \mapsto \overline{x}$ of S by

$$\overline{\lambda v + \mu} = \lambda \overline{v} + \mu \quad \text{and} \quad \overline{v} = a - v.$$

It is easy to check that $\overline{v}^2 = \overline{v^2}$, so σ is an involution of S. we have

$$\lambda v + \mu + \overline{\lambda v + \mu} = \lambda a + 2\mu,$$

and

$$\begin{aligned}(\lambda v + \mu)(\overline{\lambda v + \mu}) &= \lambda^2 v\overline{v} + \lambda\mu(v + \overline{v}) + \mu^2 \\ &= -b\lambda^2 + a\lambda\mu + \mu^2.\end{aligned}$$

Therefore $x + \overline{x} \in K$ and $x\overline{x} \in K$ for all $x \in S$. By the following Lemma 6, there exists exactly one involution σ of S with

$$x + \sigma(x) \in K \quad \text{and} \quad x\sigma(x) \in K \quad \text{for all} \quad x \in S.$$

We call it the *standard involution* of S. We denote $x + \overline{x}$ by $tr(x)$ or $tr_S(x)$ and $x\overline{x}$ by $n(x)$ or $n_S(x)$. The map $n : S \to K$ is a quadratic form and its polar form

$$b_n(x, y) = n(x + y) - n(x) - n(y)$$

has the matrix

$$\begin{pmatrix} 2 & a \\ a & -2b \end{pmatrix}$$

with respect to the basis $\{1, v\}$ of S. We say that S is a *separable* quadratic K–algebra if n is nonsingular. If $K \subset L$ is a field extension, then S is separable quadratic over K if and only if $L \otimes S$ is separable quadratic over L. Since

$$-\det \begin{pmatrix} 2 & a \\ a & -2b \end{pmatrix} = a^2 + 4b$$

is the discriminant of the polynomial $X^2 - aX - b$, S is a separable quadratic K–algebra if and only if $S \simeq K[X]/p(X)$ for some separable quadratic polynomial $p(X)$. Let now S be separable quadratic. Since

$$n(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = n(x)n(y),$$

S is a field if and only if n is anisotropic. If n is isotropic, it follows from Corollary 8 of Chapter 1 that the quadratic space (S, n) is isometric to $H(K)$. Thus there exists $e,\ f \in S$ such that $e\overline{e} = 0,\ \ f\overline{f} = 0$ and $e\overline{f} + f\overline{e} = 1$. It follows from $x + \overline{x} = tr(x) \in K$ and $x\overline{x} = n(x) \in K$ that

$$x^2 - tr(x)x + n(x) = 0, \quad x \in S.$$

Let now $1 = \lambda e + \mu f,\ \lambda,\ \mu \in K$. We have also $1 = \lambda\overline{e} + \mu\overline{f}$, hence $e = \mu\overline{f}e,\ f = \lambda\overline{e}f$ and $ef = 0$. It follows that $e = \lambda e^2$. Since $e^2 - tr(e)e + n(e) = 0$, we get $e + \overline{e} = \frac{1}{\lambda}$ and $\mu f = \lambda\overline{e}$. Similarly, we have $f = \mu f^2$. Now $1 = \overline{e}f + \overline{f}e = \frac{\mu}{\lambda}f^2 + \frac{\lambda}{\mu}e^2 = \frac{1}{\lambda}f + \frac{1}{\mu}e$, so $\lambda\mu = 1,\ \lambda = e + \mu^2 f = e + f = \mu$ and $\lambda^2 = \mu^2 = 1$. Finally we get

$$1 = \lambda^2 e^2 + \mu^2 f^2 = e^2 + f^2, \quad e^2 f^2 = 0$$

and $\{e^2,\ f^2\}$ is a pair of orthogonal idempotents in S. Therefore

$$S \simeq K \times K \qquad \text{with the involution} \qquad (\lambda, \mu) \longmapsto (\mu, \lambda).$$

To summarize, we have shown that a separable quadratic K–algebra S is either a quadratic field extension of K or is isomorphic to $K \times K$. The first case occurs if the norm of S is anisotropic and the second if the norm is isotropic. Finally we observe that for any separable quadratic K–algebra S, $S \otimes S \simeq S \times S$. An explicit isomorphism is given by $x \otimes y \mapsto (xy, x\overline{y}), x, y \in S$.

Example 5. Quaternion Algebras. We define a *quaternion algebra* over a field K to be a *c.s.* K–algebra A of dimension 4. In view of Theorem 5 of Chapter 2, A is either a central division algebra over K or $A \simeq M_2(K)$. The reduced norm is a quadratic form on A, the trace is a linear form on A and the characteristic polynomial reduces to

$$\chi(X, a) = X^2 - tr(a)X + n(a).$$

If $A = M_2(K)$, the reduced norm is the determinant. Its polar $b_{\det}$ has the matrix

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

with respect to the basis $e_1 = E_{12}, e_2 = E_{21}, e_3 = E_{11}$ and $e_4 = E_{22}$. Therefore det is a nonsingular quadratic form on $M_2(K)$. The subspace $U = \left(\begin{smallmatrix} K & 0 \\ K & 0 \end{smallmatrix}\right)$ of $M_2(K)$ is totally isotropic. Thus we get by Corollary 7 of Chapter 1 (or by a direct computation

!) an isometry of quadratic spaces

$$(M_2(K), \det) \simeq H(U) \simeq H(K) \perp H(K) = H(K^2).$$

For any matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(K)$, let $\overline{\alpha} = tr(\alpha) - \alpha$. We have

$$\overline{\alpha} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{-1}.$$

Thus $\alpha \mapsto \overline{\alpha}$ is an involution of even symplectic type of $M_2(K)$ such that

$$\alpha + \overline{\alpha} = tr(\alpha) \in K \quad \text{and} \quad \alpha\overline{\alpha} = \overline{\alpha}\alpha = \det(\alpha) \in K$$

for all $\alpha \in M_2(K)$. By the following Lemma 6, $\alpha \mapsto \overline{\alpha}$ is the unique involution σ of $M_2(K)$ with the property that $\alpha + \sigma(\alpha) \in K$ and $\alpha\sigma(\alpha) \in K$ for all $\alpha \in M_2(K)$. Let now A be any *c.s.* K–algebra of dimension 4 and let $\sigma : A \to A$ be defined by

$$\sigma(a) = \overline{a} = tr_A(a) - a.$$

Let $\alpha : L \otimes A \tilde{\to} M_2(L)$ be a splitting of A. Since $tr_A(a)$ is the trace of the matrix $\alpha(1 \otimes a)$, the map $\alpha(1 \otimes \sigma)\alpha^{-1}$ is the involution defined above for $A = M_2(K)$. Therefore σ is an involution of even symplectic type. We call σ the *standard involution* of A. We have $n_A(a) = a\sigma(a) = \sigma(a)a$ since it holds over a splitting and σ is the unique involution of A such that

$$a + \sigma(a) \in K \quad \text{and} \quad a\sigma(a) \in K \quad \text{for all} \quad a \in A.$$

Let $\varphi : A \tilde{\to} B$ be an isomorphism of *c.s.* algebras of dimension 4 and let $\sigma' = \varphi\sigma_A\varphi^{-1}$ where σ_A is the standard involution of A. The map σ' is an involution of B such that $x + \sigma'(x) \in K$ and $x\sigma'(x) \in K$ for all $x \in B$. Hence $\sigma' = \sigma_B$ and φ is automatically an isomorphism $(A, \sigma_A) \tilde{\to} (B, \sigma_B)$ of algebras–with–involutions. It follows that φ induces an isometry $(A, n_A) \tilde{\to} (B, n_B)$ of the reduced norms. In particular, a splitting of A, $\alpha : L \otimes A \tilde{\to} M_2(L)$ induces an isometry

$$L \otimes (A, n_A) = (L \otimes A, n_{L \otimes A}) \tilde{\to} (M_2(L), \det).$$

Since $(M_2(L), \det)$ is nonsingular over L, (A, n_A) is nonsingular. We have $n_A(xy) = n_A(x)n_A(y)$ for $x,\ y \in A$ and $n_A(1) = 1$. Thus A is a division algebra if and only if n_A is anisotropic. Since either A is a division algebra or $A = M_2(K)$, we see that n_A is isotropic if, and only if, $A = M_2(K)$.

Let A be a K–algebra. We say that a K–linear involution σ on A is a *standard involution* if

$$a + \sigma(a) \in K \quad \text{and} \quad a\sigma(a) \in K \quad \text{for all} \quad a \in A.$$

(In fact it suffices to assume that $a\sigma(a) \in K$ for all $a \in A$, since $(a+1)\sigma(a+1) = a\sigma(a) + a + \sigma(a) + 1$ if A has an element 1).

Lemma 6. A K–algebra A can carry at most one standard involution.

Proof. Let $a\sigma(a) = n(a)$ and $a + \sigma(a) = tr(a)$. We have

$$a^2 - tr(a)a + n(a) = 0$$

in A for any standard involution σ. Let now σ_1, σ_2 be standard involutions on A and let $tr_i(a) = a + \sigma_i(a)$, $n_i(a) = a\sigma_i(a)$. Let $\{e_1, \ldots, e_n\}$ be a basis of A with $e_1 = 1$. Since

$$e_i^2 - tr_1(e_i)e_i + n_1(e_i)e_1 = e_i^2 - tr_2(e_i)e_i + n_2(e_i)e_1$$

we get $tr_1(e_i) = tr_2(e_i)$ for $i \geq 2$, hence $\sigma_1(e_i) = \sigma_2(e_i)$ for $i \geq 2$. On the other hand, $\sigma_1(1) = 1 = \sigma_2(1)$, thus, as claimed $\sigma_1 = \sigma_2$.

The existence of standard involutions is related with the existence of composition algebras. Let A be a finite dimensional K–vector space with a bilinear multiplication $(a, b) \mapsto ab$ which has a neutral element 1, i.e. $a \cdot 1 = a = 1 \cdot a$. In the following, we call A an algebra even if the multiplication is not associative. We say that A is a *composition algebra* if there exists a nonsingular quadratic form n on A such that $n(ab) = n(a)n(b)$ for all $a,\ b \in A$. An associative K–algebra with 1, which carries a standard involution σ, is a composition algebra for the quadratic form $n(a) = a\sigma(a)$, since

$$n(ab) = ab\sigma(ab) = ab\sigma(b)\sigma(a) = a\sigma(a)b\sigma(b) = n(a)n(b).$$

The following result, which is due to Hurwitz in characteristic not 2, describes all possible composition algebras. It implies that separable quadratic algebras and *c.s.* algebras of dimension 4 are the only examples of associative algebras with a standard involution such that the corresponding norm is nonsingular.

Theorem 7. Let (A, n) be a composition algebra over K. Then either

1) $A = K$,
2) A is a separable quadratic K–algebra and $n = n_A$,
3) A is a *c.s.* K–algebra of dimension 4 and $n = n_A$,
4) A is a separable Cayley algebra. In particular $\mathrm{Dim}_K A = 8$.

Proof. We give the proof of van der Blij and Springer, which works also in characteristic 2. Let (x, y) be the polar of n, i.e. $(x, y) = n(x + y) - n(x) - n(y)$. Since by assumption n is nonsingular,

$$(x, y) = 0, \ \ \forall y \in A \qquad \Rightarrow x = 0.$$

The following formulas are deduced from $n(xy) = n(x)n(y)$ by linearization:

$$\begin{aligned} (xy_1, xy_2) &= n(x)(y_1, y_2) \\ (x_1y, x_2y) &= n(y)(x_1, x_2) \\ (x_1y_2, x_2y_1) + (x_1y_1, x_2y_2) &= (x_1, x_2)(y_1, y_2). \end{aligned} \tag{3.1}$$

We must have $n(1) = 1$. Putting $x_1 = y_2 = x$, $x_2 = z$ and $y_1 = 1$ in the third formula of (3.1), we obtain

$$(x^2 - (1, x)x + n(x) \cdot 1, z) = 0$$

for all $z \in A$. Since n is nonsingular we get

$$x^2 - (1, x)x + n(x) \cdot 1 = 0 \tag{3.2}$$

for all $x \in A$. We call $(1, x)$ the trace of x and denote it by $tr(x)$. Let $\overline{x} = tr(x) - x$. It is straightforward to check that

$$\overline{xy} = \overline{y}\,\overline{x}, \ \ \overline{\overline{x}} = x \ \text{ and } \ \overline{1} = 1.$$

Hence $x \mapsto \overline{x}$ is an involution on A. Further

$$x\overline{x} = \overline{x}x = n(x), \ \ n(x) = n(\overline{x}), \ \ (xy, z) = (y, \overline{x}z) = (x, z\overline{y}). \tag{3.3}$$

We also need the formulas

$$x(\overline{x}y) = n(x)y \qquad \text{and} \qquad (yx)\overline{x} = n(x)y. \tag{3.4}$$

For the proof of the first one, we have

$$(x(\overline{x}y), z) = (\overline{x}y, \overline{x}z) = (n(x)y, z) \quad \text{for all} \quad z \in A.$$

The proof of the other one is similar. It follows from (3.4) that $x(\overline{x}y) = (x\overline{x})y$. Therefore

$$x(xy) = x(tr(x)y - \overline{x}y) = (xtr(x) - x\overline{x})y = (xx)y$$

and similarly $(yx)x = y(xx)$. This shows that A is an *alternative algebra.* Assume now that $\mathrm{Dim}_K(A) > 1$. Since n is nonsingular, it is easy to check that there exists $u \in A$ such that the set $\{1, u\}$ is linearly independent in A and such that the restriction of n to $B_1 = K1 \oplus Ku$ is nonsingular. By (3.2), B_1 is a separable quadratic K–algebra. We have $A = B_1 \perp B_1^\perp$. If $B_1^\perp \neq 0$, the restriction of n to $B_1^\perp$ is nonsingular and there exists $v \in B_1^\perp$ such that $n(v) \neq 0$. We put $n(v) = -\lambda$, $\lambda \in K$. To conclude we use the following:

Lemma 8. Let B be a proper subalgebra of A such that the restriction of n to B is nonsingular and let $v \in B^\perp$ be such that $n(v) = -\lambda$ is not zero. Then $B \oplus vB$ is a subalgebra of A. We have

$$n(a + vb) = n(a) - \lambda n(b) \qquad \text{and} \qquad \overline{a + vb} = \overline{a} - vb$$

for $a,\ b \in B$. Further B is associative and B is commutative if A is associative.

Proof. The fact that $B \oplus vB$ is a subalgebra follows from the formulas

$$\begin{aligned} (va)b &= v(ba) \\ a(vb) &= v(\overline{a}b) \\ (va)(vb) &= -b\overline{a}\, n(v) = \lambda b\overline{a} \end{aligned} \tag{3.5}$$

for $a,\ b \in B$. We only check the first one. The proof of the others is similar. We have $\overline{v} = -v$, since $(v, 1) = 0$, and $0 = (v, a) = \overline{v}a + \overline{a}v = -va + \overline{a}v$, thus $va = \overline{a}v$ for $a \in B$. Further

$$((vb)a, z) = (vb, z\overline{a}) = (\overline{b}v, z\overline{a}) = -(\overline{b}\overline{a}, zv).$$

The last equality follows from the third formula of (3.3), using that $(v, \overline{a}) = 0$ for $a \in B$. On the other hand

$$-(\overline{b}\overline{a}, zv) = -((\overline{b}\overline{a})\overline{v}, z) = (v(ab), z).$$

This holds for all $z \in A$, hence $(vb)a = v(ab)$ as claimed. The formulas for n and the involution are easy. Let now

$$\begin{aligned} n((a+vb)(c+vd)) &= n(ac+\lambda d\overline{b}+v(cb+\overline{a}d)) \\ &= n(ac+\lambda d\overline{b}) - \lambda n(cb+\overline{a}d). \end{aligned}$$

On the other hand

$$\begin{aligned} n((a+vb)(c+vd)) &= n(a+vb)n(c+vd) \\ &= (n(a)-\lambda n(b))(n(c)-\lambda n(d)). \end{aligned}$$

Comparing both expressions and using once more that n is multiplicative, we obtain

$$(ac, \lambda d\overline{b}) + n(v)(cb, \overline{a}d) = 0$$

or

$$(ac, d\overline{b}) = (\overline{a}d, cb)$$

then it follows from (3.3) that

$$((ac)b, d) = (a(cb), d) \qquad \text{for all} \qquad a,\ b,\ c,\ d \in B.$$

Thus $(ac)b = a(cb)$ and B is associative. If A is associative, we have $(va)b = v(ab) = v(ba)$ and $ba = ab$. Therefore B is commutative.

We now go back to the proof of Theorem 7. The algebra $B_2 = B_1 \oplus vB_1$ is an associative K–algebra of dimension 4. We let it as an exercise to check that B_2 is central simple. If B_2 is a proper subalgebra of A, let $B_3 = B_2 + wB_2$ with $w \in B_2^{\perp}$. If $B_3 = A$, the formulas (3.5) show (by definition!) that A is a Cayley algebra (see the book of Schafer). If B_3 is a proper subalgebra of A, we get $B_4 = B_3 + zB_3$ with $z \in B_3^{\perp}$. By Lemma 8, B_3 must be associative and hence B_2 commutative. This is not possible.

Let A be a *c.s.* K–algebra with an involution σ of the first kind. Since σ is an isomorphism $A \tilde{\to} A^{op}$, the class of A in $Br(K)$ is of order ≤ 2. Conversely any *c.s.* K–algebra A such that its class in $Br(K)$ is of order ≤ 2 carries an involution σ of the first kind. More precisely:

Theorem 9 (Albert). Let A be a *c.s.* K–algebra such that $2[A]=0$ in $Br(K)$. 1) There exists an involution σ of the first kind on A. 2) If the dimension of A is even, the involution σ can be chosen of even orthogonal type or of even symplectic type.

Proof. We follow the proof given by Saltman. If $2[A]=0$ in $Br(K)$, $[A]=[A^{op}]$ so there exists an isomorphism $\tau : A \tilde{\rightarrow} A^{op}$ of K–algebras. Let

$$\varphi : A\otimes A \tilde{\rightarrow} \mathrm{End}_K(A)$$

be the isomorphism defined by $\varphi(a\otimes b)(x)=ax\tau(b)$. Let now ω_A be the switch of $A\otimes A$, i.e. $\omega_A(a\otimes b)=b\otimes a$. By the Skolem–Noether theorem, $\omega_A=i_u$ for some $u\in(A\otimes A)^\bullet$. If $A=\mathrm{End}_K(V)$, $A\otimes A=\mathrm{End}_K(V\otimes V)$ and $u: V\otimes V\to V\otimes V$ can be chosen as the switch ω_V. If $\alpha : L\otimes A\tilde{\rightarrow}\mathrm{End}_L(V)$ is a Galois splitting, the element $u=(\alpha\otimes\alpha)^{-1}(\omega_V)\in L\otimes A\otimes A$ is in fact in $A\otimes A$ (this can easily be checked by Galois theory). Thus $u\in(A\otimes A)^\bullet$ can be chosen such that $(\alpha\otimes\alpha)(u)=\omega_V$ for any Galois splitting. In particular $u^2=1$. Let now $\psi : A\to A$ be given by $\varphi(u)$. We have

$$\psi^2=1 \quad\text{ and }\quad \psi(ax\tau(b))=b\psi(x)\tau(a) \quad\text{ for }\quad a,\ b,\ x\in A.$$

Lemma 10. Let $w=\psi(1)\in A$. 1) We have $1=w\tau(w)=\tau(w)w$ and $\tau^2=(i_w)^{-1}$. 2) If there exists a unit $a\in A$ such that $\psi(a)=a$, then $\sigma=i_a\circ\tau$ is a K–linear involution of A.

Proof. 1) We have $1=\psi(w)=\psi(w\cdot 1)=w\tau(w)$. On the other hand $1=\psi(1\cdot w)=\tau^{-1}(w)w$. Thus w is a unit of A with inverse $\tau(w)=\tau^{-1}(w)$. Further we have $x=\psi^2(x)=\psi(\psi(x\cdot 1))=\psi(w\tau(x))=\psi(\tau(x)\cdot 1)\cdot\tau(w)=$ $w\tau^2(x)\tau(w)=(i_w\circ\tau^2)(x)$. 2) We have $\sigma(xy)=\sigma(y)\sigma(x)$ since σ is an antiautomorphism. We check that $\sigma^2=1$. It follows from $a=\psi(a)=\psi(1\cdot a)=\tau(a)w$ that $w=a\tau(a)^{-1}$. Thus

$$\sigma^2=(i_a\circ\tau)^2=i_{a\tau(a)^{-1}}\circ\tau^2=1 \quad\text{since}\quad \tau^2=i_{w^{-1}}.$$

Proof of Theorem 9. To prove the first part, we have, by Lemma 10, to construct a unit $a\in A$ such that $\psi(a)=a$. We may assume that $A=M_n(D)$, D a division algebra. Since $2[D]=0$ in $Br(K)$ there exists an antiautomorphism $\beta : D\tilde{\rightarrow} D$. If

β is an involution, we extend β to A by taking the transpose on $M_n(K)$. If β is not an involution, we construct as above a map $\psi : D \to D$ such that $\psi^2 = 1$ and $\psi(ax\beta(b)) = b\psi(x)\beta(a)$ for $a,\ b,\ x \in D$. Since $\beta^2 \neq 1,\ \beta^2 = i_w^{-1}$ for $w = \psi(1)$ implies that $w \notin K$. Thus $1 + \psi(1) \neq 0$ and $a = 1 + \psi(1)$ is the wanted element a. If $A \simeq M_n(K),\ A$ has an involution given by the transpose.

We now prove the second claim of Theorem 9. By 1) A has an involution σ, say of type ε. Let $\eta = \pm 1$. If A contains a unit of the form $u = z + \varepsilon\eta\sigma(z)$, then $\sigma' = i_u \circ \sigma$ is of type η and in particular, σ' will be of even symplectic type if $\eta = -1$. Thus to prove 2) it suffices to show that for some K–linear involution σ of A and any $\varepsilon = \pm 1$, there exists a unit of A of the form $u = z + \varepsilon\sigma(z)$. Assume that $A = M_n(D),\ D$ a division algebra, $D \neq K$. By 1) D has an involution σ_1 and it obviously suffices to find $z_1 \in D$ such that $z_1 + \varepsilon\sigma_1(z_1) \neq 0$. Since $D \neq K,\ \sigma_1 \neq 1$ so $z_1 + \varepsilon\sigma_1(z_1) = 0$ for all $z_1 \in D$ is impossible. If $A = M_n(K)$ with $n = 2m$ we write $A = M_2(K) \otimes M_m(K)$, take $\sigma = \sigma_1 \otimes \sigma_2$, where σ_1 is the standard involution of $M_2(K)$ and σ_2 is transposition. Then for $z = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right) \otimes 1, \quad z + \varepsilon\sigma(z) = \left(\begin{smallmatrix}1 & 0\\ 0 & \varepsilon\end{smallmatrix}\right) \otimes 1$ is a unit of A.

One can also give conditions for the existence of involutions of the second kind on *c.s.* algebras. For this we need the notion of corestriction. Let Z be a separable quadratic K–algebra with standard involution σ_0 and let A be a K–algebra. Then $Z \otimes A$ is a Z–algebra and, by Galois theory, A can be identified with the set of elements $y \in Z \otimes A$ such that $(\sigma_0 \otimes 1)(y) = y$. The map $\tilde{\sigma} = \sigma_0 \otimes 1$ is a σ_0–semilinear automorphism of $Z \otimes A$ such that $\tilde{\sigma}^2 = 1$. Conversely, let B be a Z–algebra with a σ_0–semilinear automorphism $\tilde{\sigma}$ such that $\tilde{\sigma}^2 = 1$. Let

$$A = \{y \in B | \tilde{\sigma}(y) = y\}.$$

Then A is a K–algebra and the multiplication map $\mu : Z \otimes A \to B,\ y \otimes a \mapsto ya$ is an isomorphism of Z–algebras such that $\tilde{\sigma} = \mu(\sigma_0 \otimes 1)\mu^{-1}$. We say that A is descended from B (and $\tilde{\sigma}$) by *Galois descent.* Obviously Galois descent also applies to other structures, like quadratic forms. If B is a Z–algebra, we denote by ${}_{\sigma_0}B$ the algebra with the Z–action twisted through σ_0, i.e. $y \cdot b = \sigma_0(y)b,\ y \in Z,\ b \in B$. The map

$$\tilde{\sigma} : B \otimes_Z {}_{\sigma_0}B \to B \otimes_Z {}_{\sigma_0}B$$

given by $\tilde{\sigma}(b \otimes c) = c \otimes b$ is σ_0–semilinear and the corresponding K–algebra

$$A = \{x \in B \otimes_Z {}_{\sigma_0}B \mid \tilde{\sigma}(x) = x\}$$

is called the *corestriction* of B and is denoted by $\mathrm{cor}(B)$. If B has a Z–linear involution σ, then $\mathrm{cor}(B)$ has an induced K–linear involution $\mathrm{cor}(\sigma)$. We can now formulate a well-known existence criterion for involutions of the second kind:

Theorem 11 (Albert, Riehm).. Let L be a separable quadratic extension of K and let A be *c.s.* over L. Then A admits an involution of the second kind if and only if $[\mathrm{cor}(A)] = 0$ in $Br(K)$.

Theorem 11 will not really be used in the following and we do not prove it. A proof can be found in the book of Scharlau (p. 309).

Let $K \subset L$ be a separable quadratic extension and let A be a *c.s.* L–algebra with a fixed involution $x \mapsto x^*$ of the second kind. In the next Lemma we describe all possible other involutions of the second kind on A.

Lemma 12. Let σ be an involution of the second kind on A.

1) There exists $g \in A^\bullet$, with $g^* = g$, such that $\sigma(x) = gx^*g^{-1}$.

2) Let $g \in A^\bullet$ such that $g^* = g$ and let $\sigma_g(x) = gx^*g^{-1}$. Then σ_g is an involution of the second kind and $\sigma_g = \sigma_{g'}$ if and only if $g = \lambda g'$ for $\lambda \in K^\bullet$.

Let $\varphi : (A, \sigma_g) \tilde{\to} (A, \sigma_{g'})$ be an isomorphism of L–algebras-with-involution. There exist $c \in A^\bullet$ and $\lambda \in K^\bullet$ such that $g' = \lambda c g c^*$.

Proof. 1) By Skolem–Noether, there exists $g \in A^\bullet$ such that $\sigma(x^*) = i_g(x)$. It then follows from $\sigma^2 = 1$ that $g^* = \nu g$ for some $\nu \in L$ such that $\nu\sigma_0(\nu) = 1$. By the following Lemma (which is a special case of Hilbert Theorem 90) there exists $\lambda \in L$ such that $\nu = \lambda^{-1}\sigma_0(\lambda)$. Replacing g by $\lambda^{-1}g$, we see that we can assume $g^* = g$. The claims 2) and 3) are similar to the corresponding claims for involutions of the first kind and we do not check them.

Lemma 13. Let $\nu \in L$ be such that $\nu\sigma_0(\nu) = 1$. There exists $\lambda \in L$ such that

$\nu = \lambda^{-1}\sigma_0(\lambda)$.

Proof. If there exists $\rho \in L$ such that $\lambda = \sigma_0(\rho) + \sigma_0(\nu)\rho \neq 0$, then $\sigma_0(\lambda)\lambda^{-1} = \nu$. If not, $\rho \mapsto -\sigma_0(\nu)\rho$ is a K–linear automorphism of L. This can only occur if $\nu = -1$ (put $\rho = 1$!). Let then z be a generator of L such that $\sigma_0(z) = 1 - z$. The element $\lambda = 1 - 2z$ is such that $\sigma_0(\lambda) = -\lambda$ and $\nu = -1 = \lambda^{-1}\sigma_0(\lambda)$.

Chapter 4

The Clifford Algebra

Let (V, q) be a quadratic form over a field K. We would like to find a K–algebra C and a K–linear map $i : V \to C$ such that

$$(4.1) \qquad i(x)^2 = q(x) \cdot 1_C \quad \text{for all} \quad x \in V.$$

We define the Clifford algebra $C(V, q)$ of (V, q) as the K–algebra which is universal with respect to the property (4.1): A *Clifford algebra* for (V, q) is a K–algebra C together with a K–linear map $i : V \to C$ verifying (4.1), such that for any K–algebra A and any K–linear map $\varphi : V \to A$ with $\varphi(x)^2 = q(x) \cdot 1_A$, there exists a unique K–algebra homomorphism $\varphi' : C \to A$ such that $\varphi = \varphi' \circ i$.

Lemma 1. For any quadratic form (V, q) over K, there exists up to isomorphism a unique Clifford algebra $(C(V, q), i)$.

Proof. The uniqueness follows from the universal property of the Clifford algebra and we let its proof as an exercise. We prove existence. Let

$$T(V) = K \oplus V \oplus V \otimes V \oplus \cdots$$

be the tensor algebra of V, let $\mathcal{J}$ be the 2–sided ideal of $T(V)$ generated by all elements $x \otimes x - q(x) \cdot 1$ for $x \in V$ and let $C = T(V)/\mathcal{J}$. We claim that C together with the canonical map

$$i : V \to TV \to TV/\mathcal{J}$$

is a Clifford algebra. Let $\varphi : V \to A$ be a K–linear map such that $\varphi(x)^2 = q(x) \cdot 1_A$. By the universal property of the tensor algebra, φ extends to a unique homomorphism $\tilde{\varphi} : TV \to A$ of K–algebras such that $\tilde{\varphi}|_V = \varphi$. We have $\tilde{\varphi}(\mathcal{J}) = 0$, so $\tilde{\varphi}$

induces, as claimed, a unique homomorphism $\varphi' : C \to A$ such that $\varphi = \varphi' \circ i$.

Since a Clifford algebra is uniquely determined up to a unique isomorphism we shall speak in the following of "the" Clifford algebra of (V, q) and we shall denote it by $C(V, q)$ or $C(q)$. From now on we identify $K \cdot 1_C$ with K.

We observe that (4.1) implies

$$i(x)i(y) + i(y)i(x) = b_q(x, y), \qquad x,\ y \in V \tag{4.2}$$

where b_q is the polar of q.

We say that a K–algebra A is *$\mathbb{Z}/2\mathbb{Z}$–graded* (or simply *graded*) if A has a direct sum decomposition $A = A_0 \oplus A_1$, as K–vector space, such that $A_i \cdot A_j \subset A_{i+j}$, $i+j$ mod 2. We have $K \cdot 1 \subset A_0$. Such a grading on the tensor algebra TV is given by

$$(TV)_0 = K \oplus V \otimes V \oplus \cdots$$
$$(TV)_1 = V \oplus V \otimes V \otimes V \oplus \cdots$$

i.e. TV is graded by the degree. The generators $x \otimes x - q(x)$ of $\mathcal{J}$ have even degree. Therefore we get a $\mathbb{Z}/2\mathbb{Z}$–grading of $C(q)$, $C(q) = C_0 \oplus C_1$, where C_0 is generated by the even products of elements of V and C_1 by the odd products. In particular C_0 is a subalgebra of C, sometimes called the *even Clifford algebra*, and $i(V) \subset C_1$. By definition a graded homomorphism $\alpha : A_0 \oplus A_1 \to A'_0 \oplus A'_1$ of $\mathbb{Z}/2\mathbb{Z}$–graded algebras is an algebra homomorphism such that $\alpha(A_i) \subset A'_i$. An immediate consequence of the universal property of the Clifford algebra is that any morphism $\varphi : (V, q) \to (V', q')$ of quadratic forms induces a graded homomorphism $C(\varphi) : C(q) \to C(q')$. In particular any isometry $\varphi : (V, q) \tilde{\to} (V', q')$ induces an isomorphism $C(\varphi) : C(q) \tilde{\to} C(q')$. As we shall see later the converse does not hold, i.e. non isometric forms may have isomorphic Clifford algebras.

Lemma 2. Let $K \subset L$ be a field extension. There is a canonical isomorphism $C(L \otimes (V, q)) \simeq L \otimes C(V, q)$ for any quadratic form (V, q).

Proof. The map $1 \otimes i : L \otimes V \to L \otimes C(V, q)$ induces a homorphism $C(L \otimes (V, q)) \to L \otimes C(V, q)$. The homomorphism $V \to L \otimes V \to C(L \otimes (V, q))$ yields the inverse homomorphism.

We now compute the Clifford algebra of an orthogonal sum. For this we need the *graded tensor product* $A\hat{\otimes}B$ of two $\mathbb{Z}/2\mathbb{Z}$–graded K–algebras $A = A_0 \oplus A_1$ and $B = B_0 \oplus B_1$. As a K–vector space $A\hat{\otimes}B = A \otimes B$. The product is defined for homogeneous elements $a,\ a' \in A,\ b,\ b' \in B$ by

$$(a \otimes b)(a' \otimes b') = (-1)^{\partial(b)\partial(a')} aa' \otimes bb',$$

where $\partial(b)$ is the degree (0 or 1) of b, and is extended by linearity to arbitrary elements. The algebra $A\hat{\otimes}B$ is graded by

$$(A\hat{\otimes}B)_0 = A_0 \otimes B_0 + A_1 \otimes B_1$$

$$(A\hat{\otimes}B)_1 = A_1 \otimes B_0 + A_0 \otimes B_1.$$

Let $A = A_0 \oplus A_1$ be a graded algebra. We call the grading

$$M_2(A)_0 = \begin{pmatrix} A_0 & A_1 \\ A_1 & A_0 \end{pmatrix} \quad \text{and} \quad M_2(A)_1 = \begin{pmatrix} A_1 & A_0 \\ A_0 & A_1 \end{pmatrix}$$

of $M_2(A)$ the *checker-board grading.* On $M_2(K)$ the checker-board grading is

$$M_2(K)_0 = \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix} \quad \text{and} \quad M_2(K)_1 = \begin{pmatrix} 0 & K \\ K & 0 \end{pmatrix}.$$

Let $B = B_0 \oplus B_1$ be any $\mathbb{Z}/2\mathbb{Z}$–graded algebra. As an exercise in the theory of graded algebras (and because it will be used later) we prove the following

Lemma 3. There exists an isomorphism of graded algebras

$$\varphi : M_2(K)\hat{\otimes}B \tilde{\to} M_2(K) \otimes B = M_2(B).$$

Proof. We define $\varphi(x \otimes 1_B) = x \otimes 1_B$ for $x \in M_2(K)$ and

$$\varphi(1 \otimes (b_0 + b_1)) = \begin{pmatrix} b_0 + b_1 & 0 \\ 0 & b_0 - b_1 \end{pmatrix} \in M_2(B).$$

Proposition 4. $C(q \perp q') \simeq C(q)\hat{\otimes}C(q')$ as graded algebras.

Proof. Let $y = (x, x') \in V \oplus V'$. The map $y \mapsto i(x) \otimes 1 + 1 \otimes i(x')$ induces a map $C(q \perp q') \to C(q)\hat{\otimes}C(q')$. On the other hand, the inclusions $x \mapsto (x, 0) \in V \oplus V'$ and $x' \mapsto (0, x') \in V \oplus V'$ extend to algebra homomorphisms $C(q) \to C(q \perp q')$ and

$C(q') \to C(q \perp q')$. These two maps combine to a homomorphism $C(q)\hat{\otimes}C(q') \to C(q \perp q')$ which is the inverse of the first map.

Let $\{e_1, \ldots, e_n\}$ be a basis of V. In view of the relations (4.1) and (4.2) the 2^n elements $1,\ i(e_1), \ldots, i(e_n),\ i(e_1)i(e_2), \ldots, i(e_{n-1})i(e_n),\ i(e_1)i(e_2)i(e_3), \ldots,$ $i(e_1)\cdots i(e_n)$ form a set of generators of $C(V, q)$ as a vector space over K. A celebrated theorem says that they form a basis of $C(V, q)$.

Theorem 5 (Poincaré–Birkhoff–Witt).. If $\{e_1, \ldots, e_n\}$ is a basis of V, the set $\{1,\ i(e_{j_1})\cdots i(e_{j_r}),\ 1 \le r \le n,\ \ 1 \le j_1 < j_2 \cdots < j_r \le n\}$ is a basis of $C(V, q)$.

Proof. If the theorem is true for q_1 and q_2 it is true for $q_1 \perp q_2$ by Proposition 4. The theorem is true if $(V, q) = \langle a \rangle$ because, if v is a generator of V with $q(v) = a$, then $TV \simeq K[X],\ \ \mathcal{J} \simeq (X^2 - q(v))$ and $C(q) \simeq K[X]/(X^2 - q(v)) = K \cdot 1 \oplus K \cdot i(v)$. Hence the theorem is true if $\{e_1, \ldots, e_n\}$ is an orthogonal basis. If the theorem is true for a given basis, it is clearly true for any basis of V. By Lemma 13 of Chapter 1 the theorem is true for any field of characteristic not 2. Let R be a domain of characteristic not 2. By embedding R into its field of fractions, we see that the theorem is true for R. If now K is a field of characteristic 2, we can write K as a quotient $\overline{R}/I$ with $\overline{R}$ a domain of characteristic zero (for example a polynomial ring over $\mathbb{Z}$). Let $\overline{V}$ be the free module with basis a set of symbols $\{\overline{e}_1, \ldots, \overline{e}_n\}$, so $V = \overline{V}/I\overline{V}$. We define a quadratic form $\overline{q}$ on $\overline{V}$ by choosing elements $a_i,\ a_{ij}\ (i \neq j)$ in $\overline{R}$ such that $a_i + I = q(e_i)$ and $a_{ij} + I = b_q(e_i, e_j)$. We have $(\overline{V},\ \overline{q}) \otimes_{\overline{R}} \overline{R}/I \simeq (V, q)$ and by Lemma 2 (or better an obvious extension of Lemma 2 for forms over commutative rings) $C(\overline{V},\ \overline{q}) \otimes_{\overline{R}} \overline{R}/I \simeq C(M, q)$. The theorem is true for $C(\overline{V},\ \overline{q})$ because $\overline{R}$ is a domain of characteristic zero. Therefore it is also true for (V, q).

Remark 6. This proof of the Poincaré–Birkhoff–Witt theorem, which is due to Kneser, works obviously also for quadratic forms over finitely generated free R–modules, R any commutative ring. In fact we have used the notion of quadratic forms over rings in the proof as well as some basic facts, which are straightforward generalizations of the corresponding facts for forms over fields.

Corollary 7. If V has dimension n, then $C(V,q)$ has dimension 2^n and $C_0,\ C_1$ have both dimension 2^{n-1}.

It follows from Theorem 5 that $i : V \to C(V,q)$ is injective. From now on we shall identify V with its image $i(V)$ in $C(q)$. We now describe the structure of the Clifford algebras for nonsingular even dimensional forms and $\frac{1}{2}$–regular odd dimensional forms. We put $C = C(V,q),\ C_0 = C_0(V,q)$ and $C_1 = C_1(V,q)$.

Theorem 8. 1) Let (V,q) be a quadratic space of even dimension $2m$ over K. Then C is a *c.s.* K–algebra, the centre $Z(C_0)$ of C_0 is a separable quadratic K–algebra. If $Z(C_0)$ is a field, C_0 is *c.s.* over $Z(C_0)$. If $Z(C_0) \simeq K \times K$, there exists, up to isomorphism, a unique *c.s.* K–algebra A such that $C_0 \simeq A \times A$ as $K \times K$–algebra.

2) Let (V,q) be $\frac{1}{2}$–regular of odd dimension $2m+1$. Then C_0 is *c.s.* over K, the centre $Z(C)$ of C is a $\mathbb{Z}/2\mathbb{Z}$–graded quadratic K–algebra $Z_0 \oplus Z_1$ such that $Z_0 = K$ and Z_1 is generated by an element z with $z^2 = \lambda \cdot 1,\ \lambda \in K^\bullet$. Further the multiplication in C induces an isomorphism $Z(C) \otimes C_0 \tilde{\to} C$.

Proof. We first prove Theorem 8 in dimension 1 and 2, then by induction for forms $(V,q) = H(K) \perp (V',q')$ and finally for arbitrary forms.

Case $n = 1$: We have $(V,q) = \langle a \rangle,\ a \neq 0$. Let $v \in V$ with $q(v) = a$. Then $C = K \cdot 1 + Kv,\ C_0 = K \cdot 1,\ C_1 = Kv$ and the multiplication is given by $v^2 = a$. The algebra C is commutative, so $Z(C) = C$.

Case $n = 2$: We assume that $(V,q) = [a,b]$. Let $V = Ku \oplus Kv$ with $q(u) = a,\ q(v) = b$ and $b_q(u,v) = 1$. Then C has the basis $\{1, u, v, uv\}$ with the relations

$$u^2 = a, \quad v^2 = b, \quad uv + vu = 1.$$

To show that C is *c.s.*, it suffices to show that $L \otimes C$ is *c.s.* over L for some field extension L of K. Let $e = \lambda u + v,\ \lambda$ a symbol. We get $q(e) = \lambda^2 a + \lambda + b$ and we choose L such that the polynomial $X^2 a + X + b$ has a root λ in L. Then e is isotropic in $L \otimes V$. By Corollary 8 of Chapter 1, $L \otimes (V,q) \simeq [0,0]$ and $L \otimes C$ is generated by elements $u,\ v$ with $u^2 = 0,\ v^2 = 0$ and $uv + vu = 1$. It is easy to verify that

$$u \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \quad v \mapsto \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$$

induces an isomorphism

$$L \otimes C \tilde{\rightarrow} M_2(L).$$

Hence C is *c.s.* over K. We have in fact proved that

$$C(H(K)) \simeq M_2(K),$$

as graded algebras, if $M_2(K)$ has the checker–board grading. This will be used later. Let now $(V, q) = [a, b]$ as above. We have $C_0 = K \cdot 1 \oplus Kuv$ and $(uv)^2 = u(1 - uv)v = uv - ab$. Thus the element $z = uv$ is a generator of C_0 such that

$$z^2 = z - ab.$$

By Example 4 of Chapter 3, C_0 is a quadratic algebra and is separable if and only if $1 - 4ab \neq 0$. Since the discriminant of q with respect to the basis $\{u, v\}$ is $4ab - 1$, $Z(C_0) = C_0$ is a separable quadratic K–algebra. In particular $Z(C_0)$ is either a field or $Z(C_0) \simeq K \times K$.

This shows that Theorem 8 holds in dimension 1 and 2. We assume now that $(V, q) = H(K) \perp (V', q')$. Let $C' = C'_0 \oplus C'_1$ be the Clifford algebra of (V', q'). We get

$$C \simeq M_2(K) \hat{\otimes} C'$$

by Proposition 4 and the fact that $C(H(K)) \simeq M_2(K)$. Thus by Lemma 3

$$C \simeq M_2(K) \otimes C' = M_2(C').$$

If we use the isomorphism $C \tilde{\rightarrow} M_2(C')$ given by Lemma 3 to identify C with $M_2(C')$, then

$$C_0 = \begin{pmatrix} C'_0 & C'_1 \\ C'_1 & C'_0 \end{pmatrix} \quad \text{and} \quad C_1 = \begin{pmatrix} C'_1 & C'_0 \\ C'_0 & C'_1 \end{pmatrix} \quad \text{in} \quad M_2(C').$$

Assume that V has even dimension, so V' also has even dimension. By induction, Theorem 8 holds for (V', q'). In particular C is *c.s.* over K since C' is *c.s.* over K. We now construct an inner automorphism of $M_2(C')$ which maps C_0 to $M_2(C'_0)$. Let $x \in V'$ be anisotropic (such an element exists since q' is nonsingular). Then x is invertible in C' with inverse $x^{-1} = x \cdot q(x)^{-1} \in C'_1$. Left and right multiplication with

x induce isomorphisms $C'_1 \tilde{\to} C'_0$ of K–vector spaces. In particular $xC'_1 = C'_0$, $C'_1x = C'_0$ and $xC'_0x = C'_0$. Thus inner conjugation with the unit $\left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right)$ of $M_2(C')$ maps

$$C_0 = \begin{pmatrix} C'_0 & C'_1 \\ C'_1 & C'_0 \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} C'_0 & C'_1x \\ xC'_1 & xC'_0x \end{pmatrix} = M_2(C'_0).$$

It follows that $Z(C_0) \simeq Z(C'_0)$ and that C_0 is as described in 1). If (V,q) is $\frac{1}{2}$–regular of odd dimension, then (V',q') is also $\frac{1}{2}$–regular of odd dimension. We have as above

$$C \simeq M_2(C') \qquad \text{and} \qquad C_0 \simeq M_2(C'_0)$$

so that, by induction on the dimension, C_0 is *c.s.* over K and $Z(C) \simeq Z(C')$ is a quadratic algebra. Since the isomorphism $C \simeq M_2(C')$ is an isomorphism of graded algebras, $Z(C) \simeq Z(C')$ as graded algebras. The last claim $Z(C) \otimes C_0 \tilde{\to} C$ is also clear by induction.

If (V,q) is arbitrary, there exists a field extension $K \subset L$ such that $L \otimes (V,q) \simeq H(L) \perp (V',q')$. Therefore Theorem 8 holds for $L \otimes (V,q)$. Assume that V has even dimension. The algebra C is *c.s.* over K since $L \otimes C$ is *c.s.* over L and $Z(C_0)$ is separable quadratic since $Z(L \otimes C_0) = L \otimes Z(C_0)$ is separable quadratic over L. If $Z(C_0)$ is a field, it also follows from Theorem 8 that C_0 is *c.s.* over $Z(C_0)$. If $Z(C_0) = K \times K$, we only get that there exists an isomorphism of $K \times K$–algebras $C_0 \tilde{\to} A \times B$, A, B *c.s.* over K with $L \otimes A \simeq L \otimes B$. To show that $A \simeq B$, we use the following

Lemma 9. Let (V,q) be nonsingular of even dimension. There exists an isomorphism

$$\varphi : Z(C_0) \otimes C \tilde{\to} \mathrm{End}_{C_0}(C) = M_2(C_0)$$

of $Z(C_0)$–algebras, where C is viewed as a right C_0–module through the multiplication in C.

Proof. We define $\varphi(z \otimes c)(x) = cxz$ for $z \in Z(C_0)$, c, $x \in C$. If $Z(C_0)$ is a field, φ is an isomorphism since $Z(C_0) \otimes C$ is a *c.s.* algebra over $Z(C_0)$ and $Z(C_0) \otimes C$, $M_2(C_0)$ have the same dimension. A similar argument works if $Z(C_0) = K \times K$. The fact that $\mathrm{End}_{C_0}(C) \simeq M_2(C_0)$ follows from $C_1 = C_0 x$ for $x \in V$ anisotropic.

We go back to the proof of Theorem 8. If $Z(C_0) = K \times K$ and $C_0 = A \times B$, we have by the above lemma

$$M_2(A) \times M_2(B) \simeq C \times C.$$

Since $M_2(A)$, $M_2(B)$ and C are simple algebras, it follows that

$$M_2(A) \simeq C \simeq M_2(B),$$

hence $A \simeq B$ by Corollary 13 of Chapter 2.

Finally if V is $\frac{1}{2}$–regular of odd dimension, C_0 is *c.s.* over K since $L \otimes C_0$ is *c.s.* over L. Further $Z(C)$ is quadratic. Let $z = z_0 + z_1$, $z_i \in C_i$ be a generator of $Z(C)$. The part z_0 of degree zero lies in the centre of C_0, hence is a scalar, so z_1 also generates $Z(C)$ as an algebra. Since $z_1^2 \neq 0$ in $L \otimes Z(C)$, $z_1^2 \neq 0$ and $Z(C)$ is as claimed.

Chapter 5

Invariants of Quadratic Forms

In this chapter and the next the fact that we do not assume char $K \neq 2$ has a strong influence on the presentation of the results. Demazure–Gabriel is a useful reference for these two chapters. Parts of Proposition 5 are copied from Micali–Revoy.

Let (V, q) be a quadratic form which is either nonsingular of even dimension or $\frac{1}{2}$–regular of odd dimension. Let

$$Z(V, q) = Z(q) = \begin{cases} Z(C_0(V, q)) & \text{if Dim } V \text{ is even} \\ Z(C(V, q)) & \text{if Dim } V \text{ is odd.} \end{cases}$$

We call $Z(q)$, which is a graded quadratic algebra, the *discriminant algebra* of (V, q). The algebra $Z(q)$ is separable if Dim V is even or if Char $K \neq 2$. Clearly any isometry $(V, q) \tilde{\to} (V', q')$ induces a graded isomorphism $Z(q) \tilde{\to} Z(q')$. By the proof of Theorem 8, Chapter 4, we have

$$Z(H(K) \perp q) \simeq Z(q) \quad \text{and} \quad Z(H(K)) \simeq K \times K,$$

hence $Z(H(U)) \simeq K \times K$ for any hyperbolic space $H(U)$.

Lemma 1. $Z(q) = Z_C(C_0)$.

Proof. The claim follows from Theorem 8, Chapter 4 and Lemma 6, Chapter 2, if Dim$V$ is odd. Assume that Dim$V$ is even. The inclusion $\subset$ is clear. Let $x \in Z_C(C_0)$ and let $x = x_0 + x_1$ be its decomposition in homogeneous parts. Since C_0 is homogeneous, x_0 and x_1 must lie in $Z_C(C_0)$. By Proposition 5 of this chapter, we have a generator z of $Z(q)$ such that $x_1 z + z x_1 = x_1$, so $(1 - 2z)x_1 = 0$. But $(1 - 2z)^2 = 1 + 4(z^2 - z) = 1 + 4r$ is a unit (Proposition 5), hence $x_1 = 0$. (The use of Proposition 5 in the proof is not very elegant but is legal since Lemma 1 is not applied in the proof of Proposition 5 !).

We call the isomorphism class of $Z(q)$ the *Arf invariant* of (V,q) and denote it by $a(q)$. We say that the Arf invariant $a(q)$ is *trivial* if $Z(q) \simeq K \times K$.

Example 2. Assume that char $K \neq 2$ and that $\{e_1, \ldots, e_n\}$ is an orthogonal basis of (V,q). The element $z = e_1 \cdots e_n$ is a generator of $Z(q)$ and

$$z^2 = (-1)^{\frac{n(n-1)}{2}} a_1 \cdots a_n = (-1)^{\frac{n(n-1)}{2}} d(e_1, \ldots, e_n).$$

Let $Z = K \cdot 1 + K \cdot z$ and $Z' = K \cdot 1 + K \cdot z'$ be two quadratic algebras with $z^2 = a$ and $(z')^2 = b$. We claim that $Z \simeq Z'$ if and only if $a = \lambda^2 b$ for some $\lambda \in K^\bullet$ (assuming char $K \neq 2$!). Let $\varphi : Z \tilde{\to} Z'$ be an isomorphism and let $\varphi(z) = \lambda z' + \mu$. Since φ is an isomorphism, $\lambda \neq 0$. We have $\varphi(z^2) = \varphi(z)^2$, so $a = \lambda^2 b + 2\lambda\mu z' + \mu^2$. Since $2\lambda \neq 0$, $\mu = 0$ and $a = \lambda^2 b$ as claimed. Therefore $Z(q)$ is determined up to isomorphism by the class of $(-1)^{\frac{n(n-1)}{2}} a_1 \cdots a_n$ in $K^\bullet/K^{\bullet 2}$ if char $K \neq 2$. This class is equal to $\mathrm{disc}(q)$ multiplied by the class of $2^n(-1)^{\frac{n(n-1)}{2}}$ in $K^\bullet/K^{\bullet 2}$, since $\mathrm{disc}(q)$ is the class of $2^n a_1 \cdots a_n$. For any $a \in K^\bullet$, let $[a]$ denote its class in $K^\bullet/K^{\bullet 2}$. The element

$$\delta(q) = [(-1)^{\frac{n(n-1)}{2}}] \cdot \mathrm{disc}(q) \in K^\bullet/K^{\bullet 2}$$

is called the *signed discriminant* of (V,q). It follows from the above discussion that, for forms of the same dimension, $Z(q) \simeq Z(q')$ if and only, if $\delta(q) = \delta(q')$ (if char $K \neq 2$).

The following property of the discriminant algebra follows from Theorem 8 of Chapter 4 or from Lemma 1 and the fact that $C(L \otimes (V,q)) \simeq L \otimes C(V,q)$, $C_0(L \otimes (V,q)) = L \otimes C_0(V,q)$.

Lemma 3. For any field extension $K \subset L$, $Z(L \otimes (V,q)) \simeq L \otimes Z(V,q)$.

We now construct a generator z of $Z(q)$, for any characteristic, given orthogonal decompositions (see Chapter 1)

$$(V,q) = [a_1, b_1] \perp \cdots \perp [a_m, b_m] \quad \text{if} \quad \mathrm{Dim} V = 2m,$$

$$(V,q) = [a_1,b_1] \perp \cdots \quad \perp [a_m,b_m] \perp \langle a_{2m+1}\rangle \quad \text{if} \quad \text{Dim}V = 2m+1.$$

We construct z by induction, using the following

Lemma 4. Let (V_1, q_1) and (V_2, q_2) be quadratic spaces of even dimensions, and let $Z_1 = Z(q_1)$, $Z_2 = Z(q_2)$. For $i = 1, 2$, we assume that Z_i has a generator z_i such that

$$z_i^2 = z_i + r_i, \quad r_i \in K \quad \text{with} \quad 1 + 4r_i \neq 0$$

and

$$z_i v_i + v_i z_i = v_i \quad \text{for all} \quad v_i \in V_i.$$

Then $Z = Z(q_1 \perp q_2)$ has a generator z such that

$$z^2 = z + r \quad \text{with} \quad r = r_1 + r_2 + 4r_1r_2, \quad \text{hence} \quad 1 + 4r = (1+4r_1)(1+4r_2)$$

and

$$zv + vz = v \qquad \text{for all} \qquad v \in V = V_1 \oplus V_2.$$

Proof. Let $z = z_1 \otimes 1 + 1 \otimes z_2 - 2z_1 \otimes z_2$ in $C(q_1 \perp q_2) = C(q_1)\widehat{\otimes} C(q_2)$. We get $z^2 = z + r$ with $r = r_1 + r_2 + 4r_1r_2$. The other claims follow by straightforward computations.

Let $(V,q) = [a,b]$ and let $\{x,y\}$ be a basis of V such that $q(x) = a$, $q(y) = b$ and $b_q(x,y) = 1$. The discriminant algebra $Z(q) = C_0$ is generated by $z = xy$ and $z^2 = z - ab$. It is easy to verify that $zv + vz = v$ for all $v \in V$. Further $1 - 4ab = -d(x,y)$ is not zero. Thus we can apply Lemma 4 to quadratic spaces V_1, V_2 of type $[a,b]$ or to orthogonal sums of such spaces. Let $V_i = [a_i, b_i]$ and

$$(V,q) = (V_1,q_1) \perp \ldots \perp (V_m,q_m).$$

We choose in each V_i a basis $\{e_i, e_{i+m}\}$ such that

$$q(e_i) = a_i, \quad q(e_{i+m}) = b_i \quad \text{and} \quad b_q(e_i, e_{i+m}) = 1$$

and put $z_i = e_ie_{i+m}$, $r_i = -q(e_i)q(e_{i+m}) = -a_ib_i$. By Lemma 4 (and induction) the element

$$z = \sum_{j=1}^{m} (-2)^{j-1} S_j(z_1, \ldots, z_m),$$

where S_j is the $j-th$ elementary symmetric function in m letters, is a generator of $Z(q)$ such that

$$z^2 = z + r, \quad r = \sum_{j=1}^{m} 4^{j-1} S_j(r_1, \ldots, r_m)$$

and $zv + vz = v$ for all $v \in V$. Further

$$1 + 4r = \prod_{i=1}^{m}(1 + 4r_i) = (-1)^m d(e_1, e_{1+m}, \ldots, e_m, e_{2m}).$$

Therefore the class of $1 + 4r$ in $K^\bullet/K^{\bullet 2}$ is the signed discriminant $\delta(q)$ of (V, q).

Let now (V, q) be of odd dimension. We assume that

$$(V, q) = (V_1, q_1) \perp \cdots \perp (V_m, q_m) \perp \langle a_{2m+1} \rangle = (V', q') \perp \langle a_{2m+1} \rangle$$

with V_i as above. Let $e_{2m+1} \in V$ be a basis of $\langle a_{2m+1} \rangle$ such that $q(e_{2m+1}) = a_{2m+1}$. By the even dimensional case, we have a generator z' of $Z(q') \subset C_0(q')$ such that $z'^2 = z' + r'$ and $z'v' + v'z' = v'$ for all $v' \in V'$. The element

$$z = e_{2m+1} \otimes (1 - 2z')$$

of $C(\langle a_{2m+1} \rangle) \hat{\otimes} C(q') = C(q)$ is of degree 1 and commutes with all elements of $C_0(q)$, thus $z \in Z(q)$. Since

$$z^2 = a_{2m+1}(1 + 4r') = (-1)^m d_0(e_1, \ldots, e_{2m}, e_{2m+1}),$$

the element z is a homogeneous generator of $Z(q)$. We call the class of $(-1)^m d_0(e_1, \ldots, e_{2m+1})$ in $K^\bullet/K^{\bullet 2}$ the signed $\frac{1}{2}$–*discriminant* of (V, q) and denote it by $\frac{1}{2}\delta(q)$. The element $\frac{1}{2}\delta(q)$ depends only on the isometry class of (V, q). By the above discussion, we have for spaces of the same odd dimension

$$Z(q) \simeq Z(q') \quad \text{(as graded algebras)} \Leftrightarrow \tfrac{1}{2}\delta(q) = \tfrac{1}{2}\delta(q').$$

Observe that if $(V, q) = [a_1, b_1] \perp \cdots \perp [a_m, b_m] \perp \langle a_{2m+1} \rangle$ and char $K = 2$, then $\frac{1}{2}\delta(q) = [a_{2m+1}] \in K^\bullet/K^{\bullet 2}$. Summarizing, we have

Proposition 5. 1) Let (V, q) be a nonsingular quadratic form of even dimension. There exists an element $z \in C_0$ such that

i) $Z(C_0) = K \cdot 1 \oplus K \cdot z$, $z^2 = z + r$, $r \in K$ and $1 + 4r \in K^\bullet$.

ii) The class of $(1 + 4r)$ in $K^\bullet/K^{\bullet 2}$ is the signed discriminant of q.

iii) $vz + zv = v$ for all $v \in V$, hence $xz + zx = x$ for all $x \in C_1$.

2) Let (V, q) be $\frac{1}{2}$–regular of odd dimension. There exists an element $z \in C_1$ such that

i) $Z(C) = K \cdot 1 \oplus K \cdot z,\ z^2 = s,\ \ s \in K^\bullet$.

ii) The class of s in $K^\bullet / K^{\bullet 2}$ is the signed $\frac{1}{2}$–discriminant of q.

The quadratic algebra $Z(q)$ has a unique standard involution σ_0. We now study how σ_0 is related to the structure of the Clifford algebra $C(q)$. By the universal property of the Clifford algebra, there exists a unique K–linear involution σ of $C(q)$ such that $\sigma(v) = -v$ for $v \in V$. We call σ the *standard involution* of $C(q)$ (even if σ is not necessarily a standard involution in the sense of Chapter 3). The involution σ' of C which is the identity on V will be called the *canonical involution* of C. Further, let $C(-1)$ be the automorphism of $C(q)$ such that $C(-1)(v) = -v$ for all $v \in V$.

Proposition 6. 1) If (V, q) is $\frac{1}{2}$–regular of odd dimension, then σ_0 is the restriction of $C(-1)$ to $Z(q)$. 2) Assume that (V, q) is nonsingular of even dimension. Then

i) $\sigma_0(x)y = yx$ for all $x \in Z(q)$ and $y \in C_1$.

ii) If the dimension of V is congruent to 2 (mod 4), σ_0 is the restriction of the standard involution σ of $C(q)$.

iii) If the dimension of V is congruent to 0 (mod 4), the standard involution σ of $C(q)$ induces the identity on $Z(q)$.

Proof. Let $z \in Z(q)$ be as in Proposition 5. The claims follow from Proposition 5, using that $\sigma_0(z) = -z$ if the dimension of V is odd and $\sigma_0(z) = 1 - z$ if the dimension of V is even. Observe that we cannot describe σ_0 if $\mathrm{Dim} V \equiv 0(4)$.

In characteristic 2, the discriminant does not give any information on q or $Z(q)$, since $\delta(q) = 1$ for any nonsingular form. On the other hand the element $r \in K$ of Proposition 5 can be used to characterize $Z(q)$. We have

Lemma 7. Let K be a field of characteristic 2 and let $Z = K \cdot 1 \oplus K \cdot z,\ \ Z' = K \cdot 1 + K \cdot z'$ be quadratic K–algebras with $z^2 = z + r,\ \ z'^2 = z' + r',\ r,\ r' \in K$. Then Z and Z' are isomorphic if and only if there exists $\mu \in K$ such that $r' - r = \mu^2 + \mu$.

Proof. Let $\varphi : Z \to Z'$ be an isomorphism given by $\varphi(z) = \lambda z' + \mu$. It follows from $\varphi(z^2) = (\varphi(z))^2$ that $\lambda^2 = \lambda$ and $\lambda^2 r' - r = \mu^2 + \mu$. Hence $\lambda = 1$ and $r' - r = \mu^2 + \mu$ as claimed. Conversely we define an isomorphism $\varphi : Z \to Z'$ by putting $\varphi(z) = \lambda z' + \mu$.

The set of elements of K of the form $\mu^2 + \mu$, $\mu \in K$ is an additive subgroup of K if char $K = 2$. We denote it by $\wp(K)$. Let (V, q) be a quadratic space and let $z \in Z(q)$ be a generator as given by Proposition 5, i.e. $z^2 = z + r, \quad r \in K$. The class of r in the additive group $K/\wp(K)$ is the *classical Arf invariant* of (V, q). We denote it by $\alpha(q)$. In view of Lemma 7, $\alpha(q)$ is an invariant of the isometry class of (V, q) and by Lemma 4

$$\alpha(q_1 \perp q_2) = \alpha(q_1) + \alpha(q_2).$$

If $(V, q) = [a_1, b_1] \perp \cdots \perp [a_m, b_m]$, then

$$\alpha(q) = a_1 b_1 + \cdots + a_m b_m.$$

In particular $\alpha(q) = 0$ for any hyperbolic space (V, q).

The following formulas hold for orthogonal sums:

Lemma 8. 1) If (V_2, q_2) is nonsingular of even dimension and (V_1, q_1) is any quadratic form, then

$$C(q_1 \perp q_2) \simeq C((1 + 4r_2)q_1) \otimes C(q_2),$$

where r_2 is as in Proposition 5 (for (V_2, q_2)).
2) If (V_2, q_2) is $\frac{1}{2}$–regular of odd dimension and (V_1, q_1) is any quadratic form, then

$$C_0(q_1 \perp q_2) \simeq C(-s_2 q_1) \otimes C_0(q_2),$$

where s_2 is as in Proposition 5 (for (V_2, q_2)). In particular

$$C_0(\langle \lambda \rangle \perp q) \simeq C(-\lambda q)$$

for any quadratic form $q : V \to K$.

Proof. 1) Let z_2 and r_2 be as in Proposition 5 (for (V_2, q_2)). The element $w_2 = 1-2z_2$ satisfies $\sigma_0(w_2) = -w_2$ and $w_2^2 = 1 + 4r_2$, where σ_0 is the standard involution of $Z(q_2)$. We define a homomorphism

$$\varphi : C(q_1 \perp q_2) = C(q_1)\hat{\otimes}C(q_2) \to C((1+4r_2)q_1) \otimes C(q_2)$$

by $\varphi(v_1 \otimes 1) = v_1 \otimes w_2$ and $\varphi(1 \otimes v_2) = 1 \otimes v_2$ for $v_i \in V_i$ (apply Proposition 6, the universal property of the graded tensor product and the universal property of the Clifford algebra !). Since V_1 and V_2 are contained in the image of φ, φ is an isomorphism.
2) Let $z_2 \in Z(q_2)$, $s_2 \in K$ be as in Proposition 5 (for q_2). We define

$$\psi : C(-s_2 q_1) \otimes C_0(q_2) \to C_0(q_1 \perp q_2)$$

by $\psi(1 \otimes x) = j_2(x)$, where $j_i : C(q_i) \to C(q_1 \perp q_2)$ is the canonical embedding, $i = 1, 2$, and $\psi(v_1) = j_1(v_1)j_2(z_2)$ for $v_1 \in V_1$. The map ψ is surjective, hence an isomorphism.

Another important invariant of quadratic forms is the *Witt invariant* $w(q)$, which takes values in the Brauer group $Br(K)$ of the field K. We define

$$w(q) = \begin{cases} [C(q)] \in Br(K) & \text{if } q \text{ is nonsingular of even dimension} \\ [C_0(q)] \in Br(K) & \text{if } q \text{ is } \tfrac{1}{2}\text{-regular of odd dimension.} \end{cases}$$

The Witt invariant obviously depends only on the isometry class of q. Further, by the proof of Theorem 8, Chapter 4, we have

$$w(H(K) \perp q) = w(q) \quad \text{ and } \quad w(H(K)) = 1$$

so $w(H(U)) = 1$ for any hyperbolic space $H(U)$. We now compute the Witt invariant of an orthogonal sum $q_1 \perp q_2$ with q_2 of even dimension. For any class $\delta \in K^\bullet/K^{\bullet 2}$ and any quadratic form q, the isometry class of $\delta \cdot q$ is well defined. With this in mind, we get from Lemma 8:

Proposition 9. Let q_2 be a nonsingular form of even dimension.

1) If q_1 is nonsingular of even dimension, then

$$w(q_1 \perp q_2) = w(\delta(q_2)q_1)w(q_2).$$

2) If q_1 is $\frac{1}{2}$–regular of odd dimension, then

$$w(q_1 \perp q_2) = w(q_1)w(-\tfrac{1}{2}\delta(q_1)q_2).$$

Let (V,q), (V',q') be quadratic forms and let $\lambda \in K^\bullet$. A K–linear isomorphism $\varphi : V \tilde{\to} V'$ such that $q'(\varphi(x)) = \lambda q(x)$ for all $x \in V$ is called a *similitude with multiplier* λ. Two similar forms have isomorphic even Clifford algebras:

Lemma 10. Let $\varphi : (V,q) \tilde{\to} (V',q')$ be a similitude with multiplier λ. There exists an isomorphism $C_0(\varphi) : C_0(q) \tilde{\to} C_0(q')$ such that

$$C_0(\varphi)(xy) = \lambda^{-1}\varphi(x)\varphi(y) \qquad \text{for} \qquad x,\ y \in V.$$

Proof. Let $T^0(V)$ be the even part of the tensor algebra of V. The algebra isomorphism $T^0(\varphi) : T^0(V) \to T^0(V')$, defined by $T^0(\varphi)(x_0 \otimes \cdots \otimes x_{2n}) = \lambda^{-n}\varphi(x_0)\cdots\varphi(x_{2n})$, induces the wanted isomorphism.

We describe now another useful isomorphism of Clifford algebras. First we need a definition. Let Z be a separable quadratic K–algebra with standard involution $\sigma_0 : z \mapsto \overline{z}$ and let $\lambda \in K^\bullet$. As in Lemma 8 of Chapter 3, we define a K–algebra

$$A = Z \oplus uZ$$

of dimension 4 by the multiplication rules

$$(z_1 + uz_2)(z_3 + uz_4) = z_1z_3 + \lambda\overline{z}_2z_4 + u(z_2z_3 + \overline{z}_1z_4).$$

The algebra A is *c.s.* of dimension 4, hence a quaternion algebra over K and has the grading $A_0 = Z$, $A_1 = uZ$. We denote it by $(\lambda,\ Z/K]$.

Proposition 11. Let (V,q) be nonsingular of even dimension. There exists an isomorphism of graded algebras

$$M_2(K) \otimes C(V,\lambda q) \tilde{\to} (\lambda, Z(q)/K] \otimes C(V,q).$$

In particular $w(\lambda q) = w(q) \cdot w((\lambda, Z(q)/K])$.

Proof. Let $Z = Z(q)$ and let $\varphi_1 : V \to (\lambda, Z/K] \otimes C(V,q)$ be given by $\varphi_1(v) = u \otimes v$, $v \in V$. By the universal property of the Clifford algebra φ extends to a homomorphism $\varphi : C(V,\lambda q) \to (\lambda, Z/K] \otimes C(V,q)$ which is injective since $C(V,\lambda q)$ is *c.s.*

Let A be the commutant of $\varphi(C(V,\lambda q))$ in $(\lambda, Z/K]\otimes C(V,q)$, so $A\otimes C(V,\lambda q)\simeq(\lambda, Z/K]\otimes C(V,q)$. The algebra A is generated by $(Z\otimes Z)^{\sigma_0\otimes\sigma_0}\simeq K\times K$ and by u, so $A\simeq(K\times K)\oplus u(K\times K)\simeq(\lambda, K\times K]$. We claim that $(\lambda, K\times K]\simeq M_2(K)$. In fact an isomorphism is induced by $K\times K\to\begin{pmatrix}K & 0\\ 0 & K\end{pmatrix}$ and $u\mapsto\left(\begin{smallmatrix}0 & \lambda\\ 1 & 0\end{smallmatrix}\right)$.

Chapter 6

Special Orthogonal Groups and Spin Groups

Let (V, q) be a quadratic form and let $O(q)$ be its orthogonal group. We denote by $\mathrm{Aut}_K^g(C)$ the group of automorphisms of the Clifford algebra $C = C_0 \oplus C_1$ of (V, q) as a graded algebra. Any $\varphi \in O(q)$ induces an element $\beta = C(\varphi) \in \mathrm{Aut}_K^g(C)$ such that $\beta V \subset V$. Conversely, let $\beta \in \mathrm{Aut}_K^g(C)$ be such that $\beta V \subset V$. Then $\varphi = \beta|_V$ is an automorphism of V such that $q(\varphi(v)) = \varphi(v)^2 = \beta(v^2) = q(v),\ v \in V$, hence $\varphi \in O(q)$. Therefore we can identify $O(q)$ with the subgroup of elements β of $\mathrm{Aut}_K^g(C)$ such that $\beta V \subset V$:

$$O(q) = \{\beta \in \mathrm{Aut}_K^g(C) \mid \beta V \subset V\}.$$

We assume in the following that (V, q) is either $\frac{1}{2}$–regular of odd dimension or nonsingular of even dimension. Let $Z(q)$ be the discriminant algebra of (V, q), i.e. the centre of C if the dimension of V is odd or the centre of C_0 if the dimension of V is even. For any $\varphi \in O(q)$ the restriction of φ to $Z(q)$ is an automorphism of $Z(q)$ as a graded algebra. Thus the restriction defines a group homomorphism

$$\rho : O(q) \to \mathrm{Aut}_K^g(Z(q)).$$

Lemma 1. The group $\mathrm{Aut}_K^g(Z(q))$ is either trivial (if the standard involution σ_0 of $Z(q)$ is the identity) or has two elements $1,\ \sigma_0$.

Proof. If $\mathrm{Dim} V$ is even, $Z(q)$ is concentrated in degree zero and has a generator z such that $z^2 = z + r$ for some $r \in K$. Let θ be a K–automorphism of $Z(q)$ and let $\theta(z) = \lambda z + \mu$. It follows from $\theta(z^2) = \theta(z)^2$ that

$$1 = \lambda + 2\mu \qquad \text{and} \qquad \mu + r = \lambda^2 r + \mu^2.$$

Substituting $\lambda = 1 - 2\mu$ in the second equation we get

$$\mu^2(4r + 1) = \mu(4r + 1).$$

By Proposition 5 of Chapter 5, $4r + 1 \neq 0$, so $\mu = 1$ or $\mu = 0$ and $\theta(z) = -z + 1$ or $\theta(z) = z$. If Dim$V$ is odd, $Z(q)$ is generated by an element z of degree 1 such that $z^2 = s,\ s \neq 0 \in K$. Thus, if $\theta \in \mathrm{Aut}_K^g(Z(q))$, we must have $\theta(z) = \lambda z$ and $\lambda^2 = 1$.

In view of Lemma 1, we may define a homomorphism $O(q) \to \mathbb{Z}/2\mathbb{Z}$, the so-called *Dickson map*, by putting:

$$Dick(\varphi) = \begin{cases} 0 & \text{if } C(\varphi)|_{Z(q)} = 1 \\ 1 & \text{if } C(\varphi)|_{Z(q)} \neq 1. \end{cases}$$

The kernel of the Dickson homomorphism is called the *special orthogonal group* and is denoted by $SO(q)$. This is not the usual definition of $SO(q)$ as kernel of the determinant map, which can only be used if the characteristic is not equal to 2. We need a different definition to include the case of characteristic 2. However the next lemma shows that the two definitions are related. Any $\varphi \in O(q)$ is represented by a matrix (also denoted φ) if we fix a basis of V. The determinant of φ is independent of the choice of the basis. Thus the determinant induces a homomorphism

$$\det : O(q) \to K^\bullet.$$

Lemma 2. Assume that (V, q) is either $\frac{1}{2}$–regular of odd dimension or nonsingular of even dimension. Then

1) $\det(\varphi) = \pm 1$ if $\varphi \in O(q)$.
2) $SO(q) \subset \mathrm{Ker}(O(q) \overset{\det}{\to} \{\pm 1\})$.
3) $SO(q) = \mathrm{Ker}(O(q) \overset{\det}{\to} \{\pm 1\})$ if (V, q) is $\frac{1}{2}$–regular or char $K \neq 2$.

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis of V and let (u_{ij}) be the matrix of $\varphi \in O(q)$ with respect to the basis, i.e.

$$\varphi(e_j) = \sum u_{ij} e_i.$$

We have $\det(u_{ij})^2 d(e_1, \ldots, e_n) = d(e_1, \ldots, e_n) \neq 0$ if q is nonsingular and $\det(u_{ij})^2 d_0(e_1, \ldots, e_n) = d_0(e_1, \ldots, e_n) \neq 0$ if q is $\frac{1}{2}$–regular. Thus $\det(u_{ij})^2 = 1$ and the first claim is proved. For the second claim, we choose a basis of (V, q) as in Lemma 17 (resp. 19) of Chapter 1 and choose a generator z of $Z(q)$ as given by

Proposition 5 of Chapter 5. Let $\varphi \in O(q)$. We claim that

$$C(\varphi)(z) = \det(\varphi)z + \mu$$

for some $\mu \in K$. This is clear if char $K = 2$, since $\det(\varphi) = 1$ by 1) and $z \mapsto z$, $z \mapsto z + 1$ are the only possible automorphisms of $Z(q)$ by Lemma 1. Assume that char $K \neq 2$. We have a unique decomposition

$$z = \lambda e_1 \cdots e_n + \text{terms of lower length}$$

by the *P.B.W.* theorem. In view of the expression for z computed between Lemma 4 and Proposition 5 of Chapter 5, the coefficient λ is not zero (since char $K \neq 2$!). We get

$$\begin{aligned} C(\varphi)(z) &= \lambda\varphi(e_1)\cdots\varphi(e_n) + \text{terms of lower length} \\ &= \lambda\det(\varphi)e_1\cdots e_n + \text{terms of lower length.} \end{aligned}$$

Since, on the other hand, $C(\varphi)(z) = \gamma z + \mu$ for some $\gamma,\ \mu \in K,\ \gamma \neq 0$, we must have $\gamma = \det(\varphi)$ by the uniqueness of the decomposition $z = \lambda e_1 \cdots e_n +$ terms of lower length. The formula $C(\varphi)(z) = \det(\varphi)z + \mu$ implies 2). We now check 3) if (V, q) is $\frac{1}{2}$–regular. Since $Z(q)$ is graded and generated by an element z of degree 1 and since $C(\varphi)$ preserves grading, we must have $C(\varphi)(z) = \det(\varphi)z$. Thus $C(\varphi)$ is the identity on $Z(q)$ if and only if $\det(\varphi) = 1$. If char $K \neq 2$, we choose an orthogonal basis $\{e_1, \ldots, e_n\}$ for V. The element $w = e_1 \cdots e_n$ is a generator of $Z(q)$. For any $\varphi \in O(q)$, the basis $\{e'_i = \varphi(e_i)\}$ is also orthogonal and $C(\varphi)(w) = e'_1 \cdots e'_n = \det(\varphi)w$. This shows 3) if char $K \neq 2$.

Example 3. Let $(V, q) = H(K)$. By Example 2 of Chapter 1,

$$O(q) = \{\left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \in M_2(K) \mid xv + uy = 1,\ \ xu = 0,\ \ yv = 0\}$$

if we identify V with K^2 through a basis given by a hyperbolic pair $\{e, f\}$. The element $z = ef$ is a generator of $Z(q)$. We have $\varphi(e) = xe + uf$, $\varphi(f) = ye + vf$ if $\varphi = \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right)$. Thus

$$C(\varphi)(z) = (xe + uf)(ye + vf) = (xv - uy)z + uy.$$

If follows that

$$SO(q) = \left\{ \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \in M_2(K),\ x \in K^\bullet \right\} \simeq K^\bullet.$$

In characteristic 2, $O(q) \cap SL_2(K) = O(q)$, so $SO(q)$ is a proper subgroup of $\mathrm{Ker}(O(q) \overset{\det}{\to} \{\pm 1\})$.

In the next section we assume that K is a field of characteristic not equal to 2. For any quadratic space (V, q) of dimension n, we define the *Lie algebra of the group* $SO(q)$ as the set

$$so(q) = \{f \in \mathrm{End}_K(V) \mid b_q(f(x), y) + b_q(x, f(y)) = 0\},$$

where b_q is the polar of q. If $q = \langle 1, \ldots, 1\rangle$, then $so(q) = \mathrm{Alt}_n(K)$. In particular $\mathrm{Dim}_K so(\langle 1, \ldots, 1\rangle) = \frac{n(n-1)}{2}$ and the K–vector space $so(q)$ is obviously a Lie algebra for the Lie product $[f, g] = f \circ g - g \circ f$. Since $\mathrm{char} K \neq 2$, any quadratic space (V, q) is diagonalizable and there exists a field extension $K \subset L$ such that $L \otimes q \simeq \langle 1, \ldots, 1\rangle$. Thus in general $\mathrm{Dim}_K so(q) = \frac{n(n-1)}{2}$ and $so(q)$ is a Lie algebra.

Let now $[V, V]$ be the K–linear subspace of $C(q)$ generated by all $[x, y] = xy - yx$, $x, y \in V$. It follows from the P.B.W. theorem that $\mathrm{Dim}_K[V, V] = \frac{n(n-1)}{2}$. Further, $[V, V]$ is a Lie algebra for the product $[\ ,\ ]$ and $[[V, V], V] \subset V$. Again this is easily seen by taking an orthogonal basis of V. Let

$$\gamma : [V, V] \to \mathrm{End}_K(V)$$

be defined by $\gamma(\xi) = [\xi, v] = \xi v - v\xi$, $\xi \in [V, V]$. We have

$$b_q([\xi, v], w) + b_q(v, [\xi, w]) = 0.$$

This can be checked for $\xi = [x, y]$ using the defining relations of the Clifford algebra and the general case follows by linearity. Thus γ is a homomorphism of Lie algebras $[V, V] \to so(q)$. We claim that γ is an isomorphism. Since both algebras have the same dimension, it suffices to check that γ is injective. If $\gamma(\xi) = 0$, then ξ lies in the centre of $C(q)$ and in the centre of $C_0(q)$ so $\xi \in K$. But $K \cap [V, V] = 0$. Therefore the Lie algebra $so(q)$ can be identified with $[V, V] \subset C_0(q)$. We observe that

$$[so(q), so(q)] = so(q) \ \text{ if } \ n \geq 3.$$

This, again, can be easily checked by taking an orthogonal basis of V and using the identification $so(q) = [V, V]$. It follows that $so(q)$ is always contained in $C_0(q)' = [C_0(q), C_0(q)]$. We shall use this remark later.

We now introduce different subgroups of the group of units of the Clifford algebra $C = C_0 \oplus C_1$ of (V,q). These groups will help to describe $O(q)$ and $SO(q)$. The field K can be of arbitrary characteristic. Let $u \in C^\bullet$ be a unit which is homogeneous , i.e. $u \in C_0^\bullet$ or $u \in C^\bullet \cap C_1$. We define the *graded inner automorphism*

$$i_u^g : C \to C \quad \text{by} \quad i_u^g(x) = (-1)^{\partial(u)\partial(x)} uxu^{-1}$$

for x homogeneous, $\partial(u)$ denoting the degree of u, i.e. $\partial(u) = 0$ if $u \in C_0$ and $\partial(u) = 1$ if $u \in C_1$. The group

$$\Gamma(q) = \{u \in C^\bullet, \ u \ \text{ homogeneous} \mid i_u^g(V) \subset V\}$$

is called the *Clifford group* of (V,q) and the subgroup

$$S\Gamma(q) = \{u \in C_0^\bullet \mid i_u(V) \subset V\} = \Gamma(q) \cap C_0$$

is the *special Clifford group.*

Let σ be the standard involution of C. We define a map

$$\mu : C \to C \quad \text{by} \quad \mu(c) = \sigma(c)c, \quad c \in C.$$

We have $\mu(v) = -q(v)$ for $v \in V$.

Lemma 4. Assume that (V,q) is nonsingular if the dimension of V is even and $\frac{1}{2}$–regular if the dimension of V is odd. Then $\mu(c) \in K^\bullet$ for $c \in \Gamma(q)$ and μ induces a group homomorphism

$$\mu : \Gamma(q) \to K^\bullet.$$

Proof. If suffices to check that $\mu(c) \in K^\bullet$ for $c \in \Gamma(q)$. The property $\mu(xy) = \mu(x)\mu(y)$ then is immediate. For any $c \in \Gamma(q)$ and $v \in V$, we have $i_c^g(v) = -\sigma(i_c^g(v))$, since $i_c^g(v) \in V$. On the other hand $\sigma(i_c^g(v)) = -i^g_{\sigma(c)^{-1}}(v)$, since $\sigma(v) = -v$. Therefore $\sigma(c)cv = v\sigma(c)c$ for all $v \in V$. It follows that $\sigma(c)c$ is in the centre of C_0 and in the centre of C, so $\sigma(c)c \in K^\bullet$.

Example 5. An element $v \in V$ belongs to $\Gamma(q)$ if and only if $q(v) \in K^\bullet$, i.e., v is anisotropic. For if $q(v) \in K^\bullet$, then

$$\begin{aligned} i_v^g(x) &= -vxv^{-1} = -vxvq(v)^{-1} = (xv - b_q(v,x))vq(v)^{-1} \\ &= x - \tfrac{b_q(v,x)}{q(v)}v = \tau_v(x). \end{aligned}$$

Thus i_v^g is the reflection τ_v.

Since $i_u^g(V) \subset V$ for $u \in \Gamma(q)$, $i_u^g \in O(q)$ and we have a group homomorphism $\Gamma(q) \to O(q)$, $u \mapsto i_u^g$. We denote it by π. Since i_u is the identity on $Z(q)$ if $u \in S\Gamma(q)$, π restricts to a homomorphism $S\pi : S\Gamma(q) \to SO(q)$.

Proposition 6. The sequences

$$1 \to K^\bullet \to \Gamma(q) \xrightarrow{\pi} O(q) \to 1$$

and

$$1 \to K^\bullet \to S\Gamma(q) \xrightarrow{S\pi} SO(q) \to 1$$

are exact.

Proof. If $i_u^g(v) = v$ for all $v \in V$, then $u \in Z_C(C_0) = Z(q)$ by Lemma 1 of Chapter 5. Thus $u \in S\Gamma(q)$ if Dim$V$ is even and $i_u^g = i_u$. But then $i_u(v) = v$ implies that $u \in Z(C) = K$. If the dimension of V is odd, either $u \in K^\bullet$ or $u = \lambda z$, z a generator of $Z(q)$ as given in Proposition 5 of Chapter 5. If $u = \lambda z$, we get $i_u^g(v) = -zvz^{-1}$, thus $zv = -vz$. But $zv + vz = v$ by Proposition 5 of Chapter 5, thus $v = 0$ which is absurd. The surjectivity of π if $(V,q) \not\simeq H(\mathbb{F}_2) \perp H(\mathbb{F}_2)$ follows from Example 5 and the fact that $O(q)$ is generated by reflections (Corollary 15 of Chapter 1). The case $(V,q) = H(\mathbb{F}_2) \perp H(\mathbb{F}_2)$ can be checked directly by counting the order of the groups. We finally verify that $S\pi$ is always surjective. Let $\varphi \in SO(q)$. We have to show that $C(\varphi) = i_u$ for some $u \in C_0^\bullet$. If Dim$V$ is even and $Z(q)$ is a field, then C_0 is *c.s.* over $Z(q)$, $C(\varphi)|_{C_0}$ is $Z(q)$–linear so by Skolem–Noether $C(\varphi)|_{C_0} = i_u$, $u \in C_0^\bullet$. If $Z(q) = K \times K$, we apply Skolem–Noether componentwise to get $C(\varphi)|_{C_0} = i_u$, $u \in C_0^\bullet$. On the other hand $C(\varphi) = i_v$ for $v \in C^\bullet$ since C is *c.s.* We have $i_v|_{C_0} = i_u$, hence $u = \delta v$ for $\delta \in Z(q)^\bullet$ and we may assume that $v \in C_0$. A similar argument works for the odd dimensional case since $Z(q)$–automorphisms of C are inner by the generalization of Skolem-Noether mentioned in Remark 12 of Chapter 2.

Let $\varphi \in SO(q)$. By Proposition 6 there exists $u \in S\Gamma(q)$ such that $C(\varphi) = i_u$ and by Lemma 4 $\mu(u) \in K^\bullet$. We call the class of $\mu(u)$ in $K^\bullet/K^{\bullet 2}$ the *spinor norm* of φ and denote it by $SN(\varphi)$. The element $SN(\varphi)$ does not depend on the choice of u such that $C(\varphi) = i_u$. If $i_u = i_v$, then $u = \lambda v$, $\lambda \in K^\bullet$ and $\mu(u) = \lambda^2\mu(v)$. Let now

$$\mathrm{Spin}(q) = \{u \in S\Gamma(q) \mid \mu(u) = 1\}.$$

Theorem 7. The sequence

$$1 \to \{\pm 1\} \to \mathrm{Spin}(q) \stackrel{S\pi}{\to} SO(q) \stackrel{SN}{\to} K^\bullet/K^{\bullet 2}$$

is exact.

Proof. Obvious by the definition of $S\pi$ and SN.

Even if its definition looks quite complicated, the group $\mathrm{Spin}(q)$ is very useful. Moreover, Theorem 7 shows that $\mathrm{Spin}(q)$ is a good "approximation" of $SO(q)$. As we shall see later, for low dimensions, the group $\mathrm{Spin}(q)$ is easier to compute than $SO(q)$. As an algebraic group it is connected and simply connected if q is of dimension ≥ 3. There are also topological reasons to introduce $\mathrm{Spin}(q)$. If $(V, q) = (\mathbb{R}^n,\ \langle 1, \ldots, 1\rangle)$, $n \geq 3$, then $\mathrm{Spin}(q)$ is the universal covering of $SO(q)$.

Another classical group associated with a quadratic from (V, q) is its *group of similitudes*. We denote it by $GO(q)$. There is an exact sequence

$$1 \to O(q) \to GO(q) \stackrel{\lambda}{\to} K^\bullet,$$

where $\lambda(\varphi)$, $\varphi \in GO(q)$, is the multiplier of the similitude φ. Let $\{e_1, \ldots, e_n\}$ be a basis of V and let $\alpha = (b_q(e_i, e_j))$ be the matrix of the polar of q. Further let φ be the matrix of $\varphi \in GO(q)$. We have

$$\varphi^t \alpha \varphi = \lambda \alpha$$

so $\lambda^n = (\det\varphi)^2$. Thus, if n is odd, λ is a square, $\lambda = \mu^2$, and $\varphi' = \mu^{-1}\varphi$ is an isometry. It follows that there exists a direct product decomposition

$$GO(q) = O(q) \times K^\bullet \quad \text{if} \quad n \quad \text{is odd.}$$

By Lemma 10 of Chapter 5, similitudes of (V, q) induce automorphisms of C_0. Assume that $\mathrm{Dim}V$ is even. We say that a similitude φ is *special* if the induced automorphism $C_0(\varphi)$ of C_0 is $Z(q)$–linear, i.e. is the identity on the centre of C_0. We denote the group of special similitudes of (V, q) by $GO_+(q)$. It contains $SO(q)$ and $K^\bullet$ but is not a direct product of these groups. The computation of $GO_+(q)$ for nonsingular quadratic forms of dimension ≤ 6 over a field of characteristic not equal to 2 was done by Dieudonné in a paper of Acta Mathematica 1952 (see the bibliography). In the next chapters, we shall study forms of dimension ≤ 6 and in particular reprove Dieudonné's results in a characteristic–free way.

Chapter 7

Quadratic Forms of Dimension 2

Let (V, q) be nonsingular of dimension 2 and let $C = C_0 \oplus C_1$ be the Clifford algebra of q. We have $C_1 = V$, $C_0 = Z(q)$ and C is *c.s.* of dimension 4. Let σ be the standard involution of C (as a Clifford algebra) and σ_0 the standard involution of $Z(q)$. By Proposition 6 of Chapter 5, σ_0 is the restriction of σ to C_0. Further it is easy to check, using a basis of C given by the Poincaré–Birkhoff–Witt theorem, that $\sigma(x)x \in K$ for all $x \in C$. Hence σ is the standard involution of C as a quaternion algebra. Writing an element $x \in C$ as $x = v + y$, $v \in C_1 = V$ and $y \in C_0$, we have $\sigma(x) = -v + \sigma_0(y)$. Thus the reduced norm n of C is given by

$$n(x) = x\sigma(x) = -q(v) + n_0(y),$$

where n_0 is the norm of $C_0 = Z(q)$, and we have an orthogonal decomposition

$$(C, n) \simeq (V, -q) \perp (C_0, n_0). \tag{7.1}$$

Proposition 1. Two quadratic spaces of dimension 2 are isometric if and only if they have the same Witt invariants and the same Arf invariants.

Proof. Let q, q' be the two forms and let $C' = C_0' \oplus V'$ be the Clifford algebra of q'. From $w(q) = w(q')$, we get $C \simeq C'$ and from $a(q) = a(q')$, we get $C_0 \simeq C_0'$. The following lemma implies that $(C, n) \simeq (C', n)$ and $(C_0, n_0) \simeq (C_0', n_0)$, so that the claim is a consequence of Witt cancellation.

Lemma 2. Let A, B be algebras with standard involutions σ_A, σ_B. Any isomorphism $\varphi : A \tilde{\to} B$ of K–algebras is an isometry of the corresponding norms $n_A(x) = x\sigma_A(x)$, $n_B(y) = y\sigma_B(y)$.

Proof. The involution $\varphi\sigma_A\varphi^{-1}$ is a standard involution of B, hence by the uniqueness of standard involutions $\varphi\sigma_A\varphi^{-1} = \sigma_B$. Thus

$$n_B(\varphi(x)) = \varphi(x)\sigma_B(\varphi(x)) = \varphi(x)\varphi(\sigma_A(x)) = \varphi(n_A(x)) = n_A(x).$$

Example 3. Let Z be a separable quadratic algebra with standard involution σ_Z. We compute the Clifford algebra of its norm. By definition, we have $C(Z, n_Z) = (1, Z/K]$, where $(1, Z/K]$ is the algebra $Z \oplus uZ$ with the multiplication rules $u^2 = 1$ and $xu = u\sigma_Z(x)$. We define a K–linear map

$$\rho : Z \to \mathrm{End}_K(Z)$$

by $\rho(x)(y) = x\sigma_Z(y)$. Since $\rho(x)^2(y) = n_Z(x)y$, the map ρ induces a homomorphism $C(Z, n_Z) \to \mathrm{End}_K(Z)$, which is an isomorphism since $C(Z, n_Z)$ is *c.s.* over K. On the other hand, if $z \in Z$ is a generator such that $z^2 = z + r$ and if we take $\{1, z\}$ as a basis of Z, it is easy to check that $C_0(Z, n_Z) \simeq Z$. We get

$$C(Z, n_Z) \simeq \mathrm{End}_K(Z) \quad \text{and} \quad C_0(Z, n_Z) \simeq Z.$$

Thus, by Lemma 2 above and Lemma 10 of Chapter 5, two quadratic separable algebras are isomorphic if and only if their norms are similar.

Proposition 4. Let (V, q) be a quadratic space of dimension 2. Then

1) (V, q) is isotropic if and only if $Z(q) = C_0 \simeq K \times K$, i.e. its Arf invariant is trivial.

2) (V, q) represents 1 if and only if $C(q) \simeq M_2(K)$, i.e. its Witt invariant is trivial. In particular, $C(q)$ is a division algebra if and only if q does not represent 1.

Proof. 1) Assume that q represents some $\lambda \neq 0 \in K$ and let $x \in V$ with $q(x) = \lambda$. The map $C_0 \to C_1 = V$ defined by $c \mapsto xc$ is an isometry $(C_0, \lambda n_0) \tilde{\to} (V, q)$ since $q(xc) = -n(xc) = -xc\sigma(xc) = -x\sigma(x)n_0(c) = q(x)n_0(c)$. Thus the claim follows from Example 3 and the fact that q is hyperbolic if and only if λq is hyperbolic.
2) Assume that $C \simeq M_2(K)$. Then by Lemma 2,

$$(C, n) \simeq (M_2(K), \det) \simeq H(K^2).$$

Further, by Proposition 4 of Chapter 1, $(V, q) \perp (V, -q) \simeq H(K^2)$, so that (7.1) and Witt cancellation imply that $(V, q) \simeq (C_0, n_0)$. This shows that q represents

1. Conversely, if q represents 1, then $(V,q) \simeq (C_0, n_0)$ and the claim follows from Example 3.

Remark 5. The hyperbolic plane $H(K)$ obviously represents any element $\lambda \in K$. Hence if the Arf invariant of a quadratic space of dimension 2 is trivial, its Witt invariant is trivial. Example 3 shows that the converse is not true.

Proposition 1 can be weakend to the following

Proposition 6. Two quadratic spaces of dimension 2 are similar if and only if they have isomorphic even Clifford algebras, i.e. the same Arf invariants.

Proof. The claim follows from the fact that $(V,q) \simeq (C_0, \lambda n_0)$ if q represents the element λ.

We conclude this chapter by computing $\mathrm{Spin}(q)$ of a quadratic space (V,q) of dimension 2. We use freely the notations of Chapter 6. The norm of C as a Clifford algebra is the reduced norm of C, so that $\mu(x) \in K$ for all $x \in C$. Since $V = C_1$, we have

$$S\Gamma(q) = C_0^\bullet$$

and

$$\mathrm{Spin}(q) = \{x \in C_0 \mid n_0(x) = 1\}.$$

Lemma 7. Let $\varphi \in SO(q)$. Then

1) $C(\varphi)|_{C_0} = 1_{C_0}$.

2) $\varphi(x) = ux, \quad x \in V$, for some $u \in C_0^\bullet$ such that $n_0(u) = 1$. Conversely, let $\rho_u : x \to ux,\ x \in V$ and $u \in C_0$, then $\rho_u \in SO(q)$ if $n_0(u) = 1$. In particular, the map $u \mapsto \rho_u$ is an isomorphism

$$\mathrm{Spin}(q) \tilde{\to} SO(q).$$

Proof. 1) Follows from the definition of $SO(q)$, since C_0 is commutative. We prove 2). Let $v \in V$ be anisotropic and let $q(v) = \lambda \neq 0$. We have for $x \in V$, $C(\varphi)(x) = C(\varphi)(\lambda^{-1}v^2x) = \lambda^{-1}C(\varphi)(v)vx$ since $vx \in C_0$ and C_0 is invariant under $C(\varphi)$. The element $u = \lambda^{-1}C(\varphi)(v)v$ lies in C_0 and $\varphi(x) = C(\varphi)(x) = ux$. Since the map φ is an isometry $q(x) = q(\varphi(x)) = q(ux) = (ux)^2 = n_0(u)x^2 = n_0(u)q(x)$, hence $n_0(u) = 1$. Conversely let $u \in C_0^\bullet$ with $n_0(u) = 1$, then $\rho_u \in O(q)$. Since $\rho_u(x)\rho_u(y) = u\sigma(u)xy$ for $x, y \in V$, ρ_u induces the identity on $Z(q)$ and $\rho_u \in SO(q)$.

The map $S\pi : \mathrm{Spin}(q) \to SO(q)$ is given by $u \mapsto i_u$. We have $i_u(x) = uxu^{-1} = u\sigma_0(u)^{-1}x$ by Proposition 6 of Chapter 5. Since $n_0(u) = 1$, $u\sigma_0(u^{-1})$ $= u^2$ and $S\pi$ can be identified with $u \mapsto \rho_{u^2}$.

Remark 8. By Example 3 any separable quadratic K–algebra is the even Clifford algebra of a quadratic space of dimension 2. We claim that any *c.s.* K–algebra A of dimension 4 is the Clifford algebra of a quadratic space of dimension 2. As in the proof of Theorem 7, Chapter 3, we can find a separable quadratic K–algebra $B \subset A$ and an element $u \in B^\perp \subset A$ ($\perp$ with respect to the reduced norm of A) such that $A = B \oplus uB$, $u^2 = \lambda \in K^\bullet$ and $ub = \sigma_B(b)u$ for $b \in B$. By the universal property of the Clifford algebra the map $B \to A$, $b \mapsto (0, ub)$, extends to an isomorphism $C(B, \lambda n_B) \simeq A$.

Chapter 8

Quadratic Forms of Dimension 3

Let (V, q) be a $\frac{1}{2}$–regular form of dimension 3 with Clifford algebra $C = C_0 \oplus C_1$. By Proposition 5 of Chapter 5, C_0 is a *c.s.* K–algebra of dimension 4, hence a separable quaternion algebra, the centre $Z(q)$ of C is a quadratic K–algebra generated by an element $z \in C_1$ such that $z^2 = s \in K$ and the class of s in $K^\bullet/K^{\bullet 2}$ is the signed $\frac{1}{2}$–discriminant of q.

Example 1. Let A be a separable quaternion algebra (i.e. a *c.s.* K–algebra of dimension 4) with standard involution σ, trace tr, norm n and let

$$A' = \{x \in A \mid x + \sigma(x) = 0\}.$$

We claim that (A', n), is $\frac{1}{2}$–regular of dimension 3. By Remark 8 of Chapter 7, we can assume that A is the Clifford algebra of a space $[a, b]$. If $\{x, y\}$ is the corresponding basis, then A' has the basis $\{1 - 2xy, x, y\}$ and $(A', n) \simeq \langle 4ab - 1\rangle \perp [-a, -b]$ is $\frac{1}{2}$–regular, as claimed. The signed $\frac{1}{2}$–discriminant of (A', n) is the class of -1 in $K^\bullet/K^{\bullet 2}$. For $A = M_2(K)$, we get

$$A' = \{x \in M_2(K) \mid tr(x) = 0\} \simeq \langle -1\rangle \perp H(K).$$

We compute the Clifford algebra of $(A', -n)$. The signed $\frac{1}{2}$–discriminant is trivial. Let Z be the quadratic K–algebra generated by a symbol $\tilde{z}$ such that $\tilde{z}^2 = 1$. We define

$$\varphi : A' \to A \otimes Z$$

by $\varphi(a) = a \otimes \tilde{z}$ for $a \in A'$. For any $a \in A$, we have $a^2 - tr(a)a + n(a) = 0$, so that $a^2 = -n(a)$ if $a \in A'$ and $\varphi(a)^2 = -n(a)$. By the universal property of the Clifford algebra, φ induces a homomorphism (also called φ)

$$\varphi : C(A', -n) \to A \otimes Z.$$

Let $\{e_0, e_1, e_2\}$ be the basis $\{1, x, y\}$ (if char $K = 2$), resp. $\{xy, x, y\}$ (if char $K \neq 2$). The element $z = e_0(1 - 2e_1e_2)$ of Proposition 5, Chapter 5, is mapped to $1 \otimes \tilde{z}$ so that φ maps $C_0(A', -n)$ into A. Since $C_0(A', -n)$ is *c.s.* over K, φ restricts to an isomorphism $C_0(A', -n) \simeq A$ and is an isomorphism $C(A', -n) \tilde{\rightarrow} A \otimes Z$. Thus

$$C(A', -n) \simeq A \otimes Z, \qquad \text{where} \qquad Z = K[X]/(X^2 - 1)$$

and

$$C_0(A', -n) \simeq A.$$

We now use Example 1 to describe (V, q) in general. Let $C(q) = C_0 \otimes Z(q)$ and $z \in Z(q)$ as above. Since z is of degree 1, the homomorphism $\rho : x \mapsto zx$ maps V into C_0. Let σ be the standard involution of C as a Clifford algebra. Using a basis of C_0 given by the *P.B.W.* theorem, it is easy to check that $x\sigma(x) \in K$ for any $x \in C_0$. Hence σ is the standard involution of C_0 as a quaternion algebra. We get $\sigma(zx) = \sigma(x)\sigma(z) = -xz = -zx$ for $x \in V$, so that $\rho(V) \subset C'_0$. Since ρ is injective and V, C'_0 have the same dimension, ρ is an isomorphism $V \tilde{\rightarrow} C'_0$. Further, since $-n(zx) = (zx)^2 = x^2z^2 = sq(x)$, ρ is an isometry

$$(V, q) \simeq (C'_0, -sn).$$

We also have $V = \{x \in C_1 \mid \sigma(x) + x = 0\}$ since ρ^{-1} maps C'_0 to the set of elements $x \in C_1$ such that $\sigma(x) + x = 0$. Summarizing we get

Proposition 2. Let (V, q) be a $\frac{1}{2}$–regular form of dimension 3. Then

1) $V = \{x \in C_1 \mid x + \sigma(x) = 0\}$, where σ is the standard involution of C.

2) $(V, q) \simeq (C'_0, -sn)$, where $C'_0 = \{x \in C_0 \mid x + \sigma(x) = 0\}$ and $s \in K$ is such that $[s] = \frac{1}{2}\mathrm{disc}(q) \in K^\bullet/K^{\bullet 2}$.

Corollary 3. Two $\frac{1}{2}$–regular forms of dimension 3 are isometric if and only if they have same Witt invariants and same $\frac{1}{2}$–discriminants. They are similar if and only if they have same Witt invariants.

Proof. If suffices to notice that if A, B are two quaternion algebras then, by uniqueness of standard involutions, any homomorphism of algebras $\varphi : A \to B$ maps A' into B'.

Corollary 4. A $\frac{1}{2}$–regular form (V, q) of dimension 3 has trivial Witt invariant if, and only if, it is isotropic.

Proof. Since q is isotropic if and only if sq is isotropic for any $s \in K^\bullet$, we can assume that $(V, q) = (A', n)$ for some *c.s.* K–algebra A of dimension 4. Then $w(q) = [A]$ in $Br(K)$. If $[A] = 1$, then $A = M_2(K)$, and $A' = s\ell_2(K)$ is isotropic. Conversely, if (A', n) is isotropic, (A, n) is isotropic and $A = M_2(K)$.

Corollary 5. $C_0(q)$ is a division algebra if and only if (V, q) is anisotropic.

We now compute the special Clifford group, the spin group and the Lie algebra of (V, q). Since the norm μ of C_0 is the reduced norm n of C_0, $\mu(x) \in K$ for all $x \in C_0$. Similarly, we claim that $\mu(x) \in K$ for all $x \in C_1$. Writing $x = uz$ with $u \in C_0$, we have $\mu(x) = uz\sigma(uz) = -z^2\mu(u) \in K$. We now claim that $i_u(V) \subset V$ for all $u \in C_0^\bullet$. By Proposition 2, $V = \{x \in C_1 \mid x = -\sigma(x)\}$. We get $\sigma(i_u(x)) = \sigma(uxu^{-1}) = -\sigma(u)^{-1}x\sigma(u) = -uxu^{-1} = -i_u(x)$ since $u\sigma(u) \in K$. This shows that

$$S\Gamma(q) = C_0^\bullet \quad \text{and} \quad \mathrm{Spin}(q) = \{u \in C_0^\bullet \mid n(u) = 1\}.$$

For any *c.s.* K–algebra A, we denote the group of elements of $M_n(A)$ of reduced norm 1 by $SL_n(A)$,

$$SL_n(A) = \{x \in M_n(A) \mid n_{M_n(A)}(x) = 1\},$$

so $\mathrm{Spin}(q) = SL_1(C_0)$. By Proposition 2, we have $(V, q) \simeq (C_0', -sn)$, where $[s] = \frac{1}{2}\delta(q) \in K^\bullet/K^{\bullet 2}$, so that

$$SO(V, q) \simeq SO(V, sq) \simeq SO(C_0', -n).$$

We assume now that $(V, q) = (A', -n)$ for some quaternion algebra A. It follows from Example 1 that

$$C_0(V, q) = A \quad \text{and} \quad C = A \otimes Z$$

with Z generated by an element z of degree 1 such that $z^2 = 1$. If we identify $V \subset C_1$ with $zV \subset C_0$, then (V, q) is identified with $(A', -n)$ as a subset of $C_0 = A$.

The map

$$S\pi : SL_1(A) \to SO(A', -n) = SO(A', n)$$

is then given by $u \mapsto i_u$, where i_u is now viewed as an automorphism of C_0 (not C). Similarly

$$S\pi : S\Gamma(A', n) = A^\bullet \to SO(A', n)$$

is identified with $u \mapsto i_u$, $u \in A^\bullet$. The map i_u is indeed an isometry of A' since $n_A(uxu^{-1}) = n_A(x)$. Proposition 6 of Chapter 6 implies that

$$SO(q) \simeq C_0^\bullet / K^\bullet.$$

In particular

$$SO(A', n) \simeq A^\bullet / K^\bullet.$$

If the $\frac{1}{2}$–regular form (V, q) is anisotropic, C_0 is a division quaternion algebra D and

$$\mathrm{Spin}(q) \simeq SL_1(D), \qquad S\Gamma(q) \simeq D^\bullet.$$

If (V, q) is isotropic, $C_0 \simeq M_2(K)$,

$$\mathrm{Spin}(q) \simeq SL_2(K), \qquad S\Gamma(q) \simeq GL_2(K)$$

and

$$SO(q) \simeq PGL_2(K).$$

Let for example $(V, q) = (\mathbb{R}^3, \langle 1, 1, 1 \rangle) = (\mathbb{H}', n)$. We have $S\Gamma(q) = \mathbb{H}^\bullet$. Since the standard involution of $C_0 = \mathbb{H}$ as a Clifford algebra is the standard involution of $\mathbb{H}$ as a quaternion algebra, we get $SN(\varphi) > 0$ for any $\varphi \in SO(\mathbb{H}', n)$ (by definition $SN(\varphi) = n_{\mathbb{H}}(u)$, where $C(\varphi) = i_u$). It then follows from Theorem 7 of Chapter 6, that

$$S\pi : \mathrm{Spin}(\mathbb{H}', n) \to SO(\mathbb{H}', n)$$

is surjective. Therefore any $\varphi \in SO(\mathbb{H}', n)$ can be represented as $\varphi(x) = axa^{-1}$ with $a \in \mathbb{H}$ of reduced norm 1.

For the Lie algebra, we get

$$so(A', n) = A' = [A, A],$$

since $so(q) \subset [C_0, C_0]$ and both algebras have the same dimension.

Chapter 9

Quadratic Forms of Dimension 4

Let (V, q) be a quadratic space of dimension 4 over K. The Clifford algebra $C = C_0 \oplus C_1$ is *c.s.* of dimension 16, the even Clifford algebra C_0 is of dimension 8, its centre $Z(q)$ is a separable quadratic K–algebra and C_0 is *c.s.* of dimension 4 over $Z(q)$ if $Z(q)$ is a field or $C_0 \simeq A \times A$ if $Z(q) = K \times K$, A *c.s.* of dimension 4 over K.

Example 1. Let A be a quaternion algebra with standard involution $a \mapsto \overline{a}$, norm n and let $\lambda \in K^\bullet$. The map

$$\varphi' : A \to M_2(A), \quad \varphi'(a) = \begin{pmatrix} 0 & \overline{a} \\ \lambda a & 0 \end{pmatrix}, \qquad a \in A$$

induces a graded homomorphism $\varphi : C(A, \lambda n) \to M_2(A)$, which must be an isomorphism by Lemma 8 of Chapter 2. If we identify both algebras through φ, we get $C_0(A, \lambda n) = A \times A$, $Z(A, \lambda n) = K \times K$ and the standard involution σ of $C(A, \lambda n)$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & -\lambda^{-1}\overline{c} \\ -\lambda\overline{b} & \overline{d} \end{pmatrix}.$$

since its restriction to $\varphi'(A)$ is -1. The canonical involution σ' corresponds to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \lambda^{-1}\overline{c} \\ \lambda\overline{b} & \overline{d} \end{pmatrix}.$$

Both involutions σ and σ' are of even symplectic type, since they are the tensor product of the standard involution of A with the involutions

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \mapsto \begin{pmatrix} x & -\lambda^{-1}u \\ -\lambda y & v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -\lambda \end{pmatrix} \begin{pmatrix} x & y \\ u & v \end{pmatrix}^t \begin{pmatrix} 1 & 0 \\ 0 & -\lambda^{-1} \end{pmatrix}$$

resp.

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} \mapsto \begin{pmatrix} x & \lambda^{-1}u \\ \lambda y & v \end{pmatrix},$$

which are of orthogonal type. Since there is a field extension $K \subset L$ such that

$$L \otimes (V, q) \simeq H(L^2) \simeq (M_2(L), \det),$$

the standard involution and the canonical involution of $C(V, q)$, V a quadratic space of dimension 4, are of even symplectic type. Since $C(A, n) \simeq M_2(A)$ and $Z(A, n) = K \times K$, the Witt invariant of (A, n) is the class of A in $Br(K)$ and the Arf invariant of (A, n) is trivial. Let A, B be quaternion algebras and

$$\psi : (A, n) \to (B, n)$$

a similitude with multiplier λ. By the above computations and Lemma 10 of Chapter 5, ψ induces an isomorphism

$$\psi' : A \times A = C_0(A, n) \tilde{\to} C_0(B, n) = B \times B.$$

Since A and B are *c.s.* algebras, it follows that $A \tilde{\to} B$. This, together with Lemma 2 of Chapter 7, shows that two quaternion algebras are isomorphic if and only if they have similar norms.

The centre $Z(q)$ of C_0 is either a quadratic field extension of K or $Z(q) \simeq K \times K$. In the first case C_0 is a quaternion algebra over $Z(q)$ and in the second $C_0 \simeq A \times A$ as a $K \times K$–algebra (see Theorem 8 of Chapter 4). In both cases C_0 has a standard $Z(q)$–linear involution (the componentwise involution in the second case).

Lemma 2. The standard $Z(q)$–linear involution of C_0 as a quaternion algebra is the restriction to C_0 of the standard involution σ of C. Further, $x\sigma(x) \in Z(q)$ for any $x \in C_1$.

Proof. There exists a field extension $K \subset L$ such that $L \otimes (V, q) \simeq H(L^2) \simeq (M_2(L), \det)$. Thus by uniqueness of the standard involution, we may assume that $(V, q) = (A, n)$ for the algebra $A = M_2(K)$. The first claim then follows from the formula for the involution given in example 1. For the second claim we may also assume that $(V, q) = (A, n)$. Let $x = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$ be an element of $C_1 = \left(\begin{smallmatrix} 0 & A \\ A & 0 \end{smallmatrix}\right)$. We have

$$x\sigma(x) = \begin{pmatrix} -\lambda b\bar{b} & 0 \\ 0 & -\lambda^{-1}c\bar{c} \end{pmatrix} \in \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix} = Z(q),$$

as claimed.

Let $n : C_1 \to Z(q)$ be the quadratic map defined by $n(x) = x\sigma(x)$. Even if $Z(q)$ is not necessarily a field, we can view $Z(q) \otimes (V, q)$ in an obvious way as a quadratic space over $Z(q)$.

Lemma 3. The multiplication in C induces an isometry $\psi : Z(q) \otimes (V, q) \simeq (C_1, -n)$. In particular $Z(q) \otimes (V, q)$ is similar to (C_0, n).

Proof. Let $y \in Z(q)$ and $v \in V$. Since $n(yv) = yv\sigma(yv) = -y^2 q(v)$, the map ψ is a morphism of quadratic spaces. Further ψ is injective because $Z(q) \otimes (V, q)$ is nonsingular. Comparing dimensions shows that ψ is an isomorphism. The last claim follows by choosing some $v \in V$ anisotropic and observing that the map $c \mapsto vc$, $c \in C_0$, is a similitude $(C_0, n) \to (C_1, n)$ with multiplier $-q(v) \neq 0$.

Assume that the Arf invariant of (V, q) is not trivial, i.e. $Z(q)$ is a quadratic field extension L of K. It follows from Lemma 3 that C_0 is a quaternion division algebra over L if and only if $L \otimes (V, q)$ is anisotropic and that $C_0 \simeq M_2(L)$ if and only if $L \otimes (V, q)$ is isotropic. On the other hand we claim that $L \otimes (V, q)$ is anisotropic if and only if (V, q) is anisotropic. Assume that $L \otimes (V, q)$ is isotropic and that (V, q) is anisotropic. Let z be a generator of L such that $z^2 = z + r$, $r \in K$ and let $u + zv \neq 0 \in L \otimes V$, u, $v \in V$ be such that $q(u + zv) = 0$. We have

$$q(u) + rq(v) = 0 \quad \text{and} \quad b_q(u, v) + q(v) = 0.$$

Let $s = q(v)$, $s \neq 0$ since q is anisotropic. We get

$$\begin{pmatrix} b_q(u,u) & b_q(u,-v) \\ b_q(-v,u) & b_q(-v,-v) \end{pmatrix} = \begin{pmatrix} -2rs & s \\ s & 2s \end{pmatrix}$$

and $\det\left(\begin{smallmatrix} -2rs & s \\ s & 2s \end{smallmatrix}\right) = -s^2(1 + 4r) \neq 0$. Therefore u, $-v$ are linearly independent and $q|_U$, $U = Ku \oplus K(-v)$, is nonsingular. The form $q|_U$ is isometric to (L, sn) where n is the norm of L, so there exists an orthogonal decomposition

$$(V, q) \simeq (L, sn) \perp (V', q').$$

By Example 3 of Chapter 7 and Lemma 10 of Chapter 5, the Arf invariant of (L, sn) is L. Since L is also the Arf invariant of (V, q), (V', q') must have trivial Arf invariant (consider the cases char $K \neq 2$ and char $K = 2$ separately). By Proposition 4 of Chapter 7, (V', q') is isotropic, hence (V, q) is isotropic. This is a contradiction. Summarizing, we get

Proposition 4. Let (V, q) be a quadratic space of dimension 4 with nontrivial Arf invariant L. Then

1) $C_0(q)$ is a quaternion division algebra over L if and only if (V, q) is anisotropic.
2) $C_0(q) \simeq M_2(L)$ if and only if (V, q) is isotropic.

Proposition 5. $V = \{x \in C_1 \mid x + \sigma(x) = 0\}$.

Proof. Let σ_0 be the standard involution of $Z(q)$ and let $\tilde{\sigma} = \psi(\sigma_0 \otimes 1)\psi^{-1}$, with ψ as in Lemma 3. We get

$$V = \{x \in C_1 \mid \tilde{\sigma}(x) = x\}$$

by Lemma 3 (and Galois descent!). But $\tilde{\sigma}(yv) = \sigma_0(y)v = vy = -\sigma(yv)$ by Proposition 6 of Chapter 5, thus $\tilde{\sigma} = -\sigma$ and $V = \{x \in C_1 \mid x = -\sigma(x)\}$ as claimed.

We now put $Z(q) = Z$ and identify $Z \otimes V$ with C_1. Let $a,\ b \in C_0$ and $x \in C_1$. The map $x \mapsto ax\sigma(b)$ is a homomorphism

$$\gamma : C_0 \otimes_Z {}_{\sigma}C_0 \to \mathrm{End}_Z(Z \otimes V) = Z \otimes \mathrm{End}_K(V).$$

Lemma 6. 1) γ is an isomorphism and restricts by Galois descent to an isomorphism

$$\gamma : \mathrm{cor}(C_0) \tilde{\to} \mathrm{End}_K(V).$$

2) The involution $\mathrm{cor}(\sigma)$ of $\mathrm{cor}(C_0)$, induced by the standard involution σ of C_0, is such that

$$\gamma \mathrm{cor}(\sigma)\gamma^{-1}(f) = h_q^{-1} f^* h_q, \quad f \in \mathrm{End}_K(V),$$

where $h_q : V \tilde{\to} V^*$ is the adjoint of q and f^* is the transpose of f.

Proof. The map γ is an isomorphism, since it is a map between *c.s.* algebras of the same dimension over Z. We prove that $\mathrm{cor}(C_0) \simeq \mathrm{End}_K(V)$. Let $f = \gamma(\sum a_i \otimes b_i) \in \mathrm{End}_K(V)$. It suffices to check that $f = \gamma(\sum b_i \otimes a_i)$. Putting $\overline{x} = \sigma(x)$, we have, by

Proposition 5, $\overline{f(v)} = -f(v)$ for $v \in V$. Since $\overline{f(v)} = \sum \overline{a_i} \otimes \overline{b_i} = -\sum b_i \otimes \overline{a_i} = -f(v)$, we get $f = \gamma(\sum b_i \otimes a_i)$ as claimed. To prove 2), we verify that

$$(9.1) \qquad (\gamma(a \otimes b))^* \circ (1 \otimes h_q) = (1 \otimes h_q) \circ \gamma(\overline{a} \otimes \overline{b})$$

for $a,\ b \in C_0$. We have

$$(1 \otimes h_q)(x)(y) = b_q(x, y) = -(x\,\overline{y} + y\,\overline{x})$$

by Lemma 3, so that (9.1) reduces to

$$(9.2) \qquad x\sigma(ay\,\overline{b}) + ay\,\overline{b}\,\sigma(x) = \overline{a}\,xb\sigma(y) + y\sigma(\overline{a}\,xb)$$

for $a,\ b \in C_0,\ x,\ y \in C_1$. The left hand side of (9.2) is equal to $tr(xb\,\overline{y}\,\overline{a})$ and the right hand side to $tr(\overline{a}xb\overline{y})$, where tr is the reduced trace of C_0 as Z–algebra. Both sides are equal since $tr(uv) = tr(vu)$ for $u,\ v \in C_0$.

Theorem 7. Two quadratic spaces of dimension 4 over K are similar if and only if they have isomorphic even Clifford algebras.

Proof. If $q,\ q'$ are similar, then $C_0(q) \simeq C_0(q')$ by Lemma 10 of Chapter 5. Conversely, let $\varphi : C_0(q) \tilde{\to} C_0(q')$ be an isomorphism of K–algebras and let $Z = Z(q)$ be the centre of $C_0(q)$. Then φ induces an isomorphism $Z \tilde{\to} Z(q')$. We view $C_0' = C_0(q')$ as a Z–algebra through this isomorphism, so that φ is Z–linear. In view of the uniqueness of standard involutions, φ is an isomorphism of Z–algebras–with–involution. By Lemma 6, φ induces an isomorphism $\psi : \mathrm{End}_K(V) \to \mathrm{End}_K(V')$ such that $\psi \circ \gamma = \gamma' \circ \mathrm{cor}(\varphi)$, where $\gamma :\ \mathrm{cor}(C_0) \tilde{\to} \mathrm{End}_K(V),\ \gamma' : \mathrm{cor}(C_0') \tilde{\to} \mathrm{End}_K(V')$ are as in Lemma 6. Hence ψ is an isomorphism of algebras–with–involution. Fixing isomorphisms $\mathrm{End}_K(V) \simeq M_4(K),\ \mathrm{End}_K(V') \simeq M_4(K)$, we can write by Skolem–Noether, $\psi(f) = \rho f \rho^{-1}$ for some K–linear isomorphism $\rho : V \tilde{\to} V'$. Since ψ is an isomorphism of algebras–with–involution, we get

$$\rho h_q^{-1} f^* h_q \rho^{-1} = h_{q'}^{-1} (\rho\ f\ \rho^{-1})^* h_{q'}$$

for all $f \in \mathrm{End}_K(V)$. This implies that $\lambda \cdot h_{q'} = \rho^* h_q \rho$ for some $\lambda \in K^\bullet$. Therefore ρ is a similitude $(V, b_q) \tilde{\to} (V', b_{q'})$ of the polar forms. To check that ρ is in fact a similitude of the quadratic spaces, we observe that

1) the reduced trace $tr : C_0 \to Z$ induces an isomorphism

$$t : \mathrm{Hom}_{C_0}(Z \otimes M, C_0) \to \mathrm{Hom}_Z(Z \otimes M, Z),$$

where we view $Z \otimes M = C_1$ as a left C_0–module through multiplication in C.

2) $t^{-1} \circ (1 \otimes h_q)(v)(v) = 1 \otimes q(v) \quad \text{for} \quad v \in V$.

3) The reduced trace commutes with φ.

3) follows by uniqueness of the standard involution. 1) and 2) can easily be checked in the case $(V, q) = (A, n)$ (see Example 1) and the general case follows from the fact that there exists a field extension $K \subset L$ such that $L \otimes (V, q) \simeq H(L^2) = (M_2(L), \det)$.

Corollary 8. Two quadratic spaces of dimension 4 are similar if they have the same Witt and Arf invariants.

Proof. By Lemma 9 of Chapter 4, we have $[C_0(q)] = [Z(q) \otimes C(q)]$ in $Br(Z(q))$ (assume that $Z(q)$ is a field or do the necessary changes if $Z(q) = K \times K$!). Therefore $C_0(q) \simeq C_0(q')$ if $Z(q) \simeq Z(q')$ and $[C(q)] = [C(q')]$ in $Br(K)$.

Not any multiplier λ can occur in Corollary 8. We have:

Lemma 9. Let (V, q) be a quadratic space of even dimension. Then $w(q) = w(\lambda q)$ if and only if $\lambda = n_0(\xi)$, $\xi \in Z(q)^\bullet$ and n_0 is the norm of $Z(q)$.

Proof. If $\lambda = n_0(\xi)$, then $V \to C(q)$ given by $v \mapsto \xi v$ extends to an isomorphism $C(\lambda q) \tilde{\to} C(q)$. If $w(q) = w(\lambda q)$, then $w((\lambda, Z(q)/K]) = 1$ by Proposition 11 of Chapter 5. The map

$$Z(q) \to (\lambda, Z(q)/K] = Z(q) \oplus uZ(q)$$

given by $x \mapsto (0, ux)$ extends by the universal property of the Clifford algebra to an isomorphism

$$C(Z(q), \lambda n_0) \simeq (\lambda, Z(q)/K].$$

By Proposition 4 of Chapter 7, $C(Z(q), \lambda n_0) \simeq M_2(K)$ if and only if λn_0 represents

1, i.e. n_0 represents λ.

Remark 10. Let Z be a quadratic algebra and let B be a quaternion algebra over Z. By Lemma 6 a necessary condition for B to be isomorphic to the even Clifford algebra of a quadratic space of dimension 4 is that the class of the corestriction of B in $Br(K)$ is trivial. As shown in Knus–Parimala–Sridharan this condition is also sufficient.

Remark 11. As an application of Theorem 7, (and Example 1) we get that a quadratic space of dimension 4 and trivial Arf invariant is similar to the norm of a quaternion algebra. This could of course be easily checked directly.

To discuss the structure of C (in particular to give conditions under which C is a division algebra) we need some results of Chapter 11. We shall see in Proposition 8 of Chapter 11 that C is a division algebra if and only if $(Z(q), n_0) \perp (V, -q)$ is anisotropic.

We now compute the groups Spin(q), the Lie algebra $so(q)$ and $GO_+(q)$ for quadratic spaces of dimension 4. By definition the group Spin(q) is a subgroup of the group $SL_1(C_0)$ of units of C_0 of Clifford norm 1. We claim that in fact

$$\mathrm{Spin}(q) = SL_1(C_0).$$

We have to check that for any $u \in SL_1(C_0)$, $i_u(V) \subset V$. By Proposition 4, $V = \{x \in C_1 \mid x + \sigma(x) = 0\}$. We get

$$\sigma(i_u(x)) = \sigma(uxu^{-1}) = -\sigma(u^{-1})x\sigma(u) = -uxu^{-1},$$

since $u\sigma(u) = 1$. Thus $\sigma(i_u(x)) = -i_u(x)$ as claimed.

Assume now that (V, q) has trivial Arf invariant. As observed in Remark 11, (V, q) is similar to the reduced norm of a quaternion algebra A. Therefore, to compute Spin(q) and $SO(q)$, we may as well assume that $(V, q) = (A, n)$. As usual, we denote by $a \mapsto \bar{a}$ the standard involution of A. By Example 1,

$$C_0 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \subset M_2(A) = C$$

or $C_0 = A \times A$. The involution σ maps (a,b) to $(\overline{a},\ \overline{b})$. Since

$$V = \left\{ \begin{pmatrix} 0 & \overline{x} \\ x & 0 \end{pmatrix}, \quad x \in A \right\},$$

the condition $i_u(V) \subset V$ for $u \in C_0^\bullet$ is equivalent to $\overline{bxa^{-1}} = a\overline{x}\, b^{-1}$ for all $x \in A$. This, in turn, is equivalent with $n(a) = n(b)$. Thus

$$S\Gamma(q) = \{(a,b) \in A \times A \mid n(a) = n(b)\},$$

$$\mathrm{Spin}(q) = \{(a,b) \in A \times A \mid n(a) = n(b) = 1\} = SL_1(A) \times SL_1(A)$$

and the homomorphism $S\pi : S\Gamma(q) \to SO(q)$, resp. $\mathrm{Spin}(q) \to SO(q)$ is given by $S\pi(a,b)(x) = bxa^{-1}$. If $A = M_2(K)$, we get

$$\mathrm{Spin}(H(K^2)) = SL_2(K) \times SL_2(K).$$

If $A = I\!H$, the spinor norm of any $\varphi \in SO(I\!H, n)$ is trivial, so that by Theorem 7 of Chapter 6, any $\varphi \in SO(I\!H, n)$ can be represented as $\varphi(x) = bxa^{-1}$ for a, b quaternions of norm 1. In general, by Proposition 6 of Chapter 6 and the above computation of $S\Gamma(q)$, any $\varphi \in SO(A, n)$ can be written as $\varphi(x) = bxa^{-1}$ for elements $a,\ b \in A$ of equal norm. We recall that $A = M_2(K)$ if (V,q) is isotropic and A is a division algebra if (V,q) is anisotropic.

If the Arf invariant of (V,q) is not trivial, the centre of $C_0(q)$ is a quadratic field extension L of K and C_0 is a quaternion algebra over L. Thus C_0 is either a division algebra over L or $C_0 \simeq M_2(L)$. By Proposition 4 the first case occurs if (V,q) is anisotropic and the second if (V,q) is isotropic. Therefore

$$\mathrm{Spin}(V,q) \simeq SL_2(L)$$

if (V,q) is isotropic and

$$\mathrm{Spin}(V,q) \simeq SL_1(B),$$

with $B = C_0$ a division algebra over L if (V,q) is anisotropic. We claim that

$$B \simeq L \otimes B_0,$$

B_0 a division algebra over K. By Lemma 5, $\mathrm{cor}(B)$ is trivial. By the theorem of Albert–Riehm (Theorem 11 of Chapter 3), B admits an involution τ of the second kind, i.e. such that its restriction to L is the standard involution σ_0 of L. Now $\tau\sigma\tau$

is an involution of B which is L–linear and such that $\tau\sigma\tau(x)\cdot x \in L$ for all $x \in B$, since $\sigma\tau(x)\cdot\tau(x) \in L$. In view of the uniqueness of the standard involution σ, we get $\tau\sigma\tau = \sigma$ or $(\tau\sigma)^2 = 1$. The map $\tilde{\sigma} = \tau\sigma : B \to B$ is σ_0–semilinear. By Galois descent, we have $B \simeq L \otimes B_0$ with $B_0 = \{x \in B \mid \tilde{\sigma}(x) = x\}$. One could also construct B_0 such that $B = L \otimes B_0$ using a basis of V: Assume that $(V, q) = [a, b] \perp [c, d]$ and let $\{x_1, y_1, x_2, y_2\}$ be a corresponding basis of V. Then

$$z = x_1y_1 + x_2y_2 - 2x_1y_1x_2y_2$$

is a generator of L and the elements $x_1y_1,\ x_1x_2, y_1x_2$ generate a subalgebra B_0 of dimension 4 over K. It can be checked that $L \otimes B_0 = C_0$, so B_0 is *c.s.* over K.

The computation of the Lie algebra $so(q)$ is simple. We have $so(q) \subset C_0' = [C_0, C_0]$ in general. Since

$$C_0' = \{x \in C_0 \mid x + tr(x) = 0\}$$

is of dimension 3 over Z, we must have

$$so(q) = C_0' = \{x \in C_0 \mid x + tr(x) = 0\}.$$

We finally compute the group of special similitudes $GO_+(q)$ of a quadratic space of dimension 4. Let

$$\rho : K^\bullet \times C_0^\bullet \to GO(q)$$

be defined by $\rho(\nu, u)(x) = \nu^{-1}ux\overline{u}$. Since $M = \{x \in C_1 \mid x + \bar{x} = 0\}$ (see (4.2.3)), $\rho(\nu, a)(x)$ is a linear automorphism of V for all $a \in C_0^\bullet$, $\nu \in R^\bullet$. Further it follows from

$$\begin{aligned} q(\rho(\nu,a)(x)) &= (\rho(\nu,a)(x))^2 \\ &= \nu^{-2}ax\bar{a}ax\bar{a} \\ &= \nu^{-2}a\sigma_0(\mu(a))q(x)\bar{a} \\ &= \nu^{-2}n_0(\mu(a))q(x) \end{aligned}$$

that $\rho(\nu, a)$ is a similitude with multiplier $\nu^{-2}n_0(\mu(a))$, where $\mu(a) = a\bar{a} \in Z$ (see (4.1.1)). We now check that $\rho(\nu, a) \in \mathrm{GO}_+(q)$. We have for all elements x, y of V

$$\begin{aligned} \rho(\nu,a)(x)\rho(\nu,a)(y) &= \nu^{-2}ax\bar{a}ay\bar{a} \\ &= \nu^{-2}a\sigma_0(\mu(a)xy\bar{a} \\ &= \nu^{-2}\mu(a)\sigma_0(\mu(u)axya^{-1} \\ &= \nu^{-2}n_0(\mu(a))axya^{-1} \end{aligned}$$

Since the products xy, $x, y \in V$, generate the algebra C_0, we see that the extension $C_0(\rho(\nu, a))$ to C_0 of the similitude $\rho(\nu, a)$ is the inner conjugation i_a by a. Thus $C_0(\rho(\nu, a))$ is Z–linear and, by definition, $\rho(\nu, a)$ is a special similitude. We now claim that the kernel of ρ is the subgroup

$$\{(n_0(z), z) \in K^\bullet \times Z^\bullet |\, z \in Z^\bullet\}$$

of $K^\bullet \times C_0^\bullet$. It follows from $\rho(\nu, a)) = 1$ that $C_0(\rho(\nu, a)) = i_a = 1_{C_0}$ and a is an element of the centre Z of C_0. We have $a = \bar{a}$ for $a \in Z$. Thus $\rho(\nu, a)(x) = x$ implies $\nu^{-1} a\sigma_0(a)x = \nu^{-1} n_0(a)x = x$ for all $x \in V$. Since V is nonsingular, we get $n_0(a) = \nu$ as claimed. We finally claim that ρ is surjective. Let $Z = Z(q)$. For any Z–module M, let ${}_{\sigma_0}M$ be the Z–module M with the action of Z twisted through σ_0. The subset E of $M_2(C)$ consisting of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} {}_{\sigma_0}C_0 & {}_{\sigma_0}C_1 \\ C_1 & C_0 \end{pmatrix}$$

is a Z–algebra. The map

$$Z \otimes V \to E, \quad x \mapsto \begin{pmatrix} 0 & x \\ x & 0 \end{pmatrix},$$

extends by the universal property of the Clifford algebra to a homomorphism $Z \otimes C \to E$, which is an isomorphism since both algebras have the same dimension and C is *c.s.* over K. We use it to identify $Z \otimes C$ with E. The standard involution of $Z \otimes C$ is

$$\sigma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$$

since σ restricted to $Z \otimes V = \{\left(\begin{smallmatrix} 0 & x \\ x & 0 \end{smallmatrix}\right),\ x \in Z \otimes V\}$ is $-1_{Z\otimes V}$. Let $f \in GO_+(q)$ with multiplier μ. The map

$$\begin{pmatrix} 0 & -\overline{x} \\ x & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & \mu^{-1} f(x) \\ f(x) & 0 \end{pmatrix}, \quad x \in V,$$

extends by the universal property of the Clifford algebra to an automorphism φ of $Z \otimes C$. It is easy to check that the restriction φ' of φ to

$$Z \otimes C_0 = \begin{pmatrix} {}_{\sigma}C_0 & 0 \\ 0 & C_0 \end{pmatrix}$$

is the automorphism $C_0(1 \otimes f)$. By Skolem–Noether (and Remark 12 of Chapter 2), $\varphi = i_u$ for some $u \in (Z \otimes C)^\bullet$. Since $f \in GO_+(q)$, $\varphi' = C_0(1 \otimes f)$ is

$Z \otimes Z$–linear, hence we also have $\varphi' = i_v, \quad v \in (Z \otimes C_0)^\bullet$. Since $i_v = i_u$ on $Z \otimes C_0 \quad u = rv, \ \ r \in Z \otimes Z = \left(\begin{smallmatrix} Z & 0 \\ 0 & Z \end{smallmatrix}\right)$ and $u \in (Z \otimes C_0)^\bullet$. Let $u = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in (Z \otimes C_0)^\bullet$, so that $f(x) = dxa^{-1}$. Since $V = \{x \in C_1 \mid x + \overline{x} = 0\}$ we get $dxa^{-1} = \overline{a}^{-1}x\overline{d}$ for all $x \in V$ or $cx = x\overline{c}$ with $c = \overline{a}d$. It follows that $cx \in V$ for all $x \in V$. Thus we get $(cx)^2 = cxx\bar{c} = c\bar{c}q(x) \in K^\bullet$ for all $x \in V$, so that $c\bar{c} \in K^\bullet$. Since also $\bar{c}xc \in V$, we have $c\bar{c}xc = \bar{c}xc\bar{c}$, hence $xc = \bar{c}x$ for all $x \in V$. It follows from $xyc = x\bar{c}y = cxy$ that $c \in Z$ and, since $\bar{c} = c$ for $c \in Z$, that $xc = cx$ for all $x \in V$. This finally implies that $c \in K^\bullet$, let $c = \nu$, so that $a = \nu\overline{d}^{-1}$ and $f(x) = \nu^{-1}dx\overline{d}$ for $d \in C_0$, as claimed. Summarizing, we get

Theorem 12. Let (V,q) be a quadratic space of dimension 4 with Clifford algebra $C = C_0 \oplus C_1$. The homomorphism $K^\bullet \times C_0^\bullet \to GO(q), \ \ (\nu, u) \mapsto \rho(\nu,u)(x) = \nu^{-1}ux\overline{u}$ induces an isomorphism

$$K^\bullet \times C_0^\bullet / \{(n_0(\xi), \xi), \ \xi \in Z^\bullet\} \tilde{\to} GO_+(q),$$

where Z is the centre of C_0.

We describe some special cases of Theorem 12. If (V,q) has trivial Arf invariant, we have $GO_+(q) \simeq GO_+(A,n)$ for some quaternion algebra A, since (V,q) is similar to (A,n). Then

$$C_0^\bullet = A^\bullet \times Z^\bullet, \quad Z^\bullet = K^\bullet \times K^\bullet \quad \text{and} \quad n_0(Z^\bullet) = K^\bullet,$$

so

$$GO_+(q) \simeq A^\bullet \times A^\bullet / \{(\lambda,\lambda), \quad \lambda \in K^\bullet\}.$$

In particular

$$GO_+(q) \simeq GL_2(K) \times GL_2(K) / \{(\lambda,\lambda), \quad \lambda \in K^\bullet\}$$

if further (V,q) is isotropic, i.e. $(V,q) = H(K^2)$.

If the Arf invariant of (V,q) is not trivial, Z is a quadratic field extension of K and $Z \otimes (V,q)$ is similar to a quaternion algebra (B,n) over Z. Then

$$GO_+(q) = K^\bullet \times B^\bullet / \{(n_0(z), z), \ \ z \in Z^\bullet\},$$

where B is a division algebra if (V,q) is anisotropic and $B = M_2(Z)$ if (V,q) is isotropic. In this case

$$GO_+(q) = K^\bullet \times GL_2(Z)/\{(n_0(z), z), \quad z \in Z^\bullet\}.$$

Chapter 10

The Pfaffian

We first recall the definition and some properties of the *pfaffian* of an alternating matrix and then define a reduced pfaffian for *c.s.* algebras. Let $x_{ij},\ \ 1 \le i < j \le 2m$ be indeterminates and let $x_{ji} = -x_{ij}$ for $i < j,\ \ x_{ii} = 0,\ \ i = 1, \dots, 2m$. The matrix $\xi = (x_{ij})$ with entries in $\mathbb{Z}[x_{ij}]$ is called the *generic alternating* $(2m \times 2m)$*–matrix*. In view of Lemma 2 of Chapter 3 its determinant is a square in $\mathbb{Q}(x_{ij})$. Since $\det\xi \in \mathbb{Z}[x_{ij}]$ and $\mathbb{Z}[x_{ij}]$ is integrally closed in $\mathbb{Q}(x_{ij})$, $\det\xi$ is the square of a polynomial $pf(\xi)$ in $\mathbb{Z}[x_{ij}]$. The polynomial $pf(\xi)$ is uniquely determined up to a factor ± 1. We normalize $pf(\xi)$ by requiring that $pf(s_m) = 1$ for $s_m = \mathrm{diag}(\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \dots, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right))$. In particular, $pf(\xi)$ is homogeneous of degree m, i.e. $pf(\lambda\xi) = \lambda^m pf(\xi)$ for $\lambda \in K$. For example, we get

$$pf \begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} \\ & 0 & x_{23} & x_{24} \\ & & 0 & x_{34} \\ & & & 0 \end{pmatrix} = x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}.$$

Let now K be a field and $\mathbb{Z}[x_{ij}] \to K[x_{ij}]$ be induced by the unique homomorphism $\mathbb{Z} \to K$. Specializing $\xi \mapsto \alpha$ for any alternating $(2m \times 2m)$–matrix α, we get

$$\det(\alpha) = pf(\alpha)^2.$$

Lemma 1. For any $\alpha \in \mathrm{Alt}_{2m}(K)$ and $\nu \in M_{2m}(K)$, we have

$$pf(\nu^t \alpha \nu) = \det(\nu) pf(\alpha).$$

Proof. It suffices to verify the claim over $\mathbb{Z}$ for α and ν generic matrices (i.e. with indeterminates a_{ij} for α and u_{ij} for ν as entries). We have $pf(\nu^t\alpha\nu)^2 = \det(\nu^t\alpha\nu) = \det(\nu)^2 pf(\alpha)^2$ over the polynomial ring $\mathbb{Z}[a_{ij}, u_{ij}]$, so that $pf(\nu^t\alpha\nu) = \pm\det(\nu)pf(\alpha)$ and the sign $\pm$ is independent of the choice of α and ν. Specializing ν to the identity matrix shows that the sign + must hold.

Let A be a *c.s.* K–algebra of dimension $4m^2$ with a K–linear involution τ. We assume that either τ is of even symplectic type or that A is isomorphic as an algebra with involution to the tensor product of two quaternion algebras with the involution given by the tensor product of the two standard involutions. For example $M_4(K)$, with the involution $x \mapsto x^t$, is isomorphic to such a tensor product. Let ε be the type of τ and let

$$\mathrm{Alt}^\tau(A) = \{x - \varepsilon\tau(x), \ \ x \in A\}$$

be the set of alternating elements of A. We claim that there exists a *reduced pfaffian* $pf_A : \mathrm{Alt}^\tau(A) \to K$ such that

$$pf_A(x)^2 = n_A(x) \quad \text{and} \quad pf_A(\tau(a)xa) = n_A(a)pf_A(x)$$

for $x \in \mathrm{Alt}^\tau(A)$, $\ a \in A$, n_A denoting the reduced norm of A. We first consider the case where τ is of even symplectic type. Let $\alpha : L \otimes A \tilde{\to} M_{2m}(L)$ be a Galois splitting of A. The involution $\alpha(1 \otimes \tau)\alpha^{-1}$ of $M_{2m}(L)$ is of the form $\tau_u(x) = ux^tu^{-1}$ with $u \in GL_{2m}(K)$ an alternating matrix. In view of Lemma 2 of Chapter 3, we can modify α by an inner automorphism of $M_{2m}(L)$ in such a way that u is the matrix s_m defined above.We get by Lemma 1 of Chapter 3,

$$\begin{aligned}\alpha(L \otimes \mathrm{Alt}^\tau(A)) &= \mathrm{Alt}_{2m}^{\tau_u}(L) \\ &= s_m \cdot \mathrm{Alt}_{2m}(L) = \mathrm{Alt}_{2m}(L) \cdot s_m^{-1}\end{aligned}$$

and we define

$$pf_A(a) = pf(\alpha(1 \otimes a)s_m) \quad \text{for} \quad a \in \mathrm{Alt}^\tau(A).$$

We first check that $pf_A(a) \in K$ of all $a \in \mathrm{Alt}^\tau(A)$. For any $g \in \mathrm{Gal}(L/K)$, let $\tilde{g} : M_{2m}(L) \to M_{2m}(L)$ be given by $\tilde{g}((a_{ij})) = (g(a_{ij}))$ i.e. $\tilde{g}$ acts entrywise. The map $\alpha(g \otimes 1)\alpha^{-1}\tilde{g}^{-1}$ is an L–automorphism of $M_{2m}(L)$ which respects the involution $\alpha(1 \otimes \tau)\alpha^{-1}$ of $M_{2m}(L)$. Hence there is $c \in GL_{2m}(L)$ such that

$$\alpha(g \otimes 1)\alpha^{-1}(x) = c\tilde{g}(x)c^{-1} \quad \text{for all} \quad x \in M_{2m}(L)$$

and $\lambda s_m = cs_mc^t$ for some $\lambda \in L^\bullet$. We have

$$pf_A(a) = pf(\alpha(1 \otimes a)s_m) = pf(c\tilde{g}(\alpha(1 \otimes a))c^{-1}s_m)$$

since $\alpha(g \otimes 1)\alpha^{-1}(\alpha(1 \otimes a)) = \alpha(1 \otimes \alpha)$. On the other hand $c^{-1}s_m = \lambda^{-1}s_m c^t$, so that

$$\begin{aligned} pf_A(a) &= pf(\lambda^{-1}c\tilde{g}(\alpha(1 \otimes a))s_m c^t) \\ &= \lambda^{-m}\det(c)pf(\tilde{g}(\alpha(1 \otimes a))s_m). \end{aligned}$$

We get $\lambda^m = \det(c)$ by taking the pfaffian of $\lambda s_m = cs_m c^t$ and

$$\begin{aligned} pf(\tilde{g}(\alpha(1 \otimes a))s_m) &= pf(\tilde{g}(\alpha(1 \otimes a)s_m)) \\ &= g(pf(\alpha(1 \otimes a)s_m)) = g(pf_A(a)), \end{aligned}$$

since s_m is defined over K. This shows that $pf_A(a) \in K$. To verify that pf_A is independent of the choice of the splitting (L, α), it suffices (as for the characteristic polynomial) to consider splittings (L, α) and (L, α') (i.e. the same field L). Let $\alpha' = i_y \circ \alpha,\ y \in GL_{2m}(L)$. Since $\alpha(1 \otimes \tau)\alpha^{-1}$ and $\alpha'(1 \otimes \tau)\alpha'^{-1}$ give the involution τ_{s_m} of $M_{2m}(L)$, we get by the discussion between Lemma 1 and Lemma 2 of Chapter 3, $\lambda s_m = ys_m y^t$ for some $\lambda \in L^\bullet$. Let now pf_A be the pfaffian defined through α and pf'_A the pfaffian defined through α'. We have

$$\begin{aligned} pf'_A(a) &= pf(\alpha'(1 \otimes a)s_m) = pf(y\alpha(1 \otimes a)y^{-1}s_m) \\ &= pf(\lambda^{-1}y\alpha(1 \otimes a)s_m y^t) = \lambda^{-m}\det(y)pf(\alpha(1 \otimes a)s_m) \\ &= pf_A(a) \end{aligned}$$

since $\lambda s_m = ys_m y^t$ implies $\lambda^m = \det(y)$ (take the pfaffian on both sides). The formulas

$$pf_A(x)^2 = n_A(x) \quad \text{and} \quad pf_A(\tau(a)xa) = n_A(a)pf_A(x)$$

follow from

$$pf_A(x)^2 = pf(\alpha(1 \otimes x)s_m)^2 = \det(\alpha(1 \otimes x)s_m) = \det(\alpha(1 \otimes x)) = n_A(x)$$

and

$$\begin{aligned} pf_A(\tau(a)xa) &= pf(s_m\alpha(1 \otimes a)^t s_m^{-1}\alpha(1 \otimes x)\alpha(1 \otimes a)s_m) \\ &= pf((s_m^{-1}\alpha(1 \otimes a)s_m)^t\alpha(1 \otimes x)s_m(s_m^{-1}\alpha(1 \otimes a)s_m)) \\ &= \det(\alpha(1 \otimes a))pf(\alpha(1 \otimes x)s_m) \\ &= n_A(a)pf_A(x). \end{aligned}$$

Further we have $pf_A(\lambda a) = \lambda^m pf_A(a)$ for $\lambda \in K$ and $pf_A(1) = pf(s_m) = 1$ (we observed earlier that $1 \in \mathrm{Alt}^\tau(A)$ if τ is of even symplectic type).

We now define the reduced pfaffian pf_A for $A = A_1 \otimes A_2,\ \ A_1,\ A_2$ quaternion algebras and $\tau = \sigma_1 \otimes \sigma_2$ the tensor product of the standard involutions σ_i of A_i. We observe that τ is of orthogonal type since $\sigma_1,\ \sigma_2$ are of symplectic type. Let $\alpha_i : L \otimes A_i \tilde{\to} M_2(L)$ be a splitting of $A_i,\ \ i = 1, 2$ (we can choose the same L for both algebras). Then $\alpha = \alpha_1 \otimes \alpha_2$ is a splitting of A and $\alpha(1 \otimes \tau)\alpha^{-1}$ is the tensor product of two copies of the involution

$$\xi = \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} v & -y \\ -u & x \end{smallmatrix}\right) = s_1 \xi^t s_1^{-1}.$$

Thus $\alpha(L \otimes \mathrm{Alt}^\tau(A)) = (s_1 \otimes s_1)\mathrm{Alt}_4(L) = \mathrm{Alt}_4(L)(s_1 \otimes s_1)^{-1}$, where

$$s_1 \otimes s_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and we define

$$pf_A(a) = pf(\alpha(1 \otimes a)(s_1 \otimes s_1)) \quad \text{for} \quad a \in \mathrm{Alt}^\tau(A).$$

As in the case of even symplectic involutions, one checks that $pf_A(a) \in K$ for all $a \in \mathrm{Alt}^\tau(A)$ and that pf_A does not depend on the choice of the splitting α (α always of the form $\alpha_1 \otimes \alpha_2$!) One has to use that $\det(u_1 \otimes u_2) = (\det u_1 \cdot \det u_2)^2$ for $u_i \in GL_2(L)$. We leave the details as an exercise.

Let now A be a *c.s.* algebra of dimension 16 with an involution τ which is either of even symplectic type or $A = A_1 \otimes A_2$ and $\tau = \sigma_1 \otimes \sigma_2,\ \ A_i$ a quaternion algebra with standard involution $\sigma_i,\ \ i = 1, 2$.

Lemma 2. $pf_A : \mathrm{Alt}^\tau(A) \to K$ is a nonsingular quadratic form on the vector space $\mathrm{Alt}^\tau(A)$ of dimension 6.

Proof. By definition of the reduced pfaffian, it suffices to consider the case of the classical pfaffian on $\mathrm{Alt}_4(K)$. The formula given at the beginning of this chapter shows that

$$(\mathrm{Alt}_4(K), pf) \simeq H(K^3).$$

We now construct a "standard involution" on $\mathrm{Alt}^{\tau}(A)$, A as above. We first consider the case $A = M_4(K)$. Let $\pi : \mathrm{Alt}_4(K) \to \mathrm{Alt}_4(K)$ be defined by

$$\pi \begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} \\ -x_{12} & 0 & x_{23} & x_{24} \\ -x_{13} & -x_{23} & 0 & x_{34} \\ -x_{14} & -x_{24} & -x_{34} & 0 \end{pmatrix} = \begin{pmatrix} 0 & -x_{34} & x_{24} & -x_{23} \\ x_{34} & 0 & -x_{14} & x_{13} \\ -x_{24} & x_{14} & 0 & -x_{12} \\ x_{23} & -x_{13} & x_{12} & 0 \end{pmatrix}.$$

We get $x\pi(x) = \pi(x)x = pf(x)$ for $x \in \mathrm{Alt}_4(K)$. Further π is, in some sense, unique:

Lemma 3. Let $\gamma : \mathrm{Alt}_4(K) \to \mathrm{Alt}_4(K)$ be a K–linear automorphism such that $\gamma(x)x \in K$ for all $x \in \mathrm{Alt}_4(K)$ (or $x\gamma(x) \in K$ for all $x \in \mathrm{Alt}_4(K)$). There exists $\lambda \in K^{\bullet}$ such that $\gamma = \lambda\pi$.

Proof. Let $\{E_{ij}\}$, $1 \le i, \; j \le 4$ be the standard basis of $M_4(K)$. Let $\{g_i\}$, $1 \le i \le 6$ be the basis $\{h_{ij} = E_{ij} - E_{ji}\}$ of $\mathrm{Alt}_4(K)$ ordered lexicographically. The condition $\gamma(g_1)g_1 \in K$ implies that $\gamma(g_1) = \mu g_6$, $\mu \in K$ and $\gamma(g_6)g_6 \in K$ implies $\gamma(g_6) = \mu' g_1$, $\mu' \in K$. The condition $\gamma(g_1 + g_6)(g_1 + g_6) \in K$ then implies $\mu = \mu'$ and the lemma follows by further similar computations.

If A is *c.s.* of dimension 16 as above, we shall define $\pi_A : \mathrm{Alt}^{\tau}(A) \to \mathrm{Alt}^{\tau}(A)$ through a splitting $\alpha : L \otimes A \tilde{\to} M_4(L)$ as above. We put

$$\alpha(1 \otimes \pi_A(a)) = s_2 \pi(\alpha(1 \otimes a)s_2) \qquad a \in A$$

in the even symplectic case and

$$\alpha(1 \otimes \pi_A(a)) = (s_1 \otimes s_1)\pi(\alpha(1 \otimes a)(s_1 \otimes s_1))$$

if $A = A_1 \otimes A_2$. Let $s = s_2$ (resp. $s_1 \otimes s_1$). We have

$$\begin{aligned} \alpha(1 \otimes a)\alpha(1 \otimes \pi_A(a)) &= \alpha(1 \otimes a)s\pi(\alpha(1 \otimes a)s) \\ &= pf(\alpha(1 \otimes a)s) = pf_A(a), \\ \alpha(1 \otimes \pi_A(a))\alpha(1 \otimes a) &= s\pi(\alpha(1 \otimes a)s)\alpha(1 \otimes a) \\ &= s(\pi(\alpha(1 \otimes a)s)\alpha(1 \otimes a)s)s^{-1} \\ &= spf(\alpha(1 \otimes a)s)s^{-1} = pf_A(a) \end{aligned}$$

so

$$\pi_A(a)a = a\pi_A(a) = pf_A(a), \qquad a \in \mathrm{Alt}^{\tau}(A).$$

Further π_A is, up to scalars, the unique isomorphism $\gamma : \mathrm{Alt}^\tau(A) \to \mathrm{Alt}^\tau(A)$ such that $\gamma(a)a \in K$ for all $a \in \mathrm{Alt}^\tau(A)$ (or such that $a\gamma(a) \in K$ for all $a \in \mathrm{Alt}^\tau(A)$). The automorphism π_A allows us to compute the Clifford algebra of $(\mathrm{Alt}^\tau(A), pf_A)$:

Proposition 4. Let $\lambda \in K^\bullet$. The map

$$\mathrm{Alt}^\tau(A) \to M_2(A), \quad x \mapsto \begin{pmatrix} 0 & \pi_A(x) \\ \lambda x & 0 \end{pmatrix}$$

induces an isomorphism $\varphi : C(\mathrm{Alt}^\tau(A), \lambda pf_A) \tilde{\to} M_2(A)$.

Proof. The existence of φ follows from the universal property of the Clifford algebra. It is an isomorphism since $C(\mathrm{Alt}^\tau(A), pf_A)$ is *c.s.* and both algebras have the same dimension.

If we identify $C(\mathrm{Alt}^\tau(A), pf_A)$ with $M_2(A)$, we get $C_0 = \left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$, $C_1 = \left(\begin{smallmatrix} 0 & A \\ A & 0 \end{smallmatrix}\right)$ and the standard involution σ of C is given by

$$\sigma\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{d} & \varepsilon\overline{b} \\ \varepsilon\overline{c} & \overline{a} \end{pmatrix} = \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \overline{d} & \overline{b} \\ \overline{c} & \overline{a} \end{pmatrix}\begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix}$$

where $a \mapsto \overline{a} = \tau(a)$ is the involution of A and ε is the type of τ. Indeed, the restriction of σ to

$$V \simeq \left\{\begin{pmatrix} 0 & \pi_A(x) \\ \lambda x & 0 \end{pmatrix}, \quad x \in \mathrm{Alt}^\tau(A)\right\}$$

is -1_V.

Let A be *c.s.* over K with an even symplectic involution τ and let $A[X] = A \otimes K[X]$ be the polynomial ring in one variable X over A. We extend τ to $A[X]$ by putting $\tau(X) = X$. We obviously have

$$\mathrm{Alt}^\tau(A[X]) = \mathrm{Alt}^\tau(A) \otimes_K K[X]$$

and we get by scalar extension a pfaffian $pf_{A[X]}$ over $A[X]$ with values in $K[X]$. Since $1 \in \mathrm{Alt}^\tau(A)$, we can define, for all $a \in \mathrm{Alt}^\tau(A)$, a polynomial $\pi\chi(X, a) \in K[X]$ by

$$\pi\chi(X, a) = pf_{A[X]}(X \cdot 1 - a).$$

We call $\pi\chi(X, a)$ the *pfaffian characteristic polynomial.* It is of degree m if A has dimension $4m^2$. In particular, if $m = 2$,

$$\pi\chi(X, a) = X^2 - pft(a)X + pf_A(a)$$

where pft is a linear form on $\mathrm{Alt}^{\tau}(A)$. We call it the *pfaffian trace* of A. We have a Cayley–Hamilton theorem. i.e. $\pi\chi(a,a) = 0$ for all $a \in \mathrm{Alt}^{\tau}(A)$.

Example 5. Let B be a quaternion algebra with standard involution $b \mapsto \overline{b}$ and let $A = M_2(B)$. The involution

$$\tau : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$$

of A is of even symplectic type since it is the tensor product of the involution $x \mapsto x^t$ of $M_2(K)$ with the standard involution of B. We get

$$\mathrm{Alt}^{\tau}(A) = \{ \left(\begin{smallmatrix} x & \overline{b} \\ b & y \end{smallmatrix}\right), \quad x,\ y \in K, \quad b \in B \}.$$

To compute the pfaffian, we split B and apply the formula $pf_A(a) =$ $pf(\alpha(1 \otimes a)s_m)$ (which defines $pf_A(a)$!). We get

$$pf_A \left(\begin{smallmatrix} x & \overline{b} \\ b & y \end{smallmatrix}\right) = x\ y - b\overline{b}.$$

Let $\gamma : \mathrm{Alt}^{\tau}(A) \to \mathrm{Alt}^{\tau}(A)$ be defined by $\gamma \left(\begin{smallmatrix} x & \overline{b} \\ b & y \end{smallmatrix}\right) = \left(\begin{smallmatrix} y & -\overline{b} \\ -b & x \end{smallmatrix}\right)$. Since $a\gamma(a) = pf_A(a)$, we must have $\gamma = \pi_A$, so

$$\pi_A \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} = \begin{pmatrix} y & -\overline{b} \\ -b & x \end{pmatrix}.$$

Further $pft(a) = b(a,1)$, where b is the polar of pf_A, so

$$pft \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} = x + y$$

(as one would guess!). In particular, we get

$$a + \pi_A(a) = pft(a) \in K \quad \text{for all} \quad a \in \mathrm{Alt}^{\tau}(A).$$

This strengthens the (heuristic) fact, already mentioned, that π_A is a "standard involution" on $\mathrm{Alt}^{\tau}(A)$.

Chapter 11

Quadratic Forms of Dimension 6

At the end of Chapter 10, we have shown that the Arf invariant of a quadratic space $(\mathrm{Alt}^{\tau}(A), \lambda pf_A)$, A a *c.s.* K–algebra of dimension 16 with an even symplectic involution and $\lambda \in K^{\bullet}$, is trivial. Conversely we claim that

Proposition 1. Let (V,q) be a quadratic space of dimension 6 with trivial Arf invariant. Assume that (V,q) represents $\lambda \in K^{\bullet}$. There exist a *c.s.* K–algebra A and an even symplectic involution τ on A such that $(V,q) \simeq (\mathrm{Alt}^{\tau}(A), \lambda pf_A)$.

Let $C = C_0 \oplus C_1$ be the Clifford algebra of (V,q) and let $e,\ f$ be two nontrivial idempotents generating $Z(q) = K \times K$. Before proving Proposition 1, we describe V as a subspace of C_1. We denote as usual the standard involution of C by σ.

Lemma 2. The map $V \to Ve,\ \ x \mapsto xe$, is an isomorphism and

$$Ve = \{(x-\sigma(x))e,\ x \in C_1\} = \{y - \sigma(y),\ y \in C_1 e\}.$$

Similarly $V \simeq Vf$ and

$$Vf = \{(x-\sigma(x))f,\ x \in C_1\} = \{y - \sigma(y),\ y \in C_1 f\}.$$

Proof. Since if suffices to check the claims over an extension $K \subset L$, we can assume that $(V,q) = (\mathrm{Alt}^{\tau}(A), pf_A)$ for some *c.s.* algebra A of dimension 16 with an even symplectic involution (for example $A = M_4(K)$ and $\tau(x) = s_2 x^t s_2^{-1}$). Then by Proposition 4 of Chapter 10,

$$C = M_2(A),\quad \sigma\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \tau(d) & -\tau(b) \\ -\tau(c) & \tau(a) \end{pmatrix},\quad C_0 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

and we can choose $e = \left(\begin{smallmatrix}1 & 0\\ 0 & 0\end{smallmatrix}\right)$, $f = \left(\begin{smallmatrix}0 & 0\\ 0 & 1\end{smallmatrix}\right)$. The space V is embedded in C as the set

$$V = \left\{ \begin{pmatrix} 0 & \pi_A(x) \\ x & 0 \end{pmatrix}, \quad x \in \mathrm{Alt}^\tau(A) \right\}.$$

All the claims of Lemma 2 can now easily be explicitly checked.

Proof of Proposition 1. The algebra $A = C_0 e$ (with $1_A = e$) is *c.s.* of dimension 16 over K. We shall construct an even symplectic involution τ on A such that $(V, q) \simeq (\mathrm{Alt}^\tau(A), \lambda pf_A)$. Replacing q by λq, we may assume that q represents 1. Let $v \in V$ be such that $q(v) = 1$ and let $P = vA$. The standard involution σ of C maps P to P since

$$\sigma(vce) = -f\sigma(c)v = -\sigma(c)ve = vc'e, \quad \text{for} \quad c' = -v\sigma(c)v,$$

by Proposition 5 of Chapter 5. Let $\tau : A \to A$ be defined by $\sigma(va) = -v\tau(a)$. We have $\tau(ab) = \tau(b)\tau(a)$ and $va = \sigma^2(va) = -\sigma(v\tau(a)) = v\tau^2(a)$, so $\tau^2 = 1$. Therefore τ is an involution of A and by Lemma 2,

$$Ve = v \cdot \mathrm{Alt}^\tau(A).$$

We claim that the type of τ is independent of the choice of v. Let $w \in V$ with $q(w) = 1$ and let $w = vu$, $u \in A$. If τ' is defined by $\sigma(wa) = -w\tau'(a)$, we get

$$\sigma(vua) = -vu\tau'(a) = -v\tau(ua) = -v\tau(a)\tau(u).$$

On the other hand $w \in V$ so $\sigma(vu) = -vu$ and $\sigma(vu) = -v\tau(u)$. It follows that $u = \tau(u)$ and $\tau' = i_u \circ \tau$. Thus τ' is of even symplectic type if and only if τ is of even symplectic type. To compute the type of τ we may now assume (as in the proof of Lemma 2) that $(V, q) = (\mathrm{Alt}^{\tau_1}(A), pf_A)$, with τ_1 an even symplectic involution of A, and we can choose $v = 1$. For this choice, we get $\tau = \tau_1$, thus τ is of even symplectic type. We finally check that the map $\rho : V \to \mathrm{Alt}^\tau(A)$ defined by $xe = v\rho(x)$ is an isometry: we have similarly

$$Vf = \mathrm{Alt}^\tau(A) \cdot v$$

and we define $\gamma : \mathrm{Alt}^\tau(A) \to \mathrm{Alt}^\tau(A)$ by the formula $\rho^{-1}(a)f = \gamma(a)v$. We get

$$\gamma(a)a = \gamma(a)vva = q(\rho^{-1}(a))e \ \text{ for all } a \in \mathrm{Alt}^\tau(A),$$

so by Lemma 3 (and the discussion following Lemma 3) of Chapter 10 , $\gamma = \nu \cdot \pi_A$ for some $\nu \in K^\bullet$ and $q(x)e = \nu pf_A(\rho(x))$ (recall that $e = 1_A$!). Since $\rho(v) = e$, $\nu = 1$

and ρ is an isometry, as claimed.

In view of the next theorem, the algebra A in Proposition 1 is determined up to isomorphism by the class of similitudes of (V, q).

Theorem 3. Let A and B be *c.s.* algebras of dimension 16 over K with pfaffians pf_A and pf_B. Then $A \simeq B$ if and only if the corresponding pfaffians are similar.

Proof. Let σ_A be the involution of A and σ_B the involution of B. Let $\beta : A \tilde{\to} B$ be an isomorphism of algebras and let $\sigma' = \beta\sigma_A\beta^{-1}$. Then β is an isomorphism $(A, \sigma_A) \tilde{\to} (B, \sigma')$ of algebras with involutions and we get a pfaffian $pf'_B : \mathrm{Alt}^{\sigma'}(B) \to K$ such that $\beta : (\mathrm{Alt}^{\sigma_A}(A), pf_A) \to (\mathrm{Alt}^{\sigma'}(B), pf'_B)$ is an isometry. Let $\sigma' = i_u \circ \sigma_B$, so

$$\mathrm{Alt}^{\sigma'}(B) = u\mathrm{Alt}^{\sigma_B}(B) = \mathrm{Alt}^{\sigma_B}(B)u^{-1}.$$

We claim that the map

$$u^{-1}\beta : \mathrm{Alt}^{\sigma_A}(A) \to \mathrm{Alt}^{\sigma_B}(B)$$

is a similitude of the corresponding pfaffians. Let

$$\gamma : \mathrm{Alt}^{\sigma_B}(B) \to \mathrm{Alt}^{\sigma_B}(B)$$

be defined by $\gamma(y) = \beta(\pi_A\beta^{-1}(uy))u$. We have $\gamma(y)y = pf_A(\beta^{-1}(uy)) \in K$ for all $y \in \mathrm{Alt}^{\sigma_B}(B)$. Therefore by Lemma 3 of Chapter 10, there exists $\nu \in K^\bullet$ such that $\nu\gamma = \pi_B$ and, as claimed, $u^{-1}\beta$ is a similitude. Conversely, let

$$\varphi : (\mathrm{Alt}^{\sigma_A}(A), pf_A) \to (\mathrm{Alt}^{\sigma_B}(B), pf_B)$$

be a similitude. By Proposition 4 of Chapter 10, φ induces a graded isomorphism $M_2(A) \tilde{\to} M_2(B)$, where both matrix algebras have the checker–board grading. In degree zero, we get $A \times A \simeq B \times B$, hence $A \simeq B$.

Example 4. Let $A = M_2(B)$, B a quaternion algebra with standard involution $b \mapsto \overline{b}$. The involution

$$\sigma_1 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{d} & -\overline{b} \\ -\overline{c} & \overline{a} \end{pmatrix}$$

of A is the tensor product of the two standard involutions. We get

$$\mathrm{Alt}^{\sigma_1}(A) = \left\{ \begin{pmatrix} b & x \\ y & -\overline{b} \end{pmatrix}, \quad b \in B,\ x,\ y \in K \right\}$$

and for the corresponding pfaffian (use a splitting !):

$$pf_1 \begin{pmatrix} b & x \\ y & -\overline{b} \end{pmatrix} = -xy - b\overline{b}$$

so that $(\mathrm{Alt}^{\sigma_1}(A), pf_1) \simeq H(K) \perp (B, -n_B)$. On the other hand, (see Example 5 of Chapter 10)

$$\sigma_2 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}$$

is of even symplectic type. We get

$$\mathrm{Alt}^{\sigma_2}(A) = \left\{ \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix}, \quad b \in B,\ \ x,\ y \in K \right\}$$

and for the corresponding pfaffian:

$$pf_2 \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} = xy - b\overline{b}$$

so that $(\mathrm{Alt}^{\sigma_2}(A), pf_2) \simeq H(K) \perp (B, -n_B)$ and both pfaffians are indeed similar.

Corollary 5. There exists a bijection between similitude classes of quadratic spaces of dimension 6 with trivial Arf invariant and isomorphism classes of *c.s.* algebras of dimension 16, with even symplectic involutions. The correspondence is given by $(V, q) \mapsto A = C_0 e$, where e is a nontrivial idempotent of the centre of C_0. Further

1) A is a division algebra if, and only if, (V, q) is anisotropic.

2) $A \simeq M_2(D)$, D a quaternion division algebra if, and only, if (V, q) has Witt index 1.

3) $A \simeq M_4(K)$ if, and only if, $(V, q) \simeq H(K^3)$.

The class of A in $Br(K)$ is the Witt invariant of (V, q).

Proof. The first claim follows from Lemma 10 of Chapter 5, Proposition 1 and Theorem 3; the others, then from Example 4.

We now apply Theorem 3 to prove a classical result of Albert. Observe that, again, we do not assume char $K \neq 2$.

Theorem 6. Any *c.s.* K–algebra of dimension 16, whose class in $Br(K)$ is of order 2, is isomorphic to a tensor product of quaternion algebras.

Proof. Let A be *c.s.* of dimension 16 such that $2[A]=0$ in $Br(K)$. By Theorem 9 of Chapter 3, there exists an even symplectic involution σ on A. Let $pf_A : \mathrm{Alt}^\sigma(A) \to K$ be the corresponding pfaffian. We have $1 \in \mathrm{Alt}^\sigma(A)$ and $pf_A(1)=1$. We denote by $b : \mathrm{Alt}^\sigma(A) \times \mathrm{Alt}^\sigma(A) \to K$ the polar of pf_A. Since pf_A is nonsingular, there exists $z \notin K \cdot 1$ such that $b(1,z)=1$. The element z is a root of its pfaffian characteristic polynomial, so

$$z^2 = z - r, \qquad \text{where} \qquad r = pf_A(z),$$

and z generates a quadratic separable K–algebra Z. With the notations of Chapter 1, we get $[1,z] \simeq (Z, n_0)$ and

$$(\mathrm{Alt}^\sigma(A), pf_A) \simeq [1,z] \perp [a,b] \perp [c,d]$$

for some quadratic spaces $[a,b]$, $[c,d]$. We remark that $[a,b] \perp [c,d]$ has Arf invariant Z (compute the discriminant if char $K \neq 2$ and the classical Arf invariant if char $K=2$). Let now $(V_1,q_1)=[a,b]$, $(V_2,q_2)=[c,d]$, $(V,q)=(V_1,q_1)\perp(V_2,q_2)$, and let $\widetilde{C}=C(-q)=A_1 \otimes A_2$ with $A_1 = C(-\delta(q_2)q_1)$, $A_2 = C(-q_2)$ (see Lemma 8 of Chapter 5). The canonical involution σ' of $\widetilde{C}$ is of even symplectic type by Example 1 of Chapter 9 and C_0 has centre Z.

Lemma 7. $(\mathrm{Alt}^{\sigma'}(\widetilde{C}), pf_{\widetilde{C}}) = (Z, n_0) \perp (V, q)$.

Proof. If suffices to prove Lemma 7 over some field extension $K \subset L$ so that we can assume that $(V,-q)=(A,n)$, where A is a quaternion algebra with reduced norm n. By Example 1 of Chapter 9, we get

$$\mathrm{Alt}^{\sigma'}(\widetilde{C}) = \left\{ \begin{pmatrix} x & b \\ \overline{b} & y \end{pmatrix}, \quad x,y \in K,\ b \in A \right\} \subset M_2(A) = C$$

and $pf_{\widetilde{C}}\left(\begin{smallmatrix} x & b \\ \overline{b} & y \end{smallmatrix}\right) = xy - b\overline{b}$ as claimed.

By Lemma 7 A and $\widetilde{C} = A_1 \otimes A_2$ have isometric pfaffians and by Theorem 3, $A \simeq A_1 \otimes A_2$. This proves Theorem 6. Lemma 7 may also be used to describe the structure of the Clifford algebra of a quadratic space of dimension 4 :

Proposition 8. Let (V, q) be a quadratic space of dimension 4. Then

1) $C(q)$ is a division algebra if, and only, if the space $(Z(q), n_0) \perp (V, -q)$ is anisotropic.

2) $C(q) \simeq M_2(D)$, D a quaternion division algebra if, and only, if the space $(Z(q), n_0) \perp (V, -q)$ has Witt index 1.

3) $C(q) \simeq M_4(K)$ if, and only, if $(Z(q), n_0) \perp (V, -q) \simeq H(K^3)$.

Proof. By Lemma 7 we have $(\mathrm{Alt}^{\sigma'}(C(q)), pf_{C(q)}) \simeq (Z, n_0) \perp (V, -q)$ so that Proposition 8 follows from Corollary 5.

Example 9. Let $A = A_1 \otimes A_2$ be a tensor product of quaternion algebras and let $\sigma = \sigma_1 \otimes \sigma_2$ be the tensor product of the corresponding standard involutions. Assume that char $K \neq 2$ and let $A_i' = (K \cdot 1)^\perp \subset A_i$ for the reduced norms. Then

$$\mathrm{Alt}^\sigma(A) = A_1' \otimes 1 + 1 \otimes A_2' \simeq A_1' \oplus A_2'.$$

We claim that

$$pf_A(x_1 + x_2) = n_{A_1}(x_1) - n_{A_2}(x_2) \quad \text{for} \quad x_i \in A_i',$$

so

$$(\mathrm{Alt}^\sigma(A), pf_A) \simeq (A_1', n_{A_1}) \perp (A_2', -n_{A_2}).$$

It suffices to check the formula over a field extension $K \subset L$. Hence we can assume that $A_1 = M_2(K)$. By Example 4, we have

$$\mathrm{Alt}^\sigma(A) = \left\{ \begin{pmatrix} b & x \\ y & -\overline{b} \end{pmatrix}, \quad x, y \in K, \quad b \in A_2 \right\}.$$

Writing b as $z + b'$, $b' \in A_2'$, we get $\overline{b} = z - b'$,

$$\begin{pmatrix} b & x \\ y & -\overline{b} \end{pmatrix} = \begin{pmatrix} z & x \\ y & -z \end{pmatrix} + \begin{pmatrix} b' & 0 \\ 0 & b' \end{pmatrix}$$

and

$$pf_A \begin{pmatrix} b & x \\ y & -\overline{b} \end{pmatrix} = -xy - z^2 - n(b') = \det \begin{pmatrix} z & x \\ y & -z \end{pmatrix} - n(b'),$$

as claimed. The quadratic space $(A_1', n_{A_1}) \perp (A_2' - n_{A_2})$ is called the *Albert form* of $A_1 \otimes A_2$. We denote it by $Q(A_1, A_2)$. In view of Theorem 3, two tensor products $A_1 \otimes A_2$ and $B_1 \otimes B_2$ of quaternion algebras are isomorphic if and only if the

Albert forms $Q(A_1, A_2)$ and $Q(B_1, B_2)$ are similar (assuming char $K \neq 2$). This result is due to Jacobson. We mention two more results of Albert which are easy consequences of Theorem 3. We assume char $K \neq 2$.

1) Let $A,\ B,\ C$ be quaternion algebras. If $[A][B][C] = 0$ in $Br(K)$, then $Q(A, B)$ is isotropic.

2) Let $A,\ B$ be quaternion algebras. Then $A \otimes B \simeq M_2(C)$ if, and only if, there exists a quadratic separable algebra Z which is contained in A and B.

1) is clear by Theorem 3. We sketch a proof of 2). If $Z \subset A$ and $Z \subset B$ then $(A, n_A) \simeq (Z, n_0) \perp (V_1, q_1)$ and $(B, n_B) \simeq (Z, n_0) \perp (V_2, q_2)$ so that (A', n_A) and (B', n_B) represent a (nonzero) common element. If follows that $Q(A, B)$ is isotropic. Conversely if $A \otimes B \simeq M_2(C)$, $Q(A, B)$ is isotropic and (A', n_A), (B', n_B) represent a common element $\lambda \in K$. If $\lambda = 0 \quad A \simeq M_2(K),\ B \simeq M_2(K)$ and the claim is obvious (take $Z = K \times K$). If $\lambda \neq 0$ and $q(v_1) = \lambda = q(v_2)$, then $Z = K \cdot 1 \oplus K \cdot v_1 \simeq K \cdot 1 \oplus K \cdot v_2$ is the algebra Z.

We now consider quadratic spaces (V, q) of dimension 6 with arbitrary Arf invariant. Let $Z = Z(q)$ be the centre of the even Clifford algebra C_0 of (V, q). Let σ be the standard involution of $C = C(q)$ and let

$$\mathrm{Alt}^\sigma(C_1) = \{x - \sigma(x),\ x \in C_1\}.$$

Lemma 10. The inclusion $V \to C_1$ induces an isomorphism

$$Z \otimes V \tilde{\to} \mathrm{Alt}^\sigma(C_1).$$

Proof. Since it suffices to prove Lemma 10 over a field extension $K \subset L$, we may assume that $(V, q) = (\mathrm{Alt}^\tau(A), pf_A)$ for A a *c.s.* K–algebra of dimension 16 with an even symplectic involution $\tau : a \mapsto \overline{a}$. The claim then follows easily from Example 4.

We now assume that q represents 1, let $v \in V$ with $q(v) = 1$, so $v^2 = 1$ in C. We have $\sigma(v) = -v$ and $\sigma_1 = i_v \circ \sigma$ is a Z–linear involution of C_0 (observe that σ is σ_0–semilinear, where σ_0 is the standard involution of Z). We claim that σ_1 is an involution of C_0 of even symplectic type. The type does not depend on the choice of $v \in V$ (such that $v^2 = 1$), so we can take $(V, q) = (\mathrm{Alt}^\tau(A), pf_A)$ as above and

$v = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = 1_A$. Then

$$\sigma_1 \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} \tau(a) & 0 \\ 0 & \tau(b) \end{pmatrix}.$$

Since τ is of even symplectic type, σ_1 is of even symplectic type. By definition of σ_1, the maps $C_1 \to C_0$ given by $\lambda_v : x \to vx$ and $\rho_v : x \mapsto xv$ induce isomorphisms

$$\lambda_v, \rho_v : \mathrm{Alt}^{\sigma}(C_1) \tilde{\to} \mathrm{Alt}^{\sigma_1}(C_0).$$

Let $pf_1 : \mathrm{Alt}^{\sigma_1}(C_0) \to K$ be the pfaffian given by σ_1 and let $\pi_1 : \mathrm{Alt}^{\sigma_1}(C_0) \to \mathrm{Alt}^{\sigma_1}(C_0)$ be such that $\pi_1(x)x = x\pi_1(x) = pf_1(x)$ for all $x \in \mathrm{Alt}^{\sigma_1}(C_0)$. We claim that ρ_v is an isometry

$$\rho_v : (Z \otimes V, 1 \otimes q) \to (\mathrm{Alt}^{\sigma_1}(C_0), pf_1).$$

We have $(1 \otimes q)(x) = -x\sigma(x)$ for all $x \in Z \otimes V = \mathrm{Alt}^{\sigma}(C_1)$. Let $\gamma : \mathrm{Alt}^{\sigma_1}(C_0) \to \mathrm{Alt}^{\sigma_1}(C_0)$ be defined by $\gamma(xv) = -v\sigma(x)$ for $x \in Z \otimes V$. We get $xv\gamma(xv) = -x\sigma(x) = (1 \otimes q)(x)$, so $\gamma = \nu\pi_1$ for some $\nu \in K^{\bullet}$. Putting $x = v$ shows that $\nu = 1$, $\gamma = \pi_1$ and as claimed, ρ_v is an isometry. Further we know that $V = \{x \in Z \otimes V \mid \sigma(x) = -x\}$ or, since $\sigma(x) = -v\pi_1(xv)$,

$$V = \{x \in Z \otimes V \mid v\pi_1(xv) = x\}. \tag{11.1}$$

We are now ready to prove the following

Theorem 11. Let (V, q), (V', q') be quadratic spaces of dimension 6 and let $C_0 = C_0(q)$, $C_0' = C_0(q')$ with the standard involutions. Then (V, q) and (V', q') are similar if and only if C_0 and C_0' are isomorphic as algebras–with–involution.

Proof. We assume that the centre Z of C_0 is a field (the other case is similar). Since φ maps Z to the centre Z' of C_0', we view C_0' as a Z–algebra through φ. Then φ is a Z–linear isomorphism. Let $\varphi : C_0 \tilde{\to} C_0'$ be an isomorphism as algebras–with–involution, i.e. such that $\varphi\sigma = \sigma\varphi$, σ the standard involution. We can assume that V and V' represent 1 (since only similitude classes matter), so let $v \in V$ with $q(v) = 1$ and $v' \in V'$ with $q'(v') = 1$. Let σ_1 be the involution $i_v \circ \sigma$ of C_0 and $\sigma_1' = i_{v'} \circ \sigma$. Further let $pf_1 : \mathrm{Alt}^{\sigma_1}(C_0) \to Z$, $pf_1' : \mathrm{Alt}^{\sigma_1'}(C_0') \to Z$ be the corresponding pfaffians and

$$\pi_1 : \mathrm{Alt}^{\sigma_1}(C_0) \to \mathrm{Alt}^{\sigma_1}(C_0), \quad \pi_1' : \mathrm{Alt}^{\sigma_1'}(C_0') \to \mathrm{Alt}^{\sigma_1'}(C_0')$$

be such that $x\pi_1(x) = pf_1(x)$, $x'\pi_1'(x') = pf_1'(x)$. The involution $\sigma' = \varphi\,\sigma_1\,\varphi^{-1}$ of C_0' is of even symplectic type and, writing $\sigma' = i_u \circ \sigma_1'$, $u \in C_0^\bullet$, we get $\sigma_1'(u) = u$ or $v'\sigma(u)v' = u$. Since $\varphi\,\sigma = \sigma\,\varphi$, it follows that $\varphi\, i_v\, \sigma\, \varphi^{-1} = \varphi\, i_v\, \varphi^{-1}\, \sigma = i_u\, i_{v'}\, \sigma$ so that $\varphi \circ i_v = i_{uv'} \circ \varphi$ or $\varphi(vxv) = uv'\varphi(x)v'u^{-1}$. Replacing x by $v\,x\,v$, we get $\varphi(x) = uv'\varphi(vxv)v'u^{-1}$, so there is $\mu \in Z^\bullet$ such that $\mu uv' = v'u^{-1}$. This, together with $v'\sigma(u)v' = u$, implies that $\sigma(u)u \in Z^\bullet$, so also $u\sigma(u) \in Z^\bullet$. The Z–linear isomorphism $C_0 \to C_0'$, $x \mapsto \varphi(x)u$ maps $\mathrm{Alt}^{\sigma_1}(C_0)$ to $\mathrm{Alt}^{\sigma_1'}(C_0')$ since

$$\begin{aligned} \varphi(\mathrm{Alt}^{\sigma_1}(C_0)) &= \mathrm{Alt}^{\sigma'}(C_0') = \mathrm{Alt}^{\sigma_1'}(C_0') \cdot u^{-1} \\ &= u \cdot \mathrm{Alt}^{\sigma_1}(C_0'). \end{aligned}$$

Let now $\gamma : \mathrm{Alt}^{\sigma_1}(C_0) \to \mathrm{Alt}^{\sigma_1}(C_0)$ be defined by

$$\gamma(x) = \varphi^{-1}(u\pi_1'(\varphi(x)u)).$$

Since

$$x\gamma(x) = \varphi^{-1}(\varphi(x)u\pi_1'(\varphi(x)u)) = pf_1'(\varphi(x)u) \in Z,$$

there exists $\lambda \in Z^\bullet$ such that $\gamma = \lambda\pi_1$ and $x \mapsto \varphi(x)u$ is a similitude

$$(\mathrm{Alt}^{\sigma_1}(C_0), pf_1) \to (\mathrm{Alt}^{\sigma_1'}(C_0'), pf_1')$$

with multiplier λ. We compute λ. By the discussion preceeding Theorem 11, the map $x \mapsto \varphi(xv)uv'$ is a similitude $Z \otimes (V,q) \to Z \otimes (V',q')$ with multiplier λ. Since $(1 \otimes q')(x') = -x'\sigma(x')$, we get $(1 \otimes q')(\varphi(xv)uv') =$ $(\varphi(xv)uv')\sigma(\varphi(xv)uv') = \varphi(xv)u\sigma(u)\sigma\varphi(xv)$. Now $u\sigma(u) \in Z$ and $\sigma\varphi = \varphi\sigma$, so $(1 \otimes q')(\varphi(xv)uv') = u\sigma(u)(1 \otimes q)(x)$. It follows that $\lambda = u\sigma(u)$ and $\sigma(\lambda) = \sigma_0(\lambda) = \lambda$, so $\lambda \in K^\bullet$. We claim that, in fact, $x \mapsto \varphi(xv)uv'$ restricts to a similitude $(V,q) \to (V',q')$ with multiplier λ. We have by (11.1)

$$V = \{x \in Z \otimes V \mid v\pi_1(xv) = x\}, \quad V' = \{x' \in Z \otimes V' \mid v'\pi_1'(x'v') = x'\}$$

so we have to check that $v'\pi_1'(\varphi(xv)u) = \varphi(xv)uv'$ if $x = v\pi_1(xv)$. By definition of γ and the fact that $\lambda = u\sigma(u)$, we get

$$\sigma(u)\varphi\pi_1(xv) = \pi_1'(\varphi(xv)u) \quad \text{for} \quad xv \in \mathrm{Alt}^{\sigma_1}(C_0).$$

On the other hand we obtain, using that $x = v\pi_1(xv)$,

$$\begin{aligned} \sigma(u)\varphi\pi_1(xv) &= \sigma(u)\varphi(vx) = \sigma(u)\varphi(v(xv)v) \\ &= \sigma(u)uv'\varphi(xv)v'u^{-1} = v'\varphi(xv)u\sigma(u)\sigma(u)^{-1}v' = v'\varphi(xv)uv'. \end{aligned}$$

Thus

$$v'\varphi(xv)uv' = \pi_1'(\varphi(xv)u) \quad \text{or} \quad \varphi(xv)uv' = v'\pi_1'(\varphi(xv)u)$$

as claimed.

Remark 12. The first part of Corollary 5 is a consequence of Theorem 11 if $Z = K \times K$. In fact the algebra C_0 is isomorphic to a product $A \times A^{op}$ and the standard involution σ corresponds to the involution $\sigma_A : (a, b^0) \mapsto (b, a^0)$. Any isomorphism of algebras $A \to B$ extends to an isomorphism $A \times A^{op} \to B \times B^{op}$ of algebras–with–involution. (Observe that the standard involution σ of C_0 is of the second kind).

Remark 13. Assume that the Arf invariant of (V, q) is not trivial, i.e. $Z = Z(q)$ is a field. Since

$$Z \otimes (V, q) \simeq (\mathrm{Alt}^{\sigma_1}(C_0),\ \lambda pf_1)$$

for some $\lambda \in Z^\bullet$ and some even symplectic involution σ_1 of C_0, it follows from Corollary 5 that

1) C_0 is a division algebra if, and only, if $Z \otimes (V, q)$ is anisotropic.

2) $C_0 \simeq M_2(D)$, D a quaternion division algebra over L if, and only, if $Z \otimes (V, q)$ has Witt index 1.

3) $C_0 \simeq M_4(Z)$ if and only if $Z \otimes (V, q) \simeq H(Z^3)$.

Remark 14. Let B be a *c.s.* Z–algebra, Z a separable quadratic field extension of K. The corestriction $\mathrm{cor}(B)$ is a *c.s.* K–algebra and $B \mapsto \mathrm{cor}(B)$ induces a homomorphism cor: $Br(Z) \to Br(K)$. As shown by Arason for fields of characteristic different from 2 or (in a more general context, in particular for fields of any characteristic) by Knus–Parimala–Srinivas, the sequence

$${}_2Br(K) \to_2 Br(Z) \overset{cor}{\to}_2 Br(K)$$

is exact. Here ${}_2Br(K)$ denotes the subgroup of $Br(K)$ of elements of order 2. Let now C_0 be the even Clifford algebra of a quadratic space of dimension 6. Since the standard involution σ is of the second kind, the corestriction of C_0 is trivial (Theorem 11 of Chapter 3) and by the exactness of the above sequence, C_0 is of the form $Z \otimes B$ for some *c.s.* K–algebra B. This is also true for forms of dimension

4 (see Chapter 9) and dimension 2. We believe that the even Clifford algebra of a quadratic space of arbitrary even dimension is of the form $C_0 = Z(q) \otimes B$. This is clear if $n \equiv 2\ (4)$ by Proposition 6 of Chapter 5 and if $\mathrm{Char} K \neq 2$ by Lemma 8 of Chapter 5. Observe that the algebra B is not uniquely determined by the form q (except if $Z(q) = K \times K$).

Let A be a *c.s.* Z–algebra of dimension 16 which is isomorphic to the even Clifford algebra C_0 of a quadratic space (V, q) of dimension 6 with Arf invariant Z. As we have seen a necessary condition for such an A is that A has an involution $b \mapsto b^*$ of the second kind (necessary and sufficient conditions are given in Knus–Parimala–Sridharan). Let σ be another involution of A of the second kind. By Lemma 12 of Chapter 3, $\sigma = \sigma_g$ for $g \in A^\bullet$ such that $g^* = g$ (σ_g denotes the involution $\sigma_g(x) = gx^*g^{-1}$). Further $(A, \sigma_g) \simeq (A, \sigma_{g'}) \Leftrightarrow g' = \lambda c g c^*$ for $\lambda \in K^\bullet$ and $c \in A^\bullet$. In this case we call g and g' similar. By Theorem 10, the similitude classe of (V, q) corresponds to the similitude class of g.

Remark 15. Let (V, q) and (V', q') be quadratic spaces of dimension 6 with the same Arf invariant. We choose as a representative of the Arf invariant the centre Z of $C_0(q)$ and view $C_0(q')$ as a Z-algebra through the choice of an isomorphism $Z \tilde{\to} Z(C_0(q'))$. We claim that $C_0(q)$ and $C_0(q')$ are isomorphic K–algebras if and only if the quadratic spaces $(V, q) \otimes Z$ and $(V', q') \otimes Z$ are similar. Let $\varphi : C_0(q) \tilde{\to} C_0(q')$ be an isomorphism of K-algebras, so that $\varphi \otimes 1$ is an isomorphism of the even Clifford algebras of the spaces $(V, q) \otimes Z$ and $(V', q') \otimes Z$. Since $Z \otimes Z \tilde{\to} Z \times Z$ (an isomorphism being $\xi :\ x \otimes y \mapsto (xy, x\sigma_0(y))$, these spaces have trivial Arf invariant. Hence, by Corollary 5, they are similar. Conversely, if the quadratic spaces $(V, q) \otimes Z$ and $(V', q') \otimes Z$ are similar, there exists an isomorphism of Z-algebras $C_0(q) \otimes Z \tilde{\to} C_0(q') \otimes Z$ (see Lemma 10 of Chapter 5). The isomorphism $\xi : Z \otimes Z \tilde{\to} Z \times Z$ composed with the projection $Z \times Z \to Z$ onto the first factor induces a homomorphism of K-algebras $C_0(q') \otimes Z \to C_0(q')$. Let φ be the composition

$$C_0(q) \to C_0(q) \otimes Z \tilde{\to} C_0(q') \otimes Z \to C_0(q').$$

The map φ is K-linear and maps the centre Z of $C_0(q)$ into the centre Z' of $C_0(q')$. By the uniqueness of the standard involution of quadratic algebras, the restriction φ_Z of φ to Z is a morphism $(Z, n_Z) \to (Z', n_{Z'})$ of quadratic spaces of the same dimension. Since φ_Z is not the zero map, φ_Z is an isomorphism. If we view $C_0(q')$ as a Z-algebra through φ_Z, φ is a Z-homomorphism between *c.s.* Z-algebras of the same dimension. Thus φ must be an isomorphism.

We now compute the special Clifford group, the spin group and the Lie algebra of a quadratic space (V,q) of dimension 6. We may assume that q represents 1, so let v with $q(v)=1$. Let $u \in C_0^\bullet$. With the same notation as in the discussion preceding Theorem 10, the condition $i_u(V) \subset V$ implies $uxu^{-1}v \in \mathrm{Alt}^{\sigma_1}(C_0)$ for all $x \in V$, in particular $\sigma_1(uxu^{-1}v) = uxu^{-1}v$, so $uxu^{-1}v = vv\sigma(u^{-1})vxv\sigma(u)v$ and $\sigma(u)u$ must be in the centre of C_0. Since $\sigma_0(\sigma(u)u) = \sigma(\sigma(u)u) = \sigma(u)u$, we get $\sigma(u)u \in K$. To simplify notations we put $\sigma(u)u = u\sigma(u) = \mu(u)$. Further since by (11.1) $V = \{x \in Z \otimes V \mid v\pi_1(xv) = x\}$, $i_u(V) \subset V$ is equivalent with $v\pi_1(uxu^{-1}v) = uxu^{-1}$ for all $x \in V$. We have, using that $\pi_1(ay\sigma_1(a)) = n(a)\sigma_1(a)^{-1}\pi(y)a^{-1}$, n the reduced norm,

$$\begin{aligned} v\pi_1(uxu^{-1}v) &= v\pi_1(uxv\mu(u)^{-1}\sigma_1(u)) \\ &= v\mu(u)^{-1}\sigma_1(u)^{-1}\pi(xv)u^1 n(u) \\ &= \mu(u)^{-1}\sigma(u)^{-1}v\pi(xv)u^{-1}n(u) \\ &= \mu(u)^{-2}n(u)uxu^{-1}. \end{aligned}$$

Thus $i_u(V) \subset V$ is equivalent with $n(u) = \mu(u)^2$ and

$$\begin{aligned} S\Gamma(q) &= \{u \in C_0^\bullet \mid n(u) = \mu(u)^2\} \\ \mathrm{Spin}(q) &= \{u \in S\Gamma(q) \mid \mu(u) = 1\}. \end{aligned}$$

Let Z be a quadratic field extension of K. For any *c.s.* Z–algebra A with an involution of the second kind σ, we define an involution $\alpha \mapsto \alpha^*$ of $M_n(A)$ by

$$\alpha^* = (\sigma(a_{ij}))^t \quad \text{if} \quad \alpha = (a_{ij}) \in M_n(A),$$

i.e. $\alpha \mapsto \alpha^*$ is the tensor product of the involution σ of A with the involution $x \mapsto x^t$ of $M_n(Z)$. We call a matrix $g \in M_n(A)$ *hermitian* if $g^* = g$ and we say that two hermitian matrices g, g' are *congruent* if there exists $x \in GL_n(A)$ such that $g' = xgx^*$.

Let $g \in M_n(A)$ be an hermitian matrix. We call the group

$$GU_n(A,g) = \{x \in GL_n(A) \mid xgx^* = \lambda g,\ \lambda \in K\}$$

the *group of unitary similitudes* of g, the group

$$U_n(A,g) = \{x \in GL_n(A) \mid xgx^* = g\}$$

the *unitary group* of g and

$$SU_n(A,g) = \{x \in U_n(A,g) \mid n_{M_n(A)}(x) = 1\}$$

the *special unitary group* of g. With these notations we get

$$\text{Spin}(V,q) = SU_1(C_0, 1). \tag{11.2}$$

We consider some special cases. First let

$$(V,q) \simeq (Z, n_Z) \perp (B, \lambda n_B), \tag{11.3}$$

where B is a quaternion algebra over K and $\lambda \neq 0 \in K$. We have

$$C(q) \simeq C(B, \lambda n_B) \widehat{\otimes} C(Z, n_Z).$$

By Example 1 of Chapter 9, $C(B, \lambda n_B)$ is isomorphic to $M_2(B)$ with the checkerboard gradation. The standard involution is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & -\lambda^{-1}\bar{c} \\ -\lambda\bar{b} & \bar{d} \end{pmatrix},\ a,b,c,d \in B,$$

where $a \mapsto \bar{a}$ is the standard involution of B. Further by Example 3 of Chapter 7

$$C(Z, n_Z) = (1, Z/K] \simeq Z \oplus uZ,$$

with the multiplication rules $xu = u\sigma_0(x),\ u^2 = 1$ (σ_0 is the involution of Z) and the standard involution of $C(Z, n_Z)$ corresponds to $x + uy \mapsto \sigma_0(x)u - uy,\ x, y \in Z$. We define a graded isomorphism

$$\psi:\ M_2(B)\widehat{\otimes}(Z \oplus uZ) \tilde{\to} M_2(B \otimes (Z \oplus uZ))$$

by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes (x + uy) \mapsto \begin{pmatrix} a \otimes (x+uy) & b \otimes (x+uy) \\ c \otimes (x-uy) & d \otimes (x-uy) \end{pmatrix}.$$

We use ψ to identify $C(q)$ with $M_2(B\otimes(Z\oplus uZ))$. In particular we get

$$C_0 = \begin{pmatrix} B\otimes Z & B\otimes uZ \\ B\otimes uZ & B\otimes Z \end{pmatrix}$$

and it is easy to check that the map

$$\begin{pmatrix} a\otimes x_1 & b\otimes ux_2 \\ c\otimes ux_3 & d\otimes x_4 \end{pmatrix} \mapsto \begin{pmatrix} a\otimes x_1 & b\otimes \sigma_0(x_2) \\ c\otimes x_3 & d\otimes \sigma_0(x_4) \end{pmatrix}$$

is an isomorphism $\varphi:\ C_0(q)\tilde{\to}M_2(B\otimes Z)$. Let σ be the standard involution of $C_0(q)$. We get

$$\sigma\begin{pmatrix} a\otimes x_1 & b\otimes ux_2 \\ c\otimes ux_3 & d\otimes x_4 \end{pmatrix} = \begin{pmatrix} \bar a\otimes \sigma_0(x_1) & \bar c\otimes \lambda^{-1}ux_3 \\ \lambda\bar b\otimes ux_2 & \bar d\otimes \sigma_0(x_4), \end{pmatrix}$$

so

$$\varphi\sigma\varphi^{-1}\begin{pmatrix} a\otimes x_1 & b\otimes x_2 \\ c\otimes x_3 & d\otimes x_4 \end{pmatrix} = \begin{pmatrix} \bar a\otimes \sigma_0(x_1) & \lambda^{-1}\bar c\otimes \sigma_0(x_3) \\ \lambda\bar b\otimes \sigma_0(x_2) & \bar d\otimes \sigma_0(x_4) \end{pmatrix}$$

Thus the transport of σ to $M_2(B\otimes Z)$ is the involution

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^* = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}\begin{pmatrix} \tilde\alpha & \tilde\beta \\ \tilde\gamma & \tilde\delta \end{pmatrix}^t\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1},$$

where $\tilde\alpha = \bar a\otimes\sigma_0(x)$ for $\alpha = a\otimes x\in B\otimes Z$. In view of (11.2) we get

(11.4) $$\mathrm{Spin}((B,\lambda n_B)\perp(Z,n_Z)) \simeq SU_2(B\otimes Z, diag(1,\lambda)),$$

If (V,q) is a quadratic space with Arf invariant $[Z]$ such that

$$(M,q)\otimes Z\simeq((B,n_B)\perp(Z,n_Z))\otimes Z$$

then, by Remark 15, $C_0(q)\simeq M_2(B\otimes Z)$. The standard involution of $C_0(q)$ is of the form $\sigma(x) = gx^*g^{-1}$ for some hermitian matrix $g\in M_2(B\otimes Z)$ (i.e. $g = g^*$). In this case

$$\mathrm{Spin}(V,q)\simeq\{x\in SL_2(B\otimes Z)\mid xgx^* = g\}\simeq SU_2(B,g).$$

We observe that g is determined up to similarity by (V,q) (see Remark 15). If , in (11.4), $B = M_2(K)$ (and $\lambda = 1$), we get

$$\mathrm{Spin}(M,q)\simeq SU_4(Z,s_2)$$

since the standard involution of $M_2(K)$ is $\alpha\mapsto s_1\alpha^ts_1^{-1}$ for $\alpha\in M_2(K)$. If $i\neq 0\in Z$ is an element of trace zero, the matrix $is_1\in M_2(Z)$ is hermitian and is congruent to $\binom{0\ 1}{1\ 0}$. In fact we have $\binom{0\ i}{1\ 0}\binom{0\ 1}{1\ 0}\binom{0\ 1}{\bar i\ 0} = is_1$. Thus

$$\mathrm{Spin}(H(K^2)\perp(Z,n_Z))\simeq SU_4(Z,\ diag(1,\ 1,\ -1,\ -1)).$$

Finally we assume that there exists an isomorphism $B \otimes Z \tilde{\to} M_2(Z)$ of algebras–with–involution where the involution on $B \otimes Z$ is the tensor product of the standard involutions and the involution on $M_2(Z)$ is the involution

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \alpha^* = \begin{pmatrix} \sigma_0(a) & \sigma_0(b) \\ \sigma_0(c) & \sigma_0(d) \end{pmatrix}^t .$$

Then

$$\mathrm{Spin}((Z, n_Z) \perp (B, \lambda n_B)) \simeq SU_4(Z, diag(1,\ 1,\ \lambda,\ \lambda)).$$

This is the case for $B = \mathbb{H}$ and $Z = \mathbb{C}$. In fact the isomorphism $\mathbb{H} = \mathbb{C} \oplus j\ \mathbb{C} \simeq M_2(\mathbb{C})$ given by

$$(x \oplus jy) \otimes z \mapsto \begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix} z$$

has the wanted property.

We now assume that (V, q) has trivial Arf invariant and that (V, q) represents 1. By Proposition 1, we can choose $(V, q) = (\mathrm{Alt}^\tau(A), pf_A)$ for some *c.s.* algebra A with an involution τ of even symplectic type. Then $C_0 \simeq A \times A$ and $\sigma(a, b) = (\tau(b), \tau(a))$. It follows that

$$\mathrm{Spin}(V, q) \simeq \{(a, \tau(a)^{-1}),\ \ a \in SL_1(A)\} \simeq SL_1(A)$$

and the map $S\pi : \mathrm{Spin}(V, q) \to SO(V, q)$ is given by

$$a \in SL_1(A) \mapsto S\pi(a)(x) = \tau(a)^{-1} x a^{-1}.$$

If (V, q) is anisotropic, A is a division algebra. If (V, q) has Witt index 1, (V, q) is similar to $H(K) \perp (B, n_B)$, B a quaternion division algebra with standard involution $b \mapsto \overline{b}$ (by Example 4). Then $A = M_2(B)$ with the involution

$$\tau \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}.$$

So

$$\mathrm{Spin}(V, q) \simeq SL_2(B).$$

If $(V, q) \simeq H(K^3)$, we have $B = M_2(K)$ in the above formula. Therefore $A = M_4(K)$ with the involution $\tau(x) = s_2 x^t s_2^{-1}$ and

$$\mathrm{Spin}(V, q) \simeq SL_4(K).$$

By definition of pf_A, the map $\theta : x \mapsto s_2^{-1}x$ is an isometry

$$\theta : (V, q) = (\mathrm{Alt}^\tau(M_4(K)), pf_{M_4(K)}) \tilde{\to} (\mathrm{Alt}_4(K), pf) = H(K^3).$$

Let $u \in \mathrm{Spin}(\mathrm{Alt}^\tau(M_4(K)), pf_{M_4(K)})$. Since

$$\theta S\pi(u)\theta^{-1}(x) = s_2^{-1}(s_2 u^t s_2^{-1})^{-1} s_2 x u^{-1} = (u^t)^{-1} x u^{-1},$$

the map $S\pi$ corresponds through θ to the map

$$SL_4(K) \to SO(\mathrm{Alt}_4(K), pf) = SO(H(K^3))$$

defined by $u \mapsto (x \mapsto (u^t)^{-1} x u^{-1})$.

We now compute the Lie algebra $so(q)$. Let

$$\mathcal{S}(C_0, \sigma) = \{x \in C_0 \mid x + \sigma(x) = 0\}.$$

We obviously have $so(q) = [V, V] \subset \mathcal{S}(C_0, \sigma)$, thus

$$so(q) = [so(q), so(q)] \subset \mathcal{S}(C_0, \sigma)' = [\mathcal{S}(C_0, \sigma), \mathcal{S}(C_0, \sigma)].$$

We claim that

$$so(q) = \mathcal{S}(C_0, \sigma)'.$$

It suffices to verify that $\mathrm{Dim}_K \mathcal{S}(C_0, \sigma)' = 15$. We can assume that $(V, q) = (A, pf_A)$ so

$$\mathcal{S}(C_0, \sigma) = \{(a, -a),\ a \in A\} \simeq A.$$

Taking further $A = M_4(K)$, we get $\mathrm{Dim}_K[A, A] = 15$ as claimed. We leave it as an exercise to compute $so(q)$ for the different cases considered above.

We finally compute the group $GO_+(q)$ of special similitudes of a quadratic space of dimension 6. Let $Z = Z(q)$ be the centre of C_0. Let $n_0(x) = x\sigma_0(x)$ be the norm of Z, n the reduced norm of C_0 (as Z–algebra), σ the standard involution of C and $\mu(u) = u\sigma(u)$. Let $GU_1(C_0) = \{u \in C_0 \mid u\ sigma(u) \in Z^\bullet$.

Theorem 16. Let G be the subgroup of $Z^\bullet \times GU_1(C_0)$ of pairs (z, u) with $z\sigma_0(z)^{-1} = n(u)\mu(u)^{-2}$. There exists an isomorphism

$$G/\{(z^2, z^{-1}),\ z \in Z^\bullet\} \tilde{\to} GO_+(q).$$

Proof. Let $C = C_0 \oplus C_1$ be the Clifford algebra of (V, q). By Lemma 10, we may identify $Z \otimes V$ with $\mathrm{Alt}^\sigma(C_1)$. For $(z, u) \in Z^\bullet \times GU_1(C_0)$, let $\rho(z, u) : \mathrm{Alt}^\sigma(C_1) \to \mathrm{Alt}^\sigma(C_1)$ be the map $\rho(z, u)(x) = zux\sigma(u)$. Since $(1 \otimes q)(x) = -x\sigma(x)$, $\rho(z, u)$ is a similitude of $Z \otimes V$ with multiplier $n_0(z)\mu(u)^2 \in K^\bullet$. We claim that $\rho(z, u)$ restricts to a similitude of V if and only if $z\sigma_0(z)^{-1} = n(u)\mu(u)^{-2}$. By (11.1) and with the notations introduced after Lemma 10, we have to check that $v\pi_1(zux\sigma(u)v) = zux\sigma(u)$ for $x \in V$. We get

$$v\pi_1(zux\sigma(u)v) = \sigma_0(z)\pi_1(uxv\sigma_1(u)).$$

It now follows from $pf_1(uc\sigma_1(u)) = n(u)pf_1(c)$ for $c \in C_0$ that

$$\pi_1(uc\sigma_1(u)) = n(u)\sigma_1(u)^{-1}\pi_1(c)u^{-1},$$

hence

$$\begin{aligned} v\pi_1(zux\sigma(u)v) &= \sigma_0(z)n(u)\sigma_1(u)^{-1}\pi_1(xv)u^{-1} \\ &= \sigma_0(z)n(u)\mu(u)^{-2}ux\sigma(u), \end{aligned}$$

using that $v\pi_1(xv) = x$, $\sigma_1(u) = vuv$ and $\mu(u) = u\sigma(u)$. Thus, as claimed, $zux\sigma(u) \in V$ if and only if $\sigma_0(z)n(u)\mu(u)^{-2} = z$. The multiplier of $\rho(z, u)$ is $n_0(z)\mu(u)^2$. The extension of $\rho(z, u)$ to C_0 is given on elements xy, x, $y \in V$, by

$$C_0(\rho(z, u))(xy) = n_0(z)^{-1}\mu(u)^{-2}zux\sigma(u)xuy\sigma(u) = uxyu^{-1}$$

(see Lemma 10 of Chapter 5), thus $\rho(z, u) \in GO_+(q)$. If $\rho(z, u) = 1$, then, by the above formula, $u \in Z$ and $zu^2 = 1$. Therefore ρ induces an injective map

$$\rho' : G/\{(z^2, z^{-1}),\ \ z \in Z^\bullet\} \to GO_+(q).$$

We check that ρ' is surjective. Let

$$E = \begin{pmatrix} {}_\sigma C_0 & {}_\sigma C_1 \\ C_1 & C_0 \end{pmatrix} \subset M_2(C).$$

The map $Z \otimes V = \mathrm{Alt}^\sigma(C_1) \to E$, $x \mapsto \left(\begin{smallmatrix} 0 & x \\ x & 0 \end{smallmatrix}\right)$ extends to an isomorphism $Z \otimes C \tilde{\to} E$ of Z–algebras and we identify $Z \otimes C$ with E through this isomorphism. Let $f : V \to V$ be a special similitude with multiplier ν. The map

$$\begin{pmatrix} 0 & x \\ x & 0 \end{pmatrix} \in Z \otimes V \mapsto \begin{pmatrix} 0 & \nu^{-1}f(x) \\ f(x) & 0 \end{pmatrix} \in\ E = Z \otimes C$$

extends to an automorphism φ of $Z \otimes C$. As in the proof of Theorem 12 of Chapter 9, one checks that $\varphi = i_u$ with $u \in (Z \otimes C_0)^\bullet$. As in Lemma 4, Chapter 6, we have $\sigma(u)u \in Z^\bullet$. The standard involution of $Z \otimes C$ viewed as an involution of E corresponds to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} \sigma(d) & \sigma(b) \\ \sigma(c) & \sigma(a) \end{pmatrix}.$$

Since

$$Z \otimes C_0 = \begin{pmatrix} {}_\sigma C_0 & 0 \\ 0 & C_0 \end{pmatrix},$$

the condition $\sigma(u)u \in Z^\bullet$ implies

$$u = \begin{pmatrix} \lambda^{-1}\sigma(d)^{-1} & 0 \\ 0 & d \end{pmatrix}$$

for some $d \in C_0^\bullet$ and $\lambda \in Z^\bullet$. If follows that $(1 \otimes f)(x) = \lambda d x \sigma(d)$. Since if $1 \otimes f$ descends to $f : C \to V$, we must have $\lambda\sigma_0(\lambda)^{-1} = n(d)^{-1}\mu(u)^2$ and $f = \rho(\lambda, d)$.

As for $\mathrm{Spin}(V, q)$, the computation of $GO_+(q)$ given in Theorem 16 can be applied to a lot of cases (see the Appendix A), depending on the type of (V, q). We only consider the cases of trivial Arf invariant. We may assume that (V, q) represents 1, so $(V, q) = (\mathrm{Alt}^\tau(A), pf_A)$ for some *c.s.* K–algebra of dimension 16 with an even symplectic involution τ. We have $C_0 \simeq A \times A$, $\sigma(a, b) = (\tau(b), \tau(a))$,

$$GU_1(C_0) = \{(\lambda\tau(d)^{-1}, d), \ \ d \in A^\bullet, \ \ \lambda \in K^\bullet\}$$

so $\mu(u) = \lambda$ for $u = (\lambda\tau(d)^{-1}, d)$ and

$$n(u)\mu(u)^{-2} = (\lambda^2\sigma_0(n_A(d))^{-1}, n_A(d)\lambda^{-2}) = z\sigma_0(z)^{-1}$$

for $z = (1, n_A(d)\lambda^{-2})$, where n_A is the reduced norm of A. Projecting $Z^\bullet \times C_0^\bullet$ onto the second factor $K^\bullet \times A^\bullet$, we get

$$G \simeq K^\bullet \times A^\bullet$$

and

$$GO_+(q) \simeq K^\bullet \times A^\bullet / \{(\lambda^2, \lambda^{-1}), \ \ \lambda \in K^\bullet\}.$$

Chapter 12

Quadratic Forms of Dimension 5

The theory of $\frac{1}{2}$–regular quadratic forms of dimension 5 is a by–product of the theory of quadratic spaces of dimension 6. We begin with an example:

Example 1. Let A be a *c.s.* K–algebra of dimension 16 with an even symplectic involution σ_A and let

$$\mathrm{Alt}^{\sigma_A}(A) = \{x + \sigma_A(x), \ \ x \in A\}$$

be the corresponding set of alternating elements. Let $pf_A : \mathrm{Alt}^{\sigma_A}(A) \to K$ be the reduced pfaffian. For any $a \in \mathrm{Alt}^{\sigma_A}(A)$. we have a pfaffian characteristic polynomial $\pi\chi(X, a) = X^2 - pft(a)X + pf_A(a)$ (see Chapter 10) and $\pi\chi(a, a) = 0$. To simplify notations, we put

$$\mathrm{Alt}^{\sigma_A}(A) = A_+, \quad pft(a) = t_+(a), \quad pf_A(a) = n_+(a)$$

and

$$A'_+ = \{a \in A_+ \mid t_+(a) = 0\}.$$

We check that (A'_+, n_+) is $\frac{1}{2}$–regular of dimension 5 and compute its Clifford algebra. Let Z be the graded quadratic K–algebra with a generator z of degree 1 such that $z^2 = 1$. We grade $A \otimes Z$ by assuming that the elements of A are of degree 0.

Proposition 2. 1) $(A'_+, -n_+)$ is $\frac{1}{2}$–regular of dimension 5. 2) There exists a graded isomorphism $C(A'_+, -n_+) \tilde{\to} A \otimes Z$. In particular $C_0(A^+, -n_+) \tilde{\to} A$ and the $\frac{1}{2}$–discriminant of $(A'_+, -n_+)$ is trivial. 3) The standard involution of $C(A_+, -n_+)$ corresponds to the involution $\sigma_A \otimes \sigma_0$, where σ_0 is the standard involution of Z, i.e. $\sigma_0(z) = -z$.

Proof. If suffices to prove 1) over an extension $K \subset L$ so that we can assume that $A = M_2(B)$, B a quaternion algebra with standard involution $b \mapsto \overline{b}$ and σ_A is given by (see Example 5 of Chapter 10)

$$\sigma_A \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix}.$$

Then

$$A_+ = \Big\{ \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} \quad x,\ y \in K,\ \ b \in B \Big\},$$

$$n_+ \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} = x\,y - b\,\overline{b}, \quad t_+ \begin{pmatrix} x & \overline{b} \\ b & y \end{pmatrix} = x + y,$$

$$A'_+ = \Big\{ \begin{pmatrix} x & \overline{b} \\ b & -x \end{pmatrix}, \quad x \in K, \quad b \in B \Big\},$$

and $(A'_+, -n_+) \simeq \langle 1 \rangle \perp (B, n_B)$ is $\frac{1}{2}$–regular. We have $a^2 = -n_+(a)$ since a satisfies its pfaffian characteristic polynomial and $t_+(a) = 0$. Thus the map

$$\varphi : A'_+ \to A \otimes Z, \quad \varphi_1(a) = a \otimes z,$$

extends, by the universal property of the Clifford algebra, to a homomorphism of graded K–algebras

$$\varphi : C(A'_+, -n_+) \to A \otimes Z.$$

Let $Z(C)$ be the centre of $C(A'_+, -n_+)$. We claim that the restriction of φ to $Z(C)$ is an isomorphism $Z(C) \tilde{\to} Z$. By passing to an extension $K \subset L$, we may assume that $(A_+, -n_+) = \langle 1 \rangle \perp (M_2(K), \det)$. Then $Z(C)$ is generated by

$$z_1 = e_0(1 - 2e_1 f_1)(1 - 2e_2 f_2),$$

where e_0 is the generator of $\langle 1 \rangle$ and the elements

$$e_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad f_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

are hyperbolic pairs in $M_2(K)$ (see Chapter 5). A computation (!) shows that $\varphi(z_1) = z$, thus as claimed $\varphi : Z(C) \tilde{\to} Z$. It then follows that φ maps $C_0(A'_+, -n_+)$ to A and is an isomorphism. To prove 3), we observe that the restriction of $\sigma_A \otimes \sigma_0$ to the image of A'_+ is -1.

Let (V, q) be a $\frac{1}{2}$–regular quadratic form of dimension 5. Since there exists an extension $K \subset L$ such that $L \otimes (V, q) \simeq \langle 1 \rangle \perp H(K^2) \simeq \langle 1 \rangle \perp (M_2(K), \det)$, it follows from Proposition 2 that the standard involution of $C_0(V,q)$ is of even symplectic type. Let C_{0+} be the corresponding set of alternating elements and $n_+ : C_{0+} \to K$ the reduced pfaffian. Let $z \in Z(q)$ be a generator of degree 1 with $z^2 = s$ and $[s] = \frac{1}{2}\delta(q)$ in $K^\bullet/K^{\bullet 2}$ (see Proposition 5 of Chapter 5), and let $\rho : V \to C_0$ be the map induced by $v \mapsto zv$. By going over to an extension $K \subset L$ and applying Proposition 2, we get that ρ is an isometry

$$(12.1) \qquad (V,q) \tilde{\to} (C'_{0+}, -sn_+).$$

Theorem 3. 1) Let (V,q) be a $\frac{1}{2}$–regular quadratic form of dimension 5. There exists $\lambda \in K^\bullet$ and A *c.s.* of dimension 16 with an even symplectic involution σ_A such that $(V,q) \simeq (A'_+, \lambda n_+)$. The class of λ in $K^\bullet/K^{\bullet 2}$ is equal to $\frac{1}{2}\delta(q)$ and (A,σ_A) is unique up to isomorphism of algebras–with–involution. 2) Two $\frac{1}{2}$–regular quadratic forms (V,q), (V',q') are isometric if and only if $\frac{1}{2}\delta(q) = \frac{1}{2}\delta(q')$ and $C_0(q) \simeq C_0(q')$ as algebras–with–(standard)–involution. 3) (V,q), (V',q') are similar if and only if $C_0(q) \simeq C_0(q')$ as algebras–with–involution.

Proof. 1) We take $\lambda = -s$ and $A = C_0$ with the standard involution.
2) It suffices to check that an isomorphism $\varphi : (A,\sigma_A) \to (B,\sigma_B)$ of algebras–with–involution induces an isometry $(A'_+, n_+) \tilde{\to} (B', n_+)$. Clearly φ maps A_+ to B_+. Let $\pi_A : A_+ \to A_+$ be such that $x\pi_A(x) = \pi_A(x)x = pf_A(x)$ and $\pi_B : B_+ \to B_+$ such that $x\pi_B(x) = \pi_B(x)x = pf_B(x)$. Let $\gamma = \varphi\pi_A\varphi^{-1} : B_+ \to B_+$. Since γ is a K–linear isomorphism such that $\gamma(x)x \in K$ for all $x \in B_+$, $\gamma = \lambda\pi_B$ for $\lambda \in K^\bullet$. It follows from $\gamma(1) = 1$ that $\lambda = 1$ and $\varphi\pi_A = \pi_B\varphi$. Thus φ is an isometry $(A_+, n_+) \tilde{\to} (B_+, n_+)$. The fact that φ restricts to an isometry $(A'_+, n_+) \tilde{\to} (B'_+, n_+)$ follows from the formula $x + \pi_A(x) = t_+(x)$ (see Example 5 of Chapter 10). Finally 3) follows from (12.1).

Remark 4. In view of Proposition 6 of Chapter 7, Corollary 3 of Chapter 8, Theorem 7 of Chapter 9, Theorem 10 of Chapter 11 and Theorem 3 above, two quadratic forms (V,q), (V',q') which are of dimension ≤ 6 and are nonsingular in even dimension, resp. $\frac{1}{2}$–regular in odd dimension, are similar if and only if the even Clifford algebras $C_0(q)$ and $C_0(q')$ are isomorphic as algebras–with–involution, where the involutions are the standard involutions.

The next result is due to Tamagawa in the case of (signed) trivial discriminant. We do not know if it holds for $\frac{1}{2}$–regular forms of dimension 5 in characteristic 2.

Proposition 5. Let K be a field of characteristic different from 2 and let (V,q) be a quadratic space of dimension 5 and signed discriminant $[d] \in K^\bullet/K^{\bullet 2}$. The following conditions are equivalent:

1) (V,q) represents d.
2) $(V,q) \simeq \langle d\rangle \perp (B, \lambda n_B)$ for some quaternion algebra B and $\lambda \in K^\bullet$.
3) $C_0(V,q) \simeq M_2(B)$ for some quaternion algebra B.

Thus C_0 is a division algebra if and only if (V,q) does not represent d.

Proof. 1) implies 2) by Remark 11 of Chapter 9, since $\langle d\rangle^\perp$ is a quadratic space of dimension 4 with trivial discriminant (and hence trivial Arf invariant). If 2) holds, then $C_0(V,q) \simeq C(B, -d\lambda n_B)$ by Lemma 8 of Chapter 5 and $C(B, -d\lambda n_B) \simeq M_2(B)$ by Example 1 of Chapter 9. Let now $C_0(V,q) \simeq M_2(B)$. By Lemma 8 of Chapter 5, we have

$$C_0(\langle -d\rangle \perp q) \simeq C(dq) \simeq C_0(dq) \otimes Z(dq) \simeq C_0(q) \times C_0(q)$$

(since $Z(dq) \simeq K \times K$). On the other hand $\langle -d\rangle \perp q$ is of dimension 6 and has trivial Arf invariant. By Corollary 5 of Chapter 11 (applied to the form $\langle -d\rangle \perp q$ and $A = C_0(dq)$), we get that $C_0(q) \simeq C_0(dq) \simeq M_2(B)$ if and only if $\langle -d\rangle \perp q$ has Witt index ≥ 1. Thus $C_0(q) \simeq M_2(B)$ implies that

$$\langle -d\rangle \perp q \simeq \langle -1\rangle \perp \langle 1\rangle \perp q' \simeq \langle -d\rangle \perp \langle d\rangle \perp q'$$

and

$$q \simeq \langle d\rangle \perp q'$$

by Witt cancellation. As claimed, q represents d.

We now compute the spinor group of a $\frac{1}{2}$–regular form of dimension 5. By Theorem 3 we may assume that $(V,q) = (A'_+, -n_+)$ for a *c.s.* K–algebra A of dimension 16 with an involution σ of even symplectic type. In view of Proposition 2 $C_0(V,q) \simeq A$ and the standard involution on C_0 is the involution σ of A. For any

$u \in A$, let $\mu(u) = u\sigma(u)$ and $n(u) = n_A(u)$. We have $Z(q) = K \cdot 1 \oplus K \cdot z$ with z of degree 1 such that $z^2 = 1$. Through the map $V \to C_0$, $v \mapsto zv$, we can identify $V \simeq A'_+ \subset C_1$ with A'_+ as a subspace of $A = C_0$. Any isometry φ of V extends to an automorphism of $A = C_0$ as an algebra–with–involution, hence to an isometry of (A_+, n_+) (or $(A_+, -n_+)$), which restricts to φ on A'_+. Thus for any $u \in A^\bullet$, i_u is an isometry of A'_+ (i.e. $i_u(A'_+) \subset A'_+$) if and only if $i_u(A_+) \subset A_+$. By Lemma 4 of Chapter 6, $\mu(u) \in K^\bullet$ if $u \in S\Gamma(A'_+, -n_+)$. On the other hand, obviously $i_u(A_+) \subset A_+$ if $u^{-1} = \nu\sigma(u)$, $\nu \in K^\bullet$. Thus

$$S\Gamma(A'_+, -n_+) = \{u \in A^\bullet \mid u\sigma(u) \in K\}.$$

We recall that a matrix $g \in M_n(A)$ is hermitian (with respect to σ) if $g = g^*$, where

$$g^* = (\sigma(a_{ij}))^t \qquad \text{if} \qquad g = (a_{ij}).$$

The group

$$GU_n(A, g) = \{x \in GL_n(A) \mid xgx^* = \lambda g, \ \ \lambda \in K^\bullet\}$$

is the group of (unitary) similitudes of g (see Chapter 11). With this definition,

$$S\Gamma(A'_+, -n_+) = GU_1(A, 1)$$

and

$$SO_+(A'_+, -n_+) \simeq GU_1(A, 1)/K^\bullet.$$

We claim that

$$\mathrm{Spin}(A'_+, -n_+) = \{x \in A^\bullet \mid x\sigma(x) = 1\}.$$

We have to check that $n_A(u) = 1$ if $u\sigma(u) = 1$. By passing to an extension $K \subset L$, we may assume that $A = M_4(K)$ and $\sigma(a) = s_2 a^t s_2^{-1}$. It follows from $u\sigma(u) = 1$ that $s_2 = us_2u^t$. Taking pfaffians shows that $\det(u) = 1$ as claimed. The map

$$\mathrm{Spin}(A'_+, -n_+) \to SO(A'_+, -n_+)$$

is given by $u \mapsto (x \mapsto uxu^{-1} = ux\sigma(u))$. In fact $x \mapsto ux\sigma(u)$ is an isometry since $n_+(ux\sigma(u)) = n_A(u)n_+(x)$ and $n_A(u) = 1$.

We consider now some special cases. Let

$$(V, q) = \langle 1 \rangle \perp (B, \lambda n_B)$$

for a quaternion algebra B with standard involution $b \mapsto \overline{b}$ and $\lambda \in K^\bullet$. By Lemma 8 of Chapter 5, we have $C_0(V,q) \simeq C(B, -\lambda n_B)$ and by Example 1 of Chapter 9, $C(B, -\lambda n_B) \simeq M_2(B)$ with the standard involution given by

$$\sigma : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} \overline{a} & \lambda^{-1}\overline{c} \\ \lambda\overline{b} & \overline{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}^t \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}^{-1}.$$

Therefore

$$SO_+(V,q) \simeq GU_2(B, diag(1,\lambda))/K^\bullet$$

and

$$\mathrm{Spin}(V,q) \simeq SU_2(B, diag(1,\lambda)).$$

If $B = M_2(K)$ and $\lambda = 1$, then $\overline{b} = s_1 b^t s_1^{-1}$, so

$$\begin{aligned} S\Gamma(\langle 1\rangle \perp H(K^2)) &= \{x \in GL_4(K) \mid x s_2 x^t s_2^{-1} \in K^\bullet\} \\ &= GSp_4(K) \end{aligned}$$

and

$$\begin{aligned} \mathrm{Spin}(\langle 1\rangle \perp H(K^2)) &= \{x \in GL_4(K) \mid x s_2 x^t s_2^{-1} = 1\} \\ &= Sp_4(K), \end{aligned}$$

if we define the *group of symplectic similitudes* $GSp_{2m}(K)$ by

$$GSp_{2m}(K) = \{x \in GL_{2m}(K) \mid x s_m x^t = \lambda s_m,\ \lambda \in K^\bullet\}.$$

and the *symplectic group* $Sp_{2m}(K)$ by

$$Sp_{2m}(K) = \{x \in GL_{2m}(K) \mid x s_m x^t = s_m\}$$

We finally show that $\langle 1\rangle \perp H(K^2)$ can be identified in a natural way with a subspace of $\mathrm{Alt}_4(K)$, the set of alternating (4×4)–matrices.

We have

$$\langle 1\rangle \perp H(K^2) = (M_4(K)'_+, -n_+)$$

for the involution $\sigma(x) = s_n x^t s_2^{-1}$, and the map $\theta : x \to s_2^{-1}x$ is an isometry

$$\theta : (M_4(K)_+, -n_+) \tilde{\to} (\mathrm{Alt}_4(K), -pf)$$

by definition of n_+. Since

$$M_4(K)'_+ = \left\{ \begin{pmatrix} x & 0 & d & -b \\ 0 & x & -c & a \\ a & b & -x & 0 \\ c & d & 0 & -x \end{pmatrix} \in M_4(K) \right\},$$

$M_4(K)'_+$ has image

$$\theta(M_4(K)'_+) = \left\{ \begin{pmatrix} 0 & -x & c & -a \\ x & 0 & d & -b \\ -c & -d & 0 & x \\ a & b & -x & 0 \end{pmatrix} \in M_4(K) \right\}.$$

We call matrices in $\theta(M_4(K)'_+)$ *alternating matrices with pfaffian trace zero* and denote $\theta(M_4(K)'_+)$ by $\mathrm{Alt}'_4(K)$. Let $u \in \mathrm{Spin}(M_4(K)'_+, -n_+)$, since $\theta\ i_u\ \theta^{-1}(x) = s_2^{-1}us_2xu^{-1} = u^{t-1}xu^{-1}$, the map

$$s\pi : \mathrm{Spin}(M_4(K)'_+, -n_+) \to SO(M_4(K)'_+, -n_+)$$

corresponds through θ to the map

$$Sp_4(K) \to SO(\mathrm{Alt}'_4(K), -pf)$$

defined by $u \mapsto (x \mapsto u^{t-1}xu^{-1})$.

We finally compute the Lie algebra of $(V, q) = (A'_+, -n_+)$. Let

$$\mathcal{S}(A) = \{x \in A \mid x + \sigma(x) = 0\}.$$

We have $so(q) \subset \mathcal{S}(A)$. Since $\mathrm{Dim}_K \mathcal{S}(A) = 10$, we get

$$so(A'_+, -n_+) = \mathcal{S}(A) = \{x \in A \mid x + \sigma(x) = 0\}.$$

Appendix A

A Chart of Results

We summarize in the following chart all the information we have obtained in these notes on the structure of Clifford algebras of forms of dimension ≤ 6. We restrict to nonsingular forms, so we assume that char $K \neq 2$ in odd dimensions. We use the following notations:

ℓ	:	the dimension of V
ν	:	the Witt index of (V, q)
L	:	a separable quadratic field extension of K
D_m	:	a central division algebra over K of dimension m^2
$L \otimes D_m$	:	a central division algebra over L of dimension m^2 induced by scalar extension from a central division algebra over K
$M_n(R)$	:	the ring of $n \times n$–matrices over R.

ℓ	(V, q)	$Z(q)$	$C_0(q)$	$C(q)$
2	$\nu = 0,\ 1 \in q(V)$	L	L	$M_2(K)$
	$\nu = 0,\ 1 \notin q(V)$	L	L	D_2
	$\nu = 1$	$K \times K$	$K \times K$	$M_2(K)$
3	$\nu = 0$	$K \times K$	D_2	$D_2 \times D_2$
	$\nu = 0,\ \nu(L \otimes q) = 0$	L	D_2	$L \otimes D_2$
	$\nu = 0,\ \nu(L \otimes q) = 1$	L	D_2	$M_2(L)$
	$\nu = 1$	$K \times K$	$M_2(K)$	$M_2(K) \times M_2(K)$
	$\nu = 1$	L	$M_2(K)$	$M_2(L)$

ℓ	(V,q)	$Z(q)$	$C_0(q)$	$C(q)$
4	$\nu=0$	$K\times K$	$D_2\times D_2$	$M_2(D_2)$
	$\nu((V,-q)\perp(L,n))=0$	L	$L\otimes D_2$	D_4
	$\nu=0,\ \nu((V,-q)\perp(L,n))=1$	L	$L\otimes D_2$	$M_2(D_2)$
	$\nu=1,\ 1\in q(H(K)^\perp)$	L	$M_2(L)$	$M_4(K)$
	$\nu=1,\ 1\notin q(H(K)^\perp)$	L	$M_2(L)$	$M_2(D_2)$
	$\nu=2$	$K\times K$	$M_2(K)\times M_2(K)$	$M_4(K)$

ℓ	(V,q)	$Z(q)$	$C_0(q)$	$C(q)$
5	Let $L=K(\sqrt{d}),\ d\notin K^{\bullet 2}$.			
	$\nu=0,\ 1\notin q(V)$	$K\times K$	D_4	$D_4\times D_4$
	$\nu=0,\ 1\in q(V)$	$K\times K$	$M_2(D_2)$	$M_2(D_2)\times M_2(D_2)$
	$\nu=0,\ d\notin q(V),\ 1\notin q(L\otimes V)$	L	D_4	$L\otimes D_4$
	$\nu=0,\ d\notin q(V),\ 1\in q(L\otimes V)$, $\nu(\langle 1\rangle^\perp)=0$ in $L\otimes V$	L	D_4	$M_2(L\otimes D_2)$
	$\nu=0,\ d\notin q(V),\ 1\in q(L\otimes V)$, $\nu(\langle 1\rangle^\perp)=2$ in $L\otimes V$	L	D_4	$M_4(L)$
	$\nu=0,\ d\in q(V)$, $\nu(L\otimes\langle d\rangle^\perp)=0$	L	$M_2(D_2)$	$M_2(L\otimes D_2)$
	$\nu=0,\ d\in q(V)$, $\nu(L\otimes\langle d\rangle^\perp)=2$	L	$M_2(D_2)$	$M_4(L)$
	$\nu=1$	$K\times K$	$M_2(D_2)$	$M_2(D_2)\times M_2(D_2)$
	$\nu=1,\ \nu(L\otimes q)=1$	L	$M_2(D_2)$	$M_2(L\otimes D_2)$
	$\nu=1,\ \nu(L\otimes q)=2$	L	$M_2(D_2)$	$M_4(L)$
	$\nu=2$	$K\times K$	$M_4(K)$	$M_4(K)\times M_4(K)$
	$\nu=2$	L	$M_4(K)$	$M_4(L)$

ℓ	(V,q)	$Z(q)$	$C_0(q)$	$C(q)$
6	$\nu=0$	$K\times K$	$D_4\times D_4$	$M_2(D_4)$
	$\nu=0,\ \nu(L\otimes q)=0$	L	$L\otimes D_4$	?
	$\nu=0,\ \nu(L\otimes q)=1$	L	$M_2(L\otimes D_2)$	?
	$\nu=0,\ \nu(L\otimes q)=3$	L	$M_4(L)$	?
	$\nu=1$	$K\times K$	$M_2(D_2)\times M_2(D_2)$	$M_4(D_2)$
	$\nu=1,\ \nu((V,-q)\perp(L,n))=1$	L	$M_2(L\otimes D_2)$	$M_2(D_4)$
	$\nu=1,\ \nu((V,-q)\perp(L,n))=2$	L	$M_2(L\otimes D_2)$	$M_4(D_2)$
	$\nu=2,\ 1\in q(H(K^2)^\perp)$	L	$M_4(L)$	$M_8(K)$
	$\nu=2,\ 1\notin q(H(K^2)^\perp)$	L	$M_4(L)$	$M_4(D_2)$
	$\nu=3$	$K\times K$	$M_4(K)\times M_4(K)$	$M_8(K)$

It would be interesting to know the structure of the Clifford algebra $C(q)$ for $\ell=6,\ \nu=0$ and $Z(q)\simeq L$. In particular one would like to know under which conditions (on q) $C(q)$ is a division algebra. We observe that the case $\nu=0,\ \nu(L\otimes q)=0$ cannot occur over $\mathbb{Q}$: Let d be the signed discriminant of q, so that $L=\mathbb{Q}(\sqrt{d})$. By Meyer's theorem (see Serre) any quadratic space of dimension ≥ 5 over $\mathbb{Q}$, which is indefinite over $\mathbb{R}$, is isotropic. So d must be negative. Let now $x\neq 0\in V$. The quadratic form $q|_{x^\perp}\perp dq|_{\mathbb{Q}x}$ is isotropic, again by Meyer's theorem, since it is indefinite over $\mathbb{R}$. Thus there exists $y \perp x$ such that $q(y) = -dq(x)$ and $L \otimes q$ is isotropic. The case $\nu = 0$, $\nu(L \otimes q) = 1$ cannot occur over $\mathbb{R}$ but can occur over $\mathbb{Q}$. An example is given by the form $\langle 1, 1, 1, 1, 1, 7\rangle$. Let $L = \mathbb{Q}(\sqrt{-7})$. If $L \otimes q$ is hyperbolic, then $L \otimes \langle 1, 1, 1, 1\rangle$ is hyperbolic, since $L \otimes \langle 1, 7\rangle$ is hyperbolic. Thus the quaternion algebra $(\frac{-1, -1}{L})$ is a matrix algebra. This is the case if $\langle 1, 1\rangle$ represents -1 over L. It would follow that -1 is a square modulo 7.

Appendix B

Spinors

We define spinors as in the book of Chevalley and compute some examples from physics. We shall only consider nonsingular forms and assume that the characteristic is not equal to 2. More on applications of Clifford algebras to physics can be read for example in the book of Hermann.

I. Spaces of even dimension.

In view of Theorem 8 of Chapter 4, the Clifford algebra $C = C(q)$ of a quadratic space (V, q) of even dimension is simple. Thus there exists up to isomorphism only one type of simple $C(q)$–modules or, in the language of representation theory, all irreducible representations of $C(q)$ are equivalent. If we select such a representation, $\rho : C(q) \to \mathrm{End}_K(W)$, we call W the *space of spinors* of (V, q), ρ the *spin representation* of $C(q)$ and the restriction ρ_0 of ρ to $C_0 = C_0(q)$ the *spin representation* of C_0 . Thus *spinors* are elements of a fixed simple $C(q)$–module. The representation ρ induces representations of $\Gamma(q), S\Gamma(q)$ and $\mathrm{Spin}(q)$. The algebra C_0 is either simple (if its center is a field) or the sum of two simple algebras (if $Z(q) \simeq K \times K$), see Theorem 8 of Chapter 4.

Lemma 1. Let $\rho : \ C \to \mathrm{End}_K(W)$ be an irreducible representation of C. The restriction ρ_0 of ρ to C_0 is irreducible if C_0 is simple and is the sum of two nonequivalent irreducible representations $\rho_0^+ : \ C_0 \to \mathrm{End}_K(W^+)$, $\rho_0^- : \ C_0 \to \mathrm{End}_K(W^-)$ if C_0 is not simple.

Proof. Since all irreducible representations of C are equivalent, we may assume that W is a minimal left ideal of C and that ρ is the regular representation, i.e. $\rho(u)y = uy$. Let $W' \neq \{0\}$ be a subspace of W of minimal dimension which is invariant under all operations $\rho_0(x)$, $x \in C_0$, so that the induced representation $C_0 \to \mathrm{End}_K(W')$ is irreducible. Let $x \in V$ be anisotropic and let $W'' = \rho(x)W'$. Since $C_1 = xC_0 = C_0x$ and $C_0 = xC_1 = C_1x$, we get $\rho_0(C_0)W'' = W''$ and $\rho(C)(W' + W'') = W' + W''$. Since ρ is irreducible, we must have $W = W' + W''$. If $W' \cap W'' \neq \{0\}$, the minimality of W' implies that $W' \cap W'' = W'$. Since W' and W'' have the same dimension, it follows that $W = W' = W''$. If $W' \cap W'' = \{0\}$, then $W = W' \oplus W''$. Thus the representation ρ_0 is either irreducible or the sum of two irreducible representations. Assume now that C_0 is not simple. Then C_0 has two types of nonequivalent irreducible representations (see Theorem 8 of Chapter 4). The representation ρ_0 being faithful, these two types occur in ρ_0. Therefore, as claimed, ρ_0 is the sum of two nonequivalent irreducible representations $W^+ = W'$ and $W^- = W''$. This case occurs if K is algebraically closed. Thus we see, by going over to the algebraic closure, that, if ρ_0 is the sum of two irreducible representations, these representations cannot be equivalent. It follows that ρ_0 must be irreducible if C_0 is simple.

The elements of W^+, W^- are called $\frac{1}{2}$*–spinors* (if W' is not equivalent to W'') and the induced representations of C_0 are the $\frac{1}{2}$*–spin representations.*

Lemma 2. Let (V, q) be a nonsingular quadratic space (of arbitrary finite dimension) non isometric to $H(\mathbb{F}_3)$. Let $v \in V$ be anisotropic and let $M = \{x \in V \mid q(x) = q(v)\}$. 1) The set M generates as a linear space V. 2) $C_0(q)$ is generated as a K–algebra by all products xy, $x, y \in M$. 3) $S\Gamma(q)$ is a set of generators of $C_0(q)$. 4) $\mathrm{Spin}(q)$ is a set of generators of $C_0(q)$.

Proof. 1) Let U be the linear hull of M. Let $w \in V$ be an anisotropic element and let τ_w be the reflection at w. Since $\tau_w(v) = v - \frac{b(v,w)}{q(w)}w$, we get that either $w \in U$ or $w \in U^\perp$. Since V has an orthogonal basis we must have $V = U \perp U^\perp$. Assume now that $U^\perp \neq 0$. Let $v \in M$ and $w \neq 0 \in M^\perp$. For any $\lambda \neq 0 \in K$, the element $\lambda v + w$ is isotropic, thus $\lambda^2 q(v) + q(w) = q(v) + q(w) = 0$ and $\lambda^2 = 1$. There exists only one field K of characteristic not 2 such that $\lambda^2 = 1$ for all $\lambda \neq 0 \in K$, namely $I\!F_3$. Since $V = U \perp U^\perp$, U and $U^\perp$ are nonsingular. It is then easy to see that $\mathrm{Dim}_K U = \mathrm{Dim}_K U^\perp = 1$ and $V = H(I\!F_3)$. 2) and 3) are immediate consequences of 1). We check 4). Since $C_0(q)$ is generated by all products of two elements of M, it is also generated by the products $a^{-1}xy$ with $a = q(x) = q(y)$. But $a^{-1}xy$ belongs to $\mathrm{Spin}(q)$.

Proposition 3. Assume that (V,q) is nonsingular of even dimension and $(V,q) \not\simeq H(I\!F_3)$. The spin representations of $S\Gamma(q)$ and $\mathrm{Spin}(q)$ are either irreducible or the sum of two irreducible nonequivalent representations.

Proof. Proposition 3 is an immediate consequence of Lemma 1 and Lemma 2.

II. Spaces of odd dimension.

Since we restrict to nonsingular forms, we must have $\mathrm{char} K \neq 2$. The algebra $C_0(q)$ is *c.s.*, hence its irreducible representations are all equivalent. We fix one, which we call the *spin representation:*

$$\rho_0 : C_0(q) \to \mathrm{End}_K(W).$$

The elements of W are called *spinors* of (V,q).

Proposition 4. The induced representations $\rho_0 : S\Gamma(q) \to \mathrm{End}_K(W)$, $\rho_0 : \mathrm{Spin}(q) \to \mathrm{End}_K(W)$ are irreducible.

Proof. As Proposition 3.

If $C(q)$ is simple, then $C(q) = L \otimes C_0(q)$, $K \subset L$ a quadratic field extension and ρ_0 can be extended in an unique way to an irreducible representation of $C(q)$:

$$1 \otimes \rho : L \otimes C_0(q) = C(q) \to \mathrm{End}_L(L \otimes W).$$

We call this representation the *spin representation* of $C(q)$.

Proposition 5. If $C(q)$ is not simple, then ρ_0 can be extended to exactly 2 non equivalent irreducible representations of C.

Proof. If $C(q)$ is not simple, we have $Z(q) \simeq K[x]/(x^2 - 1)$. Let z be a generator of degree 1 of $Z(q)$ such that $z^2 = 1$. Any $u \in C(q)$ has a unique representation $u = u_1 + u_2 z, \;\; u_i \in C_0(q)$. Since z is in the centre of $C(q)$ the maps

$$\varphi' : u \mapsto u_1 + u_2 \text{ and } \varphi'' : u_1 - u_2$$

are homomorphisms $C \to C_0$ of K–algebras. The representations $\rho' = \rho_0 \circ \varphi'$ and $\rho'' = \rho_0 \circ \varphi''$ extend ρ_0 to C. Conversely let $\rho : C \to \mathrm{End}_K(W)$ be an irreducible representation which extends ρ_0. Let $\psi = \rho(z) \in \mathrm{End}_K(W)$. We have $\psi^2 = 1$ and ψ commutes with all elements $\rho_0(C_0)$. Therefore $W = W_1 \oplus W_2$, where

$$W_1 = \{x \in W \mid \psi(x) = x\} \text{ and } W_2 = \{x \in W \mid \psi(x) = -x\}.$$

These spaces are invariant under $\rho_0(C_0)$. Since ρ is irreducible, one is zero and the other W. Thus $\psi = \pm 1$ and ρ is one of the representations ρ' or ρ''.

If $C(q)$ is not simple, the two non equivalent representations of $C(q)$ given by Proposition 5 are called the *spin representations* of $C(q)$.

In chapter 6 we identified the Lie algebra $so(q)$ with a subalgebra of $C_0(q)$. Thus a spin representation of $C_0(q)$ induces, by restriction, a representation of $so(q)$. We call this representation the spin representation of $so(q)$.

The chart of Appendix A gives an (abstract) description of spin representations in low dimensions. To have a concrete description, we need explicit representations of the Clifford algebras, i.e. explicitly given simple $C(q)$–modules. We now construct such representations for three cases occuring in physics. In some of the examples, we get representations over the real quaternions $\mathbb{H}$. Writing any quaternion z as $x + jy, \; x, y \in \mathbb{C}$, we define an injective map $\rho : \; \mathbb{H} \to M_2(\mathbb{C})$ through the regular representation $\ell_a(z) = az$. In the following we shall identify $\mathbb{H}$ with its image

$$\rho(\mathbb{H}) = \left\{ \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix}, \quad x,\, y \in \mathbb{C} \right\} \subset M_2(\mathbb{C}).$$

In particular we get for the pure quaternions

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad k = ij = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Example 6. Let $(V,q) = \langle 1,1,1 \rangle$ over $\mathbb{R}$. The algebra $C(q)$ is the *Pauli algebra.* We have (see Appendix A)

$$C(q) \simeq M_2(\mathbb{C}) \ \text{ and } \ C_0(q) \simeq \mathbb{H}.$$

Explicit isomorphisms can be constructed using the *Pauli matrices:*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{in} \quad M_2(\mathbb{C}).$$

Let $\{e_1, e_2, e_3\}$ be an orthonormal basis of V. We define

$$\varphi' : V \to M_2(\mathbb{C})$$

by $e_i \mapsto \sigma_i, \ \ i = 1,2,3$. By the universal property of the Clifford algebra, φ' extends to a homomorphism $\varphi : C(q) \to M_2(\mathbb{C})$. It is easy to check that φ' is a $\mathbb{C}$–linear isomorphism if we identify $\mathbb{C}$ with $Z(q)$ through $i \mapsto e_1e_2e_3$. The subalgebra $C_0(q)$ is mapped by φ onto the $\mathbb{R}$–subalgebra of $M_2(\mathbb{C})$ with basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1\sigma_2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \sigma_1\sigma_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2\sigma_3 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Thus φ restricts to an isomorphism $C_0 \tilde{\to} \mathbb{H}$. The isomorphism $\varphi : C \tilde{\to} M_2(\mathbb{C})$ is a spin representation. We construct an explicit representation: let $e = \frac{1}{2}\,(1 + e_3) \in C(q)$. We have $\varphi(e) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, so $\varphi(C(q)e) = \left(\begin{smallmatrix} \mathbb{C} & 0 \\ \mathbb{C} & 0 \end{smallmatrix}\right)$ and we can choose $W = \left(\begin{smallmatrix} \mathbb{C} & 0 \\ \mathbb{C} & 0 \end{smallmatrix}\right)$. Spinors are pairs $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \mathbb{C}^2$. Since $\mathrm{Spin}(V,q) = \{a \in C_0 \mid n_{C_0}(a) = 1\}$, φ induces an isomorphism

$$\begin{aligned} \mathrm{Spin}(V,q) \ &\tilde{\to} \ \{a \in \mathbb{H} \mid n_{\mathbb{H}}(a) = 1\} \\ &= \ SU_2(\mathbb{C}) = \left\{ \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix}, \ x,\ y \in \mathbb{C} \mid \det \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix} = 1 \right\}. \end{aligned}$$

The Lie algebra $so(q) = [V,V]$ is generated by $\sigma_1\sigma_2,\ \sigma_2\sigma_3$ and $\sigma_1\sigma_3$. Let

$$su_2(\mathbb{C}) = \left\{ \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix}, \ x,\ y \in \mathbb{C} \ \mid \ \mathrm{tr} \begin{pmatrix} x & -\overline{y} \\ y & \overline{x} \end{pmatrix} = 0 \right\},$$

we get $\varphi(so(q)) = su_2(\mathbb{C})$.

Example 7. Let $(V,q)=\langle 1,-1,-1,-1\rangle$ over $\mathbb{R}$. The algebra $C(q)$ is the *Minkowski algebra.* By Appendix A, we have

$$C(q)\simeq M_2(\mathbb{H}) \qquad \text{and} \qquad C_0(q)\simeq M_2(\mathbb{C}).$$

We construct explicit isomorphisms. Let $\{e_0,\ldots,e_3\}$ be an orthogonal basis of V such that $q(e_0)=1,\ \ q(e_i)=-1 \quad i=1,2,3$. Let $q_1=\langle 1,-1\rangle$ and $q_2=\langle -1,-1\rangle$, so

$$C(q_1)\tilde{\to}M_2(\mathbb{R}) \quad \text{with} \quad e_0\mapsto\begin{pmatrix}0&1\\1&0\end{pmatrix} \quad \text{and} \quad e_1\mapsto\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

$$C(q_2)\tilde{\to}\mathbb{H} \qquad \text{with} \qquad e_2\mapsto i, \qquad e_3\mapsto j$$

(where $i,\ j,\ k=ij$ are the pure quaternions in $\mathbb{H}$) and

$$\psi: C(q)\tilde{\to}M_2(\mathbb{R})\hat{\otimes}\mathbb{H}\tilde{\to}M_2(\mathbb{R})\otimes\mathbb{H}=M_2(\mathbb{H})$$

(the second isomorphism is as in Lemma 3 of Chapter 4). Explicitely

$$\psi(e_0)=\begin{pmatrix}0&1\\1&0\end{pmatrix}, \qquad \psi(e_1)=\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

$$\psi(e_2)=\begin{pmatrix}i&0\\0&-i\end{pmatrix} \qquad \text{and} \qquad \psi(e_3)=\begin{pmatrix}j&0\\0&-j\end{pmatrix}.$$

It is not obvious that ψ restricts to an isomorphism $C_0(q)\tilde{\to}M_2(\mathbb{C})$. Using a trick as in the proof of Theorem 8 of Chapter 4, we replace ψ by $\varphi=i_u\circ\psi$, where $u=\left(\begin{smallmatrix}1&0\\0&i\end{smallmatrix}\right)\in M_2(\mathbb{C})$. We get

$$\varphi(e_0)=\begin{pmatrix}0&-i\\i&0\end{pmatrix}, \qquad \varphi(e_1)=\begin{pmatrix}0&-i\\-i&0\end{pmatrix},$$

$$\varphi(e_2)=\begin{pmatrix}i&0\\0&-i\end{pmatrix} \qquad \text{and} \qquad \varphi(e_3)=\begin{pmatrix}j&0\\0&j\end{pmatrix}.$$

Then

$$\begin{aligned}
\varphi(e_0e_1) &= \begin{pmatrix}-1&0\\0&1\end{pmatrix}, & \varphi(e_0e_2) &= \begin{pmatrix}0&-1\\-1&0\end{pmatrix}, & \varphi(e_0e_3) &= \begin{pmatrix}0&-k\\k&0\end{pmatrix}\\
\varphi(e_1e_2) &= \begin{pmatrix}0&-1\\1&0\end{pmatrix}, & \varphi(e_1e_3) &= \begin{pmatrix}0&k\\k&0\end{pmatrix}, & \varphi(e_2e_3) &= \begin{pmatrix}k&0\\0&-k\end{pmatrix}
\end{aligned}$$

and

$$\varphi(e_0e_1e_2e_3)=\begin{pmatrix}-k&0\\0&-k\end{pmatrix},$$

so φ maps $C_0(q)$ to $M_2(\mathbb{C})$, with $\mathbb{C}=\mathbb{R}(k)$. The element $e=\frac{1+e_1e_0}{2}$ is an idempotent of $C(q)$ such that $\varphi(e)=\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. So $C(q)e$ is a space of spinors. We have

$$\varphi(C(q)e)=W=\begin{pmatrix}\mathbb{H}&0\\\mathbb{H}&0\end{pmatrix}.$$

By the general theory of Chapter 9 φ induces an isomorphism $\mathrm{Spin}(q) \simeq SL_2(\mathbb{C})$. Further the image of $so(q)$ is

$$sl_2(\mathbb{C}) = \{x \in M_2(\mathbb{C}) \mid \mathrm{tr}(x) = 0\}.$$

Example 8. Let $(V, q) = \langle 1, 1, 1, -1\rangle$ over $\mathbb{R}$. The algebra $C(q)$ is called the *Majorana algebra*. By our chart

$$C(q) \simeq M_4(\mathbb{R}) \quad \text{and} \quad C_0 \simeq M_2(\mathbb{C}).$$

We construct explicit isomorphisms. We decompose q as

$$q = q_1 \perp q_2 \quad \text{with} \quad q_1 = \langle -1, 1\rangle \quad \text{and} \quad q_2 = \langle 1, 1\rangle$$

and take corresponding orthogonal bases $\{e_0, e_1\}$, $\{e_2, e_3\}$. We have

$$C(q_1) \tilde{\to} M_2(\mathbb{R}), \quad e_0 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad e_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$C(q_2) \tilde{\to} M_2(\mathbb{R}), \quad e_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad e_3 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

These two isomorphisms induce

$$\begin{aligned} \psi : C(q) &\tilde{\to} C(q_1)\hat{\otimes}C(q_2) \simeq M_2(\mathbb{R})\hat{\otimes}M_2(\mathbb{R}) \\ &\tilde{\to} M_2(\mathbb{R}) \otimes M_2(\mathbb{R}) = M_4(\mathbb{R}), \end{aligned}$$

applying Lemma 3 of Chapter 4. Here again it is not obvious that ψ maps $C_0(q)$ to $M_2(\mathbb{C})$ and we first modify ψ to get a better representation (as in Example 7). To simplify notation, we use the symbols

$$\varepsilon = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \nu = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mu = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let now $\varphi = i_u \circ \psi$, where $u = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \varepsilon \end{smallmatrix}\right) \in M_4(\mathbb{R}) = M_2(M_2(\mathbb{R}))$. We have by definition of ψ

$$\psi(e_0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; \psi(e_1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$\psi(e_2) = \begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}, \; \psi(e_3) = \begin{pmatrix} \nu & 0 \\ 0 & -\nu \end{pmatrix},$$

where 1 stands for the (2×2)-unit matrix. So

$$\varphi(e_0) = \begin{pmatrix} 0 & \varepsilon \\ -\varepsilon & 0 \end{pmatrix}, \; \varphi(e_1) = \begin{pmatrix} 0 & \varepsilon \\ \varepsilon & 0 \end{pmatrix},$$

$$\varphi(e_2) = \begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix}, \ \varphi(e_3) = \begin{pmatrix} \nu & 0 \\ 0 & \nu \end{pmatrix}.$$

If we identify $\mathbb{C}$ with the subalgebra $\mathbb{R}(\varepsilon\nu)$ of $M_2(\mathbb{R})$ by putting $i = \varepsilon\nu$, we get

$$\varphi(e_0e_1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \varphi(e_0e_2) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \quad \varphi(e_0e_3) = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix},$$

$$\varphi(e_1e_2) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \varphi(e_1e_3) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \varphi(e_2e_3) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

and

$$\varphi(e_0e_1e_2e_3) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$$

so $\varphi : C_0(q) \simeq M_2(\mathbb{C})$ as claimed. The element $\tilde{e} = \frac{1+e_0e_1}{2}$ is an idempotent of $C_0(q)$ such that $\varphi(\tilde{e}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Thus

$$e = \tilde{e}\frac{e_3+1}{2} = \frac{1 + e_3 + e_0e_1 + e_0e_1e_3}{4}$$

is an idempotent of $C(q)$ such that

$$\varphi(e) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \varphi(C(q)e) = \begin{pmatrix} \mathbb{R} & 0 & 0 & 0 \\ \mathbb{R} & 0 & 0 & 0 \\ \mathbb{R} & 0 & 0 & 0 \\ \mathbb{R} & 0 & 0 & 0 \end{pmatrix}.$$

Therefore $C(q)e$ is an explicitly given space of spinors for q. As in Example 8, φ induces isomorphisms $\mathrm{Spin}(q)\tilde{\to}SL_2(\mathbb{C})$ and $so(q)\tilde{\to}sl_2(\mathbb{C})$.

Example 9. Let $(V, q) = \langle -1, 1, 1, 1, 1\rangle$ over $\mathbb{R}$. The algebra $C(q)$ is called the *Dirac algebra.* By Appendix A,

$$C(q) \simeq M_4(\mathbb{C}) \qquad \text{and} \qquad C_0(q) \simeq M_2(\mathbb{H}).$$

Let $\{e_0, \ldots, e_4\}$ be an orthogonal basis such that $q(e_0) = -1$ and $q(e_i) = 1, \ \ i = 1, \ldots, 4$. We decompose q as $q_1 \perp q_2$ with $q_1 = \langle -1, 1\rangle$ and $q_2 = \langle 1, 1, 1\rangle$, so $C(q) \simeq C(q_1)\hat{\otimes}C(q_2)$. We have, as before, an isomorphism

$$C(q_1)\tilde{\to}M_2(\mathbb{R}), \quad e_0 \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad e_1 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

and by Example 6

$$C(q_2)\tilde{\to}M_2(\mathbb{C}), \quad e_2 \mapsto \sigma_1, \quad e_3 \mapsto \sigma_2, \quad e_4 \mapsto \sigma_3,$$

σ_i the Pauli matrices. Using Lemma 3 of Chapter 4, we get

$$\psi : C(q) \tilde{\to} M_4(\mathbb{C}) = M_2(M_2(\mathbb{C}))$$

such that

$$\psi(e_0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \psi(e_1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \psi(e_2) = \begin{pmatrix} \sigma_1 & 0 \\ 0 & -\sigma_1 \end{pmatrix},$$

$$\psi(e_3) = \begin{pmatrix} \sigma_2 & 0 \\ 0 & -\sigma_2 \end{pmatrix} \quad \text{and} \quad \psi(e_4) = \begin{pmatrix} \sigma_3 & 0 \\ 0 & -\sigma_3 \end{pmatrix}.$$

Let $a \mapsto \overline{a}$ be the standard involution of $M_2(\mathbb{C})$. The involution

$$\sigma^* : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{d} & \overline{b} \\ \overline{c} & \overline{a} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

of $M_2(M_2(\mathbb{C}))$ is the identity on the images $\psi(e_i)$ of e_i, $\;i = 0, \ldots, 3$. Thus σ^* is equal to $\psi\sigma'\psi^{-1}$, where σ' is the canonical involution of $C(q)$ (usually we prefer to work with the standard involution σ of the Clifford algebra, i.e. the involution which is -1 on V. But we could not guess how σ looks like !).

We now twist ψ by an inner automorphism i_u in such a way that the diagram

$$\begin{array}{ccc} C(q) & \xrightarrow{i_u \circ \psi} & M_4(\mathbb{C}) = M_2(M_2(\mathbb{C})) \\ \cup & & \cup \\ C_0(q) & \xrightarrow{i_u \circ \psi} & M_2(\mathbb{H}) \end{array}$$

is commutative. Let

$$u = \begin{pmatrix} 1 & 0 \\ 0 & \sigma_1 \end{pmatrix} \in GL_4(\mathbb{C}),$$

where $\sigma_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ is the first Pauli matrix and let $\psi' = i_u \circ \psi$. We get

$$\psi'(e_0) = \begin{pmatrix} 0 & \sigma_1 \\ -\sigma_1 & 0 \end{pmatrix}, \quad \psi'(e_1) = \begin{pmatrix} 0 & \sigma_1 \\ \sigma_1 & 0 \end{pmatrix}, \quad \psi'(e_2) = \begin{pmatrix} \sigma_1 & 0 \\ 0 & -\sigma_1 \end{pmatrix}$$

$$\psi'(e_3) = \begin{pmatrix} \sigma_2 & 0 \\ 0 & \sigma_2 \end{pmatrix} \quad \text{and} \quad \psi'(e_4) = \begin{pmatrix} \sigma_3 & 0 \\ 0 & \sigma_3 \end{pmatrix}.$$

It follows from Example 6 that ψ' maps $C_0(q)$ to $M_2(\mathbb{H})$, as claimed. Further the involution $\widehat{\sigma} = \psi'\sigma'\psi'^{-1} = i_u\sigma^* i_u^{-1}$ is given by $\widehat{\sigma}(x) = u\sigma^*(u)\sigma^*(x)(u\sigma^*(u))^{-1}$ or

$$\widehat{\sigma}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -\sigma_1 \\ \sigma_1 & 0 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \begin{pmatrix} 0 & -\sigma_1 \\ \sigma_1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} \sigma_1\overline{d}\sigma_1 & -\sigma_1\overline{b}\sigma_1 \\ -\sigma_1\overline{c}\sigma_1 & \sigma_1\overline{a}\sigma_1 \end{pmatrix}.$$

We have $\sigma_1\overline{a}\sigma_1 = kak^{-1}$ for all $a \in M_2(\mathbb{C})$. Thus

$$\widehat{\sigma}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & \bar{k} \\ k & 0 \end{pmatrix} \begin{pmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{pmatrix} \begin{pmatrix} 0 & \bar{k} \\ k & 0 \end{pmatrix}^{-1}.$$

Observe that $\widehat{\sigma}$ is of symplectic type, as it should be. Since the standard and the canonical involutions coincide on $C_0(q)$, the computation of Spin in Chapter 12 shows that

$$\begin{aligned}\psi'(\mathrm{Spin}(q)) &= \left\{x \in M_2(\mathbb{H}) \;\middle|\; x\widehat{\sigma}(x) = 1\right\} \\ &= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{H}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & \bar{k} \\ k & 0 \end{pmatrix}\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 0 & \bar{k} \\ k & 0 \end{pmatrix}\right\}\end{aligned}$$

so ψ' is an isomorphism

$$\mathrm{Spin}(q)\tilde{\rightarrow}SU_2(\mathbb{H}, (\begin{smallmatrix} 0 & \bar{k} \\ k & 0 \end{smallmatrix})).$$

By formula (12.2) of Chapter 12, we have

$$\mathrm{Spin}(q) \simeq \mathrm{Spin}(-q)\tilde{\rightarrow}SU_2(\mathbb{H}, diag(1,\ -1).$$

In fact the hermitian matrices $(\begin{smallmatrix} 0 & \bar{k} \\ k & 0 \end{smallmatrix})$ and $(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix})$ are congruent since

$$\begin{pmatrix} 0 & \bar{k} \\ k & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{k}{2} & -\frac{k}{2} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & -\frac{k}{2} \\ 1 & \frac{k}{2} \end{pmatrix}.$$

We finally compute an idempotent of $C(q)$ which generates a simple $C(q)$–module. We have $\psi'(\frac{1+e_0e_1}{2}) = (\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}) \in M_2(\mathbb{C})$, thus

$$e = (\frac{1+e_0e_1}{2})(\frac{1+e_4}{2}) = \frac{1+e_4+e_0e_1+e_0e_1e_4}{4}$$

is such that

$$\psi'(e) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \varphi(C(q)e) = \begin{pmatrix} \mathbb{C} & 0 & 0 & 0 \\ \mathbb{C} & 0 & 0 & 0 \\ \mathbb{C} & 0 & 0 & 0 \\ \mathbb{C} & 0 & 0 & 0 \end{pmatrix}.$$

Bibliography

Arason, J.Kr.: Cohomologische Invarianten quadratischer Formen. J. Algebra 36, (1975), 448-491.

Baeza, R.: Quadratic forms over semilocal rings, Lecture Notes in Mathematics Vol. 655, Berlin, Heidelberg, New York, Springer 1978.

Bak, A.: K–theory of forms, Ann. Math. Studies 98, Princeton 1981.

Bass, H.: Unitary algebraic K–theory, Lectures Notes in Mathematics Vol. 343, Berlin, Heidelberg, New York, Springer (1973), 57-265.

Bass, H.: Clifford algebras and spinor norms over a commutative ring. Amer. J. Math. 96 (1974), 156-206.

Van der Blij, F.; Springer, T. A.: The arithmetics of octaves and the group G_2. Indag. Math. 21, (1959), 406-418.

Bourbaki, N.: Algèbre, Chapitre 9, Formes sesquilinéaires et formes quadratiques, Paris, Hermann 1959.

Chevalley, C.: The algebraic theory of Spinors, New York, Columbia Univ. Press 1954.

Cohn, P. M.: Algebra, Volume 2, London, New York, Sydney, Toronto, John Wiley and Sons 1977.

Demazure, M.; Gabriel, P.: Groupes algébriques, Paris, Masson 1970.

Dieudonné, J.: Les extensions quadratiques des corps non commutatifs et leurs applications, Acta Math. 87, (1952), 175-242.

Dieudonné, J.: Sur les groupes classiques, Paris, Hermann 1973.

Fröhlich, A.: Classgroups and hermitian modules, Progress in Mathematics 48, Boston, Basel, Stuttgart, Birkhäuser 1984.

Hermann, R.: Spinors, Clifford algebras and Cayley algebras, Interdisciplinary Mathematics Vol. VII 1974.

Herstein, I. N.: Noncommutative rings, Carus Mathematical Monographs, MAA, Washington 1968.

Jacobson, N.: Basic algebra II, San Francisco, W. H. Freeman and Company 1980.

Jacobson, N.: Some applications of Jordan norms to involutorial simple associative algebras, Adv. in Math. 48, (1983), 1-15.

Kneser, M.: Vorlesung über quadratische Formen, Göttingen, Mathematisches Institut 1973/74.

Knus, M.-A.; Parimala. R.; Sridharan, R.: A classification of rank 6 quadratic spaces via pfaffians, J. Reine Angew. Math., to appear.

Knus, M.-A.; Parimala. R.; Sridharan, R.: Azumaya algebras and pfaffians, in prep.

Knus, M.-A.; Parimala, R.; Srinivas, V.: Azumaya algebras with involutions, J. Algebra, to appear.

Lam, T. Y.: The algebraic theory of quadratic forms, Reading, Benjamin 1973.

Micali, A., Revoy, P.: Modules quadratiques, Montpellier, 1977 (or Bull. Soc. Math. France, Mémoire 63, 1979).

Saltman, D.: Azumaya algebras with involutions, J. Algebra 22 (1978), 526-539.

Schafer, R. D.: An introduction to nonassociative algebras, New York, London, Academic Press 1966.

Scharlau, W.: Quadratic and hermitian forms, Berlin, Heidelberg, New York, Springer 1985.

Serre, J.-P.: Cours d'arithmétique, Paris, Presses Universitaires de France 1970.

Swan, R.: K–theory of quadric hypersurfaces, Ann. of Math. 122 (1985), 113-153.

Tamagawa, T.: On quadratic forms and pfaffians, J. Fac. Sci. Tokyo, Sect. I, 24 (1977), 213-219.

Tits, J.: Formes quadratiques, groupes orthogonaux et algèbres de Clifford, Invent. Math. 5 (1968), 19-41.

Wagner. R.: Some Witt cancellation theorems, Amer. J. Math. 94 (1972), 206-220.

Wall, C. T. C.: On the axiomatic foundations of the theory of hermitian forms. Proc. Cambridge Phil. Soc. 67 (1970), 243-250.