Quadratic Forms over Fields

Prof. Dr. Gabriele Nebe
Lecture notes Summerschool Aachen 2023

May 30, 2023

K will usually denote a principal ideal domain, quite often a field. When it simplifies the proofs we assume that $2 \in K^\times$ is a unit. V is a finite dimensional free module over K. For more general Dedekind domains, "free" needs to be replaced by "projective", and some numbers, like the determinant, should be understood as ideals.

1 Symmetric bilinear forms

Definition 1.1. *A map $B : V \times V \to K$ is called* **symmetric bilinear form***, if*

$$B(x,y) = B(y,x) \textit{ and } B(ax+y,z) = aB(x,z) + B(y,z) \text{ for all } x,y,z \in V, a \in K.$$

$V^\perp := \{x \in V \mid B(x,y) = 0 \text{ for all } y \in V\}$ is the **radical** *of B, and B is* **non-degenerate** *if $V^\perp = \{0\}$.*

Let $e := (e_1, \ldots, e_n)$ be a basis of V. Then the **Gram matrix** of B with respect to e is defined as ${}_eB_e := (B(e_i,e_j)) \in K^{n\times n}$. If e' is a second basis of E, then $e'_i = \sum_{j=1}^n T_{ij}e_j$ with $T := (T_{ij}) \in \mathrm{GL}_n(K)$ and ${}_{e'}B_{e'} = T({}_eB_e)T^{tr}$. In particular $\det({}_{e'}B_{e'}) = \det(T)^2\det({}_eB_e)$.

Definition 1.2. $\det(V,B) := \det({}_eB_e)(K^\times)^2 \in K/(K^\times)^2$ *is called the* **determinant** *of B. We call (V,B)* **regular** *if $\det(V,B) \in K^\times$.*

In general regular bilinear forms are non-degenerate and for fields K these notions do coincide. Clearly B is regular if and only if ${}_eB_e \in \mathrm{GL}_n(K)$ if and only if $\det(V,B) \in K^\times/(K^\times)^2$.

Remark 1.3. *For non-degenerate bilinear forms over a field we have* $\dim(U)+\dim(U^\perp) = \dim(V)$ *and $V = U \oplus U^\perp$ if $B_{|U}$ is non-degenerate. In general, if (U,B) is a regular submodule of (V,B) then $V = U \perp U^\perp$.*

Proof. To see this note that regular implies primitive, i.e. a basis of U can be completed to a basis of V. Then the Gram matrix is $\begin{pmatrix} A & X \\ X^{tr} & C \end{pmatrix}$ where $A \in \mathrm{GL}_m(K)$ is a Gram matrix of $B_{|U}$. Gaussian column elimination hence can achieve $X = 0$ where the transposed row operations achieve $X^{tr} = 0$ and hence an orthogonal splitting $\begin{pmatrix} A & 0 \\ 0 & C - X^{tr}A^{-1}X \end{pmatrix}$. □

2 Quadratic forms

Definition 2.1. *(a) $Q : V \to K$ is called a* **quadratic form** *if*

(i) $Q(ax) = a^2 Q(x)$ for all $x \in V, a \in K$ *and*

(ii) $B_Q : V \times V \to K, B_Q(x, y) := Q(x+y) - Q(x) - Q(y)$ *is a symmetric bilinear form.*

We then call (V, Q) a **quadratic space***.*

(b) $\varphi : (V, Q) \to (V', Q')$ is called an **isometry** *if φ is injective, linear and $Q'(\varphi(x)) =$* $Q(x)$ for all $x \in V$.

Two quadratic forms are called **isometric***, if there is some bijective isometry.*

(c) (V, Q) is called regular, if (V, B_Q) is regular.

(d) $O(V, Q) := \{g \in \mathrm{GL}(V) \mid Q(g(x)) = Q(x)$ for all $x \in V\}$ is the **orthogonal group** *of Q.*

Remark 2.2. *If (V, B) is some bilinear form, then*

$$Q_B : V \to K, Q_B(x) := B(x, x)$$

is a quadratic form on V with $B_{Q_B} = 2B$.
If (V, Q) is a quadratic space, then (V, B_Q) is a bilinear space and $Q_{B_Q} = 2Q$.
If $2 \in K^\times$ then the notions of quadratic forms and symmetric bilinear forms are equivalent.

If $e = (e_1, \dots, e_n)$ is a basis of V then

$$Q(\sum_{i=1}^{n} a_i e_i) = \sum_{i=1}^{n} a_i^2 Q(e_i) + \sum_{i<j} a_i a_j B_Q(e_i, e_j) = (a_1, \dots, a_n)\,{}_eQ_e(a_1, \dots, a_n)^{tr}$$

where

$${}_eQ_e = \begin{pmatrix} Q(e_1) & & B_Q(e_i, e_j) \\ 0 & \ddots & \\ 0 & 0 & Q(e_n) \end{pmatrix} \in K^{n \times n}.$$

We have ${}_eQ_e + ({}_eQ_e)^{tr} = {}_eB_e$. If $B_Q(e_i, e_j) = 0$ for all $i \neq j$ (i.e. e is an **orthogonal basis**) then we write

$$Q = [Q(e_1), \dots, Q(e_n)].$$

Remark 2.3. *${}_eQ_e$ can also be seen as the Gram matrix of a (non-symmetric) bilinear form A. Then $Q(x) = A(x, x)$ for this bilinear form.*

Lemma 2.4. *Let n be odd and*

$$B := \begin{pmatrix} 2a_1 & b_{12} & \dots & b_{1n} \\ b_{12} & 2a_2 & \dots & b_{2n} \\ \vdots & \dots & \ddots & \vdots \\ b_{1n} & b_{2n} & \dots & 2a_n \end{pmatrix} \in K^{n \times n}$$

be a symmetric matrix. Then there is a polynomial $P_n \in \mathbb{Z}[x_i, y_{ij} \mid 1 \leq i < j \leq n]$ such that $\det(B) = 2P_n(a_i, b_{ij})$.

Definition 2.5. *Let (V, Q) be a quadratic space of odd dimension n. Then we put* $\det'(V, Q) := P_n(Q(e_i), B_Q(e_i, e_j))$ *for P_n as in Lemma 2.4 and call (V, Q)* **semi-regular***, if* $\det'(V, Q) \in K^\times$. $\det'(V, Q)$ *is called the* **half-determinant** *of (V, Q).*

2.1 Hyperbolic modules.

Definition 2.6. *Let V be some free module over K and $V^* = \mathrm{Hom}(V, K)$ be the dual space. Then*

$$\mathbb{H}(V) := (V \oplus V^*, Q_V), \textit{ with } Q_V(x + x^*) := x^*(x) \text{ for all } x \in V, x^* \in V^*$$

is called the **hyperbolic module** *attached to V.*

Clear. $B_{Q_V}(x + x^*, y + y^*) = x^*(y) + y^*(x)$.
If $e = (e_1, \ldots, e_n)$ is a basis of V and $(e_1^*, \ldots, e_n^*)$ is the dual basis of V^*, then the Gram matrix of $\mathbb{H}(V)$ with respect to the basis $(e_1, \ldots, e_n, e_1^*, \ldots, e_n^*)$ is $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$. In particular $\det(\mathbb{H}(V)) = (-1)^n$.

Corollary 2.7. *Let (V, Q) be a regular quadratic space and assume that there is $0 \neq v \in V$ such that $Q(v) = 0$. Then there is $u \in V$ with $Q(u) = 0$ and $B_Q(v, u) = 1$, so $\langle u, v\rangle \cong \mathbb{H}(K)$. In particular $(V, Q) \cong \mathbb{H}(K) \bigoplus (W, Q)$ for some regular quadratic space (W, Q).*

Proof. Without loss of generality we can assume that v is primitive in V, i.e. $a^{-1}v \in V$ with $0 \neq a \in K$ implies that $a \in K^\times$. As $B_Q : V \to V^*, x \mapsto B_Q(x, \cdot)$ is an isomorphism, there is $u \in V$ such that $B_Q(v, u) = 1$. Now $Q(u + av) = Q(u) + aB_Q(v, u)$ and hence we may replace u by $u + av$ so that $Q(u) = 0$. □

Definition 2.8. *A quadratic space (V, Q) is called* **anisotropic***, if $Q(v) \neq 0$ for all $0 \neq v \in V$.*

3 Quadratic forms over finite fields.

In this section we classify the quadratic forms over finite fields. So let $K = \mathbb{F}_{p^f}$ be a finite field of characteristic p and (V, Q) be some quadratic space over K. Then the multiplicative group $K^\times = K \setminus \{0\}$ is cyclic of order $p^f - 1$, in particular

Remark 3.1. *If $p \neq 2$ then $K = \{0\} \,\dot\cup\, (K^\times)^2 \,\dot\cup\, \epsilon(K^\times)^2$ and for $p = 2$ we have $K^\times = (K^\times)^2$ as the Frobenius automorphism is surjective. The quadratic forms $V_1 = [1]$ and $V_\epsilon = [\epsilon]$ (for $p \neq 2$) represent the isometry classes of one-dimensional semi-regular quadratic spaces.*

Remark 3.2. *Let (V, Q) be some regular quadratic K-module of dimension 2. If there is some $0 \neq x \in V$ such that $Q(x) = 0$ then $(V, Q) \cong \mathbb{H}(\langle x\rangle) \cong \mathbb{H}$ is isometric to a hyperbolic plane. If (V, Q) is anisotropic (i.e. $Q(x) = 0 \Rightarrow x = 0$), then $Q(V) = K$ (such quadratic K-modules are called* **universal***).*

Proof. The first statement is clear. Assume that (V, Q) is anisotropic. Since $K^2 = K$ for $p = 2$, we may assume that p is odd. Then V has an orthogonal basis (e_1, e_2) such that $Q(a_1e_1 + a_2e_2) = a_1^2t_1 + a_2^2t_2$ with $Q(e_1) = t_1 \neq 0$ and $Q(e_2) = t_2 \neq 0$. Choose $a \in K$ and put

$$M_1 := \{a_1^2t_1 \mid a_1 \in K\},\ M_2 := \{a - a_2^2t_2 \mid a_2 \in K\}.$$

Then $|M_1| = |M_2| = (|K|+1)/2$ and so $|M_1| + |M_2| = |K| + 1 > |K|$. Therefore $M_1 \cap M_2 \neq \emptyset$ i.e. there are $a_1, a_2 \in K$ such that $a_1^2 t_1 = a - a_2^2 t_2$ and $a = Q(a_1 e_1 + a_2 e_2)$. □

Example Let $V := \mathbb{F}_{p^{2f}} = K[\alpha] = K \cdot 1 \oplus K \cdot \alpha$ and $Q : V \to K$ be the norm form, i.e. $Q(x) = x x^{p^f}$. This is a quadratic form with $Q_Q(x,y) = x y^{p^f} + x^{p^f} y =$trace$(xy^{p^f})$. Moreover (V,Q) is anisotropic. We compute

$$Q(V \setminus \{0\}) = \{x^{1+p^f} \mid x \in V \setminus \{0\}\} = \langle a^{1+p^f} \rangle = K^\times \cong C_{p^f-1}$$

for any generator a of the multiplicative group of V. In particular this also shows that (V,Q) is universal. Notation: $(V,Q) = N(K)$.

Remark 3.3. *Let (V,Q) be some regular quadratic space of dimension 2. Then either $(V,Q) \cong \mathbb{H}$ or $(V,Q) \cong N(K)$ so there are exactly two isometry classes of 2-dimensional regular quadratic spaces over every finite field.*

Proof. We only need to show that any anisotropic quadratic space (V,Q) of dimension 2 is isometric to $N(K)$. Choose any basis (e_1, e_2) of V such that $Q(e_1) = 1$. Then $(V,Q) = \begin{bmatrix} 1 & c \\ & a \end{bmatrix}$ and $Q(a_1 e_1 + a_2 e_2) = a_1^2 + c a_1 a_2 + a a_2^2$. The polynomial $X^2 + cX + a \in K[X]$ is irreducible (has no zero, since Q is anisotropic) it hence defines the unique extension of degree 2 of K. Conclude that $(V,Q) \cong N(K)$ as an exercise. □

Theorem 3.4. *Let (V,Q) be a regular quadratic space of dimension $2m$. Then*

$$(V,Q) \cong \begin{cases} Q_{2m}^{+}(K) := \obot_{i=1}^{m} \mathbb{H} & = \obot_{i=1}^{m} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \quad \text{or} \\ Q_{2m}^{-}(K) := N(K) \obot \obot_{i=1}^{m-1} \mathbb{H} & = \begin{bmatrix} 1 & a \\ & b \end{bmatrix} \obot \obot_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{cases}$$

where $X^2 + aX + b \in K[x]$ irreducible. These two quadratic modules are not isometric (as we will see later).

Corollary 3.5. *Let (V,Q) be a semi-regular quadratic space of dimension $2m+1$. Then*

$$(V,Q) \cong \begin{cases} [1] \obot \obot_{i=1}^{m} \mathbb{H} & = [1] \obot \obot_{i=1}^{m} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \quad \text{or} \\ [\epsilon] \obot \obot_{i=1}^{m} \mathbb{H} & = [\epsilon] \obot \obot_{i=1}^{m} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{cases}$$

where the latter case only occurs if char$(K) \neq 2$ *(and then $\epsilon \in K^\times \setminus (K^\times)^2$). For $p \neq 2$ these two quadratic modules are not isometric because their determinants $\in K^\times/(K^\times)^2$ are different.*

Theorem 3.6. *Two regular quadratic forms over a finite field K are isometric, if and only if they have the same dimension and determinant. If* char$(K) = 2$ *then there are no regular quadratic forms of odd dimension and the determinant has to be replaced by the discriminant algebra (see Definition 5.15).*

3.1 An exercise: doubly-even self-dual codes.

Let $K = \mathbb{F}_2$, $(V,B) := (\mathbb{F}_2^n, B(c,d) := \sum_{i=1}^n c_i d_i)$ the n-dimensional $\mathbb{F}_2$-vector space with standard inner product. We also define the **weight**, $\mathrm{wt} : \mathbb{F}_2^n \to \mathbb{Z}, \mathrm{wt}(c) := |\{i \mid c_i \neq 0\}|$. Let $\mathbf{1} := (1,\ldots,1)$ be the **all ones vector**, the unique element of V of weight n.

A **code** is a subspace $C \leq \mathbb{F}_2^n$. C is called **self-dual**, if $C = C^\perp$. C is called **self-orthogonal**, if $C \subseteq C^\perp$. C is called **doubly-even**, if $\mathrm{wt}(C) \subseteq 4\mathbb{Z}$.

- (V,B) is non-degenerate.
- If $C \subseteq C^\perp$ then $\mathrm{wt}(c)$ is even for all $c \in C$ and hence $C \subseteq \mathbf{1}^\perp = \{c \in C \mid \mathrm{wt}(c) \text{ even }\}$.
- If C is doubly-even, then C is self-orthogonal.
- If (V,B) contains a doubly-even self-dual code, then $n \in 4\mathbb{Z}$.
- Define a quadratic form $Q : E := \mathbf{1}^\perp \to \mathbb{F}_2, Q(c) = \frac{\mathrm{wt}(c)}{2} + 2\mathbb{Z}$. Then B_Q is the restriction of B to $\mathbf{1}^\perp =: E$.
- If n is even then $E^\perp = \langle \mathbf{1} \rangle$ and (E,Q) is semiregular, if $n \notin 4\mathbb{Z}$.
- If n is odd then (E,Q) is regular and $(V,B) = E \bigoplus \langle \mathbf{1} \rangle$.
- Write $n = 8m + a$ with $m \in \mathbb{N}_0$, $a \in \{1,2,3,4,5,6,7,8\}$. Then $(E,Q) \cong \mathbb{H}(\mathbb{F}_2)^{4m} \bigoplus A$ with
$$A \cong \begin{cases} \{0\} & a = 1 \\ [1] & a = 2 \\ N(\mathbb{F}_2) & a = 3 \\ N(\mathbb{F}_2) \bigoplus [0] & a = 4 \\ \mathbb{H}(\mathbb{F}_2) \bigoplus N(\mathbb{F}_2) & a = 5 \\ \mathbb{H}(\mathbb{F}_2)^2 \bigoplus [1] & a = 6 \\ \mathbb{H}(\mathbb{F}_2)^2 \bigoplus N(\mathbb{F}_2) & a = 7 \\ \mathbb{H}(\mathbb{F}_2)^3 \bigoplus [0] & a = 8 \end{cases}$$
- Doubly-even self-dual codes exist if and only if $n \in 8\mathbb{Z}$.

To see the second last point, consider the cases $n \leq 9$ first and find explicit isometries. To get the periodicity distinguish the cases n even and n odd. Denote (E,Q) by E_n to indicate the length n of the codes. If $n = \ell + 8$ is odd, then E_ℓ is regular, $E_\ell \to E_n, v \mapsto (v, 0^8)$ is an isometry and $E_n = E_\ell \perp \mathbb{H}(\mathbb{F}_2)^4$. If $n = \ell + 8$ is even, then E_ℓ has a radical, embed

$$E_\ell \to E_n, v \mapsto \begin{cases} (v, 0^8) & \text{if } v_\ell = 0 \\ v \mapsto (v, 1^8) & \text{if } v_\ell = 1. \end{cases}$$

Show that with this embedding $E_n = E_\ell \perp E_9$ and that $E_9 \cong \mathbb{H}(\mathbb{F}_2)^4$.

4 Orthogonal groups and Witt's theorem

Example 4.1. *(Reflections) Let $v \in V$ be such that $Q(v) \in K^\times$. Then the* **reflection** *along v is*

$$s_v : x \mapsto x - \frac{B_Q(x,v)}{Q(v)} v \in O(V,Q).$$

Theorem 4.2. *(Witt's extension theorem)*
Let K be a field and let (V,Q) be a quadratic space and $U \leq V$. Let $\varphi : U \to V$ be an isometric embedding. Assume that either U or V is regular. Then there is some $g \in O(V,Q)$ such that $g_{|U} = \varphi$.

Corollary 4.3. *(Witt's cancellation theorem)*
Let K be a field, F, G_1, G_2 quadratic spaces such that F is regular. Then $F \obot G_1 \cong F \obot G_2 \Leftrightarrow G_1 \cong G_2$.

Proof. Let $\psi : F \obot G_1 \to F \obot G_2 =: E$ be a bijective isometry and put $F_1 := \psi(F)$. Then $F \leq E$ and $\varphi : F \to F_1 \leq E, f \mapsto \psi(f)$ is an isometry. By Theorem 4.2 there is some orthogonal transformation $g \in O(E)$ such that $g_{|F} = \varphi$.
Claim: $(g^{-1} \circ \psi)_{|G_1} : G_1 \to G_2$ is a bijective isometry.
To prove the claim it is enough to see that $(g^{-1}(\psi(G_1)) = G_2$. Since F and hence $\varphi(F)$ are regular subspaces of E, we have that

$$G_2 = F^\perp \text{ and } \psi(G_1) = \psi(F)^\perp = F_1^\perp = \varphi(F)^\perp.$$

So $g(G_2) = g(F^\perp) = g(F)^\perp = \varphi(F)^\perp = \psi(G_1)$. □

Corollary 4.4. *The two quadratic modules $\obot^{m-1} \mathbb{H} \obot N(K)$ and $\obot^m \mathbb{H}$ of Theorem 3.4 are not isometric. Otherwise $N(K) \cong \mathbb{H}$ but $N(K)$ is anisotropic.*

Definition 4.5. *A subspace $U \leq V$ is called* **totally isotropic** *if $Q(U) = \{0\}$. Theorem 4.2 implies that the maximal dimension of a totally isotropic subspace of a regular quadratic space (V,Q) is well defined. This dimension is called the* **Witt index** *of (V,Q).*

The Witt index of the hyperbolic module $\mathbb{H}(V) = (V \oplus V^*, Q(x + x^*) = x^*(x))$ equals the dimension of V.

In view of the Corollary 2.7 and Witt's cancellation theorem to classify regular quadratic spaces over fields it is enough to classify anisotropic spaces.

4.1 An exercise: The orthogonal groups over finite fields

Let $K = \mathbb{F}_\ell$, $\ell = p^f$, (V,Q) regular or semi-regular quadratic space over K. By Section 3 we have two possibilities for even dimension $\dim(V) = 2m$:

$$\begin{aligned} Q_{2m}^+ &\cong \obot_{i=1}^m \mathbb{H} & &= \obot_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ or} \\ Q_{2m}^- &\cong N(K) \obot \obot_{i=1}^{m-1} \mathbb{H} & &= \begin{bmatrix} 1 & a \\ & b \end{bmatrix} \obot \obot_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{aligned}$$

If $\dim(V) = 2m+1$ then there are 2 modules for $p \neq 2$ and one for $p = 2$:

$$\begin{array}{rlll} Q^+_{2m+1} := & [1] \oplus \bigoplus_{i=1}^m \mathbb{H} & = [1] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{or} \\ Q^-_{2m+1} := & [\epsilon] \oplus \bigoplus_{i=1}^m \mathbb{H} & = [\epsilon] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \end{array}$$

where $\epsilon \in K^* \setminus (K^*)^2$.

Since $Q^+_{2m+1} \cong \epsilon Q^-_{2m+1}$ these two quadratic modules have isomorphic orthogonal groups.

Theorem 4.6. *Let $O_{2m+1}(\mathbb{F}_\ell) := O(Q_{2m+1})$, $O^+_{2m}(\mathbb{F}_\ell) := O(Q^+_{2m})$ and $O^-_{2m}(\mathbb{F}_\ell) := O(Q^-_{2m})$. Then*

$$\begin{array}{lll} (a) & |O^+_{2m}(\mathbb{F}_\ell)| = & 2\ell^{m(m-1)}(\ell^m - 1)\prod_{i=1}^{m-1}(\ell^{2i}-1) \\ (b) & |O^-_{2m}(\mathbb{F}_\ell)| = & 2\ell^{m(m-1)}(\ell^m + 1)\prod_{i=1}^{m-1}(\ell^{2i}-1) \\ (c) & |O_{2m+1}(\mathbb{F}_\ell)| = & z\ell^{m^2}\prod_{i=1}^{m}(\ell^{2i}-1) \end{array}$$

where $z = 1$ if ℓ is even and $z = 2$ if ℓ is odd.

4.2 An exercise: Witt cancellation is not true over rings

Remark 4.7. *Witt's cancellation theorem does not hold for regular quadratic $\mathbb{Z}$-modules.*

Proof. The lattice $\tilde{\mathbb{D}}_{16}$ is a positive definite even unimodular orthogonally idecomposable lattice of dimension 16. Also $\mathbb{E}_8 \oplus \mathbb{E}_8$ is a positive definite even unimodular 16-dimensional lattice, so $(E,Q) := (\tilde{\mathbb{D}}_{16}, Q(x) := \frac{1}{2}B(x,x))$ and $(F,Q) := (\mathbb{E}_8, Q(x) := \frac{1}{2}B(x,x))^2$ are regular (positive definite) quadratic $\mathbb{Z}$-modules of rank 16. One of them is orthogonally decomposable, the other one isn't so these modules are not isometric, but

$$(E,Q) \oplus \mathbb{H}(\mathbb{Z}) \cong (F,Q) \oplus \mathbb{H}(\mathbb{Z}).$$

To construct this isometry write $\tilde{\mathbb{D}}_{16} = \langle \mathbb{D}_{16}, v = \frac{1}{2}\sum_{i=1}^{16} e_i \rangle$ and $\mathbb{H}(\mathbb{Z}) = \langle e, f \rangle$ with $Q(ae+bf) = ab$. The obvious sublattice $\mathbb{D}_8$ together with $v + e - f$ generates a sublattice L isometric to $\mathbb{E}_8$ in $\tilde{\mathbb{D}}_{16} \oplus \mathbb{H}(\mathbb{Z})$. Find a hyperbolic plane X in $L^\perp$ (generated by a vector of length 0 and some other vector having inner product 1 with this vector). Then identify $(X \oplus L)^\perp$ with the second copy of $\mathbb{E}_8$. □

5 The Clifford algebra of a quadratic space

Given a vector space V of dimension n over a field K one may associate to V the

- **Tensor algebra** $T(V) := \bigoplus_{i=0}^\infty \otimes^i V$
- **Symmetric algebra** $K[x_1, \ldots, x_n]$
- **Grassmann algebra** $\Lambda(V) := \bigoplus_{i=0}^n \Lambda^i(V)$

All these algebras can be defined using their universal property. Only the Grassmann algebra has finite dimension, 2^n; this is the Clifford algebra of the quadratic form $Q = 0$ on V.

Definition 5.1. *Let (V,Q) be a quadratic space of dimension n. Then the* **Clifford algebra** *of (V,Q) is*

$$\mathcal{C}(V,Q) := T(V)/I(V,Q)$$

where $I(V,Q)$ is the ideal in $T(V)$

$$I(V,Q) = \langle v^2 - Q(v)1 \mid v \in V \rangle.$$

Note that in $\mathcal{C}(V,Q)$ we have

$$vw + wv = (v+w)^2 - v^2 - w^2 = Q(v+w) - Q(v) - Q(w) = B_Q(v,w).$$

In particular $vw = -wv$ whenever $B_Q(v,w) = 0$, so $\mathcal{C}(V,0) = \Lambda(V)$ is the Grassmann algebra.

Note also that the definition is a bit sloppy, as we should have shown that the map from V to $\mathcal{C}(V,Q)$ is indeed injective and allows one to identify V with a subspace of $\mathcal{C}(V,Q)$.

Remark 5.2. *Inherited from the tensor algebra, the Clifford algebra has the following universal property:*
Given a K-algebra A and a K-linear map $f : V \to A$ satisfying $f(v)^2 = Q(v)1$ for all $v \in V$ then there is a unique K-algebra homomorphism $\mathcal{C}(V,Q) \to A$ mapping v to $f(v)$.

Theorem 5.3. *For any quadratic space (V,Q), the Clifford algebra is unique up to K-algebra isomorphism.*
Given a basis $e = (e_1, \ldots, e_n)$ of V, then the Clifford algebra has K-basis

$$\left(\prod_{i=1}^{r} e_{j_i} \mid r \in \mathbb{N}_0, j_1 < \ldots < j_r \right).$$

In particular $\dim(\mathcal{C}(V,Q)) = 2^n$.

The proof of the first part is the usual manipulation of universal properties. For the proof of the second part, I refer to the lecture notes of my course on quadratic forms.

As the relations $v^2 = Q(v)$ are between tensors of degree 2 and 0, and hence even, the Clifford algebra has a natural $\mathbb{Z}/2\mathbb{Z}$-grading:

Definition 5.4. *The* **even Clifford algebra** *is*

$$\mathcal{C}_0(V,Q) := \langle \prod_{i=1}^{2r} e_{j_i} \mid r \in \mathbb{N}_0, j_1 < \ldots < j_{2r} \rangle$$

and a 2^{n-1}-dimensional subalgebra of the Clifford algebra. We have $\mathcal{C}(V,Q) = \mathcal{C}_0(V,Q) \oplus \mathcal{C}_1(V,Q)$ with $\mathcal{C}_1(V,Q) = e_1\mathcal{C}_0(V,Q)$ is spanned by the products of odd length.

Lemma 5.5. *Scaling of the quadratic form does not change the isomorphism type of the even Clifford algebra: Given $a \in K^\times$ the linear map*

$$\mathcal{C}_0(V,Q) \to \mathcal{C}_0(V,aQ), \prod_{i=1}^{2r} e_{j_i} \mapsto a^{-r} \prod_{i=1}^{2r} e_{j_i}$$

is a K-algebra isomorphism.

From the universal property we get that orthogonal mappings of (V,Q) extend to K-algebra automorphisms of $\mathcal{C}(V,Q)$ preserving the grading:

Theorem 5.6. *For any $g \in O(V,Q)$ there is a unique K-algebra automorphism $c(g) \in \operatorname{Aut}(\mathcal{C}(V,Q))$ with $c(g)(v) = g(v)$ for all $v \in V$.*

Example 5.7. *Let $v \in V$ be such that $Q(v) \in K^\times$. Then the* **reflection** *along v is*

$$s_v : x \mapsto x - \frac{B_Q(x,v)}{Q(v)} v \in O(V,Q).$$

In the Clifford algebra we get for all $x \in V$:

$$vxv^{-1} = \frac{1}{Q(v)} vxv = \frac{1}{Q(v)}(-vvx + B_Q(v,x)v) = -s_v(x).$$

So $c(s_v) = c(-id_V)\kappa_v$ where $\kappa_v \in \operatorname{Aut}(\mathcal{C})$ denotes the conjugation with v.

Remark 5.8. *Let (V,Q) be a regular quadratic space. Then there is a unique group homomorphism*

$$\mathrm{SN}_Q : O(V,Q) \to K^\times/(K^\times)^2, s_v \mapsto Q(v)(K^\times)^2$$

called the **Spinor norm**.
The restriction of SN_Q to the special orthogonal group (which is generated by all products of an even number of reflections) is independent of scaling of the quadratic form.
For $\mathrm{char}(K) \neq 2$ choose an orthogonal basis $(e_1,\dots,e_n)$ so that $(V,Q) = [a_1,\dots,a_n]$. Then $-\mathrm{id}_V = s_{e_1}\cdots s_{e_n}$ has Spinor norm

$$\mathrm{SN}_Q(-\mathrm{id}_V) = Q(e_1)\cdots Q(e_n) = a_1 \cdots a_n = \det{}'(Q)$$

the half-determinant of (V,Q).

Also $\mathcal{C}(V,Q)$ is an algebra with a (canonical) involution:

Theorem 5.9. *There is a unique K-algebra anti automorphism $\iota : \mathcal{C}(V,Q) \to \mathcal{C}(V,Q)$ such that $\iota(v) = v$ for all $v \in V$. We compute $\iota(e_{i_1}\cdots e_{i_r}) = e_{i_r}\cdots e_{i_1}$ and $\iota^2 = \mathrm{id}$.*

Example 5.10.

- *$V = Ke$, $q(e) = a \in K$. Then $\mathcal{C}(V,Q) \cong K[X]/(X^2 - a)$.*
- *If $(V,Q) = [a,b]$ is of rank 2 with orthogonal basis (e_1,e_2), $Q(e_1) = a$, $Q(e_2) = b$, then*

  $$\mathcal{C}(V,Q) = \langle 1, e_1, e_2, e_1e_2 \rangle$$

  with $e_1e_2 = -e_2e_1$. The mapping $\mathcal{C}(V,Q) \to K^{4\times 4}$, defined by

  $$e_1 \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ a & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -a & 0 \end{pmatrix}, e_2 \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ b & 0 & 0 & 0 \\ 0 & b & 0 & 0 \end{pmatrix}$$

  is a K-algebra monomorphism, whose image is a free K-module of rank 4.

Definition 5.11. $\mathcal{C}([a,b]) =: \left(\frac{a,b}{K}\right)$ *is called the* **quaternion algebra** *with parameters a,b over K.*

Example 5.12. *Let $\mathbb{H} := \langle e, f \rangle$ with $Q(ae + bf) = ab$ be the hyperbolic plane. Then*

$$\mathcal{C}(\mathbb{H}) = \langle I_2, e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = ef \rangle = K^{2\times 2}$$

and $\mathcal{C}_0(\mathbb{H}) \cong K \oplus K$.

Theorem 5.13. *Assume that* $\mathrm{char}(K) \neq 2$ *and write the regular quadratic space $(V, Q) := [a_1, \ldots, a_n] = \bigoplus_{i=1}^n Ke_i$. Put $z := e_1 \ldots e_n \in \mathcal{C}(E, q) =: \mathcal{C}$. Then*

(0) $e_i z = (-1)^{n-1} z e_i$ for all $i = 1, \ldots, n$.

(a) $z^2 = (-1)^{\binom{n}{2}} a_1 \cdots a_n =: d$.

(b) The centraliser of $\mathcal{C}_0$ in $\mathcal{C}$ is $\mathcal{C}^{\mathcal{C}_0} = \langle 1, z \rangle \cong K[X]/(X^2 - d)$.

(c) If n is even, then $Z(\mathcal{C}) = K$ and $Z(\mathcal{C}_0) = \langle 1, z \rangle$.

(d) If n is odd, then $Z(\mathcal{C}) = \langle 1, z \rangle$ and $Z(\mathcal{C}_0) = K$.

Proof. (a) We compute $z^2 = e_1 \cdots e_n e_1 \cdots e_n = (-1)^{n-1} e_2 \cdots e_n e_1^2 e_2 \cdots e_n = a_1 (-1)^{n-1} (e_2 \cdots e_n)^2 = a_1 \cdots a_n (-1)^{\sum_{j=1}^{n-1} j}$.
(b) $\mathcal{C}$ has a K-basis $(1, e_1, \ldots, e_n, e_1 e_2, \ldots, e_1 e_2 \cdots e_n) = (e_{i_1} \cdots e_{i_r} \mid 0 \leq r \leq n, 1 \leq i_1 < \ldots < i_r \leq n)$. Define $e_J := e_{i_1} \cdots e_{i_r}$ if $J = \{i_1, \ldots, i_r\}$ with $1 \leq i_1 < \ldots < i_r \leq n$. Then $\mathcal{C}_0$ is generated as a K-algebra by $e_i e_j$ $(1 \leq i < j \leq n)$. For $x := \sum_{J \subseteq \{1,\ldots,n\}} x_J e_J$ we have

$$x e_i e_j = \sum_J x_J e_J e_i e_j = \sum_J (-1)^{|J \cap \{i,j\}|} x_J e_i e_j e_J = e_i e_j x$$

if and only if $x_J = 0$ if $|J \cap \{i, j\}| = 1$. So $x e_i e_j = e_i e_j x$ for all i, j if and only if $x \in \langle e_\emptyset, e_{\{1,\ldots,n\}} \rangle = \langle 1, z \rangle$.
The other statements follow by using the fact that $e_i z = (-1)^{n-1} z e_i$ for all i. □

Theorem 5.14. *Assume that (V, Q) is a regular or semi-regular quadratic space over a field K of arbitrary characteristic.*
(a) If $\dim(V)$ *is even, then $\mathfrak{c}(V, Q) := \mathcal{C}(V, Q)$ is a tensor product of quaternion algebras, $Z(\mathcal{C}(V, Q)) = K$ and $Z(\mathcal{C}_0(V, Q)) = \mathcal{C}^{\mathcal{C}_0} \cong Z$. $\mathcal{C}_0 \cong B \otimes Z$, where B is a tensor product of quaternion algebras.*
(b) If $\dim(V)$ *is odd, then $\mathfrak{c}(V, Q) := \mathcal{C}_0(V, Q)$ is a tensor product of quaternion algebras, $Z(\mathcal{C}_0(V, Q)) = K$ and $\mathcal{C}(V, Q)) = Z \otimes \mathcal{C}_0(V, Q)$ where $Z = \mathcal{C}^{\mathcal{C}_0} = Z(\mathcal{C}(V, Q))$.*

Definition 5.15. *The algebra $Z := \mathcal{C}(V, Q)^{\mathcal{C}_0(V,Q)}$ is called the* **discriminant algebra** *of the regular of semi-regular quadratic space (V, Q). If* $\mathrm{char}(K) \neq 2$ *then $Z \cong K[X]/(X^2 - d)$ where*

$$d := \begin{cases} (-1)^{\binom{n}{2}} \det{}'(B_Q) & \dim(V) \ \textit{odd} \\ (-1)^{\binom{n}{2}} \det(B_Q) & \dim(V) \ \textit{even} \end{cases}$$

so that $d(K^\times)^2 =:$ $\mathrm{disc}(V, Q)$ is the **discriminant** *of the quadratic space (V, Q). Note that $B_Q = \mathrm{diag}(2a_1, \ldots, 2a_n)$, so if n is odd we need to take the half-determinant of B_Q. The class of the central simple Clifford algebra*

$$\mathfrak{c}(V, Q) := \begin{cases} \mathcal{C}_0(V, Q) & n \ \textit{odd} \\ \mathcal{C}(V, Q) & n \ \textit{even} \end{cases}$$

in the Brauer group of K is called the **Clifford invariant** *of (V, Q).*

Remark 5.16. *Let (V, Q) be a regular quadratic space. Then we have the following invariants of the isometry class of (V, Q):*

(a) The **dimension** $\dim(V) \in \mathbb{N}_0$.

(b) The **discriminant algebra** $Z(V, Q)$*, which is an etale quadratic K-algebra with involution.*

(c) The **Clifford invariant** $c(V, Q) = [\mathfrak{c}(V, Q)]$*, which is in* $\mathrm{Br}_2(K)$.

If $K = \mathbb{R}$ then we also have the **signature** *of (V, Q) where $sign([1^a, (-1)^b]) = (a, b) \in \mathbb{N}_0 \times \mathbb{N}_0$.*

6 Quadratic forms over complete local fields

Now let R be a complete discrete valuation ring with finite residue field $k := R/\pi R$ and quotient field $K := \mathrm{Quot}(R)$. As an example you should think of the ring of p-adic integers

$$R = \mathbb{Z}_p, k = \mathbb{F}_p, K = \mathbb{Q}_p.$$

6.1 Lifting isometries

Theorem 6.1. *Let (V, Q) and (V', Q') be two regular quadratic spaces over R. Then (V, Q) and (V', Q') are isometric over R if and only if $(V/\pi V, \overline{Q})$ and $(V'/\pi V', \overline{Q'})$ are isometric over $k = R/\pi R$.*

Proof. Let $\varphi : V \to V'$ be an isomorphism of R-modules such that $Q'(\varphi(v)) \equiv Q(v) \pmod{\pi}$ for all $v \in V$. We want to replace φ by $\varphi + \pi\psi$ such that

$$Q'(\varphi(v) + \pi\psi(v)) = Q'(\varphi(v)) + \pi^2 Q'(\psi(v)) + \pi B_{Q'}(\varphi(v), \psi(v)) \equiv Q(v) \pmod{\pi^2}$$

i.e.

$$B_{Q'}(\varphi(v), \psi(v)) \equiv \frac{1}{\pi}(Q(v) - Q'(\varphi(v))) =: \tilde{Q}(v) \text{ for all } v \in V.$$

By Remark 2.3 there is some (not necessary symmetric) bilinear form $A : V \times V \to R$ such that $A(v, v) = \tilde{Q}(v)$ for all $v \in V$. Let $(x_1, \dots, x_n)$ be some R-basis of V. As $B_{Q'}$ is regular there are $v_1, \dots, v_n \in V'$ such that

$$B_{Q'}(\varphi(x_i), v_j) \equiv A(x_i, x_j) \pmod{\pi} \text{ for all } 1 \le i, j \le n.$$

Define the R-linear map $\psi : V \to V'$ by $\psi(x_i) := v_i$. Then for $x = \sum_{i=1}^n a_i x_i \in V$

$$B_{Q'}(\varphi(x), \psi(x)) = \sum_{i,j} a_i a_j B_{Q'}(\varphi(x_i), v_j) \equiv_\pi \sum_{i,j} a_i a_j A(x_i, x_j) = A(x, x) = \tilde{Q}(x).$$

□

Corollary 6.2. *(a) If (V, Q) is a regular quadratic R-module of rank ≥ 2 and $t \in R^*$, then there is some $x \in V$ with $Q(x) = t$.*
(b) If (V, Q) is regular or semi-regular of rank ≥ 3, then

$$(V, Q) = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \textstyle\bigoplus (V_1, Q_1)$$

for some regular resp. semi-regular (V_1, Q_1).
(c) There are exactly two regular 2-dimensional quadratic R-modules: $\mathbb{H}(R)$ and $N(R)$, with $\overline{N(R)} = N(k)$. $N(R)$ is the norm form on the unique quadratic unramified extension of R.
(d) If $\operatorname{char}(k)$ is odd then either $(V, Q) \cong \bigoplus_{i=1}^{n} [1]$ or $(V, Q) \cong \bigoplus_{i=1}^{n-1} [1] \bigoplus [\epsilon]$ for fixed $\epsilon \in R^* \setminus (R^*)^2$.
(e) If $\operatorname{char}(k)$ is even then the regular and semi-regular quadratic spaces are

$$(V, Q) \cong \begin{cases} [u] \bigoplus_{i=1}^{m} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{if } n = 2m+1 (\text{ some } u \in R^*) \\ \bigoplus_{i=1}^{m} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{if } n = 2m \\ \bigoplus_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \bigoplus N(R) & \text{if } n = 2m \end{cases}$$

6.2 Anisotropic quadratic spaces over complete fields

Theorem 6.3. *Let (V, Q) be an anisotropic quadratic space over K. For $i \in \mathbb{Z}$ put*

$$E_i := \{x \in V \mid Q(x) \in \pi^i R\}.$$

*Then E_i is an R-submodule of V of full rank (an R-**lattice**).*

Proof. The crucial point is that E_i is a subgroup of V. So let $x, y \in E_i$. Then $Q(x + y) = Q(x) + Q(y) + B_Q(x, y)$ and $x + y \in E_i$ if $B_Q(x, y) \in \pi^i R$. Otherwise $B_Q(x, y)R = \pi^j R$ for $j < i$. Replacing Q by $\pi^{-j}Q$ we obtain a subspace $\langle x, y \rangle$ of E_i which reduces modulo π to a hyperbolic plane. This is a contradiction to (V, Q) being anisotropic. □

Lemma 6.4. *Let L be the unramified quadratic extension of K. Then the norm form $N : L \to K$ is an anisotropic quadratic form $N(K)$ with $E_0(N(K)) \cong N(R)$. We have $Q(N(R)) = \cup_{i=0}^{\infty} \pi^{2i} R^* \cup \{0\}$*

Corollary 6.5. *$(U, Q_0) := N(K) \bigoplus {}^{\pi}N(K)$ is a universal anisotropic quadratic space of dimension 4 over K.*

Theorem 6.6. *Let (V, Q) be an anisotropic quadratic space over K. Then $\dim(V) \leq 4$ and if $\dim(V) = 4$, then $(V, Q) \cong (U, Q_0)$.*

Proof. Let $E_i := \{x \in V \mid Q(x) \in \pi^i R\}$ be the maximal lattice from Theorem 6.3. Then $E_0 \supseteq E_1 \supseteq E_2 = \pi E_0$ and

$$\dim(V) = \dim_{\overline{R}}(E_0/\pi E_0) = \dim_{\overline{R}}(E_0/E_1) + \dim_{\overline{R}}(E_1/\pi E_0).$$

The quadratic space $(E_0/E_1, \overline{Q})$ is an anisotropic $\overline{R}$ space, so $\dim(E_0/E_1) \leq 2$, and if equality holds, then $(E_0/E_1, \overline{Q}) \cong N(k)$. Similarly $(E_1/\pi E_0, \overline{\pi^{-1}Q})$ is anisotropic. So $\dim(V) \leq 4$.
Assume that $\dim(V) = 4$ and let (e_1, e_2, e_3, e_4) be an R-basis of E_0 so that $e_3, e_4 \in E_1$. Then $\langle e_1, e_2 \rangle$ is a regular submodule of (E_0, Q) whose reduction modulo π is $N(k)$, so $\underline{\langle e_1, e_2 \rangle} \cong N(R)$ from above and $(E_0, Q) \cong N(R) \textcircled{\perp} (G', \pi Q')$ such that $(E_1/\pi E_0, \overline{\pi^{-1}Q}) \cong N(k)$. This implies that $(G', Q') \cong N(R)$ and $(V, Q) \cong (U, Q_0)$. □

Then $\mathrm{Br}_2(K) = \{[K], [\mathcal{Q}(K)]\}$ where $\mathcal{Q}(K)$ is the unique central division algebra over K of dimension 4. We also assume that the characteristic of K is not 2, so that we can replace the discriminant algebra $Z(V, Q)$ of (V, Q) by the discriminant $\mathrm{disc}(V, Q) \in K^\times/(K^\times)^2$.

The following theorem gives the classification of anisotropic quadratic spaces over K.

Theorem 6.7. *(i) For each $d(K^\times)^2 \in K^\times/(K^\times)^2$ there is a unique quadratic space of dimension 1, $(V, Q) = [d]$.*

(ii) For each non-trivial $d(K^\times)^2 \in K^\times/(K^\times)^2$ there are two anisotropic quadratic spaces of dimension 2 and discriminant d that are distinguished by their Clifford invariant $\in \mathrm{Br}_2(K) = \{[K], [\mathcal{Q}(K)]\}$. Note that the Clifford invariant of (V, Q) is $[K]$ if and only if there is $v \in V$ with $Q(V) = 1$.

(iii) For each $d(K^\times)^2 \in K^\times/(K^\times)^2$ there is a unique anisotropic quadratic space of dimension 3 with $\mathrm{disc}(V, Q) = d(K^\times)^2$. We have $c(V, Q) = \mathcal{Q}$.

(iv) There is a unique anisotropic quadratic space of dimension 4. This space is universal, i.e. $Q(V) = K$ has discriminant 1 and non-trivial Clifford invariant.

(v) There are no anisotropic quadratic spaces of dimension ≥ 5 over K.

Corollary 6.8. *Two regular quadratic spaces over K are isometric, if and only if they have the same dimension, discriminant and Clifford invariant.*

7 Quadratic forms over number fields

In this last section we assume that K is a number field i.e. a finite extension of the rationals $\mathbb{Q}$.

Definition 7.1. *A property P is called* **local***, if P holds over K if and only if it holds over all completions of K.*
So a property P is a **local property** *for $\mathbb{Q}$ means that P holds for $\mathbb{Q}$ if and only if it holds for all $\mathbb{Q}_p$ (p a prime) and for $\mathbb{R} =: \mathbb{Q}_\infty$.*

The Theorem of Hasse and Minkowski says that isometry of quadratic spaces is a local property:

Theorem 7.2. *(Weak theorem of Hasse and Minkowski) Two regular quadratic spaces (V, Q) and (V', Q') over a number field K are isometric, if and only if they are isometric over all completions of K.*

As a conclusion we get a precise set of invariants of the isometry class of a quadratic space over a number field.

Corollary 7.3. *Over a number field K the isometry class of a regular quadratic space is uniquely determined by its dimension, its determinant, its Clifford invariant and its signature at all real places of K.*

Proof. By the theorem of Hasse and Minkowski it is enough to consider all completions. For the infinite places these are either $\mathbb{C}$ or $\mathbb{R}$. As $\mathbb{C}$ is algebraically closed two regular quadratic spaces are isometric if and only if they have the same dimension. Over the real numbers, the theorem by Sylvester tells us that signature and dimension classifies quadratic spaces.

For the finite places the completion is a finite extension of $\mathbb{Q}_p$, and Corollary 6.8 allows to conclude the statement from the theorem of Hasse and Minkowski. □

The strong theorem of Hasse and Minkowski states that representing zero nontrivially is also a local property, i.e. there is $0 \neq v \in V$ with $Q(v) = 0$ if and only if such vectors are contained in every completion of V. It allows to conclude, for instance, the theorem that indefinite rational quadratic spaces of dimension ≥ 5 are isotropic and indefinite rational quadratic spaces of dimension ≥ 4 are universal.

8 An application to orthogonal groups

In this section we assume that (V, Q) is a regular quadratic space over a field K.

As $O(V, Q) = O(V, aQ)$ for all $a \in K^\times$ we can only expect to be able to read off those invariants of Q from $O(V, Q)$ that are independent of scaling. Besides the dimension and real signature (up to sign) these are the ones determined by the even Clifford algebra $\mathcal{C}_0(V, Q)$. So one may expect to read off the discriminant algebra if $\dim(V)$ is even and the Clifford invariant if $\dim(V)$ is odd.

8.1 The adjoint involution

Remark 8.1. *Any regular symmetric bilinear form B defines an involution on* $\operatorname{End}(V)$*, the* **adjoint involution***, with $B(\alpha(x), y) = B(x, \alpha^{ad}(y))$ for all $x, y \in V, \alpha \in \operatorname{End}(V)$. Choosing matrices with respect to some basis e and writing $B := {}_eB_e$ we obtain $A^{ad} = BA^{tr}B^{-1}$ and*

$$O(V, B) = \{g \in \mathrm{GL}_n(K) \mid gBg^{tr} = B\} = \{g \in \mathrm{GL}_n(K) \mid g^{ad} = g^{-1}\}.$$

As A and A^{tr} have the same Jordan canonical form, they are always conjugate and so are A and A^{ad}.

Corollary 8.2. *If $g \in O(V, B)$ then g is conjugate (in $\mathrm{GL}_n(K)$) to its inverse $g^{-1} = g^{ad}$.*

Note that $A^{ad}B = (AB)^{tr}$. In particular if $A^{ad} = -A$ if and only if AB is a skew-symmetric matrix.

Theorem 8.3. *There is $X = -X^{ad} \in \mathrm{GL}_n(K)$ if and only if $n = \dim(V)$ is even. Then $\det(X)(K^\times)^2 = \det(B)$.*

Proof. It is well known that there is a skew-symmetric matrix $Y = -Y^{tr}$ of non-zero determinant if and only if n is even. Then the determinant of Y is a square, as there is $T \in \mathrm{GL}_n(K)$ such that

$$TYT^{tr} = \mathrm{diag}(\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix})$$

Now $X = -X^{ad}$ implies that $(XB) = -(XB)^{tr}$ and hence $\det(X)\det(B) = \det(XB) \in (K^\times)^2$. □

Theorem 8.4. *[1] Assume that there is $g \in O(V,B)$ such that $P(1)P(-1) \neq 0$, where P is the characteristic polynomial of g. Then $\det(g) = 1$, $n = \dim(V)$ is even, and $\det(B) = P(1)P(-1)(K^\times)^2$.*

Proof. Write $P = \prod_{i=1}^n (X - \xi_i)$ over an algebraic closure of K. As g is conjugate to g^{-1} the eigenvalue ξ_i^{-1} of g has the same multiplicity as ξ_i. As $\xi_i \neq \xi_i^{-1}$ for all i we have $\det(g) = \prod_{j=1}^n \xi_j = 1$ and n is even. Moreover

$$P(1)P(-1) = \prod_{j=1}^n (\xi_j^2 - 1) = (\prod_{j=1}^n \xi_j) \prod_{j=1}^n (\xi_j - \xi_j^{-1}) = \det(g)\det(g - g^{-1}) = \det(g - g^{-1})$$

so $P(1)P(-1) = \det(g - g^{-1}) = \det(B)$ up to squares. □

Corollary 8.5. *If $g \in O(V,B)$ is such that $g^2 = -\mathrm{id}_V$, then $\dim(V)$ is even and $\det(B) = 1$.*

Proof. Here $P = (X^2+1)^{n/2}$, so n is even and $P(1)P(-1) = 2^n$ is a square. □

8.2 The Spinor norm

As we have seen in Remark 5.8 the quadratic form Q defines a group homomorphism

$$\mathrm{SN}_Q : O(V,Q) \to K^\times/(K^\times)^2, \mathrm{SN}(s_v) = Q(v)$$

the Spinor norm. If $\mathrm{char}(K) \neq 2$ then the Spinor norm of the orthogonal mapping $-\mathrm{id}_V$ is the half-determinant of V.

Corollary 8.6. *If $-\mathrm{id}_V \in O(V,Q)'$. Then $\dim(V)$ is even and $\det(Q) \in (K^\times)^2$.*

8.3 The action on the Clifford algebra

Any orthogonal map $g \in O(V,Q)$ defines an K-algebra automorphism $c(g)$ on the Clifford algebra $\mathcal{C}(V,Q)$ that respects the grading (see Theorem 5.6). In particular $c(g)$ is an algebra automorphism of the central simple Clifford algebra $\mathfrak{c}(V,Q)$ (see Definition 5.15). The Theorem of Skolem and Noether tells us that such automorphisms are inner, and hence we obtain a projective representation

$$c : O(V,Q) \to \mathfrak{c}(V,Q)^\times/K^\times$$

that turns the simple $\mathfrak{c}(V,Q)$-module S into a projective $KO(V,Q)$-module. Clearly $\mathfrak{c}(V,Q) \cong S \otimes S^*$.

Remark 8.7. *Let χ be the character of the $KO(V,Q)$-module S. Then $\chi^2 = \sum_{i=0}^{n} \Lambda^i(\chi_V)$ where χ_V is the character of V.*

This observations sometimes allows one to read off the discriminant of Q just from the character table of a subgroup G of $O(V,Q)$:
1) Let $G \cong 2.O_8^+(2)$. Then G is perfect and its universal covering group is $\tilde{G} \cong 2^2.O_8^+(2)$. Let V be the 8-dimensional faithful $\mathbb{Q}G$-module with character χ and Q a non zero G-invariant quadratic form on V. Then $\dim(\mathfrak{c}(V,Q)) = 2^8$ and $\tilde{\chi} = \chi_W \otimes \chi_W$ for a 16-dimensional $\tilde{G}$-module W. One calculates that $\chi_W = \chi_8 + \chi_8'$ is the sum of the two irreducible characters $\chi_8, \chi_8' \neq \chi$ which belong to absolutely irreducible rational modules of degree 8 of $\tilde{G}$. Therefore the discriminant of $(V,Q) = 1$ and also $[\mathfrak{c}(V,Q)] = [\mathbb{Q}]$.
2) Let $G \cong M^cL$ and (V,q) a 22-dimensional orthogonal $\mathbb{Q}G$-module with character χ. The universal covering group of G is $3.G$. Therefore $c : G \to \mathfrak{c}(V,Q)^\times$ can be chosen to be linear. There is a unique character χ_W of G satisfying $\chi_W \otimes \chi_W = \tilde{\chi}$. In the notation of ATLAS one has $\chi_W = 2(\chi_1 + \chi_2 + \chi_3) + \chi_5 + \chi_6$. Now the character field $\mathbb{Q}[\chi_5] = \mathbb{Q}[\chi_6] = \mathbb{Q}[\sqrt{-15}]$ from which we get that the discriminant of (V,Q) is -15.

For more examples see [2].

References

[1] Eva Bayer-Fluckiger, Isometries of quadratic spaces. J. EMS **17** (2015) 1629–1656

[2] G. Nebe, Invariants of orthogonal G-modules from the character table. Exp. Math. 9 (2000) 623-630

[3] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The Book of Involutions.* AMS Coll. Publications **44** (1998)

Index