Quadratic Forms, SS 2013

Prof. Dr. Gabriele Nebe

based on
Martin Kneser: Quadratische Formen (Springer 2002)

December 5, 2016

Contents

Chapter 1

Basic notions and examples.

All rings are associative and have a unit.
A will be some commutative ring. E.g. A a field ($\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}(x)$), or a principal ideal domain ($\mathbb{Z}$, $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$, $\mathbb{Q}[x]$), but also $A = \mathbb{Z}/4\mathbb{Z}, \mathbb{Z} \oplus \mathbb{Z}, \ldots$.
E will denote some A-module such that $1x = x$ for all $x \in E$. (Most of the time E will be finitely generated.)

1 Symmetric bilinear forms

Definition 1.1. *(a) A map $b : E \times E \to A$ is called* **symmetric bilinear form**, *if*

$$b(x, y) = b(y, x) \text{ and } b(ax + y, z) = ab(x, z) + b(y, z) \text{ for all } x, y, z \in E, a \in A.$$

We then call (E, b) a **bilinear A-module**.
(b) If (E, b) and (E', b') are bilinear A-modules then an A-module homomorphism $\varphi : E \to E'$ is called an **isometry** *(sometimes* **isometric embedding***), if φ is injective and $b'(\varphi(x), \varphi(y)) = b(x, y)$ for all $x, y \in E$. Two bilinear A-modules (E, b) and (E', b') are called* **isometric**, *$(E, b) \cong (E', b')$, if there is some bijective isometry $\varphi : E \to E'$.*

Clear: The inverse of a bijective isometry is again an isometry and being isometric is an equivalence relation.

Definition 1.2. *Let (E, b) be a bilinear A-module.*

(a) $x, y \in E$ are called **orthogonal** *if $b(x, y) = 0$ (notation: $x \perp y$). For a subset $F \subset E$ we put $F^\perp := \{x \in E \mid b(x, y) = 0 \text{ for all } y \in F\}$ the* **orthogonal submodule** *of F.*

(b) E is called (inner) **orthogonal sum** *of the submodules $E_1, \ldots, E_n$,*

$$E = E_1 \perp\!\!\!\bigoplus E_2 \perp\!\!\!\bigoplus \ldots \perp\!\!\!\bigoplus E_n = \perp\!\!\!\bigoplus_{i=1}^{n} E_i$$

if $E = E_1 \oplus \ldots \oplus E_n$ is an inner direct sum and $E_i \perp E_j$ for all $i \neq j$.

(c) We call $E^* := \mathrm{Hom}_A(E, A) := \{\varphi : E \to A \mid \varphi \text{ is } A-\text{module homomorphism }\}$ the **dual module** *of E.*

(d) For a submodule $F \leq E$ and $x \in E$ let $b_F(x) : F \to A, b_F(x)(y) := b(x, y)$ for all $y \in F$.

Clear: $F^\perp$ is an A-submodule of E.
$b_F(x) \in F^*$.

Remark 1.3. *Let (E,b) be a bilinear A-module and $F \leq E$. The mapping $b_F : E \to F^*, x \mapsto b_F(x)$ is an A-module homomorphism with kernel $F^\perp$.*

Lemma 1.4. *Let (E,b) be a bilinear A-module and $F \leq E$. Then $E = F \perp F^\perp$ if and only if $F \cap F^\perp = 0$ and $b_F(F) = b_F(E)$.*

Proof. $\Rightarrow$ is clear. $\Leftarrow$: Let $b_F(E) = b_F(F)$. Let $x \in E$ and choose $y \in F$ with $b_F(x) = b_F(y)$. Then $z := x - y \in F^\perp = \ker(b_F)$ and $x = y + z$, so $E = F + F^\perp$. That the sum is direct follows from the assumption $F \cap F^\perp = 0$. □

Definition 1.5. *The bilinear A-module (E,b) is called* **non-degenerate**, *if b_E is injective (i.e. $E^\perp = \ker(b_E) = \{0\}$).*
(E,b) is called **regular**, *if E is a finitely generated projective A-module and b_E is bijective.*

Theorem 1.6. *Let (E,b) be a bilinear A-module and $F \leq E$. If $(F, b_{|F\times F})$ is regular, then $E = F \perp F^\perp$.*

Proof. (F,b) regular $\Rightarrow (b_F)_{|F} : F \to F^*$ bijective $\Rightarrow b_F(F) = b_F(E)$ and $\ker((b_F)_{|F}) = F \cap F^\perp = 0$ so by Lemma 1.4 $E = F \perp F^\perp$. □

Remark 1.7. *If $E = \bigoplus_{i=1}^n E_i$ then $E^* \cong \bigoplus_{i=1}^n E_i^*$ via $f \mapsto (f_{|E_1}, \ldots, f_{|E_n})$ where the inverse isomorphism is $(f_1, \ldots, f_n) \mapsto f$, with $f(x) = f(x_1, \ldots, x_n) = \sum_{i=1}^n f_i(x_i)$.*

In particular $(A^n)^* \cong A^n$ and if P is finitely generated and projective, then also P^* is projective.

Corollary 1.8. *Assume that the bilinear A-module (E,b) is of the form $E = \perp_{i=1}^n E_i$ and put $b_i := b_{|E_i \times E_i}$. Then we have*
(a) (E,b) is non degenerate, if and only if (E_i, b_i) is non degenerate for all i.
(b) (E,b) is regular, if and only if (E_i, b_i) is regular for all i.

Proof. The isomorphism from Remark 1.7 maps $b_E(x)$ to $((b_1)_{E_1}(x_1), \ldots, (b_n)_{E_n}(x_n))$ for $x = \sum_{i=1}^n x_i \in E$. Therefore b_E is injective, if and only if all $(b_i)_{E_i}$ are injective and b_E is an isomorphism, if and only if all $(b_i)_{E_i}$ are isomorphisms. □

1.1 Free modules, Gram matrices and determinants.

Let $E = \bigoplus_{i=1}^n Ae_i$ be a free A-module with basis $e := (e_1, \ldots, e_n)$. Then the **Gram matrix** of b with respect to e is defined as ${}_eb_e := (b(e_i, e_j)) \in A^{n\times n}$. For $x = \sum_{i=1}^n x_i e_i$ and $y = \sum_{i=1}^n y_i e_i$ we have

$$b(x,y) = (x_1, \ldots, x_n)\ {}_eb_e(y_1, \ldots, y_n)^{tr} \in A^{1\times 1} = A$$

If e' is a second basis of E, then $e'_i = \sum_{j=1}^n t_{ij} e_j$ with

$$T := (t_{ij}) \in \mathrm{GL}_n(A) := \{X \in A^{n\times n} \mid \det(X) \in A^*\}$$

and ${}_{e'}b_{e'} = T({}_eb_e)T^{tr}$. In particular $\det({}_{e'}b_{e'}) = \det(T)^2 \det({}_eb_e)$.

Definition 1.9. *Let (E,b) be a free bilinear A-module with basis e. Then* $\det(E,b) := \det({}_eb_e)(A^*)^2 \in A/(A^*)^2$ *is called the* **determinant** *of (E,b).*

Remark 1.10. *The determinant* $\det(E,b) \in A/(A^*)^2$ *is an invariant of the isometry class of the free bilinear A-module.*

Example: Let $A = \mathbb{Q}$ and $E = \mathbb{Q}e_1 \oplus \mathbb{Q}e_2$. Define two symmetric bilinear forms b and b' on E by

$$ {}_eb_e := \operatorname{diag}(1,3), \quad {}_eb'_e := \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}. $$

Then $\det(E,b) = \det(E,b') = 3$ but $(E,b) \ncong (E,b')$. Otherwise let $\varphi : (E,b') \to (E,b)$ be some isometry and $x = a_1e_1 + a_2e_2 = \varphi(e_1)$. Then $b(x,x) = a_1^2 + 3a_2^2 = b'(e,e) = 2$ which easily leads to a contradiction by considering divisibility by 2.

If e is a basis of E and e^* the dual basis of E^* (so $e_i^*(e_j) = \delta_{ij}$), then

$$ b_E(e_j) = \sum_{k=1}^{n} b_{kj}e_k^*, \text{ with } b_{kj} = b(e_k,e_j) = ({}_eb_e)_{k,j} $$

so the Gram matrix is the matrix of the linear mapping $b_E : E \to E^*$ with respect to the basis e and e^*.

Corollary 1.11. *(a) (E,b) regular $\Leftrightarrow$ $b_E : E \to E^*$ bijective $\Leftrightarrow$ ${}_eb_e \in \mathrm{GL}_n(A) \Leftrightarrow \det({}_eb_e) \in A^*$.*
(b) (E,b) non degenerate $\Leftrightarrow$ $b_E : E \to E^*$ injective $\Leftrightarrow \ker({}_eb_e) = 0 \Leftrightarrow \det({}_eb_e) \in A$ not a zero divisor.

Remark 1.12. *Assume that* $d_i := \det(B_i) \in A^*$ *where* $B_i := {}_{(e_1,\dots,e_i)}b_{(e_1,\dots,e_i)} \in A^{i\times i}$ *for all $i = 1,\dots,n$. Then* $E \cong \bigoplus_{i=1}^n Ac_i$ *with* $b(c_i,c_i) = \frac{d_i}{d_{i-1}}$ *($d_0 := 1$).*

Proof. By induction it is enough to write

$$ E_{k+1} := \oplus_{i=1}^{k+1} Ae_i = \oplus_{i=1}^{k} Ae_i \perp\!\!\!\oplus Ac_{k+1} = E_k \perp\!\!\!\oplus Ac_{k+1} $$

with $b(c_{k+1},c_{k+1}) = \frac{d_{k+1}}{d_k}$. Since $d_k = \det(B_k) \in A^*$ there is some $f_{k+1} \in \oplus_{i=1}^k Ae_i$ such that $b_{E_k}(f_{k+1}) = b_{E_k}(e_{k+1})$. Put $c_{k+1} := e_{k+1} - f_{k+1} \in E_k^\perp$. Then $(e_1,\dots,e_k,c_{k+1})$ is a basis of E_{k+1} and the base change matrix to $(e_1,\dots,e_{k+1})$ has determinant 1. Comparing the determinant of the Gram matrices we get

$$ d_k b(c_{k+1},c_{k+1}) = d_{k+1}. $$

□

Definition 1.13. *Let (E,b) be a free regular bilinear A-module with basis $(e_1,\dots,e_n)$. Let* $e_i^\# := b_E^{-1}(e_i^*) \in E$, *so $b(e_i,e_j^\#) = \delta_{ij}$ for all i,j. Then $(e_1^\#,\dots,e_n^\#)$ is called the* **dual basis of** *E. The Gram matrix of b is the base change matrix between the basis and its dual basis.*

Remark 1.14. *Let (E,b) be a bilinear A-module and $F \le E$. Then $(F^\perp)^\perp \supseteq F$.*
If E is regular and $F \le E$ a free submodule with a basis that can be extended to a basis of E, then $(F^\perp)^\perp = F$.
In particular if A is a field and (E,b) a regular A-vector space then $(F^\perp)^\perp = F$ and $\dim(F) + \dim(F^\perp) = \dim(E)$ *for any subspace $F \le E$.*

Proof. If $F = Ae_1 \oplus \ldots \oplus Ae_m$ such that $E = Ae_1 \oplus \ldots \oplus Ae_m \oplus Ae_{m+1} \oplus \ldots \oplus Ae_n$, then $F^\perp = Ae_{m+1}^\# \oplus \ldots \oplus Ae_n^\#$ and hence $(F^\perp)^\perp = F$.
For fields we obtain $\dim(F) = \dim(F^*) = \dim(b_F(E)) = \dim(E) - \dim(\ker(b_F)) = \dim(E) - \dim(F^\perp)$. □

Example. Let $A = \mathbb{Z}$, $E = Ae$, $b(e,e) = 1$, $F = A(2e)$ then $F^\perp = \{0\}$ and $(F^\perp)^\perp = E \neq F$.

1.2 Free bilinear modules, some examples.

(a) Here A is an arbitrary ring and we take $\mathbb{I}_n(A) = \bigoplus_{i=1}^n Ae_i$ with $b(e_i, e_j) = \delta_{ij}$. The Gram matrix of this basis is the unit matrix, so $e_i^\# = e_i$, the module is regular.
(b) From now on we take $A = \mathbb{Z}$ and introduce some important lattices. $\mathbb{I}_n := \mathbb{I}_n(\mathbb{Z})$ is sometimes called the standard lattice. We define

$$\mathbb{A}_{n-1} := \{\sum_{i=1}^n x_i e_i \in \mathbb{I}_n \mid \sum_{i=1}^n x_i = 0\}.$$

Then $(e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n)$ is a $\mathbb{Z}$-basis of $\mathbb{A}_{n-1}$. The rank of $\mathbb{A}_{n-1}$ is $n-1$ and $\det(\mathbb{A}_{n-1}) = n$. $\mathbb{A}_{n-1}$ is not regular but non-degenerate.
$\mathbb{D}_n := \{\sum_{i=1}^n x_i e_i \in \mathbb{I}_n \mid \sum_{i=1}^n x_i \in 2\mathbb{Z}\}$ has basis $(e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n, e_{n-1} + e_n)$, determinant 4 and rank n. For the Gram matrices we find

$$\mathcal{G}(\mathbb{A}_n) := \begin{pmatrix} 2 & -1 & 0 & \ldots & \ldots & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & -1 & 2 & -1 \\ 0 & \ldots & \ldots & 0 & -1 & 2 \end{pmatrix}, \quad \mathcal{G}(\mathbb{D}_n) := \begin{pmatrix} 2 & -1 & 0 & \ldots & \ldots & 0 & 0 \\ -1 & 2 & -1 & 0 & \ldots & 0 & 0 \\ 0 & -1 & 2 & -1 & \ldots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & -1 & 2 & -1 & -1 \\ 0 & \ldots & \ldots & 0 & -1 & 2 & 0 \\ 0 & \ldots & \ldots & 0 & -1 & 0 & 2 \end{pmatrix}$$

1.3 Bilinear modules over fields.

Theorem 1.15. *Let (E, b) be a finite dimensional bilinear vector space over some field A. Then $E = E_1 \perp\!\!\!\oplus E_2 \perp\!\!\!\oplus \ldots \perp\!\!\!\oplus E_r \perp\!\!\!\oplus F$ with E_i regular for all i, $\dim(E_i) = 1$ or 2 and $F = E^\perp$ (so $b(F, E) = b(F, F) = \{0\}$). If $\mathrm{char}(A) \neq 2$ all E_i can be chosen to be of dimension 1. In this case (E, b) has an orthogonal basis (which can be computed with a variant of Gram Schmidt)*

Proof. Induction over the dimension of E. $\dim(E) = 0$ and $\dim(E) = 1$ are trivial. So assume that $\dim(E) = n > 0$.
(a) If $b(E, E) = \{0\}$ then $E = E^\perp =: F$ and we are done.
(b) So assume that $b(E, E) \neq \{0\}$. Then we have two possibilities:
(i) There is some $e \in E$ such that $b(e, e) \neq 0$. Then $Ae \leq E$ is a regular subspace and we may hence write $E = Ae \perp\!\!\!\oplus (Ae^\perp)$ with $\dim(Ae^\perp) = \dim(E) - 1 = n - 1$ and proceed by induction.
(ii) For all $e \in E$ we have $b(e, e) = 0$. Then there are $e, f \in E$ such that $b(e, f) \neq 0$ and $\langle e, f\rangle \leq E$ is a regular subspace, so $E = \langle e, f\rangle \perp\!\!\!\oplus \langle e, f\rangle^\perp$ with $\dim(\langle e, f\rangle^\perp) = n - 2$ and again we proceed by induction. Note that case (b) (ii) cannot happen if $2 \neq 0 \in A$, as then

$$b(e + f, e + f) = b(e, e) + 2b(e, f) + b(f, f) = 0 + 2b(e, f) + 0 \neq 0.$$

□

Example. $E = \langle e, f\rangle$ with $b(f,f) = b(e,e) = 0$, $b(e,f) = 1$, Gram matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $b(\alpha e + \beta f, \alpha e + \beta f) = 2\alpha\beta$ which is 0 for all $\alpha, \beta \in A$ if the characteristic of A is 2. If $\mathrm{char}(A) \neq 2$ then we may write $E = A(e+f) \perp A(e-f)$.

2 Quadratic forms.

As before let E be an A-module.

Definition 2.1. *(a) $q : E \to A$ is called a* **quadratic form** *if*
(i) $q(ax) = a^2 q(x)$ for all $x \in E, a \in A$ and
(ii) $b_q : E \times E \to A, b_q(x,y) := q(x+y) - q(x) - q(y)$ is a symmetric bilinear form.
We then call (E,q) a **quadratic A-module**.

(b) $\varphi : (E,q) \to (E',q')$ is called an **isometry** *between the two quadratic A-modules (E,q) and (E',q'), if φ is an injective A-module homomorphism such that $q'(\varphi(x)) = q(x)$ for all $x \in E$. The two modules are called* **isometric**, *if there is some bijective isometry between them: $(E,q) \cong (E',q')$.*

(c) The **orthogonal sum** *of two quadratic A-modules is*

$$(E,q) \bigoplus\!\!\!\!\!\perp (E',q') := (E \oplus E', q \perp q') \text{ with } (q \perp q')(x,x') := q(x) + q'(x').$$

Remark 2.2. *If (E,b) is some bilinear A-module, then*

$$q_b : E \to A, q_b(x) := b(x,x)$$

is a quadratic form on E with $b_{q_b} = 2b$.
If (E,q) is a quadratic A-module, then (E,b_q) is a bilinear A-module and $q_{b_q} = 2q$.
Given some A-module E, there are hence mappings

$$\begin{aligned} f :&\ \text{sym. bifo on } E \to \text{ quad. forms on } E, \quad b \mapsto b_q \\ b :&\ \text{quad. forms on } E \to \text{ sym. bifo on } E, \quad q \mapsto q_b \end{aligned}$$

such that $f \circ g = 2\mathrm{id}$ and $g \circ f = 2\mathrm{id}$.
If $2 \in A^*$ then the notions of quadratic forms and symmetric bilinear forms are equivalent: Given some bilinear A-module (E,b) then (E,Q_b) is a quadratic A-module with $Q_b(x) := \frac{1}{2}b(x,x)$ such that $b = b_{Q_b}$.

Definition 2.3. *(a) A quadratic A-module (E,q) is called* **regular**, *if (E,b_q) is regular.*
(b) A quadratic A-module (E,q) is called **non degenerate**, *if (E,b_q) is non degenerate.*
(c) An element x of the quadratic A-module (E,q) is called **singular**, *is $q(x) = 0$.*
(d) A submodule $F \leq E$ of the quadratic A-module (E,q) is called **singular**, *is $q(F) = \{0\}$.*
(e) (E,q) is called **anisotropic**, *if for all $x \in E$: $q(x) = 0 \Rightarrow x = 0$.*

Attention. If 2 is a zero divisor in A, then the condition $q(F) = \{0\}$ is stronger than $F \subset F^\perp$.

2.1 Free quadratic modules and Gram matrices.

Let $E = \bigoplus_{i=1}^n Ae_i$ be a free A-module, $q : E \to A$ a quadratic form. Then

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

where

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

Notation

$$(E, q) := \begin{bmatrix} q(e_1) & & b_q(e_i, e_j) \\ & \ddots & \\ & & q(e_n) \end{bmatrix}$$

respectively $(E, q) = [q(e_1), \ldots, q(e_n)]$ if $b_q(e_i, e_j) = 0$ for all $i \neq j$.
If 2 is not a zero divisor, we put $b_{ij} := b_q(e_i, e_j)$ for all i, j and use the notation

$$(E, q) = \left\langle \begin{matrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ldots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{matrix} \right\rangle.$$

For example let $E = Ae_1$ with $q(e_1) = 1$ then $(E, q) = [1] = \langle 2 \rangle$. If $2 \notin A^*$ then (E, q) is not regular.
Let $E = Ae_1 \oplus Ae_2$ with $q(a_1 e_1 + a_2 e_2) = a_1 a_2$. Then

$$(E, q) = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} = \left\langle \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \right\rangle =: \mathbb{H}.$$

This quadratic space is called the **hyperbolic plane**. Since $\det(E, b_q) = -1$ the hyperbolic plane is always regular.

Lemma 2.4. *Let (E, q) be a quadratic A-module such that E is a finitely generated projective A-module. Then there is a bilinear form $a : E \times E \to A$ such that $a(x, x) = q(x)$.*

Proof. If E is a free A-module then we may take the upper triangular matrix Q from above as the Gram matrix of a. In general we find a projective A-module P such that $P \oplus E$ is a finitely generated free A-module and then restrict the bilinear form a on $P \oplus E$ to E. □

Remark 2.5. *Let (E, q) be a quadratic A-module such that $E = \bigoplus_{i=1}^n Ae_i$ is free, and let (F, q') be any quadratic A-module. An A-module homomorphism $\varphi : E \to F$ is an isometry, if and only if φ is injective, $q(e_i) = q'(\varphi(e_i))$ for all i and $b_q(e_i, e_j) = b_{q'}(\varphi(e_i), \varphi(e_j))$.*

Lemma 2.6. *Let n be odd and*

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

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

Proof. The proof is elementary linear algebra and follows from the Leibniz rule $\det(B) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^n B_{i,$
Let

$$S := \{\pi \in S_n \mid \pi = \pi^{-1}\} \text{ and}$$
$$T := \{\pi \in S_n \mid \pi \neq \pi^{-1}\} = X \dot\cup \{\pi^{-1} \mid \pi \in X\}.$$
$$\pi \in S \Rightarrow \exists i \in \{1,\dots,n\}, \pi(i) = i \text{ because } n \text{ is odd .}$$
$$\pi \in X \Rightarrow \prod_{i=1}^n B_{i,\pi(i)} = \prod_{i=1}^n B_{\pi(i),(i)} \prod_{i=1}^n B_{i,\pi^{-1}(i)}$$

because B is symmetric. Since $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$ we have

$$\det(B) = 2\sum_{\pi\in X} \operatorname{sgn}(\pi) \prod_{i=1}^n B_{i,\pi(i)} + \sum_{\pi\in S} \operatorname{sgn}(\pi) \underbrace{\prod_{i=1}^n B_{i,\pi(i)}}_{2|} = 2P_n(a_i, b_{ij}).$$

□

Corollary 2.7. *Let (E,q) be a free quadratic A-module of odd rank n. If $2 \notin A^*$ then (E,q) is not regular. Then we put $\det'(E,q) := P_n(q(e_i), b_q(e_i,e_j))$ for P_n as in Lemma 2.6 and call (E,q)* **semi-regular**, *if $\det'(E,q) \in A^*$.*

Clear. $2 \in A^*$ then (E,q) is regular if and only if it is semi-regular.
If $(E,q) = (E_1,q_1) \perp\!\!\!\perp (E_2,q_2)$ with free modules of rank $\dim_A(E_1) = 2n$, $\dim_A(E_2) = 2m+1$, then $\det'(E,q) = \det(E_1,q_1)\det'(E_2,q_2)$.

Example: $E = \mathbb{Z}e_1$ with $q(e_1) = 1$. Then (E,q) is semi-regular but no regular.

Theorem 2.8. *Let A be a field and (E,q) a finite dimensional quadratic A-vector space. Then there are subspaces $E_1,\dots,E_r$, $F_1,\dots,F_s$, $G \leq E$ such that*

- $\dim(E_i) = 2$, $(E_i, q_{|E_i})$ *regular for all* $1 \leq i \leq r$.
- $\dim(F_i) = 1$, $(F_i, q_{|F_i})$ *semi-regular for all* $1 \leq i \leq s$.
- $q(G) = \{0\}$
- $(E,q) = E_1 \perp\!\!\!\perp \dots \perp\!\!\!\perp E_r \perp\!\!\!\perp F_1 \perp\!\!\!\perp \dots \perp\!\!\!\perp F_s \perp\!\!\!\perp G$.

If $\operatorname{char}(A) \neq 2$ then one may choose $r = 0$ (and all F_i are regular). Then (E,q) is regular, if and only if $G = 0$.
If $\operatorname{char}(A) = 2$ then one may choose $s \leq [A : A^2]$.
(E,q) regular, if and only if $s = 0$ and $G = 0$.
(E,q) semi-regular, if and only if $s \leq 1$ and $G = 0$.

Note if $\operatorname{char}(A) = 2$ then $A^2 := \{a^2 \mid a \in A\}$ is a subfield of A. If $|A| < \infty$ then $A^2 = A$ and hence $[A : A^2] = 1$, but for $A = \mathbb{F}_2(x)$ we have $A^2 = \mathbb{F}_2(x^2)$ and $[A : A^2] = 2$.
Proof. The theorem follows from Theorem 1.15 in the case that $\operatorname{char}(A) \neq 2$. So we will assume $\operatorname{char}(A) = 2$. By Theorem 1.15 we may write

$$(E, b_q) = E_1 \perp\!\!\!\perp \dots \perp\!\!\!\perp E_r \perp\!\!\!\perp F$$

with regular 2-dimensional quadratic subspaces E_i and $b_q(F,F) = \{0\}$ (so $F = E^\perp$).
If remains to decompose F: Since $b_q(F,F) = 0$ the restriction of the quadratic form $q : F \to A$ is a

$\mathbb{Z}$-linear map, $q(x+y) = q(x)+q(y)$ for all $x, y \in F$ satisfying $q(ax) = a^2 q(x)$ for all $a \in A, x \in F$. So

$$G := \{x \in F \mid q(x) = 0\} = \ker(q_{|F}) \leq F$$

is a linear subspace (closed under addition and scalar multiplication) of F. The image $q(F) \leq A$ of q is an A^2-subspace of A. Choose $f_i \in F$ such that $(q(f_1), \ldots, q(f_s))$ is an A^2-basis of $q(F)$. Then $(f_1 + G, \ldots, f_s + G)$ is an A-basis of F/G:
generating set: $f \in F$, $q(f) = \sum_{i=1}^s a_i^2 q(f_i)$, then $f - \sum_{i=1}^s a_i f_i \in G$.
linearly independent: $\sum_{i=1}^s a_i f_i \in G \Leftrightarrow \sum_{i=1}^s a_i^2 q(f_i) = 0 \Leftrightarrow a_i^2 = 0$ for all $i \Leftrightarrow a_i = 0$ for all i since a field does not have zero divisors.
So

$$F = Af_1 \perp\!\!\!\perp Af_2 \perp\!\!\!\perp \ldots \perp\!\!\!\perp Af_s \perp\!\!\!\perp G$$

with $s = \dim_{A^2}(q(F)) \leq [A : A^2]$ and $q(f_i) \neq 0$, so Af_i semi-regular. □

Example. Take $A = \mathbb{F}_2(x)$, $E = A^3$, $q((t_1, t_2, t_3)) = t_1^2 + xt_2^2 + x^2 t_3^2$, so $(E, q) = [1, x, x^2]$. Then $\det'(E, q) = 4x^3 = 0$ so E is not semi-regular. We compute $G = \langle (x, 0, 1) \rangle$ and

$$E = \langle (1, 0, 0) \rangle \perp\!\!\!\perp \langle (0, 1, 0) \rangle \perp\!\!\!\perp G$$

with $q((1, 0, 0)) = 1$, $q((0, 1, 0)) = x$ an $\mathbb{F}_2(x^2)$-basis of $\mathbb{F}_2(x)$.

2.2 Hyperbolic modules.

Definition 2.9. *Let G be some A-module. Then*

$$\mathbb{H}(G) := (G \oplus G^*, q_G), \text{ with } q_G(x + x^*) := x^*(x) \text{ for all } x \in G, x^* \in G^* = \mathrm{Hom}_A(G, A)$$

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

Clear. $b_{q_G}(x + x^*, y + y^*) = x^*(y) + y^*(x)$.
If $G = \bigoplus_{i=1}^n Ae_i$ is a free A-module and $(e_1^*, \ldots, e_n^*)$ is the dual basis of G^*, then the Gram matrix if $\mathbb{H}(G)$ with respect to the basis $(e_1, \ldots, e_n, e_1^*, \ldots, e_n^*)$ is $\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$.

Definition 2.10. *(a) Let E be an A-module. A submodule $F \leq E$ is called* **primitive** *if there is some $G \leq E$ such that $E = F \oplus G$.*
(b) Let (E, b) be a bilinear A-module. A submodule $F \leq E$ is called **sharply primitive** *if F is a finitely generated projective submodule such that $b_F(E) = F^*$.*

Example. $E = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ then $\mathbb{Z}(e_1 + e_2)$ is primitive but $\mathbb{Z}(2e_1)$ is not primitive.

Lemma 2.11. *Let $S, F \leq (E, b)$ be submodules such that F is f.g. projective. $b_F : S \to F^*$ is an isomorphism. Then $b_S : F \to S^*$ is an isomorphism.*

Proof. There is a natural isomorphism $\varphi : F \to (F^*)^*$ defined by $\varphi(f)(f^*) = f^*(f)$ for all $f \in F, f^* \in F^*$. The isomorphism $b_F : S \to F^*$ yields a natural isomorphism $b_F^* : (F^*)^* \to S^*$ defined by $b_F^*(\alpha)(s) := \alpha(b_F(s))$ for all $\alpha \in (F^*)^*$, $s \in S$. We claim that $b_S = b_F^* \circ \varphi$. For $f \in F$, $s \in S$ we have

$$b_F^*(\varphi(f))(s) = b_F(s)(f) = b(s, f) = b(f, s) = b_F(s).$$

□

Remark 2.12. *(i) $F \leq (E,b)$ such that $(F, b_{|F\times F})$ is regular, then F is sharply primitive.*
(ii) $F \leq (E,b)$ sharply primitive, then F is primitive.
(iii) (E,b) regular, $F \leq E$ primitive, then F is sharply primitive.

Proof. (i) $b_F(F) = F^* \Rightarrow b_F(E) = F^*$.
(ii) Since F is projective, also F^* is projective and the exact sequence

$$0 \to F^\perp \to E \stackrel{b_F}{\to} F^* \to 0$$

splits so there is some submodule $S \leq E$ such that $b_F : S \to F^*$ is an isomorphism. Put $G := S^\perp$. Then $G \leq E$, $F \cap G = \{0\}$, and $F + G = E$. Choose $e \in E$. By Lemma 2.11 there is some $f \in F$ such that $b_S(e) = b_S(f)$ and so $g := e - f \in S^\perp$.
(iii) E is finitely generated and projective and F is a direct summand of E, so also F is a finitely generated projective A-module. To see that $b_F(E) = F^*$ let $f \in F^*$ be arbitrary. Write $E = F \oplus G$ and extend f to a linear form on E by putting $f(x+y) = f(x)$ for all $x \in F, y \in G$. Then $f \in E^* = b_E(E)$ so there is some $e \in E$ such that $f = b_F(e)$. □

Theorem 2.13. *Let (E,q) be a quadratic A-module and $F \leq E$ a sharply primitive singular ($q(F) = \{0\}$) submodule. Then there is a direct summand $H \leq E$ such that $F \leq H$ and $H \cong \mathbb{H}(F)$. If F is free with basis $(f_1, \ldots, f_m)$ then one can extend this basis to some basis $(f_1, \ldots, f_m, g_1, \ldots, g_m)$ of H such that $b_q(f_i, g_j) = \delta_{ij}$ and $q(\langle g_1, \ldots, g_m\rangle) = \{0\}$.*

Proof. We use Remark 1.7 to see that the dual module of a finitely generated projective module is again projective. The A-module homomorphism $b_F : E \to F^*$ is onto. As F^* is projective, we may hence find a direct summand $G \leq E$ such that $b_F : G \to F^*$ is an isomorphism. Since $q(F) = \{0\}$ we have $F \leq \ker(b_F)$ and hence $F \cap G = \{0\}$. Put $H := F \oplus G$. It remains to replace G by a complement $\tilde{G}$ of F in H to achieve that $q(\tilde{G}) = \{0\}$.
By Lemma 2.4 there is some bilinear form $a : G \times G \to A$ such that $q(x) = a(x,x)$ for all $x \in G$. Since $b_F(G) = F^*$ we also get $b_G(F) = G^*$, in particular for any $x \in G$ there is a unique $y := \alpha(x) \in F$ such that

$$a(z,x) = b_q(z, \alpha(x)) \text{ for all } z \in G.$$

The map $\alpha : G \to F$ is an A-module homomorphism (Exercise !) and $\{x - \alpha(x) \mid x \in G\} =: \tilde{G}$ has the desired properties since for all $\alpha \in G$

$$q(x - \alpha(x)) = q(x) + q(\alpha(x)) - b_q(x, \alpha(x)) = q(x) + 0 - q(x) = 0.$$

If F is free then we can give a more precise algorithm. Since F is sharply primitive there are $(e_1, \ldots, e_m) \in E^m$ such that $b_q(f_i, e_j) = \delta_{ij}$. Put $g_1 := e_1 - q(e_1)f_1$. Then

$$q(g_1) = q(e_1) - q(e_1)b_q(e_1, f_1) + q(e_1)^2 q(f_1) = q(e_1) - q(e_1) = 0.$$

For $j = 2, \ldots, m$ we put

$$g_j = e_j - \sum_{i=1}^{j-1} b_q(g_i, e_j) f_i - q(e_j) f_j.$$

Then $b_q(g_j, f_i) = b_q(e_j, f_i) = \delta_{ij}$ since $F \subseteq F^\perp$. For $1 \leq k < j$ we find

$$b_q(g_j, g_k) = b_q(e_j, g_k) - \underbrace{\sum_{i=1}^{j-1} b_q(g_i, e_j) b_q(f_i, g_k)}_{= b_q(g_k, e_j)} - q(e_j) \underbrace{b_q(f_j, g_k)}_{=0} = 0.$$

Since $q(F) = 0$ we compute

$$q(g_j) = q(e_j) - \sum_{i=1}^{j-1} b_q(g_i, e_j)\underbrace{b_q(f_i, e_j)}_{=0} - q(e_j)b_q(f_j, e_j) = 0.$$

□

Theorem 2.14. *Let (E, q) be a quadratic A-module such that E is a projective A-module. Then there exists an isometric embedding $\varphi : (E, q) \to \mathbb{H}(E) = (E \oplus E^*, q_E(x + x^*) = x^*(x))$ such that $\varphi(E)^\perp \cong (E, -q)$. If (E, q) is regular, then*

$$\mathbb{H}(E) \cong \varphi(E) \perp\!\!\!\perp \varphi(E)^\perp = (E, q) \perp\!\!\!\perp (E, -q).$$

Proof. By Lemma 2.4 there is some bilinear form $a : E \times E \to A$ such that $q(x) = a(x, x)$ for all $x \in E$. Let

$$\begin{aligned} a_E : &\quad E \to E^*, \quad x \mapsto (y \mapsto a(y, x) = a_E(x)(y)) \\ a'_E : &\quad E \to E^*, \quad x \mapsto (y \mapsto a(x, y) = a'_E(x)(y)) \end{aligned}$$

and define $\varphi : E \to \mathbb{H}(E), x \mapsto x + a_E(x)$. Then φ is an injective A-module homomorphism that satisfies $q_E(\varphi(x)) = a_E(x)(x) = a(x, x) = q(x)$ for all $x \in E$, so $\varphi : (E, q) \to \mathbb{H}(E)$ is an isometry. The orthogonal space is

$$\varphi(E)^\perp = \{x + x^* \in E \oplus E^* \mid b_{q_E}(z + a_E(z), x + x^*) = a(x, z) + x^*(z) = 0 \text{ for all } z \in E\}$$

so $\varphi(E)^\perp = \{x - a'_E(x) \mid x \in E\} \cong (E, -q)$. since $q_E(x - a'_E(x)) = -a'_E(x)(x) = -a(x, x) = -q(x)$ for all $x \in E$. The rest follows, since regular submodules are always orthogonal summands. □

2.3 Quadratic forms over finite fields.

In this section we will apply Theorem 2.8 to classify the quadratic forms over finite fields. So let $A = \mathbb{F}_{p^n}$ be a finite field of characteristic p and (E, q) be some quadratic A-module. Then the multiplicative group $A^* = A \setminus \{0\}$ is cyclic of order $p^n - 1$, in particular

Remark 2.15. *If $p \neq 2$ then $A = \{0\} \dot\cup (A^*)^2 \dot\cup \epsilon(A^*)^2$ and for $p = 2$ we have $A^* = (A^*)^2$. The modules $E_0 = [0]$, $E_1 = [1]$ and $E_\epsilon = [\epsilon]$ (for $p \neq 2$) represent the isometry classes of one-dimensional quadratic A-modules.*

Remark 2.16. *Now let (E, q) be some regular quadratic A-module of dimension 2. If there is some $0 \neq x \in E$ such that $q(x) = 0$ then $(E, q) \cong \mathbb{H}(\langle x \rangle) \cong \mathbb{H}$ is isometric to a hyperbolic plane. If (E, q) is anisotropic (i.e. $q(x) = 0 \Rightarrow x = 0$), then $q(E) = A$ (such quadratic A-modules are called* **universal***).*

Proof. The first statement is clear. Assume that (E, q) is anisotropic. Since $A^2 = A$ for $p = 2$, we may assume that p is odd. Then E 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 $a \in A$ and put

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

Then $|M_1| = |M_2| = (|A| + 1)/2$ and so $|M_1| + |M_2| = |A| + 1 > |A|$. Therefore $M_1 \cap M_2 \neq \emptyset$ i.e. there are $a_1, a_2 \in A$ such that $a_1^2t_1 = a - a_2^2t_2$ and $a = q(a_1e_1 + a_2e_2)$. □

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

$$q(E \setminus \{0\}) = \{x^{1+p^n} \mid x \in E \setminus \{0\}\} = \langle a^{1+p^n} \rangle = A^* \cong C_{p^n-1}$$

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

Remark 2.17. *Let (E,q) be some regular quadratic A-module of dimension 2. Then either $(E,q) \cong \mathbb{H}$ or $(E,q) \cong N(A)$ so there are exactly 2 isometry classes of 2-dimensional regular quadratic A-modules.*

Proof. We only need to show that any anisotropic quadratic A-module (E,q) of dimension 2 is isometric to $N(A)$. Choose any basis (e_1,e_2) of E such that $q(e_1) = 1$. Then $(E,q) = \begin{bmatrix} 1 & c \\ & a \end{bmatrix}$ and $q(a_1e_1 + a_2e_2) = a_1^2 + ca_1a_2 + aa_2^2$. The polynomial $X^2 + cX + a \in A[X]$ is irreducible (has no zero, since q is anisotropic) it hence defines the unique extension of degree 2 of A. Conclude that $(E,q) \cong N(A)$ as an exercise. □

Remark 2.18. *Let (E,q) be some A-module of dimension ≥ 3. Then there is some $0 \neq x \in E$ such that $q(x) = 0$.*

Proof. We use Theorem 2.8 to write E as an orthogonal sum $E = V \perp W$ with $\dim(V) = 2$ and $\dim(W) = 1$. Then either V contains such a vector x or V is anisotropic, and therefore universal. Then choose $0 \neq w \in W$. Since V is universal, there is some $v \in V$ such that $q(v) = -q(w)$ and then $q(v+w) = 0$. □

Theorem 2.19. *Let (E,q) be some quadratic A-module over the finite field A. Then*

$$(E,q) = V \perp W \perp G$$

with V regular or semi-regular and anisotropic of dimension ≤ 2, W an orthogonal sum of hyperbolic planes and $q(G) = \{0\}$.

Proof. Everything follows from Theorem 2.8 and the above considerations. □

Corollary 2.20. *Let (E,q) be a regular quadratic A-module of dimension $2m$. Then*

$$(E,q) \cong \begin{cases} \bigoplus_{i=1}^m \mathbb{H} & = \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ or} \\ N(A) \oplus \bigoplus_{i=1}^{m-1} \mathbb{H} & = \begin{bmatrix} 1 & a \\ & b \end{bmatrix} \oplus \bigoplus_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{cases}$$

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

Corollary 2.21. *Let (E,q) be a semi-regular quadratic A-module of dimension $2m+1$. Then*

$$(E,q) \cong \begin{cases} [1] \oplus \bigoplus_{i=1}^m \mathbb{H} & = [1] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ or} \\ [\epsilon] \oplus \bigoplus_{i=1}^m \mathbb{H} & = [\epsilon] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{cases}$$

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

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

Let $A = \mathbb{F}_2$, $(V, b) := (\mathbb{F}_2^n, b(c,d) := \sum_{i=1}^n c_i d_i)$ 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 $(V, b) = E \perp\!\!\!\perp \langle \mathbf{1} \rangle$.
- Write $n = 8m + a$ with $m \in \mathbb{N}_0$, $a \in \{1, 2, 3, 4, 5, 6, 7, 8\}$. Then $(E, q) \cong \mathbb{H}(\mathbb{F}_2)^{4m} \perp\!\!\!\perp A$ with

$$A \cong \begin{cases} \{0\} & a = 1 \\ [1] & a = 2 \\ N(\mathbb{F}_2) & a = 3 \\ N(\mathbb{F}_2) \perp\!\!\!\perp [0] & a = 4 \\ \mathbb{H}(\mathbb{F}_2) \perp\!\!\!\perp N(\mathbb{F}_2) & a = 5 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp\!\!\!\perp [1] & a = 6 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp\!\!\!\perp N(\mathbb{F}_2) & a = 7 \\ \mathbb{H}(\mathbb{F}_2)^3 \perp\!\!\!\perp [0] & a = 8 \end{cases}$$

- 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 $E_9 \cong \mathbb{H}(\mathbb{F}_2)^4$.

3 Quadratic forms over principal ideal domains.

Let R be a principal ideal domain with field of fractions K.

Definition 3.1. *Let V be a finite dimensional vector space over K, $n := \dim(V)$. An R-***lattice** *$E \leq V$ is a free R-submodule of V of rank n, so there is some K-basis $(e_1, \ldots, e_n)$ of V that is an R-basis of E, i.e. $E = \bigoplus_{i=1}^n Re_i$. The basis $(e_1, \ldots, e_n)$ is called a* **lattice basis** *of E.*
Let E be some R-lattice in V. An R-submodule $M \leq E$ is called **primitive** *in E, if there is some $N \leq E$ such that $E = M \oplus N$.*

Remark 3.2. *(a) If L and M are R-lattices in V then also $L \cap M$ and $L + M$.*
(b) Let $b : V \times V \to K$ be a non-degenerate symmetric bilinear form and $E \leq V$ an R-lattice with basis $(e_1, \ldots, e_n)$. Then

$$E^\# := \{v \in V \mid b(e, v) \in R \text{ for all } e \in E\}$$

is again a lattice in V with basis $(e_1^\#, \ldots, e_n^\#)$. $E^\#$ is called the **dual lattice** *of E.*

Proof. (a) Exercise.
(b) $E^\# = \{v \in V \mid b(v, \sum_{i=1}^n a_i e_i) \in R \text{ for all } a_1, \ldots, a_n \in R\} = \{v \in V \mid b(v, e_i) \in R \text{ for all } i\}$. By the definition of dual basis we have for any $v \in V$,

$$v = \sum_{i=1}^n b(v, e_i) e_i^\#$$

so $E^\# = \langle e_1^\#, \ldots, e_n^\# \rangle_R$ is the lattice spanned by the dual basis. □

Theorem 3.3. *Let $M \leq E$, E an R-lattice in V. Then M is primitive in E, if and only if E/M has no torsion, if and only if $M = KM \cap E$.*

Proof. By the main theorem on f.g. modules over principal ideal domains, there is some basis $(e_1, \ldots, e_n)$ of E such that $M = \langle d_1 e_1, \ldots, d_m e_m \rangle_R$ with $d_i \in R$, $m \leq n$. Then $E/M = R/(d_1) \oplus \ldots \oplus R/(d_m) \oplus R^{n-m}$ has no torsion $\Leftrightarrow d_i \in R^*$ for all $i \Leftrightarrow M = \langle e_1, \ldots, e_m \rangle$ and $E = M \oplus N$ with $N = \langle e_{m+1}, \ldots, e_n \rangle$. The last equivalence follows since $KM = \{v \in V \mid$ there is some $0 \neq r \in R$ such that $rv \in M\}$, so $KM \cap E/M =$Tors(E/M). □

Corollary 3.4. *If (V, b) is regular, $E \leq V$ a lattice, $X \subset E$, then $X^\perp := \{e \in E \mid b(e, x) = 0 \text{ for all } x \in X\}$ is a primitive submodule of E.*

Proof. (a) submodule: Let $\alpha, \beta \in R, e, f \in X^\perp$, $x \in X$. Then

$$b(x, \alpha e + \beta f) = \alpha b(x, e) + \beta b(x, f) = 0 + 0 = 0$$

so also $\alpha e + \beta f \in X^\perp$.
(b) primitive: Assume that $e \in E$, $0 \neq \alpha \in R$ such that $\alpha e \in X^\perp$. Then for all $x \in X$

$$b(\alpha e, x) = \alpha b(e, x) = 0 \Rightarrow b(e, x) = 0$$

because R is an integral domain. So $e \in X^\perp$. □

Theorem 3.5. *Let (E, b) be some finitely generated free R-module with non degenerated symmetric bilinear form $b : E \times E \to R$. If $F \leq E$ is a primitive submodule then*

$$\det(F, b_{|F}) \det(E, b) = c^2 \det(F^\perp, b_{|F^\perp})$$

for some $c \in R$ with $c \mid \det(E, b)$.

Proof. Consider $G := (E,b) \perp\!\!\!\perp (F,-b_{|F})$. Let $k := \operatorname{rank}(F)$, then $\det(G) = \det(E,b)\det(F,b_{|F})(-1)^k$ and G contains the singular submodule $F' := \{(x,x) \mid x \in F\} \leq E \perp\!\!\!\perp F$. Let $H \leq E$ such that $E = H \oplus F^\perp$. Then

$$G = E \oplus F' = H \oplus F^\perp \oplus F' \text{ with } b(F',F') = \{0\} = b(F',F^\perp)$$

so we get a Gram matrix of G of the form

$$\operatorname{Gram}(G) = \begin{pmatrix} \star & \star & C \\ \star & B & 0 \\ C^{tr} & 0 & 0 \end{pmatrix}$$

where $B = \operatorname{Gram}(F^\perp)$, $C = (b(h_i, f_j'))$, $(h_1,\ldots,h_k)$ basis of H, $(f_1',\ldots,f_k')$ basis of F'. Therefore

$$\det(G) = (-1)^k c^2 \det(F^\perp) \text{ with } c = \det(C)$$

and $\det(E)\det(F) = c^2\det(F^\perp)$.
It remains to show that $c \mid \det(E)$. To see this consider the decomposition $E = J \oplus F = H \oplus F^\perp$ where the complements H and J exist since F and $F^\perp$ are primitive in E. Consider the "mixed" Gram matrix

$$A = \begin{pmatrix} b(H,J) & b(F^\perp,J) \\ b(H,F) & b(F^\perp,F) \end{pmatrix} = \begin{pmatrix} b(H,J) & b(F^\perp,J) \\ C & 0 \end{pmatrix}.$$

Then $c \mid \det(A) = \det(E)u$ for some $u \in R^*$, so also $c \mid \det(E)$. □

Corollary 3.6. *If (E,b) is a regular bilinear R-module, $F \leq E$ primitive then $\det(F) = \det(F^\perp)u$ for some $u \in R^*$.*

Example: $(E,b) = \mathbb{I}_n = \langle 1,\ldots,1\rangle$. $f = e_1 + \ldots + e_n \in \mathbb{I}_n$, $b(f,f) = n = \det(\langle f\rangle)$, so $\mathbb{A}_{n-1} := \langle f\rangle^\perp$ has determinant $\det(\mathbb{A}_{n-1}) = \det(\langle f\rangle) = n$.

Theorem 3.7. *Let (V,b) be a regular bilinear K-vector space of dimension n, $F \leq E \leq V$ two R-lattices in V.*
(a) There are $d_1,\ldots,d_n \in R \setminus \{0\}$ such that $E/F \cong R/(d_1) \oplus \ldots \oplus R/(d_n)$.
(b) $\det(F) = d_1^2 d_2^2 \ldots d_n^2 \det(E)$.
(c) For $R = \mathbb{Z}$ we have $[E:F] = d_1 \cdots d_n$ and $\det(F) = [E:F]^2 \det(E)$.

Proof. By the main theorem on f.g. modules over principal ideal domains there is a basis e of E and elements $d_1,\ldots,d_n \in R$ such that $f := (d_1e_1,\ldots,d_ne_n)$ is a basis of F. For the Gram matrix we hence get ${}_fb_f = \operatorname{diag}(d_1,\ldots,d_n)\ {}_eb_e \operatorname{diag}(d_1,\ldots,d_n)$ so $\det(F) = d_1^2d_2^2\ldots d_n^2\det(E)$. □

Corollary 3.8. *Let E,F be two $\mathbb{Z}$-lattices in the regular bilinear $\mathbb{Q}$-vector space (V,b).*
If there is some sublattice L such that $[E:L] = [F:L]$ then $\det(E) = \det(F)$.
If there is some overlattice L such that $[L:E] = [L:F]$ then $\det(E) = \det(F)$.

Example 3.9. $\mathbb{I}_n > \mathbb{D}_n := \{\sum_{i=1}^n a_ie_i \mid a_i \in \mathbb{Z}, \sum_{i=1}^n a_i \text{ even}\}$. *Then $[\mathbb{I}_n : \mathbb{D}_n] = 2$ so $\det(\mathbb{D}_n) = 4$. If n is even, then $2(\frac{1}{2}\sum_{i=1}^n e_i) \in \mathbb{D}_n$, so*

$$\tilde{\mathbb{D}}_n := \langle \mathbb{D}_n, \frac{1}{2}\sum_{i=1}^n e_i\rangle$$

contains $\mathbb{D}_n$ *as a sublattice of index 2. Therefore* $\det(\tilde{\mathbb{D}}_n) = \det(\mathbb{I}_n) = 1$.
If $n \equiv 0 \pmod 4$, *then* $b(\tilde{\mathbb{D}}_n, \tilde{\mathbb{D}}_n) \subseteq \mathbb{Z}$.
If $n \equiv 0 \pmod 8$, *then* $Q_b(\tilde{\mathbb{D}}_n) \subseteq \mathbb{Z}$ *where* $Q_b(x) := \frac{1}{2}b(x,x)$.
Define $\mathbb{E}_8 := \tilde{\mathbb{D}}_8$, *so* $(\mathbb{E}_8, Q_b)$ *is a regular quadratic* $\mathbb{Z}$*-module.*

$$\mathbb{E}_7 := \{\sum_{i=1}^{8} a_i e_i \in \mathbb{E}_8 \mid a_7 = a_8\} = \{x \in \mathbb{E}_8 \mid b(x, e_7 - e_8) = 0\},\ \textit{so}\ \det(\mathbb{E}_7) = 2$$

$$\mathbb{E}_6 := \{\sum_{i=1}^{8} a_i e_i \in \mathbb{E}_8 \mid a_6 = a_7 = a_8\} = \langle e_6 - e_7, e_7 - e_8\rangle^{\perp},\ \textit{so}\ \det(\mathbb{E}_6) = 3$$

4 Orthogonal groups and Witt's theorem.

4.1 The orthogonal group.

Definition 4.1. *Let* (E,q) *be a quadratic* A*-module. Then*

$$O(E) := O(E,q) := \{\varphi : E \to E \mid \varphi \textit{ is an } A\textit{-module automorphism}, q(\varphi(x)) = q(x) \text{ for all } x \in E\}$$

is called the **orthogonal group** *of* (E,q).

Clear: $g \in O(E) \Rightarrow b_q(g(x), g(y)) = b_q(x,y)$ for all $x, y \in E$.

Example 4.2. *(reflections as orthogonal transformations): Let* (E,q) *be a quadratic* A*-module and* $e \in E$ *such that* $q(e) \in A^*$. *Then*

$$s_e : E \to E, s_e(x) = x - b_q(x,e)q(e)^{-1}e$$

is called the **reflection** *along* e. *We have*

(a) $s_e^2 = \mathrm{id}_E$

(b) $s_e(e) = -e$, $s_e(x) = x$ *if* $b_q(e,x) = 0$.

(c) $s_e \in O(E,q)$, *because for* $x \in E$

$$\begin{array}{l} q(s_e(x)) = q(x - b_q(x,e)q(e)^{-1}e) = \\ q(x) - b_q(x, b_q(x,e)q(e)^{-1}e) + b_q(x,e)^2 q(e)^{-2} q(e) = \\ q(x) - b_q(x,e)^2 q(e)^{-1} + b_q(x,e)^2 q(e)^{-1} = q(x) \end{array}$$

(d) For any $g \in O(E,q)$ *we compute* $g s_e g^{-1} = s_{g(e)}$.
$(g s_e g^{-1})(x) = g(s_e(g^{-1}(x))) = g(g^{-1}(x) - b_q(g^{-1}(x), e)q(e)^{-1}e) = x - b_q(x, g(e))q(g(e))^{-1}g(e)$
for all $x \in E$ *where we used the fact that* $b_q(g^{-1}(x), e) = b_q(x, g(e))$ *applying the orthogonal transformation* g *to both vectors.*

(e) $S(E,q) := \langle s_e \mid e \in E, q(e) \in A^*\rangle \trianglelefteq O(E,q)$ *is called the* **reflection subgroup** *of* $O(E,q)$. *By (d) this is a normal subgroup of the orthogonal group.*

(f) If $2 \in A^*$ *then we may write* $E = Ae \perp (Ae)^{\perp}$ *and* $s_e = -\mathrm{id}_{Ae} \perp \mathrm{id}_{(Ae)^{\perp}}$ *is the reflection at the hyperplane* $(Ae)^{\perp}$.

Example 4.3. *$S(\mathbb{A}_{n-1}) \cong S_n$ and $O(\mathbb{A}_{n-1}) = \langle -id, S(A_{n-1})\rangle \cong C_2 \times S_n$.*
Recall that $\mathbb{A}_{n-1} = \{\sum_{i=1}^n x_i e_i \in \mathbb{I}_n \mid \sum_{i=1}^n x_i = 0\}$. From this we find that $\{x \in \mathbb{A}_{n-1} \mid q(x) \in \mathbb{Z}^* = \{\pm 1\}\} = \{e_i - e_j \mid i \neq j\}$. To get the isomorphism $S(\mathbb{A}_{n-1}) \cong S_n$ we consider the action of $s_{e_i - e_j}$ (for $i \neq j$) on $(e_1, \ldots, e_n)$:

$$s_{e_i-e_j}(e_k) = e_k - (\delta_{ik} - \delta_{jk})(e_i - e_j) = \begin{cases} e_k & k \notin \{i,j\} \\ e_i & k = j \\ e_j & k = i \end{cases} = e_{\sigma_{ij}(k)}$$

where $\sigma_{ij} = (i,j) \in S_n$.

4.2 Witt's theorem for fields of characteristic $\neq 2$.

Theorem 4.4. *(Witt's extension theorem)*
Let A be a field of characteristic $\neq 2$ and (E,q) a finite dimensional quadratic A-vector space. Let $F \leq E$ be some regular subspace and $\varphi : F \to E$ an isometric embedding. Then there is some $g \in O(E,q)$ such that $g_{|F} = \varphi$. This g can be constructed as a product of at most $2\dim(F)$ reflections. In particular if (E,q) is regular, then $O(E,q) = S(E,q)$ and any orthogonal transformation is a product of at most $2\dim(E)$ reflections.

Proof. We use induction on the dimension of F.
$\dim(F) = 1$: Then $F = Af_1$ with $q(f_1) \neq 0$ (since F is regular). Let $f_2 := \varphi(f_1)$. Then

$$q(f_1 - f_2) + q(f_1 + f_2) = 2(q(f_1) + q(f_2)) = 4q(f_1) \neq 0.$$

(a) If $q(f_1 - f_2) \neq 0$ then put $e := f_1 - f_2$. We compute

$$s_e(f_1) = f_1 - b_q(f_1, f_1 - f_2)q(f_1 - f_2)^{-1}(f_1 - f_2) = f_1 - \frac{2q(f_1) - b_q(f_1, f_2)}{q(f_1) + q(f_2) - b_q(f_1, f_2)}(f_1 - f_2) = f_2.$$

(b) If $q(f_1 + f_2) \neq 0$ then put $e := f_1 + f_2$. As before we compute $s_e(f_1) = -f_2$ so $g := s_{f_2} \circ s_e \in S(E,q)$ maps f_1 to f_2.
$\dim(F) = n > 1$: Then $F = Af_1 \perp \ldots \perp Af_n$ with $q(f_i) \neq 0$ for all i. By assumption there is some $g \in O(E,q)$ such that $\varphi(f_i) = g(f_i)$ for all $1 \leq i \leq n-1$ and g is a product of at most $2(n-1)$ reflections. Replacing φ by $\varphi_1 := g^{-1} \circ \varphi$ we achieve that $\varphi_1(f_i) = f_i$ for all $1 \leq i \leq n-1$. Then $\varphi_1(f_n) =: f_n'$ satisfies $f_n' \perp f_i$ for all $1 \leq i \leq n-1$. As in the case $\dim(F) = 1$ we find that either $q(f_n - f_n') \neq 0$ and put $g_1 := s_{f_n - f_n'}$ or $q(f_n + f_n') \neq 0$ and put $g_1 := s_{f_n'} \circ s_{f_n + f_n'}$ to construct an orthogonal transformation g_1 of E with $g_1(f_i) = f_i$ for all $1 \leq i \leq n-1$ and $g_1(f_n) = f_n'$. Then $g \circ g_1 \in S(E,q)$ has the desired properties. □

Corollary 4.5. *(Witt's cancellation theorem)*
Let A be a field of characteristic $\neq 2$, F, G_1, G_2 quadratic spaces over A, F regular. Then $F \perp G_1 \cong F \perp G_2 \Leftrightarrow G_1 \cong G_2$.

Proof. Let $\psi : F \perp G_1 \to F \perp G_2 =: E$ 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 4.4 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 4.6. *For $p \neq 2$ the two quadratic modules $\bigoplus^{m-1} \mathbb{H} \bigoplus N(A)$ and $\bigoplus^m \mathbb{H}$ of Theorem 2.20 are not isometric. Otherwise $N(A) \cong \mathbb{H}$ but $N(A)$ is anisotropic.*

Example 4.7. *Let $A = \mathbb{F}_2$, $E = A^3$, $b(x,y) = x_1y_1 + x_2y_2 + x_3y_3$. $F_1 := \langle (1,0,0) \rangle$, $F_2 := \langle (1,1,1) \rangle$. Then $F_1 \cong F_2$ but*

$$F_1^\perp = \langle (0,1,0), (0,0,1) \rangle : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$F_2^\perp = \langle (1,1,0), (0,1,1) \rangle : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

do not satisfy $F_1^\perp \cong F_2^\perp$ (because $b(x,x) = 0$ for all $x \in F_2^\perp$.) So

$$E = F_1 \bigoplus F_1^\perp = F_2 \bigoplus F_2^\perp, F_1 \cong F_2 \text{ but } F_1^\perp \ncong F_2^\perp$$

in particular Witt's cancellation theorem does not hold for bilinear spaces over fields of characteristic 2.

Example 4.8. *This example shows that it is necessary to assume that F is regular: Let A be an arbitrary field, $E = Ae_1 \bigoplus Ae_2 \bigoplus Ae_3 = [1,-1,0]$ with $q(e_1) = 1$, $q(e_2) = -1$, $q(e_3) = 0$. Then $F_1 := A(e_1 + e_2)$ and $F_2 = Ae_3$ are isometric as $q(e_1 + e_2) = q(e_3) = 0$, but $E^\perp = F_2$ and $F_1 \not\subseteq E^\perp$, so the isometry $F_1 \to F_2, (e_1 + e_2) \mapsto e_3$ cannot be extended to some orthogonal transformation of E.*

4.3 Witt's theorem for arbitrary fields.

Theorem 4.9. *(Witt's extension theorem)*
Let (E,q) be a finite dimensional quadratic A-vector space over some field A. Let $F_1, F_2 \leq E$ be sharply primitive subspaces and $\varphi : F_1 \to F_2$ a bijective isometry. Then there is some $g \in O(E,q)$ such that $g_{|F_1} = \varphi$.

The proof will be given in more generality (for local rings) in Section 4.5. Here we will first state some consequences:

With the same proof as Corollary 4.5 we conclude from Theorem 4.9 Witt's cancellation theorem for arbitrary fields.

Corollary 4.10. *(Witt's cancellation theorem)*
Let F, G_1, G_2 be quadratic spaces over the field A such that F is regular. Then $F \bigoplus G_1 \cong F \bigoplus G_2 \Leftrightarrow G_1 \cong G_2$.

Corollary 4.11. *Let A be a field and (E,q) a finite dimensional quadratic A-vectorspace.*

(a) If $F_1, F_2 \leq E$ are singular and sharply primitive with $\dim(F_1) = \dim(F_2)$ then there is some $g \in O(E,q)$ such that $g(F_1) = F_2$.

(b) Any two maximal singular sharply primitive subspaces F_1, F_2 have the same dimension.

(c) $\mathrm{ind}(E,q) :=$ the dimension of a maximal singular sharply primitive subspace is called the **Witt index** *of (E,q).*

Proof. Singular subspaces satisfy $q(F_1) = q(F_2) = \{0\}$, so they are isometric, if and only if they are isomorphic. To see (a) choose any isomorphism $\varphi : F_1 \to F_2$. As this is an isometry Theorem 4.9 tells us that there is some $g \in O(E,q)$ such that $g_{|F_1} = \varphi$, in particular $g(F_1) = F_2$.
For (b) take two maximal singular sharply primitive subspaces and assume that $\dim(F_1) > \dim(F_2)$. Let F_1' be some subspace of F_1 such that $\dim(F_1') = \dim(F_2)$. Then also F_1' is sharply primitive and singular, so by (a) there is some orthogonal transformation $g \in O(E,q)$ such that $g(F_1') = F_2$. But then $g(F_1) > F_2$ is sharply primitive singular subspace that properly contains F_2 which contradicts the maximality of F_2. □

Corollary 4.12. *Let A be a finite field and consider the quadratic spaces of Theorem 2.20.* $\operatorname{ind}(\bigoplus^{m-1} \mathbb{H} \oplus N(A)) = m-1$ *and* $\operatorname{ind}(\bigoplus^{m} \mathbb{H}) = m$, *in particular the two quadratic modules are not isometric.*

Corollary 4.13. *Let (E,q) be a quadratic vector space over the field A of Witt index n. Then $(E,q) \cong (F, q_{|F}) \oplus \mathbb{H}(A^n)$ with* $\operatorname{ind}(F, q_{|F}) = 0$. *If (E,q) is regular, then $(F, q_{|F})$ is anisotropic and uniquely determined up to isometry. Then $(F, q_{|F})$ is called the* **anisotropic kernel** *of (E,q).*

4.4 Orthogonal groups over finite fields.

Let $A = \mathbb{F}_\ell$, $\ell = p^f$, (E,q) regular or semi-regular quadratic space over A. By Section 2.3 we have two possibilities for even dimension $\dim(E) = 2m$:

$$\begin{aligned} (E,q_+) &\cong \bigoplus_{i=1}^m \mathbb{H} &&= \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ or} \\ (E,q_-) &\cong N(A) \oplus \bigoplus_{i=1}^{m-1} \mathbb{H} &&= \begin{bmatrix} 1 & a \\ & b \end{bmatrix} \oplus \bigoplus_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{aligned}$$

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

$$\begin{aligned} (E,q_1) := \; & [1] \oplus \bigoplus_{i=1}^m \mathbb{H} &&= [1] \oplus \bigoplus_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \text{ or} \\ (E,q_\epsilon) := \; & [\epsilon] \oplus \bigoplus_{i=1}^m \mathbb{H} &&= [\epsilon] \oplus \bigoplus_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \end{aligned}$$

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

Since $(E,q_1) \cong (E, \epsilon q_\epsilon)$ these two quadratic modules have isomorphic orthogonal groups.

Lemma 4.14. *Let $s(E,q) := |\{x \in E \mid q(x) = 0$ and $\langle x \rangle$ sharply primitive $\}|$. Then*

$$\begin{array}{lll} s(E,q_+) = & (\ell^m - 1)(\ell^{m-1} + 1) & \dim(E) = 2m \\ s(E,q_-) = & (\ell^m + 1)(\ell^{m-1} - 1) & \dim(E) = 2m \\ s(E,q_1) = s(E,q_\epsilon) = & \ell^{2m} - 1 = (\ell^m - 1)(\ell^m + 1) & \dim(E) = 2m+1 \end{array}$$

Proof. The formulas are true for $m = 0$ (in the first and last cases) and $m = 1$ in the second case, because $s(0) = 0$, $s(N(A)) = 0$, $s([1]) = s([\epsilon]) = 0$.
We proceed by induction in the four cases. Write $(E,q) = V \oplus H$ with $\dim(V) = n$ and $H = \langle h_1, h_2 \rangle = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$. Let $x = y + z \in E$ with $y \in V$, $z = z_1 h_1 + z_2 h_2 \in H$. Then $q(x) = q(y) + q(z) = q(y) + z_1 z_2$. If x is sharply primitive with $q(x) = 0$ then either

- $y = 0$ and $z_1 z_2 = 0$ $z_1 + z_2 \neq 0$: $\# = 2(\ell - 1)$

- $y \neq 0$, $q(y) = 0$, and $z_1 z_2 = 0$: $\# = s(V)(2\ell - 1)$
- $q(y) \neq 0$, and $z_1 z_2 = -q(y)$: $\# = (\ell^n - s(V) - 1)(\ell - 1)$

So $s(V \bigoplus H) = \ell s(V) + (\ell^n + 1)(\ell - 1)$ so we obtain the following recursion for $a_n := s(V)$:

$$a_{n+2} - \ell^{n+1} + 1 = \ell(a_n - \ell^{n-1} + 1) = \ell^2(a_{n-2} - \ell^{n-3} + 1) = \dots.$$

In the first case $n = 2m$ and we may continue until $a_0 = 0$ to find that

$$a_{2m} - \ell^{2m-1} + 1 = \ell^m(1 - \ell^{-1}) \Rightarrow s(E, q_+) = a_{2m} = \ell^{2m-1} + \ell^m - \ell^{m-1} - 1.$$

In the second case $n = 2m$ and we may continue until $a_2 = 0$ to find that

$$a_{2m} - \ell^{2m-1} + 1 = \ell^{m-1}(1 - \ell) \Rightarrow s(E, q_-) = a_{2m} = \ell^{2m-1} - \ell^m + \ell^{m-1} - 1.$$

In the third case $n = 2m + 1$ and $a_1 = 0$. Then $a_{2m+1} - \ell^{2m} + 1 = 0$ and so $a_{2m+1} = \ell^{2m} - 1$. □

Theorem 4.15. *Let $O_{2m+1}(\mathbb{F}_\ell) := O(E, q_1)$, $O^+_{2m}(\mathbb{F}_\ell) := O(E, q_+)$ and $O^-_{2m}(\mathbb{F}_\ell) := O(E, q_-)$. 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.

Proof. We only prove (a), the other two cases are left as an exercise. Write $(E, q) = H \bigoplus V$ where $H = \langle h_1, h_2 \rangle = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$. Let $U_1 := \mathrm{Stab}_{O(E,q)}(h_1)$, $U_2 := \mathrm{Stab}_{U_1}(h_2)$. Then

$$|O(E, q)| = |O(E, q)h_1| \cdot |U_1| = |O(E, q)h_1| \cdot |U_1 h_2||U_2|.$$

By Theorem 4.4 $U_2 = O(V) \cong O^+_{2(m-2)}(\mathbb{F}_\ell)$ and $|O(E, q)h_1| = s(E, q)$. To compute $|U_1 h_2|$ let $u \in U_1$. Then $u(h_1) = h_1$ and $u(h_2) = h$ with $q(h) = 0$ and $b_q(h_1, h) = 1$. So $h = h_2 + ah_1 + v$ with $a \in \mathbb{F}_\ell$, $v \in V$, $q(h) = a + q(v) = 0$, so $a = -q(v)$. Therefore

$$Uh_2 = \{h_2 - q(v)h_1 + v \mid v \in V\} \text{ and } |Uh_2| = |V|$$

and we find

$$|O^+_{2m}(\mathbb{F}_\ell)| = (\ell^m - 1)(\ell^{m-1} + 1)\ell^{2m-2}|O^+_{2m-2}(\mathbb{F}_\ell)| = \prod_{j=1}^{m}(\ell^j - 1)(\ell^{j-1} + 1)\ell^{2j-2}.$$

□

4.5 Witt's theorem for local rings*.

Let A be a local ring and $I \trianglelefteq A$ be the unique maximal ideal of A. Then $A^* = A \setminus I$, so an element of A is either contained in I or a unit. Examples for local rings are of course fields but also

$$\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\}$$

for any prime p. Any projective module over a local ring is free.

Theorem 4.16. *Let (E, b) be a free finitely generated A module with symmetric bilinear form b. Then there is a decomposition*

$$E = E_1 \perp \ldots \perp E_r \perp F$$

with regular submodules $E_i \leq E$ of rank 1 or 2 and a module F with $b(F, F) \subset I$. E is regular if and only if $F = \{0\}$.

Proof. As an exercise, following the proof of Theorem 1.15. □

Note that we cannot expect something analogous to Theorem 2.8 for arbitrary local rings: Let $a \in I$. Then free quadratic A-module

$$(E, q) = \begin{bmatrix} 1 & a \\ & 0 \end{bmatrix}$$

satisfies $q(E) \not\subseteq I$ and $b_q(E, E) \subseteq I$ but (E, q) is not the orthogonal sum of 1-dimensional quadratic A-modules if $a \notin 2A$.

Theorem 4.17. *Let (E, q) be regular quadratic A-module over a local ring A. If $2 \in A^*$ then (E, q) has an orthogonal basis.*
If $2 \notin A^*$, then (E, q) is the orthogonal sum of 2-dimensional regular submodules.
Any semi-regular quadratic module is the orthogonal sum of a semi-regular quadratic module of dimension 1 and a regular quadratic module.

Proof. As an exercise, following the proof of Theorem 2.8. □

Theorem 4.18. *Let (E, q) be a quadratic module over a local ring A, $F, G, H \leq E$ so that F, G free of finite rank and*

$$(1) \quad b_F(H) = F^*, b_G(H) = G^*$$

Let $t : F \to G$ be a bijective isometry such that

$$(2) \quad tx \equiv x \pmod{H} \text{ for all } x \in F.$$

Then there is an orthogonal transformation $u \in O(E, q)$ such that

$$u_{|F} = t, ux \equiv x \pmod{H} \text{ for all } x \in E, ux = x \text{ for all } x \in H^\perp.$$

In the special case $E = H$ we obtain Witt's extension theorem for local rings and hence all its corollaries from Section 4.3

Corollary 4.19. *(Witt's theorem for local rings) If F, G are sharply primitive free submodules of the quadratic A-module (E, q) and $t : F \to G$ an isometry, then there is $u \in O(E, q)$ such that $u_{|F} = t$.*

For the proof of Theorem 4.18 we aim to construct u as a product of reflections s_h with $h \in H$ (which is only possible under additional conditions). Then $u_{|H^\perp} = \mathrm{id}$ is automatically satisfied. To find enough reflections we need additional assumptions. Put $\overline{A} = A/I$, $\overline{H} = H/IH$. If $C \subseteq H$ then we put

$$\overline{C}^\perp := \{x \in \overline{H} \mid \overline{b}(x, \overline{c}) = 0 \text{ for all } c \in C\}$$

Lemma 4.20. *Under the assumptions of Theorem 4.18 suppose that either*

$$(3)\quad \overline{A} \ncong \mathbb{F}_2 \text{ and } \overline{q}(\overline{H}) \neq \{0\} \qquad \text{or}$$
$$(4)\quad \overline{A} \cong \mathbb{F}_2 \text{ and } \overline{q}(\overline{H}^{\perp}) \neq \{0\}$$

Then there is such an $u \in O(E,q)$ as in Theorem 4.18 that is a product of reflections s_h with $h \in H$.

Proof. We proceed by induction on $\operatorname{rank}(F) = \operatorname{rank}(G) =: r$, where the hardest case is the one for $r = 1$.
$r = 1$: Then $F = Af$, $G = Ag$ with $g = tf = f + h$ with $h \in H$ and $q(g) = q(f) + q(h) + b_q(f,h) = q(f)$. If $q(h) \in A^*$, then $s_h(f) = g$ and hence $u = s_h$ is such an extension.
Otherwise

$$(5)\quad q(h) = -b_q(f,h) = b_q(g,h) \in I.$$

We want to find a reflection s_e so that $s_e(f)$ is transformed into g by one more reflection. Write $g = s_e(f) + d$, so

$$d = b_q(f,e)q(e)^{-1}e + h \text{ and } q(d) = b(f,e)b(g,e)q(e)^{-1} + q(h).$$

If $q(e)$ and $q(d)$ are invertible, then $s_d(s_e(f))) = g$ and $s_d \circ s_e$ is the desired extension of t. So we need to find some $e \in H$ such that

$$q(e) \notin I, b(f,e) \notin I, b(g,e) \notin I.$$

For $x \in \{g,f\}$ let $\overline{H_x} := \{\overline{h} \in \overline{H} \mid b(x,h) \in I\}$. Because of condition (1) both subspaces have co-dimension 1 in $\overline{H}$ and we need to show that

$$\overline{q}(\overline{H} \setminus (\overline{H}_f \cup \overline{H}_g)) \neq \{0\}.$$

Put $M := \overline{H} \setminus (\overline{H}_f \cup \overline{H}_g)$. If $\overline{q}(M) = \{0\}$ then choose $\overline{x} \in \overline{H}_f \cap \overline{H}_g$ and $\overline{y} \in M$. Then for all $\overline{a} \in \overline{A}$ we get $\overline{ax} + \overline{y} \in M$ so

$$\overline{q}(\overline{ax} + \overline{y}) = \overline{a}^2\overline{q}(\overline{x}) + \overline{a}\overline{b}(\overline{x},\overline{y}) + \overline{q}(\overline{y}) = 0$$

If $\overline{A}$ contains at least 3 elements, then this implies that

$$(6)\ \overline{q}(\overline{x}) = \overline{b}(\overline{x},\overline{y}) = \overline{q}(\overline{y}) = 0.$$

Equation (5) shows that we may take $\overline{x} = \overline{h}$ and conclude that $\overline{b}(\overline{h}, M) = 0$. As M generates $\overline{H}$ we even obtain $\overline{b}(\overline{h}, \overline{H}) = 0$. Since $g = f + h$ we get $\overline{H}_g = \overline{H}_f$ and any vector of $\overline{H}$ is either in $M = \overline{H} \setminus \overline{H}_f$ or in $\overline{H}_f$. Then (6) reads as $\overline{q}(\overline{H}) = 0$ contradicting the assumption (3).
If $\overline{A} = \mathbb{F}_2$ then we obtain (6) for all $\overline{x}, \overline{y} \in \overline{H}^{\perp}$. Clearly $\overline{H}^{\perp} \cap \overline{H}_f = \overline{H}^{\perp} \cap \overline{H}_g$ and again any vector of $\overline{H}^{\perp}$ is either in $\overline{H}^{\perp} \setminus \overline{H}_f$ or in $\overline{H}^{\perp} \cap \overline{H}_f$, so again by (6) we obtain $\overline{q}(\overline{H}^{\perp}) = 0$ contradicting the assumption (4).
$r > 1$: Now assume that $r > 1$ and let $(f_1, \ldots, f_r)$ be an A-basis of F. By induction hypothesis we get some product of reflections s_h with $h \in H$ mapping f_i to $t(f_i)$ for $i = 1, \ldots, r-1$. Multiplying t by this product we may hence assume that

$$(7)\ t(f_i) = f_i \text{ for } i = 1, \ldots, r-1.$$

By assumption (1) there are $h_1, \ldots, h_r \in H$ such that $b(f_i, h_j) = \delta_{ij}$ and

$$H = \bigoplus_{i=1}^{r} Ah_i \oplus D \text{ where } D = F^{\perp} \cap H.$$

Put $\tilde{H} := Ah_r + D$. Then by (7) we have $tx - x \in \tilde{H}$ for all $x \in F$. Since $s_h(f_i) = f_i$ for all $i = 1, \dots, r-1$ and $h \in \tilde{H}$ it is enough to apply the case $r = 1$ for Af_r instead of F and $\tilde{H}$ instead of H to conclude the proof of the Lemma. So we need to check conditions (1)-(4) for Af_r and $\tilde{H}$. (1) is true, since $h_r \in \tilde{H}$. (2) has been shown above. For a suitable choice of the $f_1, \dots, f_r$ we may achieve (3) resp. (4). By assumption there is some $\overline{h} \in \overline{H}$ (resp. $\overline{H}^\perp$) such that $\overline{q}(\overline{h}) \neq 0$. We choose $\overline{h}_r \in \overline{H} \setminus \overline{D}$ such that $\overline{h} \in \overline{A}\overline{h}_r + \overline{D}$ and then extend $\overline{h}_r$ to a basis $(\overline{h}_1, \dots, \overline{h}_r)$ of $\overline{H}/\overline{D}$. Representatives h_i of the $\overline{h}_i$ then form an A-basis of H/D, the dual basis is then a basis of F for which $\tilde{H}$ has all necessary properties. □

Proof. (of Theorem 4.18) The idea is to replace E by some space $\tilde{E}$ so that the conditions (3) or (4) are satisfied and then use Lemma 4.20. Let $\mathbb{H}(A) = Ae \oplus Af$ with $q(ae + a'f) = aa'$ and put

$$\tilde{E} = E \perp\!\!\!\oplus \mathbb{H}(A), \tilde{F} := F \perp\!\!\!\oplus Ae,\ \tilde{G} := G \perp\!\!\!\oplus Ae, \tilde{H} := H \perp\!\!\!\oplus A(e+f), \tilde{t} = t \perp\!\!\!\oplus \mathrm{id}_{Ae}.$$

As $q(e+f) = 1$ (and $\overline{e+f} \in \overline{H}^\perp$ if $\overline{A} = \mathbb{F}_2$) we may apply Lemma 4.20 to this new situation to find some $\tilde{u} \in O(\tilde{E})$ as a product of reflections along elements of $\tilde{H}$. As $b(\tilde{H}, e-f) = 0$ we compute $\tilde{u}(e) = \tilde{t}(e) = e$ and $\tilde{u}(e-f) = e - f$, so $\tilde{u} = u \perp\!\!\!\oplus \mathrm{id}_{\mathbb{H}(A)}$ with $u \in O(E, q)$ as requested. □

4.6 Witt's theorem for $\mathbb{Z}$-lattices.

Let (V, b) be a non-degenerate bilinear $\mathbb{Q}$-vector space. We call (V, b) **positive definite**, if $b(x, x) > 0$ for all $x \in V$, $x \neq 0$, i.e. if $(V \otimes \mathbb{R}, b)$ is a Euclidean vector space.

Definition 4.21.

- *A $\mathbb{Z}$-lattice L in (V, b) is called* **positive definite**, *if (V, b) is positive definite.*
- *A $\mathbb{Z}$-lattice L in (V, b) is called* **unimodular**, *if $L^\# = L$, so if (L, b) is a regular bilinear $\mathbb{Z}$-module.*
- *L is called* **even**, *if $b(\ell, \ell) \in 2\mathbb{Z}$ for all $\ell \in L$. Then $q : L \to \mathbb{Z}, q(\ell) := \frac{1}{2}b(\ell, \ell)$ defines an integral quadratic form on L with $b_q = b$.*
- *L is called* **orthogonally indecomposable**, *if $L = L_1 \perp\!\!\!\oplus L_2$ implies that either $L_1 = \{0\}$ or $L_2 = \{0\}$.*

Clear: Even unimodular lattices are the regular quadratic $\mathbb{Z}$-modules.
$\mathbb{H}(\mathbb{Z})$ is an even unimodular lattice.
$\mathbb{E}_8$ is also an even unimodular lattice, as well as $\tilde{\mathbb{D}}_{8n}$

Theorem 4.22. *Let (L, b) be a positive definite $\mathbb{Z}$-lattice. Then for any $a \in \mathbb{Z}$ the set $L_{\leq a} := \{\ell \in L \mid b(\ell, \ell) \leq a\}$ is finite.*

Proof. For the proof we give an algorithm to compute $L_{\leq a}$ using the Gram Schmidt orthogonalisation process:
Let $(b_1, \dots, b_n)$ be a $\mathbb{Z}$-basis of L.
For $i = 1, \dots, n$ compute the projection b_i' of b_i onto $\langle b_1, \dots, b_{i-1}\rangle_{\mathbb{Q}}^\perp = \langle b_1', \dots, b_{i-1}'\rangle_{\mathbb{Q}}^\perp$.

$$b_i' := b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j' \text{ with } \mu_{ij} = \frac{b(b_i, b_j')}{b(b_j', b_j')}.$$

Then $B' := (b'_1, \ldots, b'_n)$ is an orthogonal basis of (V, b) with $\langle b_1, \ldots, b_i\rangle_{\mathbb{Q}} = \langle b'_1, \ldots, b'_i\rangle_{\mathbb{Q}}$ for all i.
Let $\ell := \sum_{i=1}^n a_i b_i \in L_{\leq a}$. Then $\ell = \sum_{j=1}^n \alpha_j b'_j$ with $\alpha_j \in \mathbb{Q}$,
$\alpha_n = a_n$, $\alpha_{n-1} = a_{n-1} - \mu_{n,n-1}a_n$, ...

$$b(\ell, \ell) = \sum_{j=1}^{n} \alpha_j^2 (b'_j, b'_j) \leq a$$

yields that $a_n^2 b(b'_n, b'_n) \leq a$. So we only have finitely many possibilities for $a_n \in \mathbb{Z}$. In general

$$\alpha_j^2(b'_j, b'_j) = (a_j - \sum_{i=j+1}^{n} \mu_{i,j} a_i)^2 (b'_j, b'_j) \leq S - \sum_{i=j+1}^{n} \alpha_i^2 (b'_i, b'_i)$$

whence one gets only finitely many possibilities for $a_j \in \mathbb{Z}$, $j = n, n-1, \ldots, 1$. □

Corollary 4.23. *(L, q) positive definite $\mathbb{Z}$-lattice $\Rightarrow$*

$$O(L, q) := \{g \in \mathrm{GL}(L) \mid q(g(x)) = q(x) \text{ for all } x \in L\}$$

is a finite subgroup of $\mathrm{GL}(L) \cong \mathrm{GL}_n(\mathbb{Z})$.

Proof. Let $(e_1, \ldots, e_n)$ be a basis of L and $a := \max\{q(e_i) \mid 1 \leq i \leq n\}$. Then for any $g \in O(L, q)$ we have $q(g(e_i)) = q(e_i)$ hence the candidates of the images $g(e_i)$ lie in the finite set $M := \{\ell \in L \mid q(\ell) \leq a\}$. As g is uniquely determined by $g(e_1), \ldots, g(e_n)$ we get $|O(L, q)| \leq |M|^n$.
□

Theorem 4.24. *(Kneser) Every $\mathbb{Z}$-lattice L in the positive definite bilinear $\mathbb{Q}$-space (V, b) can be written uniquely as an orthogonal sum of indecomposable sublattices.*

Proof. We start the algorithm with a small definition: We call a vector $x \in L$ **indecomposable**, if there are no $y, z \in L \setminus \{0\}$ for which $x = y + z$ and $b(y, z) = 0$.
Then any vector $0 \neq x \in L$ is sum of indecomposable vectors:
This is clear if x is indecomposable. Otherwise $x = y + z$ with $b(x, x) = b(y, y) + b(z, z)$ so $0 < b(y, y) < b(x, x)$ and $0 < b(z, z) < b(x, x)$. If one of the summands y or z is not indecomposable, then one can write it as sum of vectors of smaller norm. By Theorem 4.22 the set $L_{\leq b(x,x)}$ is finite, so this method constructs x as a sum of indecomposable vectors after finitely many steps.
In particular, L is generated by indecomposable vectors (but there are usually infinitely many indecomposable vectors in L). Let $\mathcal{I} := \{x \in L \mid x \text{ is indecomposable }\}$
We introduce an equivalence relation on $\mathcal{I}$: Two indecomposable vectors $x, y \in \mathcal{I}$ are called **connected**, if there are indecomposable vectors $x_0 = y, x_1, \ldots, x_t = z$ in $\mathcal{I}$ such that $(x_i, x_{i+1}) \neq 0$ for all i. This relation partitions $\mathcal{I}$ into finitely many classes $K_1, \ldots, K_s$.
Let $L_i := \langle K_i\rangle_{\mathbb{Z}}$.
Then $L = L_1 \perp \ldots \perp L_s$ is the unique decomposition of L into indecomposable sublattices. □

Examples:

- For $\mathbb{I}_n = \perp^n \langle 1\rangle$ the orthogonally indecomposable summands are the sublattices $\mathbb{Z}e_i$.
- The lattice $\mathbb{A}_n$ is indecomposable.
  Because $\mathbb{A}_n$ is an even lattice, so $(\mathbb{A}_n)_{<2} = \{0\}$ and the vectore $e_{ij} = e_i - e_j \in (\mathbb{A}_n)_{=2}$ are indecomposable. As $b(e_{1j}, e_{1k}) > 0$ for all j, k these ly in one connected component. But these vectors generate the space (they even generate the lattice $\mathbb{A}_n$), so $\mathbb{A}_n$ is indecomposable.

- The lattice $\mathbb{D}_n$ is indecomposable if $n \geq 3$, $\mathbb{D}_2 = \langle e_1 + e_2 \rangle \perp \langle e_1 - e_2 \rangle$. (Exercise)
- For $n \in 4\mathbb{Z}$ the lattice $\tilde{D}_n$ is indecomposable if $n > 4$. We have $\tilde{D}_4 \cong \mathbb{I}_4$. (Exercise).
- $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$ are indecomposable.

Corollary 4.25. *If L, M, N are positive definite $\mathbb{Z}$-lattices with $L \perp M \cong L \perp N$, then $M \cong N$.*

So Witt's theorem holds for positive definite $\mathbb{Z}$-lattices, but

Remark 4.26. *Witt's 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 $\mathbb{E}_8 \perp \mathbb{E}_8$ 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. Using Theorem 4.24 we see that these two modules are not isometric, but

$$(E, q) \perp \mathbb{H}(\mathbb{Z}) \cong (F, q) \perp \mathbb{H}(\mathbb{Z}).$$

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 $\tilde{\mathbb{D}}_{16} \perp \mathbb{H}(\mathbb{Z})$. 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 $(X \perp L)^\perp$ with the second copy of $\mathbb{E}_8$. □

5 The Witt group.

Definition 5.1. *Two quadratic A-modules E_1, E_2 are called* **Witt-equivalent**, *if there are hyperbolic A-modules H_1 and H_2 such that $E_1 \perp H_1 \cong E_2 \perp H_2$.*

$$W(A) := \{[(E, q)] \mid (E, q) \text{ regular quadratic } A\text{-module } \}$$

is called the **Witt group** *of A.*

Remark 5.2. *$W(A)$ is a commutative group with $[E] + [F] := [E \perp F]$. We have $[\mathbb{H}] = 0$ and $-[(E, q)] = [(E, -q)]$ since $[(E, q) \perp (E, -q)]$ is hyperbolic by Theorem 2.14.*

Remark 5.3. *Assume that A is a principal ideal domain (e.g. a field). Since the rank of any hyperbolic A-module is even we obtain a well defined group homomorphism*

$$e : \ W(A) \to \mathbb{Z}/2\mathbb{Z}, [(E, q)] \mapsto \ \mathit{rank}(E) + 2\mathbb{Z}.$$

Let $W_1(A) := \ker(e)$. Then $W(A)/W_1(A) \cong \mathbb{Z}/2\mathbb{Z}$ if $2 \in A^*$ and $W(A) = W_1(A)$ if $2 \notin A^*$.

Remark 5.4. *Let A be a field or more generally a local ring. Then by Witt's theorem, any regular quadratic A-module (E, q) decomposes uniquely (up to isometry) as $E = F \perp G$ with G hyperbolic and F anisotropic ($\mathrm{ind}(F) = 0$). Then $[E] = [F] \in W(A)$. So every class in $W(A)$ has a unique (up to isometry) anisotropic representative.*

Example 5.5. *If A is an algebraically closed field then $W_1(A) = 0$, so $W(A) \cong \mathbb{Z}/2\mathbb{Z}$ if $\mathrm{char}(A) \neq 2$ and $W(A) = 0$ if $\mathrm{char}(A) = 2$. In particular $e : W(\mathbb{C}) \to \mathbb{Z}/2\mathbb{Z}$ is an isomorphism.*
(Show as an exercise that any regular quadratic space of dimension ≥ 2 over an algebraically closed field contains a sharply primitive singular vector.)

Example 5.6. *The Witt group of $\mathbb{R}$: Recall Sylvester's theorem: Any regular quadratic space over $\mathbb{R}$ is equivalent to $\bigoplus^a[1]\bigoplus\bigoplus^b[-1]$. The signature of this space is defined as $a-b$. As $[1]\bigoplus[-1]=\mathbb{H}$ the signature gives a group isomorphism $W(\mathbb{R})\cong\mathbb{Z}$.*

Definition 5.7. *Let (E,q) be a free quadratic A-module with basis $(e_1,\dots,e_n)$ where $n=2m$ or $n=2m+1$. Then*

$$d(E):=(-1)^m\det(E,q)(A^*)^2$$

is called the **discriminant** *of E.*

Remark 5.8. *$d(\mathbb{H})=1$ and $d(E_1\bigoplus E_2)=d(E_1)d(E_2)$ if $e(E_i)=0$, so $d:W_1(A)\to A^*/(A^*)^2$ is a group homomorphism if A is a principal ideal domain (i.e. all f.g. projective A-modules are free).*

Example 5.9. *The Witt group of a finite field. Let $\ell:=p^f$ be some prime power and $A=\mathbb{F}_\ell$. If $p\neq 2$, then the unique anisotropic quadratic spaces are $[1]$, $[\epsilon]$, $N(A)=(\mathbb{F}_{\ell^2},N)$, so*

$$W(\mathbb{F}_\ell)=\{0,[1],[\epsilon],[N(A)]\}$$

is a group of order 4. It is cyclic, if and only if $[1]\bigoplus[1]$ is anisotropic, so if and only if $\ell\equiv -1 \pmod 4$.
If $p=2$, then all regular quadratic spaces have even dimension and $N(A)$ is the unique anisotropic regular quadratic space. So we have

$$W(\mathbb{F}_\ell)=\begin{cases}\langle[1]\rangle\cong C_4 & \text{if } \ell\equiv -1 \pmod 4\\ \langle[1]\rangle\times\langle[\epsilon]\rangle\cong C_2\times C_2 & \text{if } \ell\equiv 1 \pmod 4\\ \langle[N(\mathbb{F}_\ell)]\rangle\cong C_2 & \text{if } \ell \text{ is even}\end{cases}$$

Note that for $p\neq 2$ the discriminant is a group isomorphism $d:W_1(\mathbb{F}_\ell)\to\mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^2\cong C_2$. So rank mod 2 and discriminant describe the elements in the Witt group. For $p=2$ none of the mappings (e, d) is useful, to distinguish $N(\mathbb{F}_\ell)$ and $\mathbb{H}(\mathbb{F}_\ell)$ we need to interpret the discriminant not in $A^*/(A^*)^2$ but as a polynomial $X^2-d\in A[X]$ defining a separable quadratic extension of A. This will turn up naturally as a certain subalgebra of the Clifford algebra of (E,q), that we will define later.

5.1 The Witt group of finite abelian groups.

Definition 5.10. *Let A be a finite abelian group. A* **symmetric bilinear form** *$b:A\times A\to\mathbb{Q}/\mathbb{Z}$ is a biadditve map such that $b(x,y)=b(y,x)$ for all $x,y\in A$. We then also call (A,b) a* **bilinear group**. *The form b is called* **regular**, *if*

$$b_A:A\to A^*:=\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z}),a\mapsto(x\mapsto b(a,x))$$

is an isomorphism.
A **quadratic form** *is a map $q:A\to\mathbb{Q}/\mathbb{Z}$ such that $q(na)=n^2q(a)$ for all $n\in\mathbb{Z}$ and $b_q:(x,y)\mapsto q(x+y)-q(x)-q(y)$ is a symmetric bilinear form. (A,q) is called a* **quadratic group**. *The form q is called* **regular** *if b_q is regular.*

Example: Every finite dimensional $\mathbb{F}_p$-linear space is a finite abelian group. If (V,q) is a quadratic $\mathbb{F}_p$-module (for some prime p) then the identification $\mathbb{F}_p\cong\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ makes (V,q) to a quadratic abelian group.

Example 5.11. *(discriminantgroup) Let L be an integral $\mathbb{Z}$-lattice in a regular $\mathbb{Q}$-space (V, b). The b defines a regular symmetric bilinear form*

$$\overline{b} : L^{\#}/L \times L^{\#}/L \to \mathbb{Q}/\mathbb{Z}, \overline{b}(x + L, y + L) := b(x, y) + \mathbb{Z}$$

on the discriminant group $(L^{\#}/L, \overline{b})$. If L is even, then we obtain a regular quadratic form

$$q : L^{\#}/L \to \mathbb{Q}/\mathbb{Z}, x + L \mapsto \frac{1}{2}b(x, x) + \mathbb{Z}$$

with $b_q = \overline{b}$.

Lemma 5.12. *Any regular finite bilinear group (A, b) is the orthogonal sum of its Sylow p-subgroups, $(A, b) = \perp_p (A_p, b)$. A similar result holds for quadratic abelian groups.*

Proof. It is enough to show that $A_p \perp A_\ell$ for distinct prime $p \neq \ell$. So let $x \in A_p$ and $y \in A_\ell$ and choose $k, t \in \mathbb{N}$ such that $p^k x = \ell^t y = 0$ and $c, d \in \mathbb{Z}$ with $cp^k + d\ell^t = 1$. Then

$$b(x, y) = cp^k b(x, y) + d\ell^t b(x, y) = cb(p^k x, y) + db(x, \ell^t y) = 0 + 0 = 0.$$

□

Definition 5.13. *Let (A, b) be a regular bilinear group. If $N \leq A$ is a subgroup then also*

$$N^{\perp} := \{a \in A \mid b(a, n) = 0 \text{ for all } n \in N\}.$$

(A, b) is called **weakly metabolic***, if there is a subgroup $N \leq A$ with $N = N^{\perp}$.*
A regular quadratic group (A, q) is called **weakly metabolic***, if there is a subgroup $N \leq A$ with $N\perp = N$ and $q(N) = \{0\}$.*
The **Witt group** *W of bilinear groups (resp. WQ of quadratic groups) is the Grothendieckgroup of the set of all isometry classes of regular bilinear groups (resp. regular quadratic groups) modulo the weakly metabolic groups.*
For a prime p the Witt group of regular bilinear p-groups (resp. regular quadratic p-groups) is denoted by $W(p)$ (resp. $WQ(p)$).

Clearly $(A, b) \perp (A, -b)$ is weakly metabolic for any regular bilinear group (A, b), as $N := \{(a, a) \mid a \in A\} = N^{\perp}$. So $-[(A, b)] = [(A, -b)]$ in W.

Remark 5.14. *$W \cong \prod_p W(p)$ and $WQ \cong \prod_p WQ(p)$.*

Remark 5.15. *If (A, b) is regular and $N \leq A$ any subgroup then $(N^{\perp})^{\perp} = N$.*

Proof. The main point here is that $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, so every group homomorphism $\varphi : N \to \mathbb{Q}/\mathbb{Z}$ can be extended to some element in A^*.
We always have $N \subset (N^{\perp})^{\perp}$. Now $N^{\perp} \leq A$ and $N^{\perp} = \ker(b_N : A \to N^*)$. As b_A is an isomorphism, also b_N is surjective and $|A| = |N^*||N^{\perp}| = |N||N^{\perp}|$. Similarly $|A| = |N^{\perp}||(N^{\perp})^{\perp}|$ so we obtain equality. □

Lemma 5.16. *Let (A, b) be a regular bilinear group and $N \leq (A, b)$ with $N \subset N^{\perp}$. Then b defines a regular symmetric bilinear form $\overline{b}$ on $N^{\perp}/N$ defined by*

$$\overline{b}(x + N, y + N) := b(x, y) \text{ for all } x, y \in N^{\perp}$$

Then $(A, b) \perp (N^{\perp}/N, -\overline{b})$ is weakly metabolic. A similar statement holds for quadratic forms if one additionally assumes that $q(N) = \{0\}$.

Proof. $\bar{b}$ is well defined and regular since $(N^\perp)^\perp = N$. The subgroup $U := \{(x, \overline{x}) \mid x \in N^\perp\}$ of $(A, b) \perp (N^\perp/N, -\bar{b})$ satisfies $U \subset U^\perp$. But $|U| = |N^\perp| = \frac{|A|}{|N|} = |U^\perp|$ since $|A \times N^\perp/N| = |A|\frac{|A|}{|N|}\frac{1}{|N|} = |U|^2$. □

Theorem 5.17. *Every element of W (resp. WQ) has a unique anisotropic representative.*

Proof. Choose (A, b) in $[(A, b)]$ of minimal cardinality. Assume that there is some $x \in A$ with $x \neq 0$ and $b(x, x) = 0$. Then $N := \langle x \rangle \leq A$ satisfies $N \subset N^\perp$. By Lemma 5.16 $[(A, b)] = [(N^\perp/N, \bar{b})]$ contradicts the minimality of $|A|$.
To see the uniqueness (up to isometry) let (A, b) and (A', b') be two anisotropic representatives of the same class in W. Then $(A \oplus A', (b, -b'))$ is weakly metabolic, so there is some subgroup $N \leq A \oplus A'$ such that $N = N^\perp$. As A is anisotropic all $n' \in A'$ with $(0, n') \in N$ satisfy $n' = 0$ and similarly the kernel of the first projection is 0. As $|N| = |N^\perp| = \sqrt{|A||A'|}$ we find that $|A| = |A'|$ and the map $\varphi : A \to A', \varphi(a) := a'$ if and only if $(a, a') \in N$ is a well defined isometry between (A, b) and (A', b').
For quadratic forms similar proofs are left as exercise. □

Remark 5.18. *Every anisotropic regular bilinear group has square free exponent.*

Proof. Let (A, b) be anisotropic. Let $x \in A$, $n \in \mathbb{N}$, $n > 1$ with $n^2 x = 0$. Then $b(nx, nx) = b(n^2 x, x) = b(0, x) = 0$ and hence $nx = 0$, because (A, b) is anisotropic. □

Corollary 5.19. *$W(p) = WQ(p) \cong W(\mathbb{F}_p)$ if $p \neq 2$. $W(2) \cong C_2$.*

Proof. For $p \neq 2$ quadratic forms and symmetric bilinear forms are equivalent concepts.

$$W(\mathbb{F}_p) \to WQ(p), (q : V \to \mathbb{F}_p) \mapsto (\frac{1}{p}q : V \to \mathbb{Q}/\mathbb{Z})$$

is a group homomorphism of which we now construct the inverse. Let (A, q) be an anisotropic representative of $[(A, q)] \in WQ(p)$. Then by Remark 5.18 A is elementary abelian and hence a vector space over $\mathbb{F}_p$, $q : A \to \frac{1}{p}\mathbb{Z}/\mathbb{Z}$, so $(A, pq) \in W(\mathbb{F}_p)$.
To see that $W(2) = C_2$ we show that every regular bilinear $\mathbb{F}_2$-space (V, b) of dimension > 1 is isotropic. If (V, b) is anisotropic, then for $x \neq y \in V \setminus \{0\}$ we get $b(x, x) = b(y, y) = 1$ and hence $b(x + y, x + y) = 0$ a contradiction. □

Theorem 5.20. *$WQ(2) \cong C_8 \times C_2$.*

To determine $WQ(2)$ we need *Gauss sums* on finite quadratic groups.

Definition 5.21. *Let $e(t) := \exp(2\pi i t)$. Then $e : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^*$ is a group homomorphism.*
For a finite quadratic group (A, q) put

$$\Gamma(A, q) := \frac{1}{\sqrt{|A|}} \sum_{a \in A} e(q(a)),\ \gamma_p(A, q) := \frac{1}{\sqrt{|A_p|}} \sum_{a \in A_p} e(q(a)).$$

Lemma 5.22. $\Gamma(A, q) = \prod_p \gamma_p(A, q)$.
$\Gamma((A_1, q_1) \perp (A_2, q_2)) = \Gamma(A_1, q_1) \cdot \Gamma(A_2, q_2))$.
If (A, q) is weakly metabolic then $\gamma_p(A, q) = 1$ for all primes p.
In particular we get a group homomorphism $\gamma_p : WQ \to \mathbb{C}^*$.

Proof. The first two statements are clear. Now assume that (A,q) is weakly metabolic. Then (A_p,q) weakly metabolic for all primes p, because the Sylow p-subgroup N_p of the metaboliser $N=N^\perp\le(A,q)$, $q(N)=\{0\}$ also satisfies $N_p=N_p^\perp\le(A_p,q)$ and $q(N_p)=\{0\}$. So wlog $A=A_p$ and $N\le A$, $N=N^\perp$, $q(N)=\{0\}$. Write $A=\dot\cup_{i=1}^k a_i+N$ with $a_1=0$. Then

$$\sum_{a\in A}e(q(a))=\sum_{i=1}^k\sum_{n\in N}e(q(a_i+n))=\sum_{i=1}^k\sum_{n\in N}e(q(a_i)+b_q(a_i,n))=\sum_{i=1}^k e(q(a_i))\sum_{n\in N}e(b_q(a_i,n)).$$

If $a_i\notin N=N^\perp$, then $n\mapsto b_q(a_i,n)$ is a non-trivial group homomorphism from N to $\mathbb{Q}/\mathbb{Z}$. So there is $n_0\in N$ with $b_q(a_i,n_0)\neq 0$. Then

$$\sum_{n\in N}e(b_q(a_i,n))=\sum_{n\in N}e(b_q(a_i,n+n_0))=e(b_q(a_i,n_0))\sum_{n\in N}e(b_q(a_i,n)).$$

This implies that for $i\neq 1$ the sum $\sum_{n\in N}e(b_q(a_i,n))=0$. For $i=1$ we get $b_q(a_1,n)=b_q(0,n)=0$ for all $n\in N$, hence $\sum_{n\in N}e(b_q(a_i,n))=|N|=\sqrt{|A|}$. □

Definition 5.23. *For $k=1,3$ and $\ell=1,3,5,7$ define*

$$\phi_k:=(\mathbb{Z}/2\mathbb{Z},q),\ \textit{with } q(1)=\frac{k}{4}+\mathbb{Z},\ \textit{and } \psi_\ell:=(\mathbb{Z}/4\mathbb{Z},q),\ \textit{with } q(1)=\frac{\ell}{8}+\mathbb{Z}.$$

Put

$$\chi:=(\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z},q)=(\mathbb{F}_4,\frac{1}{2}N)=\begin{bmatrix}1/2 & 1/2\\ & 1/2\end{bmatrix}$$

with $q(x)=\frac{1}{2}$ for all $x\neq 0$.

Remark 5.24. *ϕ_k and ψ_ℓ are regular quadratic groups. We compute*

$$\gamma_2(\phi_1)=\frac{1}{\sqrt{2}}(1+e(\frac{1}{4}))=\frac{1+i}{\sqrt{2}}=\zeta_8,$$

$$\gamma_2(\psi_1)=\frac{1}{2}(1+\zeta_8+\zeta_8^4+\zeta_8^9)=\zeta_8,$$

$$\gamma_2(\chi)=\frac{1}{2}(1+(-1)+(-1)+(-1))=-1.$$

Lemma 5.25. *In $WQ(2)$ we have*

(1) $8[\phi_1]=0$.

(2) $2[\phi_1]=2[\psi_1]$.

(3) $k[\psi_1]=[\psi_{k\pmod 8}]$ *for k odd.*

(4) $4[\psi_1]=[\chi]$.

(5) $[\phi_1]+[\phi_3]=0$.

Proof. (1) Let $(a_1, \ldots, a_8)$ be a basis of $\perp^8 \phi_1$ and

$$N := \langle a_1 + a_2 + a_3 + a_4, a_3 + a_4 + a_5 + a_6, a_5 + a_6 + a_7 + a_8, a_1 + a_3 + a_5 + a_7 \rangle.$$

Then $N \leq N^\perp$, $q(N) = \{0\}$ and $|N| = 2^4$, so $N = N^\perp$ and $\perp^8 \phi_1$ is weakly metabolic.
(2) Let (a_1, a_2) be a basis of $\psi_1 \perp \psi_1$ and $e := 2a_1 + 2a_2$. Then $q(e) = 0$ and $\langle e \rangle^\perp = \langle 2a_1, 2a_2, a_1 + a_2 \rangle$. Hence $(a_1 + a_2, a_1 + 3a_2)$ is a basis of $\langle e \rangle^\perp / \langle e \rangle \cong \phi_1 \perp \phi_1$.
(3)-(5) As an exercise. Note that $[\psi_1] + [\psi_7]$ is weakly metabolic, and so $[\psi_7] = -[\psi_1] = 7[\psi_1]$ by (1) and (2). □

Proof. (of Theorem 5.20) We show that

$$WQ(2) = \langle [\phi_1] \rangle \oplus \langle [\phi_1] - [\psi_1] = [\phi_1] + [\psi_7] \rangle \cong C_8 \times C_2.$$

We know that $[\phi_1]$ has order 8 and $4[\phi_1] \neq [\phi_1] + [\psi_7]$. Since the order of the abelian group of $[\phi_1] + [\psi_7]$ (which is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$) is not a square, the quadratic group $[\phi_1] + [\psi_7]$ cannot be weakly metabolic. So $[\phi_1] + [\psi_7]$ has order 2. It remains to show that

$$WQ(2) = \langle [\phi_k], [\psi_\ell], [\chi] \mid k = 1, 3, \ell = 1, 3, 5, 7 \rangle =: X.$$

Let (A, q) be an anisotropic quadratic 2-group. Show that $[(A, q)] \in X$ by induction on $|A|$.
We first note that the exponent of A divides 4. Otherwise A contains an element $x \in A$ of order 8 and

$$q(4x) = 16q(x) = 8b_q(x, x) = b_q(8x, x) = 0$$

so $4x$ isotropic, a contradiction to (A, q) being anisotropic.
If $a \in A$ is an element of order 4 then $q(a) = \frac{k}{8} + \mathbb{Z}$ for $k \in \{1, 3, 5, 7\}$ since $b_q(4a, a) = 8q(a) = 0$ and $q(2a) = 4q(a) \neq 0$. But then $A = \langle a \rangle \perp \langle a \rangle^\perp$ and $\langle a \rangle \cong \psi_k$.
So we may assume that $\exp(A) = 2$. If there is some $a \in A$ with $q(a) = \frac{k}{4}$ for some odd k, then the regular form ϕ_k splits as orthogonal summand. It hence remains to treat the case that $q(A \setminus \{0\}) = \{\frac{1}{2} + \mathbb{Z}\}$. But then $(A, 2q \pmod{2\mathbb{Z}})$ is an anisotropic quadratic space over $\mathbb{F}_2$, hence isometric to $N(\mathbb{F}_2)$ whence $A \cong \chi$. □

Corollary 5.26. *The exponent of WQ is 8. In particular the image of γ_p is contained in the subgroup $\langle \zeta_8 \rangle \leq \mathbb{C}^*$,*

$$\Gamma : WQ \to \langle \zeta_8 \rangle \leq \mathbb{C}^*.$$

More precisely we have

$$\gamma_p(WQ) \subseteq \langle \zeta_8 \rangle \cap \mathbb{Q}[\sqrt{p}, \zeta_{2p}]^* = \begin{cases} \langle \zeta_8 \rangle & p = 2 \\ \langle -1 \rangle & p \equiv_4 1 \\ \langle i \rangle & p \equiv_4 3 \end{cases}$$

5.2 Maximal lattices.

We return to our example where R is a principal ideal domain, K its field of fractions. Let (V, q) be a finite dimensional quadratic space over K. We want to study full R-lattices in (V, q).

Definition 5.27. *Let $d \in R$, (V, q) a quadratic K-vector space. An R-lattice $E \leq V$ is called d-**maximal** (or just a **maximal lattice** if $d \in R^*$), if*
(a) $q(E) \subseteq dR$ and
(b) E is maximal with (a), i.e. for all lattices $L \leq V$ with $E \leq L$ and $q(L) \subseteq dR$ we have $L = E$.

Theorem 5.28. *Let (V,q) be regular or semi-regular. Then any R-lattice $E \leq V$ with $q(E) \subseteq R$ is contained in a maximal R-lattice.*

Proof. Write $E = \langle e_1, \ldots, e_n \rangle_R$. Let δ denote the determinant if (V,q) is regular and the semi-determinant, if this space is semi-regular. If E is not maximal then there is some lattice $F = \langle f_1, \ldots, f_n \rangle_R$ such that $E \subsetneq F$, $q(F) \subseteq R$. We compute $\delta(E) = [F:E]^2\delta(F)$ so $\delta(F)$ is a proper divisor of $\delta(E) \neq 0$. Since R is Noetherian (as a principal ideal domain) R has no infinite extending divisor chains so this process finishes after finitely many steps. □

Example: It is necessary to assume that (V,q) is regular or semi-regular. Taking $q = 0$ we will never obtain a maximal lattice.

Theorem 5.29. *Let (V,q) be a quadratic K-vector space such that* $\mathrm{ind}(V,q) > 0$. *Let $L \leq V$ be a maximal lattice. Then $L = L' \perp H$ with $H \cong \mathbb{H}(R) \cong \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}$.*

Proof. If $\mathrm{ind}(V,q) \neq 0$ then there is some $0 \neq e \in V$ such that $q(e) = 0$ and $b(V,e) = K = Kb(L,e)$. As R is a principal ideal domain, there is some $c \in R$ such that $Ke \cap L = R(ce)$. Replacing e by ce we may assume that $e \in L$ is a primitive vector. We have $b(e,L) \trianglelefteq R$ so $b(e,L) = dR$ for some d. Put $E := \langle L, \frac{1}{d}e \rangle$. Then

$$q(E) \subseteq q(L) + b_q(L, \frac{1}{d}e) + q(\frac{1}{d}e)R \subseteq R$$

so $d \in R^*$ because of the maximality of L. So $b(L,e) = R$ and hence Re is a singular sharply primitive submodule of (L,q). The result follows by Theorem 2.13. □

Corollary 5.30. *If $(V,q) = (V',q') \perp \perp_{i=1}^m \mathbb{H}(K)$ then any maximal lattice L in (V,q) is of the form $L = L' \perp \perp_{i=1}^m \mathbb{H}(R)$.*

5.3 Milgram-Braun formula

Lemma 5.31. *Let (V,q) be a regular quadratic space over $\mathbb{Q}$ and $L \leq V$ an even $\mathbb{Z}$-lattice in (V,q) (i.e. $q(L) \subseteq \mathbb{Z}$). Then q defines a regular quadratic form $q_L : L^\#/L \to \mathbb{Q}/\mathbb{Z}$. The map*

$$\delta : W(\mathbb{Q}) \to WQ; [(V,q)] \mapsto [(L^\#/L, q_L)]$$

is a well defined group homomorphism with kernel isomorphic to $W(\mathbb{Z})$.

Proof. δ is well defined:
We first show that the class of $(L^\#/L, q_L)$ in WQ does not depend on the choice of the even lattice L in V:
If $L_0 \leq L$ is a sublattice, then $L/L_0 \leq L_0^\#/L_0$ is a subgroup with dual group $(L/L_0)^\perp = L^\#/L_0$ and $q_{L_0}(L/L_0) = \{0\}$. So by Lemma 5.16 $[L_0^\#/L_0, q_{L_0}] = [L^\#/L, q_L] \in WQ$.
In general, if L_1, L_2 are two even lattices in V, then $L_0 := L_1 \cap L_2$ is also an even lattice and

$$[L_1^\#/L_1, q_{L_1}] = [L_0^\#/L_0, q_{L_0}] = [L_2^\#/L_2, q_{L_2}].$$

Clearly hyperbolic modules map to zero and the map is compatible with orthogonal sums, so δ is a well defined group homomorphism.

The kernel of δ consists of those quadratic spaces (V,q) that admit an even unimodular lattice (L,q), so $(V,q)=\iota(L,q)=(\mathbb{Q}L,q)$, where

$$\iota : W(\mathbb{Z}) \hookrightarrow W(\mathbb{Q}), [(L,q)] \mapsto [(\mathbb{Q}L,q)].$$

ι is injective by Theorem 5.29: Because ι is a well-defined group homomorphism injectivity follows from computing the kernel of ι. If $\iota([(L,q)])=0$, then $(\mathbb{Q}L,q)\cong\mathbb{H}(\mathbb{Q})^m$ for some m. But then (L,q) is a maximal lattice in $\mathbb{H}(\mathbb{Q})^m$, so by Theorem 5.29 $(L,q)\cong\mathbb{H}(\mathbb{Z})^m$. □

Theorem 5.32. *(Milgram-Braun formula) Let $L\leq(V,q)$ be an even lattice in the rational quadratic space (V,q) of signature $\sigma\in\mathbb{Z}$. Then $\Gamma(L^\#/L,q_L)=e(\sigma/8)$.*

Proof. (following Husemöller-Milnor) By Lemma 5.31 we know that $\Gamma(L):=\Gamma(L^\#/L,q_L)$ does not depend on the choice of an even lattice L in (V,q). We also know that $\Gamma(L_1\perp L_2)=\Gamma(L_1)\Gamma(L_2)$ (see Lemma 5.22). So it is enough to show the formula for 1-dimensional lattices $L=\mathbb{Z}e$ with $q(e)=m$. Wlog we assume that $m>0$. Then $L^\#=\mathbb{Z}\frac{1}{2m}e$, $|L^\#/L|=2m$ and

$$\Gamma(L)=\frac{1}{\sqrt{2m}}\sum_{k=0}^{2m-1}e(\frac{k^2}{4m}).$$

To evaluate this Gauss sum, we introduce a periodic function $f:\mathbb{R}\to\mathbb{C}$ by

$$f(t):=\sum_{k=0}^{2m-1}\exp(\pi i\frac{(k+t)^2}{2m}).$$

Then $f(0)=f(1)=\sqrt{2m}\Gamma(L)$ and f is 1-periodic, continuous and piecewise smooth, so its Fourier-series converges to f everywhere,

$$f(t)=\sum_{n=-\infty}^{\infty}a_n\exp(-2\pi int),\ \text{where } a_n=\int_0^1 f(t)\exp(2\pi int)dt.$$

Then $\sqrt{2m}\Gamma(L)=f(0)=\sum_{n=-\infty}^{\infty}a_n$. To evaluate

$$a_n=\sum_{k=0}^{2m-1}\int_0^1\exp\left(2\pi i\left(\frac{(k+t)^2}{4m}+nt\right)\right)dt$$

we check that $\frac{(k+t)^2}{4m}+nt=(k+t+2mn)^2/(4m)\pmod{\mathbb{Z}}$ and substitute $s=k+t+2mn$ to find

$$a_n=\sum_{k=0}^{2m-1}\int_{k+2mn}^{k+2mn+1}\exp(2\pi i\frac{s^2}{4m})ds=\int_{2mn}^{2m(n+1)}\exp(\pi i\frac{s^2}{2m})ds$$

and hence $\sqrt{2m}\Gamma(L)=\sum_{n=-\infty}^{\infty}a_n=\int_{-\infty}^{\infty}\exp(\pi i\frac{s^2}{2}m)ds$. We now substitute $u=\frac{s}{\sqrt{2m}}$ to see that $\Gamma(L)=\int_{-\infty}^{\infty}\exp(\pi iu^2)du$ is independent of m. So $\Gamma(L)=\gamma_2(\phi_1)=\zeta_8=e(\frac{1}{8})$. □

Corollary 5.33. *(Even lattices of odd determinant.) Let (L,q) be an even lattice of odd determinant in the regular quadratic $\mathbb{Q}$-vector space (V,q) of signature σ. Then $\sigma\in2\mathbb{Z}$. If $\sigma\in2+4\mathbb{Z}$ then there is some prime $p\equiv_4-1$ that divides $\det(L)$ to some odd power.*
Even unimodular lattices (L,q) exist, if and only if $\sigma\in8\mathbb{Z}$.

Proof. We already know that the dimension of L is even, so is its signature. If the signature is in $2+4\mathbb{Z}$, then $\Gamma(L) \in \{\pm i\}$. As $i \notin \mathbb{Q}[\sqrt{p}, \zeta_p]$ for primes $p \equiv_4 1$, we need that some prime $p \equiv_4 -1$ divides $\det(L) = |L^\# / L|$.
$\sigma \in 8\mathbb{Z}$ is necessary for the existence of an even unimodular lattice by Milgram's formula. We need to show that for any signature $\sigma \in 8\mathbb{Z}$ there is some even unimodular lattice of signature σ. If $\sigma = 8a > 0$ then we may take $L = \mathbb{E}_8^a$. If $\sigma = -8a < 0$ then take $(\mathbb{E}_8, -q)^a$. To obtain a lattice of a given dimension and signature $\pm 8a$ add a suitable sum of hyperbolic planes $\mathbb{H}(\mathbb{Z})$. □

5.4 The Witt group of $\mathbb{Q}$.

Let (V, q) be a regular quadratic space over $\mathbb{Q}$. Then (V, q) has an orthogonal basis $(V, q) = \langle a_1, \ldots, a_n \rangle$ with $a_i \in \mathbb{Z}$ square free. In particular

$$W(\mathbb{Q}) = \langle \langle a \rangle \mid a \in \mathbb{Z}, \text{ square free } \rangle$$

Theorem 5.34. $W(\mathbb{Q}) \cong W(\mathbb{R}) \oplus W \cong \mathbb{Z} \oplus \bigoplus_p W(p)$.

Proof. Since $\mathbb{Q} \subset \mathbb{R}$, the signature defines a canonical epimorphism $S : W(\mathbb{Q}) \to W(\mathbb{R}) \cong \mathbb{Z}$. We now want to construct a canonical epimorphism $\delta_b : W(\mathbb{Q}) \to W$. Let (V, b) be a regular bilinear $\mathbb{Q}$-space and $L \leq V$ an integral $\mathbb{Z}$-lattice in V. Then b defines a regular symmetric bilinear form

$$\beta_L : L^\# / L \times L^\# / L \to \mathbb{Q}/\mathbb{Z}.$$

and as in Lemma 5.31 we obtain a well defined group homomorphism

$$\delta_b : W(\mathbb{Q}) \to W, [(V, b)] \mapsto [(L^\# / L, \beta_L)].$$

Note that the finite abelian group $(L^\# / L, \beta_L)$ is the orthogonal sum of its Sylow p-subgroups. For a prime p denote by δ_p the composition of δ_b with the projection onto the Sylow p-subgroup,

$$\delta_p : W(\mathbb{Q}) \to W(p).$$

To show that $W(\mathbb{Q}) \cong W(\mathbb{R}) \oplus W$ (via the isomorphism (S, δ_b)) consider the subgroup

$$U_k = \langle \langle a \rangle \mid a \in \mathbb{Z}, \text{ all prime factors of } a \text{ are } \leq k \rangle \leq W(\mathbb{Q})$$

Then the signature S is an isomorphism $S : U_1 \cong \mathbb{Z} \cong W(\mathbb{R})$ and $U_1 \leq \ker(\delta_b)$. The subgroup $U_2 = \langle \langle 1 \rangle, \langle -1, 2 \rangle \rangle$ is isomorphic to $W(\mathbb{R}) \times W(2) \cong \mathbb{Z} \times C_2$. This follows because $\langle -1, 2 \rangle \leq \ker(S)$ has order 2 in $W(\mathbb{Q})$, as $\langle -1, 2, -1, 2 \rangle$ contains the self-orthogonal subspace $\langle (1, 1, 1, 0), (0, 1, 2, 1) \rangle$.
By induction on k we want to show that $U_k \cong W(\mathbb{R}) \bigoplus_{p \leq k} W(p)$.
For $k = 1$ and $k = 2$ we have already seen this and it is clear that $U_k = U_{k-1}$ if k is not a prime. If $k = p$ is a prime, then it is enough to show that $U_p / U_{p-1} \cong W(\mathbb{F}_p)$.

Lemma 5.35. *Let p be an odd prime. Define $\delta_p : W(\mathbb{Q}) \to W(\mathbb{F}_p)$, on the generators $\{\langle a \rangle \mid a \in \mathbb{Z}$ square free $\}$ by*

$$\begin{aligned} \delta_p(\langle a \rangle) &:= \langle \overline{a} \rangle \quad a \in \mathbb{Z}, p \nmid a \\ \delta_p(\langle pa \rangle) &:= \langle \overline{a} \rangle \quad a \in \mathbb{Z}, p \nmid a. \end{aligned}$$

Then δ_p gives an isomorphism $U_p / U_{p-1} \to W(\mathbb{F}_p)$.

Proof. Clearly δ_p is surjective and $U_{p-1} \subseteq \ker(\delta_p)$. Need to show that $U_{p-1} = \ker((\delta_p)_{U_p})$.
Let $a_1, \ldots, a_r \in \mathbb{Z}$ such that $|a_i| \leq p-1$ and $a \in \mathbb{Z}$, $0 < |a| < p$ so that $a_1 \cdots a_r \equiv_p a$. Then

$$\langle ap \rangle \equiv \langle a_1 \cdots a_r p \rangle \pmod{U_{p-1}}.$$

We show this by induction on r. If $r = 1$ then nothing is to show.
For $r = 2$ let $a_1 a_2 = a + kp$ with $k \in \mathbb{Z}$. If $k = 0$, then nothing is to show. If $k \neq 0$, then $0 < |k| < p$ and

$$\langle a, kp \rangle \cong \langle a + kp, (a + kp)akp \rangle = \langle a_1 a_2, a_1 a_2 akp \rangle$$

because $\langle a, kp \rangle$ represents $a + kp$ and both forms have the same determinant. Multiplying by p we obtain

$$\langle ap, k \rangle \cong \langle a_1 a_2 p, a_1 a_2 ak \rangle$$

so $\langle ap \rangle \equiv \langle a_1 a_2 p \rangle \pmod{U_{p-1}}$. If r is arbitrary, then this consideration yield the induction step. So we have shown that $U_p = \langle U_{p-1}, \langle ap \rangle \mid 1 \leq |a| < p \rangle$.
To show the lemma, we show that the forms $\langle ap \rangle$ modulo U_{p-1} satisfy the same relations as the $\langle \overline{a} \rangle$ in $W(\mathbb{F}_p)$. If $\overline{a} = \overline{b}\overline{c}^2$, then $\langle \overline{a} \rangle = \langle \overline{b} \rangle \in W(\mathbb{F}_p)$, which yields $\langle ap \rangle \equiv \langle bc^2 p \rangle = \langle bp \rangle$ modulo U_{p-1}. So it is enough to consider $\langle p \rangle$ and $\langle \epsilon p \rangle$ with $\epsilon \in \mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$. If -1 is a square in $\mathbb{F}_p$, then there is $z \in \{1, \ldots, p-1\}$ such that $z^2 = (-1) + kp \equiv_p -1$. Then $e_1 + ze_2$ in $\langle p \rangle \perp \langle p \rangle$ has norm kp^2, so $\langle p \rangle \perp \langle p \rangle \cong \langle k \rangle \perp \langle \ell \rangle \in U_{p-1}$. Similarly $\langle \epsilon p \rangle \perp \langle \epsilon p \rangle \in U_{p-1}$.
If one may choose $\epsilon = -1$ then $\langle p \rangle + \langle -p \rangle = 0$ in $W(\mathbb{Q})$, so $\langle \epsilon p \rangle = -\langle p \rangle$ and we have to show that $\langle p \rangle + \langle p \rangle + \langle p \rangle + \langle p \rangle \equiv 0 \pmod{U_{p-1}}$ and $\langle p \rangle + \langle p \rangle \equiv \langle \epsilon p \rangle \perp \langle \epsilon p \rangle \pmod{U_{p-1}}$. Then there are $a, b \in \{1, \ldots, p-1\}$ such that $a^2 + b^2 = \epsilon + kp$. The vector $ae_1 + be_2 \in \langle p \rangle \perp \langle p \rangle$ has norm $\epsilon p + kp^2$, so $\langle p, p \rangle \equiv \langle \epsilon p, \epsilon p \rangle \pmod{U_{p-1}}$. □
□

Corollary 5.36. *To regular rational bilinear spaces (E_1, b_1) and (E_2, b_2) are isometric, if and only if $\dim(E_1) = \dim(E_2)$, $\operatorname{sgn}(b_1) = \operatorname{sgn}(b_2)$ and $\delta_p(b_1) = \delta_p(b_2)$ for all primes p.*

Proof. These conditions yield equality in the Witt group, so there are hyperbolic modules $\mathbb{H}_1$, $\mathbb{H}_2$ with

$$(E_1, b_1) \perp \mathbb{H}_1 \cong (E_2, b_2) \perp \mathbb{H}_2.$$

Since $\dim(E_1) = \dim(E_2)$, we get $\mathbb{H}_1 = \mathbb{H}_2$ and by Witt's cancellation theorem, this implies that $(E_1, b_1) \cong (E_2, b_2)$. □

Chapter 2

Quadratic forms over discrete valuation rings.

6 Discrete valuation rings.

Definition 6.1. *(a) A* **discrete valuation ring** *R is a local principal ideal domain (commutative, without zero divisors) which is not a field.*
(b) Let K be a field. A **discrete valuation** *of K is a mapping $v : K \to \mathbb{Z} \cup \{\infty\}$ such that*
(o) There is some $x \in K^*$ such that $v(x) \neq 0$.
(i) $v(x) = \infty \Leftrightarrow x = 0$.
(ii) $v(xy) = v(x) + v(y)$ for all $x, y \in K^*$.
(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

Clear: $v(1) = 0$, $v(x^{-1}) = -v(x)$, $v : K^* \to (\mathbb{Z}, +)$ is a group homomorphism so the image of v is an ideal $a\mathbb{Z}$ of $\mathbb{Z}$. Replacing v by $\frac{1}{a}v$ we hence may assume that v is **normalized**, i.e. $v(K^*) = \mathbb{Z}$.

Remark 6.2. *$v(x + y) = \min\{v(x), v(y)\}$ if $v(x) \neq v(y)$.*

Proof. First note that $v(\zeta) = 0$ for any $\zeta \in R$ such that $\zeta^n = 1$ for some n. In particular $v(-1) = 0$ and $v(-y) = v(y)$.
Assume that $v(x) < v(y)$. Then

$$v(x) = v(x + y - y) \geq \min\{v(x + y), v(y)\} \geq \min\{v(x), v(y)\} = v(x).$$

We therefore have equality everywhere and $v(x+y) = v(x)$ (note that $v(y) > v(x)$ by assumption). □

Example 6.3. *Let $p \in \mathbb{Z}$ be a prime. $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$, $v_p(\frac{a}{b}p^i) = i$ if $p \nmid ab$, $v_p(0) = \infty$ is a discrete valuation with valuation ring $\mathbb{Z}_{(p)} := \{x \in \mathbb{Q} \mid v_p(x) \geq 0\} = \{\frac{a}{b} \in \mathbb{Q} \mid p \nmid b\}$ and maximal ideal $p\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) > 0\}$.*

Proposition 6.4. *(a) Let R be a discrete valuation ring with maximal ideal $\wp = \pi R \neq \{0\}$. Then $K := \mathrm{Quot}(R) = \dot{\cup}_{i \in \mathbb{Z}} \pi^i R^* \cup \{0\}$ and the mapping $v : K \to \mathbb{Z} \cup \{\infty\}, v(\pi^i R^*) := i, v(0) := \infty$ is a discrete valuation of K.*
(b) If $v : K \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation, then $R := \{x \in K \mid v(x) \geq 0\}$ is a discrete valuation ring with maximal ideal $\{x \in K \mid v(x) \geq 1\} =: \wp = \pi R$ for any $\pi \in K$ with $v(\pi) \geq 1$ minimal.

Proof. (a) Since R is a local ring the units are $R^* = R \setminus \wp$. Any element $a \in R$ is either a unit ($a \in R^*$) or a multiple of π and then $a_1 := \pi^{-1}a \in R$. Also a_1 is either a unit or a multiple of π. Continuing like this, we may write any non zero element of R in a unique way as $a = \pi^n u$ with $u \in R^*$ and $n \in \mathbb{Z}_{\geq 0}$. Similarly any element $0 \neq x = \frac{a}{b} \in \mathrm{Quot}(R) = K$ can be written as $\pi^i w$ with $w \in R^*$ and $i \in \mathbb{Z}$ in a unique way. Therefore v is well defined. It clearly satisfies (o), (i) and (ii). So it remains to show the strong triangular inequality. Let $x \in \pi^i R^*$, $y \in \pi^j R^*$, $i, j \in \mathbb{Z}$, $i \geq j$. Then $x + y \in \pi^j R$ and so $v(x + y) \geq j = \min\{v(x), v(y)\}$.
(b) We prove that R is a ring: $0 \in R$, $1 \in R$, $a, b \in R \Rightarrow ab \in R$ and $a + b \in R$.
The unit group of R is $R^* = \{x \in K \mid v(x) \geq 0 \text{ and } -v(x) \geq 0\} = \{x \in K \mid v(x) = 0\}$. In particular $\wp$ is the unique maximal ideal of R. Choose $\pi \in \wp$ such that $v(\pi)$ is minimal. Then for any $z \in \wp$ we have $v(z) \geq v(\pi)$ and hence $z\pi^{-1} \in R$. So $\wp = \pi R$ is a principal ideal. □

Remark 6.5. *Let R be a discrete valuation ring and $x \in K = \mathrm{Quot}(R)$. Then either $x \in R$ or $x^{-1} \in \wp$. In particular $K = R \cup \{x^{-1} \mid 0 \neq x \in \wp\}$.*

6.1 Completion

Remark 6.6. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation and $s \in (0, 1)$. Then v defines an* **ultra-metric**

$$d : K \times K \to \mathbb{R}_{\geq 0}, d(x, y) := s^{v(x-y)}$$

where $s^\infty := 0$. This means that d satisfies the following three axioms:
(i) $d(a, b) = 0$ if and only if $a = b$.
(ii) $d(a, b) = d(b, a)$ for all $a, b \in K$.
(iii) $d(a, c) \leq \max\{d(a, b), d(b, c)\}$ for all $a, b, c \in K$.

Definition 6.7. *A metric space (M, d) is called* **complete***, if any Cauchy sequence in M converges towards a limit in M.*

Theorem 6.8. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of the field K. Put $\mathcal{R}$ the ring of all Cauchy sequences in K and $\mathcal{N}$ the ideal of all sequences in K that converge to 0. Then $\mathcal{N} \trianglelefteq \mathcal{R}$ is a maximal ideal and hence $\overline{K} := \mathcal{R}/\mathcal{N}$ is a field. The valuation v extends to a valuation v of $\overline{K}$ and $\overline{K}$ is complete. The mapping $\varphi : K \hookrightarrow \overline{K}, a \mapsto (a, a, a, a \ldots) + \mathcal{N}$ is injective and the image is dense in $\overline{K}$. The field $\overline{K}$ is called the* **completion** *of K. It is unique up to isomorphism.*

Proof. See the lecture Computeralgebra. □

Theorem 6.9. *Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a discrete valuation of the field K with valuation ring R and maximal ideal πR. Define*

$$S := \lim_{\leftarrow} R/\pi^i R = \{(a_0, a_1, \ldots) \mid a_i \in R/\pi^{i+1}R, a_i + \pi^i R = a_{i-1}\}.$$

Then S is an integral domain and $\varphi : R \to S, a \mapsto (a + \pi R, a + \pi^2 R, \ldots)$ is a ring monomorphism. The valuation v extends uniquely to a valuation v of S, $v(a_0, a_1, \ldots,) := i$ if $a_i \neq 0$, $a_{i-1} = 0$. S is complete with respect to this valuation and $\overline{K} := \mathrm{Quot}(S)$ is the completion of K.

Proof. S is a ring with component wise operations since the projections $a + \pi^i R \mapsto a + \pi^{i-1}R$ are ring homomorphisms.
φ is injective because $\bigcap_{i=0}^{\infty} \pi^i R = \{0\}$.

It is clear that v is a valuation that extends the valuation of R (exercise).
To see the completeness of S let $(x_n)_{n\geq 0}$ be a Cauchy sequence in S, so $\lim_{n,m\to\infty} v(x_n - x_m) = \infty$ or more concrete that for all $k \geq 0$ there is some $N(k) \in \mathbb{N}$ such that $v(x_n - x_m) > k$ for all $n, m \geq N(k)$. Wlog assume that $(N(n))_{n\geq 0}$ is monotone increasing. Put $x = (x_{N(k),k})_{k\geq 0}$. Then $x \in S$ since

$$x_{N(k),k} + \pi^k R = x_{n,k} + \pi^k R = x_{n,k-1} = x_{N(k-1),k-1}$$

for all $n \geq N(k)$. Similarly one shows that $v(x - x_n) \to \infty$ for $n \to \infty$ so x is the limit of the Cauchy sequence. □

6.2 The p-adic numbers.

Let $K = \mathbb{Q}$, $v = v_p$ for some prime p, $R = \mathbb{Z}_{(p)}$. Then the completion of $\mathbb{Q}$ w.r.t. v_p is denoted by $\mathbb{Q}_p$, the **field of p-adic numbers**. The completion of $\mathbb{Z}_{(p)}$ is the valuation ring

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} = \lim_{\leftarrow} \mathbb{Z}/p^i\mathbb{Z}.$$

the **ring of p-adic integers**. Any $x \in \mathbb{Z}_p$ can be written uniquely as $x = \sum_{i=0}^{\infty} a_i p^i$ with $a_i \in \{0, 1, \ldots, p-1\}$.

Theorem 6.10. *The ring $\mathbb{Z}_p$ of p-adic integers has the following properties:*
(i) $\mathbb{Z}$ is a subring of $\mathbb{Z}_p$ dense with respect of d, but $\mathbb{Z}_p$ uncountable. $(\mathbb{Z}_p, d)$ is complete.
(ii) $\mathbb{Z}_p^* = \mathbb{Z}_p - p\mathbb{Z}_p$ is the unit group of $\mathbb{Z}_p$.
(iii) Any $a \in \mathbb{Z}_p$, $a \neq 0$, is of the form $a = p^n u$ with $u \in \mathbb{Z}_p^*$ and $n = v_p(a)$.
(iv) All ideals $\neq 0$ of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$, $n \in \mathbb{N}$. We have $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.
(v) $\mathbb{Z}_p$ is an integral domain, with respect to v_p it is a Euclidean domain. (vi) $\mathbb{Z}_p^* \cong C_{p-1} \times (\mathbb{Z}_p, +)$ for $p \neq 2$ and $\mathbb{Z}_2^* \cong C_2 \times (\mathbb{Z}_2, +)$.
(vii) $\mathbb{Q}_p/\mathbb{Z}_p \cong \bigcup_{i\geq 0} \frac{1}{p^i}\mathbb{Z}/\mathbb{Z} \leq \mathbb{Q}/\mathbb{Z}$ as an additive group.
(viii) $\mathbb{Z}_p$ is compact, i.e. any sequence in $\mathbb{Z}_p$ has a convergent subsequence.

Proof. Exercise □

6.3 Hensel's Lemma

Theorem 6.11. *Let K be a discrete valuated complete field with valuation v, valuation ring R. Let $f \in R[X]$ be a polynomial and $a_0 \in R$ such that*

$$v(f(a_0)) > 2v(f'(a_0))$$

Then there is some $a \in R$ such that $f(a) = 0$. More precisely the sequence

$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)} \in R$$

converges towards some $a \in R$ such that $f(a) = 0$ and $v(a - a_0) \geq v(f(a_0)) - v(f'(a_0)) > 0$.

Proof. Note that $f(t+x) = f(t) + f_1(t)x + f_2(t)x^2 + \ldots$, for $f_i(t) \in R[t]$, $f_1(t) = f'(t)$. Define $b_0 := -\frac{f(a_0)}{f'(a_0)}$. Then $v\left(\frac{f(a_0)}{f'(a_0)}\right) = v(f(a_0)) - v(f'(a_0)) > v(f'(a_0)) \geq 0$, so $a_1 \in R$.
Moreover $v(f(a_0+b_0)) \geq \min\{v(f_i(a_0)b_0^i) \mid i \geq 2\}$, since $f(a_0) + f_1(a_0)\cdot b_0 = 0$. Therefore $v(f(a_1)) \geq 2v(b_0) > v(f(a_0))$. Now $f'(t+x) = f'(t) + 2xf_2(t) + \ldots$ implies $v(f'(a_1) - f'(a_0)) \geq v(b_0) \geq v(f'(a_0))$, so $v(f'(a_1)) = v(f'(a_0))$.
This shows that $f(a_i)$ converges to 0 $v(f(a_i)) \to \infty$).
We now show that (a_i) is a Cauchy sequence:
$v(a_{n+1} - a_n) = v(b_n) = v\left(-\frac{f(a_n)}{f'(a_n)}\right) = v(f(a_n)) - v(f'(a_n)) \to \infty$, because that first summand is strictly monotonously increasing (in $\mathbb{Z}$) and the second summand is constant. So if $m > n$: $v(a_m - a_n) = v((a_m - a_{m-1}) + (a_{m-1} - a_{m-2}) + \ldots + (a_{n+1} - a_n)) \geq \min\{v(a_i - a_{i-1}) \mid n < i \leq m\} \to \infty$ which means that (a_i) is a Cauchy sequence. □

6.4 Example: The square classes in $\mathbb{Q}_p^*$.

Lemma 6.12. *Let $p \neq 2$ be a prime. Then $\mathbb{Z}_p^* = (\mathbb{Z}_p^*)^2 \dot\cup \epsilon(\mathbb{Z}_p^*)^2$ and the square classes in $\mathbb{Q}_p^*$ are represented by $1, \epsilon, p, \epsilon p$. Here $\epsilon \in \mathbb{Z}_p^*$ is any element such that $\epsilon + p\mathbb{Z}_p \notin (\mathbb{F}_p^*)^2$.*

Proof. Let $a \in \mathbb{Z}_p^*$. Then $a + p\mathbb{Z}_p \in (\mathbb{F}_p^*)^2$ or $\epsilon a + p\mathbb{Z}_p \in (\mathbb{F}_p^*)^2$. In the first case $f(X) := X^2 - a \in \mathbb{Z}_p[X]$ has a zero a_0 mod p and in the second case $f(X) := X^2 - a\epsilon$. In both cases $v_p(f'(a_0)) = v_p(2a_0) = 0$ since $2 \in \mathbb{Z}_p^*$ and also $a_0 \in \mathbb{Z}_p^*$, so by Hensel's lemma there is some $\alpha := a_\infty \in \mathbb{Z}_p$ such that $f(\alpha) = 0$. So $\alpha^2 = a$ and $a \in (\mathbb{Z}_p^*)^2$ or $\alpha^2 = \epsilon a$ and $a \in \epsilon(\mathbb{Z}_p^*)^2$.
Any element in $\mathbb{Q}_p^*$ is of the form up^j for $u \in \mathbb{Z}_p^* = (\mathbb{Z}_p^*)^2 \dot\cup \epsilon(\mathbb{Z}_p^*)^2$ and $j \in \mathbb{Z}$. After multiplication be a certain power of $p^2 \in (\mathbb{Q}_p^*)^2$ we may assume that $j \in \{0, 1\}$. So the square classes in $\mathbb{Q}_p^*$ are represented by $1, \epsilon, p, \epsilon p$. It is clear that no two of them represent the same square class. □

Example. $\sqrt{-1} \in \mathbb{Z}_5$: We need to find a zero of $f(X) := X^2 + 1$ using Hensel's Lemma. Put $a_0 := 2$. Then $f(a_0) = 5$ and $f'(a_0) = 4 \equiv -1 \pmod 5$.

$$a_1 := a_0 - f(a_0)/f'(a_0) = 2 + 5 = 7 \pmod{25} \text{ satisfies } f(a_1) = 49 + 1 \equiv 0 \pmod{25}.$$

$a_2 := 7 + 50 = 2 + 5 + 50$, $a_3 = 2 + 5 + 50 + 5^3 = 2,121, \ldots$ $a_\infty = 2,121342303220\ldots$.

Lemma 6.13. *The square classes in $\mathbb{Z}_2^*$ are represented by $\{1, 3, 5, 7\}$ and the ones in $\mathbb{Q}_2^*$ by $\{1, 3, 5, 7, 2, 6, 10, 14\}$.*

Proof. We just give the argument for $\mathbb{Z}_2^*$, the square classes in $\mathbb{Q}_2^*$ are then obtained in the same way as for odd primes. We use the same approach as before, trying to find a zero of the polynomial $f(X) = X^2 - a \in \mathbb{Z}_2[X]$ using Hensel's lemma. But now $f'(X) = 2X$ and so for any $a_0 \in \mathbb{Z}_2^*$ the valuation $v_2(f'(a_0)) = v_2(2) = 1$. To apply Hensel's Lemma we hence need to find a zero a_0 of f modulo $2^3 = 8$. Any odd integer $a = 1 + 2m$ satisfies

$$a^2 = (1+2m)^2 = 1 + 4m + 4m^2 = 1 + 8\frac{m(m+1)}{2} \equiv 1 \pmod 8$$

so $((\mathbb{Z}/8\mathbb{Z})^*)^2 = \{1\}$ and the square classes in $(\mathbb{Z}/8\mathbb{Z})^*$ are represented by $M := \{1, 3, 5, 7\}$. For $a \in \mathbb{Z}_2^*$ we find a unique $m \in M$ such that $a \equiv m \pmod 8$. Then $f(X) := X^2 - am \in \mathbb{Z}_2[X]$ has a zero a_0 mod 8 which can be lifted by Hensel's lemma to some $\alpha = a_\infty \in \mathbb{Z}_2^*$ satisfying $\alpha^2 = am$. □

7 Lattices over discrete valuation rings.

Let R be a discrete valuation ring with maximal ideal πR and residue field $\overline{R} = R/\pi R$. Denote by $K := \mathrm{Quot}(R)$ the field of fractions of R, (V, q) a f.d. quadratic K-space, (V, b) a f.d. bilinear K-space, $E \leq V$ an R-lattice in V.

Theorem 7.1. *(a) If* $\mathrm{char}(\overline{R}) \neq 2$*, then any R-lattice E in the bilinear K-space (V, b) has some orthogonal basis, i.e.* $E = \bigoplus_{i=1}^{n} Re_i$ *such that* $b(e_i, e_j) = 0$ *for all* $i \neq j$*.*
(b) If $\mathrm{char}(\overline{R}) = 2$*, then any R-lattice E in the bilinear K-space (V, b) is the orthogonal sum of lattices of rank* 1 *or* 2*, i.e.* $E = \bigoplus_{i=1}^{n} E_i$ *such that* $b(E_i, E_j) = \{0\}$ *for all* $i \neq j$ *and* $\dim(E_i) \leq 2$*.*

Proof. (1) If $b(E, E) = \{0\}$ then any lattice basis of E has the desired properties.
(2) So assume that $b(E, E) \neq \{0\}$. Then we can always multiply b by some power of π to achieve that $b(E, E) \subseteq R$ but not $b(E, E) \subseteq \pi R$.
(a) There is some $e_1 \in E$ such that $b(e_1, e_1) \notin \pi R$: Then Re_1 is a regular submodule of the bilinear R-module (E, b) and hence $E = Re_1 \perp\!\!\!\perp e_1^{\perp}$. Then continue with $e_1^{\perp}$.
(b) For all $x \in E$ we have $b(x, x) \in \pi R$. Note that this case cannot occur if $\mathrm{char}(\overline{R}) \neq 2$, because there are always $x, y \in E$ with $b(x, y) \notin \pi R$. If $b(x, x)$ and $b(y, y) \in \pi R$ then $b(x + y, x + y) = b(x, x) + b(y, y) + 2b(x, y) \notin \pi R$ because $2 \in R^*$. Also for residue characteristic 2 there are $e_1, e_2 \in E$ such that $b(e_1, e_2) \notin \pi R$. Then $\langle e_1, e_2 \rangle$ is a regular submodule of E and $E = \langle e_1, e_2 \rangle \perp\!\!\!\perp \langle e_1, e_2 \rangle^{\perp}$. □

Example: $\mathbb{Z}_{(2)}\mathbb{A}_3$ with Gram matrix $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$. Put $E_1 := \langle e_1, e_2 \rangle : \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Then $\det(E_1) = 3$ so E_1 is a regular submodule. We compute $E_1^{\perp} = \langle e_3 - \frac{1}{3}e_1 - \frac{1}{3}e_2 =: e \rangle$ and get the new Gram matrix $\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 4/3 \end{pmatrix}$.

Remark 7.2. *Let E be some R-lattice in a quadratic K-vector space (V, q) such that $q(V) \neq \{0\}$. Then $O(E, q)$ contains reflections.*

Proof. We can always scale the quadratic form so that $q(E) \subset R$, but $q(E) \not\subset \pi R$. Then there is some $e \in E$ with $q(e) \in R^*$ and hence $s_e \in O(E, q)$. Note that the orthogonal group does not change if we scale the quadratic form. □

7.1 The Jordan decomposition.

Theorem 7.3. *Any R-lattice L in a regular bilinear K-space (V, b) has a decomposition*

$$L = (L_a, \pi^a b_a) \perp (L_{a+1}, \pi^{a+1} b_{a+1}) \perp \ldots \perp (L_c, \pi^c b_c)$$

with $a \leq c \in \mathbb{Z}$ such that (L_i, b_i) are regular bilinear R-lattices (possibly 0). The dimensions $n_a := \dim(L_a)$ are uniquely determined as well as the determinant $\det(\overline{b_a}) \in \overline{R}^*/(\overline{R}^*)^2$*.*

Proof. The existence follows by applying Theorem 4.16 successively. As (V, b) is a regular bilinear K-space, there is a unique $a \in \mathbb{Z}$ such that for $b' := \pi^{-a} b$ satisfies $b'(L, L) \subset R$ but $b'(L, L) \not\subseteq \pi R$. By Theorem 4.16 (applied to the R-module (L, b')), there is a regular R-lattice (L_a, b') with $(L, b') = (L_a, b') \perp (L', b')$ such that $b'(L', L') \subset \pi R$. We continue with $(L', \pi^{-a'} b')$ until we obtain the full Jordan decomposition.

To obtain the uniqueness of the invariants note that $E := (L/\pi L, \overline{b'})$ is a bilinear $\overline{R}$-space with radical $E' = L'/\pi L'$. So the determinant of (L_a, b') is modulo π exactly the one of the bilinear $\overline{R}$-space $(E/E', \overline{b'})$ and hence well defined in $\overline{R}^*/(\overline{R}^*)^2$. Also $\dim(L_a) = \dim_{\overline{R}}(E/E')$. □

Exercise: Implement an algorithm to compute this Jordan splitting for the rings $\mathbb{Z}_{(p)}$.

7.2 Lifting isometries

General setup: R discrete valuation ring, $\pi R \trianglelefteq_{max} R$, $K = \mathrm{Quot}(R)$, $\overline{R} = R/\pi R$. (V, q) quadratic K-space, $b = b_q$, $E \leq V$ an R-lattice.

Definition 7.4. *Let (V, q), (V', q') be two quadratic K-spaces. For a linear map $u : V \to V'$ let*

$$b'_u : V' \to V^*, y \mapsto b'_u(y) : (x \mapsto b_{q'}(u(x), y)).$$

Theorem 7.5. *Keep the notation from Definition 7.4. Let $E \leq V$ be an R-lattice in V such that*

$$q'(u(x)) \equiv q(x) \pmod{\pi^k} \text{ for all } x \in E(\text{ some } k \in \mathbb{N}).$$

Let F be a f.g. R-submodule of V' such that

$$E^* = \mathrm{Hom}_R(E, R) = b'_u(F) + \pi E^* \text{ and } \pi^k q'(F) \subseteq \pi R.$$

Then there is a linear mapping $u' : E \to V'$ such that $u'(x) - u(x) \in \pi^k F$ for all $x \in E$ and $q'(u'(x)) \equiv q(x) \pmod{\pi^{k+1}}$ for all $x \in E$.

Proof. We construct u' as $u'(x) = u(x) + \pi^k v(x)$ for some linear mapping $v : E \to F$. Then

$$q'(u'(x)) = q'(u(x)) + \pi^{2k} q'(v(x)) + \pi^k b'(u(x), v(x)) \overset{!}{\equiv} q(x) \pmod{\pi^{k+1}} \text{ for all } x \in E.$$

We automatically have $\pi^{2k} q'(v(x)) \in \pi^{2k} q'(F) \subseteq \pi^{k+1} R$. So we need to achieve

$$b'(u(x), v(x)) \equiv \frac{1}{\pi^k}(q(x) - q'(u(x))) =: \tilde{q}(x) \pmod{\pi} \text{ for all } x \in E.$$

By Lemma 2.4 there is some (not necessary symmetric) bilinear form $a : E \times E \to R$ such that $a(x, x) = \tilde{q}(x)$ for all $x \in E$. Let $(x_1, \ldots, x_n)$ be some R-basis of E. By assumption there are $v_1, \ldots, v_n \in F$ such that

$$b'(u(x_i), v_j) \equiv a(x_i, x_j) \pmod{\pi} \text{ for all } 1 \leq i, j \leq n.$$

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

$$b'(u(x), v(x)) = \sum_{i,j} a_i a_j b'(u(x_i), v_j) \equiv_\pi \sum_{i,j} a_i a_j a(x_i, x_j) = a(\sum_{i=1}^n a_i x_i, \sum_{j=1}^n a_j x_j) = a(x, x) = \tilde{q}(x).$$

□

Corollary 7.6. *If additionally R is complete then there is an isometric embedding $\tilde{u} : E \to V'$ such that $\tilde{u}(x) - u(x) \in \pi^k F$ for all $x \in E$.*

Proof. The mapping u' of the statement of Theorem 7.5 satisfies

$$b'(u'(x),y) = b'(u(x),y) + \underbrace{\pi^k b'(v(x),y)}_{\pi\pi^k q'(F)\subseteq \pi R} \text{ for all } x\in E, y\in F.$$

In particular $b'_{u'}(F)+\pi E^* = b'_u(F)+\pi E^*$ and u' satisfies the assumption of Theorem 7.5 for $k+1$ instead of k. We hence can use Theorem 7.5 to construct a sequence $u^{(m)}: E\to V'$ with $u^{(0)}=u$,

$$u^{(m)}(x)\equiv u^{(m-1)}(x) \pmod{\pi^m F} \text{ and } q'(u^{(m)}(x))\equiv q(x) \pmod{\pi^{m+k}} \text{ for all } x\in E$$

Then $\tilde{u} := \lim_{m\to\infty} u^{(m)}$ is the desired isometry. □

Corollary 7.7. *Let R be complete (F,q') a regular quadratic R-module, $u:(E,q)\to(F,q')$ linear such that $\overline{u}:(\overline{E},\overline{q})\to(\overline{F},\overline{q'})$ an isometry. Then there is an isometry $\tilde{u}:(E,q)\to(F,q')$ with $\tilde{u}(x)\equiv u(x) \pmod{\pi F}$ for all $x\in E$.*
In particular if $(\overline{E},\overline{q})\cong(\overline{F},\overline{q'})$ then $(E,q)\cong(F,q')$.

Proof. The isometry $\overline{u}$ is injective, so $\overline{E}^*\cong\overline{u}(\overline{E})^*$. As we work with vector spaces, every $\overline{R}$-linear form on $\overline{u}(\overline{E})$ can be extended to $\overline{F}$, and $\overline{F}$ is regular, so

$$\overline{u}(\overline{E})^* = \overline{b'}_{\overline{u}(\overline{E})}(\overline{F}) \cong \overline{b}_{\overline{u}}(\overline{F}).$$

So u satisfies the assumptions of Theorem 7.5 for $k=1$. The corollary hence follows from Corollary 7.6. □

Corollary 7.8. *R complete, then $W(R)\cong W(\overline{R})$.*

Corollary 7.9. *Let R be complete such that $\overline{R}=\mathbb{F}_\ell$ is a finite field.*
(a) If (E,q) is a regular quadratic R-module of rank ≥ 2 and $t\in R^*$, then there is some $x\in E$ with $q(x)=t$.
(b) If (E,q) is regular or semi-regular of rank ≥ 3, then

$$(E,q) = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \perp (E_1,q_1)$$

for some regular resp. semi-regular (E_1,q_1).
(c) There are exactly two regular 2-dimensional quadratic R-modules: $\mathbb{H}(R)$ and $N(R)$, with $\overline{N(R)}=N(\mathbb{F}_\ell)=(\mathbb{F}_{\ell^2},N)$ is the unique 2-dimensional anisotropic $\mathbb{F}_\ell$ module.
(d) If ℓ is odd then either $(E,q)\cong\perp_{i=1}^n[1]$ or $(E,q)\cong\perp_{i=1}^{n-1}[1]\perp[\epsilon]$ for fixed $\epsilon\in R^*\setminus(R^*)^2$.
(e) If ℓ is even then

$$(E,q)\cong\begin{cases} [1]\perp\perp_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{if } n=2m+1 \\ \perp_{i=1}^m \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} & \text{if } n=2m \\ \perp_{i=1}^{m-1} \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} \perp N(R) & \text{if } n=2m \end{cases}$$

Proof. (a) Define $(F, q') := [t]$ so $F = Rf$ with $q'(f) = t$. We apply Corollary 7.6 with E and F interchanged. Since $\overline{E}$ is universal, there is some $y \in E$ with $\overline{q(y)} = \overline{t} \neq 0$. Then $y \notin \pi E$, so by the regularity of E, there is some $z \in E$ with $b(z, y) = 1$. Define $u : F \to E$ by $u(f) = y$. Then u satisfies the assumptions of Theorem 7.5 for $k = 1$ and we obtain an isometry $\tilde{u} : F \to E$. Put $x := \tilde{u}(f)$.
(b) By the classification of quadratic forms over finite fields, the Witt index of $(\overline{E}, \overline{q})$ is $\mathrm{ind}(\overline{E}, \overline{q}) > 0$, so

$$(\overline{E}, \overline{q}) \cong \underbrace{\langle \overline{e}_1, \overline{e}_2 \rangle}_{\cong \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix}} \perp\!\!\!\perp (\overline{E}_1, \overline{q}_1).$$

with (semi)regular $(\overline{E}_1, \overline{q}_1)$. Let $H := \mathbb{H}(R) = \begin{bmatrix} 0 & 1 \\ & 0 \end{bmatrix} = \langle h_1, h_2 \rangle$ and $u : H \to E$ defined by $u(h_i) := e_i$ $(i = 1, 2)$. Then Corollary 7.6 yields the existence of an isometric embedding $\tilde{u} : H \to (E, q)$ and the regular submodule $\langle \tilde{u}(h_1), \tilde{u}(h_2) \rangle \cong H$ splits as an orthogonal summand of (E, q). □

8 Quadratic forms over complete discrete valuated fields.

We assume that R is a complete discrete valuation ring, $K = \mathrm{Quot}(R)$, $\overline{R} = R/\pi R$. (V, q) a regular or semi-regular quadratic space over K.

Lemma 8.1. *Assume that* $\mathrm{ind}(V, q) = 0$. *For* $x, y \in V$ *with* $q(x) \in \pi^{i-1}R$, $q(y) \in \pi^i R$ *we obtain* $b(x, y) \in \pi^i R$.

Proof. Assume that $b(x, y) \notin \pi^i R$ and let $u \in R^*$ such that $b(x, y) = \pi^j u$ for some $j < i$. Replace q by $\pi^{-j} u^{-1} q$ to achieve that $q(x) \in R$, $q(y) \in \pi R$, $b(x, y) = 1$. Then $E := \langle x, y \rangle_R$ satisfies $(E/\pi E, \overline{q}) = \begin{bmatrix} \star & 1 \\ & 0 \end{bmatrix}$, so $\overline{E}$ regular and hyperbolic. Therefore $(\overline{E}, \overline{q}) \cong \mathbb{H}(\overline{R})$ and so $(E, q) \cong \mathbb{H}(R)$ is not anisotropic, contradicting the assumption that $\mathrm{ind}(V, q) = 0$. □

Theorem 8.2. *Let* $\mathrm{ind}(V, q) = 0$. *For* $i \in \mathbb{Z}$ *put*

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

Then E_i *is an* R*-lattice in* V.

Proof. By Lemma 8.1 we have for $x, y \in E_i$ also $x + y \in E_i$, so E_i is an abelian group. Clearly E_i is closed under multiplication by elements of R, so E_i is an R-module. We need to show that E_i contains a basis of V. If $(e_1, \ldots, e_n)$ is a K-basis of V, then suitable multiples of e_i are contained in E_i, therefore E_i contains a sublattice L of full rank. As $b(E_i, E_i) \subseteq \pi^i R$ we have

$$L \subseteq E_i \subseteq \pi^i E_i^{\#} \subseteq \pi^i L^{\#}$$

and so (by the main theorem on f.g. modules over principal ideal domains) E_i is a lattice in V. □

Corollary 8.3. *Let* (V, q) *be a regular or semi-regular quadratic* K*-space. Then any two maximal* R*-lattices are isometric.*

Proof. By Corollary 4.13 we can write $(V,q) = (V',q') \perp \perp^m \mathbb{H}(K)$ with $m = \operatorname{ind}(V,q)$ and (V',q') anisotropic, unique up to isometry. So any maximal R-lattice in (V,q) is isometric to $E_0(V',q') \perp \perp^m \mathbb{H}(R)$. □

We now additionally assume that $\overline{R} = R/\pi R = \mathbb{F}_\ell$ is finite. Then we know that $N(\mathbb{F}_\ell) := (\mathbb{F}_{\ell^2}, N)$ is the unique anisotropic quadratic $\mathbb{F}_\ell$-vector space of dimension 2. Let $(G,q) = N(R)$ be the regular quadratic R-module from Corollary 7.9 such that $(\overline{G},\overline{q}) = N(\mathbb{F}_\ell)$.

Lemma 8.4. *(KG,q) is an anisotropic K-vector space and $q(G) = \cup_{i=0}^{\infty} \pi^{2i} R^* \cup \{0\}$*

Proof. (KG,q) is anisotropic: Otherwise there is some $0 \neq g \in KG$ such that $q(g) = 0$. Multiplying by a suitable power of π we may achieve that $g \in G \setminus \pi G$. But then $0 \neq \overline{g} \in \overline{G}$ with $\overline{q}(\overline{g}) = 0$ contradicts the fact that $(\overline{G},\overline{q}) = N(\mathbb{F}_\ell)$ is anisotropic.
$\supseteq$: It is clearly enough to show that $R^* \subset q(G)$. So let $G = \langle e, f\rangle$, $q(xe + yf) = ax^2 + bxy + cy^2$, where we assume that $b = 0$ if $2 \in R^*$. Then the regularity of (G,q) implies that $b \in R^*$ if $2 \notin R^*$ and $ac \in R^*$ if $2 \in R^*$.
Let $u \in R^*$. Since $\overline{N(R)}$ is universal, there are $x_0, y_0 \in R$ such that $q(x_0 e + y_0 f) = ax_0^2 + bx_0y_0 + cy_0^2 \equiv u \pmod{\pi}$. As $u \in R^*$, one of x_0 or y_0 is not in πR. Wlog assume that $x_0 \notin \pi R$ if $2 \in R^*$ and $y_0 \notin \pi R$ if $2 \notin R^*$. Consider the polynomial $p(x) := ax^2 + (by_0)x + cy_0^2 - u \in R[x]$. Then $p(x_0) \in \pi R$, $p'(x_0) = 2ax_0 + by_0 \in R^*$ (by our choice in both cases). In particular by Hensel's lemma there is some $x_\infty \in R$ such that $q(x_\infty) = 0$, so $q(x_\infty e + y_0 f) = u$.
$\subseteq$: We need to show that all elements in $q(G)$ have even valuation. Clearly $G = \{g \in KG \mid q(g) \in R\}$ is the unique maximal lattice in KG. Let $g \in G$ with $q(g) = \pi^{2m+1}u$ for $u \in R^*$ such that m is minimal. Then also $q(\pi^{-m}g) = \pi u \in R$ so $\pi^{-m}g \in G$, by the maximality of G. This implies that $m = 0$ and $q(g) = \pi u$. Then $g \notin \pi G$ so $\overline{g} \neq 0$ but $\overline{q}(\overline{g}) = 0$ contradicting the fact that $N(\mathbb{F}_\ell)$ is anisotropic. □

Corollary 8.5. *$(U,q_0) := (KG,q) \perp (KG,\pi q)$ is a universal anisotropic K-vector space of dimension 4.*

Theorem 8.6. *Let (V,q) be a regular or semi-regular quadratic space over K with $\operatorname{ind}(V,q) = 0$. 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 8.2. 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 $(E_0/E_1,\overline{q}) \cong N(\mathbb{F}_\ell)$. 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 $N(\mathbb{F}_\ell)$, so $\langle e_1,e_2\rangle \cong (G,q)$ from above and $(E_0,q) \cong (G,q) \perp (G',\pi q')$ such that $(E_1/\pi E_0, \overline{\pi^{-1}q}) \cong (\overline{G'},\overline{q'}) \cong N(\mathbb{F}_\ell)$. This implies that $(G',q') \cong (G,q)$ and $(V,q) \cong (U,q_0)$. □

8.1 The Witt group of $\mathbb{Q}_p$.

Just to avoid the technical details to construct a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form from an $\mathbb{F}_\ell$-valued form we now restrict to the case that $R = \mathbb{Z}_p$ and $K = \mathbb{Q}_p$. Then we may identify K/R with a

subgroup of $\mathbb{Q}/\mathbb{Z}$,

$$\mathbb{Q}_p/\mathbb{Z}_p \cong \mathbb{Z}[\frac{1}{p}]/\mathbb{Z} \leq \mathbb{Q}/\mathbb{Z}.$$

Theorem 8.7. *We have the exact sequence*

$$0 \to W(\mathbb{Z}_p) \xrightarrow{\iota} W(\mathbb{Q}_p) \xrightarrow{\delta} WQ(p) \to 0$$

where $\delta((V,q)) = [(L^\#/L, q_L)]$ *is the homomorphism analogous to the one in Lemma 5.31 (so* $\delta([(V,q)]) = [(E_0(V,q)^\#/E_0(V,q), \overline{q})]$ *if* (V,q) *is anisotropic) and* $\iota([(L,q)]) = [(\mathbb{Q}_pL, q)]$. *This sequence is split, hence*

$$W(\mathbb{Q}_p) \cong WQ(p) \oplus W(\mathbb{Z}_p) \cong \begin{cases} C_4 \times C_4 & p \equiv -1 \pmod 4 \\ C_2^4 & p \equiv 1 \pmod 4 \\ C_2 \times C_2 \times C_8 & p = 2. \end{cases}$$

Proof. As in Section 5.4 we may define δ also on arbitrary representatives (V,q) by choosing any $\mathbb{Z}_p$-lattice $L \leq V$ such that $q(L) \subseteq \mathbb{Z}_p$ and mapping $[(V,q)] \to [(L^\#/L, \overline{q}]$.
The surjectivity is easily shown by constructing explicit preimages:
First let p be odd. Then $WQ(p) \cong W(\mathbb{F}_p) = \langle [1], [\epsilon] \rangle$. Choose $u \in \mathbb{Z}_p^*$ with $\overline{u} = \epsilon$ and define the 1-dimensional spaces (V, q_1) and (V, q_ϵ) by $V = \mathbb{Q}_p e$ with $q_1(e) := p$ resp. $q_\epsilon(e) := pu$.
For $p = 2$ a lift of ϕ_k is given by $(\mathbb{Q}_2 e, q_k)$ with $q_k(e) := k$. a lift of ψ_ℓ is $(\mathbb{Q}_2 e, q)$ with $q(e) = 2\ell$ and χ is lifted by the 2-dimensional space $(\mathbb{Q}_2 G, 2q)$. This construction also finds a left inverse to δ, showing that this sequence is split.
Moreover the map δ is a group homomorphism with $[(V,q)] \in \ker(\delta)$ if and only if there is some lattice $L \leq V$ with $q(L) \subset \mathbb{Z}_p$ and $L^\# = L$. Then (L,q) is a regular $\mathbb{Z}_p$-module and hence the kernel of this map is the Witt group of $\mathbb{Z}_p$. □

Corollary 8.8. *The explicit isomorphism is* $W(\mathbb{Q}_2) = \langle [1] \rangle \times \langle [1,-2] \rangle \times \langle [1,1,1,-3] \rangle \cong C_8 \times C_2 \times C_2$.

Proof. The Witt group of $\mathbb{Q}_2$ is generated by the one dimensional forms $[a]$ where a represents the square classes in $\mathbb{Q}_2$, so $a \in \{1,3,5,7,2,6,10,14\}$. We have $[a,b] \cong [a+b, ab(a+b)]$ for all a, b and $[1,7] \sim [3,5] \sim \mathbb{H}$ so we obtain the following relations

[1]	[3]	[5]	[7]	[2]	[6]	[10]	[14]
1	0	0	1	0	0	0	0
0	1	1	0	0	0	0	0
1	0	0	1	−1	0	0	−1
1	−1	0	0	1	−1	0	0
1	−1	0	0	0	0	1	−1
1	0	0	−1	0	1	−1	0
2	0	0	0	−2	0	0	0
0	0	2	0	0	0	−2	0

$\sim$

[1]	[3]	[5]	[7]	[2]	[6]	[10]	[14]
1	0	0	1	0	0	0	0
0	1	1	0	0	0	0	0
0	0	1	1	0	0	1	−3
0	0	0	2	0	0	0	−2
0	0	0	0	1	0	0	1
0	0	0	0	0	1	−1	−2
0	0	0	0	0	0	2	2
0	0	0	0	0	0	0	8

□

Chapter 3

Clifford algebras.

9 Construction of the Clifford algebra.

Definition 9.1. *Let (E,q) be a quadratic A-module. An A-algebra $\mathcal{C} := \mathcal{C}(E,q)$ together with an A-module homomorphism $g : E \to \mathcal{C}$ is called a* **Clifford algebra**, *if*

(a) For all $x \in E$ we have $g(x)^2 = q(x)1_{\mathcal{C}}$ and

(b) For any A-algebra B and any A-module homomorphism $f : E \to B$ with $f(x)^2 = q(x)1_B$ there is a unique A-algebra homomorphism $\varphi : \mathcal{C} \to B$ such that $\varphi \circ g = f$.

Remark 9.2. *In $\mathcal{C}(E,q)$ we have $g(x)^2 = q(x)$ so for any $x, y \in E$ we compute*

$$g(x)g(y) + g(y)g(x) = (g(x) + g(y))^2 - g(x)^2 - g(y)^2 = q(x+y) - q(x) - q(y) = b_q(x,y).$$

In particular $g(x)g(y) = -g(y)g(x)$ if $x \perp y$.

Theorem 9.3. *For any quadratic A-module (E,q) there is a Clifford algebra $\mathcal{C}(E,q)$. This Clifford algebra is unique up to A-algebra isomorphism.*

Proof. The uniqueness follows from the universal property: If $(\mathcal{C}_1, g_1)$ and $(\mathcal{C}_2, g_2)$ are two Clifford algebras for (E,q), then there are unique A-algebra homomorphisms $\varphi_1 : \mathcal{C}_1 \to \mathcal{C}_2$ and $\varphi_2 : \mathcal{C}_2 \to \mathcal{C}_1$ with $\varphi_1 \circ g_1 = g_2$ and $\varphi_2 \circ g_2 = g_1$. So $g_1 = \varphi_2 \circ \varphi_1 \circ g_1$ and both mappings $\mathrm{id}_{\mathcal{C}_1}$ and $\varphi_2 \circ \varphi_1$ are algebra homomorphisms $\varphi : \mathcal{C}_1 \to \mathcal{C}_1$ such that $\varphi \circ g_1 = g_1$. By the universal property of $\mathcal{C}_1$ this yields $\varphi_2 \circ \varphi_1 = \mathrm{id}_{\mathcal{C}_1}$. Similarly $\varphi_1 \circ \varphi_2 = \mathrm{id}_{\mathcal{C}_2}$, so $\varphi_1^{-1} = \varphi_2$ are algebra isomorphisms.
Existence: Let $\{e_i : i \in S\}$ be some generating set of E and let D be the free A-module with basis

$$\{[e_{i_1}, \ldots, e_{i_r}] \mid r \in \mathbb{N}_0, i_1, \ldots, i_r \in S\}$$

Then D becomes an A-algebra by putting

$$[e_{i_1}, \ldots, e_{i_r}] \cdot [e_{j_1}, \ldots, e_{j_s}] := [e_{i_1}, \ldots, e_{i_r}, e_{j_1}, \ldots, e_{j_s}].$$

Then $1_D = []$. Let $I \trianglelefteq D$ be the 2-sided ideal generated by

- $\sum a_i[e_i]$, if $\sum a_i e_i = 0$ in E.
- $[e_i]^2 - q(e_i)[]$ for all $i \in S$.
- $[e_i, e_j] + [e_j, e_i] - b_q(e_i, e_j)[]$ for all $i, j \in S$.

Put $\mathcal{C} := D/I$ and $g : E \to \mathcal{C}$, $g(e_i) := [e_i] + I$. Then

$$g(\sum a_i e_i)^2 = \sum a_i^2 [e_i]^2 + \sum_{i \neq j} a_i a_j ([e_i, e_j] + [e_j, e_i]) + I$$
$$= \sum a_i^2 q(e_i)[] + \sum_{i \neq j} a_i a_j b_q(e_i, e_j)[] + I = q(\sum a_i e_i)[] + I$$

so $g(e)^2 = q(e)1_{\mathcal{C}}$ for all $e \in E$. We need to show the universal property for $\mathcal{C}$. So let B be some A-algebra and $f : E \to B$ an A-module homomorphism with $f(e)^2 = q(e)1_B$ for all $e \in E$. Define $\tilde{\varphi} : D \to B$ by $\tilde{\varphi}([e_i]) = f(e_i)$ for all $i \in S$. Since D is the free A-algebra on the $\{[e_i] : i \in S\}$ this defines a unique A-algebra homomorphism. We show that $\tilde{\varphi}(I) = \{0\}$.

- $\tilde{\varphi}(\sum a_i[e_i]) = \sum a_i f(e_i) = f(\sum a_i e_i) = 0$, if $\sum a_i e_i = 0$ in E.
- $\tilde{\varphi}([e_i]^2 - q(e_i)[]) = \tilde{\varphi}([e_i]^2) - q(e_i)\tilde{\varphi}([]) = f(e_i)^2 - q(e_i)1_B$ for all $i \in S$.
- $\tilde{\varphi}([e_i, e_j] + [e_j, e_i] - b_q(e_i, e_j)[]) = f(e_i)f(e_j) + f(e_j)f(e_i) - b_q(e_i, e_j)1_B = 0$ for all $i, j \in S$.

So $I \subseteq \ker(\tilde{\varphi})$ so there is some A-algebra homomorphism $\varphi : \mathcal{C} \to B$ such that $\varphi(x + I) = \tilde{\varphi}(x)$ for all $x \in D$. The uniqueness of φ follows from the fact that the $[e_i]+I$ generate the A-algebra $\mathcal{C}$. □

Remark 9.4. *If S is ordered (in our cases S will be finite), then*

$$\mathcal{C} = \langle g(e_{i_1}) \cdots g(e_{i_r}) \mid r \in \mathbb{N}_0, i_1 < \ldots < i_r \rangle.$$

Remark 9.5. *$D = D_0 \oplus D_1$ as an A-module, where*

$$D_0 = \langle [e_{i_1}, \ldots, e_{i_{2r}}] \mid r \in \mathbb{N}_0, i_j \in S \rangle_{A-module}$$

and

$$D_1 = \langle [e_{i_1}, \ldots, e_{i_{2r+1}}] \mid r \in \mathbb{N}_0, i_j \in S \rangle_{A-module}$$

We have $D_i D_j \subseteq D_{i+j}$ (indices mod 2). Let $I_i := I \cap D_i$. Then $I = I_0 \oplus I_1$, as the generators of I are homogeneous of even or odd degree, and so

$$\mathcal{C} = D/I = D_0/I_0 \oplus D_1/I_1 = \mathcal{C}_0 \oplus \mathcal{C}_1$$

with $\mathcal{C}_i \mathcal{C}_j \subseteq \mathcal{C}_{i+j}$.

Theorem 9.6. *Let $u \in O(E, q)$. Then there is a unique A-algebra automorphism $c(u) : \mathcal{C}(E, q) \to \mathcal{C}(E, q)$ such that $c(u)(g(e)) = g(u(e))$ for all $e \in E$. We have $c(-id)(x_0 + x_1) = x_0 - x_1$ for all $x_0 \in \mathcal{C}_0$, $x_1 \in \mathcal{C}_1$.*

Proof. The existence of $c(u)$ follows immediately from the universal property of $\mathcal{C}(E, q)$ applied to the homomorphism $f : E \to \mathcal{C}(E, q), e \mapsto g(u(e))$. We have $c(u^{-1})c(u) = \mathrm{id}_{\mathcal{C}}$ so $c(u)$ is an automorphism □

Example 9.7. *Let $e \in E$ such that $q(e) \in A^*$. Then $g(e)^{-1} = q(e)^{-1} g(e)$, so $g(e) \in \mathcal{C}^*$ and $c(-s_e)(x) = g(e)xg(e)^{-1}$ for all $x \in \mathcal{C} = \mathcal{C}(E, q)$.*
To see this it is enough to compute $c(-s_e)(g(a))$ for $a \in E$.

$$g(e)g(a)g(e)^{-1} = (-g(a)g(e) + b_q(a, e))g(e)^{-1} = -g(a) + b_q(a, e)q(e)^{-1}g(e) = -g(s_e(a)).$$

Theorem 9.8. *There is a unique A-algebra anti automorphism $\iota : \mathcal{C}(E,q) \to \mathcal{C}(E,q)$ such that $\iota(g(e)) = g(e)$ for all $e \in E$. We compute $\iota(g(e_{i_1}) \cdots g(e_{i_r})) = g(e_{i_r}) \cdots g(e_{i_1})$ and $\iota^2 = \mathrm{id}$.*

Proof. This follows from the universal property of $\mathcal{C} := \mathcal{C}(E,q)$ applied to the A-algebra $B = \mathcal{C}^{op}$ (which is $\mathcal{C}$ as an A-module with multiplication $a \star b = ba$ for all $a, b \in \mathcal{C}$ and $f = g : E \to B$. $\square$

Example 9.9.

- *Let $E = Ae$ be free of rank 1, $q(e) = a \in A$. Then $\mathcal{C}(E,q) \cong A[X]/(X^2 - a)$.*
- *If $E = [a,b]$ is free of rank 2 with orthogonal basis (e_1, e_2), $q(e_1) = a$, $q(e_2) = b$, then*

$$\mathcal{C}(E,q) = \langle 1, g(e_1), g(e_2), g(e_1)g(e_2) \rangle_{A-module}$$

with $g(e_1)g(e_2) = -g(e_2)g(e_1)$. The mapping $\mathcal{C}(E,q) \to A^{4\times 4}$, defined by

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

is an A-algebra monomorphism, whose image is a free A-module of rank 4, so $\mathcal{C}(E,q)$ is free of rank 4.

Theorem 9.10. *If E is a free A-module with basis $(e_1, \ldots, e_r)$, then $\mathcal{C}(E,q)$ is a free A-module of rank 2^r with basis*

$$\mathcal{G} := (g(e_{i_1}) \cdots g(e_{i_s}) : s \in \mathbb{N}_0, 1 \le i_1 < \ldots < i_s \le r)$$

By Remark 9.4 this is always a generating set as an A-module. So we need to show the A-linear independence of these products. For this we need some preparation:

Definition 9.11. *(graded tensor product) Let $C = C_0 \oplus C_1$ and $D := D_0 \oplus D_1$ be two A-algebras such that*

$$C_i C_j \subseteq C_{i+j},\ D_i D_j \subseteq D_{i+j}, i, j, i+j \in \{0,1\} = \mathbb{F}_2$$

Then the **graded tensor product** *is defined as*

$$C \hat{\otimes} D = C \otimes D \text{ as } A\text{-module}$$

with multiplication

$$(c_i \otimes d_j)(c'_\ell \otimes d'_k) = (-1)^{\ell j} c_i c'_\ell \otimes d_j d'_k.$$

Remark 9.12. *The graded tensor product $C \hat{\otimes} D$ is a C_2-graded algebra with*

$$(C \hat{\otimes} D)_0 = C_0 \otimes D_0 \oplus C_1 \otimes D_1 \text{ and } (C \hat{\otimes} D)_1 = C_0 \otimes D_1 \oplus C_1 \otimes D_0.$$

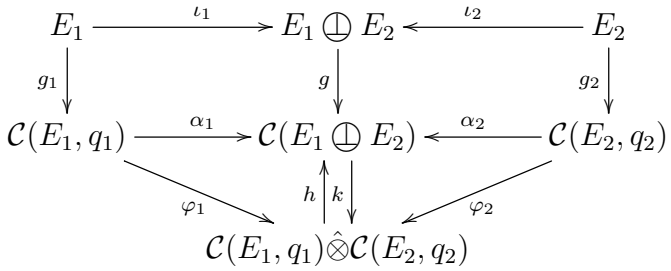
The mapping $g_C : C \to C \hat{\otimes} D, c \mapsto c \otimes 1$ resp. $g_D : D \to C \hat{\otimes} D, d \mapsto 1 \otimes d$ have the following universal property: If $K = K_0 \oplus K_1$ is another C_2-graded A-algebra and $f_C : C \to K, f_D : D \to K$ are graded A-algebra homomorphisms such that

$$\star f_C(c_i) f_D(d_j) = (-1)^{ij} f_D(d_j) f_C(c_i) \text{ for all } i.j \in \{0,1\}, c_i \in C_i, d_j \in D_j$$

then there is a unique graded A-algebra homomorphism $h : C \hat{\otimes} D \to K$ with $h \circ g_C = f_C$ and $h \circ g_D = f_D$. (h is uniquely defined on the generators by $h(c \otimes 1) = f_C(c)$ and $h(1 \otimes d) = f_D(d)$.)

Theorem 9.13. $\mathcal{C}((E_1,q_1)\perp\!\!\!\perp(E_2,q_2)) \cong \mathcal{C}(E_1,q_1)\hat{\otimes}\mathcal{C}(E_2,q_2)$.

Proof.



Let $\iota_i : E_i \to E_1 \perp\!\!\!\perp E_2 =: (E,q)$ be the obvious embedding, g, g_1, g_2 the homomorphisms of E, E_1, E_2 into their Clifford algebras. Then $f_1 := g \circ \iota_1 : E_1 \to \mathcal{C}(E,q)$ satisfies $f_1(x)^2 = q_1(x)$ for all $x \in E_1$, so by the universal property of $\mathcal{C}(E_1,q_1)$ there is a unique $\alpha_1 : \mathcal{C}(E_1,q_1) \to \mathcal{C}(E,q)$ such that $\alpha_1 \circ g_1 = g \circ \iota_1$. Similarly we get $\alpha_2 : \mathcal{C}(E_2,q_2) \to \mathcal{C}(E,q)$. We compute

$$\alpha_1(g_1(e_1))\alpha_2(g_2(e_2)) = -\alpha_2(g_2(e_2))\alpha_1(g_1(e_1)) \text{ for all } e_i \in E_i.$$

As the $g_i(e_i)$ generate the algebra $\mathcal{C}(E_i,q_i)$, the algebra homomorphisms α_i satisfy condition $\star$ from Remark 9.12. Because of the universal property of the graded tensor product, there is a unique algebra homomorphism $h : \mathcal{C}(E_1,q_1)\hat{\otimes}\mathcal{C}(E_2,q_2) \to \mathcal{C}(E,q)$ with $h \circ \varphi_i = \alpha_i$.
We now show that h is an isomorphism. Consider

$$f : E_1 \perp E_2 \to \mathcal{C}(E_1,q_1)\hat{\otimes}\mathcal{C}(E_2,q_2), f(e_1+e_2) := \varphi_1(g_1(e_1)) \otimes 1 + 1 \otimes \varphi_2(g_2(e_2)).$$

Then

$$\begin{aligned}
&f(e_1+e_2)^2 = (\varphi_1(g_1(e_1)) \otimes 1 + 1 \otimes \varphi_2(g_2(e_2)))^2 = \\
&(\varphi_1(g_1(e_1)) \otimes 1)^2 + (1 \otimes \varphi_2(g_2(e_2)))^2 + (\varphi_1(g_1(e_1)) \otimes 1)(1 \otimes \varphi_2(g_2(e_2))) + (1 \otimes \varphi_2(g_2(e_2)))(\varphi_1(g_1(e_1)) \otimes 1) \\
&= \varphi_1(g_1(e_1)^2) \otimes 1 + 1 \otimes \varphi_2(g_2(e_2)^2) + \varphi_1(g_1(e_1)) \otimes \varphi_2(g_2(e_2)) - \varphi_1(g_1(e_1)) \otimes \varphi_2(g_2(e_2)) \\
&= (q_1(e_1) + q_2(e_2))1 \otimes 1.
\end{aligned}$$

So by the universal property for $\mathcal{C}(E,q)$ there is some $k : \mathcal{C}(E,q) \to \mathcal{C}(E_1,q_1)\hat{\otimes}\mathcal{C}(E_2,q_2)$ with $k \circ g \circ \iota_i = \varphi_i \circ g_i$ for $i = 1,2$. Then $h \circ k = \mathrm{id}$ and $k \circ h = \mathrm{id}$ again by the universal property. □

Corollary 9.14. *If $(E,q) = [a_1,\ldots,a_r]$ is a free A-module with orthogonal basis $(e_1,\ldots,e_r)$, then $\mathcal{C}(E,q)$ is a free A-module with basis $(g(e_{i_1})\cdots g(e_{i_s}) \mid s \in \mathbb{N}_0, 1 \le i_1 < \ldots < i_s \le r)$. So Theorem 9.10 is true for free A-modules with orthogonal basis and hence in particular for all rings A, such the $2 \in A^*$.*

Corollary 9.15. *Theorem 9.10 is true if A is an integral domain with* $\mathrm{char}(A) = 0$.

Proof. Let $B = \mathrm{Quot}(A)$, $E = \bigoplus Ae_i$, $BE = \bigoplus Be_i$. Then $\mathrm{char}(B) \neq 2$ so BE has some orthogonal basis $(e_1,\ldots,e_r) \in E^r$, and $\mathcal{C}(BE,q)$ is a free B-module with basis $\mathcal{G} := (g(e_{i_1})\cdots g(e_{i_s}) \mid s \in \mathbb{N}_0, 1 \le i_1 < \ldots < i_s \le r)$. The elements of $\mathcal{G}$ are also linearly independent over A, so the rank of $\mathcal{C}(E,q)$ is at least 2^r. But it is generated by 2^r elements, so therefore it is free on these 2^r elements. □

Proof. (of Theorem 9.10 in the general case) Let $(a_i : i \in S)$ be some generating set of the ring A (recall that A is commutative), $\tilde{A} := \mathbb{Z}[\lambda_i : i \in S]$, $f : \tilde{A} \to A, \lambda_i \mapsto a_i$ and $I = \ker(f)$, then

$A = \tilde{A}/I$. Let (E, q) be a free quadratic A-module with basis $(e_1, \ldots, e_r)$, $(\tilde{E}, \tilde{q})$ the free quadratic $\tilde{A}$-module with basis $(\tilde{e}_1, \ldots, \tilde{e}_r)$, and $\tilde{q}$ some quadratic form on $\tilde{E}$ that satisfies

$$\tilde{q}(\sum_{i=1}^{r} \tilde{x}_i \tilde{e}_i) + I = q(\sum_{i=1}^{r} (\tilde{x}_i + I) e_i).$$

Such a quadratic form can be constructed by choosing preimages in $\tilde{A}$ of the entries of the Gram matrix

$$\begin{bmatrix} q(e_1) & & b_q(e_i, e_j) \\ & \ddots & \\ & & q(e_r) \end{bmatrix}.$$

By the corollary above $\mathcal{C}(\tilde{E}, \tilde{q})$ is a free $\tilde{A}$-module with basis $\tilde{\mathcal{G}} := (\tilde{g}(\tilde{e}_{i_1}) \cdots \tilde{g}(\tilde{e}_{i_s}) \mid s \in \mathbb{N}_0, 1 \leq i_1 < \ldots < i_s \leq r)$. Therefore $\tilde{\mathcal{G}} + I = (\tilde{x} + I \mid x \in \tilde{\mathcal{G}})$ is an A-basis of $\mathcal{C}(\tilde{E}, \tilde{q})/I\mathcal{C}(\tilde{E}, \tilde{q}) =: \overline{\mathcal{C}}$. The mapping $f : E \to \overline{\mathcal{C}}$ defined by

$$f(\sum_{i=1}^{r} x_i e_i) := \sum_{i=1}^{r} \tilde{x}_i \tilde{g}(\tilde{e}_i) + I\mathcal{C}(\tilde{E}, \tilde{q})$$

is well defined, independent of the choice of the preimage $\tilde{x}_i$ of x_i and satisfies $f(e)^2 = q(e)1 \in \overline{\mathcal{C}}$ for all $e \in E$. By the universal property of $\mathcal{C}(E, q)$ there is some A-algebra homomorphism $\varphi : \mathcal{C}(E, q) \to \overline{\mathcal{C}}$ with $\varphi(g(\sum x_i e_i)) = f(\sum x_i e_i)$ In particular we compute

$$\varphi(g(e_{i_1}) \cdots g(e_{i_s}) = \tilde{g}(\tilde{e}_{i_1}) \cdots \tilde{g}(\tilde{e}_{i_s}) + I\mathcal{C}(\tilde{E}, \tilde{q})$$

so $\varphi(\mathcal{G}) = \tilde{G} + I\mathcal{C}(\tilde{E}, \tilde{q})$ is linearly independent. Therefore also $\mathcal{G}$ is linearly independent. This concludes the proof of Theorem 9.10. □

Corollary 9.16. *If (E, q) is a f.g. projective quadratic A-module, then $g : E \to \mathcal{C}(E, q)$ is injective.*

Proof. Write E as a direct summand of a free A-module of finite rank and extend q to some quadratic form on the free module. Then by Theorem 9.10 the corresponding map g from the free module in the Clifford algebra is injective and so is its restriction $g : E \to \mathcal{C}(E, q)$. □

In the following we will hence identify E with $g(E)$ and write $e_1 e_2$ instead of $g(e_1)g(e_2)$. We also have $A \cong A1_{\mathcal{C}} \subseteq \mathcal{C}(E,q)$.

Remark 9.17. *Let (E, q) be some f.g. free quadratic A-module, $a \in A^*$.*

(i) $\mathcal{C}_0(E, q) \cong \mathcal{C}_0(E, aq)$ via $h : \mathcal{C}_0(E, aq) \to \mathcal{C}_0(E, q), h(xy) = axy$ for all $x, y \in E$.

(ii) If $F = E \perp\!\!\!\perp \langle f \rangle$ with $q(f) = -a$ then $h : \mathcal{C}(E, aq) \to \mathcal{C}_0(F, q)$ defined by $x \mapsto xf$ for all $x \in E$ is an A-algebra isomorphism.

Proof. As an exercise. □

9.1 Some examples of Clifford algebras

Definition 9.18. *Let B be an A-algebra. Then an A-algebra antiautomorphism $^-$ is called a* **canonical involution**, *if*

$$t(x) := x + \overline{x} \in A \text{ and } n(x) := x\overline{x} \in A \text{ for all } x \in B.$$

Remark 9.19. *Let B be an A-algebra with a canonical involution $^-$, $x, y \in B$.*

- $\overline{\overline{x}} = \overline{t(x) - x} = t(x) - \overline{x} = x$
- $x^2 - t(x)x + n(x) = 0$.
- $n(xy) = xy\overline{xy} = xy\overline{yx} = n(x)n(y)$.
- $n(x+y) = (x+y)(\overline{x}+\overline{y}) = x\overline{x} + y\overline{y} + x\overline{y} + y\overline{x} = n(x) + n(y) + t(x\overline{y})$
- $n : B \to A$ *is a quadratic form with* $b_n(x, y) = t(x\overline{y})$.

Definition 9.20. *A simple A-algebra Q with $\dim_A(Q) = 4$ that admits a canonical involution is called a* **quaternion algebra**.

Examples:
(i) $B = A^{2\times 2}$ is a quaternion algebra with $n = \det$, $t =$trace. For this define

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} := \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Then $n(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = ad - bd$, so $(A^{2\times 2}, \det) \cong \mathbb{H}(A) \perp\!\!\!\perp \mathbb{H}(A)$.
(ii) $B = A[X]/(X^2 - aX + b)$, $x := X + (X^2 - aX + b)$, $(1, x)$ is an A-basis of B and $^- : B \to B, \overline{\alpha + \beta x} := \alpha + \beta(a - x)$ is a canonical involution with $(B, n) \cong \begin{bmatrix} 1 & a \\ & b \end{bmatrix}$. (B, n) is regular, if and only if $a^2 - 4b \in A^*$.

Remark 9.21. *Let (E, q) be some free quadratic A-module. If $\mathcal{C}(E, q)$ has a canonical involution $^-$, then*

$$\overline{a} = \iota(c(-\mathrm{id})(a)) \text{ for all } a \in \mathcal{C}(E, q).$$

Proof. For $x \in E$ we compute $x^2 - q(x) = 0$, so $^- : \mathcal{C} \to \mathcal{C}$ satisfies $\overline{x} = -x$ for all $x \in E$. As $-x = \iota(c(-\mathrm{id}))(x)$ and $\iota \circ c(-\mathrm{id})$ is an antiautomorphism, we get that $\overline{a} = \iota(c(-\mathrm{id})(a))$ for all $a \in \mathcal{C}(E, q)$. □

Example 9.22. *Let $(E, q) = \begin{bmatrix} a & b \\ & c \end{bmatrix}$ be some free quadratic A-module of rank 2 with basis (e_1, e_2). Then*

(o) $\mathcal{C}(\mathbb{H}(A)) \cong A^{2\times 2}$ by mapping the two usual generators to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ resp. $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

(i) $\mathcal{C}_0(E, q) = \langle 1, z := e_1e_2 \rangle$ with $n(z) = z\overline{z} = e_1e_2e_2e_1 = q(e_1)q(e_2) = ac$ and $t(z) = z + \overline{z} = e_1e_2 + e_2e_1 = b_q(e_1, e_2) = b$, so

$$(\mathcal{C}_0(E, q), n) \cong \begin{bmatrix} 1 & b \\ & ac \end{bmatrix}.$$

(ii) $^- = \iota \circ c(-\mathrm{id})$ *is a canonical involution on* $\mathcal{C}(E,q)$ *and*

$$(\mathcal{C}(E,q),n) = (\mathcal{C}_1,n) \perp\!\!\!\bigoplus (\mathcal{C}_0,n) \cong (E,-q) \perp\!\!\!\bigoplus (\mathcal{C}_0,n)$$

which follows from the fact that $\mathcal{C}_1 = E$ *and* $n(x) = x\overline{x} = -q(x)$ *for all* $x \in E$.

(iii) If there is some $e \in E$ *with* $a := q(e) \in A^*$, *then* $x \mapsto xe : \mathcal{C}_0 \to \mathcal{C}_1$ *is an* A*-module isomorphism with* $q(xe) = -n(xe) = -xe\overline{ex} = q(e)x\overline{x} = an(x)$ *for all* $x \in \mathcal{C}_0$, *so* $(\mathcal{C}_0, an) \cong (E,q)$.

(iv) Assume that $E^\perp = \{0\}$. *Then* $\mathcal{C}_0(E,q) = \{x \in \mathcal{C}(E,q) \mid xy = yx \text{ for all } y \in \mathcal{C}_0(E,q)\} = \mathcal{C}^{\mathcal{C}_0}$ *and* $Z(\mathcal{C}) = A$.
Clearly $\mathcal{C}_0 = \langle 1, z\rangle$ *is commutative, so we need to show that there is some* $x \in \mathcal{C}_1 = E$ *such that* $zx \neq xz$. *If* $zx = xz$, *then*

$$xe_1e_2 + e_1xe_2 = e_1e_2x + e_1xe_2 \Rightarrow b_q(x,e_1)e_2 = b_q(x,e_2)e_1.$$

As (e_1,e_2) *is a basis of* E, *this implies that* $b_q(x,e_1) = b_q(x,e_2) = 0$ *and so* $x \in E^\perp = \{0\}$.

(v) If A *is a field and* (E,q) *regular, then* $\mathcal{C}(E,q)$ *is a quaternion algebra.*
We will prove that $\mathcal{C}(E,q)$ *is simple in Lemma 10.4 below.*

10 The center of the Clifford algebra.

Definition 10.1. *Let* C *be some* A*-algebra* $B \subset C$. *Then the* **centraliser of** B **in** C *is* $C^B = \{x \in C \mid xy = yx \text{ for all } y \in B\}$.

Theorem 10.2. *Let* A *be some field of characteristic* $\neq 2$ *and* $(E,q) = [a_1,\dots,a_n] = \perp\!\!\!\bigoplus_{i=1}^n Ae_i$ *be some regular quadratic* A*-space,* $z := e_1 \dots e_n \in \mathcal{C}(E,q) =: \mathcal{C}$. *Then*

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

(b) $\mathcal{C}^{\mathcal{C}_0} = \langle 1, z\rangle \cong A[X]/(X^2 - d)$.

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

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

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 an A-basis $(1, e_1, \dots, e_n, e_1e_2, \dots, e_1e_2\cdots e_n) = (e_{i_1} \cdots e_{i_r} \mid 0 \leq r \leq n, 1 \leq i_1 < \dots < i_r \leq n)$. Define $e_J := e_{i_1} \cdots e_{i_r}$ if $J = \{i_1, \dots, i_r\}$ with $1 \leq i_1 < \dots < i_r \leq n$. Then $\mathcal{C}_0$ is generated as an A-algebra by e_ie_j $(1 \leq i < j \leq n)$. For $x := \sum_{J \subseteq \{1,\dots,n\}} x_J e_J$ we have

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

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

Theorem 10.3. *Let E be a free A-module with basis $(e_1, \ldots, e_n)$, $q : E \to A$ a quadratic form with $q(E)A = A$. Put $\mathcal{C} := \mathcal{C}(E, q)$, $\mathcal{C}_0 := \mathcal{C}_0(E, q)$, and $Z := \mathcal{C}^{\mathcal{C}_0}$. Then there is a unique A-algebra automorphism $\alpha \in \mathrm{Aut}_A(Z)$ such that*

$$xz = \alpha(z)x \text{ for all } x \in E, z \in Z.$$

Then $\alpha^2 = \mathrm{id}$ and $Z(\mathcal{C}) = \{z \in Z \mid \alpha(z) = z\}$.

Proof. Uniqueness: Let $x_i \in E$, $a_i \in A$ such that $1 = \sum_{i=1}^k a_i q(x_i)$. We have $x_i z = \alpha(z)x_i$ for all i, so

$$\sum_{i=1}^k a_i x_i z x_i = \sum_{i=1}^k a_i \alpha(z) x_i^2 = \alpha(z) \sum_{i=1}^k a_i q(x_i) = \alpha(z) \text{ for all } z \in Z \ (\star).$$

Existence: Define α by the equation $(\star)$. Then $\alpha(z) \in Z$ for all $z \in Z$ because for all $x, y \in E$, $z \in Z$ we compute

$$\begin{aligned} \alpha(z)xy = &\ \textstyle\sum_{i=1}^k a_i x_i z \underbrace{x_i x}_{\in \mathcal{C}_0} y = \sum_{i=1}^k a_i x_i x_i x z y = xzy \\ xy\alpha(z) = &\ \textstyle\sum_{i=1}^k a_i x \underbrace{y x_i}_{\in \mathcal{C}_0} z x_i = xz \sum_{i=1}^k a_i x_i x_i y = xzy \end{aligned}$$

which implies that $z \in \mathcal{C}^{\mathcal{C}_0}$ as the xy generate $\mathcal{C}_0$ as an algebra. For $x \in E$, $z \in Z$ we then compute

$$\alpha(z)x = \sum_{i=1}^k a_i x_i z \underbrace{x_i x}_{\in \mathcal{C}_0} = \sum_{i=1}^k a_i x_i^2 x z = xz.$$

Moreover $\alpha^2 = \mathrm{id}$ as

$$\alpha(\alpha(z)) = \sum_{j=1}^k a_j x_j (\sum_{i=1}^k a_i x_i z x_i) x_j = \sum_{j=1}^k a_j x_j (\sum_{i=1}^k a_i x_i x_i) x_j z = z$$

again because $x_i x_j \in \mathcal{C}_0$ commutes with z. So $\alpha^2 = \mathrm{id}$. Similarly one checks that $\alpha(z_1 z_2) = \alpha(z_1)\alpha(z_2)$:

$$\begin{aligned} &\alpha(z_1)\alpha(z_2) = (\textstyle\sum_{i=1}^k a_i x_i z_1 x_i)(\sum_{j=1}^k a_j x_j z_2 x_j) = \\ &\textstyle\sum_{i,j} a_i a_j x_i z_1 x_i x_j z_2 x_j = \sum_{i,j} a_i a_j x_i x_i x_j z_1 z_2 x_j = \sum_j a_j x_j z_1 z_2 x_j = \alpha(z_1 z_2). \end{aligned}$$

□

Examples:
If $x \in E$ is such that $q(x) \in A^*$ then $\alpha(z) = xzx^{-1}$ for all $z \in Z$.
If $E = [a_1, \ldots, a_n]$ and $Z = A[e_1 \cdots e_n] \cong A[X]/(X^2 - d)$, then $\alpha(e_1 \cdots e_n) = (-1)^{n-1} e_1 \cdots e_n$.
If $E = Ae$ then $\mathcal{C} = A \oplus Ae$ is commutative, $\mathcal{C}_0 = A$ and $\alpha = \mathrm{id}$.
If $E = Ae_1 \oplus Ae_2$ regular and $^-$ the canonical involution of $\mathcal{C}$ then α is the restriction of $^-$ to Z.

Lemma 10.4. *Let K be a field $(E, q) = \begin{bmatrix} a & b \\ & c \end{bmatrix}$ regular with basis (e_1, e_2) then $Z(E, q) = A$ and $\mathcal{C} := \mathcal{C}(E, q)$ is a simple K-algebra.*

Proof. By Example 9.22 we only need to show that $\mathcal{C} := \mathcal{C}(E,q)$ is simple. So assume that $0 \neq I \trianglelefteq \mathcal{C}$, $0 \neq x = x_0 + x_1 \in I$ so that $x_i \in \mathcal{C}_i$. If $x_1 = 0$ then replace x by xe with $e \in E$ $q(e) \neq 0$, so wlog $x_1 \neq 0$. We have that $\mathcal{C}_0 = \mathcal{C}^{\mathcal{C}_0} = \langle 1, z = e_1e_2\rangle \cong A[X]/(X^2 - bX + ac)$ and $(\overline{z} - z)^2 = (\alpha(z) - z)^2 = b^2 - 4ac \in A^*$. As $x \in I$ also $zx - xz = zx_1 - x_1z = (z - \alpha(z))x_1 \in I$ and hence $x_1 \in I$. Since (E,q) is regular, there is some $y \in E$ such that $0 \neq b_q(x_1, y) = x_1y + yx_1 \in I$, hence $1 \in I$ and so $I = \mathcal{C}$. □

Lemma 10.5. *Let $E = E_1 \perp E_2$ and $\alpha, \alpha_1, \alpha_2$ be the corresponding automorphisms of $\mathcal{C}^{\mathcal{C}_0}$, $\gamma, \gamma_1, \gamma_2 = c(-\mathrm{id})$ the automorphisms of the Clifford algebras extending $-\mathrm{id} \in O(E_i, q)$. If E_i and $\mathcal{C}(E_i)^{\mathcal{C}_0(E_i)}$ are free A-modules then*

$$\mathcal{C}(E)^{\mathcal{C}_0(E)} = \{z \in \mathcal{C}(E_1)^{\mathcal{C}_0(E_1)} \otimes \mathcal{C}(E_2)^{\mathcal{C}_0(E_2)} \mid (\alpha_1 \otimes \gamma_2)(z) = (\gamma_1 \otimes \alpha_2)(z)\}.$$

Proof. We know that $\mathcal{C}(E) = \mathcal{C}(E_1)\hat{\otimes}\mathcal{C}(E_2)$. $\mathcal{C}_0(E)$ is generated by $\mathcal{C}_0(E_1) \otimes 1$, $1 \otimes \mathcal{C}_0(E_2)$ and the products $x_1 \otimes x_2$ with $x_i \in E_i$. Let $z = \sum u_i \otimes v_i \in \mathcal{C}(E)^{\mathcal{C}_0(E)}$. As z commutes with $\mathcal{C}_0(E_1) \otimes 1$ and $1 \otimes \mathcal{C}_0(E_2)$ this implies that $u_i \in \mathcal{C}(E_1)^{\mathcal{C}_0(E_1)}$ and $v_i \in \mathcal{C}(E_2)^{\mathcal{C}_0(E_2)}$. For $x_i \in E_i$ compute

$$(x_1 \otimes x_2)z = \textstyle\sum_i (x_1 \otimes x_2)(u_i \otimes v_i) = \sum (x_1\gamma_1(u_i) \otimes x_2v_i) =$$
$$\textstyle\sum \alpha_1(\gamma_1(u_i))x_1 \otimes \alpha_2(v_i)x_2 = \sum \alpha_1(\gamma_1(u_i)) \otimes \gamma_2(\alpha_2(v_i))x_1 \otimes x_2 = (\alpha_1 \circ \gamma_1 \otimes \gamma_2 \circ \alpha_2)(z)(x_1 \otimes x_2).$$

Since $\alpha_i^2 = \gamma_i^2 = \mathrm{id}$ we see that $z \in \mathcal{C}(E)^{\mathcal{C}_0(E)}$ if $(\alpha_1 \otimes \gamma_2)(z) = (\gamma_1 \otimes \alpha_2)(z)$. Also

$$(x_1 \otimes 1)z = (\alpha_1 \otimes \gamma_2)(z)(x_1 \otimes 1) \text{ and}$$
$$(1 \otimes x_2)z = (\gamma_1 \otimes \alpha_2)(z)(1 \otimes x_2)$$

so $\alpha = (\alpha_1 \otimes \gamma_2)_{|Z} = (\gamma_1 \otimes \alpha_2)_{|Z}$. □

Lemma 10.6. *In the notation of Lemma 10.5, if $Z_i \cong A[X]/(X^2 - X + c_i) \subseteq \mathcal{C}_0(E_i)$ for $i = 1, 2$ and $(\alpha_i)_{|Z_i}$ is the canonical involution, then $Z \cong A[X]/(X^2 - X + c)$ with $c = c_1 + c_2 - 4c_1c_2$ and $\alpha_{|Z}$ is the canonical involution.*

Proof. For $i = 1, 2$ write $Z_i := A \oplus Az_i = Az_i \oplus A\alpha(z_i)$ with $z_i^2 - z_i + c_i = 0$, $\alpha_i(z_i) + z_i = 1$. Then

$$z = a_{11}z_1 \otimes z_2 + a_{12}z_1 \otimes \alpha_2(z_2) + a_{21}\alpha_1(z_1) \otimes z_2 + a_{22}\alpha_1(z_1) \otimes \alpha_2(z_2) \in Z \Leftrightarrow (\alpha_1 \otimes \gamma_2)(z) = (\gamma_1 \otimes \alpha_2)(z)$$

which yields $a_{11} = a_{22}$ and $a_{12} = a_{21}$ as $z_i \in \mathcal{C}_0(E_i)$ and hence $\gamma_i(z_i) = z_i$. So $Z = Az \oplus A\alpha(z)$ with $z = z_1 \otimes z_2 + \alpha_1(z_1) \otimes \alpha_2(z_2)$ and $\alpha(z) = z_1 \otimes \alpha_2(z_2) + \alpha_1(z_1) \otimes z_2$. We compute $z + \alpha(z) = (z_1 + \alpha(z_1)) \otimes (z_2 + \alpha(z_2)) = 1$ and $z\alpha(z) = \ldots = c_1 + c_2 - 4c_1c_2$. □

Theorem 10.7. *(a) Let (E,q) be regular and free of even rank $2m$ and write $E = \bigperp_{i=1}^m E_i$ with $E_i = Ae_{2i-1} \oplus Ae_{2i}$ such that $b_q(e_{2i-1}, e_{2i}) = 1$. Then*

$$\mathcal{C}(E)^{\mathcal{C}_0(E)} = A \oplus Az \cong A[X]/(X^2 - X + c)$$

with $z \in \mathcal{C}_0(E)$, $z + \alpha(z) = 1$, $z\alpha(z) = c$ and $(\alpha(z) - z)^2 = 1 - 4c = (-1)^m \det(e_1, \ldots, e_{2m}) \in A^*$. So here $Z(\mathcal{C}(E)) = A$ and $Z(\mathcal{C}_0(E)) = A[z]$.
(b) If F is semi-regular and free of odd rank $2m + 1$ then $F = E \perp Af$ where E is as in (a) and $q(f) = a \neq 0$. Then

$$\mathcal{C}(F)^{\mathcal{C}_0(F)} = A \oplus At \cong A[X]/(X^2 - b)$$

with $t \in \mathcal{C}_1(F)$, $\alpha = \mathrm{id}$ and $b = (-1)^m \det'(e_1, \ldots, e_{2m}, f) \in A^*$.
So here $Z(\mathcal{C}(F)) = A[t]$ and $Z(\mathcal{C}_0(F)) = A$.
Moreover $\mathcal{C}_0(F) \cong \mathcal{C}(E, -aq)$ and $\mathcal{C}(F) = \mathcal{C}_0(F) \otimes Z(\mathcal{C}(F))$.

Proof. (a) We proceed by induction on m. $m = 1$ has been done in Example 9.22 and Lemma 10.4. The induction step follows from Lemma 10.5: Write $E = E_1' \perp E_2'$ with $E_1' = \bigperp_{i=1}^{m-1} E_i$ and $E_2' = E_m$. Let $Z_i' := \mathcal{C}(E_i')^{\mathcal{C}_0(E_i')} = A \oplus Az_i$ with $z_i + \alpha_i(z_i) = 1$ and $z_i\alpha_i(z_i) = c_i$, $(-1)^{m-1}\det(e_1,\dots,e_{2m-2}) = 1-4c_1 = (\alpha_1(z_1)-z_1)^2$, $-\det(e_{2m-1},e_{2m}) = 1-4c_2 = (\alpha_2(z_2)-z_2)^2$. By Lemma 10.5 $\mathcal{C}(E)^{\mathcal{C}_0(E)} = A \oplus Az$ where $z = z_1 \otimes z_2 + \alpha_1(z_1) \otimes \alpha_2(z_2)$ satisfies $z + \alpha(z) = 1$ and $z\alpha(z) = c_1 + c_2 - 4c_1c_2 =: c$. We compute $(\alpha(z) - z)^2 = (\alpha(z) + z - 2z)^2 = (1 - 2z)^2 = 1 - 4z + 4z^2 = 1 - 4c = (1 - 4c_1)(1 - 4c_2) = (-1)^{m-1}\det(e_1,\dots,e_{2m-2})(-1)\det(e_{2m-1},e_{2m}) = (-1)^m\det(e_1,\dots,e_{2m})$.
(b) Write $z = u + ve_{2m+1} \in \mathcal{C}(F)$ where $u, v \in \mathcal{C}(E)$. By Lemma 10.5 we have $z \in \mathcal{C}(F)^{\mathcal{C}_0(F)}$ if and only if $u, v \in \mathcal{C}(E)^{\mathcal{C}_0(E)}$ satisfy $\alpha(u) = u$ and $\alpha(v) = -v$, so by (a)

$$\mathcal{C}(F)^{\mathcal{C}_0(F)} = \langle 1, t := (\alpha(z) - z)e_{2m+1}\rangle$$

where $z \in \mathcal{C}(E)^{\mathcal{C}_0(E)}$ is as in (a). We compute

$$((\alpha(z)-z)e_{2m+1})^2 \overset{z\in\mathcal{C}_0(E)}{=} (\alpha(z)-z)^2e_{2m+1}^2 = (-1)^m\det(e_1,\dots,e_{2m})q(e_{2m+1}) = (-1)^m\det'(e_1,\dots,e_{2m+1}).$$

The map $g : E \to \mathcal{C}_0(F)$, $x \mapsto xf$ satisfies $g(x)^2 = (xf)^2 = -aq(x)$ for all $x \in F$. Therefore there is a unique A-algebra homomorphism $\epsilon : \mathcal{C}(E, -aq) \to \mathcal{C}_0(F)$ extending this map. As the $(xf : x \in E)$ generate $\mathcal{C}_0(F)$ as an A-algebra, this homomorphism is surjective and hence bijective as both algebras are free of the same rank. □

Theorem 10.8. *Let A be a field, $E = (E_1, q_1) \perp (E_2, q_2)$.*
(a) If (E_1, q_1) is regular of even dimension $2m$ with basis $(e_1, \dots, e_{2m})$ then

$$\mathcal{C}(E) \cong \mathcal{C}(E_1, q_1) \otimes \mathcal{C}(E_2, dq_2) \text{ where } d = (-1)^m\det(e_1, \dots, e_{2m}).$$

(b) If (E_1, q_1) is semi-regular of odd dimension $2m + 1$ with basis $(e_1, \dots, e_{2m+1})$ then $\mathcal{C}_0(E) \cong \mathcal{C}_0(E_1, q_1) \otimes \mathcal{C}(E_2, dq_2)$ where $d = (-1)^{m+1}\det'(e_1, \dots, e_{2m+1})$.

Proof. (a) We know that $\mathcal{C}(E) = \mathcal{C}(E_1)\hat{\otimes}\mathcal{C}(E_2)$. We search a subalgebra D such that $\mathcal{C}(E_1)\hat{\otimes}\mathcal{C}(E_2) = \mathcal{C}(E_1) \otimes D$, so D commutes with $\mathcal{C}(E_1)$. We have

$$\mathcal{C}(E)^{\mathcal{C}_0(E_1)} = \mathcal{C}(E_1)^{\mathcal{C}_0(E_1)} \otimes \mathcal{C}(E_2) = Z_1 \otimes \mathcal{C}(E_2)$$

with $Z_1 = \mathcal{C}(E_1)^{\mathcal{C}_0(E_1)} \subseteq \mathcal{C}_0(E_1)$ because $\dim(E_1)$ is even. $w \in \mathcal{C}(E)^{\mathcal{C}_0(E_1)}$ lies in $\mathcal{C}(E)^{\mathcal{C}(E_1)}$ if and only if $(x \otimes 1)w = w(x \otimes 1)$ for all $x \in E_1$. Write $Z_1 = \langle z_1, \alpha_1(z_1)\rangle$ and $w = z_1 \otimes w_1 + \alpha_1(z_1) \otimes w_2$ with $w_1, w_2 \in \mathcal{C}(E_2)$. Then

$$w(x \otimes 1) = z_1x \otimes \gamma_2(w_1) + \alpha_1(z_1)x \otimes \gamma_2(w_2) = x\alpha_1(z_1) \otimes \gamma_2(w_1) + xz_1 \otimes \gamma_2(w_2)$$

and $(x \otimes 1)w = xz_1 \otimes w_1 + x\alpha_1(z_1) \otimes w_2$. We obtain equality if and only if $\gamma_2(w_1) = w_2$, i.e.

$$\mathcal{C}(E)^{\mathcal{C}(E_1)} = 1 \otimes \mathcal{C}_0(E_2) \oplus (\alpha_1(z_1) - z_1) \otimes \mathcal{C}_1(E_2) \subseteq \mathcal{C}(E_1)\hat{\otimes}\mathcal{C}(E_2)$$

The isomorphism between $\mathcal{C}(E)^{\mathcal{C}(E_1)}$ and $\mathcal{C}(E_2, dq_2)$ is given by $(1 \otimes x_1x_2) \mapsto d^{-1}x_1x_2$, $(\alpha_1(z_1) - z_1) \otimes x \mapsto x$ for all $x, x_1, x_2 \in E_2$.
(b) Write $(E_1, q_1) = \langle f\rangle \perp (E_1', q_1')$ with (E_1', q_1') regular of even dimension $2m$ and $a = q(f) \neq 0$. Then

$$\mathcal{C}_0(E) \cong \mathcal{C}((E_1', -aq_1') \perp (E_2, -aq_2)) \cong \mathcal{C}(E_1', -aq_1')\hat{\otimes}\mathcal{C}(E_2, (-1)^{m+1}\det(q_1')aq_2) \cong \mathcal{C}_0(E_1, q_1)\hat{\otimes}\mathcal{C}(E_2, \delta q_2)$$

where the first isomorphism is from Theorem 10.7 (b) writing $E = (E_1' \perp E_2) \perp Af$ and the second one from part (a) of the present theorem. The last isomorphism is again from Theorem 10.7 (b) applied to $E_1 = E_1' \perp Af$. □

Corollary 10.9. *Let A be a field, (E,q) regular or semi regular.*
(a) If $\dim(E)$ is even, then $\mathcal{C}(E,q)$ is a tensor product of quaternion algebras, $Z(\mathcal{C}(E,q)) = A$ and $Z(\mathcal{C}_0(E,q)) = \mathcal{C}(E,q)^{\mathcal{C}_0(E,q)} \cong Z$. $\mathcal{C}_0(E,q) \cong B \otimes Z$, where B is a tensor product of quaternion algebras.
(b) If $\dim(E)$ is odd, then $\mathcal{C}_0(E,q)$ is a tensor product of quaternion algebras, $Z(\mathcal{C}_0(E,q)) = A$ and $\mathcal{C}(E,q)) = Z \otimes \mathcal{C}_0(E,q)$ where $Z = \mathcal{C}(E,q)^{\mathcal{C}_0(E,q)} = Z(\mathcal{C}(E,q))$.

11 The Spin group and the Spinor Norm

Theorem 11.1. *Let (E,q) be a f.g. projective quadratic A-module. Let $\Gamma(E,q) := \{\alpha \in \mathrm{Aut}(\mathcal{C}(E,q)) \mid \alpha(E) \subseteq E\}$. Then $\gamma : \Gamma(E,q) \to O(E,q), \alpha \mapsto \alpha_{|E}$ is a group isomorphism.*

Proof. Clearly γ is a group homomorphism. We have $\gamma(c(u)) = u$ for all $u \in O(E,q)$, where $c(u) \in \mathrm{Aut}(\mathcal{C}(E,q))$ is the automorphism defined by $c(u)(e) = u(e)$ for all $e \in E$. So γ is surjective. The injectivity follows because any automorphism of $\mathcal{C}(E,q)$ is uniquely determined by its values on the generators (as an algebra), the elements of E. □

Remark 11.2. *For $\alpha \in \Gamma$ we have $\alpha(\mathcal{C}_0) \subseteq \mathcal{C}_0$ and $\alpha(\mathcal{C}_1) \subseteq \mathcal{C}_1$ so α is a graded algebra automorphism. In particular α induces an automorphism on $Z := \mathcal{C}(E,q)^{\mathcal{C}_0(E,q)}$. Put $\Gamma_0(E,q) := \{\alpha \in \Gamma(E,q) \mid \alpha_{|Z} = \mathrm{id}_{|Z}\}$. Then $\Gamma_0 \trianglelefteq \Gamma$. If (E,q) is a regular quadratic A-module over a field A, then Γ_0 is a normal subgroup of index 2 in Γ.*

Definition 11.3. *Let (E,q) be a regular or semi-regular quadratic module over an arbitrary ring A and put $Z := \mathcal{C}(E,q)^{\mathcal{C}_0(E,q)}$. Then*

$$SO(E,q) := \{u \in O(E,q) \mid c(u)_{|Z} = \mathrm{id}\} = \gamma(\Gamma_0(E,q))$$

is called the **special orthogonal group**.

Let A be a field and E be a regular quadratic A-module with basis $(e_1, \ldots, e_n)$. If $\mathrm{char}(A) \neq 2$, then we may define the special orthogonal group by

$$SO(E,q) := \{\varphi \in O(E,q) \mid \det(\varphi) = 1\} \trianglelefteq_2 O(E,q).$$

For fields of characteristic $\neq 2$ every orthogonal transformation is a product of reflections. As reflections have determinant -1, we get that $SO(E,q) = \{t \in O(E,q) \mid t = s_{f_1} \cdots s_{f_{2t}}\}$.
This definition also applies to rings of characteristic 2, however, if (E,q) is only semi-regular, say $E = E_1 \perp\!\!\!\perp Ae$ with $q(e) \in A^*$, E_1 regular, then $e \in E^\perp$ and $s_e = \mathrm{id}_E$, so any product of reflections is the product of arbitrarily many reflections.

Remark 11.4. *Let A be a field of characteristic $\neq 2$. Then $SO(E,q) = \{u \in O(E,q) \mid \det(u) = 1\} = \{u \in O(E,q) \mid u = s_{f_1} \cdots s_{f_{2t}}\}$.*

Proof. Note that any orthogonal transformation is a product of reflections and reflections have determinant 1. So any $u \in O(E,q)$ with $\det(u) = 1$ is a product of an even number of reflection. If $u = s_{f_1} \cdots s_{f_{2t}}$ then

$$c(u) = \gamma^{2t} \kappa_{f_1 \cdots f_{2t}} = \kappa_{f_1 \cdots f_{2t}}$$

is the conjugation with $f_1 \cdots f_{2t} \in \mathcal{C}_0^*$. It hence induces the identity on Z. All three descriptions yield normal subgroups of index 2 in $O(E,q)$, hence they coincide. □

Theorem 11.5. *Let (E,q) be a regular or semi-regular quadratic module over a field A. Let*

$$\begin{aligned} G &:= \{g \in \mathcal{C}(E,q)^* \mid gEg^{-1} = E\} \text{ and} \\ G_0 &:= \{g \in \mathcal{C}_0(E,q)^* \mid gEg^{-1} = E\} \end{aligned}$$

Then $\Gamma_0(E,q) = \{\kappa_g : g \in G_0\}$ where $\kappa_g : \mathcal{C} \to \mathcal{C}, x \mapsto gxg^{-1}$. The kernel of the group epimorphism $G_0 \to \Gamma_0(E,q), g \mapsto \kappa_g$ is $Z(\mathcal{C}(E,q))^* \cap \mathcal{C}_0(E,q)^* = A^*$

Proof. Let $\alpha \in \Gamma_0(E,q)$. Then $\alpha_{|\mathcal{C}_0} \in \mathrm{Aut}(\mathcal{C}_0)$.
If $Z(\mathcal{C}_0) = A$, then $\mathcal{C}_0$ is a central simple A-algebra and by the Theorem of Skolem and Noether any automorphism is inner, so there is $p \in \mathcal{C}_0^*$, such that $\alpha = \kappa_p$ on $\mathcal{C}_0$. But then $\mathcal{C} = \mathcal{C}_0 \oplus Z$ and κ_p and α both induce the identity on Z, so $\kappa_p = \alpha \in \mathrm{Aut}(\mathcal{C})$.
If $Z(\mathcal{C}_0) = Z \neq A$, then $Z(\mathcal{C}) = A$ and again by Skolem/Noether, there is some $p \in \mathcal{C}^*$ with $\kappa_p = \alpha \in \mathrm{Aut}(\mathcal{C})$. As $\kappa_p(z) = z$ for all $z \in Z$ we have $p \in \mathcal{C}^Z = \mathcal{C}_0$. □

Definition 11.6. *Let ι be the involution of $\mathcal{C}(E,q)$ defined by $\iota(e) = e$ for all $e \in E$ and define*

$$N : \mathcal{C}(E,q) \to \mathcal{C}_0(E,q), x \mapsto x\iota(x).$$

Clearly $N(e) = q(e)$ for any $e \in E$, but in general $N(c) \notin A$ for $c \in \mathcal{C}(E,q)$. However we have

Lemma 11.7. *$N(g) \in A^*$ for all $g \in G$.*

Proof. We need to show that for $g \in G$ the element $g\iota(g) \in A^*$. The first remark is that $\iota(g) \in G$. We then compute for $e \in E$

$$(g\iota(g))e(g\iota(g))^{-1} = g\iota(g)e\iota(g^{-1})g^{-1} = g\iota(g^{-1}eg)g^{-1} = g(g^{-1}eg)g^{-1} = e.$$

Therefore $g\iota(g) \in \ker(\kappa) \cap \mathcal{C}_0 = A^*$. □

Definition 11.8. *Let A be a field and (E,q) regular. For $u = \gamma(\kappa_g) \in SO(E,q)$ define the* **Spinor norm**

$$\mathrm{SN}(u) := g\iota(g) \in A^*/(A^*)^2$$

and

$$SO^+(E,q) := \{u \in SO(E,q) \mid \mathrm{SN}(u) = 1\}$$

the kernel of the Spinor norm.

Clearly: $SO^+(E,q) \trianglelefteq SO(E,q) \trianglelefteq O(E,q)$ and $SO(E,q)/SO^+(E,q)$ is isomorphic to a subgroup of $A/(A^*)^2$, in particular an elementary abelian 2-group. If we put

$$\mathrm{Spin}(E,q) := \{g \in G_0 \mid g\iota(g) = 1\}.$$

then $SO^+(E,q) = \{\gamma(\kappa_g) \mid g \in \mathrm{Spin}(E,q)\}$.

Diagramm.

Clearly: If $e, f \in E$ with $q(e)q(f) \in A^*$ then $\mathrm{SN}(s_e s_f) = q(e)q(f)(A^*)^2$.

Example 11.9. *Let A be a field and $(E,q) = \mathbb{H}(A) = \langle e, f\rangle$ with $q(e) = q(f) = 0$ and $b_q(e,f) = 1$. The only singular vectors in $\mathbb{H}(A)$ are the multiples of e and f. So any orthogonal transformation $u \in O(E,q)$ satisfies*

$$\begin{aligned} u = t_a : &\quad e \mapsto ae, f \mapsto a^{-1}f \quad \text{or} \\ u = s_{e-af} : &\quad e \mapsto af, f \mapsto a^{-1}e \end{aligned}$$

for some $a \in A^*$. We see that $SO(\mathbb{H}(A)) = \{t_a \mid a \in A^*\}$. As $t_a = s_{e-f}s_{e-af}$ we compute $\mathrm{SN}(t_a) = q(e-f)q(e-af) = a(A^*)^2$.

Exercise: Let A be a field and (E,q) be either regular or semi-regular of rank ≤ 4. Then $\mathrm{Spin}(E,q) = \{g \in \mathcal{C}_0(E,q) \mid N(g) = 1\}$.

Theorem 11.10. *Let A be a field, (E,q) a regular quadratic space. Let $g \in SO(E,q)$, $G \leq SO(E,q)$.*

- *If g has odd order then $\mathrm{SN}(g) = 1$.*
- $\mathrm{SN}(g^2) = 1$.
- *If $[G : G']$ is odd then $\mathrm{SN}(G) = \{1\}$.*
- *If $\mathrm{char}(A) \neq 2$ and $g^2 = 1$, then $\mathrm{SN}(g) = \det(E_{-1}(g), q)$, where $E_{-1}(g) = \{x \in E \mid g(x) = -x\}$.*
- *If $\mathrm{char}(A) \neq 2$ and $g^2 = -1$, then $\det(E,q) = 1$.*
- *If $\mathrm{char}(A) \neq 2$ and $[G : G']$ is odd then $\det(E_{-1}(g), q) = 1$ for all $g \in G$ with $g^2 = 1$. In particular if $-1 \in G$ and $[G : G']$ is odd then $\det(E,q) = 1$.*

Proof. Only (iv) needs a proof: Let $(e_1, \ldots, e_m)$ be an orthogonal basis of $E_{-1}(g)$. As $g \in SO(E,q)$ we have that m is even. Moreover $g = s_{e_1} \cdots s_{e_m}$ and hence $\mathrm{SN}(g) = q(e_1) \cdots q(e_m) = 2^{-m} \det(E_{-1}(g), q) = \det(E_{-1}(g), q)$. □

12 Invariants of elements of the Witt group

Recall that $W(A) = \{[(E,q)] \mid (E,q) \text{ regular }\}$ with $(E,q) \sim (E',q')$ if and only if $(E,q) \perp (E',-q')$ hyperbolic. With respect to the orthogonal sum, the set $W(A)$ becomes an abelian group.

12.1 The discriminant algebra and the Arf invariant

Let A be a commutative ring.

Definition 12.1.
- *A* **quadratic A-algebra** *B is a free (commutative) A-algebra of rank 2, $B = A[X]/(X^2 - aX + b)$. It is called* **separable**, *if $a^2 - 4b \in A^*$. We will call it* **special**, *if we may choose $a = 1$.*
- *Let $z := X + (X^2 - aX + b) \in B$. Then $\gamma : z \mapsto a - z$ is the canonical involution on B.*
- *Define a multiplication on the set of all separable quadratic A-algebras by*

$$B_1 \circ B_2 := \{x \in B_1 \otimes B_2 \mid (\gamma_1 \otimes \mathrm{id})(x) = (\mathrm{id} \otimes \gamma_2)(x)\}.$$

Remark 12.2. *The set of all isomorphism classes special separable quadratic A-algebras forms an Abelian group $Q(A)$ with $B \circ B \cong B_0 = A[X]/(X^2 - X)$ the unit element of $Q(A)$.*

Proof. Let $B_i = \langle z_i, \gamma_i(z_i) = 1 - z_i \rangle \cong A[X]/(X^2 - X + b_i)$ $(i = 1, 2)$ Then

$$B := B_1 \circ B_2 = \langle z_1 \otimes z_2 + \gamma_1(z_1) \otimes \gamma_2(z_2) =: z, \gamma(z) \rangle$$

with $\gamma := \gamma_1 \otimes \mathrm{id}$. We compute $z^2 - z + b = 0$ with $b = b_1 + b_2 - 4b_1b_2$, and $(1-4b) = (1-4b_1)(1-4b_2) \in A^*$. In particular the neutral element is B_0. We compute

$$B \circ B = A[X]/(X^2 - X + (2b - 4b^2)) \cong B_0$$

as $X^2 - X + 2b - 4b^2 = (X - 2b)(X + 2b - 1)$. □

Lemma 12.3. *Assume that A is a field of characteristic 2. Then the map $\wp : a \mapsto a^2 + a$ is $\mathbb{F}_2$-linear and its image $\wp(A) \leq A$ is a subgroup of the additive group of A and*

$$\varphi : Q(A) \to A/\wp(A) \cong \ker(\wp), A[X]/(X^2 - X + b) \mapsto b + \wp(A)$$

is a group isomorphism.

Proof. The additivity of φ is checked in the proof above, as $4b_1b_2 = 0$. So we get a group epimorphism $A \to Q(A), b \mapsto [A[X]/(X^2 - X + b)$. The kernel of this map is the set of $a \in A$ for which $X^2 - X + a$ is reducible, which are those a that are of the form $c^2 - c$ for some $c \in A$ (a zero of $X^2 - X + a$). □

Definition 12.4. *Let A be a local ring. For a regular quadratic A-module (E, q) we define the* **discriminant algebra** $d''(E, q) := \mathcal{C}(E, q)^{\mathcal{C}_0(E,q)} \in Q(A)$.
If A is a field of characteristic 2 and (E, q) a regular quadratic A-module then the **Arf invariant** *of (E, q) is $\varphi(d''(E, q)) \in A/\wp(A)$.*

Example.
Let $A = \mathbb{F}_\ell$ be a finite field of characteristic 2. Then $\ker(\wp) = \{a \in A \mid a^2 = a\} \cong \mathbb{F}_2$ so $A/\wp A \cong C_2$ and the Arf invariant of $N(\mathbb{F}_\ell)$ is the non-trivial element in $A/\wp A$.

Example:
If $(E, q) = \perp\!\!\!\perp (E_i, q_i)$ with $E_i = \langle e_{2i-1}, e_{2i}\rangle$ and $b(e_{2i-1}, e_{2i}) = 1$ then $\varphi(d''(E, q)) = \sum_i q(e_{2i-1})q(e_{2i})$.

Remark 12.5. *By Lemma 10.6 the discriminant algebra satisfies*

$$d''(E_1 \perp\!\!\!\perp E_2) = d''(E_1) \circ d''(E_2)$$

if the rank of E_1 or E_2 is even. We easily check that $d''(\mathbb{H}(A)) = B_0$ and hence get an group homomorphism

$$d'' : W_1(A) \to Q(A)$$

where $W_1(A) \leq W(A)$ is the kernel of the dimension mod 2 homomorphism. Let $W_2(A) := \ker(d'') \leq W_1(A)$.

12.2 The Clifford invariant

(The notion Clifford invariant might be historically not correct, as this was introduced by Witt, but it is easier to memorize.)

Let A be a field. Recall that the **Brauer group** of A is the group of all isomorphism classes of central A-division algebras

$$\mathrm{Br}(A) := \{[D] \mid D \text{ is an } A \text{ division algebra, } Z(D) = A\}$$

with $[D_1] \circ [D_2] = D$ if there are m, n such that $(D_1 \otimes D_2)^{n\times n} \cong D^{m\times m}$. Then $[A]$ is the unit element of this group. The multiplication is well defined, as the tensor product of two central simple A-algebras is again a central simple A-algebra and any central simple A-algebra B is isomorphic to a matrix ring of a unique division algebra $B \cong D^{m\times m}$ where D^{op} is the endomorphism ring of the unique simple B-module.

Definition 12.6. *Let (E,q) be a regular quadratic A-module. If $\dim(E)$ is even, then $c(E,q) := \mathcal{C}(E,q)$ and if $\dim(E)$ is odd, then $c(E,q) := \mathcal{C}_0(E,q)$ is a central simple A-algebra. So $c(E,q) \cong D^{m\times m}$ for some division algebra D and some m. Define the* **Clifford invariant** $\mathfrak{c}(E,q) := [D] \in \mathrm{Br}(A)$.

Clear: Let A be a field and (E,q) a regular quadratic A-module. If $\dim(E)=1$ then $c(E,q)=A$. If $\dim(E)=2$ then $c(E,q)=\mathcal{C}(E,q)$ is a central simple A-algebra of dimension 4. So this is either a division algebra or isomorphic to $A^{2\times 2}$. As $\mathcal{C}(E,q)$ carries a canonical involution, this algebra is a division algebra, if and only if the norm form of $\mathcal{C}(E,q)$ is anisotropic. As we have seen in Example 9.22 the norm form is

$$\begin{aligned}(\mathcal{C}(E,q),n) &= (\mathcal{C}_1,n)\perp(\mathcal{C}_0,n) \cong (E,-q)\perp(\mathcal{C}_0,n)\\ (\mathcal{C}_0,n) &\cong \begin{bmatrix} 1 & b \\ & ac \end{bmatrix}\\ (E,q) &\cong \begin{bmatrix} a & b \\ & c \end{bmatrix}.\end{aligned}$$

We have $\mathcal{C}(E,q)\cong A^{2\times 2}$, if and only if (E,q) represents 1 (i.e. there is some $e\in E$ with $q(e)=1$). If $\dim(E)=3$, then write $(E,q)=(E_1,q_1)\perp Af$ where $a=q(f)\in A^*$. Then $c(E,q)=\mathcal{C}_0(E,q)=\mathcal{C}(E_1,-aq_1)$ is the Clifford algebra of a regular quadratic space of dimension 2.

Theorem 12.7. *$\mathfrak{c}: W_2(A)\to Br(A)$ is a well defined group homomorphism.*

Proof. By Theorem 10.8 we have $\mathfrak{c}(E_1)\circ\mathfrak{c}(E_2)=\mathfrak{c}(E_1\perp E_2)$ if $\dim(E_i)$ is even and $d''(E_1)=1$. Moreover $\mathfrak{c}(\mathbb{H}(A))=[A]$, so the map is a well defined group homomorphism. □

$$W(A)\geq W_1(A)=\ker(\dim \pmod 2)\geq W_2(A)=\ker(d'')\geq W_3(A)=\ker(\mathfrak{c}).$$

The Witt group of $\mathbb{Q}_p$.

Example 12.8. *The invariants of the 4-dimensional anisotropic space over $\mathbb{Q}_p$.*
Let $\mathcal{U}_p = (\mathbb{Q}_pG,q)\perp(\mathbb{Q}_pG,pq)$ be the unique anisotropic space of dimension 4 over $\mathbb{Q}_p$, where (G,q) is the regular quadratic $\mathbb{Z}_p$-module with

$$(G/pG,\overline{q})\cong(N(\mathbb{F}_p))\cong(\mathbb{F}_{p^2},N).$$

Then $d''(\mathcal{U}_p)=d''((\mathbb{Q}_pG,q))d''((\mathbb{Q}_pG,pq))=d''((\mathbb{Q}_pG,q))^2=1$. Moreover

$$\mathcal{C}(\mathcal{U}_p)\cong\mathcal{C}((\mathbb{Q}_pG,q))\otimes\mathcal{C}((\mathbb{Q}_pG,dpq))$$

where $d=-\det(\mathbb{Q}_pG)$. Since (G,q) represents all elements of $\mathbb{Z}_p^*$, it also represents 1, so $\mathcal{C}((\mathbb{Q}_pG,q))\cong\mathbb{Q}_p^{2\times 2}$. But $\mathcal{C}((\mathbb{Q}_pG,dpq))=:\mathcal{Q}_p$ is a division algebra, as $(G,dpq)\cong(G,pq)$ represents exactly those elements of $\mathbb{Z}_p$ whose valuation is odd. Using the fact that all anisotropic 4-dimensional spaces are isometric to $\mathcal{U}_p$, we can also show that the Clifford algebra of any 2-dimensional regular quadratic space over $\mathbb{Q}_p$ is either isomorphic to $\mathbb{Q}_p^{2\times 2}$ or to $\mathcal{Q}_p$, which is the unique division algebra of dimension 4 over $\mathbb{Q}_p$.

We have

$$W(\mathbb{Q}_p)\cong\begin{cases} C_4\times C_4 & p\equiv 3 \pmod 4\\ (C_2\times C_2)^2 & p\equiv 1 \pmod 4\\ C_8\times C_2\times C_2 & p=2\end{cases}$$

The filtration reads as

$$\begin{array}{ll} W(\mathbb{Q}_p) & \bullet \\ & | \quad e : W(\mathbb{Q}_p)/W_1(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \\ W_1(\mathbb{Q}_p) & \bullet \\ & | \quad d : W_1(\mathbb{Q}_p)/W_2(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \cong \begin{cases} C_2 \times C_2 & p \text{ odd} \\ C_2^3 & p = 2 \end{cases} \\ W_2(\mathbb{Q}_p) & \bullet \quad = \langle [\mathcal{U}_p] \rangle \\ & | \quad c : W_2(\mathbb{Q}_p)/W_3(\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{Br}_2(\mathbb{Q}_p) = \{[\mathbb{Q}_p], [\mathcal{Q}_p]\} \cong \{1, -1\} \\ W_3(\mathbb{Q}_p) & \bullet \quad = 0 \end{array}$$

Some explicit computations

From now on we assume that A is a field and $\mathrm{char}(A) \neq 2$. We want to compute in the subgroup of the Brauer group of A that is generated by quaternion algebras.

Definition 12.9. *For $a, b \in A^*$ define the* **quaternion symbol**

$$(a, b)_A := (a, b) := \mathfrak{c}([a, b]) \in \mathrm{Br}(A).$$

Remark 12.10. *For $a, b, c, u, v \in A^*$ we have*

(i) $(a, b)_A = (b, a)_A$.

(ii) $(au^2, bv^2)_A = (a, b)_A$.

(iii) $(a, -ab)_A = (a, b)_A$.

(iv) $(a, a)_A = (a, -1)_A = (-1, a)_A$

(v) $(a, -a)_A = [A]$.

(vi) $(a, bc) = (a, b)(a, c)$

(vii) $(ab, c) = (a, c)(b, c)$

(viii) $(1, a) = (a, 1) = [A]$.

Proof. (i), (ii), clear. (iii): Put $[a, b] = \langle e \rangle \perp\!\!\!\perp \langle f \rangle$ and $[a, -ab] = \langle g \rangle \perp\!\!\!\perp \langle h \rangle$. Define $\varphi : [a, -ab] \to \mathcal{C}([a, b])$ by $\varphi(xg + yh) := xe + yef$. Then

$$\varphi(xg + yh)^2 = (xe + yef)^2 = x^2a + xye^2f + \underbrace{xyefe}_{-xye^2f} + \underbrace{y^2efef}_{-y^2e^2f^2} = x^2a - y^2ab = q(xg + yh).$$

So by the universal property of $\mathcal{C}([a, -ab])$ the A-linear map φ can be extended uniquely to an A-algebra homomorphism $\varphi : \mathcal{C}([a, -ab]) \to \mathcal{C}([a, b])$. As $\mathcal{C}([a, -ab])$ is a simple algebra and $\varphi \neq 0$, the kernel of φ is 0, so φ is an isomorphism, since both algebras have the same dimension.
(iv) follows from (iii) using (ii).
(v) $\mathcal{C}([a, -a]) = \mathcal{C}(\mathbb{H}(A)) = A^{2\times 2}$.
(vi) We want to show that

$$\mathcal{C}([a, b]) \otimes \mathcal{C}([a, c]) \cong \mathcal{C}([a, bc]) \otimes \mathcal{C}([c, -a^2c]).$$

The last factor is $(c,-a^2c)=(c,-c)=[A]$ by (ii) and (v). Let $(1,e_1,e_2,e_3)$ and $(1,f_1,f_2,f_3)$ be the standard bases of $\mathcal{C}([a,b])$ and $\mathcal{C}([a,c])$, so

$$e_1^2=a, e_2^2=b, e_3=e_1e_2=-e_2e_1; f_1^2=a, f_2^2=c, f_3=f_1f_2=-f_2f_1.$$

Put $C:=\mathcal{C}([a,b])\otimes\mathcal{C}([a,c])$ and define subalgebras

$$B:=\langle 1\otimes 1, e_1\otimes 1, e_2\otimes f_2, e_3\otimes f_2\rangle$$
$$D:=\langle 1\otimes 1, 1\otimes f_2, e_1\otimes f_3, -ce_1\otimes f_1\rangle$$

Then $B\cong\mathcal{C}([a,bc]), D\cong\mathcal{C}([c,-a^2c])$ and B and D commute. Moreover $C=\langle B,D\rangle=BD$ so

$$B\otimes D\to C, (x\otimes y)\mapsto xy$$

is a A-algebra isomorphism.
(vii) follows from (vi) and (i) and (viii) using (vii): $(a,1)=(a,1)(a,1)=[A]$. □

Theorem 12.11. *Let A be a field of characteristic $\neq 2$, $a_1,\dots,a_n\in A^*$, $n=2m$ even, $r:=m-1$, $s:=\frac{m(m-1)}{2}$. Then*
(a) $\mathfrak{c}([a_1,\dots,a_n])=\prod_{1\le j<i\le n}(a_j,a_i)(-1,\prod_{i=1}^n a_i)^r(-1,-1)^s$.
(b) $\mathfrak{c}([a_1,\dots,a_{n-1}])=\prod_{1\le j<i\le n-1}(a_j,a_i)(-1,\prod_{i=1}^{n-1} a_i)^r(-1,-1)^s$.

Proof. By induction over m. The case $m=1$ is the definition.
$m-1\Rightarrow m$: By Theorem 10.8 we have

$$\mathfrak{c}([a_1,\dots,a_n])=\mathfrak{c}([a_1,\dots,a_{n-2}])\mathfrak{c}([ba_{n-1},ba_n])$$

where $b=(-1)^{m-1}\prod_{i=1}^{n-2}a_i2^{n-2}$ or (since 2^{n-2} is a square) $b:=(-1)^{m-1}\prod_{i=1}^{n-2}a_i$.
We compute $\mathfrak{c}([ba_{n-1},ba_n])$:

$$\begin{aligned}
&((-1)^{m-1}\textstyle\prod_{i=1}^{n-2}a_ia_{n-1},(-1)^{m-1}\prod_{j=1}^{n-2}a_ja_n)=\\
&(-1,(-1)^{m-1}\textstyle\prod_{j=1}^{n-2}a_ja_n)^{m-1}\prod_{i=1}^{n-1}(a_i,(-1)^{m-1}\prod_{j=1}^{n-2}a_ja_n)=\\
&(-1,-1)^{m-1}(-1,\textstyle\prod_{j=1}^{n-2}a_j)^{m-1}(-1,a_n)^{m-1}(\prod_{i=1}^{n-2}a_i,-1)^{m-1}\prod_{i,j=1}^{n-2}(a_i,a_j)\\
&\textstyle\prod_{i=1}^{n-2}(a_i,a_n)(a_{n-1},-1)^{m-1}\prod_{i=1}^{n-2}(a_i,a_{n-1})(a_{n-1},a_n)=\\
&(-1,-1)^{m-1}(a_na_{n-1},-1)^{m-1}\textstyle\prod_{i=1}^{n-2}(a_i,a_i)\prod_{i=1}^{n-2}(a_i,a_{n-1}a_n)(a_{n-1},a_n)=\\
&(-1,-1)^{m-1}(a_na_{n-1},-1)^{m-1}(-1,\textstyle\prod_{i=1}^{n-2}a_i)\prod_{1\le i<j\le n,n-1\le j\le n}(a_i,a_j)
\end{aligned}$$

So by induction hypothesis we compute

$$\begin{aligned}
&\mathfrak{c}([a_1,\dots,a_{n-2}])\mathfrak{c}([ba_{n-1},ba_n])=\\
&\textstyle\prod_{1\le j<i\le n-2}(a_j,a_i)(-1,\prod_{i=1}^{n-2}a_i)^{r-1}(-1,-1)^{(m-1)(m-2)/2}\\
&(-1,-1)^r(a_na_{n-1},-1)^r(-1,\textstyle\prod_{i=1}^{n-2}a_i)\prod_{1\le i<j\le n,n-1\le j\le n}(a_i,a_j)=\\
&\textstyle\prod_{1\le j<i\le n}(a_j,a_i)_(-1,\prod_{i=1}^n a_i)^r(-1,-1)^s
\end{aligned}$$

To get (b) we use that $\mathfrak{c}([a_1,\dots,a_{n-1}])=\mathfrak{c}([-a_{n-1}a_1,\dots,-a_{n-1}a_{n-2}])$ by Theorem 10.8 (b) applied to $E_1=[a_{n-1}]$. We then apply part (a) of the present theorem to see that

$$\begin{aligned}
&\mathfrak{c}([-a_{n-1}a_1,\dots,-a_{n-1}a_{n-2}])=\\
&\textstyle\prod_{1\le j<i\le n-2}(-a_{n-1}a_j,-a_{n-1}a_i)(-1,\prod_{i=1}^{n-2}-a_{n-1}a_i)^{r-1}(-1,-1)^{(m-1)(m-2)/2}=\\
&\textstyle\prod_{i=1}^{n-2}(-a_{n-1},a_i)^{i-1}\prod_{j=1}^{n-2}(-a_{n-1},a_j)^{n-2-j}\prod_{1\le j<i\le n-2}(a_j,a_i)(-a_{n-1},-a_{n-1})^{(n-2)(n-3)/2}\\
&(-1,\textstyle\prod_{i=1}^{n-2}a_i)^{r-1}(-1,(-a_{n-1})^{n-2})^{r-1}(-1,-1)^{(m-1)(m-2)/2}=\\
&\textstyle\prod_{1\le j<i\le n-2}(a_j,a_i)\prod_{i=1}^{n-2}(-a_{n-1},a_i)(-1,-1)^{(m-1)(m-2)/2+(m-1)}(-1,\prod_{i=1}^{n-2}a_i)^{r-1}(-1,a_{n-1})^{m-1}=\\
&\textstyle\prod_{1\le j<i\le n-2}(a_j,a_i)\prod_{i=1}^{n-2}(a_{n-1},a_i)(-1,-1)^s(-1,\prod_{i=1}^{n-1}a_i)^r
\end{aligned}$$

□

Chapter 4

Local-Global Principles.

Let K be a global field, i.e. a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$.

Definition 12.12. *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 $\mathbb{R} =: \mathbb{Q}_\infty$.*

We want to show that isometry of quadratic spaces is a local property, so two rational quadratic spaces (E, q) and (E', q') are isometric, if and only if all their completions

$$(E \otimes \mathbb{Q}_p, q) \cong (E' \otimes \mathbb{Q}_p, q') \text{ for all } p \in \mathbb{P} \cup \{\infty\}$$

which is the weak theorem of Hasse and Minkowski. We even have the strong Theorem of Hasse and Minkowski that (E, q) is isotropic, if an only if $(E \otimes \mathbb{Q}_p, q)$ is isotropic for all $p \in \mathbb{P} \cup \{\infty\}$. So the Witt index of (E, q) is the minimum of the Witt indices over all completions.

13 The Theorem of Hasse and Minkowski.

13.1 The Witt group of $\mathbb{Q}$ revisited.

In Section 5.4 we have seen that

$$s := (\sigma, \delta_2, \sum_{p>2} \delta_p) : W(\mathbb{Q}) \to \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{p>2} W(\mathbb{F}_p)$$

is an isomorphism, where $\sigma([(E, q)])$ is the signature of the rational quadratic space (E, q), $\delta_2(E, q) \neq 0$ if and only if $v_2(\det(E, q))$ is odd, and for $p > 2$ $\delta_p(E, q) = [(L^\#/L)_p, \overline{q})] \in W(\mathbb{F}_p)$. For odd primes p, the map δ_p is defined on the 1-dimensional forms by $\delta_p([\langle pa \rangle]) = [\langle \overline{a} \rangle]$ and $\delta_p([\langle a \rangle]) = 0$ for $a \in \{1, \ldots, p-1\}$.

We also recall the Gauss sum, $\gamma : W(\mathbb{Q}) \to \langle \zeta_8 \rangle l \mathbb{C}^*$, defined by

$$\gamma([E, q]) := \frac{1}{\sqrt{|L^\#/L|}} \sum_{x+L \in L^\#/L} \exp(2\pi i q(x))$$

where L is any even lattice in E, q (so $q(L) \subseteq \mathbb{Z}$). As the Sylow p-subgroups of the finite abelian quadratic group $L^\#/L$ are orthogonal to each other, we have $\gamma = \prod_p \gamma_p$, where

$$\gamma_p(E, q) = \frac{1}{\sqrt{|\operatorname{Syl}_p(L^\#/L)|}} \sum_{x+L \in \operatorname{Syl}_p(L^\#/L)} \exp(2\pi i q(x))$$

Lemma 13.1. *Let $a \in \mathbb{Z}$ be odd. Then $\gamma_2(\langle a\rangle) = \zeta_8^a$ and*

$$\gamma_2(\langle 2a\rangle) = \begin{cases} \zeta_8 & a \equiv 1 \pmod 4 \\ \zeta_8^{-1} & a \equiv -1 \pmod 4. \end{cases}$$

Proof. Let $(E,q) = \langle a\rangle$, then $E = \langle e\rangle$ with $q(e) = \frac{a}{2}$ and $\langle 2e\rangle =: L$ is an even lattice in (E,q). Then $L^\# = \langle \frac{1}{2a}e\rangle$ and the 2-Sylow subgroup of $L^\#/L$ is generated by $\frac{1}{2}e + L$ with $q(\frac{1}{2}e) = \frac{a}{8}$ (and has order 4). So

$$\gamma_2(E,q) = \frac{1}{2}(\zeta_8^0 + \zeta_8^a + \zeta_8^{4a} + \zeta_8^{9a}) = \zeta_8^a.$$

If $(E,q) = \langle 2a\rangle$ then $E = \langle e\rangle$ with $q(e) = a$ and $L = \langle e\rangle$ is even with $L^\# = \langle \frac{1}{2a}e\rangle$. Again the 2-Sylow subgroup of $L^\#/L$ is generated by $\frac{1}{2}e + L$. Now this group has order 2 and $q(\frac{1}{2}e) = \frac{a}{4}$. So

$$\gamma_2(E,q) = \frac{1}{\sqrt{2}}(1 + \zeta_8^{2a}) = \begin{cases} \frac{1}{\sqrt{2}}(1+i) = \zeta_8 & a \equiv 1 \pmod 4 \\ \frac{1}{\sqrt{2}}(1-i) = \zeta_8^{-1} & a \equiv -1 \pmod 4. \end{cases}$$

□

Remark 13.2. *There is a unique homomorphism*

$$t := (t_\infty, t_2, \prod_{p>2} t_p) : \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{p>2} W(\mathbb{F}_p) \to \langle \zeta_8\rangle$$

such that $t \circ s = \gamma_2$, i.e. $\gamma_2([(E,q)]) = t_\infty(\sigma(E,q))t_2(\delta_2(E,q))\prod_{p>2} t_p(\delta_p(E,q))$ for all $[(E,q)] \in W(\mathbb{Q})$.

Theorem 13.3. *(a) $t_\infty(n) = \zeta_8^n$ for all $n \in \mathbb{Z} = W(\mathbb{R}) = \sigma(W(\mathbb{Q}))$.*
(b) $t_2 = 1$.
(c) $t_p(\langle 1\rangle) = \zeta_8^{p-1}$ for all primes $p > 2$.
(d) $t_p([N(\mathbb{F}_p)]) = -1$ for all primes $p > 2$.

Proof. (a) Let $u := [\langle 1\rangle] \in W(\mathbb{Q})$. Then $\gamma_2(u) = \zeta_8$ and $\delta_2(u) = \delta_p(u) = 0$ for all primes p. As $\sigma(u) = 1$ we hence have $\gamma_2(u) = t_\infty(1) = \zeta_8$. The statement follows from the fact that t_∞ is a group homomorphism.
(b) Let $u := [\langle 1, -2\rangle]$. Then $\delta_p(u) = 0$ for all $p > 2$, $\sigma(u) = 0$, $\delta_2(u) = 1$. Therefore

$$t_2(1) = \gamma_2(u) = \gamma_2(\langle 1\rangle)\gamma_2(\langle -2\rangle) = \zeta_8\zeta_8^{-1} = 1.$$

(c) Let $u := [\langle -1, p\rangle]$. Then $\delta_q(u) = 0$ for all primes $q \neq p$, $\sigma(u) = 0$, $\delta_p(u) = \langle 1\rangle$ so

$$t_p([\langle 1\rangle]) = \gamma_2(u) = \gamma_2(\langle -1\rangle)\gamma_2(\langle p\rangle) = \zeta_8^{-1}\zeta_8^p = \zeta_8^{p-1}.$$

(d) For $p \equiv 3 \pmod 4$ the statement follows from (c) as here the form $\langle 1\rangle$ generates $W(\mathbb{F}_p) \cong C_4$. In particular $N(\mathbb{F}_p) = \langle 1, 1\rangle$ and hence

$$t_p([N(\mathbb{F}_p)]) = t_p([\langle 1\rangle])^2 = \zeta_8^{2(p-1)} = -1.$$

The case $p \equiv 1 \pmod 4$ is more difficult. The strategy is to find any 2-dimensional form over $\mathbb{F}_p$ for which $t_p \neq 1$. As there are only two 2-dimensional forms ($\mathbb{H}(\mathbb{F}_p)$ and $N(\mathbb{F}_p)$), one may conclude that this form is $N(\mathbb{F}_p)$ and satisfies $t_p([N(\mathbb{F}_p)]) = -1$.
First assume that $p \equiv 5 \pmod 8$. Then consider $u = [\langle p, -2p\rangle]$. Then $\delta_q(u) = 0$ for all primes

$2 < q \neq p$, $\sigma(u) = 0$ and $\delta_p(u) = [\langle 1, -2\rangle]$ has even dimension. As $t_2 = 1$ the value $\delta_2(u)$ has no relevance. Hence

$$t_p([\langle 1, -2\rangle]) = \gamma_2(u) = \gamma_2(\langle p\rangle)\gamma_2(\langle -2p\rangle) = \zeta_8^p\zeta_8^{-1} = \zeta_8^{p-1} = \zeta_8^4 = -1.$$

From this we hence have that $\langle 1, -2\rangle$ is an anisotropic form over $\mathbb{F}_p$ and hence 2 is not a square mod p. The same computation also shows that t_p of this form is 1 for $p \equiv 1 \pmod 8$ which shows (assuming that the theorem be proved) that 2 is a square mod p. To finish the proof, we need one lemma:

Lemma 13.4. *Let $p \equiv 1 \pmod 8$ be a prime. Then there is an odd prime $q < \sqrt{p} < p$ such that p is not a square modulo q.*

Assume the lemma, let q be the prime of this lemma and consider $u = [\langle 1, -p, -q, pq\rangle] \in W(\mathbb{Q})$. Then $\gamma_2(u) = \zeta_8^(1 - p - q + pq) = 1$ because $p \equiv 1 \pmod 8$. We have $\sigma(u) = 0$, $\delta_\ell(u) = 0$ for all primes $2 < l \neq p, q$. We have

$$\begin{aligned}\delta_q(u) &= \langle -1, p\rangle = N(\mathbb{F}_q) \text{ since } p \text{ is not a square}\\ \delta_p(u) &= \langle -1, q\rangle.\end{aligned}$$

By induction we have $t_p(N(\mathbb{F}_q)) = -1$ and therefore also $t_p(\langle -1, q\rangle) = -1$. (The induction starts with $p = 17, q = 3$.) □

Proof. (of Lemma 13.4) Let m be the odd number with $m < \sqrt{p} < m + 2$ and put

$$N := \left(\tfrac{p-1^2}{4}\right)\left(\tfrac{p-3^2}{4}\right)\cdots\left(\tfrac{p-m^2}{4}\right) = \prod_{i=1,odd}^{m}\tfrac{p-i^2}{4} <$$
$$\tfrac{m+2+1}{2}\tfrac{m+2-1}{2}\tfrac{m+2+3}{2}\tfrac{m+2-3}{2}\cdots\tfrac{m+2+m}{2}\tfrac{m+2-m}{2} = (m+1)!.$$

We now show that is q is a prime with $q < \sqrt{p}$ so that p is a square mod q, then q divides N to at least the same power as it divides $(m+1)!$. This then yields a contradiction, as all prime divisors of $(m+1)!$ are $< \sqrt{p}$ and also $N < (m+1)!$. Note that $m < \sqrt{p}$ and $m + 1$ is even implies that all prime divisors of $(m+1)!$ are $< \sqrt{p}$. So let q be a prime $q < \sqrt{p}$. Then

$$v_q((m+1)!) = \sum_i \lfloor \frac{m+1}{q^i} \rfloor.$$

Now assume that p is a square modulo q. As $p \equiv 1 \pmod 8$ for any $s \in \mathbb{N}$ there is an a such that

$$(\star)\ a^2 \equiv p \pmod{4q^s}.$$

We can add $2q^s$ to a or replace a by $2q^s - a$, so there are solutions of $(\star)$ in $(0, q^s)$, $(q^s, 2q^s)$, ..., so q^s divides at least $\lfloor \frac{m+1}{q^s} \rfloor$ factors of N, so $v_q(N) \geq \sum_i \lfloor \frac{m+1}{q^i} \rfloor$. □

Recall that the Clifford invariant on $W(\mathbb{Q}_p)$ only takes two values: $[\mathbb{Q}_p]$ or $[\mathcal{Q}_p]$. Identify $\mathrm{Br}_2(\mathbb{Q}_p)$ with $\{1, -1\}$ and put $\mathfrak{c}(E, q) := -1$ iff $\mathfrak{c}(E, q) = [\mathcal{Q}_p]$.

Lemma 13.5. *Let (E, q) be a regular quadratic $\mathbb{Q}$-vector space of dimension 4 and determinant $\in (\mathbb{Q}^*)^2$. Then $t_p(\delta_p(E, q)) = \mathfrak{c}(E \otimes \mathbb{Q}_p)$ for all prime $p > 2$ (including ∞) and $\mathfrak{c}(E \otimes \mathbb{Q}_2) = \gamma_2(E, q) \in \{1, -1\}$.*

Proof. By the assumption $d''(E,q) = 1$ we get that $\mathfrak{c}(E \otimes \mathbb{Q}_p) = 1$ if and only if $E \otimes \mathbb{Q}_p \cong \mathbb{H}(\mathbb{Q}_p) \bigoplus \mathbb{H}(\mathbb{Q}_p)$. So assume that $\mathfrak{c}(E \otimes \mathbb{Q}_p) = -1$.
If $p \neq 2$ and $p \neq \infty$ then $E \otimes \mathbb{Q}_p \cong \mathcal{U}_p$ and hence $\delta_p(E) \cong N(\mathbb{F}_p)$ and so $t_p(\delta_p(E)) = -1$.
To deal with $p = \infty$ we note that (E,q) is either positive or negative definite, so $\sigma(E,q) = \pm 4$ and so $t_\infty(\sigma(E)) = \zeta_8^{\pm 4} = -1$.
Also for $p = 2$ the assumption $c(E \otimes \mathbb{Q}_2) = -1$ is equivalent to $E \otimes \mathbb{Q}_2 = \mathcal{U}_2$ (the anisotropic quadratic space of dimension 4). As γ_2 only depends on the 2-Sylow subgroup of $L^\#/L$ this invariant can be read off from $E \otimes \mathbb{Q}_2 \cong \langle 1,1,1,1\rangle$. So $\gamma_2(E,q) = \zeta_8^4 = -1$. □

Theorem 13.6. *Let (E,q) be a regular quadratic $\mathbb{Q}$-vector space. Then*

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} \mathfrak{c}(E \otimes \mathbb{Q}_p) = 1.$$

Proof. The statement is true for 1-dimensional spaces, as these have trivial Clifford invariant.
It is also true if $\dim(E) = 4$ and $d''(E) = 1$ by the preceding lemma and the fact that $\gamma_2(E,q) = \prod_{p>2} t_p(\delta_p(E,q)) t_\infty(\sigma(E,q))$..
As the Clifford invariant can be computed as a product of the Clifford invariant of 1- and 2-dimensional orthogonal summands, it is enough to handle the case of dimension 2. So let $\dim(E) = 2$ and $d := \det(E)$. Put $(E_1, q_1) := [1,d]$ a 2-dimensional space of the same determinant as E. As E_1 represents 1, we have $\mathcal{C}(E_1) = \mathbb{Q}^{2\times 2}$ and so also

$$\mathcal{C}(E_1 \otimes \mathbb{Q}_p) = \mathcal{C}(E_1) \otimes \mathbb{Q}_p = \mathbb{Q}_p^{2\times 2}.$$

Let $V := (E,q) \bigoplus (E_1, -q_1)$ so that $[V] + [(E_1,q_1)] = [(E,q)] \in W(\mathbb{Q})$. Then $[\mathcal{C}(V)] = [\mathcal{C}(E,q)]$. But V is a 4-dimensional space of determinant 1, so by the Lemma above, $\mathcal{C}(V)$ satisfies the product rule. □

13.2 The quadratic reciprocity law.

Definition 13.7. *Let p be an odd prime, $a \in \mathbb{Z}$ not divisible by p. Then put*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \equiv \square \pmod p \\ -1 & a \equiv \not\square \pmod p. \end{cases}$$

Theorem 13.8. *(Quadratic reciprocity law) (a) If p, q are odd primes then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

(b) If p is an odd prime then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

(c) If p is an odd prime then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Proof. For (a) we consider $V := \langle 1, -p, -q, pq\rangle$. Then $\mathfrak{c}(V\otimes\mathbb{R}) = 1$, $\mathfrak{c}(V\otimes\mathbb{Q}_p) = \left(\frac{q}{p}\right)$, $\mathfrak{c}(V\otimes\mathbb{Q}_q) = \left(\frac{p}{q}\right)$ and

$$\mathfrak{c}(V\otimes\mathbb{Q}_2) = \gamma_2(V) = \zeta_8^{1-p-q+pq} = \zeta_8^{(1-p)(1-q)} = (-1)^{(p-1)(q-1)/4}$$

To see (b) consider $V := \langle 1, -2, -p, 2p\rangle$. Then $\mathfrak{c}(V\otimes\mathbb{R}) = 1$, $\mathfrak{c}(V\otimes\mathbb{Q}_p) = \left(\frac{2}{p}\right)$, and

$$\mathfrak{c}(V\otimes\mathbb{Q}_2) = \gamma_2(V) = \zeta_8^{1-p}\zeta_8^{-1}\cdot\begin{cases}\zeta_8 & p\equiv 1 \pmod 4\\ \zeta_8^{-1} & p\equiv -1 \pmod 4\end{cases} = \begin{cases}\zeta_8^{1-p} & p\equiv 1 \pmod 4\\ \zeta_8^{-1-p} & p\equiv -1 \pmod 4\end{cases}$$

For the last statement let $V = \langle 1, 1, -p, -p\rangle$. Then $\mathfrak{c}(V\otimes\mathbb{R}) = 1$, $\mathfrak{c}(V\otimes\mathbb{Q}_p) = \left(\frac{-1}{p}\right)$, and

$$\mathfrak{c}(V\otimes\mathbb{Q}_2) = \gamma_2(V) = \zeta_8^{2-2p} = (-1)^{(p-1)/2}.$$

□

13.3 The Theorem by Hasse and Minkowski

Theorem 13.9. *Let (V, q) be a regular quadratic space over $\mathbb{Q}$. Then (V, q) is hyperbolic if and only if $(\mathbb{Q}_p \otimes V, q)$ is hyperbolic for all $p \in \mathbb{P}\cup\{\infty\}$.*

Proof. $\Rightarrow$ is clear.
$\Leftarrow$: Assume that $(\mathbb{Q}_p \otimes V, q)$ is hyperbolic for all $p \in \mathbb{P}\cup\{\infty\}$. Then $s([(V, q)]) = 0$ and hence $[(V, q)] = 0$ in $W(\mathbb{Q})$, which is equivalent to (V, q) hyperbolic. □

Corollary 13.10. *(Weak form of Hasse/Minkowski) Let $(V, q), (W, q')$ be regular quadratic spaces over $\mathbb{Q}$ for which $(\mathbb{Q}_p \otimes V, q) \cong (\mathbb{Q}_p \otimes W, q')$ for all $p \in \mathbb{P}\cup\{\infty\}$. Then $(V, q) \cong (W, q')$.*

Proof. $(V, q) \cong (W, q') \Leftrightarrow (V, q)\perp(W, -q')$ is hyperbolic. □

So isometry of rational quadratic spaces is a local property.

Corollary 13.11. *A regular quadratic space (V, q) over $\mathbb{Q}$ is determined up to isometry by the invariants:*

- $\dim(V)$
- $\sigma(V, q)$ *(the real signature)*
- $d(V, q)$ *the discriminant in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$*
- $\mathfrak{c}(V, q) \in \mathrm{Br}_2(\mathbb{Q})$ *the Clifford invariant.*

So we have:

$$\begin{array}{rl} W(\mathbb{Q}) & \bullet \\ & \mid\ e : W(\mathbb{Q})/W_1(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \\ W_1(\mathbb{Q}) & \bullet \\ & \mid\ d : W_1(\mathbb{Q})/W_2(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Q}^*/(\mathbb{Q}^*)^2 \cong \bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z} \\ W_2(\mathbb{Q}) & \bullet \\ & \mid\ c : W_2(\mathbb{Q})/W_3(\mathbb{Q}) \xrightarrow{\sim} \mathrm{Br}_2(\mathbb{Q}) \cong \bigoplus_{p\in\mathbb{P}} \mathbb{Z}/2\mathbb{Z} \\ W_3(\mathbb{Q}) & \bullet\ = \langle[\mathbb{E}_8 \otimes \mathbb{Q}]\rangle \\ & \mid\ \cong \mathbb{Z} \\ 0 & \bullet \end{array}$$

Theorem 13.12. *(Hasse/Minkowski) Let (V,q) be a regular quadratic space over $\mathbb{Q}$. Then* $\operatorname{ind}(V,q) > 0$ *if and only if* $\operatorname{ind}(V\otimes\mathbb{Q}_p,q)>0$ *for all* $p\in\mathbb{P}\cup\{\infty\}$.

Proof. For the proof we distinguish the cases $\dim(V)=2,3,4$ and $\dim(V)\geq 5$.
• For $\dim(V)=2$ we have $\operatorname{ind}(V,q)>0$ if and only if (V,q) is hyperbolic, so the statement follows from Theorem 13.9.
• Now let $\dim(V)=3$. Put $W:=V\perp\langle -d(V)\rangle$ where $d(V):=(-1)^{\binom{\dim(V)}{2}}\det(V)=-\det(V)$ is the discriminant of V. Then $d(W)=1$, $\dim(W)=4$. For any $p\in\mathbb{P}\cup\{\infty\}$ we have $\operatorname{ind}(W\otimes\mathbb{Q}_p)>0$, so $W\otimes\mathbb{Q}_p\cong X_p\perp\mathbb{H}(\mathbb{Q}_p)$ with $\dim(X_p)=2$, $d(X_p)=1$. As we have seen in the exercises this implies that $X_p\cong\mathbb{H}(\mathbb{Q}_p)$, so $W\otimes\mathbb{Q}_p$ is hyperbolic for all $p\in\mathbb{P}\cup\{\infty\}$, so again by Theorem 13.9 also $W\cong\mathbb{H}(\mathbb{Q})\perp\mathbb{H}(\mathbb{Q})$. Now

$$\mathbb{H}(\mathbb{Q})\perp\mathbb{H}(\mathbb{Q})\perp\langle d(V)\rangle\cong W\perp\langle d(V)\rangle\cong V\perp\langle -d(V)\rangle\perp\langle d(V)\rangle\cong V\perp\mathbb{H}(\mathbb{Q})$$

So $V\cong\mathbb{H}(\mathbb{Q})\perp\langle d(V)\rangle$ has $\operatorname{ind}(V)=1$.
• Now let $\dim(V)=4$. This is the hardest case. We try to find W such that $V\cong W\perp\mathbb{H}(\mathbb{Q})$. Put $V_p:=V\otimes\mathbb{Q}_p$. Then $\operatorname{ind}(V_p)>0$, so $V_p\cong W_p\perp\mathbb{H}(\mathbb{Q}_p)$ for some quadratic space W_p with $d(W_p)=d(V_p)$ for all primes $p\in\mathbb{P}\cup\{\infty\}$. We try to construct some 2-dimensional rational quadratic space W such that $W\otimes\mathbb{Q}_p\cong W_p$ for all $p\in\mathbb{P}\cup\{\infty\}$. Then by Theorem 13.9 we have

$$W\perp\mathbb{H}(\mathbb{Q})\cong V \text{ because these spaces are isometric locally everywhere.}$$

Let L be some $\mathbb{Z}$-lattice in V, $d:=d(L)\in\mathbb{Z}$, then $d(W_p)=d(\mathbb{Q}_p^*)^2$, so $W_p\cong\langle a_p,-da_p\rangle$ for $a_p=p^{\alpha_p}b_p\in\mathbb{Q}_p^*$ where $b_p\in\mathbb{Z}_p^*$, $\alpha_p\in\{0,1\}$ with $\alpha_p=0$ for all p not dividing $2d(L)$ (in particular $\alpha_p>0$ only for finitely many p).
We try to construct $W=\langle a,-da\rangle$ with $a=b\prod_p p^{\alpha_p}$. For all

$$p\mid 2d(L) \text{ we want that } a\equiv a_p \pmod{4p^{\alpha_p+1}\mathbb{Z}_p}$$

so $b\equiv\prod_{r\neq\infty,p}r^{-\alpha_r}b_p \pmod{4p^{\alpha_p+1}\mathbb{Z}_p}$. Then a and a_p are in the same square class in $\mathbb{Q}_p$ and hence $W\otimes\mathbb{Q}_p\cong W_p$ for all $p\mid 2d(L)$. By Dirichlet's theorem on primes in arithmetic progressions we may and will choose b such that $\pm b=q$ is a prime, where the sign is to be chosen so that $W\otimes\mathbb{R}\cong W_\infty$. Then for all primes $p\neq q$ we have $W\otimes\mathbb{Q}_p\cong W_p$, because these two spaces have the same dimension, the same determinant and the same Clifford invariant (which is $[\mathbb{Q}_p]$ if $p\not| 2bd(L)$). By the product formula we also have $\mathfrak{c}(W\otimes\mathbb{Q}_q)=\mathfrak{c}(W_q)$ and $d(W\otimes\mathbb{Q}_q)=d(W_q)$ by construction. So $W\perp\mathbb{H}(\mathbb{Q})\cong V$ by the weak Theorem of Hasse and Minkowski, in particular V contains isotropic vectors.
• The last case is $\dim(V)\geq 5$. Here we find a subspace $W\leq V$ of dimension $\dim(W)=4$ such that $W\otimes\mathbb{Q}_p$ is isotropic for all $p\in\mathbb{P}\cup\{\infty\}$. Then by the previous step W is isotropic over $\mathbb{Q}$ and hence also V.
To construct such a W let $U\leq V$ be a 3-dimensional subspace such that $U\otimes\mathbb{R}$ is isotropic. Let $L\leq U$ be an integral $\mathbb{Z}$-lattice. For all primes p that do not divide $2\det(L)$ we have that $U\otimes\mathbb{Q}_p$ is isotropic. So there are only finitely many primes p such that $\operatorname{ind}(U\otimes\mathbb{Q}_p)=0$.
Claim. For these p there is a $y_p\in V\otimes\mathbb{Q}_p$ such that $\operatorname{ind}(U\otimes\mathbb{Q}_p\perp\langle y_p\rangle)>0$.
To construct such a y_p consider 2 cases: If $\operatorname{ind}(U^\perp\otimes\mathbb{Q}_p)>0$ then $U^\perp\otimes\mathbb{Q}_p$ represents all elements of $\mathbb{Q}_p$ so we may take an arbitrary $x_p\in U\setminus\{0\}$ and choose $y_p\in U^\perp\otimes\mathbb{Q}_p$ such that $q(y_p)=-q(x_p)$. If $\operatorname{ind}(U^\perp\otimes\mathbb{Q}_p)=0$ then there is $x_p\in U\otimes\mathbb{Q}_p$ and $y_p\in U^\perp\otimes\mathbb{Q}_p$ such that $q(x_p)=-q(y_p)\neq 0$ (because $V\otimes\mathbb{Q}_p=(U\otimes\mathbb{Q}_p)\perp(U^\perp\otimes\mathbb{Q}_p)$ is isotropic). We now choose some $y\in V$ such that $y\equiv y_p \pmod{p^N}$ for N large enough. Then $W:=\langle U,y\rangle$ is the desired subspace of dimension 4. □

Corollary 13.13. *Let (V,q) be a regular quadratic space over $\mathbb{Q}$ and $t \in \mathbb{Q}^*$. Then $t \in q(V)$ if and only if $t \in q(V \otimes \mathbb{Q}_p)$ for all $p \in \mathbb{P} \cup \{\infty\}$.*

Proof. $t \in q(V \otimes \mathbb{Q}_p)$ if and only if $\mathrm{ind}(V \otimes \mathbb{Q}_p \perp [-t]) > 0$. □

Corollary 13.14. *(Meyer's theorem) Any indefinite regular quadratic space over $\mathbb{Q}$ of dimension ≥ 5 has positive Witt index.*

14 Integral quadratic forms.

14.1 Hermite's inequality

Theorem 14.1. *(Hermite inequality) Let $E \leq (V,q)$ be a $\mathbb{Z}$-lattice in the n-dimensional regular quadratic space (V,q) over $\mathbb{Q}$. Then*

$$\min(E) := \min\{|q(x)| \mid x \in E, x \neq 0\} \leq \frac{1}{2}\left(\frac{4}{3}\right)^{(n-1)/2} |\det(E)|^{1/n}.$$

Proof. Induction on $n = \dim(E)$. Let $m := \min(E)$, $d := |\det(E)|$.
For $n = 1$ we have $d = 2m$.
So let $n > 1$. If $m = 0$ then the statement is trivial. So assume $m > 0$ and choose $e_1 \in E$ with $q(e_1) = m$. Let

$$\pi : V \to e_1^{\perp}, x \mapsto x - \frac{b(x,e_1)}{2m} e_1$$

be the orthogonal projection onto $e_1^{\perp}$ and put $E' := \pi(E) = \langle \pi(e_2), \ldots, \pi(e_n)\rangle_{\mathbb{Z}}$, $m' := \min(E')$ and $d' := \det(E')$. Then $d = 2md'$.
Let $x' \in E'$. Then there is $x \in E$, $t \in [-1/2, 1/2]$ such that $x = x' + te_1$. Then $q(x) = q(x') + t^2 q(e_1)$ shows that

$$m \leq |q(x)| \leq m' + \frac{1}{4}m \text{ and hence } m \leq \frac{4}{3}m'.$$

By induction hypotheses we have $m' \leq \frac{1}{2}\left(\frac{4}{3}\right)^{(n-2)/2}\left(\frac{d}{m}\right)^{1/(n-1)}$ and hence

$$(2m)^{n-1} \leq \left(\frac{4}{3}\right)^{n-1}(2m')^{n-1} \leq \left(\frac{4}{3}\right)^{n-1}\left(\frac{4}{3}\right)^{(n-1)(n-2)/2}\frac{d}{2m} = \left(\frac{4}{3}\right)^{(n-1)n/2}\frac{d}{2m}$$

so $(2m)^n \leq \left(\frac{4}{3}\right)^{(n-1)n/2} d$ which is the statement of the theorem. □

Theorem 14.2. *For given $n, d \in \mathbb{N}$ there are only finitely many isometry classes of integral lattices E in regular quadratic $\mathbb{Q}$-spaces such that $|\det(E)| \leq d$ and $\dim(E) = n$.*

Proof. We again proceed by induction on the dimension n, where the case $n = 1$ is clear.
Now let $n > 1$ and E be some integral lattice in a regular n-dimensional space with $\det(E) \leq d$. we put $m := \min(E)$.
If $m > 0$ then choose some $e_1 \in E$ with $|q(e_1)| = m$ and put $F := \langle e_1\rangle_{\mathbb{Z}}$. If $m = 0$ then we choose some primitive vector $e_1 \in E$ such that $q(e_1) = 0$. We have $b(e_1, E) = a\mathbb{Z}$ for $a > 0$ such that $a^2 \mid |\det(E)| \leq d$, because

$$E \leq_a \tilde{E} := \langle E, \frac{1}{a}e_1\rangle \subseteq (\tilde{E})^{\#} \leq_a E^{\#}$$

Then choose $e_2 \in E$ such that $b(e_1, e_2) = a$ and put $F := \langle e_1, e_2 \rangle$. Then

$$\mathrm{Gram}(F) = \begin{pmatrix} 0 & a \\ a & c \end{pmatrix} \sim \begin{pmatrix} 0 & a \\ a & c-2a \end{pmatrix}$$

so we may assume wlog that $-a \leq c \leq a$ and hence there are only finitely many possibilities for this lattice F.
In both cases ($m > 0$ and $m = 0$) put $G := E \cap F^{\perp}$. By Theorem 3.5 $|\det(G)| \leq |\det(E)||\det(F)|$ and $\dim(G) = \begin{cases} n-1 \\ n-2 \end{cases}$. So by induction hypothesis, there are only finitely many possibilities for the lattice G. As

$$F \perp\!\!\!\perp G \subseteq E \subseteq E^{\#} \subseteq F^{\#} \perp\!\!\!\perp G^{\#}$$

we also have only finitely many possibilities for the lattice E. □

Example 14.3. *(Integral lattices of determinant ±1) Let E be an n-dimensional integral lattice of determinant ±1. As $\frac{4}{3}^2 < 2$ we have that $\min(E) = 0$ or $\min(E) = 1$ if $n \leq 5$. Hence for $n \leq 5$ all integral unimodular lattices are of the form*

$$I_{r,s,t} := < 1 >^r \perp\!\!\!\perp < -1 >^s \perp\!\!\!\perp \mathbb{H}(\mathbb{Z})^t$$

with either $r = s = 0$ and $t \leq 2$ or $t = 0$ and $r + s = n \leq 5$.

14.2 Genera of lattices.

Definition 14.4. *Two lattices $E \leq (V, q)$ and $E' \leq (V', q')$ are said to be in the same* **genus***, if and only if $E \otimes \mathbb{R} \cong E' \otimes \mathbb{R}$ and for all primes $p \in \mathbb{P}$ the p-adic lattices $E \otimes \mathbb{Z}_p \cong E' \otimes \mathbb{Z}_p$ are isometric. Notation $E \sim E'$.*

Clear By the theorem of Hasse and Minkowski we have $(V, q) \cong (V', q')$, so we usually assume that $(V, q) = (V', q')$, i.e. the lattices live in the same regular rational quadratic space.
Any genus of lattices is a union of isometry classes.

Theorem 14.5. *Every genus of lattices contains only finitely many isometry classes.*

Proof. This easily follows from the previous subsection together with the fact that $\det(E) = \det(E')$ if E and E' are in the same genus. □

Example. For $E = E^{\#}$ and $\dim(E) \leq 5$ the genus of E consists only of a single class: $\mathrm{genus}(I_{r,s,t}) = [I_{r,s,t}]$ for $r + s + 2t \leq 5$.

Example. Let $E = \langle \begin{smallmatrix} 2 & 1 \\ 1 & 12 \end{smallmatrix} \rangle$ and $E' = \langle \begin{smallmatrix} 4 & 1 \\ 1 & 6 \end{smallmatrix} \rangle$. Then $E \sim E'$ but E and E' are not isometric, because $\min(E) = 1$ and $\min(E') = 2$. To see that E and E' are in the same genus, we first note that both are even positive definite lattices of determinant 23. So they are isometric over $\mathbb{Z}_p$ for all primes $p \in \mathbb{P} \cup \{\infty\}$ except possibly for $p = 23$. For $p = 23$ we note that 2 and 4 are squares in $\mathbb{F}_{23}$, hence also in $\mathbb{Z}_{23}$, so $E \cong [1] \perp [23] \cong E'$.

Example. Let $E = \langle \begin{smallmatrix} 2 & 1 \\ 1 & 8 \end{smallmatrix} \rangle$ and $E' = \langle \begin{smallmatrix} 4 & 1 \\ 1 & 4 \end{smallmatrix} \rangle$. Then E and E' are not in the same genus, because they are not isometric over $\mathbb{Z}_3$.

In particular we have seen that isometry of lattices is not a local property. However equality of lattices is such a local property:

Theorem 14.6. *Let V be a finite dimensional rational vector space and $E \leq V$ be some fixed $\mathbb{Z}$-lattice in V. Then there is a bijection*

$$\beta : \{E' \leq V \mid E' \ \mathbb{Z}\text{-lattice}\} \to \{(E'_p)_{p\in\mathbb{P}} \mid E'_p \leq V \otimes \mathbb{Q}_p \ \mathbb{Z}_p\text{-lattice}, E'_p = E \otimes \mathbb{Z}_p \,\mathrm{faa}\, p\} =: M(E)$$

(where faa *means "for all but finitely many") defined by $\beta(E') := (E' \otimes \mathbb{Z}_p)_{p\in\mathbb{P}}$ with inverse $\gamma : (E'_p)_{p\in\mathbb{P}} \mapsto \bigcap V \cap E'_p$.*

Proof. (a) $\beta(E') \in M(E)$ for all lattices E' in V, as the base change matrix between the lattice bases of E and E' only involves finitely many primes in the denominators of the entries and the determinant.
(b) $\gamma((E'_p))$ is a lattice in V, because $E'_p = E \otimes \mathbb{Z}_p$ for all but finitely many primes p. Hence there are $a_p, b_p \in \mathbb{Z}$ such that

$$p^{a_p}(E \otimes \mathbb{Z}_p) \subseteq E'_p \subseteq p^{b_p}(E \otimes \mathbb{Z}_p)$$

with $a_p = b_p = 0$ for all but finitely many primes p. Therefore

$$(\prod p^{a_p})E = \bigcap_{p\in\mathbb{P}}((p^{a_p}E \otimes \mathbb{Z}_p) \cap V) \subseteq \bigcap_{p\in\mathbb{P}}(E'_p \cap V) = \gamma((E'_p)) \subseteq \bigcap_{p\in\mathbb{P}}((p^{b_p}E \otimes \mathbb{Z}_p) \cap V) = (\prod p^{b_p})E$$

and hence $\gamma((E'_p)_{p\in\mathbb{P}})$ is a lattice.
(c) $\gamma(\beta(E')) = E'$: This follows from the fact that $\mathbb{Z} = \bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)}$: Clearly $E' \subseteq \gamma(\beta(E'))$. To see the other inclusion let $(e'_1, \ldots, e'_n)$ be a $\mathbb{Z}$-basis of E'. Then any element of V is expressed uniquely as a rational linear combination $x = \sum_{i=1}^n a_i e'_i$. Now $x \in \gamma(\beta(E'))$ if and only if all $a_i \in \mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ for all $p \in \mathbb{P}$.
(d) $\beta(\gamma((E'_p)_{p\in\mathbb{P}})) = (E'_p)_{p\in\mathbb{P}}$: Let $E' := \gamma((E'_p)_{p\in\mathbb{P}})$ and $(e'_1, \ldots, e'_n)$ be some $\mathbb{Z}$-basis of E'. For $x \in E'_q$ there are $a_i \in \mathbb{Q}_q$ with $x = \sum_{i=1}^n a_i e'_i$, because $E'_q \leq V \otimes \mathbb{Q}_q = E' \otimes \mathbb{Q}_q$. Write $a_i = a'_i + a''_i$ with $a''_i \in \mathbb{Z}_q$, $a'_i = \frac{b_i}{q^m}$, $b_i \in \mathbb{Z}$ and $m > 0$. Then $\sum a''_i e'_i \in \mathbb{Z}_q \otimes E'$ and $x - \sum a''_i e'_i = \sum a'_i e'_i \in E'_q$. Because the $a'_i \in \mathbb{Q}$ are rational, we have $\sum a'_i e'_i \in E'_q \cap V$. For $p \neq q$ we even have that $\sum a'_i e'_i \in (\mathbb{Q} \cap \mathbb{Z}_p)E' \subseteq V \cap E'_p$ and hence $\sum a'_i e'_i \in \bigcap_p (V \cap E'_p) = E'$. Therefore $a'_i \in \mathbb{Z}$ and hence $E'_q \subseteq E' \otimes \mathbb{Z}_p$. The other inclusion is obvious. □

Theorem 14.7. *Let $E \leq (V, q)$ be a $\mathbb{Z}$-lattice in the regular rational quadratic space (V, q). Let $t \in \mathbb{Q}^*$ be such that $t \in q(E \otimes \mathbb{R})$ and $t \in q(E \otimes \mathbb{Z}_p)$ for all $p \in \mathbb{P}$. Then there is some lattice E' in the genus of E such that $t \in q(E')$.*

Note that t is not necessarily represented by E itself as the example $t = 1$ and $E = \langle \begin{smallmatrix} 4 & 1 \\ 1 & 6 \end{smallmatrix} \rangle$ shows. Also if E does no represent 1, it represents 1 everywhere locally and $E' = \langle \begin{smallmatrix} 2 & 1 \\ 1 & 12 \end{smallmatrix} \rangle$ in the genus of E represents 1.
Proof. We first observe that $t \in q(V \otimes \mathbb{Q}_p)$ for all $p \in \mathbb{P} \cup \{\infty\}$. So by the Theorem of Hasse and Minkowski there is some $x \in V$ with $q(x) = t$. Write $x = \sum_{i=1}^n a_i e_i$ where $(e_1, \ldots, e_n)$ is some $\mathbb{Z}$-basis of E. Let S be the set of primes that divide the denominator of some of the a_i. Then $|S| < \infty$ and $x \in E \otimes \mathbb{Z}_p$ for $p \notin S$. For $p \in S$ there is by assumption $x_p \in E \otimes \mathbb{Z}_p$ such that $q(x_p) = t$. Then by Witt's theorem there is an isometry $u_p \in O(V \otimes \mathbb{Q}_p)$ such that $u_p(x_p) = x$. Put

$$E' := \bigcap_{p\notin S}(E \otimes \mathbb{Z}_p \cap V) \cap \bigcap_{p\in S}(u_p(E \otimes \mathbb{Z}_p) \cap V).$$

Then E' is a lattice in V, $x \in E'$ and $(E' \otimes \mathbb{Z}_p) \cong E \otimes \mathbb{Z}_p$ for all $p \in \mathbb{P}$, i.e. E' is in the genus of E. □

Corollary 14.8. *If* $\mathrm{genus}(E) = [E]$, *then* $t \in q(E)$.

Example 14.9. *(a) (Euler 1749) A number* $t \in \mathbb{Z} \setminus \{0\}$ *is the sum of two squares if and only if* $t > 0$ *and* $v_p(t)$ *is even for all primes* $p \equiv 3 \pmod 4$.
(b) (Gauß 1801) A number $t \in \mathbb{Z} \setminus \{0\}$ *is the sum of three squares if and only if* $t > 0$ *and* t *is not of the form* $4^a(8b+7)$.
(c) (Lagrange 1770) Any $t \in \mathbb{N}$ *is the sum of four squares.*

Proof. For $r = 2, 3, 4$ we have that $\mathrm{genus}(I_r) = [I_r]$ so it suffices to consider the quadratic equations over all completions $\mathbb{Z}_p$. More details are left to the exercises. □

14.3 Unimodular lattices

Lemma 14.10. *Let* $E_i = E_i^{\#}$ *be two unimodular* $\mathbb{Z}$*-lattices of the same signature, then* $\mathbb{Q}E_1 \cong \mathbb{Q}E_2$ *and* $E_1 \otimes \mathbb{Z}_p \cong E_2 \otimes \mathbb{Z}_p$ *for all primes* $p > 2$.

Proof. We have $\det(E_1) = \det(E_2) = (-1)^s$ if the signature is $r - s$, $n = \dim(E_i) = r + s$. So for $p > 2$ the lattice $E_1 \otimes \mathbb{Z}_p$ and $E_2 \otimes \mathbb{Z}_p$ are regular quadratic lattices of the same determinant, and hence isometric. In particular $\mathbb{Q}_p \otimes E_1 \cong \mathbb{Q}_p \otimes E_2$ for all $p \in \mathbb{P} \cup \{\infty\}$, $p \neq 2$. From the product formula 13.6 we get that $c(\mathbb{Q}_2 \otimes E_1) = c(\mathbb{Q}_2 \otimes E_2)$. As both spaces have the same dimension and determinant this implies that also $\mathbb{Q}_2 \otimes E_1 \cong \mathbb{Q}_2 \otimes E_2$. So by the theorem of Hasse and Minkowski $\mathbb{Q}E_1 \cong \mathbb{Q}E_2$. □

Lemma 14.11. *Every odd unimodular* $\mathbb{Z}_2$*-lattice* L *has an orthogonal basis. More precisely there are* $r, s \in \mathbb{Z}_{\geq 0}$, $d \in \{1, -1, 3, -3\}$ *such that* $L \cong \bigoplus^r \langle 1\rangle \bigoplus^s \langle -1\rangle \bigoplus \langle d\rangle$. *If* $\det(L) \in \{\pm 1\}$ *then* $L \cong \mathbb{Z}_2 \otimes I_{r,s}$.

Proof. We proceed by induction on the dimension $n = \dim(L)$. Let $e_1 \in L$ be arbitrary such that $b(e_1, e_1) =: a_1$ is odd. Then $a_1 \in \mathbb{Z}_2^*$ and hence $L = \mathbb{Z}_2 e_1 \perp M$ for some unimodular lattice M. If M is odd then we may proceed by induction. Otherwise we need to choose a different e_1: So assume that M is even and choose $e_2 \in M$ arbitrarily. As $M = M^{\#}$ there is some $e_3 \in M$ such that $b(e_2, e_3) = 1$. Replace e_1 by $e_1' := e_1 + e_2$. Then $b(e_1', e_1') = a_1 + b(e_2, e_2)$ is odd and $e_3' := e_1 - a_1 e_3 \in \langle e_1'\rangle^{\perp}$ satisfies that $b(e_3', e_3') = a_1 + a_1^2 b(e_3, e_3)$ is odd. So $L = \mathbb{Z}_2 e_1' \perp M'$ with M' odd unimodular of dimension $n - 1$.
So we arrive at some orthogonal basis $L \cong \langle_1, \ldots, a_n\rangle$ with $a_i \in \{1, -1, 3, -3\}$. If $a_i \in \{\pm 3\}$ then replace e_i by $e_i + 2e_n$ to achieve that $b(e_i, e_i) \in \{\pm 1\} + 8\mathbb{Z}_2$, so after multiplication of e_i by some unit $b(e_i, e_i) \in \{\pm 1\}$. □

Exercise For $r \geq 4$ we have $I_{r,s} \otimes \mathbb{Z}_2 \cong I_{r-4,s+4} \otimes \mathbb{Z}_2$.

Theorem 14.12. *(a) For all* $(r, s) \in \mathbb{Z}_{\geq 0}^2$ *there is a unique genus of odd unimodular* $\mathbb{Z}$*-lattices of signature* $r - s$ *and dimension* $r + s$. *It is represented by* $I_{r,s} = \bigoplus^r \langle 1\rangle \bigoplus^s \langle -1\rangle$.
(b) Even unimodular lattices only exist if $r - s \in 8\mathbb{Z}$. *For fixed* $(s + 8t, s)$ *they belong to a single genus represented by* $\bigoplus^s \mathbb{H}(\mathbb{Z}) \perp \bigoplus^t \mathbb{E}_8$ *(for* $t \geq 0$*) resp.* $\bigoplus^s \mathbb{H}(\mathbb{Z}) \perp \bigoplus^{-t} (\mathbb{E}_8, -q)$ *(for* $t \leq 0$*).*

Proof. To see (b) we note that we already showed that even unimodular lattices exist if and only if the signature is in $8\mathbb{Z}$. Clearly the given lattices are such even unimodular lattices. It remains to show that all even unimodular lattices of signature (r, s) belong to the same genus. The real isometry class is determined by the signature and over $\mathbb{Z}_p$ (including $p = 2$) these lattices are

regular quadratic forms. So these are isometric if and only if they are isometric over $\mathbb{F}_p$, if and only if they have the same determinant.
For (a) we can see that the real space and the isometry class of $L \otimes \mathbb{Z}_p$ for odd primes p are uniquely determined by the signature (r, s) as in (b). So we know that $L \otimes \mathbb{Z}_p \cong I_{r,s} \cong \mathbb{Z}_p$ for all $p > 2$ including ∞. For $p = 2$ we need the lemma above: As the determinant of L is ± 1 we see that $L \otimes \mathbb{Z}_2 \cong I_{r',s'} \otimes \mathbb{Z}_2$ for some r', s' with $s' \equiv s \pmod 2$. By the product formula we also know that $c(\mathbb{Q}_2 \otimes L) = c(\mathbb{Q}_2 \otimes I_{r',s'}) = c(\mathbb{Q}_2 \otimes I_{r,s})$. This determines $s \pmod 4$ and hence $\mathbb{Z}_2 \otimes L \cong \mathbb{Z}_2 \otimes I_{r,s}$. □

14.4 Weak approximation

In the whole section, S will be a finite set of places of the global field $\mathbb{Q}$. The following definitions and theorems may be transferred to arbitrary global fields.

Definition 14.13. *Let $S \subset \mathbb{P} \cup \{\infty\}$ be a finite set of places of $\mathbb{Q}$. Define $\mathbb{Z}(S) := \mathbb{Z}[\frac{1}{p} \mid p \in S \backslash \{\infty\}]$ to be the set of rational numbers for which the denominator only involves primes from S.*

Theorem 14.14. *(Strong approximation for numbers) For any $\ell \in S$ the image of the diagonal embedding $\mathbb{Z}(S) \hookrightarrow \prod_{p \in S \backslash \{\ell\}} \mathbb{Q}_p$ is dense with respect to the p-adic product distance.*

Proof. (Kneser 23.1) in the exercises. □

Applying the approximation for numbers to the coefficients of the vectors with respect to some lattice basis we conclude

Corollary 14.15. *Let L be a lattice in the finite dimensional rational vector space V. Then the image of the diagonal embedding $\mathbb{Z}(S)L \hookrightarrow \prod_{p \in S \backslash \{\ell\}} \mathbb{Q}_p \otimes V$ is dense.*

Theorem 14.16. *Let (V, q) be a regular quadratic space over $\mathbb{Q}$. Then the image of the diagonal embedding $SO(V) \hookrightarrow \prod_{p \in S} SO(V \otimes \mathbb{Q}_p)$ is dense.*

Proof. Let $u_p \in SO(V \otimes \mathbb{Q}_p)$. Then u_p is a product of an even number of reflections:

$$u_p = s_{a_{p,1}} \cdots s_{a_{p,2r}}$$

where we may assume that the length $2r$ is the same for all $p \in S$. (Otherwise we multiply by a product of squares of reflections.) We have $s_a(x) = x - \frac{b(x,a)}{q(a)} a$, in particular the mapping

$$\{a \in V \mid q(a) \neq 0\} \subset \mathbb{Q}^n \to \mathbb{Q}^{n \times n}, {}^B a \mapsto {}^B s_a^B$$

is continuous. By Corollary 14.15 we may approximate all the $a_{p,i}$ by some $a_i \in V$, (all $p \in S$) if the approximation is close enough, then $q(a_i) \neq 0$ and $u := s_{a_1} \cdots s_{a_{2r}} \in O(V)$ approximates u_p for all $p \in S$. □

Clear: We cannot hope to get this approximation property also for the group $O(V)$ as one cannot simultaneously approximate orthogonal mappings with different determinant. However we may approximate elements with different Spinor norm, because the $q(a_i)$ can approximate different $q(a_{i,p}) \in \mathbb{Q}_p$ for all the finitely may places $p \in S$.

Corollary 14.17. *Assume that E, F are lattices in V that are in the same genus. Then there is some isometry $u \in O(V)$ such that $E \otimes \mathbb{Z}_p = u(F) \otimes \mathbb{Z}_p$ for all $p \in S$.*

Proof. By definition there are $u_p \in O(V \otimes \mathbb{Q}_p)$ such that $E \otimes \mathbb{Z}_p = u_p(F \otimes \mathbb{Z}_p)$ for all $p \in \mathbb{P}$. In the case $\det(u_p) = -1$ we can multiply u_p by some reflection in $O(F \otimes \mathbb{Z}_p)$ so that we may assume wlog that $u_p \in SO(V \otimes \mathbb{Q}_p)$. Finitely many u_p (for $p \in S$) may be approximated simultaneously by some $u \in SO(V)$, so that $u(F) \otimes \mathbb{Z}_p = u_p(F \otimes \mathbb{Z}_p)$. □

Definition 14.18. *Let L be a lattice in the regular quadratic space (V, q). For $t \in \mathbb{Q}$ put*

$$L(t) := \{\ell \in L \mid q(\ell) = t\} \text{ and } V(t) := \{x \in V \mid q(x) = t\}.$$

Theorem 14.19. *Assume that $\dim(V) \geq 2$, $t \in \mathbb{Q}^*$ such that $V(t) \neq \emptyset$. Then the image of the diagonal embedding*

$$V(t) \hookrightarrow \prod_{p \in S} (V \otimes \mathbb{Q}_p)(t)$$

is dense.

Proof. Let $x_p \in (V \otimes \mathbb{Q}_p)(t)$ for all $p \in S$ and choose $x \in V(t)$. By Witt's theorem there is some $u_p \in O(V \otimes \mathbb{Q}_p)$ such that $u_p(x) = x_p$. Replacing u_p by $u_p s_a$ for some non-singular $a \in V$ with $a \perp x$ (this is possible because $t \neq 0$ and $\dim(V) > 1$) we may assume that all $u_p \in SO(V \otimes \mathbb{Q}_p)$. So we may approximate u_p (for all $p \in S$) simultaneously by some $u \in SO(V)$. Then $u(x)$ approximates the $x_p = u_p(x)$. □

Recall the definition of the spin group

$$\mathrm{Spin}(V, q) := \{u \in \mathcal{C}_0(V, q) \mid uVu^{-1} = V, N(u) = 1\}$$

Then $\mathrm{Spin}(V, q) \to SO^+(V, q), u \mapsto (\kappa_u)_{|V}$ is an epimorphism with kernel $\{\pm 1\}$. If $\mathrm{char}(K) \neq 2$ then $O(V, q)$ is generated by reflections and

$$SO^+(V, q) = \{s_{a_1} \cdots s_{a_{2r}} \mid r \in \mathbb{N}, a_1, \ldots, a_{2r} \in V, q(a_1) \cdots q(a_{2r}) = 1\}$$

and hence also $\mathrm{Spin}(V, q) = \{a_1 \cdots a_{2r} \mid r \in \mathbb{N}, a_1, \ldots, a_{2r} \in V, q(a_1) \cdots q(a_{2r}) = 1\}$.

Lemma 14.20. *Let (E, q) be some quadratic space over a field A with $\mathrm{ind}(E, q) > 0$. Suppose that $(E, q) \ncong \mathbb{H}(\mathbb{F}_2) \perp \mathbb{H}(\mathbb{F}_2)$. Then $\mathrm{Spin}(E, q) = \langle ef \mid e, f \in E, q(e)q(f) = 1\}$.*

Proof. As we have seen in an example the lemma is true for $E = \mathbb{H}(A)$. (exercise)
Let $N := \langle ef \mid e, f \in E, q(e)q(f) = 1\}$. Then for any $g \in V$, $q(g) \neq 0$ we have $gNg^{-1} = N$ and hence $N \trianglelefteq \mathcal{C}(V)^*$.
By assumption $V = \mathbb{H} \perp W$. Now assume that $u := f_1 \cdots f_{2m} \in \mathrm{Spin}(V, q)$. Then there are $h_i \in \mathbb{H}$ such that $q(f_i) = q(h_i)$ for all $i = 1, \ldots, 2m$, therefore

$$uN = f_1 \cdots f_{2m} N = h_1 \cdots h_{2m} N \in \mathcal{C}(V)^*/N.$$

But $h_1 \cdots h_{2m} \in N$ so also $u \in N$ and the lemma is proved. □

Theorem 14.21. *(Weak approximation for Spin groups) If $\dim(V) \geq 3$ then the image of the diagonal embedding of $\mathrm{Spin}(V)$ is dense in $\prod_{p \in S} \mathrm{Spin}(V \otimes \mathbb{Q}_p)$.*

Proof. If we enlarge S then we get a stronger statement, so we may assume that $\mathrm{ind}(V \otimes \mathbb{Q}_\ell) > 0$ for all $\ell \notin S$ (choose a maximal integral lattice L in V and include to S all prime divisors of $2\det(L)$ and the infinite place).
Let $(u_p) \in \prod_{p\in S} \mathrm{Spin}(V \otimes \mathbb{Q}_p)$ and write

$$u_p = f_{p,1} \cdots f_{p,2m} \text{ for } f_{p,i} \in V \otimes \mathbb{Q}_p, \prod q(f_{p,i}) = 1.$$

Again we may assume that all such expressions have the same length, as we may multiply by $ff^{-1} = f(q(f)^{-1}f) = 1$ for any $f \in V$ with $q(f) \neq 0$.
We now want to approximate the $f_{p,i}$ simultaneously by some $f_i \in V$ so that $q(f_1) \cdots q(f_{2m}) = 1$. To this aim we first approximate the $f_{p,i}$ for all $p \in S$ and $i = 1, \ldots 2m-1$ by some vectors $f_i \in V$. Then we look for the last vector f_{2m} as an approximation of $f_{p,2m}$ for all $p \in S$ with the additional condition $q(f_{2m}) = \prod_{i=1}^{2m-1} q(f_i)^{-1}$. The equation

$$(\star) q(x) = \prod_{i=1}^{2m-1} q(f_i)^{-1} =: t$$

has a solution $x_p \in V \otimes \mathbb{Q}_p$ with x_p close to $f_{p,2m}$ for all $p \in S$ whenever the approximation of $f_{p,i}$ is good enough. Now $V \otimes \mathbb{Q}_p$ is has positive Witt index for $p \notin S$, so $(\star)$ also has a solution $x_p \in V \otimes \mathbb{Q}_p$ for these p. By the strong theorem of Hasse and Minkowski this implies that $(\star)$ also has a solution $x \in V$. In particular $V(t) \neq \emptyset$ and so we may apply Theorem 14.19 to construct a solution $x \in V(t)$ that approximates all the finitely many x_p with $p \in S$. □

As the mapping

$$\prod_{p\in S} \mathrm{Spin}(V \otimes \mathbb{Q}_p) \to \prod_{p\in S} SO^+(V \otimes \mathbb{Q}_p)$$

is continuous and surjective we get the following

Corollary 14.22. *If* $\dim(V) \geq 3$ *then the image of the diagonal embedding of* $SO^+(V)$ *is dense in* $\prod_{p\in S} SO^+(V \otimes \mathbb{Q}_p)$.

14.5 Strong approximation

In this section let $T \subset \mathbb{P} \cup \{\infty\}$ be some finite set of places. As before $L \leq V$ will denote a lattice in some regular quadratic space (V, q) over $\mathbb{Q}$. Recall the definition $\mathbb{Z}(T) := \mathbb{Z}[\frac{1}{p} \mid p \in T]$

Definition 14.23. *For* $t \in \mathbb{Q}$ *put*

$$L(T, t) := \{\ell \in \mathbb{Z}(T)L \mid q(\ell) = t\}.$$

We also define

$$\begin{aligned}
&SO^+(V, q) := \{u \in SO(V, q) \mid \mathrm{SN}(u) = 1\}\\
&O(L, T) := \{u \in O(V, q) \mid u(L \otimes \mathbb{Z}_p) = L \otimes \mathbb{Z}_p \text{ for } p \notin T\}\\
&SO(L, T) := \{u \in SO(V, q) \mid u(L \otimes \mathbb{Z}_p) = L \otimes \mathbb{Z}_p \text{ for } p \notin T\}\\
&SO^+(L, T) := \{u \in SO^+(V, q) \mid u(L \otimes \mathbb{Z}_p) = L \otimes \mathbb{Z}_p \text{ for } p \notin T\}\\
&\mathrm{Spin}(L, T) := \{u \in \mathrm{Spin}(V, q) \mid u \in \mathcal{C}_0(L \otimes \mathbb{Z}_p) \text{ for } p \notin T\}
\end{aligned}$$

Here and in the following we identify $u \in O(V)$ *with its image* $u \in O(V \otimes \mathbb{Q}_p)$.

Theorem 14.24. *(strong approximation theorem) Let (V,q) be a regular quadratic space of dimension ≥ 4 over $\mathbb{Q}$, $t \in \mathbb{Q}^*$ such that $V(t) \neq \emptyset$. Assume that $\infty \in T$ and that $\mathrm{ind}(V \otimes \mathbb{Q}_\ell) > 0$ for some $\ell \in T$. Let L be some $\mathbb{Z}$-lattice in V so that $(V \otimes \mathbb{Q}_p)(t) \cap L \otimes \mathbb{Z}_p =: (L \otimes \mathbb{Z}_p)(t) \neq \emptyset$ for all $p \notin T$. Then the image of the diagonal embedding*

$$L(T,t) \hookrightarrow \prod_{t \in T \setminus \{\ell,\infty\}} (V \otimes \mathbb{Q}_p)(t)$$

is dense.

Note that the strongest version of the strong approximation theorem asserts that under the assumptions

$$L(T,t) \hookrightarrow \prod_{t \in T \setminus \{\ell\}} (V \otimes \mathbb{Q}_p)(t)$$

is dense. However, for our purposes it is enough to prove Theorem 14.24 as stated. For the proof we need two lemmata (and even then it is quite technical but elementary). I refer to Kneser's book, p. 98-101.

Theorem 14.25. *(strong approximation for the spin group) Let (V,q) be a regular quadratic space over $\mathbb{Q}$, $\dim(V) =: n \geq 3$, Assume that $\mathrm{ind}(V \otimes \mathbb{Q}_\ell) > 0$ for some $\ell \in T$. Then for any $\mathbb{Z}$-lattice L in V the images of the diagonal embeddings*

$$\mathrm{Spin}(L,T) \overset{\varphi}{\hookrightarrow} \prod_{p \in T \setminus \{\ell,\infty\}} \mathrm{Spin}(V \otimes \mathbb{Q}_p) \text{ and } SO^+(L,T) \hookrightarrow \prod_{p \in T \setminus \{\ell,\infty\}} SO^+(V \otimes \mathbb{Q}_p)$$

are dense.

As in the strong approximation theorem, we may omit ∞ in the statement and hence also approximate at the real place, however for our purposes the above statement is enough.
Proof. As the mapping

$$\prod_{p \in T \setminus \{\ell,\infty\}} \mathrm{Spin}(V \otimes \mathbb{Q}_p) \to \prod_{p \in T \setminus \{\ell,\infty\}} SO^+(V \otimes \mathbb{Q}_p)$$

is continuous and surjective, it is enough to prove the theorem for the Spin groups.
So let

$$(u_p)_{p \in T \setminus \{\ell,\infty\}} \in \prod_{p \in T \setminus \{\ell,\infty\}} \mathrm{Spin}(V \otimes \mathbb{Q}_p)$$

We want to approximate the u_p simultaneously by some element $u \in \mathrm{Spin}(L,T)$. Note that we may enlarge T by adding some finite set of primes r and setting $u_r := 1$. If the approximation u is close enough, then automatically $u \in \mathrm{Spin}(L \otimes \mathbb{Z}_r)$ and hence the denominators of u and u^{-1} will not involve the prime r. In particular we may enlarge T so that $L \otimes \mathbb{Z}_p$ is regular for all $p \notin T$. Then $\mathrm{ind}(V \otimes \mathbb{Q}_p) > 0$ for all primes $p \notin T$.
First assume that $n = 3$. Then $\mathrm{Spin}(V) = \{x \in \mathcal{C}_0(V) \mid x\overline{x} = 1\} = (V', q')$, where $V' := \mathcal{C}_0(V)$ is a 4-dimensional quadratic space for $q' : x \mapsto x\overline{x}$. For all primes p for which $\mathrm{ind}(V \otimes \mathbb{Q}_p) > 0$ we also have $\mathrm{ind}(V' \otimes \mathbb{Q}_p) > 0$. Let $L' := \mathcal{C}_0(L)$. Then by the strong approximation theorem 14.24 the image of the embedding $L'(T,1) \hookrightarrow \prod_{p \in T \setminus \{\ell,\infty\}} (V' \otimes \mathbb{Q}_p)(1)$ is dense which is precisely the statement of Theorem 14.25.
Now assume that $n \geq 4$. Put

$$G := \prod_{p \in T \setminus \{\ell,\infty\}} \mathrm{Spin}(V \otimes \mathbb{Q}_p) \text{ and } F := \overline{\varphi(\mathrm{Spin}(L,T))}$$

so F is the subgroup of all elements of G that may be approximated by some element in $\mathrm{Spin}(L,T)$. Then F is a closed subgroup of G and we need to show that $F=G$.
Let $\mathcal{G}:=\{(1,...,u_{p_0},...)\in G \mid u_{p_0}=ef, e,f\in V\otimes\mathbb{Q}_{p_0}, q(e)q(f)=1\}$. We first show that $\mathcal{G}\subseteq F$. As V is dense in $V\otimes\mathbb{Q}_{p_0}$ we may assume that $e,f\in V$ so $t:=q(e)=q(f)^{-1}\in\mathbb{Q}$. Let $T'\supseteq T$ be a set of places that contains T so that $t\in\mathbb{Z}_p^*$ for all $p\notin T'$ and put

$$\begin{array}{ll} e_p=e, f_p=f & \text{for } p=p_0\\ e_p=e, f_p=e^{-1}=t^{-1}e & \text{for } p\in T'\setminus\{\infty,\ell\}, p\neq p_0\end{array}$$

By the strong approximation theorem 14.24 there are $e'\in L(T',t)$, $f'\in L(T',t^{-1})$, such that $e'f'$ approximates $(1,\dots,(ef)_{p_0},\dots,1)\in\mathcal{G}$.
As the ef generate $\mathrm{Spin}(V\otimes\mathbb{Q}_p)$ if $\mathrm{ind}(V\otimes\mathbb{Q}_p)>0$ we find that F contains all elements $(u_p)_{p\in T\setminus\{\ell,\infty\}}\in G$ for which $u_p=1$ if $\mathrm{ind}(V\otimes\mathbb{Q}_p)=0$.
Now assume that $(u_p)_{p\in T\setminus\{\ell,\infty\}}\in G$ is an arbitrary element in G. By the weak approximation theorem for Spin groups there is some $u'\in\mathrm{Spin}(V)$ that approximates all the u_p simultaneously. If $u'\in\mathrm{Spin}(L,T)$ then we are done. In any case $u'\in\mathrm{Spin}(L,T')$ for some suitable $T'\supseteq T$. We search for some $u=u'u''\in\mathrm{Spin}(L,T)$ with $u''\in\mathrm{Spin}(L,T')$ such that $u''\sim_p 1$ for $p\in T\setminus\{\ell,\infty\}$ and $u'u''\sim_p 1$ for $p\in T'\setminus T$. For the latter primes we assumed that $\mathrm{ind}(V_p)>0$, so we already know how to approximate all such (u_p'') by a single $u''\in\mathrm{Spin}(L,T')$. If the approximation is good enough then $u-u'u''\sim u-1\in\mathbb{Z}_p^{n\times n}$ for $p\in T'\setminus T$. In particular the matrix of u (with respect to some lattice basis of L) does not involve p in the denominator, so $u\in\mathrm{Spin}(L,T)$. □

14.6 Spinor genera

Definition 14.26. *Two lattices $L\leq(V,q_V)$ and $M\leq(W,q_W)$ in the regular quadratic $\mathbb{Q}$ spaces V and W belong to the same* **Spinor genus**, *if there is an isometry $u:V\to W$ and orthogonal transformations $v_p\in SO^+(V\otimes\mathbb{Q}_p,q_V)$ such that $M\otimes\mathbb{Z}_p=u(v_p(L\otimes\mathbb{Z}_p))$ for all primes $p\in\mathbb{P}$.*

Clearly spinor genera partition the set of isometry classes of lattices into equivalence classes. Any genus of lattices is a union of finitely many Spinor genera.

Theorem 14.27. *Let (V,q) be a regular quadratic space, $\dim(V)\geq 3$, $\ell\in\mathbb{P}\cup\{\infty\}$ such that $\mathrm{ind}(V\otimes\mathbb{Q}_\ell)>0$. Let L be some lattice in V. Then any isometry class $[M]$ in the Spinor genus of L contains some lattice $M'\subseteq V$ such that $M'\otimes\mathbb{Z}_p=L\otimes\mathbb{Z}_p$ for all primes $p\neq\ell$.*

Corollary 14.28. *Let (V,q) be a regular quadratic space, $\dim(V)\geq 3$, $\mathrm{ind}(V\otimes\mathbb{R})>0$. Then any Spinor genus of lattices in V consists of a single isometry class.*

Proof. (of Theorem 14.27) Let $u\in O(V)$, $v_p\in SO^+(V\otimes\mathbb{Q}_p)$ be the orthogonal transformation so that $u^{-1}(M\otimes\mathbb{Z}_p)=v_p(L\otimes\mathbb{Z}_p)$ for all primes $p\in\mathbb{P}$. Since M and L are lattices in the same space V, we have $L\otimes\mathbb{Z}_p=u^{-1}(M\otimes\mathbb{Z}_p)$ for almost all primes $p\in\mathbb{P}$. Let

$$T:=\{p\in\mathbb{P}\mid L\otimes\mathbb{Z}_p\neq u^{-1}(M\otimes\mathbb{Z}_p)\}\cup\{\ell\}.$$

Then T is finite. By the strong approximation theorem for Spin groups 14.25 there is some $v\in SO^+(V,q)\cap O(L\otimes\mathbb{Z}(T))$ so that

$$v(L\otimes\mathbb{Z}_p)=v_p(L\otimes\mathbb{Z}_p)\text{ for }p\in T\setminus\{\ell\}\text{ and }v(L\otimes\mathbb{Z}_p)=(L\otimes\mathbb{Z}_p)\text{ for }p\notin T.$$

Then $v(L)\otimes\mathbb{Z}_p=v_p(L\otimes\mathbb{Z}_p)=(u^{-1}(M)\otimes\mathbb{Z}_p)$ for all $p\in\mathbb{P}\setminus\{\ell\}$. □

Example: The assumption that $\dim(V) \geq 3$ is necessary. To see this consider

$$L = \quad \langle e, f\rangle_{\mathbb{Z}} = \quad \langle \begin{smallmatrix} 0 & 9 \\ 9 & 2 \end{smallmatrix} \rangle$$
$$\text{and} M = \langle \tfrac{1}{4}e, 4f\rangle_{\mathbb{Z}} = \langle \begin{smallmatrix} 0 & 9 \\ 9 & 32 \end{smallmatrix} \rangle$$

Then L and M are not isometric, as L represents 2 but M does not. However both lattices are indefinite and they lie in the same Spinor genus: To see this we first note that $\mathbb{Z}_p \otimes L = \mathbb{Z}_p \otimes M$ for all $p \neq 2$. So we only need to find some $u \in SO^+(\mathbb{Q}_2 \otimes L)$ such that $u(\mathbb{Z}_2 \otimes L) = \mathbb{Z}_2 \otimes M$. To this aim we write both lattices are hyperbolic planes,

$$L = \langle e, f - \frac{1}{9}e\rangle_{\mathbb{Z}} = \langle \begin{smallmatrix} 0 & 9 \\ 9 & 0 \end{smallmatrix} \rangle \text{ and } M = \langle \frac{1}{4}e, 4f - \frac{16}{9}\frac{1}{4}e = 4(f - \frac{1}{9}e)\rangle_{\mathbb{Z}} = \langle \begin{smallmatrix} 0 & 9 \\ 9 & 0 \end{smallmatrix} \rangle$$

The transformation $u : e \mapsto \frac{1}{4}e,\ f - \frac{1}{9}e \mapsto 4(f - \frac{1}{9}e)$ is hence an orthogonal mapping $u \in O(\mathbb{Q}_2 \otimes L)$. By Example 11.9 we see that $u = t_{\frac{1}{4}} \in SO(\mathbb{Q}_2 \otimes L)$ has Spinor norm $\frac{1}{4} \in (\mathbb{Q}_2^*)^2$.

Lemma 14.29. *Let (V, q) be a regular quadratic space, $\dim(V) \geq 3$, $a \in \mathbb{Q}^*$ with $a > 0$ if $\mathrm{ind}(V \otimes \mathbb{R}) = 0$. Then there is some $u \in SO(V)$ with $\mathrm{SN}(u) = a(\mathbb{Q}^*)^2$.*

Proof. For $p \in \mathbb{P} \cup \{\infty\}$ we look for vectors $x_p,\ y_p \in V \otimes \mathbb{Q}_p$ such that $q(x_p)q(y_p) = a$. By assumption this is no problem for $p = \infty$. It is also no problem if $\dim(V) \geq 4$ or $\mathrm{ind}(V \otimes \mathbb{Q}_p) > 0$ as then $q(V \otimes \mathbb{Q}_p) = \mathbb{Q}_p$. If $\dim(V) = 3$ and $\mathrm{ind}(V \otimes \mathbb{Q}_p) = 0$ then $c \notin q(V \otimes \mathbb{Q}_p)$ if and only if $V \otimes \mathbb{Q}_p \perp [-c]$ is anisotropic, so if and only if $V \otimes \mathbb{Q}_p \perp [-c] \cong \mathcal{U}_p$. Then $c(\mathbb{Q}_p^*)^2 = 2\det(V \otimes \mathbb{Q}_p) = 2\det(V)(\mathbb{Q}_p^*)^2$. For these primes p we choose

$$b_p \in (\mathbb{Q}_p)^* \setminus 2\det(V)(\mathbb{Q}_p^*)^2 \setminus 2a\det(V)(\mathbb{Q}_p^*)^2$$

As there are at least 4 square classes, this is possible. Then we solve $q(y_p) = b_p$ and $q(x_p) = \frac{a}{b_p}$ to obtain the solution.
For these finitely many exceptional p and for $p = \infty$ we approximate x_p by some $x \in V$ so that $q(x)/q(x_p) \in (\mathbb{Q}_p^*)^2$. Then there is some $y \in V$ such that $q(y) = a/q(x)$ by the theorem of Hasse and Minkowski, as there are y_p with $q(y_p) = a/q(x)$ for all $p \in \mathbb{P} \cup \{\infty\}$. Then $u := s_x s_y$ has Spinor norm a. □

Theorem 14.30. *Let (V, q) be a regular quadratic space, $\dim(V) \geq 3$, L a lattice in V so that for all $p \in \mathbb{P}$*

$$(\star) \quad \mathrm{SN}(SO(L \otimes \mathbb{Z}_p)) \supseteq \mathbb{Z}_p^*(\mathbb{Q}_p^*)^2.$$

Then the genus of L consists of a single Spinor genus.
Exercise: The condition $(\star)$ is satisfied, if one of the Jordan components of $L \otimes \mathbb{Z}_p$ has dimension ≥ 2.

Proof. Let M be a lattice in the genus of L. As $O(M \otimes \mathbb{Z}_p)$ contains reflections, there there are $u_p \in SO(V \otimes \mathbb{Q}_p)$ such that $u_p(L \otimes \mathbb{Z}_p) = M \otimes \mathbb{Z}_p$. We take $u_p = 1$ for all p for which $M \otimes \mathbb{Z}_p = L \otimes \mathbb{Z}_p$, i.e. for almost all p. Let $\mathrm{SN}(u_p) = p^{\alpha_p} b_p (\mathbb{Q}_p^*)^2$ with $b_p \in \mathbb{Z}_p^*$, $\alpha_p = 0$ and $b_p = 1$ for almost all p. By Lemma 14.29 there is some $u \in SO(V)$ such that $\mathrm{SN}(u) = \prod_p p^{\alpha_p}$ Then $M \otimes \mathbb{Z}_p = u(u^{-1}u_p(L \otimes \mathbb{Z}_p))$ and $\mathrm{SN}(u^{-1}u_p) = b_p(\mathbb{Q}_p^*)^2$. By assumption there is some $w_p \in SO(L \otimes \mathbb{Z}_p)$ with $\mathrm{SN}(w_p) = b_p^{-1}(\mathbb{Q}_p^*)^2$. Then $u^{-1}(M) \otimes \mathbb{Z}_p = u^{-1}u_p w_p(L \otimes \mathbb{Z}_p)$ with $\mathrm{SN}(u^{-1}u_p w_p) = 1$. □

14.7 Kneser neighboring method

Definition 14.31. *Two lattices L, M in the regular quadratic space (V, q) are called* **neighbors** *or p-neighbors, if $[L : L \cap M] = [M : L \cap M] = p$.*
Define a distance on the set of lattices in $\mathbb{Z}[\frac{1}{p}]L \cap \mathrm{genus}(L)$ by $d(L, M) = s$ if and only if $[L : L \cap M] = [M : L \cap M] = p^s$.

Clear: If L and M are neighbors, then $\det(L) = \det(M)$. If $L \otimes \mathbb{Z}_p$ and $M \otimes \mathbb{Z}_p$ are both maximal lattices in $\mathbb{Q}_p \otimes V$, then L and M belong to the same genus.

Theorem 14.32. *Let $L \neq M$ be two lattices in V such that $\mathbb{Z}[\frac{1}{p}]L = \mathbb{Z}[\frac{1}{p}]M$ (or equivalently $\mathbb{Z}_\ell \otimes L = \mathbb{Z}_\ell \otimes M$ for all $\ell \in \mathbb{P} \setminus \{p\}$). If $L \otimes \mathbb{Z}_p$ and $M \otimes \mathbb{Z}_p$ are maximal even then there is a chain of neighboring lattices*

$$L = L_0, L_1, \ldots, L_s = M$$

such that all L_i belong to the genus of L and such that L_i and L_{i-1} are p-neighbors.

Proof. Let $v \in M \setminus (L \cap M)$ such that $pv \in L \cap M$. Then $b(v, v) \in \mathbb{Z}$. Since L is p-maximal integral, the vector v is not in the dual lattice of L and hence $L_v := \{\ell \in L \mid b(v, \ell) \in \mathbb{Z}\}$ is a proper sublattice of L of index p. Put $L_1 := L_v + \mathbb{Z}v$. Then L_1 is an integral lattice containing $L_v = L \cap L_1$ of index p. So alse L_1 is p-maximal integral, L_1 is a neighbor of L and $L_1 \cap M = L \cap M + \mathbb{Z}v$ so $d(L_1, M) = d(L, M) - 1$. By induction we obtain the theorem. □

By the strong approximation property 14.27 we hence obtain the following corollary which yields an algorithm to enumerate the Spinor genus of a lattice.

Corollary 14.33. *Let L and M be lattices in the same Spinor genus. Assume that $\mathrm{ind}(L \otimes \mathbb{Q}_p) > 0$ for some prime $p \in \mathbb{P}$. Then there is a lattice M' in the isometry class of M and a chain*

$$L = L_0, L_1, \ldots, L_s = M'$$

such that all L_i belong to the genus of L and such that L_i and L_{i-1} are p-neighbors.

Lemma 14.34. *The integral 2-neighbors of I_n are isometric to $\mathbb{D}_m^+ \perp I_{n-m}$ with $m \in 4\mathbb{Z}$, $0 \leq m \leq n$ and $m \neq 4$.*

Proof. Let L be an integral neighbor of I_n. Then $M := L \cap I_n$ is a sublattice of index 2 in I_n, so there is some $v \in I_n = I_n^\#$ such that $M = \{\ell \in I_n \mid (v, \ell) \in 2\mathbb{Z}\}$. Moreover M only depends on the class $v + 2I_n$, so we may assume that $v = v_J := \sum_{i \in J} e_i$ for some subset $J \subset \{1, \ldots, n\}$. Then the sublattice M is isometric to $\mathbb{D}_{|J|} \oplus I_{n-|J|}$. Note that all v_J with constant $|J|$ are in the same orbit under $\mathrm{Aut}(I_n) \cong C_2 \wr S_n$. The unimodular lattice L is hence isometric to some sublattice of $\mathbb{D}_{|J|}^\# \oplus I_{n-|J|}$ that contains $\mathbb{D}_{|J|} \oplus I_{n-|J|}$. As $I_{|J|}$ is the only unimodular sublattice of $\mathbb{D}_{|J|}^\#$ for $|J|$ odd or $|J| \equiv 2 \pmod 4$ and for $|J| \in 4\mathbb{Z}$ the other two unimodular sublattices are isometric to $\mathbb{D}_{|J|}^+$ the statement follows if we observe that $\mathbb{D}_4^+ \cong I_4$. □

Corollary 14.35. *The genera of I_6 and I_7 only consist of a single class.*

Proof. All 2-neighbors of I_6 or I_7 are isometric to I_6 resp. I_7. As the neighboring graph is connected, we obtain that these lattices are unique in their Spinor genus. But for unimodular lattices Spinor genus and genus coincide by Theorem 14.30. □

14.8 The Mass formula.

If $L_1, \ldots, L_h$ is a system of representatives of isometry classes of lattices in the genus of L then

$$\sum_{i=1}^{h} |\operatorname{Aut}(L_i)|^{-1} = \operatorname{mass}(\operatorname{genus}(L))$$

where $\operatorname{mass}(\operatorname{genus}(L))$ can be read off from the local stabilizers $\operatorname{Stab}_{O(V\otimes\mathbb{Q}_p,q)}(L\otimes\mathbb{Z}_p)$ (local densities).
Idea: The isometry classes of lattices are the $O(V,q)$-orbits in the $O(V\otimes\mathbb{A},q)$-orbit $\operatorname{genus}(L)$, where $\mathbb{A} := \{x \in \mathbb{R}\times\prod_p \mathbb{Q}_p \mid x_p \in \mathbb{Z}_p \text{ for almost all } p\}$ the **adele ring** of $\mathbb{Q}$ and $\operatorname{Aut}(L) = \{g \in O(V,q) \mid g(L) = L\}$ is the stabilizer of L in $O(V,q)$.

The proof of the mass formula uses analytic techniques. But for a finite group G acting on finite set M this is very easy. Let $m_1G, \ldots, m_hG$ be the orbits of G on M and $S_i := \operatorname{Stab}_G(m_i)$. Then

$$|M| = \sum_{i=1}^{h} |m_iG| = \sum_{i=1}^{h} \frac{|G|}{|S_i|}$$

and hence

$$\sum_{i=1}^{h} \frac{1}{|S_i|} = \frac{|M|}{|G|}.$$

In our situation this reads as

$$\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(L_i)|} = \frac{|O(V\otimes\mathbb{A},q)\cdot L|}{|O(V,q)|} = \frac{|O(V\otimes\mathbb{A},q)|}{|\operatorname{Aut}(L_{\mathbb{A}})||O(V,q)|}$$

which needs to be replaced by

$$\sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(L_i)|} = \mu(O(V,q)\backslash O(V\otimes\mathbb{A},q)/\operatorname{Aut}(L_{\mathbb{A}}))$$

where μ is a suitable measure.

The mass of self-dual binary codes and self-dual doubly-even binary codes

For a given length $N = 2n$ let

$$M_I := \{C \le \mathbb{F}_2^N \mid C = C^\perp, C \text{ singly even }\} \text{ and } M_{II} := \{C \le \mathbb{F}_2^N \mid C = C^\perp, C \text{ doubly even }\}$$

(where we only define M_{II} if N is a multiple of 8). Then the orthogonal group of $V := \langle\mathbf{1}\rangle^\perp/\langle\mathbf{1}\rangle$ acts transitively on M_I and M_{II} because the elements of M_{II} and M_I correspond to maximal totally singular (resp. not totally singular) self-dual subspaces of V. In particular the cardinality

$$|M_I| = a_N = \prod_{i=1}^{n-1}(2^i+1) \text{ and } |M_{II}| = b_N = 2\prod_{i=1}^{n-2}(2^i+1)$$

is just the index of the stabiliser of such a maximal isotropic subspace.

The symmetric group S_N also acts on M_I and M_{II}. Two codes are called **equivalent**, if and only if, they are in the same orbit under the S_N. Let $[C]$ denote the equivalence class of C. We also define the **automorphism group**

$$\operatorname{Aut}(C) := \operatorname{Stab}_{S_N}(C) = \{\pi \in S_N \mid \pi(C) = C\}.$$

Theorem 14.36. *Let* $M_I = [C_1] \dot\cup \ldots \dot\cup [C_k]$ *and* $M_{II} = [D_1] \dot\cup \ldots \dot\cup [D_h]$. *Then*

$$\sum_{i=1}^{k} \frac{1}{|\operatorname{Aut}(C_i)|} = \frac{a_N}{N!} \text{ and } \sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(D_i)|} = \frac{b_N}{N!}.$$

Proof. $M_I = [C_1] \dot\cup \ldots \dot\cup [C_k]$ is a disjoint union of orbits under S_N. The length of the orbit is $|[C_i]| = \frac{|S_N|}{\operatorname{Stab}_{S_N}(C_i)} = \frac{N!}{|\operatorname{Aut}(C_i)|}$. So

$$a_N = |M_I| = \sum_{i=1}^{k} |[C_i]| = (N!) \sum_{i=1}^{k} \frac{1}{|\operatorname{Aut}(C_i)|}$$

□

Note that for $N \in 8\mathbb{Z}$ we have $a_N = \frac{2^{n-1}+1}{2} b_N$.

Theorem 14.37. *Let* N *be a multiple of 8 and* $L_1, \ldots, L_k$ *be a system of representatives of isometry classes of positive definite odd unimodular lattices of dimension* $N = 2n$. *Let* $M_1, \ldots, M_h$ *be a system of representatives of isometry classes of positive definite even unimodular lattices of dimension* N. *Then*

$$\sum_{i=1}^{k} \frac{1}{|\operatorname{Aut}(L_i)|} = \frac{(2^n-1)(2^{n-1}+1)}{2} \sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(M_i)|}.$$

Proof. Let L be some odd unimodular lattice and $L_0 \leq L$ be its even sublattice. Then (by the assumption that $N \in 8\mathbb{Z}$) $L_0^\# / L_0 \cong C_2 \times C_2$ and the two other lattices M and M' between $L_0^\#$ and L_0 are even unimodular lattices. (As these properties can be seen over the 2-adics, it is enough to consider $L \otimes \mathbb{Z}_2 \cong I_N$ to see this.) So any odd unimodular lattice L has exactly 2 even neighbors. On the other hand given any even unimodular lattice M any unimodular (even or odd) neighbor $L = \langle L \cap M, x \rangle$ is obtained by joining an isotropic vector $x \in \frac{1}{2}M \setminus M$. Put $D := L + M$. Then D contains exactly 3 unimodular lattices, 2 of them are even and 1 on them is odd. So the number of odd neighbors of M is exactly the number of 1-dimensional isotropic subspaces D/M of $\frac{1}{2}M/M$ which is $(2^n-1)(2^{n-1}+1)$ by Lemma 4.14. □

The proof of the last theorem also describes a strategy how to enumerate the positive definite odd and even unimodular lattices in a given dimension simultaneously. For instance for dimension 24, there are exactly 24 isometry classes of even unimodular lattices, but 156 isometry classes of odd unimodular lattices in dimension 24. We apply the Kneser-neighbor-method for the prime 2, to enumerate the genus of even unimodular lattices: We start with some even unimodular lattice L (e.g. $L = \mathbb{E}_8^2$ for $n = 24$). Then we find representatives of all orbits of $\operatorname{Aut}(L)$ on the sublattices M_0 of index 2 in L. Each such M_0 defines a unique 2-neighbor L' of L, i.e. an even unimodular lattice L' such that $L' \cap L = M_0$. Let M be the unique other lattice in $M_0^\# / M_0 \cong C_2 \times C_2$. Then M is an odd unimodular lattice. During the neighboring method one hence enumerates also all odd unimodular lattices M. I strongly encourage you to implement this method in MAGMA. Note that the lattice M_0 contains $2L$, so corresponds to a 23-dimensional subspace of $L/2L \cong \mathbb{F}_2^{24}$, i.e. of the form $v^\perp$ for some $v \in \mathbb{F}_2^{24}$. There is a MAGMA function OrbitsOfSpaces, that computes representatives of the $\operatorname{Aut}(L)$-action on either the vectors v or the subspaces $v^\perp$.

Chapter 5

Orthogonal representations of finite groups.

15 Representations of finite groups.

Let G be a finite group and K be a field. A K-**representation** of degree n of G is a group homomorphism $\Delta : G \to \mathrm{GL}_n(K)$.

Two K-representations Δ, Δ' of degree n are called **equivalent** if there is some $A \in \mathrm{GL}_n(K)$ such that $A\Delta(g)A^{-1} = \Delta'(g)$ for all $g \in G$.

$\chi_\Delta : G \to K, g \mapsto \mathrm{trace}(\Delta(g))$ is called the **character** of Δ.

Theorem 15.1. *If* $\mathrm{char}(K) = 0$ *then* $\Delta \sim \Delta'$ *if and only if* $\chi_\Delta = \chi_{\Delta'}$.

Any K-representation $\Delta : G \to \mathrm{GL}_n(K)$ defines a KG-module structure on the vector space $K^n =: V$ where KG is the group ring

$$KG = \{\sum_{g \in G} a_g g \mid a_g \in K\}$$

So KG is the free K-module on G with multiplication extending the group multiplication by distributivity. The group algebra carries a natural involution $^\circ : KG \to KG, \sum a_g g \mapsto \sum a_g g^{-1}$.

Theorem 15.2. *(Maschke's theorem) KG is a semi-simple algebra if and only if* $\mathrm{char}(K) \not| |G|$.

Proof. Assume that $\mathrm{char}(K) \not| |G|$. The trace of $g \in G$ on the regular KG-module KG is 0 for $1 \neq g \in G$ and $|G|$ for $g = 1$. So $\frac{1}{|G|}$ times the regular trace defines a bilinear form on KG so that $(g^{-1} : g \in G)$ is the dual basis of G. This shows that KG is a separable algebra if $\mathrm{char}(K)$ does not divide the group order. □

So if $\mathrm{char}(K) \not| |G|$ then every KG-module is the direct sum of simple modules, so every representation Δ is equivalent to a completely reducible representation

$$\Delta = \mathrm{diag}(\Delta_1, \ldots, \Delta_s)$$

where the $\Delta_i : G \to \mathrm{GL}_{x_i}(K)$ are irreducible representations.

The endomorphism ring of the representation Δ (or the module V) is

$$\mathrm{End}_G(V) = \mathrm{End}_{KG}(V) = \mathrm{End}(\Delta) = \{X \in K^{n \times n} \mid X\Delta(g) = \Delta(g)X\} \leq K^{n \times n}.$$

It is a skew-field if Δ is irreducible.

Definition 15.3. *Let $\Delta : G \to \mathrm{GL}_n(K)$ be a representation. Then*

$$\mathcal{F}(\Delta) := \{B \in K^{n\times n} \mid B = B^{tr},\ \Delta(g)B\Delta(g)^{tr} = B \text{ for all } g \in G\}$$

is called the space of Δ-invariant bilinear forms. Similarly

$$\mathcal{Q}(\Delta) := \{q : K^n \to K \mid q \text{ quadratic form }, q(x\Delta(g)) = q(x) \text{ for all } x \in K^n\}$$

is the space of Δ-invariant quadratic forms.

Clearly the map $q \mapsto \mathrm{Gram}(b_q)$ maps $\mathcal{Q}(\Delta)$ into $\mathcal{F}(\Delta)$ and this is a bijection, if $\mathrm{char}(K) \neq 2$.

Remark 15.4. *Let Δ be an irreducible representation of G, $D := \mathrm{End}(\Delta)$. Assume that $\mathcal{F}(\Delta) \neq \{0\}$. Then any $0 \neq B_0 \in \mathcal{F}(\Delta)$ defines an involution $^-$ on the division algebra D defined by $\overline{a} := B_0 a^{tr} B_0^{-1}$ for all $a \in D$. Then*

$$\mathcal{F}(G) = \{aB_0 \mid a = \overline{a} \in D\}.$$

Example. Let $K = \mathbb{R}$ and $\Delta : G \to \mathrm{GL}_n(\mathbb{R})$. Then $B_0 := \frac{1}{|G|}\sum_{g\in G} \Delta(g)\Delta(g)^{tr} \in \mathcal{F}(\Delta)$ is a positive definite Δ-invariant form. If Δ is irreducible, then $\mathcal{F}(\Delta) = \{aB_0 \mid a \in \mathbb{R}\}$:
Let $B \in \mathcal{F}(\Delta)$. Then there is some matrix $T \in \mathrm{GL}_n(K)$ such that $TB_0T^{tr} = I_n$ and $TBT^{tr} = \mathrm{diag}(a_1, \ldots, a_n)$. In particular $b := a_1B_0 - B \in \mathcal{F}(\Delta)$ has a non-zero radical $V^{\perp,b}$, which is hence an invariant submodule of $V = K^n$. By the irreducibility of Δ this implies that $b = 0$ so $B = a_1B_0$.

Example. Let $K = \mathbb{Q}$ and $\Delta : G \to \mathrm{GL}_n(\mathbb{Q})$ be irreducible. Let $D := \mathrm{End}(\Delta)$. Then D is a division algebra with center

$$L = \mathbb{Q}(\chi_\Delta) := \mathbb{Q}(\chi(g) : g \in G)$$

the character field of χ_Δ, $[L : \mathbb{Q}] =: d$, and L is some abelian number field. Let $m^2 := \dim_L(D)$. A famous theorem by Brauer and Speiser tells us that $m \in \{1, 2\}$ if L is totally real. Then we call D definite, if $D \otimes_L \mathbb{R} \cong \mathbb{H}$. Again this property does not depend on the choice of the real embedding of L into $\mathbb{R}$, as D has "uniformly distributed invariants". Then

$$D \otimes_{\mathbb{Q}} \mathbb{R} \cong \begin{cases} \bigoplus^{d/2} \mathbb{C}^{m\times m} & \text{if } L \text{ is totally complex} \\ \bigoplus^{d} \mathbb{R} & \text{if } L = D \text{ is totally real} \\ \bigoplus^{d} \mathbb{R}^{2\times 2} & \text{if } L \text{ is totally real, } D \text{ indefinite} \\ \bigoplus^{d} \mathbb{H} & \text{if } L \text{ is totally real, } D \text{ definite} \end{cases}$$

and $\dim(\mathcal{F}(\Delta)) = \frac{d}{2}m^2$, d, $3d$, d in the respective cases.

16 Equivariant Witt groups.

Let R be a Dedekind ring with field of fractions K (or K an arbitrary field) and A a finite dimensional K-algebra. An **involution** $^\circ$ on A is a K-linear map $^\circ : A \to A$ with $(ab)^\circ = b^\circ a^\circ$ and $(a^\circ)^\circ = a$ for all $a, b \in A$. Let $\Lambda \subseteq A$ be an R-**order** in A, so a subring that is an R-lattice in A. We assume that $\Lambda^\circ = \Lambda$.

Example. G a finite group, $A = KG$, $\Lambda = RG$, $^\circ : A \to A, \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}$.

A Λ **torsion-module** is a finitely generated R torsion-module with an R-linear right action by Λ. For a Λ torsion-module V we define the **dual torsion-module** to be $V^* := \mathrm{Hom}(V, K/R)$.

Definition 16.1. *Let $B = A$ and $L = K$ or $B = \Lambda$ and $L = R$. Let V be a right B-module that is projective and finitely generated as an L-module and $b : V \times V \to L$ be a symmetric L-bilinear form or $B = \Lambda$, $R \neq K$, V a Λ-torsion-module and $b : V \times V \to K/R$ a symmetric R-bilinear form.*

(i) *b is called B-**equivariant**, if $b(va, w) = b(v, wa^\circ)$ for all $v, w \in V$, $a \in B$. We then call (V, b) a **orthogonal B-module**. b is called **regular**, if $V \to V^* : v \mapsto (w \mapsto b(v, w))$ is an isomorphism. (Note that we do not automatically assume that V is projective as an L-module, this would not make much sense for torsion modules.) Two orthogonal B-modules $(V_1, b_1), (V_2, b_2)$ are called **isometric**, if there is an isometry $\varphi : (V_1, b_1) \to (V_2, b_2)$ such that $\varphi(vb) = \varphi(v)b$ for all $v \in V_1$, $b \in B$.*

(ii) *Let (M, b) be a regular orthogonal B-module. Then (M, b) is called **metabolic**, if there is some B-submodule $N \leq M$ with $N = N^\perp$.*

(iii) *Two regular orthogonal B-modules $(V_1, b_1), (V_2, b_2)$ are called **Witt-equivalent** if there are metabolic B-modules (M_1, ψ_1) and (M_2, ψ_2) such that $(V_1, b_1) \perp (M_1, \psi_1) \cong (V_2, b_2) \perp (M_2, \psi_2)$ as orthogonal B-modules.*

Remark 16.2. *Let (V, b) be some orthogonal B-module. Then $\mathrm{rad}(V, b) = \{v \in V \mid b(v, V) = \{0\}\}$ is a B-invariant submodule of V. More general, if $U \leq V$ is a B-submodule of V, then $U^\perp := \{v \in V \mid b(v, U) = \{0\}\}$ is B-invariant.*

Remark 16.3. *The set of equivalence classes of L-projective regular orthogonal B-modules (resp. Λ-torsion modules) is a group w.r.t. orthogonal sums called the **Grothendieck-Witt-group** $GW(B, \circ)$ (resp. $GW^t(\Lambda, \circ)$) of regular orthogonal B-modules (resp. Λ-torsion-modules).*

Remark 16.4. *If $A = A_1 \oplus A_1^\circ$ for some A-ideal A_1, then $GW(A, \circ) = \{0\}$.*

Proof. Let ϵ be the central idempotent in A with $A_1 = A\epsilon$. Then $\epsilon^\circ = (1-\epsilon)$ is the central idempotent of A with $A_1^\circ = A(1-\epsilon)$. For any regular orthogonal A-module (V, b) we have $V = V\epsilon \oplus V(1-\epsilon)$ with $b(V\epsilon, V\epsilon) = b(V, V\epsilon\epsilon^\circ) = b(V, 0) = \{0\}$. Similarly $V(1-\epsilon)$ is an isotropic submodule of V. So V is metabolic. □

Definition 16.5. *A B-submodule $U \leq V$ of the orthogonal B-module (V, b) is called **isotropic**, if $U \neq 0$ and $b(v, w) = 0$ for all $v, w \in U$ (so $U \subseteq U^\perp$).*
*(V, b) is called B-**anisotropic**, if V has no B-invariant isotropic submodule.*

Exercise. If (V, b) is an orthogonal A-module and $U \leq V$ an isotropic A-submodule, then b induces an A-equivariant bilinear form $\overline{b}$ on $U^\perp/U$. Moreover $(U^\perp/U, \overline{b})$ is anisotropic if and only is $U \leq V$ is a maximal isotropic submodule.

Lemma 16.6. *Let (V, b) be a regular orthogonal A-module.*

(i) *The class of (V, b) has a unique (up to A-isometry) A-anisotropic representative in $GW(A, \circ)$. This is isometric to $(U^\perp/U, \overline{b})$ for any maximal isotropic A-submodule $U \leq V$.*

(ii) *If (V, b) is A-anisotropic, then (V, b) is the orthogonal sum of simple regular orthogonal A-modules.*

(iii) *If $[(V, b)] = 0 \in GW(A, \circ)$ then (V, b) is metabolic.*

Proof. (i) Uniqueness: Let (V, b) and (W, c) be two A-anisotropic orthogonal A-modules representing the same element in $GW(A, \circ)$. Then

$$[(V, b)] - [(W, c)] = [(V, b)] + [(W, -c)] - ([(W, c)] + [(W, -c)]) = [(V \bigoplus W, b \perp (-c))]$$

is metabolic. So there is an A-invariant submodule $N = N^\perp \leq (V \bigoplus W, b \perp (-c))$. Then $N \cap V$ and $N \cap W$ are either $\{0\}$ or isotropic A-submodules of V respectively W. As V and W are A-anisotropic, $N \cap V = N \cap W = 0$. Now $\dim(N) + \dim(N^\perp) = \dim(V) + \dim(W)$ so $\pi_V(N) = V$, $\pi_W(N) = W$ and there is an A-module isomorphism $\varphi : V \to W$ so that

$$N = \{(x, \varphi(x)) \in V \bigoplus W\}$$

Now N is isotropic, so $b(x) = c(\varphi(x))$, which means that φ is an isometry.
Existence: Let (V, b) be an orthogonal A-module and $U \leq V$ a maximal isotropic sub A-module. Then b induces an A-invariant form b' on $U^\perp/U$ and $(U^\perp/U, b')$ is A-anisotropic. So we need to show that $M := (V, b) \bigoplus (U^\perp/U, -b')$ is metabolic. Let $X := \{(x, x + U) \in M \mid x \in U^\perp\}$. Then $X \leq M$ is an A-invariant submodule and $X \subset X^\perp$. Indeed we have $X = X^\perp$, because if $z \in V$, $y \in U^\perp$ with $(z, y + U) \in X^\perp$. Then $b(z, x) = b(y, x)$ for all $x \in U^\perp$ and hence $z - y =: u \in U = (U^\perp)^\perp$. But $y \in U^\perp$ then implies $z = y + u \in U^\perp$ and $(z, y + U) = (z, z + U) \in X$. This shows that $X = X^\perp$ and that M is metabolic.
(ii) Let $N \leq V$ be an A-submodule of V. Then also $N^\perp \leq_A V$ and so $N \cap N^\perp$ is an isotropic A-submodule of V. As V is anisotropic this implies that $N \cap N^\perp = 0$ and $V = N \bigoplus N^\perp$. In particular any simple A-submodule N has a complement $N^\perp$. Choosing the next simple A-submodule $N_1 \leq N^\perp$, we can write $V = N \bigoplus N_1 \bigoplus (N^\perp \cap N_1^\perp)$. Continuing this way we can decompose V as a direct sum of simple modules, i.e. V is a semi-simple A-module.
(iii) Let $[(V, b)] = 0 \in GW(A, \circ)$ and let $N \leq V$ be a maximal isotropic submodule of V. Then (V, b) is Witt equivalent to the anisotropic space $(N^\perp/N, \bar{b})$, so we may assume that (V, b) is anisotropic. Let (V', b') be a metabolic A-module so that $(V, b) \bigoplus (V', b')$ is metabolic. Let $N = N^\perp$ be a maximal isotropic A-submodule of (V', b'). Then $\tilde{N} := \{0\} \perp N$ is an isotropic submodule of the metabolic module $(V, b) \bigoplus (V', b')$ with $(\tilde{N})^\perp/\tilde{N} \cong (V, b)$ is anisotropic. So $\tilde{N}$ is maximal isotropic. As $(V, b) \bigoplus (V', b')$ is metabolic we have $\tilde{N}^\perp = \tilde{N}$ so $V = \{0\}$. □

Remark 16.7. *Lemma 16.6 and its proof can be easily transferred also to Λ-torsion modules. (exercise)*

Part (ii) of this lemma does not hold in general for anisotropic quadratic A-modules (V, q) if $\mathrm{char}(K) = 2$. Assume for instance that $G \cong C_2$ acts on the quadratic space $\mathbb{H}(\mathbb{F}_2) = \langle e, f\rangle$ by interchanging e and f. Then $\langle e + f\rangle$ is the unique G-invariant submodule and $q(e + f) = 1$, so this module is not isotropic and $\mathbb{H}(\mathbb{F}_2)$ an anisotropic quadratic $\mathbb{F}_2G$-module.

However we have the following theorem

Theorem 16.8. *Let K be a finite field of $\mathrm{char}(K) = 2$ and (V, q) be an anisotropic quadratic A-module. Then either (V, q) is semi-simple or V contains a non-zero maximal self-orthogonal submodule $U \subseteq U^\perp$. Then $U \cong K$ and $U^\perp/U$ is semi-simple.*

Proof. If V is anisotropic with respect to b_q, then V is semisimple by Lemma 16.6 (ii). If not then let $0 \neq U \leq V$ be some maximal self-orthogonal A-invariant submodule of V (i.e. $U \subseteq U^\perp$). Then $q(U) \neq \{0\}$. As

$$q(x + y) = q(x) + q(y) - b_q(x, y) \text{ and } b_q(U, U) = 0$$

the quadratic form is an $\mathbb{F}_2$-linear mapping from U to K satisfying $q(xa) = aa^\circ q(x)$ for all $x \in U$. In particular the kernel of q is an A-submodule of U. Now V is anisotropic with respect to q so the kernel of this mapping is 0. The image of q is a K^2-submodule of K. We assumed that $K^2 = K$ so $U \cong K$.
As we have seen in the proof of Lemma 16.6 (iii) the factor module $(U^\perp/U, b_q)$ is anisotropic with

respect to the induced bilinear form b_q. In particular Lemma 16.6 (ii) shows that $U^\perp/U$ is semi-simple. □

Lemma 16.6 suggests the following description of $GW(A, \circ)$:

Let $V_1, \dots, V_s$ be a system of representatives of the simple A-modules, that admit regular A-equivariant symmetric bilinear forms $b_i \neq 0$. Let

$$D_i := \mathrm{End}_A(V_i) := \{x \in \mathrm{End}_K(V_i) \mid vax = vxa \text{ for all } a \in A, v \in V_i\}$$

be the endomorphism ring of V_i. Then by Schur's lemma, D_i is a division algebra. Moreover b_i defines an involution $\bar{}$ on D_i by taking the adjoint endomorphism so $b_i(vd, w) = b_i(v, w\bar{d})$ for all $v, w \in V_i$, $d \in D_i$.

The space of symmetric A-equivariant symmetric bilinear forms on V_i is then

$$\{b_i^{(d)} : (v, w) \mapsto b_i(vd, w) \mid d = \bar{d} \in D_i\}$$

In particular if $\{d \in D_i \mid d = \bar{d}\}$ is not contained in the center of D_i then the involution $\bar{}$ depends on the choice of b_i.

Remark 16.9. *As A carries an involution the dual module $V^* := \mathrm{Hom}_K(V, K)$ of any right A-module V becomes a right A-module by putting*

$$(fa)(v) := f(va^\circ) \text{ for all } f \in V^*, v \in V, a \in A.$$

Then b_i induces an A-module isomorphism between V_i and its dual module $V_i^* = \mathrm{Hom}_K(V_i, K)$,

$$b_i^* : V_i \to V_i^*, v \mapsto (x \mapsto b_i(v, x))$$

and $\{V_1, \dots, V_s\}$ is the set of simple A-modules that are isomorphic to their dual.

Theorem 16.10. *With the notation from above we have*

$$GW(A, \circ) \cong \bigoplus_{i=1}^{s} GW(D_i, \bar{}).$$

Proof. Let (V, b) be a regular orthogonal A-module. Then by Lemma 16.6 (i) its class in $GW(A, \circ)$ has a unique anisotropic representative (V', b'). This module is an orthogonal sum of simple A-modules by Lemma 16.6 (ii), so

$$(V', b') = \bigoplus_{i=1}^{s} (\bigoplus_{j=1}^{d_i} (V_i, b_i^{(d_{ij})}))$$

We hence obtain a group homomorphism

$$\bigoplus_{i=1}^{s} W(D_i, \bar{}) \to GW(A, \circ)$$

defined on the 1-dimensional forms $\langle d_i \rangle \in W(D_i, \bar{})$ with $d_i = \bar{d_i} \in D_i$ by $\langle d_i \rangle \mapsto (V_i, b_i^{(d_i)})$. I omit the proof that this is a well defined isomorphism. □

Remark 16.11. *Let K be either algebraically closed or a finite field of characteristic 2. Then all D_i are either K or finite fields of characteristic 2 and hence $GW(D_i, \bar{}) \cong \mathbb{Z}/2\mathbb{Z}$ via the dimension modulo 2. So $GW(A, \circ) \cong (\mathbb{Z}/2\mathbb{Z})^s$.*

Example. Let G be a finite group, $A = \mathbb{F}_2 G$. Let (V, b) be a regular orthogonal A-module. Then (V, b) is metabolic, if and only if all self-dual simple $\mathbb{F}_2 G$-modules $S \cong S^* = \mathrm{Hom}_{\mathbb{F}_2}(S, \mathbb{F}_2)$ that occur in V as composition factors have even multiplicity.

17 The sequence $GW(\Lambda) \to GW(A) \to GW^t(\Lambda)$.

Let R be a Dedekind domain with field of fractions K, A a separable K-algebra with involution $^\circ$ and $\Lambda = \Lambda^\circ \subset A$ be some involution invariant R-order. As we have seen before for $A = \mathbb{Q}$ and $\Lambda = \mathbb{Z}$ we then have an exact sequence

$$(\star) \quad 0 \to GW(\Lambda, {}^\circ) \xrightarrow{\iota} GW(A, {}^\circ) \xrightarrow{\delta} GW^t(\Lambda, {}^\circ).$$

For $A = \mathbb{Q}$ and $\Lambda = \mathbb{Z}$ the mapping δ is surjective. However surjectivity already fails for arbitrary number fields $A = K$ and $\Lambda = \mathbb{Z}_K$, where the cokernel of δ is $C(K)/C(K)^2$ the largest exponent 2 factor group of the class group of K (see Husemoller, Milnor: Symmetric Bilinear Forms, IV, Ex. 3.4).

We want to define ι and δ in our general situation:

We define $\iota : GW(\Lambda, {}^\circ) \to GW(A, {}^\circ)$ by $\iota([(M,b)]) := [(KM,b)]$. This is clearly a well defined group homomorphism.

Lemma 17.1. *$\iota : GW(\Lambda, {}^\circ) \to GW(A, {}^\circ)$ is injective.*

Proof. Let (M,b) be a regular orthogonal Λ-lattice so that $\iota([(M,b)]) = [(KM,b)]$ is metabolic. Let V be a maximal isotropic A-submodule of (KM,b). As K is the field of fractions of R we have $V = K(V \cap M)$. Now (M,b) is a maximal integral lattice in (KM,b), therefore $V \cap M$ is a maximal isotropic Λ-submodule of M. So also (M,b) is metabolic. □

Also the mapping δ is defined as in the classical case:

Definition 17.2. *Let $\delta : GW(A, {}^\circ) \to GW^t(\Lambda, {}^\circ)$ be defined by $\delta([V,b]) := [(L^\#/L, \overline{b})]$, where L is some integral Λ-lattice in the regular orthogonal A-module (V,b).*

As we have seen in Section 5.4 this definition does not depend on the choice of a Λ-lattice L in V:

Lemma 17.3. *Let (M,b) be a regular orthogonal Λ-torsion module and $N \leq M$ a Λ-submodule with $N \subset N^\perp$. Then b induces a regular Λ-equivariant form on $N^\perp/N$ and $(M,b) \perp\!\!\!\perp (N^\perp/N, -\overline{b})$ is metabolic.*

Proof. Let $X := \{(x, x+N) \mid x \in N^\perp\} \subset M \oplus N^\perp/N$. Then $X = X^\perp$, because $X \subset X^\perp$ and for $y \in M, z \in N^\perp$ with $b(x,y) = b(x,z)$ for all $x \in N^\perp$ we have $y - z \in (N^\perp)^\perp = N$. □

Lemma 17.4. *The mapping $\delta : GW(A, {}^\circ) \to GW^t(\Lambda, {}^\circ)$ is well defined.*

Proof. Let L_1, L_2 be two maximal integral Λ-lattices in the regular orthogonal A-module (V,b). Then b defines non-degenerate bilinear forms

$$\overline{b}_i : L_i^\#/L_i \times L_i^\#/L_i \to K/R,\ \overline{b}_i(a+L_i, b+L_i) := b(a,b) + R \ (i = 1,2).$$

Let $M := L_1 \cap L_2$. Then M is an integral Λ-lattice in V and $M^\# = L_1^\# + L_2^\#$. Moreover L_1/M and L_2/M are isotropic Λ-submodules of $(M^\#/M, \overline{b})$ with $(L_i/M)^\perp = L_i^\#/M$ $(i = 1,2)$. So by Lemma 17.3 we have in $GW^t(\Lambda, {}^\circ)$ that

$$[(L_1^\#/L_1, \overline{b}_1)] = [(M^\#/M, \overline{b})] = [(L_2^\#/L_2, \overline{b}_2)]. \qquad \square$$

Lemma 17.5. *$\iota(GW(\Lambda, {}^\circ)) = Ker(\delta)$.*

Proof. We have $\iota(GW(\Lambda,\ ^\circ)) \subseteq Ker(\delta)$. To see the other inclusion let (V,b) be a regular orthogonal A-module with $\delta([(V,b)]) = 0$. Let L be a maximal integral Λ-lattice in (V,b). Then $(L^\#/L, \bar{b})$ is an anisotropic Λ-torsion-module, that is 0 in $GW^t(\Lambda,\ ^\circ)$. So $(L^\#/L, \bar{b})$ is metabolic and anisotropic, which implies that $L^\# = L$. So $(L, b_{|L})$ is a regular orthogonal Λ-module and hence $[(V,b)]$ in the image of ι. □

Remark 17.6. *There is a (non canonical) isomorphism*

$$GW^t(\Lambda,\ ^\circ) \cong \oplus_\wp GW(R/\wp \otimes_R \Lambda,\ ^\circ)$$

where $\wp$ runs through the maximal ideals of the Dedekind domain R.

Proof. Let $[(M,b)] \in GW^t(\Lambda,\ ^\circ)$ where (M,b) is the anisotropic representative of its class. Clearly (M,b) is the orthogonal sum of its $\wp$-primary components $(M,b) = \textcircled{\perp}(M,b)_\wp$. Since $(M,b)_\wp$ is anisotropic, it is annihilated by $\wp$, so $(M,b)\wp$ is a $R/\wp$-module and b takes values in $\wp^{-1}/R \leq K/R$. Choose some isomorphism $\varphi_\wp : \wp^{-1}/R \to R/\wp$. Then $(M, \varphi_\wp \circ b)_\wp \in GW(R/\wp R \otimes \Lambda,\ ^\circ)$. □

17.1 The Witt decomposition matrix.

We now assume that R is a local ring (e.g. $R = \mathbb{Z}_p$ or a finite extension thereof) with residue field $k := R/\wp$, K its field of fraction, A a separable K algebra that carries a K-linear involution and Λ some involution invariant R-order in A. Let $\mathfrak{a} := \Lambda/J(\Lambda)$ be the largest semisimple quotient of Λ. Then $\mathfrak{a}$ is a semisimple k-algebra. We assume that R is big enough, so that k splits $\mathfrak{a}$ and K splits A, i.e. $A = \bigoplus_{i=1}^t K^{n_i \times n_i}$. Let $V_1, \ldots, V_s$ be a system of representatives of the simple A-modules, that admit regular A-equivariant symmetric bilinear forms $b_i \neq 0$. By assumption $\mathrm{End}(V_i) = K$, so b_i is unique up to scalar multiples. Let $S_1, \ldots, S_h$ be a system of representatives of the simple $\mathfrak{a}$-modules, that admit regular Λ-equivariant symmetric bilinear forms $f_j \neq 0$. Again all invariant forms on S_j are scalar multiples of f_j. Let $e_1, \ldots, e_h$ be a system of representatives of the involution invariant primitive idempotents in Λ so that $e_i S_j = \delta_{ij} S_j$.

Let L_i be an integral Λ-lattice in (V_i, b_i). Then there is a basis $B = \cup_{i=1}^h B e_i$ of $L_j = \perp_{i=1}^h L_j e_i$, so that the Gram-matrix of b_j wrt B has the form $diag(a_{ji} f_i \mid i \in r_j)$ for certain $a_{ji} \in R_j^{d_{ji} \times d_{ji}}$, with d_{ji} the multiplicity of S_i in $L_j/\wp L_j$ (the so called **decomposition number**).

Definition 17.7. *The* **Witt-decomposition matrix** $WD(\Lambda)$ *wrt $b_1, \ldots, b_s$ and $f_1, \ldots, f_h$ is the $s \times h$-matrix with entries*

$$WD(\Lambda)_{j,i} := a_{ji} \in W(K,\ ^\circ).$$

Eine $s \times h$-Matrix $WD(\Lambda)$

Example The group ring $\mathbb{Z}_3 S_6$ has 3 blocks, two of which are full matrix rings over $\mathbb{Z}_3$. The only non-trivial block is the principal block and it has a Witt decomposition matrix

	1	1′	6	4	4′
1	(**1**)	.	.	.	.
1′	.	(**1**)	.	.	.
5a	(**1**)	.	.	(**3**)	.
5a'	.	(**1**)	.	.	(**3**)
5b	(**1**)	.	.	.	(**3**)
5b'	.	(**1**)	.	(**3**)	.
16	(**1**)	(**1**)	(−**1**)	(**3**)	(**3**)
10	.	.	(**1**)	(**3**)	.
10′	.	.	(**1**)	.	(**3**)

18 Clifford algebras as G-algebras.

[1]

Let (V,q) be a non-degenerate quadratic space over the field K and G be a subgroup of the orthogonal group $O(V,q)$. Then (V,q) is also called an *orthogonal KG-module*. We want to develop practical methods to obtain information on $\mathcal{C}(V,q)$ from the character $\chi = \chi_V$ of the G-module V.

Since $G \leq O(V,q)$, the action of $O(V,q)$ on $\mathcal{C}(V,q)$ restricts to a linear representation $\Delta_{\mathcal{C}(V,q)}$ of G on the Clifford algebra that respects the grading:

Remark 18.1. *The character of the KG-module $\mathcal{C}(V,q)$ respectively $\mathcal{C}_0(V,q)$ is*

$$\tilde{\chi} := \sum_{i=0}^{n} \Lambda^i(\chi) \text{ respectively } \tilde{\chi}_0 := \sum_{i=0, i \text{ even}}^{n} \Lambda^i(\chi)$$

where $\Lambda^i(\chi)$ is the i-th exterior power of the natural character χ of G on V.

Proof. Let $(e_1,\ldots,e_n) =: e$ be a basis of V and

$$\mathcal{G} := \mathcal{G}(e) = (1, e_1, \ldots, e_n, e_1e_2, \ldots, e_1\cdots e_n)$$

be a basis of $\mathcal{C}(V,q)$. Let $g \in G$ and $A = \Delta^e(g)$ be the matrix of g w.r.t. the basis e. As $e_ie_j = -e_je_i + b(e_i,e_j)1$ the matrix of $c(g)$ with respect to the basis $\mathcal{G}$ is

$${}^{\mathcal{G}}c(g)^{\mathcal{G}} = \begin{pmatrix} 1 & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & A & 0 & \ldots & \ldots & 0 \\ \star & 0 & \Lambda^2(A) & 0 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & 0 & \Lambda^{n-1}(A) & 0 \\ \vdots & & & \ddots & 0 & \det(A) \end{pmatrix}$$

□

Note that

$$\tilde{\chi}(g) = (-1)^n p_g(-1) \text{ for all } g \in G$$

where p_g is the characteristic polynomial of g on V. With this trick one can calculate $\tilde{\chi}(g)$ (and $\tilde{\chi}_0(g)$) with the help of GAP by restricting χ to the subgroup $\langle g\rangle \leq G$, for any group G whose character table and power map is known.

Assumption. From now on we assume that the order of the commutator factor group G/G' is odd. We then have $G \leq SO^+(V,q)$. As we have seen before $SO^+(V,q) = \{\gamma(\kappa_g) \mid g \in \mathrm{Spin}(V,q)\}$. The mapping

$$P : SO^+(V,q) \to \mathrm{Spin}(V,q) \subseteq \mathfrak{c}(V,q), u = \gamma(\kappa_g) \mapsto g$$

is a so called projective representation of $SO^+(V,q)$ satisfying $P(u)P(v) = \pm P(uv)$. Note that $P(u)$ depends upon the choice of $g \in \mathrm{Spin}(V,q)$ with $u = \kappa_g$, so up to ± 1.

Lemma 18.2. *Let $P_0 := P_{|G}$. Then $P_0 \otimes P_0 : G \to \mathrm{GL}(\mathfrak{c}(V,q))$ is a linear representation equivalent to $\Delta_{\mathfrak{c}(V,q)}$.*

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

Proof. The mapping $P_0 : G \to \mathrm{Spin}(V,q), g \mapsto P_0(g)$ is a projective representation of G. $\mathrm{Spin}(V,q) \leq \mathcal{C}_0(V,q)^*$ acts on the simple $\mathfrak{c}(V,q)$-module W. Let $D := \mathrm{End}_{\mathfrak{c}(V,q)}(W)$. The regular $\mathfrak{c}(V,q)$-module $\mathfrak{c}(V,q)$ (with $\mathfrak{c}(V,q)$ acting by left multiplication) is then isomorphic to the tensor product $W \otimes_D W^*$. But $\mathfrak{c}(V,q)$ is an algebra with an involution, which shows that $W \cong W^*$, so

$$_{\mathfrak{c}(V,q)}\mathfrak{c}(V,q) \cong W \otimes_D W^*.$$

The representation $P_0 \otimes_D P_0$ of G is linear and equivalent to the linear representation $\Delta_{\mathfrak{c}(V,q)}$ of G on $\mathfrak{c}(V,q)$. □

Corollary 18.3. *Assume that $char(K) \neq 2$ and let $g \in G$ be an element of order 2 and e the dimension of the -1-eigenspace of g in V. Then $P_0(g)^2 = (-1)^{\binom{e}{2}}\mathrm{id}$.*

Proof. Let $v_1, \ldots, v_e$ be an orthogonal basis of the -1-eigenspace of g on V. Then $P_0(g) = a_g v_1 \ldots v_e$ and $\overline{P_0(g)} = a_g v_e \ldots v_1 = (-1)^{\binom{e}{2}} P_0(g)$. Since $P_0(g)\overline{P_0(g)} = id$, one has $P_0(g)^2 = (-1)^{\binom{e}{2}} id$. □

If $\mathfrak{c}(V,q) \cong D^{a\times a}$ for some central K-division algebra D, then the simple $\mathfrak{c}(V,q)$-module W is isomorphic to D^a. Over the algebraic closure of K, the $\mathfrak{c}(V,q)$-module W is isomorphic to the sum of m copies of a simple module, where m is the *index* of D ($\dim_K(D) = m^2$).

We now fix a covering group $u : \tilde{G} \to G$ of G such that P_0 is equivalent to a linear representation of $\tilde{G}$. Let W be the simple $\mathfrak{c}(V,q)$-module and m the index of $\mathrm{End}_{\mathfrak{c}(V,q)}(W)$.

Corollary 18.4. *Let $m\chi_W$ be the character of a linear $K\tilde{G}$-module that is equivalent to W over the algebraic closure of K. Regarding χ as a character of $\tilde{G}$ one has*

$$\chi_W \otimes \chi_W = \begin{cases} \tilde{\chi} & n \text{ even} \\ \tilde{\chi}_0 & n \text{ odd.} \end{cases}$$

For the next theorem we additionally assume that K is a number field. In general $\mathfrak{c}(V,q)$ is a tensor product of quaternion algebras. Since K is a number field, this implies that $\mathfrak{c}(V,q)$ is a matrix ring over a quaternion algebra and $\mathcal{C}_0(V,q) \cong D^{a\times a}$ where $D = L := Z(\mathcal{C}_0(V,q))$ or D is a quaternion division algebra over L.

Theorem 18.5. *With the notations above let m be the Schur index of D, W the simple $\mathcal{C}_0(V,q)$-module and $m\chi_W$ the corresponding character of $\tilde{G}$. Assume that there is an absolutely irreducible character ψ of $\tilde{G}$ occurring with odd multiplicity in χ_W.*

(a) If n is even and $L = Z(\mathcal{C}_0(V,q))$ is a field then L is a subfield of the character field $K(\psi)$.

(b) Assume that n is odd. If the Schur index of ψ is odd, then $K(\psi)$ splits D. Otherwise let U be the irreducible $K\tilde{G}$-module whose character contains ψ. Then $D \subset \mathrm{End}_{K\tilde{G}}(U)$.

Proof. We have $P_0(G) \leq \mathrm{Spin}(V,q)$ is already contained in $\mathcal{C}_0(V,q)$ and therefore $\mathrm{End}_{\mathcal{C}_0(V,q)}(W) \subseteq \mathrm{End}_{\tilde{G}}(W)$.

In both cases $\mathcal{C}_0(V,q) \cong D^{a\times a}$ and $\dim_K(\mathcal{C}_0(V,q)) = a^2m^2[L:K] = 2^{n-1}$ is a power of 2. Let x be the multiplicity of ψ in χ_W, U the irreducible K-module whose character contains ψ and $D_U := \mathrm{End}_{K\tilde{G}}(U)$. Then D_U is a skew field with center $K(\psi)$ and of index, say, m_U. Let U' be the U-homogeneous component in $W_{|\tilde{G}}$. Then $\mathrm{End}_{K\tilde{G}}(U') \cong D_U^{y\times y}$ for some $y \in \mathbb{N}$. Since the multiplicity of ψ in $m\chi_W$ and the multiplicity of ψ in $\chi_{U'}$ are equal, one has

$$\star \quad mx = ym_U.$$

Since D has no zero divisors, D embeds into $\mathrm{End}_{K\tilde{G}}(U')$ and hence

$$A := D_U^{op} \otimes_{K(\psi)} (D \otimes_K K(\psi)) \to D_U^{op} \otimes_{K(\psi)} D_U^{y\times y} \cong K(\psi)^{m_U^2 y \times m_U^2 y} =: B$$

where D_U^{op} denotes the opposite algebra of D_U. If $K(\psi)\otimes_K L$ is a field then let $\epsilon := [L : K] \in \{1, 2\}$. Then A is a central simple $K(\psi) \otimes_K L$-algebra isomorphic to $\tilde{D}^{k\times k}$ for some central $K(\psi) \otimes_K L$-division algebra $\tilde{D}$ of index, say, $\tilde{m}$. If $K(\psi) \otimes_K L$ is not a field then let $\epsilon := 1$. Then A is a direct sum of two isomorphic central simple $K(\psi)$-algebras isomorphic to $\tilde{D}^{k\times k}$ for some central $K(\psi)$-division algebra $\tilde{D}$ of index, say, $\tilde{m}$.

In both cases the dimension of A over its center is

$$(\star\star) \quad m_U^2 \cdot m^2 = \tilde{m}^2 \cdot k^2$$

and the $K(\psi)$-dimension of a simple A-module is $\epsilon \cdot \tilde{m}^2 \cdot k$ and divides the $K(\psi)$-dimension of the simple B-module, which is $m_U^2 \cdot y$

$$\epsilon \cdot \tilde{m}^2 \cdot k \text{ divides } m_U^2 \cdot y.$$

We claim that $\tilde{m}$ is odd and $\epsilon = 1$. Since K is a number field, m is either 1 or 2. If $m = 1$, then m_U and y are odd by $\star$ (recall that x is odd) and hence also $\tilde{m}$ and ϵ are odd.
Assume that $m = 2$. Then $\star$ implies that either m_U is even and $y \cdot \frac{m_U}{2}$ is odd, or y is even and $m_U \cdot \frac{y}{2}$ is odd. Assume that $2 \mid \tilde{m}$. If m_U is even, then 2^3 divides $\tilde{m}^2 \cdot k$ and if m_U is odd, then 2^2 divides $\tilde{m}^2 \cdot k$. But this power of 2 does not divide $m_U^2 \cdot y$ in both cases, which is a contradiction. Therefore $\tilde{m}$ is odd and k is even. If m_U is even, then 4 divides k by $(\star\star)$ and therefore ϵ is odd. If m_U is odd, then also $\epsilon = 1$ since k is even and $\frac{y}{2}$ is odd. Therefore the claim follows. In particular $\epsilon = 1$ and hence L is a subfield of $K(\psi)$ which proves (a).
Now we prove (b). Since n is odd, $L = K$ and $([D_U]^{-1} \cdot [D \otimes_K K(\psi)])$ has odd order in the Brauer group of $K(\psi)$ because

$$([D_U]^{-1} \cdot [D \otimes_K K(\psi)])^{\tilde{m}} = 1 \in \mathrm{Br}(K(\psi))$$

Therefore the local index $m_\wp(D_U)$ is even, if and only if the local index $m_\wp(D \otimes_K K(\psi))$ is 2, for all (infinite and finite) places $\wp$ of $K(\psi)$. Hence $D \otimes_K K(\psi)$ embeds into D_U. □

In the applications absolutely irreducible orthogonal G-modules (V, q) over totally real number fields K are of special interest. Then q is (positive or negative) definite. If n is even, then the discriminant of q is negative, if $n \equiv 2 \pmod 4$ and positive, if $4 \mid n$.

Corollary 18.6. *In addition to the assumptions of the theorem let K be a totally real number field and assume that (V, q) is definite.*

(a) Let n be even. If $[K(\psi) : K]$ is odd or $n \equiv 0 \pmod 4$ and all intermediate fields $K(\psi) \supset L \supset K$ of degree $[L : K] = 2$ are complex fields, then the discriminant $d_\pm(V, q) = 1$.
If $n \equiv 2 \pmod 4$, then $K(\psi)/K$ has a totally complex intermediate field L with $[L : K] = 2$. One of these fields is isomorphic $K[\sqrt{d_\pm(V, q)}]$.

(b) Assume that n is odd. If ψ has Schur index 1, then the Clifford invariant $[\mathfrak{c}(V, q)]$ satisfies

$$[\mathfrak{c}(V, q) \otimes_K K(\psi)] = [K(\psi)] \in \mathrm{Br}_2(K(\psi)).$$

If ψ has Schur index 2 then $[K(\psi) \otimes_K \mathfrak{c}(V, q)] = [\mathrm{End}_{K(\psi)\tilde{G}}(U)] \in \mathrm{Br}_2(K(\psi))$ for the irreducible $K(\psi)G$-module U with character 2ψ.

18.1 Examples.

We now apply the methods presented before to some irreducible representations of finite quasi simple groups. The notations are taken from the ATLAS.

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 $d_\pm(V,q) = 1$ and also $[\mathfrak{c}(V,q)] = [\mathbb{Q}]$.
Of course, that $d_\pm(V,q) = 1$ is well known and can also be seen by inspection of the modular constituents of V.
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 $P_0 : G \to \mathfrak{c}(V,q)$ 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 $\mathbb{Q}[\chi_5] = \mathbb{Q}[\chi_6] = \mathbb{Q}[\sqrt{-15}]$. Since $\dim(V) \equiv 2 \pmod 4$, Corollary 18.6 yields $d_\pm(V,q) = -15$.
3) Let $G \cong S_6(3)$ and χ the irreducible character of degree 78 with orthogonal $\mathbb{Q}G$-module (V,q). The universal covering group of G is $\tilde{G} \cong 2.S_6(3)$. Let χ_W be the character of $\tilde{G}$ on the simple $\mathfrak{c}(V,q)$-module. If $g \in G$ is an element of order 2 in class $2B$ in the notation of ATLAS, then $-g$ has a 42-dimensional fixed space on V. Therefore χ_W is a faithful character of $\tilde{G}$ by Corollary 18.3. With GAP one finds that there is only one faithful character χ_W of $\tilde{G}$ satisfying $\chi_W \otimes \chi_W = \tilde{\chi}$. The character χ_W contains the two complex conjugate irreducible characters ψ_1 and ψ_2 of degree 13 with multiplicity 1683. Since $\dim(V) \equiv 2 \pmod 4$ and $\mathbb{Q}[\psi_1] = \mathbb{Q}[\sqrt{-3}]$ Corollary 18.6 yields $d_\pm(V,q) = -3$.
4) The applications are not restricted to the characteristic 0 case. Let V be the 4-dimensional $\mathbb{F}_2A_6$-module. If V admits a non-degenerate A_6-invariant quadratic form q, then there is a projective representation $A_6 \to \mathcal{C}_0((V,q))^*$ yielding an irreducible $\overline{\mathbb{F}_2}A_6$-module of dimension 2. Since there is no such module, one concludes that V is not of quadratic type.
Now let (V,q) be a 4-dimensional simple orthogonal $\mathbb{F}_3A_5$-module. Then there is a linear representation $2.A_5 \to \mathcal{C}_0(V,q)^*$ giving rise to a nontrivial action of $\bar{\mathbb{F}}_32.A_5$ on the 2-dimensional simple $\mathcal{C}_0(V,q)$-module. Since the two irreducible $\bar{\mathbb{F}}_32.A_5$-modules of dimension 2 are only realisable over $\mathbb{F}_9$, the determinant $d_\pm(V,q) = -1$ is not a square in $\mathbb{F}_3^*$.
5) Let $G = U_3(5)$ and (V,q) be a 21-dimensional simple orthogonal $\mathbb{Q}G$-module. The universal covering group of G is $3.G$. Therefore $P_0 : G \to \mathfrak{c}(V,q)$ 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 the ATLAS one has $\chi_W = 2\chi_1 + \chi_2 + 2\chi_3 + 2\chi_7 + 2\chi_{10} + \chi_{11} + \chi_{12} + \chi_{13} + \chi_{14}$. The character field of χ_2 (of degree 20) is $\mathbb{Q}$ and its rational Schur index is 2. If U is the irreducible $\mathbb{Q}G$-module with character $2\chi_2$ then $\mathrm{End}_{\mathbb{Q}G}(U) = \mathcal{Q}_{\infty,5}$ the rational quaternion algebra ramified only at 5 and the infinite place. Now Corollary 18.6 yields $[\mathfrak{c}(V,q)] = [\mathcal{Q}_{\infty,5}]$.

19 Orthogonal Frobenius reciprocity.

[2]

Let G be a finite group with subgroup $H \subset G$ and K be a field of characteristic 0. If W is a right KH-module, then the *induced module* W^G defined as $W^G = W \otimes_{KH} KG$ is a KG-module. On the other hand, by restriction, any KG-module V can also be viewed as a KH-module.

[2] G. Nebe, Orthogonal Frobenius reciprocity. J. Algebra 225, 250-260 (2000)

Classical Frobenius reciprocity establishes a canonical isomorphism between the vector spaces of homomorphisms

$$(F) \quad Hom_{KH}(W,V) \cong Hom_{KG}(W^G,V), \quad \varphi \mapsto \varphi^G.$$

Now assume that W admits a non-degenerate symmetric bilinear form $F_W : W \times W \to K$ that is H-invariant, i.e. $F_W(v,w) = F_W(vh,wh)$ for all $v,w \in W, h \in H$. Call such a pair (W,F_W) an *orthogonal KH-module*. Then F_W defines a G-invariant form F_W^G on W^G such that (W^G,F_W^G) becomes an orthogonal KG-module.

If (V,F_V) is an orthogonal KG-module, then it is natural to ask what happens with the *KH-isometries* $Isom_{KH}((W,F_W),(V,F_V)) :=$

$$\{\varphi \in Hom_{KH}(W,V) \mid F_W(w,w') = F_V(\varphi(w),\varphi(w')) \text{ for all } w,w' \in W\}$$

if one applies Frobenius reciprocity. Note that here by definition isometries are injective but not necessarily surjective. Since Frobenius reciprocity does not respect injectivity of the mappings, one has to dualise the right hand side of (F) to again get isometries: F_V induces a KG-isomorphism between V and its dual $V^* := Hom_K(V,K)$. Let F_V^* be the form on V^* such that this isomorphism is an isometry. Assume that V is a *uniform* KG-module, which means that F_V generates the space of all G-invariant symmetric bilinear forms on V. Then orthogonal Frobenius reciprocity gives a canonical bijection

$$Isom_{KH}((W,F_W),(V,F_V)) \cong Isom_{KG}((V^*,F_V^*),((W^G)^*,(F_W^G)^*))$$

defined by

$$\varphi \mapsto \frac{dim(V)}{dim(W^G)}(\varphi^G)^*.$$

Here the condition that V is uniform is clearly necessary. Otherwise the restriction of F_V to $\varphi(W)$ might not determine the G-invariant form F_V. The constant can be easily remembered by taking V and W to be the trivial modules. Then W^G and also $(W^G)^*$ is the permutation module with orthonormal basis $(w \otimes g_1, \ldots, w \otimes g_s)$ and the trivial KG-submodule of W^G is generated by $v := \sum_{j=1}^s w \otimes g_j$ with squared length $(F_W^G)^*(v,v) = s$.

In the next section this orthogonal Frobenius reciprocity and two useful generalisations are proved. It is applied in the last section to determine the rational isometry class of some irreducible orthogonal $\mathbb{Q}S_n$-modules.

19.1 Orthogonal Frobenius reciprocity.

Let K be a field of characteristic 0 and G be a finite group with subgroup $H \subseteq G$. Let $G = \dot{\cup}_{i=1}^s Hg_i$ be a decomposition of G into H-cosets.

If W is a KH-module with K-basis $(b_1,\ldots,b_m)$ then $(b_1 \otimes g_1, \ldots, b_m \otimes g_1, b_1 \otimes g_2, \ldots, b_m \otimes g_s)$ is a K-basis for the KG-module W^G. The action of $g \in G$ on W^G is calculated combining the permutation of the cosets induced by g with the action of H on W: If $g_ig = hg_j$ with $h \in H$ then $(w \otimes g_i)g = wh \otimes g_j$ for all $w \in W$.

If $\varphi : W \to V_{|H}$ is a KH-homomorphism, then $\varphi^G : W^G \to V$ defined by $\varphi^G(\sum_{i=1}^s w_i \otimes g_i) = \sum_{i=1}^s \varphi(w_i)g_i$ is a KG-homomorphism. The mapping $\varphi \mapsto \varphi^G$ is independent of the choice of the coset representatives g_i and defines a K-isomorphism $Hom_{KH}(W,V_{|H}) \to Hom_{KG}(W^G,V)$ with inverse $Hom_{KG}(W^G,V) \to Hom_{KH}(W,V_{|H}); \varphi \mapsto \varphi_{|W}$, the restriction to W, where W is identified with $W \otimes 1 \subseteq W^G$

If (W,F_W) is an orthogonal KH-module, then F_W^G defined by

$$F_W^G(w \otimes g_i, w' \otimes g_j) := \delta_{ij}F_W(w,w') \quad (w,w' \in W, 1 \le i,j \le s)$$

is a non-degenerate G-invariant symmetric bilinear form on W^G.

Any non-degenerate symmetric G-invariant bilinear form F_V on the KG-module V defines a KG-isomorphism $\tilde{F}_V : v \mapsto F_V(\cdot, v)$ between V and the dual space $V^* = Hom_K(V, K)$. Note that V^* is again a right KG-module, via $(fg)(v) = f(vg^{-1})$ for all $v \in V, f \in V^*, g \in G$. Let F_V^* be the form on V^*, for which $\tilde{F}_V$ is an isometry: For $f \in V^*$ let $v_f := \tilde{F}_V^{-1}(f) \in V$. Then

$$F_V^*(f, h) := F_V(v_f, v_h) \text{ for all } f, h \in V^*.$$

Theorem 19.1. *Let K be a field of characteristic 0, (W, F_W) an orthogonal KH-module, and (V, F_V) a uniform orthogonal KG-module. If $\varphi : (W, F_W) \to (V, F_V)$ is a KH-isometry, then the transposed mapping*

$$(\varphi^G)^* : (V^*, \frac{dim(W^G)}{dim(V)} F_V^*) \to ((W^*)^G, (F_W^*)^G)$$

is a KG-isometry.

Remark 19.2. *The constant $\frac{dim(W^G)}{dim(V)}$ can be easily remembered by taking V and $W = \langle w \rangle$ with $F_W(w, w) = 1$ to be the trivial modules. Then W^G and also $(W^G)^*$ is the permutation module with orthonormal basis $(w \otimes g_1, \ldots, w \otimes g_s)$ and the trivial KG-submodule of W^G is generated by $v := \sum_{j=1}^s w \otimes g_j$ with squared length $(F_W^G)^*(v, v) = s$.*

To prove the theorem it is convenient to choose a basis of W and V and work with matrices. So F_V, F_W also denote the Gram matrices of F_V respectively F_W with respect to the chosen basis, g_k the matrix describing the action of $g_k \in G$, right multiplication with φ the corresponding mapping φ etc.

Lemma 19.3. *Let (W, F_W) be an orthogonal KH-module and (V, F_V) be an orthogonal KG-module. Let $\varphi \in Isom_{KH}((W, F_W), (V, F_V))$. Then the orthogonal projection $P_W \in End_{KH}(V)$ onto $\varphi(W)$ is given by right multiplication with*

$$P_W := F_V \varphi^{tr} F_W^{-1} \varphi.$$

If V is a uniform KG-module, then

$$Tr_{G/H}(P_W) := \sum_{j=1}^s g_j^{-1} P_W g_j = \frac{dim(W^G)}{dim(V)} id_V.$$

Proof. A straightforward calculation shows that P_W is the orthogonal projection onto $\varphi(W)$. Therefore $P_W F_V$ is the Gram matrix of a symmetric H-invariant bilinear form on V. By construction $Tr_{G/H}(P_W) \in End_{KG}(V)$ is a KG-endomorphism of V. Since $g_j F_V = F_V (g_j^{tr})^{-1}$, the trace

$$Tr_{G/H}(P_W) F_V = \sum_{j=1}^s g_j^{-1} P_W F_V (g_j^{-1})^{tr}$$

is the Gram matrix of a G-invariant symmetric bilinear form on V. Since V is a uniform KG-module, this implies that $Tr_{G/H}(P_W)$ is a scalar matrix. The trace of the matrix P_W is

$$tr(P_W) = tr(F_V \varphi^{tr} F_W^{-1} \varphi) = tr(\varphi F_V \varphi^{tr} F_W^{-1}) = dim(W).$$

Hence the trace of $Tr_{G/H}(P_W)$ is $s \cdot dim(W) = dim(W^G)$ and $Tr_{G/H}(P_W) = \frac{dim(W^G)}{dim(V)} id_V$. □

Proof of Theorem 19.1.
Let $(w_a|1 \le a \le m)$ be a K-basis of W and $v_a := \varphi(w_a)$ $(1 \le a \le m)$. Then the set $\{v_a g_i \mid 1 \le i \le s, 1 \le a \le m\}$ generates the vector space V over K, because V is an irreducible KG-module. Therefore V^* is generated by the functions

$$f_{a,i} = \tilde{F}_V(v_a g_i) \quad (1 \le a \le m, 1 \le i \le s).$$

Since F_W^G is non-degenerate there are unique $w_j^{(a,i)} \in W$ $(1 \le j \le s)$ such that

$$(\varphi^G)^*(f_{a,i}) = \tilde{F}_W^G(\sum_{j=1}^{s} w_j^{(a,i)} \otimes g_j) \text{ for all } 1 \le a \le m, 1 \le i \le s.$$

For $1 \le a, b \le m$, $1 \le i, k \le s$ one has

$$(\varphi^G)^*(f_{a,i})(w_b \otimes g_k) = f_{a,i}(\varphi^G(w_b \otimes g_k)) = f_{a,i}(v_b g_k) = F_V(v_b g_k, v_a g_i).$$

On the other hand

$$(\varphi^G)^*(f_{a,i})(w_b \otimes g_k) = F_W^G(w_b \otimes g_k, \sum_{j=1}^{s} w_j^{(a,i)} \otimes g_j) = F_W(w_b, w_k^{(a,i)}).$$

Choosing K-bases and working with matrices one therefore gets

$$F_W(w_k^{(a,i)})^{tr} = \varphi g_k F_V g_i^{tr} v_a^{tr} \quad \text{for all } 1 \le i, k \le s, 1 \le a \le m.$$

Hence the scalar product of $(\varphi^G)^*(f_{b,k})$ and $(\varphi^G)^*(f_{a,i})$ with respect to $(F_W^*)^G$ is

$$\sum_{j=1}^{s} w_j^{(b,k)} F_W (w_j^{(a,i)})^{tr} = \sum_{j=1}^{s} v_b g_k (F_V g_j^{tr} \varphi^{tr} F_W^{-1} \varphi g_j F_V) g_i^{tr} v_a^{tr}.$$

By Lemma 19.3

$$\sum_{j=1}^{s} F_V g_j^{tr} \varphi^{tr} F_W^{-1} \varphi g_j F_V = \sum_{j=1}^{s} g_j^{-1} P_W g_j F_V = \frac{dim(W^G)}{dim(V)} F_V$$

and therefore

$$(F_W^G)^*((\varphi^G)^*(f_{b,k}), (\varphi^G)^*(f_{a,i})) = \frac{dim(W^G)}{dim(V)} F_V^*(f_{b,k}, f_{a,i})$$

for all $1 \le i, k \le s$, $1 \le a, b \le m$, which proves the theorem. □

If W^G contains simple KG-modules with multiplicity > 1 then Theorem 19.1 does not give a complete decomposition of the orthogonal KG-module (W^G, F_W^G).

Theorem 19.4. *Let (W, F_W) be an orthogonal KH-module and let (V, F_V) be an absolutely irreducible orthogonal KG-module. Assume, there is $C = C^{tr} \in GL_n(K)$ such that $(\varphi_1, \ldots, \varphi_n) : (W^n, C \otimes F_W) \to (V, F_V)$ is a KH-isometry. Then*

$$((\varphi_1^G)^*, \ldots, (\varphi_n^G)^*) : ((V^*)^n, \frac{dim(W^G)}{dim(V)} C \otimes F_V^*) \to ((W^*)^G, (F_W^*)^G)$$

is a KG-isometry.

Proof. With the notation from the proof of Theorem 19.1 let $v_a^{(x)} := \varphi_x(w_a)$ and $f_{a,i}^{(x)} = \tilde{F}_V(v_a^{(x)} g_i)$ for $1 \leq a \leq m, 1 \leq x \leq n, 1 \leq i \leq s$. As above one calculates

$$(1) \quad (F_W^*)^G((\varphi_y^G)^*(f_{b,k}^{(y)}), (\varphi_x^G)^*(f_{a,i}^{(x)})) = \sum_{j=1}^{s} (v_b^{(y)} g_k F_V g_j^{tr} \varphi_y^{tr} F_W^{-1})(\varphi_x g_j F_V g_i^{tr} (v_a^{(x)})^{tr}).$$

Now $F_V \varphi_y^{tr} F_W^{-1} \varphi_x \in End_{KH}(V)$ has trace $c_{x,y} dim(W)$, where $c_{x,y}$ is the x,y-entry of C, since $\varphi_x F_V \varphi_y^{tr} = c_{x,y} F_W$. Therefore

$$\sum_{j=1}^{s} F_V g_j^{tr} \varphi_y^{tr} F_W^{-1} \varphi_x g_j \in End_{KG}(V)$$

is an endomorphism of trace $c_{x,y} dim(W^G)$. Since V is an absolutely irreducible KG-module, this endomorphism is scalar, hence the right hand side of (1) is

$$c_{x,y} \frac{dim(W^G)}{dim(V)} v_b^{(y)} g_k F_V g_i^{tr} (v_a^{(x)})^{tr} = c_{x,y} \frac{dim(W^G)}{dim(V)} F_V^*(f_{b,j}^{(y)}, f_{a,i}^{(x)}). \qquad \square$$

In Theorem 19.1 the KG-module V was assumed to be uniform. If one drops this assumption, one has to know more about the KH-isometry $\varphi : W \to V$ to identify the invariant form F_V.

Let (W, F_W) be an orthogonal KH-module and (V, F_V) be an irreducible orthogonal KG-module. Let C be the space of symmetric KG-endomorphisms of V,

$$C := \{\varphi \in End_{KG}(V) \mid \varphi \tilde{F}_V = \tilde{F}_V \varphi^*\}$$

and D the space of symmetric KH-endomorphisms of W. Assume that there is a K-linear mapping $\alpha : C \to D$ satisfying $tr(c)/dim_K(V) = tr(\alpha(c))/dim_K(W)$ for all $c \in C$.

Proposition 19.5. *With the notations above let $\varphi : (W, \alpha(c) F_W) \to (V, c F_V)$ be a KH-isometry for all $0 \neq c \in C^+$. Then*

$$(\varphi^G)^* : (V^*, \frac{dim(W^G)}{dim(V)} F_V^*) \to ((W^*)^G, (F_W^*)^G)$$

is a KG-isometry.

Proof. The proof of the proposition is analogous to the one of Theorem 19.1. It only remains to show that the statement of Lemma 19.3 holds with the assumption of the proposition. But the assumptions on φ guarantee that for all $c \in C$

$$tr(c F_V g_j^{tr} \varphi^{tr} F_W^{-1} \varphi g_j) = tr(\varphi c F_V \varphi^{tr} F_W^{-1}) = tr(\alpha(c)) = tr(c) \frac{dim(W)}{dim(V)}.$$

Now C is the eigenspace of the mapping $End_{KG}(V) \to End_{KG}(V), \quad \varphi \mapsto \tilde{F}_V \varphi^* \tilde{F}_V^{-1}$, which is orthogonal with respect to the trace bilinear form. Therefore the restriction of the trace bilinear form of the separable algebra $End_{KG}(V)$ to C is non-degenerate, and therefore

$$\sum_{j=1}^{s} F_V g_j^{tr} \varphi^{tr} F_W^{-1} \varphi g_j = \frac{dim(W^G)}{dim(V)} id_V. \qquad \square$$

20 The Specht modules $S^{(n-k,k)}$.

The representation theory of the symmetric group S_n is very well understood. The irreducible representations, so called Specht modules S^λ, of S_n over a field of characteristic 0 are in bijection with the partitions λ of n. They have the remarkable property that S^λ occurs with multiplicity one as a submodule of a permutation module M^λ, such that all the other constituents of M^λ belong to partitions that are smaller than λ for a suitable ordering. So the Specht modules are good candidates to apply orthogonal Frobenius reciprocity (Theorem 19.1).

A particular easy construction for S^λ can be given, if the partition λ of n has only two parts. So let $k, l, n \in \mathbb{N}$ with $1 \leq k \leq l \leq \frac{n}{2}$ and let $S_l \times S_{n-l}$ denote the Young subgroup of the symmetric group S_n, which is the set stabiliser of the subset $\{1, \ldots, l\}$ of $\{1, \ldots, n\}$.

Let $M^{(n-k,k)}$ be the S_n-permutation module having the k-element subsets of $\{1, \ldots, n\}$ as an orthonormal $\mathbb{Q}$-basis. Denote the corresponding S_n-invariant symmetric bilinear form by $I_{\binom{n}{k}}$. Then

$$dim_{\mathbb{Q}}(M^{(n-k,k)}) = \binom{n}{k} \text{ and } M^{(n-k,k)} = 1_{S_k \times S_{n-k}}^{S_n}.$$

For a fixed subset $T \subset \{1, \ldots, n\}$ let $\sigma_T : M^{(n-k,k)} \to \mathbb{Q}$ be the $\mathbb{Q}$-linear mapping defined by

$$\sigma_T(S) := \begin{cases} 0 & T \not\subseteq S \\ 1 & T \subseteq S \end{cases}$$

for all k-element subsets $S \subset \{1, \ldots, n\}$. Then the Specht module $S^{(n-k,k)} \subseteq M^{(n-k,k)}$ is

$$S^{(n-k,k)} = \bigcap_{T \subseteq \{1,\ldots,n\}, |T|<k} Ker(\sigma_T).$$

$S^{(n-k,k)}$ is an absolutely irreducible S_n-submodule of $M^{(n-k,k)}$. Therefore the S_n-invariant symmetric bilinear forms on $S^{(n-k,k)}$ are rational multiples of the restriction F_k of $I_{\binom{n}{k}}$.

Young's rule says that the $\mathbb{Q}S_n$-module $M^{(n-l,l)}$ is the direct sum of all $S^{(n-k,k)}$ with $k \leq l$. Hence by classical Frobenius reciprocity the fixed space of $S_l \times S_{n-l}$ on $S^{(n-k,k)}$ is one-dimensional, say spanned by some $v \neq 0$. To apply orthogonal Frobenius reciprocity it suffices to calculate the length of v:

Theorem 20.1. *Let $1 \leq k \leq l \leq \frac{n}{2}$. Then there is $v \in S^{(n-k,k)}$ with $vg = v$ for all $g \in S_l \times S_{n-l}$ satisfying*

$$F_k(v, v) = a(l, k) := \binom{n+1-k}{k}\binom{n-l}{k}\binom{l}{k}^{-1}.$$

To prove this theorem we need 2 lemmata on binomial coefficients.

Lemma 20.2.

$$\sum_{j=0}^{k} \binom{l-k+j}{j}\binom{n-l-j}{k-j} = \binom{n+1-k}{k}.$$

Proof. First assume $l = k$. Then the left hand side ist

$$\sum_{j=0}^{k} \binom{n-k-j}{k-j} = \sum_{j=0}^{k} \binom{n-2k+j}{j} = \binom{n-2k+k+1}{k} = \binom{n+1-k}{k}.$$

To show the statement in the general case let $d(l,l+1)$ denote the difference of the left hand sides for l and $l+1$. Then

$$d(l,l+1)=\sum_{j=0}^{k}\binom{l-k+j}{j}\binom{n-l-j}{k-j}-\binom{l-k+j+1}{j}\binom{n-l-j-1}{k-j}=$$

$$\sum_{j=0}^{k}\binom{n-l-j}{k-j}(\binom{l-k+j}{j}-\binom{l-k+j+1}{j})+\sum_{j=0}^{k}\binom{l-k+j+1}{j}\binom{n-l-j-1}{k-j-1}$$

since $\binom{n-l-j-1}{k-j}=\binom{n-l-j}{k-j}-\binom{n-l-j-1}{k-j-1}$. The difference in brackets is $\binom{l-k+j}{j}-\binom{l-k+j+1}{j}=-\binom{l-k+j}{j-1}$.

If one substitutes the summation index $i=j+1$ in the second sum, one finds

$$d(l,l+1)=-\sum_{j=0}^{k}\binom{n-l-j}{k-j}\binom{l-k+j}{j-1}+\sum_{i=1}^{k+1}\binom{l-k+i}{i-1}\binom{n-l-i}{k-i}=0.$$

Hence the left hand side is independent of l and the lemma follows. □

Lemma 20.3. *Let $k\le l\le\frac{n}{2}$. For $0\le i\le k$ define*

$$a_i:=(-1)^i\prod_{j=0}^{i-1}\frac{n-l-k+j+1}{l-j}.$$

Then

$$\sum_{i=x}^{x+b}a_i\binom{n-l-k+x+b}{x+b-i}\binom{l-x}{i-x}=0 \text{ for all } 0\le x\le x+b\le k.$$

Proof. Let $A:=\prod_{j=1}^{x+b}(n-l-k+j)$ be the product of the numerator of the first binomial coefficient with the numerator of a_i and let $B:=\prod_{j=0}^{x-1}(l-j)^{-1}$ be quotient of the numerator of the second binomial coefficient with the denominator of a_i. Then the sum in the lemma simplifies to

$$BA\sum_{i=x}^{x+b}(-1)^i\frac{1}{(i-x)!(b+x-i)!}=\frac{BA}{b!}(-1)^x\sum_{j=0}^{b}(-1)^j\frac{b!}{j!(b-j)!}=0.\qquad\square$$

Proof of Theorem 20.1:
The orbits of $S_l\times S_{n-l}=Stab_{S_n}(\{1,\dots,l\})$ on the k-element subsets T of $\{1,\dots,n\}$ are parametrised by $|T\cap\{1,\dots,l\}|$. For $0\le j\le k$ let $v_j\in M^{(n-k,k)}$ be the sum over all k-element subsets of $\{1,\dots,n\}$ that intersect $\{1,\dots,l\}$ in j elements. Then $(v_0,\dots,v_k)$ is a basis of the fixed space of $S_l\times S_{n-l}$ on $M^{(n-k,k)}$. For the standard scalar product one finds

$$I_{\binom{n}{k}}(v_i,v_j)=\delta_{ij}\binom{n-l}{k-j}\binom{l}{j}.$$

Let a_i be as in Lemma 20.3, T be a $(k-b)$-element subset of $\{1,\dots,n\}$ and $x:=|T\cap\{1,\dots,l\}|$. Then

$$\sigma_T(\sum_{i=0}^{k}a_iv_i)=\sum_{i=x}^{x+b}a_i\binom{n-l-k+x+b}{x+b-i}\binom{l-x}{i-x}=0$$

by Lemma 20.3. Therefore

$$\sum_{i=0}^{k} a_i v_i \in S^{(n-k,k)}.$$

Now

$$a_i = (-1)^i \prod_{j=0}^{i-1} \frac{n-l-k+j+1}{l-j} = (-1)^i \frac{(n-l-(k-i))!}{(n-l-k)!} \frac{(l-i)!}{l!}.$$

Substituting $j = k - i$, the length of $\sum_{i=0}^{k} a_i v_i$ becomes

$$\sum_{j=0}^{k} a_{k-j}^2 \binom{n-l}{j} \binom{l}{k-j} =$$

$$\sum_{j=0}^{k} \frac{(n-l)!l!((l-k+j)!)^2((n-l-j)!)^2}{j!(n-l-j)!(k-j)!(l-k+j)!(l!)^2((n-l-k)!)^2}$$

$$= \frac{(n-l)!}{l!(n-l-k)!} \sum_{j=0}^{k} \frac{(l-k+j)!(n-l-j)!}{j!(k-j)!(n-l-k)!} =$$

$$\frac{(n-l)!(l-k)!}{l!(n-l-k)!} \sum_{j=0}^{k} \binom{n-l-j}{k-j} \binom{l-k+j}{j}.$$

By Lemma 20.2 this equals $a(l,k)$. □

Orthogonal Frobenius reciprocity (Theorem 19.1) now allows to deduce from Theorem 20.1 the following recursion formula for the rational isometry class of F_k.

Corollary 20.4. *For $0 \leq l, k \leq \frac{n}{2}$ and $0 \neq a \in \mathbb{Q}$ let $[aF_k]$ respectively $[I_{\binom{n}{l}}]$ denote the class of aF_k respectively $I_{\binom{n}{l}}$ in the Witt group $W(\mathbb{Q})$. Then*

$$[I_{\binom{n}{l}}] = \sum_{k=0}^{l} [\frac{\binom{n}{l}}{\binom{n}{k} - \binom{n}{k-1}} a(l,k) F_k] = \sum_{k=0}^{l} [\binom{n-2k}{l-k} F_k]$$

where $a(l,k)$ is as in Theorem 20.1.

Remark 20.5. *In principle this method can also be used to obtain the rational isometry classes of the other irreducible orthogonal S_n-modules using Theorem 19.4. However the combinatorics to determine explicit bases for the fixed space of the corresponding Young subgroups on these modules gets much more involved so one cannot hope to get formulas for arbitrary n.*

Chapter 6

Ausgewählte Übungsaufgaben.

Aufgabe 1.
Sei (E, b) ein freier bilinearer A-Modul vom Rang $n \in \mathbb{N}$ und $G_E \in A^{n\times n}$ eine Gram-Matrix von (E, b). Dann gilt:

(i). $\det(G_E)$ ist kein Nullteiler $\Leftrightarrow$ die Abbildung $b_E : E \to E^*, x \mapsto (y \mapsto b(x, y))$ ist injektiv.

(ii). $\det(G_E) \in A^* \Leftrightarrow$ die Abbildung b_E ist bijektiv.

(iii). Sei A ein Körper und (E, b) nicht ausgeartet. Dann ist (E, b) regulär.

Aufgabe 2.
Sei A ein Integritätsbereich, $K = \mathrm{Quot}(A)$ und (V, b) ein regulärer bilinearer K-Vektorraum der Dimension n. Ein (volles) A-*Gitter* in V ist ein A-Teilmodul $L \leq V$ für den es zwei K-Basen $(e_1, \ldots, e_n)$ und $(f_1, \ldots, f_n)$ gibt, so dass

$$Ae_1 \oplus \ldots \oplus Ae_n \subseteq L \subseteq Af_1 \oplus \ldots \oplus Af_n.$$

(i). Ist A Noethersch, so ist L endlich erzeugt.

(ii). $L^\# := \{x \in V \mid b(x, L) \subseteq A\}$ ist ein Gitter (das sogenannte *duale Gitter* zu L).

(iii). Gib einen Isomorphismus $\varphi : L^\# \to L^* = \mathrm{Hom}_A(L, A)$ an.

(iv). $(L, b_{L\times L})$ ist regulärer bilinearer Modul $\Leftrightarrow L = L^\#$.

Ab jetzt sei $A = \mathbb{Z}$ und $b(L, L) \subseteq \mathbb{Z}$. L heit dann ein *ganzes* $\mathbb{Z}$-Gitter und es ist $L \subseteq L^\#$.

(5) $L^\#/L \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$, wo $d_1, \ldots, d_n$ die Invariantenteiler einer Gram-Matrix von L sind.

(6) Bestimme zunächst den Isomorphietyp von $L^\#/L$, und dann Erzeuger von $L^\#$ für folgende $\mathbb{Z}$-Gitter:

(a) $L = \mathbb{I}_n := \mathbb{Z}^n = \langle e_1, \ldots, e_n\rangle$

(b) $L = \mathbb{A}_{n-1} := \langle e_1 - e_2, e_2 - e_3, \ldots, e_{n-1} - e_n\rangle \subseteq \mathbb{Z}^n$ für $2 \leq n \in \mathbb{N}$

(c) $L = \mathbb{D}_n := \langle \mathbb{A}_{n-1}, e_{n-1} + e_n\rangle \subseteq \mathbb{Z}^n$

(7) Für welche $n \in \mathbb{N}$ sind $\mathbb{I}_n$, $\mathbb{A}_{n-1}$ bzw. $\mathbb{D}_n$ nicht ausgeartet, für welche $n \in \mathbb{N}$ sind sie regulär?

Aufgabe 3. Sei A ein kommutativer Ring, E ein A-Modul und seien $S, F \leq E$ Untermoduln. Zusätzlich sei F endlich erzeugt und projektiv, und $b_F : S \to F^*$ ein Isomorphismus.

(i). Zeige: F ist *reflexiv*, d.h. $F \cong F^{**}$.
Hinweis: zeige dies zunächst für endlich erzeugte freie Moduln.

(ii). Beweise Lemma 2.12: $b_S : F \to S^*$ ist ein Isomorphismus.
Hinweis: b_F induziert einen Isomorphismus $b_F^* : (F^*)^* \to S^*$.

Aufgabe 4. Sei R Noetherscher Integritätsbereich mit Quotientenkörper K, $L = L^\#$ ein R-Gitter im regulären K-Vektorraum (V, b), $U \leq V$ mit (U, b) regulär.

(i). Für $X := U \cap L$ ist $(X^\perp)^\#/X^\perp \cong X^\#/X$.

(ii). Wir definieren das gerade unimodulare $\mathbb{Z}$-Gitter $\mathbb{E}_8$ von Rang 8 und zwei seiner Teilgitter:

$$\begin{aligned}
\mathbb{E}_8 &:= \langle \mathbb{D}_8, \tfrac{1}{2}\textstyle\sum_{i=1}^8 e_i \rangle \\
\mathbb{E}_7 &:= \{\textstyle\sum_{i=1}^8 a_i e_i \in \mathbb{E}_8 \mid a_7 = a_8\} = \{x \in \mathbb{E}_8 \mid b(x, e_7 - e_8) = 0\} \\
\mathbb{E}_6 &:= \{\textstyle\sum_{i=1}^8 a_i e_i \in \mathbb{E}_8 \mid a_6 = a_7 = a_8\} = \langle e_6 - e_7, e_7 - e_8 \rangle^\perp
\end{aligned}$$

Zeige: $\mathbb{E}_8 = \mathbb{E}_8^\#$, $\mathbb{E}_7^\#/\mathbb{E}_7 = \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{E}_6^\#/\mathbb{E}_6 = \mathbb{Z}/3\mathbb{Z}$.

(iii). Berechne $\mathbb{E}_6^\#$ und $\mathbb{E}_7^\#$.

Aufgabe 5. Auf $V = \mathbb{F}_2^n$ definiere die symmetrische Bilinearform $b(x, y) := \sum_{i=1}^n x_i y_i$. Einen Teilraum $C \leq V$ nennt man auch Code. C heit *selbstdual*, falls $C = C^\perp$ und *selbstorthogonal*, falls $C \subseteq C^\perp$. Das *Gewicht* eines $c \in V$ ist $\mathrm{wt}(c) := \#\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}$. Ein Code C heit *gerade* bzw. *doppelt gerade*, falls $\mathrm{wt}(c) \in 2\mathbb{Z}$ bzw. $\mathrm{wt}(c) \in 4\mathbb{Z}$ für alle $c \in C$. Bezeichne $\mathbf{1} := (1, \ldots, 1) \in V$, $E := \mathbf{1}^\perp$.

- (V, b) ist nicht ausgeartet.
- Ist $C \subseteq C^\perp$, so ist $\mathrm{wt}(C) \subset 2\mathbb{Z}$ und deshalb ist $C \subseteq \mathbf{1}^\perp = \{c \in V \mid \mathrm{wt}(c) \text{ gerade }\}$.
- Ist C doppelt gerade, dann ist C selbstorthogonal.
- Enthält (V, b) einen doppelt geraden selbstdualen Code, dann ist $n \in 4\mathbb{Z}$.
- $q : E := \mathbf{1}^\perp \to \mathbb{F}_2, q(c) = \frac{\mathrm{wt}(c)}{2} + 2\mathbb{Z}$ ist eine quadratische Form mit $b_q = b_{|E \times E}$.
- Ist n gerade, dann $E^\perp = \langle \mathbf{1} \rangle$, und (E, q) ist semiregulär wenn $n \notin 4\mathbb{Z}$.
- Ist n ungerade, dann ist (E, q) regulär and $(V, b) = E \perp\!\!\!\perp \langle \mathbf{1} \rangle$.

- Schreibe $n = 8m + a$ mit $m \in \mathbb{N}_0$, $a \in \{1, 2, 3, 4, 5, 6, 7, 8\}$. Dann ist $(E, q) \cong \mathbb{H}(\mathbb{F}_2)^{4m} \perp A$ mit[1]

$$A \cong \begin{cases} \{0\} & a = 1 \\ [1] & a = 2 \\ N(\mathbb{F}_2) & a = 3 \\ N(\mathbb{F}_2) \perp [0] & a = 4 \\ \mathbb{H}(\mathbb{F}_2) \perp N(\mathbb{F}_2) & a = 5 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp [1] & a = 6 \\ \mathbb{H}(\mathbb{F}_2)^2 \perp N(\mathbb{F}_2) & a = 7 \\ \mathbb{H}(\mathbb{F}_2)^3 \perp [0] & a = 8 \end{cases} \tag{0.1}$$

- Doppelt gerade selbstduale Codes existieren in V genau dann wenn $n \in 8\mathbb{Z}$.

Aufgabe 6.

Beweise das Gegenbeispiel aus Bemerkung 4.24 und zeige damit, dass der Satz von Witt nicht für reguläre quadratische $\mathbb{Z}$-Moduln gilt:

$$\widetilde{\mathbb{D}}_{16} \perp \mathbb{H}(\mathbb{Z}) \cong \mathbb{E}_8 \perp \mathbb{E}_8 \perp \mathbb{H}(\mathbb{Z})$$

Hinweis: Um diese Isometrie zu konstruieren, schreibe $\tilde{\mathbb{D}}_{16} = \langle \mathbb{D}_{16}, v = \frac{1}{2}\sum_{i=1}^{16} e_i \rangle$ und $\mathbb{H}(\mathbb{Z}) = \langle e, f \rangle$ mit $q(ae + bf) = ab$. In $\tilde{\mathbb{D}}_{16} \perp \mathbb{H}(\mathbb{Z})$ erzeugt das offensichtliche Teilgitter $\mathbb{D}_8$ zusammen mit $v + e - f$ ein Teilgitter L, welches isometrisch ist zu $\mathbb{E}_8$. Finde eine hyperbolische Ebene X in $L^\perp$ (erzeugt von einem Vektor von Länge 0 und einem anderen Vektor, der mit ihm inneres Produkt 1 hat). Identifiziere dann $(X \perp L)^\perp$ mit der zweiten Kopie von $\mathbb{E}_8$.

Aufgabe 7.

Sei R ein diskreter Bewertungsring mit maximalem Ideal πR, und $K := \mathrm{Quot}(R)$.

(i). Zeige: ein R-Gitter L im regulären bilinearen K-Vektorraum (V, b) besitzt eine *Jordan-Zerlegung*, d.h. eine Zerlegung

$$L = (L_a, \pi^a b_a) \perp (L_{a+1}, \pi^{a+1} b_{a+1}) \perp \cdots \perp (L_c \pi^c b_c)$$

für gewisse $a \le c \in \mathbb{Z}$, so dass die (L_i, b_i) für $a \le i \le c$ jeweils entweder Rang 0 haben oder reguläre bilineare R-Gitter sind. Die $\dim(L_i)$ und $\det(\overline{b_i}) \in (R/\pi R)^*/((R/\pi R)^*)^2$ sind durch L eindeutig bestimmt.

Zeige weiter: für $R = \mathbb{Z}_p$ mit $p \neq 2$ sind die $(L_i, \pi^i b_i)$ bis auf Isometrie eindeutig durch L festgelegt. Für $R = \mathbb{Z}_2$ gilt dies zumindest dann, wenn alle b_i gerade Gitter sind.

(ii). Beschreibe einen Algorithmus `JordanDecomposition(A, p)`, der zu einem $\mathbb{Z}_{(p)}$-Gitter mit Gram-Matrix A eine Jordan-Zerlegung berechnet. Implementiere diesen Algorithmus dann in Magma[2].

(Achtung: hier meinen wir wirklich $\mathbb{Z}_{(p)}$, nicht $\mathbb{Z}_p$!)

(iii). Zeige, evtl. unter Zuhilfenahme dieses Algorithmus:

[1] Untersuche die Fälle $n = 1, \ldots 9$ konkret und unterscheide dann zwischen $n = \ell + 8$ gerade und ungerade. Bette E_ℓ isometrisch in E_n ein, so dass das $E_\ell^\perp \to E_n^\perp$ und schreibe so $E_n = E_\ell \perp \mathbb{H}(\mathbb{F}_2)^4$.

[2] unter http://magma.maths.usyd.edu.au/calc/ kann man Magma-Programme ausführen

(a) Die $\mathbb{Z}_p$-Gitter mit Gram-Matrizen

$$\begin{pmatrix} 8 & 1 \\ 1 & 8 \end{pmatrix} \text{ und } \begin{pmatrix} 2 & 1 \\ 1 & 32 \end{pmatrix}$$

sind für alle Primzahlen p isometrisch. Zeige weiter: Aufgefasst als Gitter über $\mathbb{Z}$ sind sie aber nicht isometrisch.

(b) Das $\mathbb{Z}_2$-Gitter L mit Gram-Matrix

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

hat zwei essentiell verschiedene Jordan-Zerlegungen $(L_0, b_0) \perp\!\!\!\perp (L_1, 2b_1)$ und $(L'_0, b'_0) \perp\!\!\!\perp (L'_1, 2b'_1)$ mit $(L_0, b_0) \ncong (L'_0, b'_0)$.

Aufgabe 8.

Sei L ein gerades $\mathbb{Z}$-Gitter im regulären bilinearen $\mathbb{Q}$-Vektorraum (V, b). Sei $(L_0, b_0) \perp\!\!\!\perp (L_1, pb_1)$ eine p-Jordan-Zerlegung von L mit $p \neq 2$. Weiter gelte $\dim(L_0) > 0$ und $k := \dim(L_1) > 0$ und $L^\#/L$ ist eine nicht triviale elementar abelsche p-Gruppe.

Zeige: $\operatorname{sign}(\mathbb{R}L) \equiv 2\varepsilon - 2 - (p-1)k \bmod 8$, wo $\varepsilon = 1$ falls $\det(b_i) = (\mathbb{Z}_p^*)^2$, und $\varepsilon = -1$ sonst.

Hinweis: Gauß-Summen. Es genügt, die Gauß-Summe $\Gamma(L)$ mit dem anisotropen Vertreter von $L^\#/L$ in $WQ(p)$ zu berechnen (drei Fälle).

Es darf benutzt werden, dass

$$\frac{1}{\sqrt{p}} \sum_{a=0}^{p-1} \zeta_p^{a^2} = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ i, & p \equiv 3 \bmod 4 \end{cases}$$

Aufgabe 9.

Sei R ein diskreter Bewertungsring mit maximalem Ideal πR. Sei $q(x_1, \ldots, x_n)$ eine quadratische Form über R. Zeige:

(i). Sei $0 \neq t \in R$. Es existiert genau dann eine Lösung von $q(x_1, \ldots, x_n) = t$, wenn $t = \pi^{2k} u$ für ein $k \in \mathbb{Z}, u \in R$ und eine primitive Darstellung $(x_1, \ldots, x_n)$ für u existiert (d.i. $q(x_1, \ldots, x_n) = u$ mit $x_i \in R$ für alle $1 \leq i \leq n$ und $x_i \notin \pi R$ für mindestens ein $1 \leq i \leq n$).

(ii). Die quadratische Form $q(x_1, x_2) = x_1^2 + x_2^2$ über $\mathbb{Z}_p$ stellt genau dann $u \in \mathbb{Z}_p$ primitiv dar, wenn einer der folgenden Fälle erfüllt ist:

(a) $p \equiv 1 \bmod 4$

(b) $p \equiv 3 \bmod 4$ und $p \not| u$, d.h. $u \in \mathbb{Z}_p^*$

(c) $p = 2$ und $u \equiv 1, 2, 5 \bmod 8$ (*Hinweis*: eine solche Darstellung für u liefert $x_1^2 = u - x_2^2 \equiv 1 \bmod 8$. Lifte nach $\mathbb{Z}_2$, um zu zeigen dass die Bedingung hinreichend ist.)

(iii). Die quadratische Form $q(x_1, x_2, x_3) = \sum_{i=1}^3 x_i^2$ über $\mathbb{Z}_p$ stellt genau dann $u \in \mathbb{Z}_p^*$ primitiv dar, wenn einer der folgenden Fälle erfüllt ist:

(a) $p \neq 2$

(b) $p = 2$ und $u \equiv 1, 2, 3, 5, 6 \bmod 8$ (*Hinweis*: benutze Teil (2), um zu zeigen dass die Bedingung hinreichend ist.)

(iv). Die quadratische Form $q(x_1, x_2, x_3, x_4) = \sum_{i=1}^{4} x_i^2$ über $\mathbb{Z}_2$ stellt genau dann $u \in \mathbb{Z}_2^*$ primitiv dar, wenn $u \not\equiv 0 \mod 8$.

(v). Die quadratische Form $q(x_1, x_2, x_3, x_4, x_5) = \sum_{i=1}^{5} x_i^2$ über $\mathbb{Z}_2$ stellt jedes $u \in \mathbb{Z}_2^*$ primitiv dar.

Aufgabe 10.

Sei A ein kommutativer Ring. Sei (E, q) ein freier quadratischer A-Modul vom Rang 2 mit Basis (e_1, e_2).

Dann gilt:

(i). Ist E regulär und ist $q(e_1) = 1$, dann ist $\mathcal{C}(E, q) \cong A^{2\times 2}$.

(ii). Für die quadratische Form $n : \mathcal{C}(E) \to A, x \mapsto x\overline{x}$ gilt

$$(C_0(E, q), n) \cong \begin{bmatrix} 1 & b \\ & ac \end{bmatrix}.$$

(iii). Sei $\iota : \mathcal{C}(E, q) \to \mathcal{C}(E, q)$ definiert wie in (9.8). Dann ist $\bar{} = \iota \circ c(-id)$ eine kanonische Involution auf $\mathcal{C}(E, q)$ im Sinne von (9.18). Es gilt

$$(\mathcal{C}(E, q), n) = (\mathcal{C}_1, n) \perp\!\!\!\perp (\mathcal{C}_0, n) \cong (E, -q) \perp\!\!\!\perp (\mathcal{C}_0, n).$$

(iv). Falls es ein $e \in E$ gibt mit $a := q(e) \in A^*$, dann ist $(\mathcal{C}_0, an) \cong (E, q)$.

(v). Ist $E^\perp = \{0\}$, dann gilt $\mathcal{C}_0(E, q) = \{x \in \mathcal{C}(E, q) \mid xy = yx \text{ for all } y \in \mathcal{C}_0(E, q)\}$, und $Z(\mathcal{C}) = A$.

Hinweise: siehe Beispiel (9.22). Für Teil (1) betrachte den $\mathcal{C} := \mathcal{C}(E, q)$-invarianten Teilmodul $(1 - e)\mathcal{C} \leq \mathcal{C}$, um einen expliziten Isomorphismus anzugeben.

Aufgabe 11.

Sei $n \in 8\mathbb{Z}$ und $\mathbf{1} := (1, \ldots, 1) \in \mathbb{F}_2^n$. Setze $V := \mathbf{1}^\perp / \langle \mathbf{1} \rangle$ und $q : V \to \mathbb{F}_2, q(x + \langle \mathbf{1} \rangle) := \frac{wt(x)}{2} + 2\mathbb{Z}$. Sei $U \leq V$ ein maximal isotroper Teilraum. Dann gilt nach Aufgabe 5, dass $V \cong \mathbb{H}^{(n-2)/2}$ ist und somit $\dim(U) = \frac{n-2}{2}$.

(i). U ist das Bild eines selbstdualen doppelt-geraden Codes C_U in $\mathbb{F}_2^n$ unter der Projektion $\mathbf{1}^\perp \to V$.

(ii). Die Abbildung $D : O(V, q) \to \mathbb{Z}/2\mathbb{Z}$, $g \mapsto (-1)^{\dim(U/U \cap g(U))}$ ist ein Homomorphismus mit Kern $SO(V, q)$.

Insbesondere gilt $\mathrm{Stab}_{O(V,q)}(U) \subseteq SO(V, q)$.

(iii). Die symmetrische Gruppe S_n operiert durch Permutation der Einträge auf $\mathbb{F}_2^n$, lässt $\mathbf{1}$ fest und bettet somit natürlich in $O(V, q)$ ein. Zeige, dass die Einschränkung von D auf S_n das Signum ist.

(iv). Folgere: für einen selbstdualen doppelt-geraden Code $C \leq \mathbb{F}_2^n$ gilt $\mathrm{Aut}(C) \leq A_n \trianglelefteq S_n$.

Aufgabe 12.

Bestimme die Clifford Invariante und die Diskriminante für die regulären anisotropen quadratischen Räume über $\mathbb{Q}_p$. Stelle das Ergebnis als Tabelle dar.

Begründe kurz, dass $\mathcal{C}([1,d]) \cong \mathbb{Q}_p^{2\times 2}$.

Zeige, dass alle auftretenden zentralen $\mathbb{Q}_p$-Divisionsalgebren entweder $\mathbb{Q}_p$ oder $\mathcal{Q}_p = \mathfrak{c}(\mathcal{U}_p)$ sind.

Aufgabe 13.

Sei $L \leq (V,q)$ ein gerades $\mathbb{Z}$-Gitter, und p eine Primzahl mit $p \nmid \det(L)$. Sei

$$N(L) := \{M \leq (V,q) \mid M \text{ gerades } \mathbb{Z}-\text{Gitter}, [L : L\cap M] = [M : L\cap M] = p\}.$$

Ein Element $M \in N(L)$ heit dann (gerader) *p-Nachbar* von L.

Zeige:

(i). Ist $M \in N(L)$, dann liegen M und L im selben Geschlecht.

(ii). Für $y \in L\backslash pL$ mit $p^2 \mid q(y)$ ist $L_y := \{l \in L \mid b(y,l) \in p\mathbb{Z}\}$ ein Teilgitter von Index p in L und $M := L_y + \langle \frac{y}{p} \rangle$ ein p-Nachbar von L.

(iii). Ist $M \in N(L)$, dann gibt es ein $y \in L\backslash pL$, so dass $p^2|q(y)$ und $M = \left\langle L_y, \frac{1}{p}y \right\rangle =: L^{(y)}$.

(iv). Die Abbildung $\langle y + pL\rangle \mapsto L^{(y)}$ ist eine Bijektion zwischen den isotropen eindimensionalen Teilräumen in $(L/pL, \overline{q})$ und $N(L)$.

Aufgabe 14.

Sei K ein Körper mit $\mathrm{char}(K) \neq 2$. Seien (V,q) und (W,q') reguläre bilineare Räume über K.

(i). Durch $b : (V\otimes W)\times(V\otimes W) \to K$, $(v\otimes w, v'\otimes w') \mapsto b_q(v,v')\cdot b_{q'}(w,w')$ wird eine Bilinearform auf $V\otimes W$ definiert.

$Q : V\otimes W \to K, v\otimes w \mapsto q(v)q'(w)$ definiert eine quadratische Form mit $b_Q = b$.

(ii). Mit der Multiplikation $\otimes$ und der Addition $\perp$ wird $W(K)$ zu einem Ring.

(iii). Die Signatur ist ein Ringisomorphismus $W(\mathbb{R}) \to \mathbb{Z}$.

(iv). $e : W(K) \to \mathbb{Z}/2\mathbb{Z}$, $[(V,q)] \mapsto \dim(V) \bmod 2$ ist ein Ringhomomorphismus mit Kern $W_1(K)$.

(v). Bezeichne $d(V) := d(V,q) := (-1)^{\binom{\dim(V)}{2}} \det(V,q)$ die Diskriminante von (V,q). Dann ist

$$d(V\otimes W) = d(V)^{\dim(W)} d(W)^{\dim(V)}.$$

(vi). Es ist $\mathfrak{c}(V\otimes W) = \mathfrak{c}(V)^{\dim(W)}\mathfrak{c}(W)^{\dim(V)}(d(V),d(W))^{\dim(V)\dim(W)-1}$.

Nun bezeichne $BW(K) := \mathrm{Br}_2(K)\times\mathbb{Z}/2\mathbb{Z}\times K^*/(K^*)^2$ den *Brauer-Wall-Ring* von K. Die Addition in $BW(K)$ ist definiert durch

$$\begin{aligned}(c_1,0,d_1)+(c_2,0,d_2) &= (c_1c_2(d_1,d_2),0,d_1d_2)\\ (c_1,0,d_1)+(c_2,1,d_2) &= (c_1c_2(d_1,-d_2),1,d_1d_2)\\ (c_1,1,d_1)+(c_2,1,d_2) &= (c_1c_2(d_1,d_2),0,-d_1d_2)\end{aligned}$$

und die Multiplikation durch

$$(c_1,e_1,d_1)(c_2,e_2,d_2) = (c_1^{e_2}c_2^{e_1}(d_1,d_2)^{e_1e_2+1}, e_1e_2, d_1^{e_2}d_2^{e_1}).$$

(7) Zeige: $w_K : W(K) \to BW(K) : (V,q) \mapsto ([\mathfrak{c}(V,q)], \dim(V)+2\mathbb{Z}, d(V,q))$ ist ein Ringhomomorphismus.

Gebe für $K = \mathbb{Q}_p$ die Bilder der Elemente aus $W(K)$ unter w_K explizit an.

Chapter 7

Lösungen zu den Übungsaufgaben.

von David Lorch

Aufgabe 1.

(ii) (Matthias Künzer) Wir schreiben $M = (m_{i,j})_{i,j}$. Sei M' die Adjunkte von M, die an Position (i, j) den Eintrag $(-1)^{i+j} \det M_{j,i}$ hat, wobei $M_{j,i}$ aus M durch Streichen der $j$ten Zeile und der $i$ten Spalte hervorgeht. Nach der Cramerschen Regel ist $M'M = MM' = \det M \cdot I_n$.

(1) Ist f nun ein Automorphismus, so sei g ein Inverses, und N die beschreibende Matrix von g. Es folgt $MN = 1$, und daraus $(\det M)(\det N) = \det(MN) = 1$.

Ist umgekehrt $\det M$ invertierbar, so ist $(\det M)^{-1}M'$ die inverse Matrix zu M, und also die beschreibende Matrix des inversen Endomorphismus.

(2) Ist $\det M$ kein Nullteiler, so folgt f"ur $v \in A^n$ aus $vM = 0$, da"s $vMM' = (\det M) \cdot v = 0$, und also $v = 0$. Somit ist $f : v \mapsto vM$ injektiv.

Ist umgekehrt $\det M$ ein Nullteiler, so sei $x \in A$ mit $x \neq 0$ und $x(\det M) = 0$ gew"ahlt. Sei $r \in [1, n]$ minimal mit $x \det X = 0$ f"ur jede $r \times r$-Untermatrix X von M, die also aus M durch Streichen von $n - r$ beliebigen Zeilen und $n - r$ beliebigen Spalten hervorgeht.

Ist $r = 1$, so ist $xM = 0$, und z.B. $(x, 0, \ldots, 0) \neq 0$ ein Vektor, der von M annulliert wird und so die Injektivit"at von f widerlegt.

Sei nun $r \geq 2$ angenommen. Sei Y eine $(r-1) \times (r-1)$-Untermatrix von M mit $x \det Y \neq 0$. W"ahle die Eintr"age in einer in Y nicht auftretenden Zeile in den Spaltenpositionen von Y, um Y zu einer Untermatrix $Y' \in A^{r \times (r-1)}$ von M zu erg"anzen. F"ur $i \in [1, n]$ sei $y_{(i)} \in A^{r \times 1}$ der aus den Eintr"agen von M der $i$ten Spalte und der Zeilenpositionen von Y' gebildete Spaltenvektor. Sei $Y'_{(i)} \in A^{r \times r}$ die um die Spalte $y_{(i)}$ rechts erg"anzte Matrix Y'. Diese Matrix hat nun entweder eine Spalte doppelt, oder aber ist bis auf Permutation eine Untermatrix von M. Nach Wahl von r ist daher stets $x \cdot \det Y'_{(i)} = 0$.

Eine Entwicklung von $Y'_{(i)}$ nach der eben angef"ugten letzten Spalte liefert $d_i := \det Y_{(i)} = \sum_{z \in Z} m_{z,i} c_z$ f"ur gewisse $c_z \in A$, wobei Z die Menge der in Y' auftretenden Zeilenpositionen bezeichne. Dabei gibt es ein $t \in Z$ mit $c_t = \pm \det Y$, und also $xc_t \neq 0$. Nun ist aber $xd_i = 0$ stets, und also $\sum_{z \in Z}(xc_z)m_{z,i} = 0$ stets, was eine nichttriviale Linearkombination der Nullzeile aus den Zeilen von M darstellt, wie zur Widerlegung der Injektivit"at von f erforderlich.

(3) Sei z.B. $A = \mathbb{Z}/(4)$, $n = 1$ und f die Multiplikation mit 2. Dann ist $\det M = 2 \neq 0$, aber f ist wegen $f(2) = 0$ nicht injektiv.

Aufgabe 3.

(i). Wir nehmen zunächst an dass F e.e. und frei ist. Ein $\varphi \in F^* = \mathrm{Hom}(F, A)$ ist dann eindeutig festgelegt durch die $\varphi(e_i)$. Also ist F^* frei auf den $E := (e_1^*, \ldots, e_n^*)$, definiert durch $e_i^*(e_j) = \delta_{ij}$. Analog ist F^{**} frei auf $E^{**} := (e_1^{**}, \ldots, e_n^{**})$. Der Homomorphismus $\psi : F \to F^{**}, f \mapsto (g \mapsto g(f))$ bildet die Basis E von F auf die Basis E^{**} von F^{**} ab, ist also ein Isomorphismus.

Ist nun F e.e. und projektiv, dann ist F direkter Summand eines *endlich erzeugten* freien Moduls. Man betrachte etwa den Epimorphismus $\pi : A^E \to F$, wo $E = (e_1, \ldots, e_n)$ ein Erzeugendensystem von F ist: da F projektiv, spaltet die kurze exakte Sequenz $0 \hookrightarrow \ker(\pi) \to R^E \twoheadrightarrow F \to 0$, d.h. $R^E \cong F \oplus R^E/\iota(\ker(\pi))$.

Es existiert also ein endlich erzeugter freier Modul G, so dass $F \oplus F' \cong G \cong G^{**} \cong F^{**} \oplus (F')^{**}$ ist. Die Einschränkung dieses Isomorphismus auf F liefert die Reflexivität. (F' ist endlich erzeugt als Quotient von G, und projektiv als direkter Summand von G.)

(ii). Lemma 2.11 in der Vorlesung.

Aufgabe 4.

(i). Wir benutzen eine Aussage aus der Vorlesung *Gitter und Codes* über das subdirekte Produkt von Gittern:

Sei $V = U_1 \oplus U_2$, $\pi_i \in \mathrm{End}(V)$ die Projektionen auf U_i. Sei L ein volles Gitter in V, so dass $L_i := L \cap U_i$ ein volles Gitter in U_i ist ($i = 1, 2$). (dann ist $U_i = KL_i$ und L_i ist reines Teilgitter in L.) Setze $L_i' := L\pi_i$. Dann ist $L_i \leq L_i'$ ($i = 1, 2$) und es gilt:

$$L_1'/L_1 \cong L_2'/L_2 \cong L/(L_1 \oplus L_2) \cong (L_1' \oplus L_2')/L.$$

Beweis.

Klar ist $L_1'/L_1 \cong (L_1' \oplus L_2)/(L_1 \oplus L_2) \cong (L_1' \oplus L_2')/(L_1 \oplus L_2')$.
Wir betrachten zunächst die Projektion $\pi_1 : L \to L_1'$. Gefolgt vom natürlichen Epimorphismus $L_1' \to L_1'/L_1$ liefert sie eine surjektive Abbildung $\overline{\pi_1} : L \to L_1'/L_1$. Sei

$$K_1 := \ker(\overline{\pi_1}) = \{\ell \in L \mid \ell\pi_1 \in L_1\}.$$

Für $\ell = x_1 + x_2 \in L$ mit $x_i \in U_i$ ist $\ell\pi_1 = x_1 \in L_1 = U_1 \cap L$ genau dann wenn $x_1 \in L$ und somit $x_2 = \ell - x_1 \in L \cap U_2 = L_2$ liegt. Also ist $K_1 = L_1 \oplus L_2$ und nach dem Homomorphiesatz gilt

$$L_1'/L_1 = \mathrm{Bild}(\overline{\pi_1}) \cong L/\ker(\overline{\pi_1}) = L/(L_1 \oplus L_2).$$

Ebenso erhält man $L_2'/L_2 \cong L/(L_1 \oplus L_2)$. Für die letzte Isomorphie zeigen wir, dass $L_1' + L = L_1' \oplus L_2'$. Denn dann ist nach dem Noetherschen Isomorphiesatz

$$(L_1' \oplus L_2')/L = (L_1' + L)/L \cong L_1'/(L_1' \cap L) = L_1'/L_1.$$

Nach Definition ist $L_1' + L = \langle L_1', L\rangle$. Es ist $x_1 \in L_1'$ genau dann wenn $x_1 \in U_1$ und es gibt ein $\ell \in L$, $x_2 \in U_2$ mit $\ell = x_1 + x_2$ (dann notwendigerweise $x_2 \in L_2'$). Also ist $L_1' + L \subseteq L_1' \oplus L_2'$.

Umgekehrt liegt natürlich $L_1' \subset L_1' + L$ und obige Rechnung zeigt auch $L_2' \subset L_1' + L$ und damit $L_1' + L = L_1' \oplus L_2'$. □

Nun zum Beweis der Aufgabe. Wir wenden obiges Lemma an auf $U_1 := KX$, $U_2 := U_1^\perp = KX^\perp$, $L_1 = X = U_1 \cap L$, $L_2 = X^\perp = U_2 \cap L$. Damit bleibt zu zeigen, dass $L_1' = \pi_1(L) = X^\#$ und $L_2' = \pi_2(L) = (X^\perp)^\#$.

Dazu sei $x \in X$ und $l \in L$, dann ist $(x, l) = (x, \pi_1(l)) \in \mathbb{Z}$ und daher $\pi_1(L) \subseteq X^\#$. Sei $B' := (b_1, \ldots, b_k)$ eine Gitterbasis von X. Weil U regulär ist, ist X ein reines Teilgitter von L. Deshalb kann B' zu einer Gitterbasis $B = (b_1, \ldots, b_n)$ von L ergänzt werden. Da L unimodular ist ($L = L^\#$), ist auch die duale Basis $B^* = ({b_1}^*), \ldots, {b_n}^*)$ eine Gitterbasis von L, und $({b_{k+1}}^*, \ldots, {b_n}^*)$ eine Gitterbasis von $X^\perp$. Es folgt, dass $X^\# = \langle \pi_1({b_1}^*), \ldots, \pi_1({b_k}^*) \rangle \subseteq \pi_1(L)$.

Aufgabe 7.

(i). Existenz der Zerlegung: Induktion nach $n := \dim(L)$. Für $n = 0$ ist nichts zu zeigen.

Sei nun $n > 0$, und sei $A = (a_{ij})_{1 \le i,j \le n}$ eine Gram-Matrix von L bzgl. einer Basis $B = (b_1, \ldots, b_n)$. Wähle einen Eintrag a_{ij} aus A mit der unter den Einträgen von A minimal auftretenden π-Bewertung r.

(a) $r > 0$: dann fahre fort mit $\pi^{-1}A$.

(b) $r = 0$ und $i = j$: OE sei $i = j = 1$. Durch simultane Zeilen- und Spaltenumformungen kann die erste Zeile und Spalte von A ausgeräumt werden. Fertig mit Induktion.

(c) $r = 0$ und $i \neq j$: OE sei $i = 1, j = 2$. Falls $2 \in R^*$, ist nach der simultanen Zeilen- und Spaltenumformung $b_1' := b_1 + b_2$ aber $\nu_\pi(b_1') = 0$, fahre fort wie in Fall (b). Andernfalls ist der 2×2-Minor $(a_{i,j})_{1 \le i,j \le 2}$ invertierbar, da $\nu_\pi(a_{11}a_{22} - a_{12}^2) = 0$. Also ist jedes Tupel (x, y) Linearkombination von (a_{11}, a_{12}) und (a_{12}, a_{22}), d.h. die ersten beiden Zeilen und Spalten können durch simultane Zeilen- und Spaltenumformungen ausgeräumt werden und man ist fertig mit Induktion.

Zu den Eindeutigkeitsaussagen für $R = \mathbb{Z}_p$: angenommen, es existieren zwei Zerlegungen $\bigperp(L_i, \pi^i b_i)$ und $\bigperp(L_i', \pi^i b_i')$. Es genügt, $(L_0, b_0) \cong (L_0', b_0')$ zu zeigen und dann mit dem reskalierten Gitter $(L_1, \pi^0 b_i) \perp \cdots \perp (L_c, \pi^{c-1} b_c)$ fortzusetzen. Dann ist $\det(L) + \pi R = \det(L_0) + \pi R = \det(L'_0) + \pi R$, und auch die Dimensionen von L_0 bzw. L'_0 müssen offenbar gleich sein. ber $\mathbb{F}_p$ lassen sich die beiden Zerlegungen nun schreiben als $(\overline{L}, \overline{b}) \cong (\overline{L_0}, \overline{b_0}) \perp Q \cong (\overline{L_0'}, \overline{b_0'}) \perp Q$ mit $Q := \{l + \pi R \in \overline{L} : b(l, l) \in \pi R\}$. Also $(\overline{L_0}, \overline{b_0}) \cong (\overline{L}, \overline{b})/Q \cong (\overline{L_0'}, \overline{b_0'})$ Da alle auftretenden Jordan-Komponenten regulär sind (für $p = 2$ stellt das die Zusatzbedigung sicher, dass alle L_i gerade Gitter sind), existieren die zugehörigen quadratischen $\mathbb{F}_p$-Moduln, und sind ebenfalls isometrisch. Da diese als orthogonale Summanden von L außerdem scharf primitiv sind, liftet diese Isometrie nach $\mathbb{Z}_p$. Setze fort mit den um π^{-1} reskalierten restlichen Summanden, also mit $(L_1, \pi^0 b_1) \perp \cdots \perp (L_c, \pi^{c-1} b_c)$.

(iii). (a) Dass die Gitter über $\mathbb{Z}$ nicht isometrisch sind, sieht man z.B., weil ihre Minima verschieden sind (8 bzw. 2).

(b) Bezeichne $(L_0, b_0) \perp (L_1 \perp 2b_1)$ das bereits jordanzerlegte Gitter aus der Aufgabenstellung. Durch Addieren des dritten Basisvektors zur zweiten Zeile und Spalte und anschließenden Ausräumen der dritten Zeile und Spalte erhält man den $\mathbb{Z}_2$-invertierbaren

Basiswechsel $b'_1 := b_1$, $b'_2 := b_2 + b_3$, $b'_3 := \frac{2}{7}b_1 - \frac{4}{7}b_2 + \frac{3}{7}b_3$, bezüglich dem das Gitter $\mathbb{Z}_2 \otimes L$ die Gram-Matrix

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & 4 & 0 \\ 0 & 0 & \frac{6}{7} \end{pmatrix} \tag{0.1}$$

besitzt, welches wir mit $(L'_0, b'_0) \perp\!\!\!\perp (L'_1, b'_1)$ bezeichnen. Aber L_0 und L'_0 sind als $\mathbb{Z}$-Gitter nicht isometrisch, denn ihre Determinanten unterscheiden sich modulo 8 nicht um ein Quadrat.

Aufgabe 8.

Sei $D := (L^\#/L, \overline{q})$, wobei $\overline{q} : L^\#/L \to \mathbb{Q}/\mathbb{Z}, x + L \mapsto \frac{1}{2}b(x,x) + \mathbb{Z}$.

Von D spalten wir solange hyperbolische Ebenen ab, bis ein anisotroper Rest bleibt. Falls $k = \dim(L_1)$ ungerade ist, bleibt stets ein Rest von Dimension 1, und falls k gerade ist bleibt ein Rest von Dimension 0 oder 2.

Nur für diese Fälle berechnen wir die Gauß-Summe. Mit dem Hinweis aus der Aufgabenstellung ist

$$\Gamma([1]) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ i, & p \equiv 3 \bmod 4 \end{cases} \tag{0.2}$$

Bezeichne ε ein Element aus $\mathbb{F}_p^* \backslash (\mathbb{F}_p^*)^2$. Da $\Gamma([1]) + \Gamma([\varepsilon]) = \sum_{l=0}^{p-1} {\zeta_p}^l = 0$ (ζ_p ist Nullstelle des p-ten Kreisteilungspolynoms), folgt $\Gamma([\varepsilon]) = -\Gamma([1])$. Aus der Multiplikativität der Gauß-Summe erhält man dann die Werte für den zweidimensionalen anisotropen Raum über $\mathbb{F}_p$ (d.i. $[1, \varepsilon]$, falls $-1 \in (\mathbb{F}_p^*)^2$, also falls $p \equiv 1 \bmod 4$, und andernfalls ist $[1,1]$ anisotrop). Man erhält also folgende Gauß-Summen für die ein- und zweidimensionalen anisotropen Räume:

Γ	$[1]$	$[\varepsilon]$	$(\mathbb{F}_{p^2}, N)$
$p \equiv 1 \bmod 4$	1	-1	-1
$p \equiv 3 \bmod 4$	i	$-i$	-1

Mit der Formel von Milgram/Braun ist $\zeta_8^{\mathrm{sign}(\mathbb{R}L)} = \Gamma(L^\#/L, \overline{q})$. Um die Gleichung aus der Aufgabenstellung zu beweisen, muss also die Determinante des regulären bilinearen Raums $(L_1, b_1) \cong (1, \ldots, 1, a)$ (mit $a + p\mathbb{Z} \in \{1, \varepsilon\}$) mit der des quadratischen Raums $D = \mathbb{H}^m \perp\!\!\!\perp A$ (mit $A \in \{[], [1], [\varepsilon], [(\mathbb{F}_{p^2}, N)]\}$) verglichen werden.

Ist $k = \dim(L_1)$ ungerade, so muss man zum Beweis der Gleichung nach $p \bmod 8$ unterscheiden. Denn für $p \equiv 1 \bmod 4$ ist -1 ein Quadrat in $\mathbb{F}_p$, und für $p \equiv \pm 1 \bmod 8$ ist 2 ein Quadrat in $\mathbb{F}_p$:

(i). Ist -1 kein Quadrat, dann ist $\det(\mathbb{H})$ kein Quadrat. Ist gleichzeitig $k \in 4\mathbb{Z} + 3$ und ist also $D = \mathbb{H}^m \perp\!\!\!\perp [b]$ für eine ungerade Zahl $m = \frac{k-1}{2}$ hyperbolischer Ebenen, dann unterscheiden sich $a = \det((L_1, b_1))$ und b um ein Nichtquadrat ε.

(ii). Ist 2 kein Quadrat, dann unterscheidet sich die Determinante des zu (L_1, b_1) gehörigen quadratischen Raums um ein Nichtquadrat. Es ändert sich also das Vorzeichen von $\Gamma(L^\#/L)$.

Für gerades k entfällt die Unterscheidung, ob 2 ein Quadrat in $\mathbb{F}_p$ ist, da beim bergang zum quadratischen Raum eine gerade Anzahl von Vorfaktoren $\frac{1}{2}$ auftritt. Es genügt also dann die Fälle $p \equiv 1 \bmod 4$ und $p \equiv -1 \bmod 4$ zu behandeln.

Anmerkung: Eine Herleitung der Summenformel für $\Gamma([1])$ aus der Aufgabenstellung findet sich etwa in Ireland/Rosen, A Classical Introduction To Modern Number Theory, Proposition (6.4.3).

Aufgabe 9.

vgl. Abschnitt 15 im Kneser.

Aufgabe 10.

vgl. Beispiel 9.22.

Aufgabe 11.

(ii) Allgemein sei $V = \mathbb{H}^m$, und $\mathrm{char}(K)$ beliebig. Wähle $U \leq V$ mit maximal isotrop, also $q(U) = \{0\}$ und $\dim(U) = m$.

Es sei

$$D : O(V) \to \{\pm 1\}, g \mapsto (-1)^{\dim(U/(g(U)\cap U))}. \tag{0.3}$$

Zu zeigen: D ist Gruppenepimorphismus mit Kern $SO(V)$. Beweis:

(a) Nach dem Satz von Witt operiert $O(V)$ transitiv auf $J := \{U \leq V \mid q(U) = \{0\}, \dim(U) = m\}$. Haben wir gezeigt, dass D ein Homomorphismus ist, dann ist D automatisch unabhängig von U.

(b) Wir definieren einen Graphen Γ mit Eckenmenge J, in dem zwei Ecken U und W genau dann durch Kanten verbunden sind, wenn $\dim(U/(U \cap W)) = 1 (= \dim(W/(U \cap W)))$. Auf Γ definieren wir noch $d : J \times J \to \mathbb{N}_0$, $d(U, W) :=$ Abstand von U und W in Γ.

(c) Falls $\dim(U/(U \cap W)) = 1$, dann existiert ein $x \in V$ mit $q(x) = 1$ und $W = s_x(U)$, wobei s_x die Spiegelung an x bezeichne:

Sei dazu $e \in U \backslash U \cap W$. Dann ist $e \notin W = W^\perp$, also existiert ein $f \in W$ mit $b_q(e, f) = 1$. Setze $x := e + f$. Dann ist $s_x|_{U\cap W} = \mathrm{id}|_{U\cap W}$, $s_x(e) = e - \frac{b_q(x,e)}{q(x)}x = e - x = -f$, und analog $s_x(f) = -e$.

Also wird $U = \langle e, U \cap W\rangle$ unter s_x abgebildet auf $\langle f, U \cap W\rangle = W$.

(d) Es ist $d(U, W) = \dim(U/(U \cap W))$: Beweis mit Induktion nach $k := \dim(U/(U \cap W))$.

Für $k = 1$ ist der Abstand d in Γ definiert als $\dim(U/(U \cap W))$.

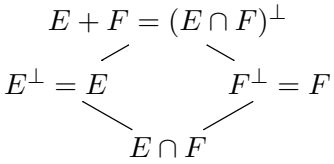
Für $k > 1$ konstruieren wir ein W_1, das in Γ näher an U liegt, nämlich so dass $d(W_1, W) = 1$ und $\dim(U/(W_1 \cap U)) = k-1$. Sei dazu $e \in U\backslash(U\cap W)$. Da $e \notin W = W^\perp$, ist $b_W(e)$ nicht die Nullabbildung. Deshalb ist $e^\perp \cap W = \mathrm{Kern}(b_W(e)) < W$ vom Index 1 in W. Der total isotrope Raum $W_1 := (e^\perp \cap W) + \langle e\rangle$ liegt deshalb in J.

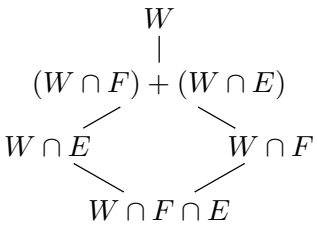
Es ist $U \cap (W + \langle e\rangle) = U \cap W_1$ und $d(W, W_1) = 1$ nach Wahl von W_1, und außerdem $\dim(U/(U \cap W_1)) = \dim(U/(U \cap W)) - 1$. Es ist darum $d(U, W) \leq d(U, W_1) + d(W_1, W) \leq_{\text{Ind.vorauss.}} k - 1 + 1 = k = \dim(U/(U \cap W))$. Es ist aber auch, für einen Weg $(W, W_1, \ldots, W_l, U)$ von W über W_1 zu U der Länge $d(U, W_1) + 1$ in Γ: $\dim(U/(U\cap W)) \leq \dim(U/(U\cap W_l)) + \dim((U\cap W_l)/(U\cap W_l\cap W_{l-1})) + \cdots + \dim((U\cap W_l\cap\cdots\cap W_2)/(U\cap W_l\cap W_{l-1}\cap\cdots\cap W_1)) = d(U, W_1) + 1$. Es gilt also $d(W_1, W) = k$.

(e) Angenommen es gäbe einen Kreis ungerader Länge in Γ, dann gäbe es Ecken E, F, W in Γ mit $d(E, W) = d(F, W) = k$ und $d(E, F) = 1$.

i. Dann wäre $E \cap W = F \cap W$: betrachte dazu den quadratischen $\mathbb{F}_2$-Vektorraum $X := (E + F)/(E \cap F)$. Dieser ist isotrop, da E (und F) nach Definition von Γ

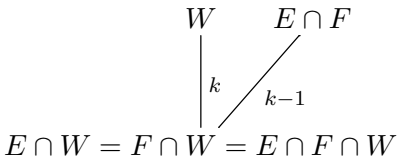
total isotrop sind. Es muss also $X \cong \mathbb{H}$ sein. Die hyperbolische Ebene hat zwei total singuläre Teilräume.





Angenommen, $E \cap W \neq F \cap W$. Dann kann man $e \in (W \cap E) \backslash (W \cap F \cap E)$, $f \in (W \cap F) \backslash (W \cap F \cap E)$ wählen. Es ist dann $\langle e, f \rangle \subseteq W$, also $q(\langle e, f \rangle) = 0$. Da $E = \langle e, E \cap F \rangle$, $F = \langle f, E \cap F \rangle$ und $E + F = \langle e, f, E \cap F \rangle$ für gewisse $x, y \in V$ gilt, wären aber die drei Teilräume $\langle e + E \cap F \rangle$, $\langle f + E \cap F \rangle$ und $\langle e, f, E \cap F \rangle$ alle verschieden und total singulär. Widerspruch, deshalb ist $E \cap W = F \cap W$.

ii. Also haben wir folgende Situation:



Es ist $b_W(E \cap F) \leq U^*$ ein Teilraum der Dimension $\dim((E \cap F)/(W \cap E \cap F)) = (m-1)-(m-k) = k-1$. Also $\dim(W/(W \cap (E \cap F)^\perp)) = \dim(W/(W \cap (E+F))) = k-1$. Deshalb existiert ein $z \in (E+F) \cap W$ mit $z \notin E$ und $z \notin F$. Da $z \in W$, ist $q(z) = 0$, $\langle z + E \cap F \rangle \leq (E+F)/(E \cap F)$ ist isotrop, aber $z \notin E \cup F$, und deshalb haben wir mit den bereits oben definierten $\langle e + E \cap F \rangle$, $\langle f + E \cap F \rangle$ wieder insgesamt drei total singuläre Teilräume von $X = (E+F)/(E \cap F)$ gefunden. Widerspruch.

Γ kann also keine Kreise ungerader Länge haben.

(f) Für alle $g, h \in O(V)$ ist $d(U, g(U)) + d(g(U), (g \circ h)(U)) = d(U, g(U)) + d(U, h(U)) \equiv d(U, gh(U)) \bmod 2$:

Das folgt aus (v)., denn $d(U, g(U)) + d(U, h(U)) + d(U, gh(U))$ ist die Länge eines Kreises in Γ.

Insbesondere ist $D : O(V) \to \{\pm 1\}$ ein Homomorphismus. Weiter folgt aus (iii)., dass $D(s_x) = -1$, und dass $\mathrm{Kern}(D)$ die geraden Produkte von Spiegelungen sind. Wir zeigen noch $\dim(U/(U \cap s_x(U))) = 1$. Dazu sei $x \notin U = U^\perp$, dann ist $U = (x^\perp \cap U) \oplus \langle e \rangle$. $U \cap s_x(U) \supseteq x^\perp \cap U$, und $s_x(u + ae) = u + ae - \frac{b_q(x, ae)}{q(x)} x \notin U$.

Aufgabe 12

Lemma: Für die Clifford-Invarianten zweidimensionaler Räume über $\mathbb{Q}_p$ gilt $\mathfrak{c}([a,b]) = 1 \Leftrightarrow [a,b]$ stellt 1 dar.

Beweis: "$\Leftarrow$": Falls $E = [a,b]$ den Wert 1 darstellt, existiert ein $e \in \mathcal{C}(E)$, linear unabhängig zu 1, mit $e^2 = 1$. Also ist $(e-1)(e+1) = 0$ und beide Faktoren sind ungleich Null, d.h. $\mathcal{C}(E)$ ist nicht nullteilerfrei, also keine Divisionsalgebra. Die einzige andere zentral einfache Algebra über $\mathbb{Q}_p$ ist aber der Matrixring $\mathbb{Q}_p^{2\times 2}$, also das triviale Element der Brauergruppe. (Das funktioniert aber auch allgemein, wie in Aufgabe 10(i) kann man aus der Operation von $\mathcal{C}(E)$ auf $(1-e)\mathcal{C}(E)$ einen expliziten Isomorphismus nach $\mathbb{Q}_p^{2\times 2}$ konstruieren.)

"$\Rightarrow$": Falls $\mathfrak{c}([a,b]) = 1$, ist $\mathcal{C}(E)$ keine Divisionsalgebra, d.h. es gibt ein $x \in \mathfrak{c}([a,b])$ mit Norm 0. Als quadratischer Raum (wie in Beispiel 9.22(ii)) ist $\mathcal{C}(E) = [1, -a, -b, ab]$ (mit Basis

$(1, e_1, e_2, e_1e_2)$) also isotrop. Man sieht leicht ein, dass für einen regulären quadratischen Raum (E, q) über einem Körper K genau dann $a \in q(E)$, wenn $E \perp [-a]$ nicht anisotrop ist. Der Raum $\mathcal{C}(E)'$, der durch die Basis (e_1, e_2, e_1e_2) definiert sei, stellt also -1 dar, und kann deshalb als $[-1] \perp \mathcal{C}(E)''$ geschrieben werden. Vergleich der Diskriminanten ergibt $d(\mathcal{C}(E)'') = -1$, d.h. der Raum $\mathcal{C}(E)''$, also auch $\mathcal{C}(E)'$, ist hyperbolisch und deshalb isotrop. Mit demselben Argument wie oben stellt der Raum $[-a, -b]$ also den Wert $-ab$ dar. Es gibt also ein Tupel (x, y), für das gilt: $-ax^2 - by^2 = -ab$. Dann ist aber $q(\frac{y}{a}, \frac{x}{b}) = 1$.

Die regulären anisotropen Räume über $\mathbb{Q}_p$ mit Clifford-Invariante $-1 = [\mathcal{Q}_p]$ sind also genau diejenigen, die 1 nicht darstellen. Wir bestimmen eine Liste der regulären anisotropen quadratischen Räume über $\mathbb{Q}_p$, und entscheiden ob sie jeweils 1 darstellen oder nicht.

Lemma: Sei (E, q) zweidimensionaler quadratischer Raum über einen Körper K und nicht ausgeartet, mit $1 \in q(E)$. Dann ist $q(E) \leq K^*/(K^*)^2$ eine Untergruppe.

Beweis: Für ein $a(K^*)^2 \in K^*/(K^*)^2$ ist $(E, q) \cong [1, a]$. Es ist $K[x]/(x^2 - a)$ ein Körper, falls das eben gewählte $a \notin (K^*)^2$. Sein Galoisautomorphismus ist $t \mapsto -t$, also $\mathrm{Norm}(x + y\sqrt{a}) = x^2 - ay^2$. Die Norm ist multiplikativ und entspricht also der quadratischen Form auf $[1, -a]$. Der hyperbolische Fall $(E, q) \cong [1, -1]$ ist klar. □

Lemma: Sei (E, q) zweidimensionaler quadratischer Raum über einem Körper K und nicht ausgeartet, mit $1 \in q(E)$. Für $\lambda \in q(E)$ stellen die quadratischen Formen auf V und seiner Reskalierung ${}^{\lambda}V$ dieselben Werte dar, für $\lambda \notin q(E)$ sind die Wertemengen disjunkt.

Beweis: $q(E) \leq K^*/(K^*)^2$, also $x \in {}^{\lambda}q(E) \cap q(E) \Rightarrow q({}^{\lambda}E) = \lambda \cdot q(E) = q(E)$. □

Für die anisotropen zweidimensionalen Formen über $\mathbb{Q}_2$, die 1 darstellen: $E = [a, b]$ stellt mindestens zwei verschiedene Quadratklassen dar (für $a = b$ nämlich a und $2a$) und eine weitere Quadratklasse, die man immer durch Einsetzen von $(1, 2)$ erhält. Man sieht schnell, dass E nicht alle Quadratklassen darstellt. Also müssen wegen obigen Lemma genau 4 Werte angenommen werden, und den vierten bekommt man aus der Gruppeneigenschaft. Die anisotropen zweidimensionalen Formen, die 1 nicht darstellen, bekommt man durch Reskalierung.

$\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ sei im Folgenden vertreten durch $\{1, 3, 5, 7, 2, 6, 10, 14\}$ für $p = 2$, und durch $\{1, \varepsilon, p, p\varepsilon\}$ für $p \neq 2$.

Ein zweidimensionaler quadratischer Raum ist genau dann hyperbolisch, wenn die Quadratklasse seiner Determinante die Quadratklasse von -1 ist. Unter den Räumen, die 1 darstellen, ist also genau $[1, 7]$ hyperbolisch für $p = 2$, $[1, 1] = [1, -1]$ für $p \equiv 1 \bmod 4$, und $[1, \varepsilon] = [1, -1]$ für $p \equiv 3 \bmod 4$.

Man erhält insgesamt folgende anisotrope Räume der Dimension 2, und die von ihnen dargestellten Quadratklassen:

Für $\mathbb{Q}_2$:

$\mathfrak{c}(E) = 1$	Quadratklassen	$\mathfrak{c}(E) = -1$	Quadratklassen
$[1, 1]$	$2, 10, 1, 5$	$[3, 3]$	$6, 14, 3, 7$
$[1, 3]$	$1, 3, 5, 7$	$[2, 6]$	$2, 6, 10, 14$
$[1, 5]$	$6, 14, 1, 5$	$[3, 7]$	$2, 10, 3, 7$
$[1, 2]$	$2, 6, 1, 3$	$[5, 10]$	$10, 14, 5, 7$
$[1, 6]$	$6, 10, 1, 7$	$[3, 2]$	$2, 14, 3, 5$
$[1, 10]$	$10, 14, 1, 3$	$[5, 2]$	$5, 7, 2, 6$
$[1, 14]$	$2, 14, 1, 7$	$[3, 10]$	$6, 10, 3, 5$

Für $\mathbb{Q}_p$, $p > 2$:

$\mathfrak{c}(E)=1$	Quadratklassen	$\mathfrak{c}(E)=-1$	Quadratklassen
$[1,-\varepsilon]$	$1,\varepsilon$	$[p,-p\varepsilon]$	$p,p\varepsilon$
$[1,p]$	$1,p$	$[\varepsilon,p\varepsilon]$	$\varepsilon,p\varepsilon$
$[1,p\varepsilon]$	$1,p\varepsilon$	$[\varepsilon,p]$	ε,p

Dass es in Dimension 4 nur einen einzigen anisotropen Raum gibt, ist bereits aus der Vorlesung bekannt. Es bleiben also noch die dreidimensionalen anisotropen Räume zu bestimmen. Für $p>2$ sieht man aus der Tabelle für den zweidimensionalen Fall und der Bemerkung von oben (dass $a\in q(E)$, genau dann wenn $E\perp[-a]$ nicht anisotrop ist), dass die vier nicht isometrischen Reskalierungen von $[p,-p\varepsilon,-\varepsilon]$ anisotrop sind. Für $p=2$ sieht man genauso, dass die acht Reskalierungen von $[1,1,1]$ anisotrop sind. Dass diese Räume jeweils nicht isometrisch sind, sieht man aus den dargestellten Quadratklassen – so stellt etwa $[p,-p\varepsilon,-\varepsilon]$ jede Quadratklasse bis auf $-\det([p,-p\varepsilon,-\varepsilon])$ dar. Weil wir die anisotropen Räume anderer Dimension und die Ordnung der Witt-Gruppe bereits kennen, wissen wir, dass wir damit bis auf Isometrie alle gefunden haben.

Als Clifford-Invariante der dreidimensionalen anisotropen Räume E über $\mathbb{Q}_p$ erhält man mit (12.11)(b):

$$\mathfrak{c}([e_1,e_2,e_3])=\begin{cases}-1, & p=2\\ -1, & p\equiv 1 \bmod 4\\ 1, & p\equiv 3 \bmod 4\end{cases} \tag{0.4}$$

Aufgabe 14

(i). $b: V\times W\times V\times W\to K$, $(v,w,v',w')\mapsto b_q(v,v')b_q(w,w')$ ist eine K-multilineare Abbildung und induziert deshalb die gewünschte Abbildung auf $(V\otimes W)\times(V\otimes W)$. Die zugehörige Gram-Matrix ist das Kroneckerprodukt der Gram-Matrizen von V und W, Q ist die zugehörige quadratische Form.

(ii). Die hyperbolische Ebene $\mathbb{H}$ ist das neutrale Element der Multiplikation, denn für einen eindimensionalen Raum $V=[a]$ ist $V\otimes\mathbb{H}=\begin{pmatrix}0 & a\\ a & 0\end{pmatrix}$ hyperbolisch. Da $\operatorname{char}(K)\neq 2$ genügt es, die eindimensionalen Räume zu betrachten.

Die Distributivität von $\otimes$ und $\perp$ sieht man sofort aus den Eigenschaften des Kroneckerprodukts.

(iii). Seien $V=[1^r,(-1)^s]$, $W=[1^{r'},(-1)^{s'}]\in W(\mathbb{R})$. Dann erhält man aus dem Kroneckerprodukt der Gram-Matrizen: $[V]\otimes[W]=[[1^{rr'+ss'},(-1)^{rs'+r's}]]$, also $\operatorname{sign}(V\otimes W)=rr'+ss'-rs'-r's=(r-s)(r'-s')=\operatorname{sign}(V)\operatorname{sign}(W)$. Der Rest ist klar.

(iv). $\dim(V\otimes W)=\dim(V)\dim(W)$ (Kroneckerprodukt). Ferner ist die Dimension hyperbolischer Räume gerade.

(v). Sei $n:=\dim(V),\widetilde{n}:=\dim(W)$. Es ist $\mathrm{d}(V\otimes W)=(-1)^{\binom{mn}{2}}\det(V\otimes W)=(-1)^{\binom{mn}{2}}\det(V)^m\det(W)^n$ (Kroneckerprodukt!) – bleibt zu zeigen, dass $(-1)^{\binom{mn}{2}}=(-1)^{n\binom{m}{2}}(-1)^{m\binom{n}{2}}$, also dass $mn(mn-1)\equiv nm(m-1)+mn(n-1)=mn(m+n)-2mn \bmod 4$. Man sieht schnell, dass diese Gleichung immer erfüllt ist.

(vi). Für einen quadratischen Raum (E,q) über K und $\alpha\in K$ bezeichne ${}^{\alpha}E$ den reskalierten Raum $(E,\alpha q)$. Wie in Satz (12.11) bezeichne weiter $m(E):=\left\lceil\frac{\dim(E)}{2}\right\rceil$, $r(E):=m(E)-1\equiv\binom{\dim(E)}{2} \bmod 2$, $s(E):=\binom{m(E)}{2}$.

Sei $n+1 := \dim(V)$ und $\widetilde{n} := \dim(W)$.

Einige Vorbemerkungen:

(a) Ist $\gamma \in K^*$, dann ist nach Satz (12.11): $\mathfrak{c}(\gamma W) = (\gamma,-1)^{\binom{\widetilde{n}}{2}}(\gamma,\det(W))^{\widetilde{n}-1}(-1,\gamma)^{\widetilde{n}r(W)}\mathfrak{c}(W)$. Also ist

$$\mathfrak{c}(\gamma W) = \begin{cases} (\gamma, d(W))c(W), & \widetilde{n} = \dim(W) \in 2\mathbb{Z} \\ (\gamma,(-1)^{\binom{\widetilde{n}}{2}+r(W)})\mathfrak{c}(W) = \mathfrak{c}(W), & \text{sonst} \end{cases} \tag{0.5}$$

(b) Sei $V = [a_1,\ldots,a_n] =: V' \perp\!\!\!\perp [a_{n+1}]$, und sei n ungerade. Dann ist $r(V) = r(V'), s(V) = s(V'), m(V) = m(V')$. Weiter ist $\mathfrak{c}(V) = \mathfrak{c}(V')\cdot(d(V'),a_{n+1})$.
Ist n gerade, dann ist $r(V) = r(V')+1$, $s(V) = s(V')+m(V')$, $m(V) = m(V')+1$ und $\mathfrak{c}(V) = \mathfrak{c}(V')(\det(V'),-a_{n+1})(-1,a_{n+1})^{r(V')}(-1,-1)^{m(V')}$.

(c) Nach (12.10) haben die Quaternionensymbole, nach (12.11) auch beliebige Clifford-Invarianten von Räumen über K Ordnung 2 in der Brauer-Gruppe von K.

(d) Ist $\widetilde{n} = \dim(W)$ gerade und $V = V' \perp\!\!\!\perp [a_{n+1}]$, dann gilt: $\dim(V'\otimes W) = n\widetilde{n}$ ist gerade. Mit dem Kroneckerprodukt und (10.8)(a) erhält man $\mathfrak{c}(V\otimes W) = \mathfrak{c}((V'\perp\!\!\!\perp[a_{n+1}])\otimes W) = \mathfrak{c}(V'\otimes W \perp\!\!\!\perp {}^{a_{n+1}}W) = \mathfrak{c}(V'\otimes W)\mathfrak{c}({}^{(-1)^{\frac{n\widetilde{n}}{2}}\det(V'\otimes W)a_{n+1}}W)$.
Ist $\widetilde{n}$ ungerade und V wie oben, dann ist $\dim(V'\otimes W) = n\widetilde{n}$ ungerade. Wir behaupten, dass folgender Zusatz zu (10.8) gilt: Haben E_1 und E_2 beide ungerade Dimension, dann ist $C(E) \cong C_0(E_1,q_1)\otimes C_0(E_2,q_2)\otimes \left(\begin{smallmatrix} d'(E_1),d'(E_2) \\ K \end{smallmatrix}\right)$, wobei die $d'(E_i)$ wie in (10.8)(b) die Halbdiskriminanten der mit $\frac{1}{2}$ reskalierten Bilinearformen b_{q_i} sind. Also gilt dann auch $\mathfrak{c}(V\otimes W) = \mathfrak{c}(V'\otimes W)\mathfrak{c}({}^{a_{n+1}}W)(d(V'\otimes W), d({}^{a_{n+1}}W))$.
Beweis: Es bettet $\mathcal{C}_0(E_1)\otimes\mathcal{C}_0(E_2)$ in $\mathcal{C}(E_1 \perp\!\!\!\perp E_2) \cong \mathcal{C}(E_1)\hat{\otimes}\mathcal{C}(E_2)$ ein. Hat E_1 eine Orthogonalbasis $(e_1,\ldots,e_n)$ und E_2 eine Orthogonalbasis $(\widetilde{e_1},\ldots,\widetilde{e_{\widetilde{n}}})$, und setzt man $z_{E_1} := \prod e_i \in Z(\mathcal{C}(E_1))$ und $z_{E_2} := \prod \widetilde{e_i} \in Z(\mathcal{C}(E_2))$, dann hat $Z := \mathcal{C}(E_1 \perp\!\!\!\perp E_2)^{\mathcal{C}_0(E_1)\perp\mathcal{C}_0(E_2)}$ eine K-Basis $(1\otimes 1, z_{E_1}\otimes 1, 1\otimes z_{E_2}, z_{E_1}\otimes z_{E_2})$, die genau die Relationen von $\left(\begin{smallmatrix} d(E_1),d(E_2) \\ K \end{smallmatrix}\right)$ erfüllt.

Nun zum Beweis der eigentlichen Aussage, mit Induktion nach $n = \dim(V)$ und $\widetilde{n} = \dim(W)$:

Induktionsanfang: für $n = \widetilde{n} = 1$ sind alle auftretenden Clifford-Invarianten trivial, die Aussage ist klar.

Induktionsvoraussetzung: Sei die Aussage für festes n, $\widetilde{n} \in \mathbb{N}$ bereits bewiesen.

Induktionsschritt: Es ist lediglich der Schritt $n \to n+1$ zu zeigen, da man die Rollen von V und W vertauschen kann.

- Sei zunächst $\widetilde{n} = \dim(W)$ gerade und $n = \dim(V) \in \mathbb{N}$ beliebig.
  Mit der Induktionsvoraussetzung und der dritten und vierten Vorbemerkung gilt

$$\begin{aligned} \mathfrak{c}(V\otimes W) &= \mathfrak{c}(V')^{\widetilde{n}}\mathfrak{c}(W)^n(d(V'),d(W))^{n\widetilde{n}-1}\mathfrak{c}({}^{(-1)^{\frac{n\widetilde{n}}{2}}\det(V'\otimes W)a_{n+1}}W) \\ &= \mathfrak{c}(W)^n(d(V'),d(W))\mathfrak{c}({}^{(-1)^{\frac{n\widetilde{n}}{2}}\det(W)^n a_{n+1}}W) \\ &= \mathfrak{c}(W)^{n+1}(d(V'),d(W))((-1)^{\frac{n\widetilde{n}}{2}}\det(W)^n a_{n+1}, d(W)) \end{aligned}$$

(Die letzte Gleichheit gilt nach der ersten Vorbemerkung.)

Zu zeigen ist $\mathfrak{c}(V \otimes W) \stackrel{!}{=} \mathfrak{c}(W)^{n+1}(d(V), d(W))$ (wieder wegen dritter Vorbemerkung).
Falls n ungerade, ist $d(V) = -a_{n+1}d(V')$, und da für gerades $\widetilde{n}$ gilt $\binom{\widetilde{n}}{2} \equiv \frac{\widetilde{n}}{2} \bmod 2$, ist:
$(d(V'), d(W))((-1)^{\frac{n\widetilde{n}}{2}} \det(W)^n a_{n+1}, d(W))$
$= ((-1)^{\binom{\widetilde{n}}{2}} \det(W)(-1)d(V), d(W)) = (-d(W), d(W))(d(V), d(W)) = (d(V), d(W))$,
was zu zeigen war.
Falls n gerade, ist $d(V) = a_{n+1}d(V')$ und ebenfalls $(d(V'), d(W))((-1)^{\frac{n\widetilde{n}}{2}} \det(W)^n a_{n+1}, d(W)) = (-d(V)d(W), d(W)) = (d(V), d(W)$.

- Sei nun $\widetilde{n}$ ungerade, und schreibe wieder $V = V' \bigoplus [a_{n+1}]$.
  Wir dürfen annehmen, dass auch $n+1$ ungerade ist, da man sonst die Rollen von V und W in der Gleichung vertauschen kann und im ersten Fall ist.
  Analog zu oben folgt aus der Induktionsvoraussetzung und den Vorbemerkungen:

$$\begin{aligned}
\mathfrak{c}(V \otimes W) &= \mathfrak{c}(V' \otimes W)\mathfrak{c}({}^{a_{n+1}}W)(d(V' \otimes W), d({}^{a_{n+1}}W)) \\
&= \mathfrak{c}(V' \otimes W)\mathfrak{c}(W)(d(V' \otimes W), d(W)a_{n+1}) \\
&= \mathfrak{c}(V')^{\widetilde{n}}\mathfrak{c}(W)^n(d(V'), d(W))^{n\widetilde{n}-1}\mathfrak{c}(W)(d(V' \otimes W), d(W)a_{n+1}) \\
&= \mathfrak{c}(V')(d(V'), d(W))\mathfrak{c}(W)(d(V' \otimes W), d(W)a_{n+1}) \\
&= \mathfrak{c}(V')(d(V'), d(W))\mathfrak{c}(W)(d(V'), d(W)a_{n+1}) = \mathfrak{c}(V')\mathfrak{c}(W)(d(V'), a_{n+1})
\end{aligned}$$

  Zu zeigen ist $\mathfrak{c}(V \otimes W) \stackrel{!}{=} \mathfrak{c}(V)^{\widetilde{n}}\mathfrak{c}(W)^{n+1}(d(V), d(W))^{(n+1)\widetilde{n}-1} = \mathfrak{c}(V)\mathfrak{c}(W)$.
  Es bleibt also zu zeigen, dass $\mathfrak{c}(V) \stackrel{!}{=} \mathfrak{c}(V')(d(V'), a_{n+1})$. Dies folgt mit der zweiten Vorbemerkung.

Index