

# QUADRATIC FORMS AND CLASS FIELDS II: LECTURE NOTES

NICOLAS DAANS

## CONTENTS

Notations and conventions	2
Acknowledgements	2
1. Lecture 1	2
1.1. Bilinear and quadratic forms	2
1.2. Orthogonality and diagonalisation	6
1.3. Exercises	8
2. Lecture 2	9
2.1. Isotropic, totally isotropic, and hyperbolic forms	9
2.2. Witt's Theorems	12
2.3. Exercises	14
3. Lecture 3	14
3.1. Tensor products of symmetric bilinear spaces	14
3.2. Exercises	18
4. Lecture 4	18
4.1. Witt equivalence and the Witt ring	18
4.2. Determinants and discriminants	20
4.3. Multiplicative forms	21
4.4. Exercises	23
5. Lecture 5	24
5.1. Powers of the fundamental ideal	24
5.2. Exercises	25
6. Lecture 6	26
6.1. Signatures and orderings	26
6.2. Field extensions	28
6.3. Exercises	31
Index	32
References	33

---

*Date:* Wednesday 29<sup>th</sup> March, 2023.

**Notations and conventions.** We denote by  $\mathbb{N}$  the set of natural numbers. We write  $\mathbb{N}^+$  for the proper subset of non-zero numbers. For a ring  $R$ , we denote by  $R^\times$  the set of invertible elements of  $R$ ; if  $R$  is a field, then  $R^\times = R \setminus \{0\}$ .

**Acknowledgements.** The course follows to a large extent the exposition from Lam’s book [Lam05]. For this introductory course, we focus on fields of characteristic different from 2, where the theory of quadratic forms is simpler than over fields of characteristic 2. The book of Elman, Karpenko and Merkurjev [EKM08] is a great reference for those who want to learn more about quadratic form theory over fields of arbitrary characteristic, and some parts of this course which hold in arbitrary characteristic, are inspired by their work. Finally, I gratefully acknowledge the inspiration taken from the course “Quadratic Forms” taught by Karim Johannes Becher at the University of Antwerp in Belgium, which has to a large extent shaped my vision on modern quadratic form theory.

## 1. LECTURE 1

1.1. **Bilinear and quadratic forms.** Let always  $K$  be a field,  $n \in \mathbb{N}$ .

1.1.1. **Definition.** A *symmetric bilinear space over  $K$*  is a pair  $(V, B)$  where

- $V$  is a finite-dimensional vector space over  $K$ , and
- $B : V \times V \rightarrow K$  is a symmetric and bilinear map, i.e. for all  $x, x', y \in V$  and  $a \in K$  we have

$$\begin{aligned} B(x, y) &= B(y, x), \\ B(x + x', y) &= B(x, y) + B(x', y), \\ B(ax, y) &= aB(x, y). \end{aligned}$$

We call the map  $B$  a *symmetric bilinear form on  $V$* . We define the dimension of  $(V, B)$  to be the dimension of  $V$ , and denote this by  $\dim(V, B)$  or simply  $\dim B$ .

Let  $n = \dim(V, B)$ . Given a basis  $\mathcal{B} = (e_1, \dots, e_n)$  of  $V$ , we define  $\mathcal{M}_{\mathcal{B}}(B) = [B(e_j, e_i)]_{i,j=1}^n$ , which we call *the matrix of  $(V, B)$  with respect to  $\mathcal{B}$* .

1.1.2. **Proposition.** Let  $V = K^n$  and let  $\mathfrak{B} = (e_1, \dots, e_n)$  be the canonical basis. Let  $B$  be a symmetric bilinear form on  $V$ . For column vectors  $x = [x_1 \dots x_n]^T$  and  $y = [y_1, \dots, y_n]^T$  we have

$$B(x, y) = x^T \mathcal{M}_{\mathfrak{B}}(B)y.$$

*Proof.* This is clear from the bilinearity of  $B$ . □

1.1.3. **Definition.** A *quadratic space over  $K$*  is a pair  $(V, q)$  where

- $V$  is a finite-dimensional vector space over  $K$ , and
- $q : V \rightarrow K$  is a map satisfying the following:
  - (1)  $\forall a \in K, \forall x \in V : q(ax) = a^2q(x)$ ,

(2) the map

$$\mathfrak{b}_q : V \times V \rightarrow K : (x, y) \mapsto q(x + y) - q(x) - q(y)$$

is a symmetric bilinear form on  $V$ .

We call the map  $q$  a *quadratic form on  $V$* , and  $\mathfrak{b}_q$  its *polar form*. We define the dimension of  $(V, q)$  to be the dimension of  $V$ , and denote this by  $\dim(V, q)$  or simply  $\dim q$ .

**1.1.4. Definition.** Let  $(V, B)$  and  $(V', B')$  be symmetric bilinear spaces over  $K$ . An isomorphism of  $K$ -vector spaces  $I : V \rightarrow V'$  is called an *isometry between  $(V, B)$  and  $(V', B')$*  if, for all  $v, w \in V$ , one has  $B(v, w) = B'(I(v), I(w))$ . Similarly, given quadratic spaces  $(V, q)$  and  $(V', q')$  over  $K$ , an isomorphism of  $K$ -vector spaces  $I : V \rightarrow V'$  is called an *isometry between  $(V, q)$  and  $(V', q')$*  if, for all  $v \in V$ , one has  $q(v) = q'(I(v))$ .

We call two symmetric bilinear spaces  $(V, B)$  and  $(V, B')$  (respectively two quadratic spaces  $(V, q)$  and  $(V', q')$ ) *isometric*, which we denote by  $(V, B) \cong (V', B')$  (respectively  $(V, q) \cong (V', q')$ ) if there exists an isometry between them.

Traditionally, a quadratic form over  $K$  is often defined to be a homogeneous polynomial of degree 2 over  $K$ . Definition 1.1.3 can be seen as a coordinate-free version of this, as the following proposition indicates.

**1.1.5. Proposition.** *Let  $n \in \mathbb{N}$  and let  $f \in K[X_1, \dots, X_n]$  be a homogeneous polynomial of degree 2. The map*

$$q_f : K^n \rightarrow K : (x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$$

*is a quadratic form on  $K^n$ .*

*Conversely, given a quadratic space  $(V, q)$  of dimension  $n$ , there exists a homogeneous degree 2 polynomial  $f \in K[X_1, \dots, X_n]$  such that  $(V, q)$  is isometric to  $(K^n, q_f)$ .*

*Proof.* For the first part of the statement, one verifies that the defined map satisfies the conditions stated in Definition 1.1.3.

The second part of the statement is left as an exercise. □

**1.1.6. Proposition.** *Let  $f, g \in K[X_1, \dots, X_n]$  be homogeneous polynomials of degree 2. The quadratic spaces  $(K^n, q_f)$  and  $(K^n, q_g)$  are isometric if and only if there exists  $C \in \text{GL}_n(K)$  such that*

$$f([x_1 \dots x_n]^T) = g([x_1 \dots x_n] C)^T)$$

*for all  $x_1, \dots, x_n \in K$ .*

*Proof.* Exercise. □

1.1.7. *Example.* Suppose  $\text{char}(K) \neq 2$ . Let  $f(X_1, X_2) = X_1 \cdot X_2$  and  $g(X_1, X_2) = X_1^2 - X_2^2$ . We observe that

$$g\left(\frac{X_1 + X_2}{2}, \frac{X_1 - X_2}{2}\right) = f(X_1, X_2)$$

and thus, in view of Proposition 1.1.6, that  $(K^2, q_f) \cong (K^2, q_g)$ , with

$$C = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}.$$

We saw that, to a quadratic form  $q$ , one can associate a symmetric bilinear form  $\mathfrak{b}_q$  on the same space. It is also possible to obtain a quadratic form from a symmetric bilinear form: if  $(V, B)$  is a symmetric bilinear space, then

$$q_B : V \rightarrow K : v \mapsto B(v, v)$$

is easily seen to be a quadratic form. If  $\text{char}(K) \neq 2$ , then these two operations are each others inverses (up to scaling by  $\frac{1}{2}$ ), and hence the studies of quadratic and symmetric bilinear forms over  $K$  are essentially the same:

1.1.8. **Proposition.** *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space. Then  $q$  is equal to the quadratic form associated to the form  $\frac{1}{2}\mathfrak{b}_q$ . Conversely, if  $(V, B)$  is a symmetric bilinear space, then  $B$  is equal to  $\frac{1}{2}\mathfrak{b}_q$  where  $q = q_B$ .*

*Proof.* This is a straightforward computation. □

Over fields of characteristic 2, one can still associate to each quadratic form a symmetric bilinear form and to each symmetric bilinear form a quadratic form as before, but these operations are not invertible. In fact, one needs to make an entirely separate study of quadratic and symmetric bilinear forms! We refer the interested reader to [EKM08, Chapters I and II].

We now go on to study basic properties of quadratic forms.

1.1.9. **Definition.** Let  $(V, q)$  be a quadratic space over  $K$ .

- We call  $q$  *isotropic* if there exists  $v \in V \setminus \{0\}$  such that  $q(v) = 0$ , or *anisotropic* otherwise.
- Given  $a \in K^\times$ , we say that  $q$  *represents*  $a$  if  $\exists v \in V$  with  $a = q(v)$ . We write

$$D_K(q) = \{a \in K^\times \mid \exists v \in V : a = q(v)\}.$$

If  $D_K(q) = K^\times$ , we say that  $q$  is *universal*.

1.1.10. *Examples.*

- (1) Let  $f(X_1, X_2) = X_1 \cdot X_2$ . Then  $q_f$  is isotropic, since  $f(1, 0) = 0$ .  $q_f$  is also universal, since,  $f(1, a) = a$  for any  $a \in K^\times$ .
- (2) Let  $f(X_1, X_2) = X_1^2 + X_2^2$ .  $q_f$  is isotropic if and only if  $-1$  is a square in  $K$ .  $D_K(q_f)$  is the set of elements of  $K$  which are a sum of two squares.

- (3) Let  $f(X_1, X_2) = (X_1 + X_2)^2$ . Then  $q_f$  is isotropic since  $f(1, -1) = 0$ .  $D_K(q_f)$  consists of those elements of  $K$  which are squares.

The last example is somewhat peculiar: the quadratic form  $q_f$  with  $f(X_1, X_2) = (X_1 + X_2)^2$  is of dimension 2, but after a base change, one of the variables disappears. Indeed,

$$f(X_1 - X_2, X_2) = X_1^2.$$

We will often want to exclude from our study quadratic forms which have this property.

For a  $K$ -vector space  $V$ , we denote by  $V^*$  the dual space, i.e. the space of linear maps  $V \rightarrow K$ . Recall that  $\dim(V^*) = \dim(V)$ .

**1.1.11. Proposition.** *Let  $(V, B)$  be a symmetric bilinear space. Let  $\mathcal{B}$  be a basis for  $V$ . The following are equivalent.*

- (a)  $\forall v \in V \setminus \{0\}, \exists w \in V : B(v, w) \neq 0$ ,
- (b) *The map  $V \rightarrow V^* : v \mapsto (w \mapsto B(v, w))$  is a  $K$ -isomorphism.*
- (c) *The matrix  $M_{\mathcal{B}}(B)$  is invertible.*

*Proof.* Exercise. □

**1.1.12. Definition.** We call a symmetric bilinear space  $(V, B)$  *nonsingular* if the above equivalent conditions hold. We call a quadratic space  $(V, q)$  nonsingular if its polar form is nonsingular. Otherwise, we call the space *singular*. We use the same terminology for the symmetric bilinear and quadratic forms themselves.

We now show that, at least over fields of characteristic not 2, singular forms are precisely those for which, after a base change, one of the variables disappears.

**1.1.13. Proposition.** *Let  $(V, q)$  be a quadratic space over  $K$  and  $v \in V$ . Consider the statements*

- (a)  $\mathfrak{b}_q(v, w) = 0$  for all  $w \in V$ ,
- (b) for all  $w \in V$  we have  $q(w + v) = q(w)$ .

*We have that (b)  $\Rightarrow$  (a) in general. If  $\text{char}(K) \neq 2$ , then (a) and (b) are equivalent.*

*In particular, it follows that, if  $\text{char}(K) \neq 2$ , a quadratic space  $(V, q)$  is singular if and only if there exists  $v \in V \setminus \{0\}$  such that for all  $w \in V$  we have  $q(w + v) = q(w)$ .*

*Proof.* If (b) holds, then  $q(v) = q(v + 0) = q(0) = 0$ , whence for any  $w \in V$  we have  $\mathfrak{b}_q(v, w) = q(v + w) - q(v) - q(w) = 0$ .

Now assume that  $\text{char}(K) \neq 2$  and (a) holds. Then in particular  $0 = \mathfrak{b}_q(v, v) = 2q(v)$  and thus  $q(v) = 0$ . It follows that, for any  $w \in V$ , we have  $q(v + w) = q(v) + q(w) + \mathfrak{b}_q(v, w) = q(w)$ , so (b) holds. □

If  $\text{char}(K) \neq 2$ , a nonsingular quadratic form over  $K$  is also called *regular* or *nondegenerate*. Note that, if  $\text{char}(K) = 2$ , these terms have more specialised, distinct meanings.

1.1.14. *Remark.* So far, I have been somewhat careful in making the distinction between a symmetric bilinear/quadratic *space* and a symmetric bilinear/quadratic *form*. This makes notation and speaking somewhat heavy. I will in the future often simply refer to the forms themselves, taking the convention that a symmetric bilinear/quadratic space ‘knows’ its domain.

## 1.2. Orthogonality and diagonalisation.

1.2.1. **Definition.** Let  $(V, B)$  be a symmetric bilinear space. Let  $v, w \in V$ . We say that  $v$  and  $w$  are *orthogonal (with respect to  $B$ )* if  $B(v, w) = 0$ . We write  $v \perp w$ .

Let  $v \in V$  and  $M \subseteq V$ . We say that  $v$  is *orthogonal to  $M$  (with respect to  $B$ )* if  $B(v, w) = 0$  for all  $w \in M$ . We write  $v \perp M$ . Similarly, given  $M' \subseteq V$ , we say that  $M$  is *orthogonal to  $M'$  (with respect to  $B$ )* if  $B(v, w) = 0$  for all  $v \in M$  and  $w \in M'$ , and write  $M \perp M'$ .

We write

$$M^\perp = \{v \in V \mid \forall w \in M : B(v, w) = 0\}$$

and call it the *orthogonal space of  $M$*  - note that it is always a subspace of  $V$ . We write  $v^\perp$  instead of  $\{v\}^\perp$ .

If  $U \subseteq V$  is a subspace and  $V = U \oplus U^\perp$ , we call  $U^\perp$  an *orthogonal complement of  $U$  in  $V$* .

Observe that a symmetric bilinear space  $(V, B)$  is by definition nonsingular if and only if  $V^\perp = \{0\}$ .

1.2.2. **Proposition.** *Let  $(V, B)$  be nonsingular,  $U \subseteq V$  a subspace. Then*

$$\dim U + \dim U^\perp = \dim V \quad \text{and} \quad (U^\perp)^\perp = U.$$

*Proof.* Consider the  $K$ -linear maps

$$\begin{aligned} \varphi_1 : U^\perp &\rightarrow V^* : v \mapsto (w \mapsto B(v, w)) \\ \varphi_2 : V^* &\rightarrow U^* : f \mapsto f|_U. \end{aligned}$$

We observe that  $\varphi_1$  is injective by the nonsingularity of  $(V, B)$ , that  $\varphi_2$  is surjective, and that the image of  $\varphi_1$  is precisely the kernel of  $\varphi_2$  by definition of  $U^\perp$ . As such, we compute that

$$\begin{aligned} \dim V &= \dim V^* = \dim(\text{Ker } \varphi_2) + \dim(\text{Im } \varphi_2) \\ &= \dim(\text{Im } \varphi_1) + \dim U^* = \dim(U^\perp) + \dim(U) \end{aligned}$$

as desired.

For the second statement, observe that we trivially have  $U \subseteq (U^\perp)^\perp$ , but that, by the first claim,  $\dim(U) = \dim((U^\perp)^\perp)$ , whence  $U = (U^\perp)^\perp$  as desired.  $\square$

We now define an operation on the set of quadratic spaces over  $K$ .

**1.2.3. Proposition.** *Let  $(V_1, q_1)$  and  $(V_2, q_2)$  be quadratic spaces over  $K$ . Let  $V = V_1 \times V_2$  and consider the map*

$$q : V \rightarrow K : (x, y) \mapsto q_1(x) + q_2(y).$$

*Furthermore, consider the natural embeddings  $\iota_1 : V_1 \rightarrow V : x \mapsto (x, 0)$  and  $\iota_2 : V_2 \rightarrow V : x \mapsto (0, x)$ . We have that  $(V, q)$  is a quadratic space, and  $q$  is nonsingular if and only if both  $q_1$  and  $q_2$  are. Furthermore,  $i_1(V_1) \perp i_2(V_2)$  with respect to  $\mathfrak{b}_q$ .*

*Proof.* Easy verification. □

**1.2.4. Definition.** Let  $(V_1, q_1)$  and  $(V_2, q_2)$  be quadratic spaces over  $K$ . We call the space  $(V, q)$  defined in Proposition 1.2.3 the *orthogonal sum of  $(V_1, q_1)$  and  $(V_2, q_2)$*  and we denote the form  $q$  by  $q_1 \perp q_2$ .

**1.2.5. Proposition.** *Let  $(V_i, q_i)$  and  $(V'_i, q'_i)$  be quadratic spaces for  $i = 1, 2, 3$ . We have the following computation rules:*

- $\dim(q_1 \perp q_2) = \dim(q_1) + \dim(q_2)$ .
- $q_1 \perp q_2 \cong q_2 \perp q_1$ , and  $q_1 \perp (q_2 \perp q_3) \cong (q_1 \perp q_2) \perp q_3$ .
- If  $q_1 \cong q'_1$  and  $q_2 \cong q'_2$ , then  $q_1 \perp q_2 \cong q'_1 \perp q'_2$ .

*Proof.* Easy verifications. □

**1.2.6. Proposition.** *Let  $(V, q)$ ,  $(V_1, q_1)$  and  $(V_2, q_2)$  be quadratic spaces over  $K$ . Then  $q \cong q_1 \perp q_2$  if and only if there are  $K$ -subspaces  $W_1$  and  $W_2$  of  $V$  with  $W_1 \perp W_2$  with respect to  $\mathfrak{b}_q$ ,  $V = W_1 \oplus W_2$ , and such that  $(W_i, q|_{W_i}) \cong (V_i, q_i)$  for  $i = 1, 2$ .*

*Proof.* Suppose that  $\iota$  is an isomorphism  $q_1 \perp q_2 \rightarrow q$  and let  $W_1$  and  $W_2$  be the images under this isomorphism of  $V_1 \times \{0\}$  and  $\{0\} \times V_2$  respectively. One verifies easily that these are as desired.

Conversely, assume that  $W_1$  and  $W_2$  are subspaces of  $V$  with  $W_1 \perp W_2$ ,  $V = W_1 \oplus W_2$ , and such that  $(W_i, q|_{W_i}) \cong (V_i, q_i)$  for  $i = 1, 2$ . Without loss of generality, we may assume that  $V_i = W_i$  and  $q_i = q|_{W_i}$ . Let  $\iota$  be the unique  $K$ -linear map  $V \rightarrow V_1 \times V_2$  which maps a vector  $w \in W_1$  to  $(w, 0)$  and a vector  $w \in W_2$  to  $(0, w)$ . Clearly this is an isomorphism of  $K$ -vector spaces. Consider an arbitrary vector in  $V$ , which we may write as  $w_1 + w_2$  for  $w_1 \in W_1$  and  $w_2 \in W_2$ . Since  $W_1 \perp W_2$ , we have that  $\mathfrak{b}_q(w_1, w_2) = 0$ . We compute that

$$\begin{aligned} q(w_1 + w_2) &= q(w_1) + q(w_2) + \mathfrak{b}_q(w_1, w_2) = q(w_1) + q(w_2) \\ &= q_1(w_1) + q_2(w_2) = (q_1 \perp q_2)(w_1, w_2) = (q_1 \perp q_2)(\iota(w_1 + w_2)). \end{aligned}$$

Hence  $\iota$  is the desired isometry. □

We now discuss a special class of quadratic forms called diagonal forms. As it will turn out, in characteristic different from 2, every quadratic form is isometric to a diagonal form (see Corollary 1.2.10).

1.2.7. **Definition.** Let  $a_1, \dots, a_n \in K$ . We denote by  $\langle a_1, \dots, a_n \rangle_K$  the quadratic form

$$K^n \rightarrow K : (x_1, \dots, x_n) \mapsto \sum_{i=1}^n a_i x_i^2.$$

We call such a form a *diagonal form*. If the field  $K$  is clear from the context we might simply write  $\langle a_1, \dots, a_n \rangle$  instead of  $\langle a_1, \dots, a_n \rangle_K$ .

Note that  $\langle a_1, \dots, a_n \rangle_K \cong \langle a_1 \rangle_K \perp \dots \perp \langle a_n \rangle_K$ .

1.2.8. **Proposition.** Let  $n \in \mathbb{N}$  and  $a_1, \dots, a_n \in K$ , let  $q = \langle a_1, \dots, a_n \rangle$ . If  $\text{char}(K) \neq 2$ , then  $q$  is singular if and only if  $a_i = 0$  for some  $i \in \{1, \dots, n\}$ . If  $\text{char}(K) = 2$ , then  $q$  is singular as soon as  $n \geq 2$ .

*Proof.* Exercise. □

1.2.9. **Proposition.** Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space over  $K$ ,  $d \in K^\times$ . Then  $d \in D_K(q)$  if and only if  $q \cong \langle d \rangle \perp (V', q')$  for some quadratic space  $(V', q')$ .

*Proof.* Clearly  $d = d \cdot 1^2 + q'(0) \in D_K(\langle d \rangle \perp (V', q'))$  for any quadratic space  $(V', q')$ .

Conversely, assume that  $d \in D_K(q)$ . Let  $W$  be any subspace of  $V$  such that  $V = V^\perp \oplus W$ . Then  $(W, q|_W)$  is nonsingular, and, in view of Proposition 1.1.13, we have  $D_K(q|_W) = D_K(q)$ . We may thus restrict our quadratic form to  $W$ , and assume without loss of generality that  $q$  is nonsingular.

Now take  $v \in V$  with  $q(v) = d$ . Set  $U = v^\perp$ . We have  $v \notin v^\perp$  (since  $\mathfrak{b}_q(v, v) = 2d \neq 0$ ) and  $\dim(U) = \dim(V) - 1$  by Proposition 1.2.2, hence  $V = Kv \oplus U$ . Clearly  $q|_{Kv} \cong \langle d \rangle$ , so  $q \cong \langle d \rangle \perp (U, q|_U)$  in view of Proposition 1.2.6. □

1.2.10. **Corollary.** Assume  $\text{char}(K) \neq 2$ , let  $(V, q)$  be a quadratic space over  $K$  of dimension  $n$ . Then there exist  $a_1, \dots, a_n \in K$  such that  $q \cong \langle a_1, \dots, a_n \rangle$ .

*Proof.* Apply Proposition 1.2.9 inductively. □

### 1.3. Exercises.

- (1) Complete the proofs of Proposition 1.1.5, Proposition 1.1.6, Proposition 1.1.11 and Proposition 1.2.8.
- (2) Illustrate by an example that the implication (a)  $\Rightarrow$  (b) in Proposition 1.1.13 does not hold in general if  $\text{char}(K) = 2$ .
- (3) Consider the quadratic form on  $\mathbb{Q}^3$  given by the following polynomial:

$$f(X_1, X_2, X_3) = 3X_1^2 + 6X_1X_2 + 3X_2^2 - X_2X_3.$$

Explicitly construct a diagonal quadratic form  $q$  on  $\mathbb{Q}^3$  such that  $(\mathbb{Q}^3, q_f) \cong (\mathbb{Q}^3, q)$ .



2. LECTURE 2

Let always  $K$  be a field.

2.0.1. **Definition.** Let  $(V, q)$  be a quadratic space. If  $W$  is a subspace of  $V$ , the quadratic space  $(W, q|_W)$  is called a *subform* of  $(V, q)$ . By abuse of terminology, we will also call a quadratic space  $(U, q')$  which is isometric to  $(W, q|_W)$  for some subspace  $W$  of  $V$  a subform of  $(V, q)$ .

In this lecture, we will get closer to a classification of quadratic spaces over a given field, by decomposing quadratic spaces as orthogonal sums of subforms with specific properties.

2.1. **Isotropic, totally isotropic, and hyperbolic forms.** Recall from Definition 1.1.9 the definition of an isotropic quadratic form.

2.1.1. **Definition.** Let  $(V, q)$  be a quadratic space. We call  $(V, q)$  *totally isotropic* if  $q(v) = 0$  for all  $v \in V$ . If  $W$  is a subspace of  $V$ , we call  $W$  totally isotropic if  $(W, q|_W)$  is totally isotropic.

Observe that a non-zero totally isotropic space is always singular.

2.1.2. **Proposition.** *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space. Then the map*

$$\bar{q} : V/V^\perp \rightarrow K : \bar{v} \mapsto q(v)$$

*is a well-defined nonsingular quadratic form.*

*Proof.* The well-definedness follows from the fact that, for  $v \in V$  and  $w \in V^\perp$ , one has  $q(v + w) = q(v)$  by Proposition 1.1.13. It is then easy to verify that the map is a quadratic form.

For the nonsingularity, consider  $v \in V$  such that  $\bar{v} \neq 0$ , i.e.  $v \notin V^\perp$ . Then there exists  $w \in V$  with  $0 \neq \mathfrak{b}_q(v, w) = \mathfrak{b}_{\bar{q}}(\bar{v}, \bar{w})$ , whereby  $\bar{v} \notin (V/V^\perp)^\perp$ . Hence  $(V/V^\perp)^\perp = \{0\}$ , and thus  $(V/V^\perp, \bar{q})$  is nonsingular.  $\square$

The following observation was already used implicitly in the proof of Proposition 1.2.9.

2.1.3. **Proposition.** *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space. Let  $W$  be an orthogonal complement of  $V^\perp$ . We have that*

$$(V, q) \cong (V^\perp, q|_{V^\perp}) \perp (W, q|_W),$$

*that  $(V^\perp, q|_{V^\perp})$  is totally isotropic, and that  $(W, q|_W) \cong (V/V^\perp, \bar{q})$ .*

*Proof.* The first isometry is immediate from Proposition 1.2.6. The fact that  $(V^\perp, q|_{V^\perp})$  is totally isotropic follows from Proposition 1.1.13.

Finally, consider the map

$$\iota : W \rightarrow V/V^\perp : w \mapsto \bar{w}.$$

Since  $W \cap V^\perp = \{0\}$  we have that  $\iota$  is injective, hence by comparing dimensions,  $\iota$  is bijective. Furthermore, by definition we have for  $w \in W$  that  $q(w) = \bar{q}(\bar{w}) = \bar{q}(\iota(w))$ . Hence we have obtained the required isometry  $(W, q|_W) \cong (V/V^\perp, \bar{q})$ .  $\square$

We can thus, in characteristic away from 2, decompose any quadratic space into the orthogonal sum of a totally isotropic space and a nonsingular space, and this decomposition is unique up to isometry.

We now want to study nonsingular isotropic forms. Nonsingular one-dimensional quadratic forms are always anisotropic.

**2.1.4. Definition.** We call the quadratic form  $(K^2, q_f)$  with  $f(X_1, X_2) = X_1 \cdot X_2$  the *hyperbolic plane over  $K$*  and denote it by  $\mathbb{H}_K$ .

**2.1.5. Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space over  $K$ . Let  $v \in V \setminus \{0\}$  such that  $q(v) = 0$ . Then there is a subspace  $W \subseteq V$  with  $v \in W$  such that  $(W, q|_W)$  is isometric to  $\mathbb{H}_K$ .*

*Proof.* Since  $(V, q)$  is nonsingular, there exists  $w \in V$  such that  $a = \mathfrak{b}_q(v, w) \neq 0$ . We may replace  $w$  by  $a^{-1}w$  and assume without loss of generality that  $a = 1$ . Observe that  $w \notin Kv$ , so that  $W = Kv \oplus Kw$  is a 2-dimensional subspace of  $V$ . Consider the map

$$\iota : K^2 \rightarrow W : (x, y) \mapsto xv + y(w - q(w)v).$$

Clearly this is a  $K$ -isomorphism of vector spaces. We compute that, for  $x, y \in K$ , we have

$$\begin{aligned} q(\iota(x, y)) &= q(xv + y(w - q(w)v)) \\ &= (x - yq(w))^2 q(v) + y^2 q(w) + \mathfrak{b}_q((x - yq(w))v, yw) \\ &= 0 + y^2 q(w) + (x - yq(w))y \mathfrak{b}_q(v, w) = xy. \end{aligned}$$

Hence  $(W, q|_W) \cong \mathbb{H}_K$ .  $\square$

In particular, it follows from Proposition 2.1.5 that the hyperbolic plane is, up to isometry, the only two-dimensional nonsingular isotropic quadratic form over  $K$ . We also obtain the following

**2.1.6. Corollary.** *Every nonsingular isotropic quadratic space is universal.*

*Proof.* We know from Examples 1.1.10 that  $\mathbb{H}_K$  is universal. But by Proposition 2.1.5 every nonsingular isotropic quadratic space contains  $\mathbb{H}_K$  as a subspace, hence is also universal.  $\square$

**2.1.7. Corollary.** *Let  $(V, q)$  be a nonsingular quadratic space and  $d \in K^\times$ . We have that  $d \in D_K(q)$  if and only if  $q \perp \langle -d \rangle_K$  is isotropic.*

*Proof.* Exercise.  $\square$

**2.1.8. Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space,  $W$  a nonsingular subspace of  $V$ . Then  $V = W \oplus W^\perp$ ,  $(V, q) \cong (W, q|_W) \perp (W^\perp, q|_{W^\perp})$ , and also  $(W^\perp, q|_{W^\perp})$  is nonsingular.*

*Proof.* Since  $(V, q)$  is nonsingular, we have  $\dim W + \dim W^\perp = \dim V$  by Proposition 1.2.2. Since  $(W, q|_W)$  is nonsingular, we further have  $W \cap W^\perp = \{0\}$ . Hence, we obtain  $V = W \oplus W^\perp$ , and the natural induced  $K$ -isomorphism  $V \rightarrow W \times W^\perp$  gives the required isometry  $(V, q) \cong (W, q|_W) \perp (W^\perp, q|_{W^\perp})$ ; see Proposition 1.2.6.

Finally, since  $(W^\perp)^\perp = W$  by Proposition 1.2.2, we obtain  $(W^\perp)^\perp \cap W^\perp = W \cap W^\perp = \{0\}$ , whereby  $(W^\perp, q|_{W^\perp})$  is nonsingular.  $\square$

In the sequel, we will use the following notation: for a quadratic space  $(V, q)$  and  $n \in \mathbb{N}$ , we write

$$n \times (V, q) = (V^n, \underbrace{q \perp \dots \perp q}_{n \text{ times}}).$$

We will denote the described quadratic form on  $V^n$  simply by  $n \times q$ . By convention,  $0 \times (V, q)$  denotes the unique zero-dimensional quadratic space over  $K$ .

**2.1.9. Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space,  $n \in \mathbb{N}$ . The following are equivalent.*

- (1)  $V$  contains a totally isotropic subspace of dimension  $n$ ,
- (2)  $V$  contains a subform isometric to  $n \times \mathbb{H}_K$ .

*Proof.* For  $n = 0$  there is nothing to show, assume from now on that  $n \geq 1$ .

Assume (2). Then  $V$  has subspaces  $W_1, \dots, W_n$  such that  $W_i \perp W_j$  and  $W_i \cap W_j = \{0\}$  for any  $i \neq j$  and such that  $(W_i, q|_{W_i}) \cong \mathbb{H}_K$ . Let  $w_i \in W_i \setminus \{0\}$  be such that  $q(w_i) = 0$ . Then  $Kw_1 \oplus \dots \oplus Kw_n$  is an  $n$ -dimensional totally isotropic subspace of  $V$ .

Conversely, assume (1). We argue via induction on  $n$  - recall that the case  $n = 0$  is covered, so we assume  $n \geq 1$ . Let  $W$  be a totally isotropic subspace of  $V$  of dimension  $n$  and let  $v \in W \setminus \{0\}$ . By Proposition 2.1.5 there exists  $w \in V$  such that, for  $W' = Kv \oplus Kw$ , we have  $(W', q|_{W'}) \cong \mathbb{H}_K$ . By Proposition 2.1.8 this implies that  $(V, q) \cong \mathbb{H}_K \perp (U, q|_U)$  for  $U = (W')^\perp$ , and furthermore  $(U, q|_U)$  is nonsingular. Further, since  $W \subseteq v^\perp$ , we have

$$U \cap W = (W')^\perp \cap W = v^\perp \cap w^\perp \cap W = w^\perp \cap W$$

whereby  $\dim(W \cap U) \geq n - 1$ . Hence  $(U, q|_U)$  contains a totally isotropic subspace  $W \cap U$  of dimension  $n - 1$ . The statement now follows by the induction hypothesis.  $\square$

**2.1.10. Corollary.** *Let  $(V, q)$  be a nonsingular quadratic space of dimension  $2n$ , where  $n \in \mathbb{N}$ . The following are equivalent.*

- (1)  $V$  contains a totally isotropic subspace of dimension  $n$ ,
- (2)  $(V, q) \cong n \times \mathbb{H}_K$ .

**2.1.11. Definition.** We say that a nonsingular quadratic space of dimension  $2n$  (for some  $n \in \mathbb{N}$ ) is *hyperbolic* if it contains a totally isotropic subspace of dimension  $n$ .

Given a quadratic space  $(V, q)$ , we define the *Witt index* of  $(V, q)$  to be the maximal possible dimension of a totally isotropic subspace of  $(V/V^\perp, \bar{q})$ . We denote it by  $i_W(V, q)$ , or simply  $i_W(q)$ .

**2.1.12. Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space. Then  $(V, q) \perp (V, -q)$  is hyperbolic.*

*Proof.* Let  $n = \dim V$ . Then  $\dim(V \times V) = 2n$ . Let  $W = \{(v, v) \in V \times V \mid v \in V\}$ . Then  $W$  is a subspace of  $V \times V$  of dimension  $n$ , and it is a totally isotropic subspace of  $(V, q) \perp (V, -q)$ , since for any  $v \in V$  we have  $(q \perp -q)(v, v) = q(v) - q(v) = 0$ .

Since  $(V, q) \perp (V, -q)$  is nonsingular (by Proposition 1.2.3) and has a totally isotropic subspace of dimension  $n$ , it is hyperbolic.  $\square$

**2.2. Witt's Theorems.** We are now in a position to prove the two most important structure theorems on quadratic forms, named after Ernst Witt. We will prove them, as Witt did in the 1930's, under the assumption that  $\text{char}(K) \neq 2$ . Versions in characteristic 2 exist and can be proven with extra assumptions and a lot more work, see [EKM08, Section 8].

**2.2.1. Lemma.** *Assume that  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space, and let  $v, w \in V$  be such that  $q(v) = q(w) \neq 0$ . There exists an isometry  $\tau : (V, q) \rightarrow (V, q)$  such that  $\tau(x) = y$ .*

*Proof.* One computes that  $q(v+w) + q(v-w) = 4q(v) \neq 0$ , so at least one of  $q(v+w)$  and  $q(v-w)$  is non-zero. Replacing  $w$  by  $-w$  if necessary, we may assume that  $q(v-w) \neq 0$ . Now consider the map

$$\tau : V \rightarrow V : u \mapsto u - \frac{\mathfrak{b}_q(u, v-w)}{q(v-w)}(v-w).$$

One verifies that  $\tau$  gives an isometry  $(V, q) \rightarrow (V, q)$ , and that  $\tau(v) = w$ , as desired; see Exercise (2).  $\square$

**2.2.2. Theorem (Witt Cancellation Theorem).** *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$ ,  $(V_1, q_1)$  and  $(V_2, q_2)$  be quadratic spaces. If  $(V, q) \perp (V_1, q_1) \cong (V, q) \perp (V_2, q_2)$ , then  $(V_1, q_1) \cong (V_2, q_2)$ .*

*Proof.* We first reduce to the case where all involved quadratic spaces are nonsingular. To this end, use Proposition 2.1.3 to write  $(V, q) \cong (V^\perp, q|_{V^\perp}) \perp (W, q|_W)$ ,  $(V_1, q_1) \cong (V_1^\perp, q_1|_{V_1^\perp}) \perp (W_1, q|_{W_1})$  and  $(V_2, q_2) \cong (V_2^\perp, q_2|_{V_2^\perp}) \perp (W_2, q|_{W_2})$  where  $q|_W$ ,  $q_1|_{W_1}$  and  $q_2|_{W_2}$  are nonsingular. The hypothesis can be rewritten as

$$\begin{aligned} & ((V \perp V_1)^\perp, (q \perp q_1)|_{(V \perp V_1)^\perp}) \perp (W \perp W_1, (q \perp q_1)|_{W \perp W_1}) \\ & \cong ((V \perp V_2)^\perp, (q \perp q_2)|_{(V \perp V_2)^\perp}) \perp (W \perp W_2, (q \perp q_2)|_{W \perp W_2}), \end{aligned}$$

using that  $V^\perp \perp V_1^\perp = (V \perp V_1)^\perp$  and similarly  $V^\perp \perp V_2^\perp = (V \perp V_2)^\perp$ . We further have by Proposition 1.2.3 that  $(W \perp W_1, (q \perp q_1)|_{W \perp W_1})$  and  $(W \perp W_2, (q \perp q_2)|_{W \perp W_2})$  are nonsingular. In view of Proposition 2.1.3 we have

$$\begin{aligned} (W \perp W_1, (q \perp q_1)|_{W \perp W_1}) &\cong ((V \perp V_1)/(V \perp V_1)^\perp, \overline{q \perp q_1}) \\ &\cong ((V \perp V_2)/(V \perp V_2)^\perp, \overline{q \perp q_2}) \cong (W \perp W_2, (q \perp q_2)|_{W \perp W_2}), \end{aligned}$$

We conclude that we may assume for the remainder of the proof that  $(V, q)$ ,  $(V_1, q_1)$  and  $(V_2, q_2)$  are nonsingular.

By Corollary 1.2.10 we may assume that  $(V, q) \cong \langle a_1, \dots, a_n \rangle$  for some  $a_1, \dots, a_n \in K^\times$ . By inducting on  $n$ , we reduce to the situation  $n = 1$ . Let  $\iota : \langle a \rangle_K \perp (V_1, q_1) \rightarrow \langle a \rangle_K \perp (V_2, q_2)$  be an isometry. Let  $v = \iota(1, 0)$ . We have  $(\langle a \rangle_K \perp q_2)(v) = (\langle a \rangle_K \perp q_1)(1, 0) = a \cdot 1^2 = a = (\langle a \rangle_K \perp q_2)(1, 0)$ .

By Lemma 2.2.1 there exists an isometry  $\tau : \langle a \rangle_K \perp (V_2, q_2) \rightarrow \langle a \rangle_K \perp (V_2, q_2)$  with  $\tau(v) = (1, 0)$ . Thus,  $\tau \circ \iota$  gives an isometry  $\langle a \rangle_K \perp (V_1, q_1) \rightarrow \langle a \rangle_K \perp (V_2, q_2)$  mapping  $(1, 0)$  to  $(1, 0)$ . Furthermore, since  $(K \times \{0\}) \perp (\{0\} \times V_1)$  (in  $(K \times V_1, \langle a \rangle_K \perp q_1)$ ) and isometries preserve orthogonality, we obtain  $(K \times \{0\}) \perp (\tau \circ \iota)(\{0\} \times V_1)$  (in  $(K \times V_2, \langle a \rangle_K \perp q_2)$ ). So, we must have  $(\tau \circ \iota)(\{0\} \times V_1) = \{0\} \times V_2$ , whereby  $\tau \circ \iota$  induces an isometry  $(V_1, q_1) \rightarrow (V_2, q_2)$ , as desired.  $\square$

**2.2.3. Theorem** (Witt Decomposition Theorem). *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a quadratic space. There exist quadratic spaces  $(V_t, q_t)$ ,  $(V_h, q_h)$  and  $(V_a, q_a)$  such that*

$$(V, q) \cong (V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a)$$

where

- $(V_t, q_t)$  is totally isotropic,
- $(V_h, q_h)$  is hyperbolic (or zero),
- $(V_a, q_a)$  is anisotropic.

Furthermore, each of these spaces is determined up to isometry by  $(V, q)$ . In fact,  $(V_t, q_t)$  is the unique totally isotropic space of dimension  $\dim V^\perp$ , and  $(V_h, q_h)$  is the unique hyperbolic space of dimension  $2i_W(q)$ .

*Proof.* We first prove the existence of the required spaces. By Proposition 2.1.3 we can write  $(V, q) \cong (V_t, q_t) \perp (V', q')$  where  $(V_t, q_t)$  is totally isotropic of dimension  $\dim V^\perp$  and  $(V', q')$  is nonsingular. Let  $m = i_W(V, q)$ . By Proposition 2.1.9 and Proposition 2.1.8 we can write  $(V', q') \cong (V_h, q_h) \perp (V_a, q_a)$  where  $(V_h, q_h)$  is hyperbolic of dimension  $2m$ .  $(V_a, q_a)$  must be nonsingular, and in fact it is anisotropic, since otherwise one could find a totally isotropic subspace of  $(V', q')$  of dimension  $m + 1$ , contradicting the choice of  $m$ . This concludes the existence part of the proof.

For the uniqueness, assume that

$$(V, q) \cong (V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a) \cong (V'_t, q'_t) \perp (V'_h, q'_h) \perp (V'_a, q'_a)$$

where  $(V'_t, q'_t)$  is totally singular,  $(V'_h, q'_h)$  is hyperbolic, and  $(V'_a, q'_a)$  is anisotropic. Since  $(V'_t, q'_t)$  is totally isotropic and  $(V'_h, q'_h) \perp (V'_a, q'_a)$  is nonsingular, we must have

$$\dim V'_t = \dim V^\perp = \dim V_t.$$

Since  $(V_t, q_t)$  and  $(V'_t, q'_t)$  are totally isotropic of the same dimension, they must be isometric. By Theorem 2.2.2 we obtain that  $(V_h, q_a) \perp (V_a, q_a) \cong (V'_h, q'_h) \perp (V'_a, q'_a)$ . Similarly, since  $(V'_h, q'_h)$  is hyperbolic and  $(V'_a, q'_a)$  is anisotropic, we must have  $\dim V'_h = 2m = \dim V_h$ , whereby  $(V_h, q_h)$  and  $(V'_h, q'_h)$  are hyperbolic forms of the same dimension and hence isometric. Finally, applying Theorem 2.2.2 again, we obtain  $(V_a, q_a) \cong (V'_a, q'_a)$ .  $\square$

### 2.3. Exercises.

- (1) Complete the proof of Corollary 2.1.7.
- (2) Let  $(V, q)$  be a quadratic space, and consider for  $v \in V$  with  $q(v) \neq 0$  the map

$$\tau_v : V \rightarrow V : w \mapsto w - \frac{\mathfrak{b}_q(w, v)}{q(v)}v.$$

Show the following for any  $v \in V$  with  $q(v) \neq 0$ :

- (a)  $\tau_v$  is an isometry  $(V, q) \rightarrow (V, q)$ ,
  - (b)  $\tau_v(v) = -v$ , and for  $w \in v^\perp$  we have  $\tau_v(w) = w$ ,
  - (c) If  $w \in V$  is such that  $q(v) = q(w)$  and  $q(v-w) \neq 0$ , then  $\tau_{v-w}(v) = w$ .
- (3) Show that the following are equivalent for a field  $K$  with  $\text{char}(K) \neq 2$ :
    - (a) Any two nonsingular quadratic spaces over  $K$  of the same dimension are isometric.
    - (b) Every element of  $K$  is a square.
  - (4) Let  $(V, q)$  be a nonsingular isotropic space. Show that  $V$  has a basis consisting of isotropic vectors.
  - (5) Let  $(V, q)$  be a nonsingular quadratic space, set  $n = \dim V$  and  $m = i_W(q)$ . Show that every subform of  $(V, q)$  of dimension greater than  $n - m$  is isotropic.
  - (6) Assume  $\text{char}(K) \neq 2$  and let  $(V_1, q_1)$  and  $(V_2, q_2)$  be nonsingular quadratic spaces over  $K$ . Show that  $(V_2, q_2)$  is a subform of  $(V_1, q_1)$  if and only if  $i_W((V_1, q_1) \perp (V_2, -q_2)) \geq \dim V_2$ .
  - (7) Let  $K = \mathbb{F}_2$ , the field with two elements. Consider the quadratic form

$$q : K^2 \rightarrow K : (x, y) \mapsto x^2 + xy + y^2.$$

Show that  $q \perp \langle 1 \rangle_K \cong \mathbb{H}_K \perp \langle 1 \rangle_K$ , but  $q \not\cong \mathbb{H}_K$ . Conclude that Theorem 2.2.2 does not hold as stated without the assumption  $\text{char}(K) \neq 2$ .

## 3. LECTURE 3

**3.1. Tensor products of symmetric bilinear spaces.** In this section, we will define the tensor product (sometimes called Kronecker product) of two symmetric bilinear spaces. First, we define the tensor product of two  $K$ -vector spaces.

Let  $V$  and  $W$  be  $K$ -vector spaces. Denote by  $K^{(V \times W)}$  the free  $K$ -vector space over the set  $V \times W$ . That is, for each  $(v, w) \in V \times W$  we fix an element  $e_{(v,w)} \in K^{(V \times W)}$ , and then  $\{e_{(v,w)} \mid (v, w) \in V \times W\}$  is a basis of  $K^{(V \times W)}$ . Let  $A$  be the subspace of  $K^{(V \times W)}$  generated by elements of the form

$$e_{(v+av',w)} - e_{(v,w)} - ae_{(v',w)} \quad \text{or} \quad e_{(v,w+aw')} - e_{(v,w)} - ae_{(v,w')}$$

for  $v, v' \in V$ ,  $w, w' \in W$  and  $a \in K$ .

**3.1.1. Definition.** With the notations from above, we call the quotient space  $K^{(V \times W)}/A$  the *tensor product of  $V$  and  $W$* , which we denote by  $V \otimes W$  - or  $V \otimes_K W$  if we want to stress the underlying field. For  $v \in V$  and  $w \in W$  we denote by  $v \otimes w$  the class of  $e_{(v,w)}$  in this quotient space. We call an element of  $V \otimes_K W$  of the form  $v \otimes w$  for  $v \in V$  and  $w \in W$  an *elementary tensor*.

**3.1.2. Remark.** Be careful! Not every element of  $V \otimes W$  is of the form  $v \otimes w$  for  $v \in V$  and  $w \in W$ , i.e. not every element of  $V \otimes W$  is an elementary tensor. However, every element of  $V \otimes W$  is a sum of elementary tensors - although this decomposition is not unique.

The tensor product  $V \otimes W$  is best understood through the following fundamental property.

**3.1.3. Proposition** (Universal property of tensor products). *Let  $V$  and  $W$  be  $K$ -vector spaces. The map  $V \times W \rightarrow V \otimes W : (v, w) \mapsto v \otimes w$  is a bilinear map, and its image generates  $V \otimes W$ .*

*For any  $K$ -vector space  $U$  and any bilinear map  $B : V \times W \rightarrow U$ , there exists a unique linear map  $\overline{B} : V \otimes W \rightarrow U$  such that  $B(v, w) = \overline{B}(v \otimes w)$  for all  $v \in V$ ,  $w \in W$ .*

*Proof.* The bilinearity of the map  $V \times W \rightarrow V \otimes W : (v, w) \mapsto v \otimes w$  follows from the construction of  $V \otimes W$ : we have for any  $v_1, v_2 \in V$ ,  $w_1, w_2 \in W$  and  $a, b \in K$  that

$$(v_1 + av_2) \otimes (w_1 + bw_2) = (v_1 \otimes w_1) + a(v_2 \otimes w_1) + b(v_1 \otimes w_2) + ab(v_2 \otimes w_2).$$

The image of the map consists of elementary tensors, which by construction generate  $V \otimes W$ .

Now consider any bilinear map  $B : V \times W \rightarrow U$ . Since  $\{e_{(v,w)} \mid (v, w) \in V \times W\}$  form a basis of  $K^{(V \times W)}$ , there is a unique  $K$ -linear map  $\hat{B} : K^{(V \times W)} \rightarrow U$  mapping  $e_{(v,w)}$  to  $B(v, w)$  for  $(v, w) \in V \times W$ . By the bilinearity of  $B$ , we compute that for  $v_1, v_2 \in V$  and  $w_1, w_2 \in W$  we have

$$\begin{aligned} \hat{B}(e_{(v_1+av_2,w_1+bw_2)}) &= B(v_1 + av_2, w_1 + bw_2) \\ &= B(v_1, w_1) + aB(v_2, w_1) + bB(v_1, w_2) + abB(v_2, w_2) \\ &= \hat{B}(e_{(v_1,w_1)} + ae_{(v_2,w_1)} + be_{(v_1,w_2)} + abe_{(v_2,w_2)}). \end{aligned}$$

As such,  $\text{Ker}(\hat{B})$  contains all elements given as generators for the subspace  $A$  of  $K^{(V \times W)}$ , whereby  $A \subseteq \text{Ker}(\hat{B})$ . Recalling that  $V \otimes W = K^{(V \times W)}/A$ , we conclude that there exists a unique linear map  $\overline{B} : V \otimes W \rightarrow U$  such that  $\overline{B}(v \otimes w) = \hat{B}(e_{(v,w)}) = B(v, w)$  for all  $(v, w) \in V \times W$ .  $\square$

**3.1.4. Proposition.** *Let  $U, V$  and  $W$  be  $K$ -vector spaces. The tensor product satisfies the following properties.*

- (1) *There is a unique  $K$ -isomorphism  $V \otimes W \rightarrow W \otimes V$  such that  $v \otimes w \mapsto w \otimes v$  for  $v \in V$  and  $w \in W$ .*
- (2) *There is a unique  $K$ -isomorphism  $(U \otimes V) \otimes W \rightarrow U \otimes (V \otimes W)$  such that  $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$  for  $u \in U, v \in V$  and  $w \in W$ .*
- (3) *There is a unique  $K$ -isomorphism  $(U \times V) \otimes W \rightarrow (U \otimes W) \times (V \otimes W)$  such that  $((u \otimes v), w) \mapsto ((u \otimes w), (v \otimes w))$  for  $u \in U, v \in V$  and  $w \in W$ .*
- (4) *Let  $\mathfrak{B}_V$  and  $\mathfrak{B}_W$  be bases for  $V$  and  $W$  respectively. Then*

$$\{v \otimes w \mid v \in \mathfrak{B}_V, w \in \mathfrak{B}_W\}$$

*is a basis for  $V \otimes W$ . In particular,  $\dim(V \otimes W) = \dim(V) \dim(W)$ .*

*Proof.* Each of these can be proven by making use of Proposition 3.1.3.  $\square$

We can now define the tensor product of symmetric bilinear spaces.

**3.1.5. Proposition.** *Let  $(V_1, B_1)$  and  $(V_2, B_2)$  be symmetric bilinear spaces. There exists a unique  $K$ -bilinear form  $B$  on  $V_1 \otimes V_2$  such that*

$$B(v_1 \otimes v_2, w_1 \otimes w_2) = B_1(v_1, w_1) \cdot B_2(v_2, w_2)$$

*for all  $v_1, w_1 \in V_1$  and  $v_2, w_2 \in V_2$ .*

*Proof.* The uniqueness is clear, since  $V \otimes W$  is generated by elementary tensors; furthermore, since such a bilinear map would by definition be symmetric on elementary tensors, it is automatically symmetric. It thus suffices to show the existence of such a bilinear map  $B$ .

Consider first for  $(v_1, v_2) \in V_1 \times V_2$  the map

$$V_1 \times V_2 \rightarrow K : (w_1, w_2) \mapsto B_1(v_1, w_1) \cdot B_2(v_2, w_2).$$

This map is bilinear, hence by Proposition 3.1.3 induces a linear map  $B_{(v_1, v_2)} : V_1 \otimes V_2 \rightarrow K$  such that  $B_{(v_1, v_2)}(w_1 \otimes w_2) = B_1(v_1, w_1) \cdot B_2(v_2, w_2)$  for  $w_1 \in V_1$  and  $w_2 \in V_2$ . The map

$$B^* : V_1 \times V_2 \rightarrow (V_1 \otimes V_2)^* : (v_1, v_2) \mapsto B_{(v_1, v_2)}$$

is also bilinear, hence, again by Proposition 3.1.3, it induces a linear map  $\overline{B}^* : V_1 \otimes V_2 \rightarrow (V_1 \otimes V_2)^*$  such that  $\overline{B}^*(v_1 \otimes v_2) = B_{(v_1, v_2)}$  for  $(v_1, v_2) \in V_1 \times V_2$ .

Finally, consider the bilinear map

$$B : (V_1 \otimes V_2) \times (V_1 \otimes V_2) : (\alpha, \beta) \mapsto \overline{B}^*(\alpha)(\beta).$$



We compute that, for  $v_1, w_1 \in V_1$  and  $v_2, w_2 \in V_2$ , we have

$$\begin{aligned} B(v_1 \otimes v_2, w_1 \otimes w_2) &= \overline{B^*}(v_1 \otimes v_2)(w_1 \otimes w_2) \\ &= B_{(v_1, v_2)}(w_1 \otimes w_2) = B_1(v_1, w_1) \cdot B_2(v_2, w_2). \end{aligned}$$

Hence,  $B$  is as desired.  $\square$

**3.1.6. Definition.** Given symmetric bilinear spaces  $(V_1, B_1)$  and  $(V_2, B_2)$ , we call the symmetric bilinear space constructed in Proposition 3.1.5 the *tensor product* of  $(V_1, B_1)$  and  $(V_2, B_2)$ . We denote it by  $(V_1 \otimes V_2, B_1 \otimes B_2)$ .

Over fields of characteristic different from 2, we will also consider the tensor product of quadratic spaces; this is by definition the quadratic space corresponding to the tensor product of the underlying symmetric bilinear spaces, see Proposition 1.1.8. That is, for quadratic spaces  $(V_1, q_1)$  and  $(V_2, q_2)$ , we define

$$q_1 \otimes q_2 : V_1 \otimes V_2 \rightarrow K : \alpha \mapsto \frac{(B_{q_1} \otimes B_{q_2})(\alpha)}{4}.$$

In the following proposition stating some computation rules, in the interest of brevity, we represent a quadratic space just by its quadratic form.

**3.1.7. Proposition.** *Assume  $\text{char}(K) \neq 2$ . For quadratic forms  $q_1, q_2, q_3$  over  $K$  we have*

$$\begin{aligned} q_1 \otimes q_2 &\cong q_2 \otimes q_1 \\ (q_1 \otimes q_2) \otimes q_3 &\cong q_1 \otimes (q_2 \otimes q_3) \\ (q_1 \perp q_2) \otimes q_3 &\cong (q_1 \otimes q_3) \perp (q_2 \otimes q_3) \end{aligned}$$

*Proof.* Each of these follows by checking that the isomorphism of vector spaces established in Proposition 3.1.4 induces isometries of quadratic (/symmetric bilinear) spaces.  $\square$

**3.1.8. Corollary.** *Let  $m, n \in \mathbb{N}$  and let  $a_1, \dots, a_m, b_1, \dots, b_n \in K$ . We have*

$$\langle a_1, \dots, a_m \rangle_K \otimes \langle b_1, \dots, b_n \rangle_K \cong \langle a_1 b_1, \dots, a_i b_j, \dots, a_m b_n \rangle_K$$

*Proof.* This follows by Proposition 3.1.7 and the easy observation that  $\langle a \rangle_K \otimes \langle b \rangle_K \cong \langle ab \rangle_K$  for  $a, b \in K$ .  $\square$

**3.1.9. Corollary.** *Assume  $\text{char}(K) \neq 2$ . Let  $(V_1, q_1), (V_2, q_2)$  be nonsingular quadratic spaces. Then  $(V_1 \otimes V_2, q_1 \otimes q_2)$  is nonsingular.*

*Proof.* By Corollary 1.2.10 and Proposition 1.2.8 both  $(V_1, q_1)$  and  $(V_2, q_2)$  are isometric to diagonal forms where all entries are non-zero. By Corollary 3.1.8 the same holds for  $(V_1 \otimes V_2, q_1 \otimes q_2)$ , whence this form is also nonsingular.  $\square$

**3.1.10. Corollary.** *Assume  $\text{char}(K) \neq 2$ . Let  $(V, q)$  be a nonsingular quadratic space. Then  $(V, q) \otimes \mathbb{H}_K$  is hyperbolic.*

*Proof.* We have  $\mathbb{H}_K \cong \langle 1, -1 \rangle_K$  (see Example 1.1.7). Hence, by Proposition 3.1.7,

$$(V, q) \otimes \mathbb{H}_K \cong (V, q) \otimes \langle 1, -1 \rangle_K \cong (V, q) \perp (V, -q)$$

which is hyperbolic by Proposition 2.1.12.  $\square$

### 3.2. Exercises.

- (1) Prove Proposition 3.1.4 and Proposition 3.1.7.

## 4. LECTURE 4

**4.1. Witt equivalence and the Witt ring.** Throughout this subsection, all quadratic spaces are considered over a fixed field  $K$ , and we assume  $\text{char}(K) \neq 2$ .

**4.1.1. Definition.** Let  $(V^{(1)}, q^{(1)})$  and  $(V^{(2)}, q^{(2)})$  be quadratic spaces. In view of Theorem 2.2.3 we may write

$$\begin{aligned} (V^{(1)}, q^{(1)}) &\cong (V_t^{(1)}, q_t^{(1)}) \perp (V_h^{(1)}, q_h^{(1)}) \perp (V_a^{(1)}, q_a^{(1)}) \\ (V^{(2)}, q^{(2)}) &\cong (V_t^{(2)}, q_t^{(2)}) \perp (V_h^{(2)}, q_h^{(2)}) \perp (V_a^{(2)}, q_a^{(2)}) \end{aligned}$$

where

- $(V_t^{(1)}, q_t^{(1)})$  and  $(V_t^{(2)}, q_t^{(2)})$  are totally isotropic,
- $(V_h^{(1)}, q_h^{(1)})$  and  $(V_h^{(2)}, q_h^{(2)})$  are hyperbolic (or zero),
- $(V_a^{(1)}, q_a^{(1)})$  and  $(V_a^{(2)}, q_a^{(2)})$  are anisotropic.

We say that  $(V^{(1)}, q^{(1)})$  and  $(V^{(2)}, q^{(2)})$  are *Witt equivalent* if  $\dim V_t^{(1)} = \dim V_t^{(2)}$  and  $(V_a^{(1)}, q_a^{(1)}) \cong (V_a^{(2)}, q_a^{(2)})$ . We denote this by  $(V^{(1)}, q^{(1)}) \equiv (V^{(2)}, q^{(2)})$ .

Theorem 2.2.3 yields that this is indeed a well-defined equivalence relation on the class of quadratic spaces over  $K$ . One has the following easy observations.

**4.1.2. Proposition.** *Let  $(V_1, q_1)$  and  $(V_2, q_2)$  be quadratic spaces.*

- (1)  $(V_1, q_1) \cong (V_2, q_2)$  if and only if  $(V_1, q_1) \equiv (V_2, q_2)$  and  $\dim V_1 = \dim V_2$ .
- (2) *In every Witt equivalence class, there is up to isometry a unique anisotropic quadratic space. In particular, if  $(V_1, q_1) \equiv (V_2, q_2)$  and both are anisotropic, then  $(V_1, q_1) \cong (V_2, q_2)$ .*

For a quadratic space  $(V, q)$ , let us denote by  $[(V, q)]$  its Witt equivalence class. Let us denote by  $W(K)$  the set of equivalence classes of nonsingular quadratic spaces up to Witt equivalence. We will see now that this set can naturally be given a ring structure.

**4.1.3. Theorem.** *The rules*

$$\begin{aligned} \perp : W(K) \times W(K) &\rightarrow W(K) : ([V_1, q_1], [V_2, q_2]) \rightarrow [(V_1 \times V_2, q_1 \perp q_2)] \text{ and} \\ \otimes : W(K) \times W(K) &\rightarrow W(K) : ([V_1, q_1], [V_2, q_2]) \rightarrow [(V_1 \otimes V_2, q_1 \otimes q_2)] \end{aligned}$$

*are well-defined binary operations on  $W(K)$ , making  $W(K)$  into a commutative ring with addition  $\perp$  and multiplication  $\otimes$ . The class of the zero-dimensional*

form  $[\langle \rangle_K]$  is a neutral element for  $\perp$ , and  $[\langle 1 \rangle_K]$  is a neutral element for  $\otimes$ . Given  $[(V, q)] \in W(K)$ , its additive inverse is given by  $[(V, -q)]$ .

*Proof.* We first prove the well-definedness. That is, assume  $(V_1, q_1), (V'_1, q'_1), (V_2, q_2), (V_2, q'_2)$  are such that  $(V_1, q_1) \equiv (V'_1, q'_1)$  and  $(V_2, q_2) \equiv (V'_2, q'_2)$ , we need to show that  $(V_1 \times V_2, q_1 \perp q_2) \equiv (V'_1 \times V'_2, q'_1 \perp q'_2)$  and  $(V_1 \otimes V_2, q_1 \otimes q_2) \equiv (V'_1 \otimes V'_2, q'_1 \otimes q'_2)$ . Since nonsingular quadratic spaces are Witt equivalent if and only if they are isometric after adding a number of copies of the hyperbolic plane to one of them, it suffices to consider the case  $(V_1, q_1) = (V'_1, q'_1)$  and  $(V_2, q_2) = (V_2, q_2) \perp \mathbb{H}_K$ .

We compute that

$$(V_1, q_1) \perp ((V_2, q_2) \perp \mathbb{H}_K) \cong ((V_1, q_1) \perp (V_2, q_2)) \perp \mathbb{H}_K \equiv (V_1, q_1) \perp (V_2, q_2)$$

as desired. Similarly

$$\begin{aligned} (V_1, q_1) \otimes ((V_2, q_2) \perp \mathbb{H}_K) &\cong (V_1, q_1) \otimes (V_2, q_2) \perp (V_1, q_1) \otimes \mathbb{H}_K \\ &\cong (V_1, q_1) \otimes (V_2, q_2) \perp \dim(V_1) \times \mathbb{H}_K \\ &\equiv (V_1, q_1) \otimes (V_2, q_2) \end{aligned}$$

where the second isometry follows from Corollary 3.1.10. This shows that the operations  $\perp$  and  $\otimes$  are well-defined on  $W(K) \times W(K)$ . The associativity, commutativity and distributivity are immediate from the corresponding properties for  $\perp$  and  $\otimes$  on quadratic spaces. That  $[\langle \rangle_K]$  is a neutral element for  $\perp$  and  $[\langle 1 \rangle_K]$  is a neutral element for  $\otimes$ , is readily verified. Finally, that  $[(V, -q)] = -[(V, q)]$  is a reformulation of Proposition 2.1.12.  $\square$

**4.1.4. Definition.** The set  $W(K)$  endowed with the ring structure described in Theorem 4.1.3 is called the *Witt ring of  $K$* .

**4.1.5. Proposition.**  $W(K)$  has a unique ideal of index 2, which is given by

$$I(K) = \{[(V, q)] \mid \dim V \text{ even}\}.$$

*Proof.* Observe that, if two nonsingular quadratic spaces are Witt equivalent, then their dimensions differ by an even number. In particular, if one of them has even dimension, then the other too. It is easy to see that  $I(K)$  is an ideal. Furthermore, it has index 2, because for any quadratic space  $(V, q)$ , either  $[(V, q)] \in I(K)$ , or  $[(V, q) \perp \langle 1 \rangle_K] \in I(K)$ .

Assume that  $J$  is another ideal of  $W(K)$  of index 2. For  $a, b \in K^\times$ , we have that  $[\langle a \rangle_K], [\langle b \rangle_K] \in W(K)^\times \subseteq W(K) \setminus J$ , hence  $[\langle a, b \rangle_K] \in J$ . In view of Corollary 1.2.10, we conclude that  $J$  contains all classes of quadratic spaces of even dimension, hence  $I(K) \subseteq J$ . But then  $I(K) = J$ .  $\square$

**4.1.6. Definition.** The ideal  $I(K)$  described in Proposition 4.1.5 is called the *fundamental ideal of  $W(K)$* .

**4.1.7. Remark.** Over a field  $K$  with  $\text{char}(K) = 2$ , the situation is more subtle. There are natural operations  $\perp$  and  $\otimes$  on the class of *symmetric bilinear spaces*

over  $K$ , and this allows one to define a Witt ring  $W(K)$  of nonsingular symmetric bilinear forms. On the class of quadratic spaces over  $K$  there is no natural notion of tensor product, but one can still define a group operation  $\perp$ , and one obtains a different object from  $W(K)$ : the quadratic Witt group  $I_q(K)$ . While  $I_q(K)$  is not a ring, it does carry an action by  $W(K)$ :  $I_q(K)$  is a  $W(K)$ -module. See [EKM08, Sections 2, 8] for more on this.

**4.2. Determinants and discriminants.** We briefly introduce the concept of the determinant of a symmetric bilinear form. This allows us to simplify certain computations with small-dimensional quadratic forms.

**4.2.1. Proposition.** *Let  $(V_1, B_1)$  and  $(V_2, B_2)$  be isometric symmetric bilinear spaces with bases  $\mathfrak{B}_1$  and  $\mathfrak{B}_2$ . Then  $\det(M_{\mathfrak{B}_1}(B_1)) \equiv \det(M_{\mathfrak{B}_2}(B_2)) \pmod{K^{\times 2}}$ .*

*Proof.* It suffices to consider the case  $V_1 = V_2 = K^n$  for  $n = \dim(V_1)$ , and where  $\mathfrak{B}_1$  is the canonical basis  $\{e_1, \dots, e_n\}$ . Let  $C \in \mathbb{M}_n(K)^\times$  be the base change matrix between  $\mathfrak{B}_1$  and  $\mathfrak{B}_2$ , i.e. such that  $\mathfrak{B}_2 = \{Ce_1, \dots, Ce_n\}$ . We see that for column vectors  $v, w \in K^n$  we have

$$v^T C^T M_{\mathfrak{B}_1}(B) C w = B(Cv, Cw) = v^T M_{\mathfrak{B}_2}(B) w$$

whence  $M_{\mathfrak{B}_2}(B) = C^T M_{\mathfrak{B}_1}(B) C$  and hence  $\det(M_{\mathfrak{B}_2}(B)) = \det(M_{\mathfrak{B}_1}(B)) \det(C)^2 \equiv \det(M_{\mathfrak{B}_1}(B)) \pmod{K^{\times 2}}$  as desired.  $\square$

**4.2.2. Definition.** For a nonsingular symmetric bilinear space  $(V, B)$ , we define the *determinant* of  $(V, B)$  (or simply of  $B$ ) to be the equivalence class of  $\det(M_{\mathfrak{B}}(B))$  in  $K^\times / K^{\times 2}$ , where  $\mathfrak{B}$  is any basis of  $V$ . We denote it simply by  $\det(V, B)$ .

If  $\text{char}(K) \neq 2$  and  $(V, q)$  is a quadratic space over  $K$ , we define its determinant as the determinant of  $(V, \frac{b_q}{2})$ .

For the rest of this subsection, assume that all quadratic spaces are considered over a field  $K$  with  $\text{char}(K) \neq 2$ .

**4.2.3. Proposition.** *We have the following properties.*

- (1) *For nonsingular quadratic spaces  $(V_1, q_1)$  and  $(V_2, q_2)$  we have  $\det((V_1, q_1) \perp (V_2, q_2)) = \det(V_1, q_1) \cdot \det(V_2, q_2)$ .*
- (2) *For  $a_1, \dots, a_n \in K^\times$  we have  $\det(\langle a_1, \dots, a_n \rangle_K) \equiv a_1 \cdots a_n \pmod{K^{\times 2}}$ .*
- (3)  *$\det(\mathbb{H}_K) \equiv -1 \pmod{K^{\times 2}}$ .*

*Proof.* These can be verified easily via the definition.  $\square$

In general, over a field where  $-1$  is not a square, determinants of Witt equivalent quadratic forms might differ by a minus sign. This can be easily remedied.

**4.2.4. Definition.** Let  $(V, q)$  be a nonsingular quadratic space. We define its *discriminant* (in some books called *signed determinant*) to be

$$d(V, q) = (-1)^{\binom{\dim(V)}{2}} \det(V, q) \in K^\times / K^{\times 2}.$$

Observe that for a natural number  $n$  we have

$$(-1)^{\binom{n}{2}} = \begin{cases} 1 & \text{if } n \equiv 0, 1 \pmod{4} \\ -1 & \text{if } n \equiv 2, 3 \pmod{4} \end{cases}.$$

In particular, if  $m$  and  $n$  are two natural numbers and at least one of them is even, then it follows that

$$(1) \quad (-1)^{\binom{m}{2}}(-1)^{\binom{n}{2}} = (-1)^{\binom{m+n}{2}}.$$

**4.2.5. Proposition.** *If  $(V, q)$  and  $(V', q')$  are Witt equivalent nonsingular quadratic spaces, then  $d(V, q) = d(V', q')$ . Furthermore, the map*

$$IK \rightarrow K^\times / K^{\times 2} : [(V, q)] \mapsto d(V, q)$$

*is a well-defined surjective group homomorphism.*

*Proof.* For the first part, we need to check that if  $(V, q) \cong (V', q')$ , then  $d(V, q) = d(V', q')$ . It suffices to consider the case where  $(V', q') = (V, q) \perp \mathbb{H}_K$ . We compute using Proposition 4.2.3 and eq. (1) that

$$\begin{aligned} d((V, q) \perp \mathbb{H}_K) &= (-1)^{\binom{\dim(V)+2}{2}} \det((V, q) \perp \mathbb{H}_K) \\ &= -(-1)^{\binom{\dim(V)}{2}} \det(V, q) \det(\mathbb{H}_K) \\ &= (-1)^{\binom{\dim(V)}{2}} \det(V, q) = d(V, q) \end{aligned}$$

as desired. This also shows that the given map is well-defined.

The fact that it is a group homomorphism is now also immediate from Proposition 4.2.3 and eq. (1). For the surjectivity, it suffices to observe that  $d(\langle 1, -a \rangle_K) \equiv a \pmod{K^{\times 2}}$  for  $a \in K^\times$ .  $\square$

As announced, determinants are a useful invariant of quadratic spaces which can help to simplify certain calculations. We give an important example.

**4.2.6. Proposition.** *Let  $a, b, c \in K^\times$  and assume that  $c \in D_K(\langle a, b \rangle_K)$ . Then  $\langle a, b \rangle_K \cong \langle c, abc \rangle_K$ .*

*Proof.* By Proposition 1.2.9 we have  $\langle a, b \rangle_K \cong \langle c, d \rangle_K$  for some  $d \in K^\times$ . But since  $cd \equiv \det(\langle c, d \rangle_K) \equiv \det(\langle a, b \rangle_K) \equiv ab \pmod{K^{\times 2}}$ , we must have  $d \equiv abc \pmod{K^{\times 2}}$ , whereby  $\langle c, d \rangle_K \cong \langle c, abc \rangle_K$ . This concludes the proof.  $\square$

**4.3. Multiplicative forms.** When  $(V, q)$  is a quadratic space, the set  $D_K(q)$  of elements of  $K^\times$  represented by  $q$  is in general just a subset of  $K^\times$ . We now consider a class of quadratic forms where this is in fact a subgroup.

**4.3.1. Definition.** Let  $(V, q)$  be a quadratic space. We call the set

$$G_K(q) = \{a \in K^\times \mid (V, q) \cong (V, aq)\}$$

the set of *similarity factors* of  $(V, q)$ .

By a *multiplicative form over  $K$*  (some books use the term *round form*) we mean a nonsingular quadratic form  $q$  for which  $D_K(q) = G_K(q)$ .

4.3.2. *Example.* Every hyperbolic form is multiplicative, see Corollary 2.1.10.

4.3.3. **Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space over  $K$ .*

- (1)  $G_K(q)$  is a subgroup of  $K^\times$  that contains  $K^{\times 2}$ .
- (2)  $G_K(q) \cdot D_K(q) = D_K(q)$ .

*Proof.* The first part is clear. For the second part, consider  $a \in G_K(q)$  and  $d \in D_K(q)$ , then  $ad \in D_K(aq) = D_K(q)$ .  $\square$

For the rest of this subsection, assume  $\text{char}(K) \neq 2$ .

4.3.4. **Theorem (Witt).** *Let  $q$  be a multiplicative form over  $K$  and  $a \in K^\times$ . Then the form  $\langle 1, a \rangle_K \otimes q$  is multiplicative. Moreover, if  $q$  is anisotropic, then  $\langle 1, a \rangle_K \otimes q$  is either anisotropic or hyperbolic.*

*Proof.* Let  $q' = \langle 1, a \rangle_K \otimes q$ . We have  $1 \in G_K(q) = D_K(q) \subseteq D_K(q')$  and hence  $G_K(q') \subseteq D_K(q')$  by Proposition 4.3.3. Further, observe that  $D_K(q) \cup aD_K(q) = G_K(q) \cup aG_K(q) \subseteq G_K(q')$ . Now consider  $c \in D_K(q') \setminus (D_K(q) \cup aD_K(q))$  arbitrary. Then there exist  $s, t \in D_K(q) = G_K(q)$  such that  $c \in D_K(\langle s, at \rangle_K)$ . By Proposition 4.2.6 it follows that  $\langle s, at \rangle_K \cong \langle c, acst \rangle_K$ . We now compute that

$$\begin{aligned} q' &\cong q \perp aq \cong sq \perp atq \cong \langle s, at \rangle_K \otimes q \cong \langle c, acst \rangle_K \otimes q \\ &\cong cq \perp acstq \cong cq \perp acq \cong cq' \end{aligned}$$

whereby  $c \in G_K(q')$ . Since  $c \in D_K(q')$  was chosen arbitrarily, we conclude that  $q'$  is multiplicative.

For the second part, assume that  $q$  is anisotropic and  $q'$  is isotropic. Then there exist  $s, t \in D_K(q) = G_K(q)$  with  $\langle s, at \rangle_K \cong \mathbb{H}_K$ . We compute that

$$q' \cong q \perp aq \cong sq \perp atq \cong \langle s, at \rangle_K \otimes q \cong \mathbb{H}_K \otimes q$$

which is hyperbolic by Corollary 3.1.10.  $\square$

4.3.5. **Definition.** For  $n \in \mathbb{N}$  and  $a_1, \dots, a_n \in K^\times$ , we use the notation

$$\langle\langle a_1, \dots, a_n \rangle\rangle_K = \langle 1, -a_1 \rangle \otimes \dots \otimes \langle 1, -a_n \rangle_K.$$

In particular,  $\langle\langle \rangle\rangle_K = \langle 1 \rangle_K$ , and  $\langle\langle a_1 \rangle\rangle_K = \langle 1, -a_1 \rangle_K$ . We call a form which is isometric to  $\langle\langle a_1, \dots, a_n \rangle\rangle_K$  for some  $a_1, \dots, a_n \in K^\times$  an  $n$ -fold Pfister form.

4.3.6. **Theorem (Pfister).** *Let  $q$  be a Pfister form over  $K$ . Then  $q$  is multiplicative, and either anisotropic or hyperbolic.*

*Proof.* Assume that  $q$  is an  $n$ -fold Pfister form; we proceed by induction on  $n$ . For  $n = 0$  we have  $q \cong \langle 1 \rangle_K$ ; this form is anisotropic and  $D_K(q) = K^{\times 2} = G_K(q)$ . Assume now  $n > 0$ . We have that  $q \cong \langle 1, -a \rangle_K \otimes q'$  for some  $(n - 1)$ -fold Pfister form  $q'$  over  $K$ . If  $q'$  is anisotropic, then by induction hypothesis,  $q'$  is multiplicative, and by Theorem 4.3.4 also  $q$  is multiplicative and either anisotropic or hyperbolic. If  $q'$  is isotropic, then by induction hypothesis it is hyperbolic, and then also  $q$  is hyperbolic by Corollary 3.1.10.  $\square$

We mention the following partial converse to Theorem 4.3.6, the proof of which is outside the scope of this course. We will not use this result in the sequel. For a quadratic form  $q$  over  $K$  and a field extension  $L/K$ , we denote by  $q_L$  the quadratic form over  $L$  obtained by extending scalars from  $K$  to  $L$  (we will see a formal definition later, see Definition 6.2.2).

**4.3.7. Theorem (Pfister).** *Let  $q$  be an anisotropic quadratic form over  $K$ . The following are equivalent.*

- (1)  $q$  is a Pfister form,
- (2)  $D_L(q_L)$  is a subgroup of  $L^\times$  for every field extension  $L/K$ ,
- (3)  $1 \in D_K(q)$  and for every field extension  $L/K$  we have that  $q_L$  is either anisotropic or hyperbolic.

*Proof.* See [EKM08, Theorem 23.2 and Corollary 23.4]. □

**4.3.8. Remark.** Over a field  $K$  of characteristic 2, one can define a notion of Pfister form both for bilinear forms and for quadratic forms. As usual, we refer to [EKM08, Sections 7 and 9] for a characteristic-free exposition. An example of a 1-fold quadratic Pfister form is given by  $X^2 + XY + aY^2$  for  $a \in K$ . These quadratic Pfister forms still satisfy the properties of Theorem 4.3.6 in characteristic 2.

**4.4. Exercises.** In all exercises, assume  $K$  is a field with  $\text{char}(K) \neq 2$ .

- (1) Compute the Witt ring of  $\mathbb{C}$  and  $\mathbb{R}$ .
- (2) Let  $K$  be finite. Show the following:
  - (a)  $|K^\times/K^{\times 2}| = 2$ ,
  - (b) Every nonsingular 2-dimensional quadratic form over  $K$  is universal.
  - (c) Assume  $d \in K^\times \setminus K^{\times 2}$ . Every anisotropic quadratic form over  $K$  is isometric to precisely one of the following forms:

$$\langle \rangle_K \quad \langle 1 \rangle_K \quad \langle d \rangle_K \quad \langle 1, -d \rangle_K$$

- (d) If  $|K| \equiv 1 \pmod 4$ , then  $-1 \in K^{\times 2}$  and  $WK \cong (\mathbb{Z}/2\mathbb{Z})[T]/(T^2 + 1)$ .
- (e) If  $|K| \equiv 3 \pmod 4$ , then  $-1 \notin K^{\times 2}$  and  $WK \cong \mathbb{Z}/4\mathbb{Z}$ .
- (3) Show that for  $a, b \in K^\times$  and a Pfister form  $q$  over  $K$  we have  $\langle\langle a \rangle\rangle_K \otimes q \cong \langle\langle b \rangle\rangle_K \otimes q$  if and only if  $ab \in D_K(q)$ .
- (4) Let  $q$  be a 4-dimensional nonsingular quadratic form over  $K$  with  $1 \in D_K(q)$  and  $\det(q) \equiv 1 \pmod{K^{\times 2}}$ . Show that  $q$  is a Pfister form.
- (5) Let  $q$  be a universal 3-dimensional quadratic form over  $K$ . Show that  $q$  is isotropic.
- (6) Show that  $D_{\mathbb{Q}}(\langle 1, 1 \rangle_{\mathbb{Q}})$  is a subgroup of  $\mathbb{Q}^\times$ . Is the same true for  $D_{\mathbb{Q}}(\langle 1, 1, 1 \rangle_{\mathbb{Q}})$ ?
- (7) Give an example of an anisotropic quadratic form which is multiplicative but not a Pfister form.
- (8) Let  $n \in \mathbb{N}$  and suppose that  $-1$  is a sum of  $2^{n+1} - 1$  squares in  $K$ . Show that  $-1$  is a sum of  $2^n$  squares in  $K$ .

## 5. LECTURE 5

**5.1. Powers of the fundamental ideal.** Assume throughout that  $K$  is a field with  $\text{char}(K) \neq 2$  and that all quadratic spaces are considered over  $K$ .

We will consider powers of the fundamental ideal  $IK$  of the Witt ring  $WK$ . For a natural number  $n$ , we denote by  $I^n K$  the ideal of  $WK$  generated by products of  $n$  elements in  $IK$ . By convention, we set  $I^0 K = WK$ . We obtain a natural filtration

$$WK = I^0 K \supseteq I^1 K = IK \supseteq I^2 K \supseteq I^3 K \supseteq \dots$$

We can try to understand the group  $WK$  better by studying the ideals  $I^n K$ , and/or by studying the quotients  $I^n K / I^{n+1} K$ . We already know that  $WK / I^1 K \cong \mathbb{Z}/2\mathbb{Z}$ , see Proposition 4.1.5.

**5.1.1. Proposition.** *For  $n \geq 1$ , the ideal  $I^n K$  is generated as a group by the Witt classes of  $n$ -fold Pfister forms in  $K$ .*

*Proof.* First observe that, for  $a, b \in K^\times$ , we have

$$\langle a, b \rangle_K \equiv \langle a, b \rangle_K \perp \mathbb{H}_K \cong \langle 1, a \rangle_K \perp -\langle 1, -b \rangle_K \cong \langle\langle -a \rangle\rangle_K \perp -\langle\langle b \rangle\rangle_K.$$

Since every nonsingular binary quadratic form is isometric to  $\langle a, b \rangle_K$  for some  $a, b \in K^\times$  and since binary quadratic forms generate  $IK$ , we conclude that  $IK$  is generated as a group by 1-fold Pfister forms. Since an  $n$ -fold Pfister form is by definition a product of  $n$  1-fold Pfister forms, we conclude that  $I^n K$  is generated by  $n$ -fold Pfister forms, as desired.  $\square$

A quadratic form over  $K$  which is isometric to  $a\pi$  for a Pfister form  $\pi$  and an element  $a \in K^\times$  is called a *scaled Pfister form*. Observe that the class of a scaled  $n$ -fold Pfister form lies in  $I^n K$ .

**5.1.2. Lemma.** *Let  $(V, q)$  a nonsingular quadratic space over  $K$ , assume  $\dim(V) \geq 3$ . There exists a quadratic space  $(W, q')$  with  $\dim(W) = \dim(V) - 2$  and a scaled Pfister form  $(P, q_P)$  such that  $(V, q) \equiv (W', q') \perp (P, q_P)$ .*

*Proof.* In view of Corollary 1.2.10 it suffices to consider the case where  $(V, q) = \langle a, b, c \rangle_K$  for  $a, b, c \in K^\times$ . Now set  $q' = \langle -abc \rangle_K$  and  $q_P = abc \langle\langle -ab, ac \rangle\rangle_K$ . We have  $\dim(q') = 1$  and we compute that

$$q' \perp q_P \cong \langle -abc, abc \rangle_K \perp \langle a, b, c \rangle_K \cong \mathbb{H}_K \perp q \equiv q.$$

Hence  $q'$  and  $q_P$  are as desired.  $\square$

**5.1.3. Proposition.** *The homomorphism  $d : IK \rightarrow K^\times / K^{\times 2} : [(V, q)] \mapsto d(V, q)$  from Proposition 4.2.5 has kernel  $I^2 K$ . In particular,  $IK / I^2 K \cong K^\times / K^{\times 2}$ .*

*Proof.* One computes that, for any  $a, b \in K^\times$ , we have

$$d(\langle\langle a, b \rangle\rangle_K) = d(\langle 1, -a, -b, ab \rangle_K) \equiv 1 \pmod{K^{\times 2}}.$$

So, any equivalence class of a 2-fold Pfister form lies in the kernel of  $d$ . In view of Proposition 5.1.1 we conclude that  $I^2 K \subseteq \text{Ker}(d)$ .



For the converse implication, consider  $\zeta \in \text{Ker}(d)$ . By Lemma 5.1.2 we have  $\zeta \equiv [(V, q)] \pmod{I^2K}$  where  $\dim(V) = 2$ . Since  $I^2K \subseteq \text{Ker}(d)$  by the previous paragraph, we conclude that  $d(V, q) = d(\zeta) \equiv 1 \pmod{K^{\times 2}}$ . But then  $\det(V, q) = -1$ , which implies  $(V, q) \cong \mathbb{H}_K$ , whereby  $[(V, q)] = 0$ , and we conclude that  $\zeta \in I^2K$  as desired.  $\square$

**5.1.4. Proposition.** *Let  $(V, q)$  be a nonsingular quadratic space with  $[(V, q)] \in I^2K$  and  $m = \dim(V)/2 - 1$ . There exist scaled 2-fold Pfister forms  $\pi_1, \dots, \pi_m$  such that  $[(V, q)] = \sum_{i=1}^m [\pi_i]$ .*

*Proof.* If  $m = 0$  then, as in the proof of Proposition 5.1.3, we see that  $(V, q)$  must be hyperbolic, hence  $[(V, q)] = 0$ . The general case now follows from Lemma 5.1.2 by induction on  $m$ .  $\square$

**5.1.5. Question.** *Let  $n, d \in \mathbb{N}^+$ . Does there exist a natural number  $m$  such that every  $d$ -dimensional quadratic space  $(V, q)$  with  $[(V, q)] \in I^nK$  is Witt equivalent to a sum of  $m$  scaled Pfister forms?*

For  $n = 1$  the answer is easy (every binary nonsingular quadratic form is a scaled Pfister form, so one can take  $m = d/2$ ), and for  $n = 2$  one can take  $m = d/2 - 1$  by Proposition 5.1.4. For  $n = 3$  it is known that such a number  $m$  exists, and that it grows at least exponentially as a function of  $d$  [BRV10]. For  $n > 3$  it is completely open whether such a number  $m$  exists in general. Of course, over many specific fields  $K$ , often the situation is much easier.

We mention the following major theorem, without providing a proof.

**5.1.6. Theorem** (Arason-Pfister Hauptsatz, 1971). *Let  $n \in \mathbb{N}$  and let  $(V, q)$  be a nonsingular quadratic space with  $[(V, q)] \in I^nK$ .*

- (1) *Either  $\dim(V) \geq 2^n$  or  $(V, q)$  is hyperbolic.*
- (2) *If  $\dim(V) = 2^n$ , then  $(V, q)$  is a scaled  $n$ -fold Pfister form.*

*Proof.* The first part is [EKM08, Theorem 23.7]. The second part follows from combining the first part with Theorem 4.3.7.  $\square$

**5.1.7. Corollary.** *We have  $\bigcap_{n \in \mathbb{N}} I^nK = \{0\}$ .*

*Proof.* Consider a non-zero element of  $WK$ , then it is of the form  $[(V, q)]$  for some non-zero anisotropic quadratic form  $q$ . For  $n > \log_2(\dim(V))$  we have  $[(V, q)] \notin I^nK$  by Theorem 5.1.6.  $\square$

## 5.2. Exercises.

- (1) Show the following:
  - (a)  $|K^\times/K^{\times 2}| < \infty$  if and only if, for every  $n \in \mathbb{N}$ , there exist up to isomorphism only finitely many anisotropic quadratic forms of dimension  $n$ , if and only if  $WK$  is a noetherian ring,
  - (b)  $|WK| < \infty$  if and only if  $|K^\times/K^{\times 2}| < \infty$  and  $-1$  is a sum of squares in  $K$ .

## 6. LECTURE 6

**6.1. Signatures and orderings.** Much more can be said about the structure of Witt rings, see e.g. [EKM08, Chapter V] or [Lam05, Sections VIII.7 and VIII.8]. We explain one important source of structure on a field which can introduce complexity into its Witt ring: orderings. For a very detailed discussion of orderings and their interplay with quadratic forms, we refer to the book [Lam83].

**6.1.1. Definition.** Let  $K$  be a field. A (*field*) *ordering* on  $K$  is a total order relation  $\leq$  on  $K$  such that for all  $a, b, c \in K$  one has

- if  $a \leq b$ , then  $a + c \leq a + c$ ,
- if  $a \leq b$  and  $0 \leq c$ , then  $ac \leq bc$ .

A tuple  $(K, \leq)$  where  $K$  is a field and  $\leq$  is an ordering on  $K$  is called an *ordered field*.

**6.1.2. Examples.** The usual ordering on  $\mathbb{R}$  ( $a \leq b$  if and only if  $b - a$  is a square in  $\mathbb{R}$ ) makes  $\mathbb{R}$  into an ordered field.

If  $(K, \leq_K)$  is an ordered field and  $\iota : L \rightarrow K$  is an embedding of fields, then one can naturally define an ordering  $\leq_L$  on  $L$  as follows: for  $a, b \in L$ , let  $a \leq_L b$  if and only if  $\iota(a) \leq_K \iota(b)$ . In particular, an embedding of a field  $L$  into  $\mathbb{R}$  naturally induces an ordering on  $L$ .

Whether or not a field can be made to carry an ordering is characterised by the Artin-Schreier Theorem.

**6.1.3. Theorem (Artin-Schreier).** *A field  $K$  carries a field ordering if and only if  $-1$  is not a sum of squares in  $K$ .*

*Proof.* If  $K$  carries an ordering  $\leq$ , then for any  $a \in K$  one has  $0 \leq a^2$ . In particular, it follows that any sum of squares in  $K$  is positive. But  $-1$  is negative, hence it cannot be a sum of squares. See exercise (1) for details.

See [Lam83, 1.5] for a proof of the other implication. □

The above implies in particular that, if  $K$  is a field carrying an ordering, then  $\text{char}(K) = 0$ .

**6.1.4. Definition.** Let  $(K, \leq)$  be an ordered field,  $(V, q)$  a nonsingular quadratic form over  $K$ . We call  $q$  *positive definite with respect to  $\leq$*  if  $0 \leq a$  for all  $a \in D_K(q)$ , *negative definite with respect to  $\leq$*  if  $a \leq 0$  for all  $a \in D_K(q)$ , and *indefinite with respect to  $\leq$*  if it is neither positive nor negative definite.

**6.1.5. Theorem (Sylvester's law of inertia).** *Let  $(K, \leq)$  be an ordered field,  $(V, q)$  a nonsingular quadratic form over  $K$ . There exist quadratic forms  $q^+$  and  $q^-$  which are positive definite with respect to  $\leq$  and such that  $q \cong q^+ \perp -q^-$ . The numbers  $\dim(q^+)$  and  $\dim(q^-)$  depend only on  $q$ .*

*Proof.* For the existence of  $q^+$  and  $q^-$ , we may assume by Corollary 1.2.10 that  $q$  is a diagonal form, from which the statement is immediate, since every 1-dimensional nonsingular quadratic form is either positive or negative definite with respect to  $\leq$ .

For the uniqueness, assume that  $q \cong q_1^+ \perp -q_1^- \cong q_2^+ \perp -q_2^-$  for some totally positive forms  $q_1^+, q_1^-, q_2^+, q_2^-$  over  $K$ . That is, there exist subspaces  $U, W$  of  $V$  such that  $q|_U \cong q_1^+$ ,  $q|_{U^\perp} \cong -q_1^-$ ,  $q|_W \cong q_2^+$ ,  $q|_{W^\perp} \cong -q_2^-$ . We observe that  $U^\perp \cap W = 0 = U \cap W^\perp$  since  $D_K(q_1^+) \cap D_K(-q_2^-) = \emptyset = D_K(q_2^+) \cap D_K(-q_1^-)$ . From this we infer that  $\dim(U) = \dim(W)$  and thus  $\dim(U^\perp) = \dim(W^\perp)$ , whereby  $\dim(q_1^+) = \dim(q_2^+)$  and  $\dim(q_1^-) = \dim(q_2^-)$ .  $\square$

**6.1.6. Definition.** For an ordered field  $(K, \leq)$  and a nonsingular quadratic form  $q$  over  $K$ , define the *signature of  $q$  with respect to  $\leq$*  as the integer  $\dim(q^+) - \dim(q^-)$ , where  $q^+$  and  $q^-$  are as in Theorem 6.1.5 - this depends only on the isometry class of  $q$ . We denote this integer by  $\text{sign}_\leq(q)$ .

**6.1.7. Proposition.** *Let  $(K, \leq)$  be an ordered field. There is a well-defined ring homomorphism*

$$WK \rightarrow \mathbb{Z} : [(V, q)] \mapsto \text{sign}_\leq(q).$$

*Proof.* Observe that  $\text{sign}_\leq(\mathbb{H}_K) = \text{sign}_\leq(\langle 1, -1 \rangle_K) = 0$ . It follows that, if  $(V, q) \cong (W, q')$ , then  $\text{sign}_\leq(q) = \text{sign}_\leq(q')$ , showing that the map is well-defined on  $WK$ . The fact that it is a ring homomorphism is easily verified.  $\square$

The kernel of the homomorphism defined in Proposition 6.1.7 is a prime ideal of  $WK$  called the *signature ideal of  $\leq$* , which we will denote by  $I_\leq K$ .

We mention without proof two theorems about the prime ideals of the Witt ring and about torsion in the Witt ring.

**6.1.8. Theorem** (Leicht-Lorenz, Harrison, 1970). *Let  $\mathfrak{p}$  be a prime ideal of  $WK$  different from  $IK$ . Then we can define an ordering  $\leq$  on  $K$  as follows: for  $a, b \in K$  with  $a \neq b$ , set*

$$a \leq b \iff [\langle 1, a - b \rangle_K] \in \mathfrak{p}.$$

*Furthermore,  $I_\leq K \subseteq \mathfrak{p}$ .*

*Proof.* See e.g. [EKM08, Theorem 31.24].  $\square$

**6.1.9. Theorem** (Pfister's Local-global principle, 1966). *The following are equivalent for a quadratic space  $(V, q)$  over  $K$ .*

- (1)  $\text{sign}_\leq(q) = 0$  for all orderings  $\leq$  on  $K$ ,
- (2)  $[(V, q)]$  is torsion in  $WK$ ,
- (3)  $[(V, q)]$  is  $2^k$ -torsion in  $WK$  for some  $k \in \mathbb{N}$ .

*Proof.* See e.g. [Lam05, Theorem VIII.3.2].  $\square$

**6.2. Field extensions.** For a field extension  $L/K$  and a  $K$ -vector space  $V$ , the vector space  $V_L = V \otimes L$  naturally becomes an  $L$ -vector space, with  $\dim_K(V) = \dim_L(V_L)$  - see Proposition 3.1.4. Furthermore, via the embedding  $V \rightarrow V \otimes L : v \mapsto v \otimes 1$ , we may identify  $V$  with a  $K$ -subspace of  $V \otimes L$ . We will now see that this gives a natural way to ‘extend’ symmetric bilinear and quadratic forms from  $K$  to  $L$ .

**6.2.1. Proposition.** *Consider a field  $K$  and a field extension  $L/K$ . For a symmetric bilinear space  $(V, B)$  over  $K$ , there exists a unique symmetric bilinear form  $B_L$  on  $V_L = V \otimes_K L$  such that, for all  $v, w \in V$  and  $x, y \in L$ , one has*

$$B_L(v \otimes x, w \otimes y) = B(v, w)xy.$$

*Similarly, for a quadratic space  $(V, q)$  over  $K$ , there exists a unique quadratic form  $q_L$  on  $V_L$  such that, for all  $v \in V$  and  $x \in L$ , one has*

$$q_L(v \otimes x) = x^2q(v).$$

*Proof.* By redoing the proof of Proposition 3.1.5, using that  $B$  is a  $K$ -bilinear map and also  $L \times L \rightarrow L : (x, y) \mapsto xy$  is a  $K$ -bilinear map, one obtains that there exists a unique symmetric  $K$ -bilinear map  $B_L : V_L \times V_L \rightarrow L$  such that  $B_L(v \otimes x, w \otimes y) = B(v, w)xy$  for all  $v, w \in V$  and  $x, y \in L$ . One then readily verifies that this map is actually also  $L$ -bilinear.

For the second statement, let us first consider uniqueness. If  $q_L$  is a quadratic form on  $V_L$  such that  $q_L(v \otimes x) = x^2q(v)$  for all  $v \in V$  and  $x \in L$ , then clearly  $\mathfrak{b}_{q_L} = (\mathfrak{b}_q)_L$ . But  $q_L$  is completely determined by its values on elementary tensors and by  $\mathfrak{b}_{q_L}$ . This shows uniqueness.

If  $\text{char}(K) \neq 2$ , then the existence part of the statement follows from the fact that  $q(v) = \frac{1}{2}\mathfrak{b}_q(v, v)$  for all  $v \in V$ : one may just define  $q_L(\alpha) = \frac{1}{2}(\mathfrak{b}_q)_L(\alpha, \alpha)$  for  $\alpha \in V_L$ . If  $\text{char}(K) = 2$  then a more subtle argument is needed: one still has that there exists some bilinear (but not necessarily symmetric) form  $B : V \times V \rightarrow K$  such that  $q(v) = B(v, v)$  for all  $v \in V$  (see [EKM08, Section 7]) and one may then set  $q_L(\alpha) = B_L(\alpha, \alpha)$  for  $\alpha \in V_L$ .  $\square$

**6.2.2. Definition.** For a symmetric bilinear space  $(V, B)$  over  $K$  and a field extension  $L/K$  the symmetric bilinear space  $(V, B)_L = (V_L, B_L)$  over  $L$  constructed in Proposition 6.2.1 is called the *scalar extension of  $(V, B)$  to  $L$* .

Similarly, for a quadratic space  $(V, q)$ , we define the *scalar extension of  $(V, q)$  to  $L$*  as the quadratic space  $(V, q)_L = (V_L, q_L)$  constructed in Proposition 6.2.1.

For a quadratic space  $(V, q)$  over  $K$ , we will say that it is *isotropic over  $L$*  (respectively *anisotropic, hyperbolic, multiplicative, a Pfister form, ... over  $L$* ) if  $q_L$  is isotropic (respectively anisotropic, hyperbolic, multiplicative, ...).

**6.2.3. Remark.** For a homogeneous degree 2 polynomial  $f \in K[X_1, \dots, X_n]$  and a field extension  $L/K$ , we can consider  $f$  as a polynomial over  $L$ . We then have  $(K^n, q_f)_L = (L^n, q_f)$ .

One verifies easily that for quadratic spaces  $(V, q)$ ,  $(V', q')$  one has that  $(V, q) \cong (V', q')$  implies  $(V_L, q_L) \cong (V'_L, q'_L)$ , that  $(q \perp q')_L \cong q_L \perp q'_L$ ,  $(q \otimes q')_L \cong q_L \otimes q'_L$ , and  $(\mathbb{H}_K)_L = \mathbb{H}_L$ . Furthermore, if  $(V, q)$  is an  $n$ -fold Pfister form, then so is  $(V_L, q_L)$ . Putting this together, we obtain the following:

**6.2.4. Proposition.** *Assume  $\text{char}(K) \neq 2$ , let  $L/K$  be a field extension. The rule*

$$r_{L/K} : WK \rightarrow WL : [(V, q)] \mapsto [(V_L, q_L)]$$

*gives a well-defined ring homomorphism. For  $n \in \mathbb{N}$ , we have  $r_{L/K}(I^n K) \subseteq I^n L$ .*

**6.2.5. Definition.** Let  $L/K$  be a field extension. The map  $r_{L/K}$  defined in Proposition 6.2.4 is called the *restriction homomorphism*.

In the remainder of this section, we will investigate what it means that a quadratic form becomes isotropic or hyperbolic over a finite field extension. Many of the deeper theorems from quadratic form theory (e.g. Theorem 4.3.7 and Theorem 5.1.6) rely on a study of quadratic forms over arbitrary (non-algebraic) field extensions, e.g. over function fields. We refer to [EKM08, Chapters III-IV] for more on this.

**6.2.6. Theorem (Springer).** *Let  $(V, q)$  be an anisotropic quadratic space over  $K$ ,  $L/K$  a finite field extension of odd degree. Then  $(V_L, q_L)$  is anisotropic.*

*Proof.* We may reduce to the case where  $(V, q) = (K^n, q_Q)$  for some  $n \in \mathbb{N}$  and a homogeneous degree two polynomial  $Q \in K[X_1, \dots, X_n]$ . We need to show that, if there exists  $y \in L^n \setminus \{0\}$  such that  $Q(y) = 0$ , then there exists  $x \in K^n \setminus \{0\}$  with  $Q(x) = 0$ .

We proceed by induction on  $m = [L : K]$ . If  $m = 1$  there is nothing to show, assume now that  $m > 1$ . We may assume that  $L/K$  has no proper intermediate extensions, otherwise we may apply the induction hypothesis twice to conclude. In particular, we may assume that  $L = K[\alpha]$  for some  $\alpha \in L$ .

Consider the unique ring homomorphism  $K[T] \rightarrow L$  which maps  $X$  to  $\alpha$ . It is surjective, and its kernel is a non-zero prime ideal, which is generated by some irreducible polynomial  $f(T) \in K[T]$  of degree  $m$ . By the First Isomorphism Theorem, we conclude that  $L \cong K[T]/(f(T))$ . We assume without loss of generality that  $L = K[T]/(f(T))$ .

Assume now that  $y = (y_1, \dots, y_n) \in L^n \setminus \{0\}$  is such that  $Q(y) = 0$ . Let  $g_1, \dots, g_n \in K[T]$  be such that  $y_i = \overline{g_i}$  and  $m' = \max\{\deg(g_1), \dots, \deg(g_n)\} < \deg(f) = m$ . We may further assume that  $g_1(T), \dots, g_n(T)$  are coprime. Write  $g_i = \sum_{j=0}^m a_j^{(i)} T^j$  for some  $a_j^{(i)} \in K$ , and observe that

$$Q(g_1(T), \dots, g_n(T)) = Q(a_{m'}^{(1)}, \dots, a_{m'}^{(n)}) T^{2m'} + R(T)$$

for some  $R(T) \in K[T]$  with  $\deg(R(T)) < 2m'$ . Since by definition of  $m'$  not all  $a_{m'}^{(i)}$  are zero, we conclude that either  $Q(a_{m'}^{(1)}, \dots, a_{m'}^{(n)}) = 0$  and then we have found our

element  $x \in K^n$  with  $Q(x) \neq 0$ , or  $Q(a_{m'}^{(1)}, \dots, a_{m'}^{(n)}) \neq 0$ . So assume for the sequel that we are in the second case, in particular  $\deg(Q(g_1(T), \dots, g_n(T))) = 2m'$ .

Since  $Q(y) = 0$  in  $K[T]/(f(T))$ , we have that  $f(T) \mid Q(g_1(T), \dots, g_n(T))$ . More precisely, we have

$$f(T)h(T) = Q(g_1(T), \dots, g_n(T))$$

for some polynomial  $h(T) \in K[T]$ . Comparing degrees, we have

$$m + \deg(h(T)) = \deg(f(T)h(T)) = \deg(Q(g_1(T), \dots, g_n(T))) = 2m' < 2m.$$

Hence,  $\deg(h(T)) < m$ , and  $\deg(h(T))$  is odd. Let  $p(T)$  be an irreducible polynomial dividing  $h(T)$  of odd degree, then  $\deg(p(T)) < m$ . Set  $L' = K[T]/(p(T))$  and set  $y'_i = \overline{g_i}$  in  $L'$ . Then we have that  $L'/K$  is an odd degree extension with  $[L' : K] < [L : K]$ , that  $y' = (y'_1, \dots, y'_n) \neq 0$  (since  $g_1, \dots, g_n$  are not all divisible by  $p$ ) and that  $Q(y'_1, \dots, y'_n) = 0$ . We now conclude by invoking the induction hypothesis.  $\square$

**6.2.7. Corollary.** *Let  $L/K$  be a finite field extension of odd degree. Then  $r_{L/K} : WK \rightarrow WL$  is injective.*

*Proof.* Consider a non-zero element of  $WK$ . This is of the form  $[(V, q)]$  for some non-zero anisotropic quadratic space  $(V, q)$  over  $K$ . By Theorem 6.2.6 we have that  $(V_L, q_L)$  is anisotropic, whereby  $0 \neq [(V_L, q_L)] = r_{L/K}([(V, q)])$ . This shows that  $\text{Ker}(r_{L/K}) = 0$ , whereby  $r_{L/K}$  is injective.  $\square$

We now characterise what it means that an anisotropic quadratic space  $(V, q)$  becomes isotropic or hyperbolic over a quadratic extension. For the rest of this subsection, let  $K$  be a field with  $\text{char}(K) \neq 2$ , let  $d \in K^\times \setminus K^{\times 2}$  and let  $L = K[\sqrt{d}]$ .

**6.2.8. Proposition.** *Let  $(V, q)$  be an anisotropic quadratic space over  $K$ . Then  $q_L$  is isotropic if and only if there exists  $a \in D_K(q)$  such that  $\langle a, -ad \rangle_K$  is a subform of  $(V, q)$ .*

*Proof.* Since  $\langle a, -ad \rangle_L$  is isotropic for all  $a \in K^\times$ , one implication is clear.

Assume now that  $q_L$  is isotropic, so there exists  $v \in V_L \setminus \{0\}$  such that  $q_L(v) = 0$ . We may write  $v = v_0 + \delta v_1$  with  $v_0, v_1 \in V$  and  $\delta \in L$  with  $\delta^2 = d$ . We compute that

$$0 = q_L(v) = q_L(v_0 + \delta v_1) = q(v_0) + dq(v_1) + \mathfrak{b}_q(v_0, v_1)\delta.$$

Since  $\{1, \delta\}$  is a  $K$ -basis of  $L$ , we must have  $q(v_0) + dq(v_1) = 0 = \mathfrak{b}_q(v_0, v_1)$ . Since  $v \neq 0$ , both  $v_0$  and  $v_1$  are non-zero, and since  $q$  is anisotropic, this implies that  $q(v_0) = -dq(v_1) \neq 0$ . Set  $a = q(v_1)$ . We see that  $v_0$  and  $v_1$  are linearly independent and orthogonal, and thus finally that, for  $U = Kv_0 + Kv_1$ , we have  $(U, q|_U) \cong \langle a, -ad \rangle_K$ .  $\square$

**6.2.9. Corollary.** *Let  $(V, q)$  be an anisotropic quadratic space over  $K$ . Then  $q_L$  is hyperbolic if and only if there exists a quadratic space  $(V', q')$  over  $K$  such that  $(V, q) \cong \langle\langle d \rangle\rangle_K \otimes q'$ .*

*Proof.* Since  $\langle\langle d \rangle\rangle_L$  is hyperbolic, it follows from Corollary 3.1.10 that  $(\langle\langle d \rangle\rangle_K \otimes q')_L \cong \langle\langle d \rangle\rangle_L \otimes q'_L$  is hyperbolic for any non-singular quadratic space  $(V', q')$ . This concludes the proof for one implication.

For the other implication, assume that  $q_L$  is hyperbolic. We proceed by induction on  $\dim(V)$ . For  $\dim(V) = 0$  there is nothing to show (we may take  $q' = 0$ ). Assume that  $\dim(V) > 0$ . Then  $q$  is isotropic. By Proposition 6.2.8 there exists  $a \in D_K(q)$  such that  $q \cong \langle a, -ad \rangle_K \perp \hat{q}$  for some quadratic form  $\hat{q}$  over  $K$ . Since  $q_L \cong \langle a, -ad \rangle_L \perp \hat{q}_L \cong \mathbb{H}_L \perp \hat{q}_L$  and  $q_L$  is hyperbolic, by Witt Cancellation (Theorem 2.2.2) also  $\hat{q}_L$  is hyperbolic. By induction hypothesis,  $\hat{q} \cong \langle 1, -d \rangle_K \otimes \hat{q}'$  for some quadratic form  $\hat{q}'$ . Now set  $q' = \langle a \rangle_K \perp \hat{q}'$ , then this  $q'$  is as desired.  $\square$

**6.2.10. Corollary.** *Let  $q$  be an anisotropic Pfister form over  $K$  and let  $q'$  be a form such that  $q \cong \langle 1 \rangle_K \perp q'$ . Then  $q_L$  is isotropic if and only if  $-d \in D_K(q')$ .*

*Proof.* Exercise.  $\square$

**6.3. Exercises.** Let always  $K$  be a field with  $\text{char}(K) \neq 2$ .

- (1) Let  $(K, \leq)$  be an ordered field. Show the following for  $a, b, c \in K$ :
  - $-1 \leq 0 \leq 1$ ,
  - if  $a \leq b$  and  $c \leq 0$ , then  $bc \leq ac$ ,
  - $0 \leq a^2$ .
- (2) Verify the details in the proof of Proposition 6.1.7.
- (3) Use Theorem 6.1.9 to prove Theorem 6.1.3.
- (4) Let  $(K, \leq)$  be an ordered field,  $n \in \mathbb{N}$  and  $\alpha \in I^n K$ . Show that  $\text{sign}_{\leq}(\alpha) \in 2^n \mathbb{Z}$ .
- (5) Let  $K/\mathbb{Q}$  be an algebraic field extension. When  $\iota : K \rightarrow \mathbb{R}$  is an embedding, show that  $\leq_{\iota}$ , defined by

$$a \leq_{\iota} b \iff \iota(a) \leq \iota(b)$$

for all  $a, b \in K$ , is a field ordering. Conversely, for a field ordering  $\leq$  on  $K$ , show that

$$\iota_{\leq} : K \rightarrow \mathbb{R} : x \mapsto \inf \left\{ \frac{m}{n} \mid m, n \in \mathbb{N}, n \neq 0, nx \leq m \right\}$$

defines an embedding of fields. Conclude that there is a bijection between the set of field orderings on  $K$  and the set of embeddings of  $K$  into  $\mathbb{R}$ .

- (6) Let  $L = K(X)$ . Show that every anisotropic quadratic form over  $K$  remains anisotropic over  $L$ .
- (7) Prove Corollary 6.2.10.
- (8) Let  $(V, q)$  be a quadratic space and  $d \in K^{\times}$  such that  $q_{K(\sqrt{d})}$  is hyperbolic. Show that  $-d \in G_K(q)$ .

## INDEX

- anisotropic, *see also* isotropic
- definite, positive, negative, in-, 26
- determinant, 20
- diagonal form, 8
- discriminant, 20
- elementary tensor, 15
- field ordering, *see also* ordering
- fundamental ideal, 19
- hyperbolic
  - plane, 10
  - space, 12
- isometry, 3
- isotropic, 4
- multiplicative form, 21
- nonsingular, 5
- ordered field, *see also* ordering
- ordering, 26
- orthogonal, 6
- Pfister form, 22
  - scaled, 24
- polar form, 3
- quadratic
  - form, 3
  - space, 2
- representation
  - of an element by a form, 4
- restriction homomorphism, 29
- scalar extension, 28
- signature, 27
  - ideal, 27
- similarity factor, 21
- subform, 9
- symmetric bilinear
  - form, 2
  - space, 2
- tensor product
  - of symmetric bilinear spaces, 17
  - of vector spaces, 15
- totally isotropic, 9
- universal, 4
- Witt equivalent, 18
- Witt index, 12
- Witt ring, 19



## REFERENCES

- [BRV10] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli. “Essential dimension, spinor groups, and quadratic forms”. In: *Annals of Mathematics* 171 (2010), pp. 533–544.
- [EKM08] Richard Elman, Nikita Karpenko, and Alexander Merkurjev. *The Algebraic and Geometric Theory of Quadratic Forms*. Vol. 56. Colloquium Publications. American Mathematical Society, 2008.
- [Lam05] Tsit Yuen Lam. *Introduction to quadratic forms over fields*. Vol. 67. Graduate Studies in Mathematics. American Mathematical Society, 2005.
- [Lam83] Tsit Yuen Lam. *Orderings, valuations, and quadratic forms*. CBMS Regional Conference Series in Mathematics. American Mathematical Society, 1983.

CHARLES UNIVERSITY, FACULTY OF MATHEMATICS AND PHYSICS, DEPARTMENT OF ALGEBRA, SOKOLOVSKÁ 83, 18600 PRAHA 8, CZECH REPUBLIC.

*Email address:* nicolas.daans@matfyz.cuni.cz