QUADRATIC FORMS AND CLASS FIELDS II: LECTURE NOTES

NICOLAS DAANS

Contents

Date: Friday 17th May, 2024.

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 $R^\times = R \setminus \{0\}$. We will denote the set of prime numbers by $\mathbb{P}$.

Acknowledgements. The first part of the course (lectures 1–5) 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. I thank Ruben de Preter for helpful feedback on the previous year's lecture notes. 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.

The second part of the course (lectures 6–10) was previously taught by Błażej Żmija, and I have taken inspiration from his classes and lecture notes, as well as exercises, for which he claims inspiration from Gerstein's book [Ger08]. The proof of the Hasse-Minkowski Theorem in particular is inspired in turn by a note of Hatley [Hat09].

For lecture 11, I acknowledge inspiration from Schweighofer's course Real Algebraic Geometry [Sch18, Section 1.6], which I attended at the University of Konstanz in 2017.

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
- $B : V \times V \to K$ is a symmetric and bilinear map, i.e. for all $x, x', y \in V$ and $a \in K$ we have

$$B(x, y) = B(y, x),$$
$$B(x + x', y) = B(x, y) + B(x', y),$$
$$B(ax, y) = aB(x, y).$$

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

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

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
- $q : V \to K$ is a map satisfying the following:
  (1) $\forall a \in K, \forall x \in V : q(ax) = a^2 q(x)$,
  (2) the map
  $$\mathfrak{b}_q : V \times V \to K : (x, y) \mapsto q(x + y) - q(x) - q(y)$$
  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 $I : V \to V'$ 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 $I : V \to V'$ 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*

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

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 $C \in \mathrm{GL}_n(K)$ such that*

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

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

Proof. Exercise. □

1.1.7. *Example.* Suppose $\mathrm{char}(K) \neq 2$. 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

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

is easily seen to be a quadratic form. If $\mathrm{char}(K) \neq 2$, 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 $\mathrm{char}(K) \neq 2$. 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 $V \to K$. 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 $V \to V^* : v \mapsto (w \mapsto B(v, w))$ 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* $\mathrm{char}(K) \neq 2$*, then* (a) *and* (b) *are equivalent.*

In particular, it follows that, if $\mathrm{char}(K) \neq 2$*, 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 $\mathrm{char}(K) \neq 2$ 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 $q(v + w) = q(v) + q(w) + \mathfrak{b}_q(v, w) = q(v)$, so (b) holds. □

If $\mathrm{char}(K) \neq 2$, a nonsingular quadratic form over K is also called *regular* or *nondegenerate*. Note that, if $\mathrm{char}(K) = 2$, 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*

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

Proof. Consider the K-linear maps

$$\varphi_1 : U^\perp \to V^* : v \mapsto (w \mapsto B(v, w))$$
$$\varphi_2 : V^* \to U^* : f \mapsto f|_U.$$

We observe that φ_1 is injective by the nonsingularity of (V, B), that φ_2 is surjective, and that the image of φ_1 is precisely the kernel of φ_2 by definition of $U^\perp$. As such, we compute that

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

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. □

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*

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

Furthermore, consider the natural embeddings $\iota_1 : V_1 \to V : x \mapsto (x, 0)$ and $\iota_2 : V_2 \to V : x \mapsto (0, x)$. 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* $q_1 \perp q_1' \cong q_2 \perp q_2'$.

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 ι is an isomorphism $q_1 \perp q_2 \to q$ 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 ι be the unique K-linear map $V \to V_1 \times V_2$ 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 ι 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 $a_1, \ldots, a_n \in K$. We denote by $\langle a_1, \ldots, a_n \rangle_K$ the quadratic form

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

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

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

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

Proof. Exercise. □

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

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) ⇒ (b) in Proposition 1.1.13 does not hold in general if $\mathrm{char}(K) = 2$.
(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* $\mathrm{char}(K) \neq 2$*. Let* (V, q) *be a quadratic space. Then the map*
$$\overline{q} : V/V^\perp \to K : \overline{v} \mapsto q(v)$$
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 $\overline{v} \neq 0$, i.e. $v \notin V^\perp$. Then there exists $w \in V$ with $0 \neq \mathfrak{b}_q(v,w) = \mathfrak{b}_{\overline{q}}(\overline{v},\overline{w})$, whereby $\overline{v} \notin (V/V^\perp)^\perp$. Hence $(V/V^\perp)^\perp = \{0\}$, and thus $(V/V^\perp, \overline{q})$ is nonsingular. □

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

2.1.3. **Proposition.** *Assume* $\mathrm{char}(K) \neq 2$. *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* $(W, q|_W) \cong (V/V^\perp, \overline{q})$.

Proof. The first isometry is immediate form 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

$$\iota : W \to V/V^\perp : w \mapsto \overline{w}.$$

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

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

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

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 $(W, q|_W) \cong \mathbb{H}_K$. □

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. □

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. □

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 $V \to W \times W^\perp$ 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. □

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

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

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 $W_1, \ldots, W_n$ 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 $Kw_1 \oplus \ldots \oplus Kw_n$ 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 $\dim(U \cap W) \geq n-1$. Hence $(U, q|_U)$ contains a totally isotropic subspace $U \cap W$ of dimension $n-1$. The statement now follows by the induction hypothesis. □

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 W of (V, q) with $V \cap W = \{0\}$. We denote it by $i_W(V, q)$, or simply $i_W(q)$. If $\mathrm{char}(K) \neq 2$, $i_W(V, q)$ is also the maximal possible dimension of a totally isotropic subspace of $V/V^\perp$.

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. □

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'ies, under the assumption that $\mathrm{char}(K) \neq 2$. 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* $\mathrm{char}(K) \neq 2$. *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* $\tau : (V,q) \to (V,q)$ *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

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

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

2.2.2. **Theorem** (Witt Cancellation Theorem)**.** *Assume* $\mathrm{char}(K) \neq 2$. *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 $(V,q) \cong \langle a_1, \ldots, a_n \rangle$ for some $a_1, \ldots, a_n \in K^\times$. By inducting on n, we reduce to the situation $n = 1$. Let $\iota : \langle a \rangle_K \perp (V_1,q_1) \to \langle a \rangle_K \perp (V_2,q_2)$ 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 $\tau : \langle a \rangle_K \perp (V_2,q_2) \to \langle a \rangle_K \perp (V_2,q_2)$ with $\tau(v) = (1,0)$. Thus, $\tau \circ \iota$ gives an isometry $\langle a \rangle_K \perp (V_1,q_1) \to \langle a \rangle_K \perp (V_2,q_2)$ 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 $(V_1,q_1) \to (V_2,q_2)$, as desired. □

2.2.3. **Theorem** (Witt Decomposition Theorem)**.** *Assume* $\operatorname{char}(K) \neq 2$*. 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 $(V_a, q_a) \cong (V_a', q_a')$. □

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

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

Show the following for any $v \in V$ with $q(v) \neq 0$:
   (a) τ_v is an isometry $(V, q) \to (V, q)$,
   (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 $\mathrm{char}(K) \neq 2$:
   (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 $\mathrm{char}(K) \neq 2$ 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

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

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

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

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

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 $V \times W \to V \otimes W : (v, w) \mapsto v \otimes w$ is a bilinear map, and its image generates $V \otimes W$.*

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

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

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 $V \otimes W \to W \otimes V$ such that $v \otimes w \mapsto w \otimes v$ for $v \in V$ and $w \in W$.*
2. *There is a unique K-isomorphism $(U \otimes V) \otimes W \to U \otimes (V \otimes W)$ 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 $(U \times V) \otimes W \to (U \otimes W) \times (V \otimes W)$ such that $((u, v), w) \mapsto ((u \otimes w), (v \otimes w))$ 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*

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

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. □

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

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

This map is bilinear, hence by Proposition 3.1.3 induces a linear map $B_{(v_1,v_2)} : V_1 \otimes V_2 \to K$ 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

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

is also bilinear, hence, again by Proposition 3.1.3, it induces a linear map $\overline{B^*} : V_1 \otimes V_2 \to (V_1 \otimes V_2)^*$ 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. □

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

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

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

$$q_1 \otimes q_2 \cong q_2 \otimes q_1$$
$$(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$$
$$(q_1 \perp q_2) \otimes q_3 \cong (q_1 \otimes q_3) \perp (q_2 \otimes q_3)$$

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. □

3.1.8. **Corollary.** *Assum* $\mathrm{char}(K) \neq 2$. *Let* $m, n \in \mathbb{N}$ *and let* $a_1, \ldots, a_m, b_1, \ldots, b_n \in K$. *We have*

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

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 $a, b \in K$. □

3.1.9. **Corollary.** *Assume* $\mathrm{char}(K) \neq 2$. *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. □

3.1.10. **Corollary.** *Assume* $\mathrm{char}(K) \neq 2$. *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. □

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 consider over a fixed field K, and we assume $\mathrm{char}(K) \neq 2$.

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

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

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*

$$\perp\colon W(K) \times W(K) \to W(K) : ([(V_1, q_1)], [(V_2, q_2)]) \to [(V_1 \times V_2, q_1 \perp q_2)] \text{ and}$$
$$\otimes : W(K) \times W(K) \to W(K) : ([(V_1, q_1)], [(V_2, q_2)]) \to [(V_1 \otimes V_2, q_1 \otimes q_2)]$$

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. □

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 $I(K) = J$. □

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 $\mathrm{char}(K) = 2$, 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.** 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* $\det(M_{\mathfrak{B}_1}(B_1)) \equiv \det(M_{\mathfrak{B}_2}(B_2)) \bmod K^{\times 2}$.

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 $\{e_1, \ldots, e_n\}$. 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 $\mathfrak{B}_2 = \{Ce_1, \ldots, Ce_n\}$. 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 $\det(M_{\mathfrak{B}_2}(B)) = \det(M_{\mathfrak{B}_1}(B)) \det(C)^2 \equiv \det(M_{\mathfrak{B}_2}(B)) \bmod K^{\times 2}$ as desired. □

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

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

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 $a_1, \ldots, a_n \in K^\times$ we have $\det(\langle a_1, \ldots, a_n \rangle_K) \equiv a_1 \cdots a_n \bmod K^{\times 2}$.
(3) $\det(\mathbb{H}_K) \equiv -1 \bmod K^{\times 2}$.

Proof. These can be verified easily via the definition. □

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

4.2.4. **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 $cd \equiv \det(\langle c, d \rangle_K) \equiv \det(\langle a, b \rangle_K) \equiv ab \bmod K^\times$, we must have $d \equiv abc \bmod K^{\times 2}$, whereby $\langle c, d \rangle_K \cong \langle c, abc \rangle_K$. This concludes the proof. □

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 $ad \in D_K(aq) = D_K(q)$. □

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

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 4.2.4 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. □

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

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

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 $\langle\!\langle a_1, \ldots, a_n\rangle\!\rangle_K$ for some $a_1, \ldots, a_n \in K^\times$ 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. □

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 8.2.2).

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 $\operatorname{char}(K) \neq 2$.

(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:
$$\langle\rangle_K \qquad \langle 1\rangle_K \qquad \langle d\rangle_K \qquad \langle 1,-d\rangle_K$$
  (d) If $|K| \equiv 1 \bmod 4$, then $-1 \in K^{\times 2}$ and $WK \cong (\mathbb{Z}/2\mathbb{Z})[T]/(T^2+1)$.
  (e) If $|K| \equiv 3 \bmod 4$, 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 $a, b, c, d \in K^\times$. Show that $\langle a, b\rangle_K \cong \langle c, d\rangle_K$ if and only if $abcd \in K^{\times 2}$ and $\langle\langle -ab, ac\rangle\rangle_K$ is isotropic. In particular, $\langle a, b\rangle_K$ is isotropic if and only if $-ab \in K^{\times 2}$.
(5) Show that for $a, b, c, d \in K^\times$ we have $\langle\langle a, b\rangle\rangle_K \cong \langle\langle c, d\rangle\rangle_K$ if and only if there exists $e \in K^\times$ with
$$\langle\langle a, b\rangle\rangle_K \cong \langle\langle a, e\rangle\rangle_K \cong \langle\langle c, e\rangle\rangle_K \cong \langle\langle c, d\rangle\rangle_K.$$
(6) Let q be a 4-dimensional nonsingular quadratic form over K with $1 \in D_K(q)$ and $\det(q) \equiv 1 \bmod K^{\times 2}$. Show that q is a Pfister form.
(7) Let q be a universal 3-dimensional quadratic form over K. Show that q is isotropic.
(8) Show that $D_{\mathbb{Q}}(\langle 1, 1\rangle_{\mathbb{Q}})$ is a subgroup of $\mathbb{Q}^\times$. Is the same true for $D_{\mathbb{Q}}(\langle 1, 1, 1\rangle_{\mathbb{Q}})$?
(9) Give an example of an anisotropic quadratic form which is multiplicative but not a Pfister form.
(10) 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 $\mathrm{char}(K) \neq 2$ 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^nK the ideal of WK generated by products of n elements in IK. By convention, we set $I^0K = WK$. We obtain a natural filtration

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

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

5.1.1. **Proposition.** *For $n \geq 1$, the ideal I^nK 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^nK is generated by n-fold Pfister forms, as desired. □

A quadratic form over K which is isometric to $a\pi$ for a Pfister form π 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^nK.

Our first goal will be to understand the quotient IK/I^2K.

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 2-fold 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 suffice 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. □

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

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

Observe that for a natural number n we have

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

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

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

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

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

is a well-defined surjective group homomorphism with kernel I^2K. In particular, $IK/I^2K \cong K^\times/K^{\times 2}$.

Proof. For the first part, we need to check that if $(V, q) \equiv (V', q')$, then $\mathrm{d}(V, q) = \mathrm{d}(V', q')$. 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

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

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 $\mathrm{d}(\langle 1, -a\rangle_K) \equiv a \bmod K^{\times 2}$ for $a \in K^\times$.

We now compute the kernel of the morphism. One computes that, for any $a, b \in K^\times$, we have

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

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 $I^2K \subseteq \mathrm{Ker}(\mathrm{d})$.

For the converse implication, consider $\zeta \in \mathrm{Ker}(\mathrm{d})$. By Lemma 5.1.2 we have $\zeta \equiv [(V, q)] \bmod I^2K$ where $\dim(V) = 2$. Since $I^2K \subseteq \mathrm{Ker}(\mathrm{d})$ by the previous paragraph, we conclude that $\mathrm{d}(V, q) = \mathrm{d}(\zeta) \equiv 1 \bmod K^{\times 2}$. 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. □

5.1.5. **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 $\pi_1, \ldots, \pi_m$ such that $[(V, q)] = \sum_{i=1}^m [\pi_i]$.*

Proof. If $m = 0$ then, as in the proof of Proposition 5.1.4, 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. □

5.1.6. **Question.** *Let $n, d \in \mathbb{N}^+$. Does there exist a natural number m such that every d-dimensional quadratic space (V, q) with $[(V, q)] \in I^n K$ 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 5.1.5. 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.

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

(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. □

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

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 $[(V, q)] \notin I^n K$ by Theorem 5.1.7. □

5.2. **Symbols in $I^n K/I^{n+1}K$.** Assume throughout that K is a field with $\mathrm{char}(K) \neq 2$. We want to give a description of the quotients $I^n K/I^{n+1}K$ through *generators and relations*. We know from Proposition 5.1.1 that the group $I^n K$ is generated by the classes of n-fold Pfister forms over K, hence the same holds for $I^{n+1}K$. We also know that $WK/IK \cong \mathbb{Z}/2\mathbb{Z}$, and that $IK/I^2K \cong K^\times/K^{\times 2}$ via the signed discriminant map (see Proposition 5.1.4); its inverse is the map $K^\times/K^{\times 2} \to IK/I^2K$ mapping the class of an element $a \in K^\times$ to the quadratic form $\langle 1, -a\rangle_K$. We now seek to generalise this to higher powers of the fundamental ideal. The presentation in this subsection gives an ad hoc introduction to a branch of mathematics closely related to quadratic form theory, called *Algebraic K-Theory*, or sometimes *Milnor's K-Theory*.

5.2.1. **Definition.** For $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in K^\times$, we denote by $\{a_1, \ldots, a_n\}_K$ the equivalence class of $\langle\!\langle a_1, \ldots, a_n\rangle\!\rangle_K$ in $I^n K/I^{n+1}K$. We call such elements $\{a_1, \ldots, a_n\}_K \in I^n K/I^{n+1}K$ *symbols*.

We have a map $(K^\times)^n \to I^n K/I^{n+1}K : (a_1, \ldots, a_n) \mapsto \{a_1, \ldots, a_n\}_K$. Let us phrase some basic properties of this map.

5.2.2. **Proposition.** *We have the following for $a_1, \dots, a_n \in K^\times$,*

(1) (multilinearity) For $i \in \{1, \dots, n\}$ and $a_i' \in K^\times$

$$\{a_1, \dots, a_i a_i', \dots a_n\}_K = \{a_1, \dots, a_i, \dots, a_n\}_K + \{a_1, \dots, a_i', \dots, a_n\}_K,$$

(2) (2-torsion)

$$2 \times \{a_1, \dots, a_n\}_K = \{a_1, \dots, a_n\}_K + \{a_1, \dots, a_n\}_K = 0,$$

(3) (Steinberg relation) If $i \in \{1, \dots, n-1\}$ is such that $a_i + a_{i+1} = 1$, then $\{a_1, \dots, a_n\}_K = 0$.

Proof. (1): Consider the $(n-1)$-fold Pfister form $q = \langle\langle a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n\rangle\rangle$. We need to show that $[q \otimes \langle\langle a_i\rangle\rangle_K] + [q \otimes \langle\langle a_i'\rangle\rangle_K] \equiv [q \otimes \langle\langle a_i a_i'\rangle\rangle_K] \bmod I^{n+1}K$. We compute that

$$\begin{aligned} & q \otimes \langle\langle a_i\rangle\rangle_K \perp q \otimes \langle\langle a_i'\rangle\rangle_K \perp -q \otimes \langle\langle a_i a_i'\rangle\rangle_K \\ \cong\ & (q \perp -a_i q) \perp (q \perp -a_i' q) \perp -(q \perp a_i a_i' q) \\ \cong\ & (q \perp -a_i q \perp -a_i' q \perp a_i a_i' q) \perp (q \perp -q) \\ \cong\ & q \otimes \langle\langle a_i, a_{i+1}\rangle\rangle_K \perp q \otimes \langle\langle -1\rangle\rangle_K. \end{aligned}$$

Since $q \otimes \langle\langle a_i, a_{i+1}\rangle\rangle_K$ is an $(n+1)$-fold Pfister form and $q \otimes \langle\langle -1\rangle\rangle$ is hyperbolic (as $\langle\langle 1\rangle\rangle_K \cong \mathbb{H}_K$, see also Corollary 3.1.10) we obtain that

$$[q \otimes \langle\langle a_i\rangle\rangle_K] + [q \otimes \langle\langle a_i'\rangle\rangle_K] - [q \otimes \langle\langle a_i a_i'\rangle\rangle_K] = [q \otimes \langle\langle a_i, a_{i+1}\rangle\rangle_K \perp q \otimes \langle\langle -1\rangle\rangle_K] \in I^{n+1}K.$$

From this, the desired statement follows.

(2) Set $q = \langle\langle a_1, \dots, a_n\rangle\rangle_K$. We have $[q] + [q] = [q \perp q] = [q \otimes \langle\langle -1\rangle\rangle] \in I^{n+1}K$. From this the statement follows.

(3) It suffices to show that $\langle\langle a_1, \dots, a_n\rangle\rangle_K$ is hyperbolic whenever $a_i + a_{i+1} = 1$. In view of Theorem 4.3.6 it even suffices to show that $\langle\langle a_1, \dots, a_n\rangle\rangle_K$ is isotropic. This follows because $\langle\langle a_1, \dots, a_n\rangle\rangle_K$ contains as a subform $\langle 1, -a_i, -a_{i+1}\rangle_K$, which is isotropic since $1^2 - a_i 1^2 - a_{i+1} 1^1 = 0$. □

The following properties can be derived from the properties of Pfister forms and the definition of $I^n K / I^{n+1} K$, but, more interestingly, they can be proved using only only the three properties from Proposition 5.2.2 as axioms.

5.2.3. **Corollary.** *We have the following for $a_1, \dots, a_n \in K^\times$:*

(1) If $i \in \{1, \dots, n-1\}$ is such that $a_i + a_{i+1} = 0$, then $\{a_1, \dots, a_n\}_K = 0$.

(2) (invariance under permutation) For $i \in \{1, \dots, n-1\}$,

$$\{a_1, \dots, a_i, a_{i+1}, \dots, a_n\}_K = \{a_1, \dots, a_{i+1}, a_i, \dots, a_n\}_K,$$

(3) For $d \in K^\times$, $\{a_1 d^2, a_2, \dots, a_n\}_K = \{a_1, a_2, \dots, a_n\}_K$,

(4) $\{a_1, \dots, a_n\}_K = \{a_1 + a_2, -a_1 a_2, a_3, \dots, a_n\}_K$, provided that $a_2 \neq -a_1$.

Proof. Exercise. □

In an influential paper from 1970 [Mil70], John Milnor conjectured that the three properties from Proposition 5.2.2 can be used to completely axiomatise the relations between the elements $\{a_1, \dots, a_n\}_K$. He was able to establish several special cases (small values of n and specific fields), but the general case was only solved more than thirty years later by the work of Orlov, Vishik, and Voevodsky [OVV07]. Below is a version of their result, stated in the form of a universal property. The proof is far beyond the scope of this course, and we will not make use of this result in the course either.

5.2.4. **Theorem** (Orlov-Vishik-Voevodsky)**.** *Let $n \in \mathbb{N}$, G an abelian group, and $\Phi : (K^\times)^n \to G$ a map satisfying the properties from Proposition 5.2.2, i.e. for $a_1, \dots, a_n \in K^\times$, $i \in \{1, \dots, n\}$, $a_i' \in K^\times$,*

- $\Phi(a_1, \dots, a_i a_i', \dots, a_n) = \Phi(a_1, \dots, a_i, \dots, a_n) + \Phi(a_1, \dots, a_i', \dots, a_n)$,
- $2 \times \Phi(a_1, \dots, a_n) = 0$,
- *if $a_i + a_{i+1} = 1$, then $\Phi(a_1, \dots, a_n) = 0$.*

Then there exists a unique group homomorphism $\tilde{\Phi} : I^n K / I^{n+1} K \to G$ such that $\Phi(a_1, \dots, a_n) = \tilde{\Phi}(\{a_1, \dots, a_n\}_K)$ for all $a_1, \dots, a_n \in K^\times$.

Finally, we mention the following consequence of the Arason-Pfister Hauptsatz, which can be useful when classifying quadratic forms over a field.

5.2.5. **Proposition.** *For $n \in \mathbb{N}$ and $a_1, \dots, a_n, b_1, \dots, b_n \in K^\times$ we have that*

$$\{a_1, \dots, a_n\}_K = \{b_1, \dots, b_n\}_K \quad \text{if and only if} \quad \langle\langle a_1, \dots, a_n \rangle\rangle_K \cong \langle\langle a_1, \dots, a_n \rangle\rangle_K.$$

In particular, we have $\{a_1, \dots, a_n\}_K = 0$ if and only if $\langle\langle a_1, \dots, a_n \rangle\rangle_K$ is hyperbolic.

Proof. By definition we have $\{a_1, \dots, a_n\}_K = \{b_1, \dots, b_n\}_K$ if and only if $[\langle\langle a_1, \dots, a_n \rangle\rangle_K] \equiv [\langle\langle b_1, \dots, b_n \rangle\rangle_K] \bmod I^{n+1}K$. It is thus clear that if $\langle\langle a_1, \dots, a_n \rangle\rangle_K \cong \langle\langle b_1, \dots, b_n \rangle\rangle_K$, then $\{a_1, \dots, a_n\}_K = \{b_1, \dots, b_n\}_K$.

Conversely, suppose $[\langle\langle a_1, \dots, a_n \rangle\rangle_K] \equiv [\langle\langle b_1, \dots, b_n \rangle\rangle_K] \bmod I^{n+1}K$. Then the class of $\langle\langle a_1, \dots, a_n \rangle\rangle_K \perp -\langle\langle b_1, \dots, b_n \rangle\rangle_K$ lies in $I^{n+1}K$ and has dimension 2^{n+1}, so by Theorem 5.1.7 it must be isometric to a scaled $(n+1)$-fold Pfister form. In particular, by Theorem 4.3.6 it must be either anisotropic or hyperbolic. It is not anisotropic (since $1 \in D_K(\langle\langle a_1, \dots, a_n \rangle\rangle_K) \cap D_K(\langle\langle b_1, \dots, b_n \rangle\rangle_K)$, so it must be hyperbolic. In other words, $[\langle\langle a_1, \dots, a_n \rangle\rangle_K \perp -\langle\langle b_1, \dots, b_n \rangle\rangle_K] = 0$ in WK, whereby $[\langle\langle a_1, \dots, a_n \rangle\rangle_K] = [\langle\langle b_1, \dots, b_n \rangle\rangle_K]$, and since both forms have the same dimension, we conclude that indeed $\langle\langle a_1, \dots, a_n \rangle\rangle_K \cong \langle\langle b_1, \dots, b_n \rangle\rangle_K$.

The "in particular" part follows by taking $\langle\langle b_1, \dots, b_n \rangle\rangle$ hyperbolic (e.g. setting $b_1 = 1$). □

5.3. **Exercises.**

(1) Show the following for a field K with $\operatorname{char}(K) \neq 2$:

(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.

(2) Give a proof of Corollary 5.2.3 using only the computation rules from Proposition 5.2.2.

6. Lecture 6

6.1. **The p-adic numbers.** To see that a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ does not have an integral zero, one can often use modular arithmetic: if f does not have a zero over $\mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{N}$, then it can certainly not have a zero over $\mathbb{Z}$. For example, the equation $X^3 + 7XY = 16$ cannot have an integral solution, because modulo 7 it reduces to $X^3 = 2$, which has no solution in the ring $\mathbb{Z}/7\mathbb{Z}$.

Similarly, modular arithmetic can be used to show that an equation does not have a rational solution. The most famous example is the equation $X^2 = 2$, which cannot have a solution in $\mathbb{Q}$ by considerations modulo 4, after writing out a hypothetical solution in $\mathbb{Q}$ as a fraction of two coprime integers.

In this section we shall introduce, for each prime number p, a commutative ring $\mathbb{Z}_p$, called the *ring of p-adic integers*. It is an object which shall capture, in a certain sense, all information about solvability of polynomial equations modulo powers of p.

6.1.1. **Proposition.** *Let $p \in \mathbb{P}$. Consider the subset of the product ring $A_p = \prod_{n\in\mathbb{N}^+} \mathbb{Z}/p^n\mathbb{Z}$ given as*

$$\mathbb{Z}_p = \{(x_n + p^n\mathbb{Z}) \in A_p \mid (x_n)_n \in \mathbb{Z}^{\mathbb{N}} \text{ s.t. } x_n \equiv x_{n+1} \bmod p^n \text{ for all } n \in \mathbb{N}^+\}.$$

We have the following:

(i) $\mathbb{Z}_p$ is a subring of A_p of characteristic 0.
(ii) $\mathbb{Z}_p$ is an integral domain.
(iii) The ideal $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$, and we have for $m \in \mathbb{N}^+$ that

$$p^m\mathbb{Z}_p = \{(x_n + p^n\mathbb{Z})_n \in \mathbb{Z}_p \mid x_m = 0\}.$$

(iv) For all $n \in \mathbb{N}$, $p^n\mathbb{Z}_p \cap \mathbb{Z} = p^n\mathbb{Z}$, and the natural map $\mathbb{Z} \to \mathbb{Z}_p$ induces an isomorphism $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$.

Proof. Exercise. □

6.1.2. **Definition.** We call the ring $\mathbb{Z}_p$ constucted in Proposition 6.1.1 the *ring of p-adic integers*. We denote by $\mathbb{Q}_p$ its field of fractions, and call it the *field of p-adic numbers*.

It follows from Proposition 6.1.1 that a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ which has a root in $\mathbb{Z}_p$ will have a root in $\mathbb{Z}/p^m\mathbb{Z}$ for all $m \in \mathbb{N}$. Assuming the Axiom of Choice, the converse statement also holds, see Exercise (9). We will not need

this converse statement in full generality; instead, let us phrase now a powerful tool to establish explicitly solvability of equations in $\mathbb{Z}_p$; it can be seen as a p-adic version of Newton's method from numerical analysis.

For a commutative ring R and a univariate polynomial $f \in R[X]$, we denote by $f' \in R[X]$ its formal derivative, i.e. if $f = \sum_{i=0}^{n} a_i X^i$ for $n \in \mathbb{N}, a_i \in R$, then $f' = \sum_{i=0}^{n-1} (i+1) a_{i+1} X^i$.

6.1.3. **Proposition** (Hensel's Lemma)**.** *Let $f \in \mathbb{Z}_p[X]$ and let $x_1 \in \mathbb{Z}$ be such that*

$$f(x_1) \equiv 0 \not\equiv f'(x_1) \bmod p,$$

in other words, $\overline{x_1}$ is a simple root of $\overline{f}$ in $\mathbb{Z}/p\mathbb{Z}$. Then there exists $x \in \mathbb{Z}_p$ with $x - x_1 \in p\mathbb{Z}_p$ and $f(x) = 0$.

Proof. It suffices to construct recursively for $n \in \mathbb{N}^+$ an element $x_{n+1} \in \mathbb{Z}$ with

$$x_{n+1} \equiv x_n \bmod p^n \text{ and } f(x_{n+1}) \equiv 0 \bmod p^{n+1}.$$

Indeed, we may then set $x = (x_n + p^n\mathbb{Z})_n$; this is an element of $\mathbb{Z}_p$ by construction, and we further obtain $f(x) = (f(x_n) + p^n\mathbb{Z})_n = 0$ as desired.

So let $n \in \mathbb{N}^+$ and assume x_n is already given. We have in particular that

$$x_n \equiv x_1 \bmod p, f(x_n) \equiv 0 \bmod p^n \text{ and } f'(x_n) \equiv f'(x_1) \not\equiv 0 \bmod p.$$

For $e \in \mathbb{Z}$ we have (by a formal version of "Taylor's Theorem", see Exercise (3)):

$$f(x_n + ep^n) \equiv f(x_n) + f'(x_n) ep^n \bmod p^{n+1}.$$

Since by assumption p^n divides $f(x_n)$ and $f'(x_n) \not\equiv 0 \bmod p$, there exists some $e \in \mathbb{Z}$ with

$$p^{-n} f(x_n) + f'(x_n) e \equiv 0 \bmod p.$$

Thus, it suffices to set, for this value of e, $x_{n+1} = x_n + ep^n$. □

We obtain more properties of the ring $\mathbb{Z}_p$ and the field $\mathbb{Q}_p$.

6.1.4. **Proposition.** *Let $p \in \mathbb{P}$. We have the following.*

(i) $\mathbb{Z}_p$ has a unique maximal ideal, namely $p\mathbb{Z}_p$. In particular, $\mathbb{Z}_p^\times = \mathbb{Z} \setminus p\mathbb{Z}_p$.
(ii) Every nonzero ideal of $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$ for a unique $n \in \mathbb{N}$; in particular, $\mathbb{Z}_p$ is a principal ideal domain.
(iii) Every nonzero element of $\mathbb{Q}_p$ has a unique presentation of the form $p^k u$ for $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$.

Proof. (i): We already know from Proposition 6.1.1 that $p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$. Take $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ and consider the polynomial $f(X) = Xx - 1$. Since $x \notin p\mathbb{Z}_p$, its residue $\overline{x} \in \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ is invertible, so there exists $y_1 \in \mathbb{Z}$ with $f(y) = yx - 1 \equiv 0 \bmod p$. On the other hand, $f'(y_1) = x \not\equiv 0 \bmod p$. We conclude by Proposition 6.1.3 that there exists $y \in \mathbb{Z}_p$ with $0 = f(t) = yx - 1$, i.e. $y = x^{-1}$. This shows that $\mathbb{Z}_p \setminus p\mathbb{Z}_p = \mathbb{Z}_p^\times$, so $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, so $\mathbb{Z}_p$ is a local ring.

(ii) and (iii): It suffices to show that every non-zero element of $\mathbb{Z}_p$ has a unique presentation as $p^k u$ for $k \in \mathbb{N}$ and $u \in \mathbb{Z}_p^\times$, then both statements follow easily. The uniqueness is clear, as $p\mathbb{Z}_p$ is a prime ideal. The existence is clear from (i) and the fact that $\bigcap_{n\in\mathbb{N}} p^n\mathbb{Z}_p = \{0\}$ by Proposition 6.1.1. □

According to part (iii) of Proposition 6.1.4, we can write an arbitrary non-zero element $x \in \mathbb{Q}_p$ as $p^k u$ for $k \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. One sees that then $k = \max\{l \in \mathbb{Z} \mid p^{-l}u \in \mathbb{Z}_p\}$. We can thus define a map

$$v_p : \mathbb{Q}_p^\times \to \mathbb{Z} : x \mapsto \max\{l \in \mathbb{Z} \mid p^{-l}u \in \mathbb{Z}_p\}.$$

We extend this to a map $\mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ by the convention $v_p(0) = \infty$, and call v_p the *p-adic valuation* on $\mathbb{Q}_p$. Taking the convention that $a + \infty = \infty$ for all $a \in \mathbb{Z} \cup \{\infty\}$ and that $\infty > a$ for all $a \in \mathbb{Z}$, we obtain the following.

6.1.5. **Proposition.** *Let $p \in \mathbb{P}$. We have*

- *$v_p(xy) = v_p(x) + v_p(y)$ for all $x, y \in \mathbb{Q}_p$,*
- *$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$, and equality holds when $v_p(x) \neq v_p(y)$,*
- *$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$,*
- *for $x \in \mathbb{Z}$ we have $v_p(x) = \max\{l \in \mathbb{N} \mid x \in p^l\mathbb{Z}\}$. In particular, $\{z \in \mathbb{Q} \mid v_p(z) \geq 0\} = \mathbb{Z}_p \cap \mathbb{Q} = \{\frac{x}{y} \mid x \in \mathbb{Z}, y \in \mathbb{Z} \setminus p\mathbb{Z}\}$.*
- *For $x \in \mathbb{Q}$, the set $\{q \in \mathbb{P} \mid v_q(x) \neq 0\}$ is finite.*

Proof. Exercise. □

One should think of v_p as a map which measures how divisible an element is by p.

6.1.6. *Example.* 2 is not a square in $\mathbb{Q}$, here is a proof: suppose there would exist $x \in \mathbb{Q}$ with $x^2 = 2$. Then $1 = v_2(2) = v_2(x^2) = 2v_2(x) \in 2\mathbb{Z}$. Contradiction.

6.2. **The p-adic topology.** We now present another way to think about the field of p-adic numbers $\mathbb{Q}_p$, which reveals an analogy with the field of real numbers $\mathbb{R}$.

One way to show that a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ does not have a zero in $\mathbb{Q}^n$, is by showing that it does not have a zero in $\mathbb{R}^n$. Since (by definition) real numbers can be approximated arbitrarily by rational numbers (in other words, $\mathbb{Q}$ is dense in $\mathbb{R}$), and by the completeness of $\mathbb{R}$, it follows that f has a root in $\mathbb{R}^n$ if and only if for every $m \in \mathbb{N}$ there exists $x_m \in \mathbb{Q}^n$ such that $|f(x_m)| < 1/m$.

In fact, while there are many ways to construct the field $\mathbb{R}$, it is completely characterised by the conditions that it is an ordered field, $\mathbb{Q}$ is dense in $\mathbb{R}$, and $\mathbb{R}$ is complete with respect to the metric induced by the absolute value, i.e. every Cauchy sequence has a limit.

We now define a different metric on the field of rational numbers $\mathbb{Q}$ than the standard metric induced by the absolute value.

6.2.1. **Proposition.** *Let $p \in \mathbb{P}$. Consider the map*

$$d_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{R}_{\geq 0} : (x, y) \mapsto p^{-v_p(x-y)}$$

where we take the convention $p^{-\infty} = 0$. Then d_p defines a metric on $\mathbb{Q}_p$, i.e. it satisfies for $x, y, z \in \mathbb{Q}_p$

(i) $d_p(x, y) = 0$ *if and only if* $x = y$,
(ii) $d_p(x, y) = d_p(y, x)$,
(iii) $d_p(x, z) \leq \max\{d(x, y), d(y, z)\} \leq d(x, y) + d(y, z)$.

Proof. This follows immediately from Proposition 6.1.5. □

6.2.2. **Definition.** The map d_p defined in Proposition 6.2.1 is called the *p-adic metric*. The topology it induces on $\mathbb{Q}_p$ is called the *p-adic topology*. This map also induces a metric (and thus a topology) on $\mathbb{Z}_p$, $\mathbb{Q}$, and $\mathbb{Z}$, which we will also call the p-adic metric (respectively topology). The first inequality in (iii) is called the *strong triangle inequality*

6.2.3. *Example.* Consider the p-adic metric d_p on $\mathbb{Q}_p$. The ball of radius 1 around the origin is precisely $\mathbb{Z}_p$.

As for any metric space, we can talk about convergence of sequences, Cauchy sequences, open and closed subsets, dense subsets, et cetera, for the p-adic metric. The intuition should be that elements are close to eachother when their difference has high p-adic value, i.e. is divisible in $\mathbb{Z}_p$ by a high power of p. For example, one verifies that:

- given a sequence $(x_n)_n$ in $\mathbb{Q}_p$ and $x \in \mathbb{Q}_p$, we have that $(x_n)_n$ converges to x (or $\lim_{n\to\infty} x_n = x$) if for all $m \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$ one has $v_p(x - x_n) > m$.
- given a sequence $(x_n)_n$ in $\mathbb{Q}_p$, we have that $(x_n)_n$ is a Cauchy sequence if for all $m \in \mathbb{N}$ there exists $n_0 \in \mathbb{N}$ such that for all $n_1, n_2 \geq n_0$ one has $v_p(x_{n_1} - x_{n_2}) > m$.

6.2.4. **Proposition.** *The p-adic topology is a field topology, i.e. $\{x\}$ is a closed set for any $x \in \mathbb{Q}_p$, and the maps*

$$\mathbb{Q}_p \times \mathbb{Q}_p \to \mathbb{Q}_p : (x, y) \mapsto x + y$$
$$\mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \to \mathbb{Q}_p^\times : (x, y) \mapsto x \cdot y$$

are continuous.

Proof. Exercise. □

We shall show that $\mathbb{Q}_p$ is, in fact, the completion of $\mathbb{Q}$ with respect to the p-adic topology.

6.2.5. **Theorem.** *Let $p \in \mathbb{P}$. Then $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are complete with respect to the p-adic metric, i.e. every Cauchy sequence in $\mathbb{Z}_p$ (respectively $\mathbb{Q}_p$) converges to an element of $\mathbb{Z}_p$ (respectively $\mathbb{Q}_p$).*

Proof. Let $(x_n)_n$ be a Cauchy sequence in $\mathbb{Z}_p$. To show that $(x_n)_n$ converges, it suffices to show that there is a convergent subsequence. By removing intermediate

terms, we may thus assume without loss of generality that, for all $n \in \mathbb{N}$ and for all $n_1, n_2 \geq n$, $v_p(x_{n_1} - x_{n_2}) \geq n$. Write $x_n = (x_n^{(m)} + p^m\mathbb{Z})_m$ for some $x_n^{(m)} \in \mathbb{Z}$. Define $x = (x_m^{(m)} + p^m\mathbb{Z})_m$. We claim that $x \in \mathbb{Z}_p$ and $x = \lim_{n\to\infty} x_n$.

Consider $n \in \mathbb{N}^+$. For $m \geq n$ we have that $v_p(x_n - x_m) \geq n$, which implies that $x_n^{(m)} \equiv x_m^{(m)} \bmod p^n$. Applying this to $m = n+1$ in particular we obtain $x_n^{(n+1)} \equiv x_n^{(n+1)} \equiv x_{n+1}^{(n+1)} \bmod p^n$; having this for general n shows $x \in \mathbb{Z}_p$. Furthermore, we see that $v_p(x_n - x) \geq n$ by construction. This implies $\lim_{n\to\infty} x_n = x$ as desired. We have shown the completeness of $\mathbb{Z}_p$.

The completeness of $\mathbb{Q}_p$ then follows from this: consider a Cauchy sequence $(x_n)_n$ in $\mathbb{Z}_p$. There must exist some $k \in \mathbb{N}$ such that $v_p(x_n) \geq -k$ for all $n \in \mathbb{N}$. But then $(p^k x_n)_n$ is a Cauchy sequence in $\mathbb{Z}_p$, which by the previous part converges to some $x' \in \mathbb{Z}_p$, but then $(x_n)_n$ converges to $p^{-k}x'$. □

We give another presentation of p-adic numbers using infinite series. Just like with the real numbers, when $(x_n)_n$ is a sequence of p-adic numbers, we denote by $\sum_{n=0}^{+\infty} x_n$ the element $\lim_{n\to+\infty} \sum_{i=0}^{n} x_i$, *assuming that this limit converges.*

6.2.6. **Proposition.** *Let $p \in \mathbb{P}$.*

(i) For any sequence $(a_n)_n$ in $\mathbb{Z}_p$, the sum $\sum_{n=0}^{+\infty} a_n p^n$ converges in $\mathbb{Z}_p$.
(ii) For any $x \in \mathbb{Z}_p$, there exists a unique sequence $(a_n)_n$ with $a_n \in \{0, 1, \ldots, p-1\}$ such that $x = \sum_{n=0}^{+\infty} a_n p^n$.
(iii) For any $x \in \mathbb{Q}_p$, there exists a unique sequence $(a_n)_{n=v_p(x)}^{+\infty}$ with $a_n \in \{0, 1, \ldots, p-1\}$ such that $x = \sum_{n=v_p(x)}^{+\infty} a_n p^n$.

Proof. (i) follows immediately from the completeness of $\mathbb{Z}_p$ (Theorem 6.2.5).

(ii): Write $x = (x_n + p^n\mathbb{Z})_n$ for $x_n \in \mathbb{Z}$. Suppose that $x = \sum_{n=0}^{+\infty} a_n p^n$ for some $a_n \in \{0, \ldots, p-1\}$. We shall determine what values the a_n must necessarily have, which shall establish the uniqueness, and then simultaneously verify that one can always choose the a_n as such, which establishes existence in view of (i).

Since $x \equiv \sum_{n=0}^{+\infty} a_n p^n \equiv a_0 \bmod p$, we must have $a_0 \equiv x_1 \bmod p$. We thus choose a_0 as the unique element in $\{0, \ldots, p-1\}$ with this property. Now assume that $a_0, \ldots, a_{n-1}$ have been chosen such that $\sum_{i=0}^{n-1} a_i p^i \equiv x_n \bmod p^n$. Since $x_{n+1} \equiv x_n \bmod p^n$, we have that $x_{n+1} = \sum_{i=0}^{n-1} a_i p^i + p^n b$ for some $b \in \mathbb{Z}$. There is a unique $a_n \in \{0, \ldots, p-1\}$ such that $a_n \equiv b \bmod p$, and then we have by construction $x_{n+1} \equiv \sum_{i=0}^{n} a_i p^i \bmod p^{n+1}$.

(iii) follows from (ii) and Proposition 6.1.4. □

For $x \in \mathbb{Z}_p$, its unique presentation as $\sum_{n=0}^{+\infty} a_n p^n$ for $a_n \in \{0, 1, \ldots, p-1\}$ is called its *p-adic series expansion* or simply *p-adic expansion.*

6.2.7. *Example.* We find the 7-adic expansion of $\frac{142}{9}$.

Note that $\frac{142}{9} = 16 - \frac{2}{9}$. We can easily find a 7-adic expansion of 16: we have $16 = 2 \cdot 7^0 + 2 \cdot 7^1$. To find a 7-adic expansion of $\frac{1}{9}$, we shall use (see (5) below)

that, for any $k \in \mathbb{N}^+$, we have in $\mathbb{Z}_7$ that

$$\frac{1}{1-7^k} = \sum_{i=0}^{+\infty} 7^{ik}.$$

Since 9 and 7 are coprime, there must exist $k \in \mathbb{N}^+$ such that $9 \mid (7^k - 1)$; one verifies that $k = 3$ works. We compute that

$$\frac{1}{9} = \frac{1}{9} \cdot \frac{1-7^3}{1-7^3} = \frac{-38}{1-7^3} = -38 \sum_{n=0}^{+\infty} 7^{3n}$$

and thus

$$\begin{aligned}
\frac{142}{9} &= 16 - \frac{2}{9} = 2 \cdot 7^0 + 2 \cdot 7^1 + 76 \sum_{n=0}^{+\infty} 7^{3n} \\
&= 2 \cdot 7^0 + 2 \cdot 7^1 + (6 \cdot 7^0 + 3 \cdot 7^1 + 1 \cdot 7^2) \sum_{n=0}^{+\infty} 7^{3n} \\
&= 2 \cdot 7^0 + 2 \cdot 7^1 + 6 \cdot 7^0 + 6 \sum_{n=1}^{+\infty} 7^{3n} + 3 \cdot 7^1 + 3 \sum_{n=1}^{+\infty} 7^{3n+1} + \sum_{n=0}^{+\infty} 7^{3n+2} \\
&= 1 \cdot 7^0 + 6 \cdot 7^1 + \sum_{n=0}^{+\infty} (7^{3n+2} + 6 \cdot 7^{3n+3} + 3 \cdot 7^{3n+4}).
\end{aligned}$$

We see that the 7-adic representation of $\frac{142}{9}$ becomes periodic after finitely many terms. This is no coincide, see Exercise (6) below.

6.2.8. **Corollary.** *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ with respect to the p-adic topology.*

Proof. This is immediate from parts (ii) and (iii) of Proposition 6.2.6. □

Just like for the reals, one can show that $\mathbb{Q}_p$ is uniquely determined up to canonical isomorphism by the property that it is a field with a complete metric extending the p-adic metric on $\mathbb{Q}$ and in which $\mathbb{Q}$ is dense; see e.g. [EP05, Theorem 2.4.3].

6.3. **Exercises.** Let always $p \in \mathbb{P}$.

(1) Prove Proposition 6.1.1, Proposition 6.1.5, and Proposition 6.2.4 and fill in the missing details in the proof of Proposition 6.1.4.
(2) Consider the construction of $\mathbb{Z}_p$ given in Proposition 6.1.1, but instead of considering $p \in \mathbb{P}$, we do the same construction for $p = 10$. Show, by giving explicit zero divisors, that $\mathbb{Z}_{10}$ is not an integral domain.

(3) Let R be a commutative ring, $f \in R[X]$ a polynomial of degree at most n, $a \in R$. Show that

$$f(X) = f(a) + \sum_{i=1}^{n} \frac{f^{(i)}(a)(X-a)^i}{i!}$$

where $f^{(i)}$ denotes the ith formal derivative of f (i.e. $f^{(i+1)} = (f^{(i)})'$).

(4) Consider the polynomial $f(X) = 10X^4 + 3X^3 - 3X^2 + 6$. Determine whether f has a root in $\mathbb{Z}_2$, and whether f has a root in $\mathbb{Z}_3$.

(5) Show that, for $k \in \mathbb{N}^+$, one has $\sum_{i=0}^{+\infty} p^{ki} = (1-p^k)^{-1}$ in $\mathbb{Z}_p$. (*Hint:* use the fact that $\lim_{n\to\infty} p^n = 0$ in $\mathbb{Z}_p$.)

(6) Let $x \in \mathbb{Q}_p$. Show that $x \in \mathbb{Q}$ if and only if the p-adic expansion of x is eventually periodic, i.e. writing $x = \sum_{n=k}^{+\infty} a_n p^n$ for some $k \in \mathbb{Z}$, $a_n \in \{0, 1, \ldots, p-1\}$, there exists $n_0, m \in \mathbb{N}^+$ such that for all $n \geq n_0$, $a_{n+m} = a_n$.

(7) Given $x = \sum_{n=0}^{+\infty} a_n p^n$ for certain $a_n \in \{0, \ldots, p-1\}$. Find a formula for the p-adic expansion of $-x$.

(8) Show that the p-adic topology on $\mathbb{Z}_p$ is compact.

(9) Let $n \in \mathbb{N}$ and $f \in \mathbb{Z}_p[X_1, \ldots, X_n]$. Assume that, for all $m \in \mathbb{N}$, there exists $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ with $f(x_1, \ldots, x_n) \equiv 0 \bmod p^m$. Use the Axiom of Choice to infer that there exists $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ with $f(x_1, \ldots, x_n) = 0$.

(10) Show that $\mathbb{Z}_p$ is uncountable.

7. Lecture 7

7.1. **Squares in p-adic fields.** The goal of this lecture and the next will be to completely classify quadratic forms over $\mathbb{Q}_p$ for each $p \in \mathbb{P}$. We start by studying when an element of $\mathbb{Q}_p$ is a square. In view of Proposition 5.1.4, this will allow us to compute $I\mathbb{Q}_p/I^2\mathbb{Q}_p \cong \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

7.1.1. **Proposition** (Local Square Theorem)**.** *Let $p \in \mathbb{P}$ and $\alpha \in \mathbb{Z}_p$. Then $1 + 4p\alpha \in \mathbb{Z}_p^2$, that is, $1 + 4p\alpha$ is a square of a number from $\mathbb{Z}_p$.*

In particular, if $p > 2$ and $\lambda \in p\mathbb{Z}_p$, then $1 + \lambda \in \mathbb{Z}_p^2$.

Proof. Consider $f(x) = px^2 + x - \alpha \in \mathbb{Z}_p[x]$. Then

$$f(\alpha) = p\alpha^2 \equiv 0 \pmod{p} \quad \text{and} \quad f'(\alpha) = 2p\alpha + 1 \equiv 1 \not\equiv 0 \pmod{p},$$

so we can apply Hensel's Lemma (Proposition 6.1.3). We get that there exists $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$. By the quadratic formula,

$$\beta = \frac{-1 \pm \sqrt{1 + 4p\alpha}}{2p},$$

so $1 + 4p\alpha = (1 + 2p\beta)^2 \in \mathbb{Z}_p^2$ as desired.

For the "In particular" part, it is enough to apply the main part for $\alpha = \frac{\lambda}{4p}$. $\square$

7.1.2. **Corollary.** *Let $p \in \mathbb{P}\backslash\{2\}$. Let $u \in \mathbb{Z}_p$ such that $\overline{u}$ is not a square in $\mathbb{F}_p$. We have that $|\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}| = 4$; more specifically, $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} = \{\mathbb{Q}_p^{\times 2}, u\mathbb{Q}_p^{\times 2}, p\mathbb{Q}_p^{\times 2}, up\mathbb{Q}_p^{\times 2}\}$.*

Proof. We first show that u, p, and up are not squares in $\mathbb{Q}_p$. If we had $p = \alpha^2$ for some $\alpha \in \mathbb{Q}_p$, then $1 = v_p(p) = v_p(\alpha^2) = 2v_p(\alpha)$, which is not possible, since $v_p(\alpha)$ must be an integer. Thus, p is not a square in $\mathbb{Q}_p$, and by a similar argument, up is not a square in $\mathbb{Q}_p$. Assume now that $u = \alpha^2$ for some $\alpha \in \mathbb{Q}_p$. Then $0 = v_p(u) = 2v_p(\alpha)$, so, $v_p(\alpha) = 0$ and hence $\alpha \in \mathbb{Z}_p$. The equation $u = \alpha^2$ then implies $\overline{u} = \overline{\alpha}^2$ in $\mathbb{F}_p$, but this is impossible, since we assumed that $\overline{u}$ is not a square in $\mathbb{F}_p$.

Now, we need to show that an arbitrary non-zerp element of $\mathbb{Q}_p$ can be written as a square times 1, u, p, or up. So take $\alpha \in \mathbb{Q}_p^\times$ arbitrary. Write $\alpha = p^k\alpha'$ for some $k \in \mathbb{Z}$ and $\alpha' \in \mathbb{Z}_p^\times$. Since $|\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}| = 2$ (see Exercise (2) in Lecture 4) and $\overline{u} \notin \mathbb{F}_p^{\times 2}$, we have that either $\overline{\alpha'} \in \mathbb{F}_p^{\times 2}$ or $\overline{\alpha' u} \in \mathbb{F}_p^{\times 2}$. Set $\alpha'' = \alpha'$ in the first case, or $\alpha'' = \alpha' u$ in the second case.

We now show that $\alpha'' \in \mathbb{Q}_p^{\times 2}$. Since α can be written as α'' multiplied with a product of powers of p and u, this will conclude the proof that every element of $\mathbb{Q}^\times$ is a square times 1, p, u, or up. Since $\overline{\alpha''} \in \mathbb{F}_p^{\times 2}$, we can find $\beta \in \mathbb{Z}_p^\times$ such that $\overline{\alpha'} = \overline{\beta}^2$. Then $\overline{\alpha''(\beta^{-1})^2} = 1$, whereby $\alpha''(\beta^{-1})^2 \in 1 + p\mathbb{Z}_p$. By Proposition 7.1.1 we conclude that $\alpha''(\beta^{-1})^2 \in \mathbb{Q}_p^{\times 2}$ and hence $\alpha'' \in \mathbb{Q}_p^{\times 2}$, as desired. □

7.1.3. **Corollary.** *We have that $|\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}| = 8$; more specifically, $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{\pm\mathbb{Q}_2^{\times 2}, \pm 2\mathbb{Q}_2^{\times 2}, \pm 3\mathbb{Q}_2^{\times 2}, \pm 6\mathbb{Q}_2^{\times 2}\}$.*

Proof. We proceed as in the proof of Corollary 7.1.2. First, we show that $-1, 2, -2, 3, -3, 6, -6$ are all non-squares in $\mathbb{Q}_2$. For $\alpha = 2, -2, 6, -6$ we have $v_2(\alpha) = 1$, so we conclude as before that α cannot be a square. For $\alpha = -1, 3, -3$, assume that $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}_2$. Then $0 = v_2(\alpha) = 2v_2(\beta)$, so $v_2(\beta) = 0$ and thus $\beta \in \mathbb{Z}_2$. Since $\alpha = \beta^2$, we have in particular $\alpha \equiv \beta^2 \bmod 8\mathbb{Z}_2$. But it is easy to compute that in $\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$, -1, 3 and -3 are not squares.

Now, we need to show that an arbitrary non-zero element of $\mathbb{Q}_2$ can be written as a square times ± 1, ± 2, ± 3, or ± 6. This is similar as in the proof of Corollary 7.1.2 and left as an exercise. □

7.2. **2-fold Pfister forms over p-adic fields.** Now that we know what the group $I\mathbb{Q}_p/I^2\mathbb{Q}_p \cong \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ looks like, we look at the next quotient $I^2\mathbb{Q}_p/I^3\mathbb{Q}_p$. In view of Proposition 5.2.5, this means we have to study 2-fold Pfister forms over $\mathbb{Q}_p$. We shall see that $I^2\mathbb{Q}_p/I^3\mathbb{Q}_p \cong \mathbb{Z}/2\mathbb{Z}$; in other words, there is a unique anisotropic 2-fold Pfister form over $\mathbb{Q}_p$ up to isometry. We shall compute this Pfister form explicitly, and more generally, see how to decide when a 2-fold Pfister form over $\mathbb{Q}_p$ is isotropic.

7.2.1. **Lemma.** *Let $q : \mathbb{Q}_p^n \to \mathbb{Q}_p$ be an isotropic quadratic form over $\mathbb{Q}_p$. There exists $v = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ such that $q(v) = 0$ and there exists $i \in \{1, \ldots, n\}$ with $x_i \in \mathbb{Z}_p^\times$.*

Proof. As q is isotropic, there exists $0 \neq w = (y_1, \dots, y_n) \in \mathbb{Q}_p^n$ with $q(w) = 0$. Let $k = \min\{v_p(y_1), \dots, v_p(y_n)\}$. Setting $x_i = p^{-k} y_i$ and $v = (x_1, \dots, x_n)$, we compute that $q(v) = p^{-2k} q(w) = 0$ and $\min\{v_p(x_1), \dots, v_p(x_n)\} = 0$, so this vector is as desired. □

As will often be the case, the case $p \neq 2$ is the easiest, so we start with that.

7.2.2. **Lemma.** *Let $p \in \mathbb{P} \setminus \{2\}$ and consider $a_1, a_2, a_3 \in \mathbb{Z}_p^\times$. Then*

- *$\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ is isotropic if and only if $\overline{-a_1 a_2}$ is a square in $\mathbb{F}_p$. If it is anisotropic, then for any $x_1, x_2 \in \mathbb{Q}_p$ we have*
$$v_p(a_1 x_1^2 + a_2 x_2^2) = 2 \min\{v_p(x_1), v_p(x_2)\}.$$
- *$\langle a_1, a_2, a_3 \rangle_{\mathbb{Q}_p}$ is always isotropic.*

Proof. Suppose first that $\overline{-a_1 a_2}$ is a square in $\mathbb{F}_p$. By Proposition 7.1.1 there exists $c \in \mathbb{Q}_p$ with $c^2 = -a_1 a_2$. But then $a_1 (a_2)^2 + a_2 (c^2) = a_1 a_2^2 - a_1 a_2^2 = 0$, so $\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ is isotropic.

Conversely, assume that there exist $x_1, x_2 \in \mathbb{Q}_p$ with $v_p(a_1 x_1^2 + a_2 x_2^2) \neq 2 \min\{v_p(x_1), v_p(x_2)\}$; this is for example the case when $\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ is isotropic, since then one can take an isotropic vector (x_1, x_2). We shall show that $\overline{-a_1 a_2} \in \mathbb{F}_p^{\times 2}$, finishing the proof of the first part.

Clearly we have $x_1 \neq 0$ and $x_2 \neq 0$. If we multiply both x_1 and x_2 by some element $c \in \mathbb{Q}_p^\times$, both the quantities $v_p(a_1 x_1^2 + a_2 x_2^2)$ and $2 \min\{v_p(x_1), v_p(x_2)\}$ get $2 v_p(c)$ added to them, hence we still have $v_p(a_1 (c x_1)^2 + a_2 (c x_2)^2) \neq 2 \min\{v_p(c x_1), v_p(c x_2)\}$ Hence, by multiplying x_1 and x_2 by p^{-k} where $k = \min\{v_p(x_1), v_p(x_2)\}$, and switching the role of x_1 and x_2 is necessary we may assume without loss of generality that $0 = v_p(x_1) \leq v_p(x_2)$.

By assumption, $v_p(a_1 x_1^2 + a_2 x_2^2) \neq 0$, and since $a_1, a_2, x_1, x_2 \in \mathbb{Z}_p$, we must have $v_p(a_1 x_1^2 + a_2 x_2^2) > 0$. Reducing modulo p, we see $0 = \overline{a_1 x_1}^2 + \overline{a_2 x_2}^2$. But then $\overline{-a_1 a_2} = (\frac{\overline{a_2 x_2}}{\overline{x_1}})^2$. This concludes the proof of the first point.

For the second point, recall from Exercise (2) in Lecture 4 that every nonsingular 2-dimensional quadratic form over a finite field is universal. In particular this applies to the form $\langle \overline{-a_1 a_3^{-1}}, \overline{-a_2 a_3^{-1}} \rangle_{\mathbb{F}_p}$, there exist $x_1, x_2 \in \mathbb{Z}_p^\times$ such that $\overline{-a_1 a_3^{-1} x_1^2 - a_2 a_3 x_2^2} = \overline{1}$. But then by Proposition 7.1.1, there exists $x_3 \in \mathbb{Q}_p^\times$ such that $-a_1 a_3^{-1} x_1^2 - a_2 a_3^{-1} x_2^2 = x_3^2$, i.e. $a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 = 0$. This shows that $\langle a_1, a_2, a_3 \rangle_{\mathbb{Q}_p}$ is isotropic. □

7.2.3. **Lemma.** *Let $p \in \mathbb{P} \setminus \{2\}$ and $a_1, a_2, a_3, a_4 \in \mathbb{Z}_p^\times$. Then*

- *$\langle a_1, a_2, p a_3 \rangle_{\mathbb{Q}_p}$ is anisotropic if and only if $\overline{-a_1 a_2}$ is a non-square in $\mathbb{F}_p$.*
- *$\langle a_1, a_2, p a_3, p a_4 \rangle_{\mathbb{Q}_p}$ is anisotropic if and only if $\overline{-a_1 a_2}$ and $\overline{-a_3 a_4}$ are both non-squares in $\mathbb{F}_p$.*

Proof. Since $\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ is a subform of $\langle a_1, a_2, p a_3 \rangle_{\mathbb{Q}_p}$, and both $\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ and $p \langle a_3, a_4 \rangle_{\mathbb{Q}_p}$ are subforms of $\langle a_1, a_2, p a_3, p a_4 \rangle_{\mathbb{Q}_p}$, it follows from Lemma 7.2.2 that

if $\overline{-a_1a_2} \in \mathbb{F}p^{\times 2}$, then $\langle a_1, a_2, pa_3\rangle_{\mathbb{Q}_p}$ and $\langle a_1, a_2, pa_3, pa_4\rangle_{\mathbb{Q}_p}$ are isotropic, and if $\overline{-a_3a_4} \in \mathbb{F}_p^{\times 2}$, then $\langle a_1, a_2, pa_3, pa_4\rangle_{\mathbb{Q}_p}$ is isotropic.

Suppose now that $\overline{-a_1a_2}$ and $\overline{-a_3a_4}$ are not squares in $\mathbb{F}_p$; it suffices to show that $\langle a_1, a_2, pa_3, pa_4\rangle_{\mathbb{Q}_p}$ is anisotropic. By Lemma 7.2.2 we have for any $x_1, x_2, x_3, x_4 \in \mathbb{Q}_p$ that

$$v_p(a_1x_1^2 + a_2x_2^2) = 2\min\{v_p(x_1), v_p(x_2)\} \quad \text{and}$$
$$v_p(pa_3x_3^2 + pa_4x_4^2) = 1 + v_p(a_3x_3^2 + a_4x_4^2) = 1 + 2\min\{v_p(x_3), v_p(x_4)\}.$$

If $a_1x_1^2 + a_2x_2^2 + pa_3x_2^3 + pa_4x_4^2 = 0$, then $v_p(a_1x_1^2 + a_2x_2^2) = v_p(-pa_3x_3^2 - pa_4x_4^2) = v_p(pa_3x_3^2 + pa_4x_4^2)$, but in view of the above two equations this is possible only when $\min\{v_p(x_1), v_p(x_2)\} = \min\{v_p(x_3), v_p(x_4)\} = \infty$, whereby $x_1 = x_2 = x_3 = x_4 = 0$. This shows that $\langle a_1, a_2, pa_3, pa_4\rangle_{\mathbb{Q}_p}$ is anisotropic. □

7.2.4. **Proposition.** *Let $p \in \mathbb{P} \setminus \{2\}$ and $a_1, a_2 \in \mathbb{Q}_p^\times$. Write $a_1 = p^{k_1}u_1$ and $a_2 = p^{k_2}u_2$ for $k_1, k_2 \in \mathbb{Z}$ and $u_1, u_2 \in \mathbb{Z}_p^\times$. The 2-fold Pfister form $\langle\langle a_1, a_2\rangle\rangle_{\mathbb{Q}_p}$ is anisotropic if and only if one of the following occurs:*

- *k_1 is even, k_2 is odd, and $\overline{u_1} \notin \mathbb{F}_p^{\times 2}$,*
- *k_1 is odd, k_2 is even, and $\overline{u_2} \notin \mathbb{F}_p^{\times 2}$,*
- *k_1 is odd, k_2 is odd, and $\overline{-u_1u_2} \notin \mathbb{F}_p^{\times 2}$.*

Proof. Since the isometry class of $\langle\langle a_1, a_2\rangle\rangle_{\mathbb{Q}_p}$ is unaffected when multiplying a_1 or a_2 by a square, we may multiply them with a power of p^k to assume without loss of generality that $k_1, k_2 \in \{0, 1\}$.

The case where $k_1 = 0$ or $k_2 = 0$ follows immediately from Lemma 7.2.3. In the remaining case $k_1 = k_2 = 1$, it suffices to use the computation rules from Corollary 5.2.3: we have

$$\{a_1, a_2\}_{\mathbb{Q}_p} = \{u_1p, u_2p\}_{\mathbb{Q}_p} = \{(u_1 + u_2)p, -u_1u_2p^2\}.$$

Since $-u_1u_2p^2$ has even value, we have reduced to a solved case. □

7.2.5. **Corollary.** *Let $p \in \mathbb{P}\setminus\{2\}$, let $u \in \mathbb{Z}_p^\times$ such that $\overline{u} \notin \mathbb{F}_p^{\times 2}$. Then $\langle\langle u, p\rangle\rangle_{\mathbb{Q}_p}$ is the unique anisotropic 2-fold Pfister form over $\mathbb{Q}_p$ up to isometry. In particular, $I^2\mathbb{Q}_p/I^3\mathbb{Q}_p \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. By Proposition 7.2.4 the quadratic form $\langle\langle u, p\rangle\rangle_{\mathbb{Q}_p}$ is anisotropic.

It remains to show that every element of $I\mathbb{Q}_p/I^2\mathbb{Q}_p = \{0, \{u, p\}_{\mathbb{Q}_p}\}$. By Corollary 7.1.2 and in view of Corollary 5.2.3(3) it suffices to show that $\{a_1, a_2\}_{\mathbb{Q}_p} \in \{0, \{u, p\}_{\mathbb{Q}_p}\}$ where $a_1, a_2 \in \{1, u, p, up\}$. This is now easily computed as follows, using the computation rules from Proposition 5.2.2 and Corollary 5.2.3. Note that either $-1 \in \mathbb{Q}_p^{\times 2}$ or $-1 \in u\mathbb{Q}_p^{\times 2}$ (depending on whether $\overline{-1} \in \mathbb{F}_p^{\times 2}$, so $\{-1, p\}_{\mathbb{Q}_p}$ is either equal to 0 or to $\{u, p\}_{\mathbb{Q}_p}$).

- If $a_1 = 1$, or if $a_2 = 1$, or if $a_1 = a_2 = u$, then $\{a_1, a_2\}_{\mathbb{Q}_p} = 0$ by Lemma 7.2.3,
- $\{p, u\}_{\mathbb{Q}_p} = \{u, p\}_{\mathbb{Q}_p}$,

- $\{up, u\}_{\mathbb{Q}_p} = \{u, up\}_{\mathbb{Q}_p} = \{u, u\}_{\mathbb{Q}_p} + \{u, p\}_{\mathbb{Q}_p} = 0 + \{u, p\}_{\mathbb{Q}_p} = \{u, p\}_{\mathbb{Q}_p}$,
- $\{p, p\}_{\mathbb{Q}_p} = \{2p, -p^2\}_{\mathbb{Q}_p} = \{2p, -1\}_{\mathbb{Q}_p} = \{2, -1\}_{\mathbb{Q}_p} + \{p, -1\}_{\mathbb{Q}_p} = 0 + \{-1, p\}_{\mathbb{Q}_p} \in \{0, \{u, p\}_{\mathbb{Q}_p}\}$,
- $\{p, up\}_{\mathbb{Q}_p} = \{up, p\}_{\mathbb{Q}_p} = \{u, p\}_{\mathbb{Q}_p} + \{p, p\}_{\mathbb{Q}_p} \in \{0, \{u, p\}_{\mathbb{Q}_p}\}$,
- $\{up, up\}_{\mathbb{Q}_p} = \{2up, -(up)^2\}_{\mathbb{Q}_p} = \{2, -1\}_{\mathbb{Q}_p} + \{up, -1\}_{\mathbb{Q}_p} \in \{0, \{up, u\}_{\mathbb{Q}_p}\}$.

This concludes the proof. □

We now discuss the case $p = 2$.

7.2.6. **Proposition.** *$\langle\langle -1, -1\rangle\rangle_{\mathbb{Q}_2}$ is the unique anisotropic 2-fold Pfister form over $\mathbb{Q}_2$ up to isometry. In particular, $I^2\mathbb{Q}_2/I^3\mathbb{Q}_2 \cong \mathbb{Z}/2\mathbb{Z}$. Furthermore, the following table shows for which values of $a_1, a_2 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ the form $\langle\langle a_1, a_2\rangle\rangle_{\mathbb{Q}_p}$ is isotropic (0) or anisotropic (1).*

a/b	*1*	*-1*	*2*	*-2*	*3*	*-3*	*6*	*-6*
1	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
-1	*0*	*1*	*0*	*1*	*1*	*0*	*1*	*0*
2	*0*	*0*	*0*	*0*	*1*	*1*	*1*	*1*
-2	*0*	*1*	*0*	*1*	*0*	*1*	*0*	*1*
3	*0*	*1*	*1*	*0*	*1*	*0*	*0*	*1*
-3	*0*	*0*	*1*	*1*	*0*	*0*	*1*	*1*
6	*0*	*1*	*1*	*0*	*0*	*1*	*1*	*0*
-6	*0*	*0*	*1*	*1*	*1*	*1*	*0*	*0*

Proof. To see that $\langle\langle -1, -1\rangle\rangle_{\mathbb{Q}_2}$ is anisotropic, suppose for the sake of a contradiction that it is isotropic. By Lemma 7.2.1 this means there exist $x_1, \ldots, x_4 \in \mathbb{Z}_p$ with $x_1^2 + \ldots + x_4^2 = 0$ and (without loss of generality) $x_1 \in \mathbb{Z}_p^\times$. But then we have $\overline{x_1}^2 + \ldots + \overline{x_4}^2 = 0$ in $\mathbb{Z}_2/8\mathbb{Z}_2 \cong \mathbb{Z}/8\mathbb{Z}$ and $\overline{x_1} \neq 0$; one verifies that this is impossible.

To verify the table, and to prove that $I\mathbb{Q}_2/I^2\mathbb{Q}_2 = \{0, \{-1, -1\}_{\mathbb{Q}_2}\}$, we compute $\{a_1, a_2\}$ for $a_1, a_2 \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. This is sufficient, given Corollary 7.1.2. But this table can be established entirely via the computation rules of Proposition 5.2.2 and Corollary 5.2.3. □

7.3. **Exercises.**

(1) Complete the proof of Corollary 7.1.3 and Proposition 7.2.6.
(2) Let $p \in \mathbb{P}$.
   - Show that for $x, y \in \mathbb{Q}_p^\times$ with $v_p(x - y) > v_p(4x)$ we have $x \in y\mathbb{Q}_p^{\times 2}$.
   - Conclude that for $x \in \mathbb{Q}_p^\times$ the set $x\mathbb{Q}_p^{\times 2}$ is open with respect to the p-adic topology.
(3) Determine completely the set of all prime numbers p for which the quadratic form $\langle\langle 15, 33\rangle\rangle_{\mathbb{Q}_p}$ is anisotropic.

8. Lecture 8

8.1. **Classification of quadratic forms over p-adic fields.** We are ready to completely classify the quadratic forms over p-adic fields up to isometry. Recall that, by Witt Decomposition (Theorem 2.2.3), it suffices to classify the anisotropic quadratic forms up to isometry.

The 1-dimensional case is immediate: over any field K, the quadratic forms $\langle a\rangle_K$ and $\langle b\rangle_K$ are isometric (for $a, b \in K^\times$) if and only if $ab \in K^{\times 2}$. The classification of 1-dimensional quadratic forms over $\mathbb{Q}_p$ thus follows from Corollary 7.1.2 and Corollary 7.1.3.

8.1.1. **Proposition.** *Let $p \in \mathbb{P}$. Let $a_1, a_2, b_1, b_2 \in \mathbb{Q}_p^\times$. Then $\langle a_1, a_2\rangle_{\mathbb{Q}_p} \cong \langle b_1, b_2\rangle_{\mathbb{Q}_p}$ if and only if $a_1a_2b_1b_2 \in \mathbb{Q}_p^{\times 2}$ and $\{a_1a_2, a_1b_1\}_{\mathbb{Q}_2} = 0$.*

Proof. This follows from Exercise (4) of Lecture 4. □

8.1.2. **Proposition.** *Let $p \in \mathbb{P}$. Let $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}_p^\times$. Then $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p}$ is isotropic if and only if $\{-a_1a_2, -a_1a_3\}_{\mathbb{Q}_p} = 0$. Furthermore, if $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p}$ and $\langle b_1, b_2, b_3\rangle_{\mathbb{Q}_p}$ are both anisotropic, then we have $b_1b_2b_3\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p} \cong a_1a_2a_3\langle b_1, b_2, b_3\rangle_{\mathbb{Q}_p}$; in particular we have $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p} \cong \langle b_1, b_2, b_3\rangle_{\mathbb{Q}_p}$ if and only if $a_1a_2a_3b_1b_2b_3 \in \mathbb{Q}_p^{\times 2}$.*

Proof. Observe that $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p} \cong a_1a_2a_3\langle a_1a_2, a_1a_3, a_2a_3\rangle_{\mathbb{Q}_p}$.

We have that $\{-a_1a_2, -a_1a_3\}_{\mathbb{Q}_p} = 0$ if and only if $\langle\!\langle -a_1a_2, -a_1a_3\rangle\!\rangle_{\mathbb{Q}_p}$ is isotropic (Proposition 5.2.5), if and only if $\langle\!\langle -a_1a_2, -a_1a_3\rangle\!\rangle_{\mathbb{Q}_p}$ is hyperbolic (Theorem 4.3.6), if and only if its 3-dimensional subform $\langle a_1a_2, a_1a_3, a_2a_3\rangle_{\mathbb{Q}_p}$ is isotropic, if and only if $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p}$ is isotropic. This shows the first statement.

Now assume that $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}_p}$ and $\langle b_1, b_2, b_3\rangle_{\mathbb{Q}_p}$ are both anisotropic; this implies by the previous paragraph that $\{-a_1a_2, -a_1a_3\}_{\mathbb{Q}_p}$ and $\{-b_1b_2, -b_1b_3\}_{\mathbb{Q}_p}$ are both non-zero, but then by Corollary 7.2.5 or Proposition 7.2.6 they must be equal. This implies in turn via Proposition 5.2.5 that $\langle\!\langle -a_1a_2, -a_1a_3\rangle\!\rangle_{\mathbb{Q}_p} \cong \langle\!\langle -b_1b_2, -b_1b_3\rangle\!\rangle_{\mathbb{Q}_p}$. By Witt Cancellation (Theorem 2.2.2) we conclude that $\langle a_1a_2, a_1a_3, a_2a_3\rangle_{\mathbb{Q}_p} \cong \langle b_1b_2, b_1b_3, a_2a_3\rangle_{\mathbb{Q}_p}$. The rest of the statement follows by comparing determinants. □

8.1.3. **Proposition.** *Let $p \in \mathbb{P}$. There is a unique anisotropic 4-dimensional quadratic form over $\mathbb{Q}_p$ up to isometry. This form is universal.*

Proof. We know from Corollary 7.2.5 or Proposition 7.2.6 that there exists a unique anisotropic 2-fold Pfister form over $\mathbb{Q}_p$. Let us write this as $\langle\!\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$, and recall that we may choose $a_1 = a_2 = -1$ if $p = 2$, and if $p \neq 2$, then choose $a_2 = p$ and $a_1 = u \in \mathbb{Z}_p^\times$ such that $\overline{u} \notin \mathbb{F}_p^{\times 2}$.

One verifies that $\langle -a_1, -a_2, a_1a_2\rangle_{\mathbb{Q}_p}$ represents all square classes in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ except for $-\mathbb{Q}^{\times 2}$: if $p = 2$ one checks by hand that each of $1, \pm 2, \pm 3, \pm 6$ are represented by $\langle 1, 1, 1\rangle_{\mathbb{Q}_2}$, and if $p > 2$, one also verifies that $\langle -u, -p, up\rangle_{\mathbb{Q}_p}$ represents u, p and up if $-1 \in \mathbb{Q}_p^{\times 2}$, or that it represents 1, p and up if $-1 \in u\mathbb{Q}_p^{\times 2}$.

Now, take an arbitrary anisotropic 4-dimensional quadratic form q over $\mathbb{Q}_p$. As $\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$ is the unique anisotropic 2-fold Pfister form over $\mathbb{Q}_p$, we have that $q \cong c\langle d, -a_1, -a_2, a_1a_2\rangle_K$ for some $c, d \in K^\times$. Furthermore, $-d$ is not represented by $\langle -a_1, -a_2, a_1a_2\rangle_{\mathbb{Q}_p}$, so by the previous paragraph, we may assume $d = 1$. Hence $q \cong c\langle\!\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$. Furthermore, one sees similarly as in the previous paragraph that $\langle\!\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$ is universal, in particular it represents c, and hence $q \cong \langle\!\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$ since Pfister forms are multiplicative (Theorem 4.3.6). We have shown that every 4-dimensional quadratic form over $\mathbb{Q}_p$ is isometric to $\langle\!\langle a_1, a_2\rangle\!\rangle_{\mathbb{Q}_p}$, and that this form is universal. □

8.1.4. **Corollary.** *Let $p \in \mathbb{P}$. Every 5-dimensional quadratic form over $\mathbb{Q}_p$ is isotropic.*

Proof. Let q be a 5-dimensional quadratic form over $\mathbb{Q}_p$. We have $q \cong \langle a\rangle_{\mathbb{Q}_p} \perp q'$ for some $a \in \mathbb{Q}_p^\times$ and a 4-dimensional quadratic form q' by Proposition 1.2.9. If q would be anisotropic, then also q' would be anisotropic, and then by Proposition 8.1.3 it universal; in particular it represents $-a$. But then q must actually have been isotropic. □

8.2. **Quadratic forms under 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 $V \to V \otimes L : v \mapsto v \otimes 1$, 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.

8.2.1. **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

$$q_L(v \otimes x) = x^2 q(v) \quad \textit{and} \quad \mathfrak{b}_{q_L} = (\mathfrak{b}_q)_L.$$

Proof. By redoing the proof of Proposition 3.1.5, using that B is a K-bilinear map and also $L \times L \to L : (x, y) \mapsto xy$ is a K-bilinear map, one obtains that there exists a unique symmetric K-bilinear map $B_L : V_L \times V_L \to L$ 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 $q_L(v \otimes x) = x^2 q(v)$ 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 $\mathrm{char}(K) \neq 2$, 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 $\mathrm{char}(K) = 2$ then a more subtle argument is needed: one still has that there exists some bilinear (but not necessarily symmetric) form $B : V \times V \to K$ 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 $\alpha \in V_L$. □

8.2.2. **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 8.2.1 is called the *scalar extension of* (V,B) *to* K.

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 8.2.1.

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, ...).

8.2.3. *Remark.* For a homogeneous degree 2 polynomial $f \in K[X_1,\ldots,X_n]$ 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:

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

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

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

8.2.5. **Definition.** Let L/K be a field extension. The map $r_{L/K}$ defined in Proposition 8.2.4 is called the *restriction homomorphism.*

8.3. **Exercises.**

(1) Let $p \in \mathbb{P}$. How many 2-dimensional anisotropic quadratic forms exist over $\mathbb{Q}_p$, up to isometry? And how many 3-dimensional anisotropic quadratic forms, up to isometry?
(2) Determine completely the set of all $p \in \mathbb{P}$ for which $\langle 22, 42, 231, 345\rangle_{\mathbb{Q}_p}$ is anisotropic.
(3) Let K be a field, q be a non-singular 4-dimensional quadratic form over K of discriminant d. Show that $q_{K[\sqrt{d}]}$ is similar to a 2-fold Pfister form.
(4) The proof of Proposition 8.1.2 relies on Proposition 5.2.5, which in turn relies on the deep Theorem 5.1.7, which we have not proven in this course. Can you restructure the arguments in this section to avoid using Proposition 5.2.5 or Theorem 5.1.7? (*Hint:* First find a proof that $I^3\mathbb{Q}_p = 0$ for all $p \in \mathbb{P}$.)

9. Lecture 9

9.1. **Hilbert's Reciprocity Law.** We now start our way towards a classification of quadratic forms over $\mathbb{Q}$. As discussed in the previous lecture, given a quadratic form over $\mathbb{Q}$, we can consider the scalar extension to $\mathbb{R}$ or $\mathbb{Q}_p$, and the goal is to understand quadratic forms over $\mathbb{Q}$ via its scalar extensions to $\mathbb{R}$ and $\mathbb{Q}_p$ for different primes p.

The first result is called Hilbert's Reciprocity Law, and is a consequence of the Quadratic Reciprocity Law. Let us first recall the Quadratic Reciprocity Law; see any book or course on elementary number theory for a proof.

9.1.1. **Theorem** (Quadratic Reciprocity)**.** *Let $p, q \in \mathbb{P} \setminus \{2\}$ be such that $p \neq q$.*

- *-1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \bmod 4$,*
- *2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \bmod 8$,*
- *p is a square in $\mathbb{F}_q$ if and only if*
  - *$p \equiv 1 \bmod 4$ and q is a square in $\mathbb{F}_p$, or*
  - *$q \equiv 1 \bmod 4$ and q is a square in $\mathbb{F}_p$, or*
  - *$p \equiv q \equiv 3 \bmod 4$ and q is not a square in $\mathbb{F}_p$.*

9.1.2. **Lemma.** *$\langle\langle -1, -1 \rangle\rangle_{\mathbb{R}}$ is the unique anisotropic quadratic form over $\mathbb{R}$ up to isometry. For any $x, y \in \mathbb{R}^\times$, we have $\{x, y\}_{\mathbb{R}} = 0$ if and only if $x > 0$ or $y > 0$. In particular, $I\mathbb{R}/I^2\mathbb{R} \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. Exercise. □

To state Hilbert's Reciprocity Law, it will be convenient to set $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{P}' = \mathbb{P} \cup \{\infty\}$.

9.1.3. **Theorem** (Hilbert's Reciprocity Law)**.** *Let $x, y \in \mathbb{Q}^\times$. The set*

$$S = \{p \in \mathbb{P}' \mid \{x, y\}_{\mathbb{Q}_p} \neq 0\}$$

contains a finite, even number of elements.

Proof. For all but finitely many $p \in \mathbb{P} \setminus \{2\}$, $v_p(x) = v_p(y) = 0$ (see Proposition 6.1.5). By Proposition 7.2.4 we thus obtain $\{x, y\}_{\mathbb{Q}_p} = 0$ for all but these finitely many odd prime numbers. This shows that this set S is always finite.

Now consider the map

$$\oplus : I^2\mathbb{Q}/I^3\mathbb{Q} \to \bigoplus_{p \in \mathbb{P}'} I^2\mathbb{Q}_p/I^3\mathbb{Q}_p : [q] \mapsto \oplus_{p \in \mathbb{P}'}[q_{\mathbb{Q}_p}].$$

By the observation from the previous paragraph: any symbol $\{x, y\}_{\mathbb{Q}}$ becomes 0 when extending scalars to all but finitely many $\mathbb{Q}_p$, so this map is well-defined. In fact, since each of the individual maps $[q] \mapsto [q_{\mathbb{Q}_p}]$ is a group homomorphism by Proposition 8.2.4, also the map $\oplus$ is a group homomorphism.

Now consider the map

$$\Sigma : \bigoplus_{p \in \mathbb{P}'} I^2\mathbb{Q}_p/I^3\mathbb{Q}_p \to \mathbb{Z}/2\mathbb{Z} : \oplus_{p \in \mathbb{P}'}[q_p] \mapsto \sum_{p \in \mathbb{P}'} \delta_{[q_p]}$$

where $\delta_{[q_p]} = 0$ if $[q_p] = 0$ and otherwise $\delta_{[q_p]} = 1$. This is a well-defined map, and since $I^2\mathbb{Q}_p/I^3\mathbb{Q}_p \cong \mathbb{Z}/2\mathbb{Z}$ for all $p \in \mathbb{P}'$ by Corollary 7.2.5, Proposition 7.2.6, and Lemma 9.1.2, it is actually a group homomorphism.

We now make the following observation: to show the theorem is to show that the map $\Sigma \circ \oplus = 0$; in other words, the image of $\circ$ is contained in the kernel of Σ. Since $\Sigma \circ \oplus$ is a group homomorphism, it suffices to show that $\Sigma \circ \oplus$ is zero on a set of generators of $I^2\mathbb{Q}/I^3\mathbb{Q}$.

$I^2\mathbb{Q}_p/I^3\mathbb{Q}_p$ is generated by symbols $\{x, y\}_{\mathbb{Q}}$ for $x, y \in \mathbb{Q}^\times$. By the computation rules for symbols (Corollary 5.2.3) we may assume that $x, y \in \mathbb{Z}$. In fact, using bilinearity (Proposition 5.2.2) and the fact that every integer is a product of prime numbers and ± 1, we have reduced to showing the theorem in the following cases:

- $x = y = -1$,
- $x = -1$, $y = 2$,
- $x = y = 2$,
- $x = -1$, $y = p$ for some $p \in \mathbb{P} \setminus \{2\}$,
- $x = 2$, $y = p$ for some $p \in \mathbb{P} \setminus \{2\}$,
- $x = y = p$ for some $p \in \mathbb{P} \setminus \{2\}$,
- $x = p$ and $y = q$ for some distinct primes $p, q \in \mathbb{P} \setminus \{2\}$.

Each of these cases can now be checked by hand, using Theorem 9.1.1 and the computation rules for $\{x, y\}_{\mathbb{Q}_p}$ (Proposition 7.2.4, Proposition 7.2.6, Lemma 9.1.2). Let us consider the last of them and leave the others as an exercise.

So suppose $p, q \in \mathbb{P} \setminus \{2\}$ and let $S = \{p' \in \mathbb{P}' \mid \{p, q\}_{\mathbb{Q}_{p'}} \neq 0\}$. By Proposition 7.2.4 $r \notin S$ for any $r \in \mathbb{P} \setminus \{2, p, q\}$. By Proposition 7.2.6 we have that $\infty \notin S$. By Proposition 7.2.6 we have $2 \in S$ if and only if $p, q \equiv 3 \bmod 4$. Furthermore, we compute using Proposition 7.2.4 and Theorem 9.1.1 that

$$\begin{aligned} p \in S &\Leftrightarrow q \text{ is not a square in } \mathbb{F}_p \\ &\Leftrightarrow \begin{cases} p \text{ is a square in } \mathbb{F}_q & \text{if } p \equiv q \equiv 3 \bmod 4 \\ p \text{ is not a square in } \mathbb{F}_q & \text{otherwise} \end{cases} \\ &\Leftrightarrow \begin{cases} q \notin S & \text{if } p \equiv q \equiv 3 \bmod 4 \\ q \in S & \text{otherwise} \end{cases}. \end{aligned}$$

From this we conclude that $|S| \in \{0, 2\}$, and thus in particular S contains an even number of elements, as desired. □

9.2. **Approximation.** Recall from elementary number theory the Chinese Remainder Theorem:

9.2.1. **Theorem.** *Let $S \subseteq \mathbb{P}$ be a set of prime numbers and $n \in \mathbb{N}$. For each $p \in S$, let $a_p \in \mathbb{Z}$. Then there exists $a \in \mathbb{Z}$ such that $a \equiv a_p \bmod p^n$ for all $p \in S$.*

This theorem has the following reformulation in the language of p-adic numbers.

9.2.2. **Corollary.** *Let $S \subseteq \mathbb{P}$ be a set of prime numbers and $n \in \mathbb{N}$. For each $p \in S$, let $x_p \in \mathbb{Z}_p$. Then there exists $x \in \mathbb{Z}$ such that $v_p(x - x_p) > n$ for all $p \in S$.*

Proof. Exercise. □

In other words, we know that (by construction) we can for each $p \in \mathbb{P}$ approximate p-adic integers arbitrarily closely by rational integers, but in fact, one can do so for a finite set of prime numbers simultaneously. We now prove the following variation for rational numbers.

9.2.3. **Theorem** (Artin Approximation)**.** *Let $S \subseteq \mathbb{P}$ be finite and fix $q \in \mathbb{P} \setminus S$. Let $n \in \mathbb{N}$, and for each $p \in S$, fix $x_p \in \mathbb{Q}_p$, and also fix $x_\infty \in \mathbb{R}$. Then there exists $x \in \mathbb{Q}$ such that*

- *for all $p \in S$, one has $v_p(x - x_p) > n$,*
- *$|x - x_\infty| < 1/n$,*
- *for all $r \in \mathbb{P} \setminus (S \cup \{q\})$ we have $x \in \mathbb{Z}_r$. In other words, the denominator of x is not divisible by any primes outside of $S \cup \{q\}$.*

Proof. We may replace the number n in the statement by a larger natural number, as that will only strengthen the outcome. In particular, we may assume without loss of generality $n \geq -v_p(x_p)$ for all $p \in S$. Furthermore, since we can arbitarily approximate an element in $\mathbb{Q}_p$ by an element of $\mathbb{Q}$ with denominator a power of p, we may also assume that $x_p \in \mathbb{Q}$ with denominator a power of p. Similarly, by increasing n if needed, we may assume that $x_\infty \in \mathbb{Q}$ with denominator a power of q.

For each $p \in S$, we shall show the existence of an element $d_p \in \mathbb{Q}$ whose denominator is a power of q and such that

$$v_p(d_p - 1) > 2n, \quad v_{p'}(d_p) > 2n \text{ for all } p' \in S \setminus \{p\}, \text{ and } \quad |d_p| < \frac{1}{n(|S|+1)|x_p|},$$

and furthermore an element $d_\infty \in \mathbb{Q}$ whose denominator is a power of q and such that

$$v_p(d_\infty) > 2n \text{ for all } p \in S, \text{ and } \qquad |d_\infty - 1| < \frac{1}{n(|S|+1)|x_\infty|}.$$

Once we have found these elements, we will be almost done: it suffices to set $x = \sum_{p \in S} x_p d_p + x_\infty d_\infty$. We then compute that, for $p \in \mathbb{P}$,

$$\begin{aligned} v_p(x - x_p) &= v_p(x - x_p d_p + x_p d_p - x_p) \geq \min\{v_p(x - x_p d_p), v_p(x_p d_p - x_p)\} \\ &= \min\{v_p(\sum_{p' \in (S \cup \{\infty\}) \setminus \{p\}} x_{p'} d_{p'}), v_p(x_p) + v_p(d_p - 1)\} \\ &\geq \min\{\min_{p' \in (S \cup \{\infty\}) \setminus \{p\}} \{v_p(x_{p'}) + v_p(d_{p'})\}, v_p(x_p) + v_p(d_p - 1)\} > n \end{aligned}$$

by construction of the d_p's, and similarly

$$\begin{aligned}|x - x_\infty| &\leq |x - x_\infty d_\infty| + |x_\infty d_\infty - x_\infty| \\ &\leq \sum_{p \in S} |x_p||d_p| + |x_\infty||d_\infty - 1| < \frac{1}{n}.\end{aligned}$$

Thus, it now remains to show that such d_p can be constructed for each $p \in S \cup \{\infty\}$ individually.

Consider first $p \in S$. Since the multiplicative group $(\mathbb{Z}/p^{2n}\mathbb{Z})^\times$ is finite, and $\prod_{p' \in S \setminus \{p\}} p'$ represents an invertible element in $\mathbb{Z}/p^{2n}\mathbb{Z}$, there exists $N > 2n$ such that $(\prod_{p' \in S \setminus \{p\}} p')^N \equiv 1 \bmod p^{2n}$. Similarly, since q represents an invertible element in $\mathbb{Z}/p^{2n}\mathbb{Z}$, there exist arbitrarily large $M \in \mathbb{N}$ with $q^M \equiv 1 \bmod p^{2n}$. In particular, we can take M large enough so that $|(\prod_{p' \in S \setminus \{p\}} p')^N q^{-M}| < (n(|S| + 1)|x_p|)^{-1}$. Now $d_p = (\prod_{p' \in S \setminus \{p\}} p')^N q^{-M}$ is as desired.

Finally, again by similar arguments, we may choose $M \in \mathbb{N}$ large enough such that $q^M \equiv 1 \bmod p^{2n}$ for all $p \in S$, at the same time $|q^{-M}| \leq (n(|S| + 1)|x_\infty|)^{-1}$. Then $d_\infty = 1 - q^{-M}$ is as desired. □

We will need later also the following strengthening of Theorem 9.2.1, often referred to as Dirichlet's Theorem on (Primes in) Arithmetic Progressions.

9.2.4. **Theorem** (Dirichlet's Theorem)**.** *Let $m, n \in \mathbb{N}$ be coprime. There exist infinitely many $p \in \mathbb{P}$ with $p \equiv n \bmod m$.*

Proof. See for example [Neu99, Section I.10, Exercise 1]. □

Note that in the above theorem, we may replace one congruence condition with finitely many, as long as they pertain to coprime moduli, in view of Theorem 9.2.1.

9.3. **Exercises.**

(1) Give a proof of Lemma 9.1.2.
(2) Consider $\mathbb{Q}_p$ with the p-adic topology, $\mathbb{Q}_\infty = \mathbb{R}$ with the euclidean topology, and consider $\prod_{p \in \mathbb{P}'} \mathbb{Q}_p$ with the induced product topology. Show that the image of the diagonal embedding
$$\mathbb{Q} \to \prod_{p \in \mathbb{P}'} \mathbb{Q}_p : x \mapsto (x)_{p \in \mathbb{P}'}$$
is dense with respect to the product topology.
(3) Use Theorem 9.2.4 to show a converse to Theorem 9.1.3: for every finite set $S \subseteq \mathbb{P}'$ of even cardinality, there exist $x, y \in \mathbb{Q}^\times$ such that $S = \{p \in \mathbb{P}' \mid \{x, y\}_{\mathbb{Q}_p} \neq 0\}$.
(4) Use Exercise (9) from Lecture 6 to show that the following are equivalent for $n \in \mathbb{N}$ and $f \in \mathbb{Z}[X_1, \ldots, X_n]$:
   - f has a zero in $\mathbb{Z}/m\mathbb{Z}$ for all $m \in \mathbb{N}$,
   - f has a zero in $\mathbb{Z}_p$ for all $p \in \mathbb{P}$.

(5) Show that the polynomial $f(X) = (X^2 - 13)(X^2 - 17)(X^2 - 221)$ has no zero in $\mathbb{Z}$, but has a zero in $\mathbb{R}$ and in $\mathbb{Z}/m\mathbb{Z}$ for every $m \in \mathbb{N}$.

10. Lecture 10

10.1. **The Hasse-Minkowski Theorem.** We are ready to phrase and proof the Hasse-Minkowski Theorem.

10.1.1. **Theorem** (Hasse-Minkowski)**.** *Let q be an anisotropic quadratic form over $\mathbb{Q}$. Then there exists $p \in \mathbb{P}'$ such that $q_{\mathbb{Q}_p}$ is anisotropic.*

In other words, if one wants to check whether a quadratic form over q is isotropic, if suffices to prove that it is isotropic over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$. This might a priori seem like an equally hard problem since one needs to consider infinitely many prime numbers $p \in \mathbb{P}'$, but recall that if $\dim(q) \geq 3$, then q contains a subform isometric to $\langle a_1, a_2, a_3\rangle_{\mathbb{Q}}$ for some $a_1, a_2, a_3 \in \mathbb{Z} \setminus \{0\}$, and then $q_{\mathbb{Q}_p}$ is automatically isotropic for all $p \in \mathbb{P} \setminus \{2\}$ which do not divide a_1, a_2 and a_3 by Lemma 7.2.2. This leaves only finitely many prime numbers to check, and checking isotropy of quadratic forms over $\mathbb{Q}_p$ can be done algorithmically, as explained in lectures 7 and 8.

Theorem 10.1.1 has the following immediate consequence, showing that we obtain a complete classifiction of quadratic forms over $\mathbb{Q}$ via the classification of quadratic forms over each $\mathbb{Q}_p$.

10.1.2. **Corollary.** *Let q_1, q_2 be quadratic forms over $\mathbb{Q}$. If $(q_1)_{\mathbb{Q}_p} \cong (q_2)_{\mathbb{Q}_p}$ for all $p \in \mathbb{P}'$, then $q_1 \cong q_2$. In particular, the group homomorphism*

$$W\mathbb{Q} \to \prod_{p\in\mathbb{P}'} W\mathbb{Q}_p : [q] \mapsto ([q_{\mathbb{Q}_p}])_{p\in\mathbb{P}'}$$

is injective.

Proof. Exercise. □

Proof of Theorem 10.1.1. Let $n = \dim(q)$. By Corollary 1.2.10 we may assume without loss of generality $q = \langle a_1, \ldots, a_n\rangle_{\mathbb{Q}}$ for some $a_1, \ldots, a_n \in \mathbb{Q}$, and in fact we have $a_1, \ldots, a_n \in \mathbb{Q}^\times$ if we assume that q is anisotropic. By replacing q with a similar quadratic form (which does not affect isotropy over $\mathbb{Q}$ or any field extension) we may assume that $a_n = 1$ and $a_2, \ldots, a_n$ are square-free integers.

We now continue by making a case distinction on n. For $n = 1$ there is nothing to prove: $\langle 1\rangle_{\mathbb{Q}_p}$ is anisotropic for all $p \in \mathbb{P}'$.

Assume $n = 2$, i.e. $q = \langle 1, a_1\rangle_{\mathbb{Q}}$. By Exercise (4) of Lecture 1 we have that $-a_1 \notin \mathbb{Q}^{\times 2}$. This implies that either $a_1 > 0$, in which case $-a_1 \notin \mathbb{R}^{\times 2}$ and hence $q_{\mathbb{R}}$ is anisotropic, or there is $p \in \mathbb{P}$ which divides $-a_1$ an odd number of times, whereby $-a_1 \notin \mathbb{Q}_p^{\times 2}$ and hence $q_{\mathbb{Q}_p}$ is anisotropic. This concludes the proof for $n = 2$.

Assume $n = 3$. We assume that $q = \langle 1, a_1, a_2\rangle_{\mathbb{Q}}$ is isotropic over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$ and we need to show that q itself is isotropic. By switching the roles of

a_1 and a_2, we may assume $|a_1| \leq |a_2|$. In view of Corollary 2.1.7 we equivalently need to show that $\langle 1, a_1 \rangle_{\mathbb{Q}}$ represents $-a_2$, assuming it does so over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$.

We proceed by induction on $|a_2|$. If $|a_2| = |a_1| = 1$, then either $a_1 = -1$ or $a_2 = -1$, in which case q is isotropic, or $a_1 = a_2 = 1$, but in this case $q_{\mathbb{R}} = \langle 1, 1, 1 \rangle_{\mathbb{R}}$ is anisotropic, contradicting the assumption. Now assume $|a_2| > 1$. For each prime number p dividing a_2 there exists $c \in \mathbb{Z}$ with $c^2 \equiv -a_1 \bmod p$: if p divides a_1 one may just take $c = 0$, if $p = 2$ and p does not divide a_1 one may take $c = 1$, and otherwise this follows from the fact that $q_{\mathbb{Q}_p}$ is isotropic and Lemma 7.2.2. Since a_2 is square-free, by the Chinese Remainder Theorem (Theorem 9.2.1) we find $c \in \mathbb{Z}$ such that $c^2 \equiv -a_1 \bmod a_2$. Clearly we may even find such c with $|c| \leq |a_2|/2$.

It follows that $c^2 = -a_1 - a_2 b$ for some $b \in \mathbb{Z}$, whereby $-a_2 b \in D_{\mathbb{Q}}(\langle 1, a_1 \rangle_{\mathbb{Q}})$. Furthermore, we compute that

$$|b| = \left| \frac{c^2 + a_1}{a_2} \right| \leq \left| \frac{c^2}{a_2} \right| + \left| \frac{a_1}{a_2} \right| \leq \frac{|a_2|}{4} + 1 < |a_2|.$$

If we had $b \notin D_{\mathbb{Q}}(\langle 1, a_1 \rangle_{\mathbb{Q}})$, then by the induction hypothesis there exists $p \in \mathbb{P}'$ such that $b \notin D_{\mathbb{Q}_p}(\langle 1, a_1 \rangle_{\mathbb{Q}_p})$. But since $\langle 1, a_1 \rangle_{\mathbb{Q}_p}$ is multiplicative and $-a_2 b \in D_{\mathbb{Q}_p}(\langle 1, a_1 \rangle_{\mathbb{Q}_p})$, it would follow that $-a_2 \notin D_{\mathbb{Q}_p}(\langle 1, a_1 \rangle_{\mathbb{Q}_p})$, contradicting the assumption that $q = \langle 1, a_1, a_2 \rangle_{\mathbb{Q}}$ is isotropic over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$. Hence we must have $b \in D_{\mathbb{Q}}(\langle 1, a_1 \rangle_{\mathbb{Q}})$, and then by the multiplicativity of $D_{\mathbb{Q}}(\langle 1, a_1 \rangle_{\mathbb{Q}})$ also $-a_2 = (-a_2 b)/b \in D_{\mathbb{Q}}(\langle 1, a_1 \rangle_{\mathbb{Q}})$, hence we are done. This concludes the proof for the case $n = 3$.

Assume $n = 4$. We assume that $q = \langle a_1, a_2, a_3, a_4 \rangle_{\mathbb{Q}}$ is isotropic over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$ and show that q is itself isotropic.

Let $T = \{2, \infty\} \cup \{p \in \mathbb{P} \mid p \mid a_1 a_2 a_3 a_4\}$. This is a finite set. By assumption $\langle a_1, a_2 \rangle_{\mathbb{Q}_p}$ and $-\langle a_3, a_4 \rangle_{\mathbb{Q}_p}$ represent a common element in $\mathbb{Q}_p$ for each $p \in \mathbb{P}$. In view of the classification of square classes (Corollary 7.1.2 and Corollary 7.1.3) we may assume there exists for each $p \in \mathbb{P}'$ an element $z_p \in \mathbb{Z} \cap D_{\mathbb{Q}_p}(\langle a_1, a_2 \rangle_{\mathbb{Q}_p}) \cap D_{\mathbb{Q}_p}(-\langle a_3, a_4 \rangle_{\mathbb{Q}_p})$ with, for $p \in \mathbb{P}$, $v_p(z_p) \leq 1$. By Theorem 9.2.4 we may find a prime $q \in \mathbb{P} \setminus T$ and $\varepsilon \in \{1, -1\}$ such that, for $z = \varepsilon q$, $z z_\infty > 0$, $z \equiv z_2 \bmod 16$ and $z \equiv z_p \bmod p^2$ for $p \in T \setminus \{2, \infty\}$. It follows by Proposition 7.1.1 that $z z_p \in \mathbb{Q}_p^{\times 2}$ for all $p \in T$, whence $z \in D_{\mathbb{Q}_p}(\langle a_1, a_2 \rangle_{\mathbb{Q}_p}) \cap D_{\mathbb{Q}_p}(-\langle a_3, a_4 \rangle_{\mathbb{Q}_p})$ and thus $\langle a_1, a_2, -z \rangle_{\mathbb{Q}_p}$ and $\langle z, -a_3, -a_4 \rangle_{\mathbb{Q}_p}$ are isotropic for all $p \in T$. Furthermore, in view of Lemma 7.2.2, $\langle a_1, a_2, -z \rangle_{\mathbb{Q}_p}$ and $\langle z, -a_3, -a_4 \rangle_{\mathbb{Q}_p}$ are also isotropic for all $p \in \mathbb{P} \setminus (T \cup \{q\})$. Finally, by Theorem 9.1.3 we conclude that $\langle a_1, a_2, -z \rangle_{\mathbb{Q}_q}$ and $\langle z, -a_3, -a_4 \rangle_{\mathbb{Q}_q}$ must also be isotropic, and then by the case $n = 3$ we conclude that $\langle a_1, a_2, -z \rangle_{\mathbb{Q}}$ and $\langle z, -a_3, -a_4 \rangle_{\mathbb{Q}}$ are isotropic, and hence in particular q is isotropic. This concludes the proof for the case $n = 4$.

Assume $n \geq 5$. We assume that $q = \langle a_1, \ldots, a_n \rangle_{\mathbb{Q}}$ is isotropic over $\mathbb{Q}_p$ for all $p \in \mathbb{P}'$ and show that q itself is isotropic. Consider $T = \{2, \infty\} \cup \{p \in \mathbb{P} \mid a_3 a_4 \ldots a_n\}$. This is a finite set. As in the case $n = 4$, we find for each $p \in \mathbb{P}'$ an element

$z_p \in \mathbb{Z} \cap D_{\mathbb{Q}_p}(\langle a_1, a_2\rangle_{\mathbb{Q}_p}) \cap D_{\mathbb{Q}_p}(-\langle a_3, \ldots, a_n\rangle_{\mathbb{Q}_p})$. Let us write $z_p = a_1x_p^2 + a_2y_p^2$ for some $x_p, y_p \in \mathbb{Q}_p$; we may further assume $x_p,\ y_p \neq 0$ (see e.g. Exercise (4) of Section 2). By Theorem 9.2.3 we may find $x, y \in \mathbb{Q}$ such that

$$\begin{aligned} v_p(x - x_p) &> \max\{v_p(x_p), v_p(4z_p(a_1x_p)^{-1})\} \text{ for all } p \in T \setminus \{\infty\}, \\ v_p(y - y_p) &> \max\{v_p(y_p), v_p(4z_p(a_2y_p)^{-1})\} \text{ for all } p \in T \setminus \{\infty\}, \\ |x - x_\infty| &< \min\{|x_\infty|, |z_\infty(4a_1x_\infty)^{-1}|\}, \text{ and} \\ |y - y_\infty| &< \min\{|y_\infty|, |z_\infty(4a_2y_\infty)^{-1}|\}. \end{aligned}$$

Now set $z = a_1x^2 + a_2y^2$. It is clear that $z \in D_{\mathbb{Q}}(\langle a_1, a_2\rangle_{\mathbb{Q}})$ by construction, and we shall show that $z \in z_p\mathbb{Q}_p^{\times 2}$ for all $p \in T$, from which it follows that $z \in D_{\mathbb{Q}_p}(-\langle a_3, \ldots, a_n\rangle_{\mathbb{Q}_p})$ for all $p \in T$ and thus $\langle z, -a_3, \ldots, -a_n\rangle_{\mathbb{Q}_p}$ is isotropic. Since we automatically have that $\langle z, -a_3, \ldots, -a_n\rangle_{\mathbb{Q}_p}$ is isotropic for $p \in \mathbb{P} \setminus T$ (since already $-\langle a_3, \ldots, a_n\rangle_{\mathbb{Q}_p}$ is isotropic by Lemma 7.2.2), we obtain by the induction hypothesis that $\langle z, -a_3, \ldots, -a_n\rangle_{\mathbb{Q}}$ is isotropic. We conclude that q is isotropic, as desired.

It remains to show the claim that $z \in z_p\mathbb{Q}_p^{\times 2}$ for all $p \in T$. First consider $p \neq \infty$. Observe that $v_p(x + x_p) \geq v_p(x_p)$ and $v_p(y + y_p) \geq v_p(y_p)$. We compute that

$$\begin{aligned} & v_p(z - z_p) \\ = \ & v_p(a_1x^2 + a_2y^2 - a_1x_p^2 - a_2y_p^2) \\ = \ & v_p(a_1(x - x_p)(x + x_p) + a_2(y - y_p)(y + y_p)) \\ \geq \ & \min\{v_p(a_1) + v_p(x - x_p) + v_p(x + x_p), v_p(a_2) + v_p(y - y_p) + v_p(y + y_p)\} \\ > \ & v_p(4z_p) \end{aligned}$$

from which it follows that $z \in z_p\mathbb{Q}_p^{\times 2}$ by Exercise (2) of Section 7. For $p = \infty$, we compute similarly that

$$|z - z_\infty| \leq |a_1||x - x_\infty||x + x_\infty| + |a_2||y - y_\infty||y + y_\infty| < |z_\infty|$$

whereby z and z_∞ must have the same sign and thus $z \in z_\infty\mathbb{R}^{\times 2}$. □

10.2. **Exercises.**

(1) Give a proof of Corollary 10.1.2.
(2) Compute $|I^3\mathbb{Q}/I^4\mathbb{Q}|$.
(3) Let K be a field with $\mathrm{char}(K) \neq 2$. We say that two 2-fold Pfister forms q_1 and q_2 over K are *linked* if there exists $a, b, c \in K^\times$ such that $q_1 \cong \langle\langle a, b\rangle\rangle_K$ and $q_2 \cong \langle\langle a, c\rangle\rangle_K$.
   - Show that two 2-fold Pfister forms $\langle\langle a, b\rangle\rangle_K$ and $\langle\langle c, d\rangle\rangle_K$ are linked if and only if the quadratic form $\langle a, b, -ab, -c, -d, cd\rangle_K$ is isotropic, if and only if there exist $e, f \in K^\times$ such that $\{a, b\}_K + \{c, d\}_K = \{e, f\}_K$ in $I^2K/I^3/K$.
   - Show that over $K = \mathbb{Q}$, any two 2-fold Pfister forms are linked.

- Is it true that, for any $n \in \mathbb{N}$ and 2-fold Pfister forms $q_1, \dots, q_n$ over $\mathbb{Q}$, there exists $a, b_1, \dots, b_n \in \mathbb{Q}^\times$ such that $q_i \cong \langle\langle a, b_i \rangle\rangle_{\mathbb{Q}}$ for all i?

11. Lecture 11

In this final lecture, we give another application of quadratic form theory of a more algorithmic nature: Hermite's method of counting real zeros of a univariate polynomial.

Let always K be a field.

11.1. **The trace of an algebra.** Recall from linear algebra that the *trace of a matrix* $A$with entries in K, denoted by $\mathrm{Tr}(A)$, is the sum of its diagonal elements. It satisfies the property $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ for square matrices A, B of the same size.

When V is a finite-dimensional K-vector space, we can thus associate to every linear map $L : V \to V$ the *trace of the linear map* L , denoted by $\mathrm{Tr}(V)$, as the trace of the matrix of L with respect to any choice of basis of V. Note that, if $M_{\mathcal{B}}$ and $M_{\mathcal{B}'}$ are the matrices of L with respect to different bases $\mathcal{B}$ and $\mathcal{B}'$ of V, then we have $M_{\mathcal{B}} = CM_{\mathcal{B}'}C^{-1}$ for an invertible base change matrix C, and then $\mathrm{Tr}(M_{\mathcal{B}}) = \mathrm{Tr}(CM_{\mathcal{B}'}C^{-1}) = \mathrm{Tr}(CC^{-1}M_{\mathcal{B}'}) = \mathrm{Tr}(M_{\mathcal{B}'})$, so this definition does not depend on the choice of basis.

Recall that a *K-algebra* is a ring $\mathcal{A}$ containing K and such that $k\alpha = \alpha k$ for all $\alpha \in \mathcal{A}$ and $k \in K$. This last property is satisfied in particular if $\mathcal{A}$ is a commutative ring, which will be the case for all algebras which we consider in the next part. $\mathcal{A}$ is a vector space over K, and we say that $\mathcal{A}$ is a finite-dimensional K-algebra if it is finite-dimensional as a vector space over K, and write $\dim(\mathcal{A})$ for the dimension of $\mathcal{A}$ as a K-vector space.

11.1.1. **Definition.** Let $\mathcal{A}$ be a finite-dimensional K-algebra, $\alpha \in \mathcal{A}$. We define the *trace of* α, denoted by $\mathrm{Tr}_{\mathcal{A}}(\alpha)$, as the trace of the K-linear map

$$l_\alpha : \mathcal{A} \to \mathcal{A} : \beta \mapsto \alpha\beta.$$

11.1.2. **Proposition.** *Let $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ be finite-dimensional K-algebras. The trace satisfies the following properties:*

1. *The map $\mathrm{Tr}_{\mathcal{A}} : \mathcal{A} \to K$ is K-linear.*
2. *For all $a \in K$ we have $\mathrm{Tr}_{\mathcal{A}}(a) = \dim(\mathcal{A}) \cdot a$.*
3. *If $\alpha \in \mathcal{A}$ is such that $\alpha^D = 0$ for some $D \in \mathbb{N}$, then $\mathrm{Tr}_{\mathcal{A}}(\alpha) = 0$.*
4. *If $\varphi : \mathcal{A} \to \mathcal{B}$ is a ring isomorphism, then $\mathrm{Tr}_{\mathcal{A}}(\alpha) = \mathrm{Tr}_{\mathcal{B}}(\varphi(\alpha))$ for $\alpha \in \mathcal{A}$.*
5. *If $\mathcal{C} = \mathcal{A} \times \mathcal{B}$ as a ring, then for $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$ we have $\mathrm{Tr}_{\mathcal{C}}((\alpha, \beta)) = \mathrm{Tr}_{\mathcal{A}}(\alpha) + \mathrm{Tr}_{\mathcal{B}}(\beta)$.*

Proof. Exercise. □

11.2. **Hermite's method for counting real zeros.** We now explain how trace forms can be used to count the number of real zeros of a polynomial.

Assume throughout that $\mathrm{char}(K) \neq 2$. For a non-zero polynomial $f \in K[X]$ of degree d, denote by $\mathcal{A}_f$ the d-dimensional K-algebra $K[X]/(f(X))$. Given another polynomial $g \in K[X]$, we denote its equivalence class in $\mathcal{A}_f$ by $\overline{g(X)}$ if it is clear from the context what f is, or as $\overline{g(X)}^{[f]}$ if confusion is to be avoided.

11.2.1. **Definition.** Let $f, g \in K[X]$, $f \neq 0$. The *Hermite form* $H(f,g)$ is the symmetric bilinear form

$$H(f,g) : \mathcal{A}_f \times \mathcal{A}_f \to K : (\alpha, \beta) \mapsto \mathrm{Tr}_{\mathcal{A}_f}(\overline{g(X)} \cdot \alpha \cdot \beta).$$

We will also denote by $H(f,g)$ the associated quadratic form, i.e. the form

$$\mathcal{A}_f \to K : \alpha \mapsto \mathrm{Tr}_{\mathcal{A}_f}(\overline{g(X)}\alpha^2).$$

11.2.2. **Theorem.** *Let $f, g \in \mathbb{R}[X]$ with $f \neq 0$. Suppose that $m, n, p \in \mathbb{N}$ such that*

$$H(f,g) \cong m \times \langle 1 \rangle_{\mathbb{R}} \perp n \times \langle -1 \rangle_{\mathbb{R}} \perp p \times \langle 0 \rangle_{\mathbb{R}}.$$

Then

$$n + m = |\{x \in \mathbb{C} \mid f(x) = 0, g(x) \neq 0\}|, \text{ and}$$
$$n - m = |\{x \in \mathbb{R} \mid f(x) = 0, g(x) > 0\}| - |\{x \in \mathbb{R} \mid f(x) = 0, g(x) < 0\}|.$$

Let us denote the quantity $n+m$ in Theorem 11.2.2 by $C(f,g)$ and the quantity $n-m$ by $R(f,g)$, and note that we can compute these quantities just by knowing the coefficients of f and g. In particular, if f and g have coefficients in $\mathbb{Q}$ (or some other computable subfield of $\mathbb{R}$), then one can algorithmically compute $R(f,g)$ and $C(f,g)$.

From Theorem 11.2.2 we obtain in particular

$$C(f,1) = |\{x \in \mathbb{C} \mid f(x) = 0\}| \text{ and } R(f,1) = |\{x \in \mathbb{R} \mid f(x) = 0\}|.$$

In fact, one can count real roots of a polynomial f with any finite number of side conditions, for example within a given interval.

11.2.3. **Corollary.** *Let $f \in \mathbb{R}[X]$ non-zero, $m \in \mathbb{N}^+$, $g_1, \ldots, g_m \in \mathbb{R}[X]$. Then*

$$|\{x \in \mathbb{R} \mid f(x) = 0, g_1(x) > 0, \ldots, g_m(x) > 0\}| = \frac{1}{2^m} \sum_{\alpha \in \{1,2\}} R(f, g_1^{\alpha_1} \cdots g_m^{\alpha_m}).$$

Proof. Exercise. □

11.2.4. *Example.* Consider the polynomial $f(X) = X^3 - 3X + 1$. We use Hermite's method to determine how many real zeros this polynomial has, by computing the form $H(f,1)$.

We consider the algebra $\mathcal{A}_f = \mathbb{R}[X]/(X^3 - 3X + 1)$. A basis for this algebra is given by $\{1, \overline{X}, \overline{X}^2\}$. We have $\overline{X}^3 = 3\overline{X} - 1$ and $\overline{X}^4 = 3\overline{X}^2 - \overline{X}$. Thus,

with respect to this basis, the matrices corresponding to l_1, $l_{\overline{X}}$, and $l_{\overline{X}^2}$ (as in Definition 11.1.1) are

$$M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad M_{\overline{X}} = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{bmatrix}, \quad \text{and} \quad M_{\overline{X}^2} = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 3 & -1 \\ 1 & 0 & 3 \end{bmatrix}.$$

Denoting $\mathrm{Tr}_{\mathcal{A}_f}$ simply by Tr, we conclude that $\mathrm{Tr}(1) = 3$, $\mathrm{Tr}(\overline{X}) = 0$ and $\mathrm{Tr}(\overline{X}^2) = 6$, and hence $\mathrm{Tr}(\overline{X}^3) = \mathrm{Tr}(3\overline{X} - 1) = -3$ and $\mathrm{Tr}(\overline{X}^4) = \mathrm{Tr}(3\overline{X}^2 - \overline{X}) = 18$. We thus compute that for arbitrary $a, b, c \in \mathbb{R}$ one has

$$\begin{aligned} \mathrm{Tr}((a + b\overline{X} + c\overline{X}^2)^2) &= \mathrm{Tr}(a^2 + b^2\overline{X}^2 + c^2\overline{X}^4 + 2(ab\overline{X} + ac\overline{X}^2 + bc\overline{X}^3)) \\ &= 3a^2 + 6b^2 + 18c^2 + 12ac - 6bc \\ &= (a + 2c)^2 + 2(c + \frac{1}{2}b)^2 + \frac{1}{2}b^2. \end{aligned}$$

From this, we see that $H(f, 1) \cong \langle 1, 2, \frac{1}{2}\rangle_{\mathbb{R}} \cong 3 \times \langle 1\rangle_{\mathbb{R}}$, and by Theorem 11.2.2 we infer that f has $3 = R(f, 1)$ real zeros.

11.2.5. **Lemma.** *Let $f, f_1, f_2, g \in K[X]$ with $f, f_1, f_2 \neq 0$. Let $d = \deg(f)$.*

(1) If f_1 and f_2 are coprime, then

$$H(f_1 f_2, g) \cong H(f_1, g) \perp H(f_2, g).$$

(2) For $k \in \mathbb{N}^+$ we have

$$H(f^k, g) \cong k \cdot H(f, g) \perp (d(k-1)) \times \langle 0\rangle_K.$$

(3) For $a \in K$ we have

$$H(X - a, g) \cong \langle g(a)\rangle_K.$$

(4) If $K = \mathbb{R}$ and $a, b \in \mathbb{R}$ with $b \neq 0$, then

$$H((X-a)^2 + b^2, g) \cong \begin{cases} \mathbb{H}_{\mathbb{R}} & \text{if } g(a+bi) \neq 0 \\ \langle 0, 0\rangle_{\mathbb{R}} & \text{if } g(a+bi) = 0 \end{cases}.$$

Proof. (1): By the Chinese Remainder Theorem, we have that

$$\mathcal{A}_{f_1 f_2} \to \mathcal{A}_{f_1} \times \mathcal{A}_{f_2} : \alpha \mapsto (\overline{\alpha}^{[f_1]}, \overline{\alpha}^{[f_2]})$$

is a ring isomorphism, and in fact it is an isomorphism of $\mathbb{R}$-algebras. By parts (4) and (5) of Proposition 11.1.2 we compute that for $\alpha \in \mathcal{A}_{f_1 f_2}$ we have

$$\mathrm{Tr}_{\mathcal{A}_{f_1 f_2}}(\overline{g(X)}\alpha^2) = \mathrm{Tr}_{\mathcal{A}_{f_1}}(\overline{g(X)}^{[f_1]}(\overline{\alpha}^{[f_1]})^2) + \mathrm{Tr}_{\mathcal{A}_{f_2}}(\overline{g(X)}^{[f_2]}(\overline{\alpha}^{[f_2]})^2).$$

From this the desired statement follows.

(2): We may assume $k > 1$, otherwise there is nothing to show. Since the polynomial $X^i f(X)^j$ for $0 \leq i < d$ and $0 \leq j < k$ has degree $i + dj < dk = \deg(f^k)$, we see that the set $\{\overline{X}^i \overline{f(X)}^j \mid 0 \leq i < d, 0 \leq j < k\}$ is linearly independent in $\mathcal{A}_{f^k}$, hence (since its cardinality dk is the dimension of $\mathcal{A}_{f^k}$) a

basis. Let W_1 be the subspace of $\mathcal{A}_{f^k}$ spanned by $\overline{X}^i$ for $0 \leq i < d$ and W_2 the subspace spanned by $\overline{X}^i\overline{f(X)}^j$ for $0 \leq i < d$ and $1 \leq j < k$. We clearly have $\mathcal{A}_{f^k} = W_1 \oplus W_2$. In view of Proposition 1.2.6 it remains to show that $W_1 \perp W_2$ with respect to $H(f^k, g)$, that $H(f^k, g)|_{W_1} \cong k \cdot H(f, g)$, and that $H(f^k, g)|_{W_2} \cong (d(k-1)) \times \langle 0 \rangle_K$.

To this end, note that, for any $\alpha \in \mathcal{A}_{f^k}$, we have $(\alpha\overline{f(X)})^k = \alpha^k(\overline{f(X)})^k = 0$, and thus by part (3) of Proposition 11.1.2 we have $\mathrm{Tr}_{\mathcal{A}_{f^k}}(\alpha\overline{f(X)}) = 0$. Since any element of W_2 is a multiple of $\overline{f(X)}$, this shows both that $W_1 \perp W_2$ with respect to $H(f^k, g)$ and that $H(f^k, g)|_{W_2} \cong (d(k-1)) \times \langle 0 \rangle_K$.

Finally, to show that $H(f^k, g)|_{W_1} \cong k \cdot H(f, g)$, we need to show that, for $\alpha \in W_1$, $\mathrm{Tr}_{\mathcal{A}_{f^k}}(\alpha) = k \,\mathrm{Tr}_{\mathcal{A}_f}(\overline{\alpha}^{[f]})$. One verifies that, with respect to the (ordered) basis $1, \overline{X}, \ldots, \overline{X}^{d-1}, \overline{f(X)}, \overline{X}\overline{f(X)}, \ldots, \overline{X}^{d-1}\overline{f(X)}^{k-1}$, the map $l_{\overline{X}^i} : \mathcal{A}_{f^k} \to K$ for $0 \leq i < d$ (as in Definition 11.1.1) has matrix of the block form

$$\begin{bmatrix} M & 0 & 0 & \cdots & 0 \\ * & M & 0 & \cdots & 0 \\ * & * & M & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ * & * & \cdots & * & M \end{bmatrix}$$

where M is the $(d \times d)$ matrix of $l_{(\overline{X}^i)^{[f]}} : \mathcal{A}_f \to K$ with respect to the basis $1, \overline{X}, \ldots, \overline{X}^{d-1}$, and 0 denotes the $d \times d$ zero matrix. Hence the desired statement follows from standard computation with block diagonal matrcies.

Parts (3) and (4) are left as exercise. □

Proof of Theorem 11.2.2. We may assume without loss of generality that f is monic.

Suppose first that $f = f_1 \cdot f_2$ for coprime monic $f_1, f_2 \in \mathbb{R}[X]$ of degree at least 2. By (1) of Lemma 11.2.5 we have that $H(f_1 f_2, g) \cong H(f_1, g) \perp H(f_2, g)$. Furthermore, an element $x \in \mathbb{C}$ is a root of f if and only if it is either a root of f_1 or a root of f_2. We see that if the Theorem holds for f_1 and f_2, then it also holds for f. Hence, we reduce to considering the case where $f = \tilde{f}^k$ for some irreducible polynomial $\tilde{f} \in \mathbb{R}[X]$ and $k \in \mathbb{N}$.

By (2) we have $H(f, g) \cong kH(\tilde{f}, g) \perp (\deg(\tilde{f})(k-1)) \times \langle 0 \rangle_{\mathbb{R}}$, and since $k \in \mathbb{R}^{\times 2}$, this is further isometric to $H(\tilde{f}, g) \perp (\deg(\tilde{f})(k-1)) \times \langle 0 \rangle_{\mathbb{R}}$. Since an element $x \in \mathbb{C}$ is a root of f if and only if it is a root of $\tilde{f}$, we see that if the Theorem holds for $\tilde{f}$, then also for f. We have thus reduced to considering the case where f is an irreducible polynomial.

By the Fundamental Theorem of Algebra, the only irreducible polynomials in $\mathbb{R}[X]$ are linear polynomials and irreducible quadratic polynomials. For the linear polynomial $f(X) = X - a$ for $a \in \mathbb{R}$, we have $H(f, g) = \langle g(a) \rangle_{\mathbb{R}}$ by

Lemma 11.2.5(3), and thus

$$H(f,g) \cong \begin{cases} \langle 1 \rangle_{\mathbb{R}} & \text{if } g(a) > 0, \\ \langle -1 \rangle_{\mathbb{R}} & \text{if } g(a) < 0, \\ \langle 0 \rangle_{\mathbb{R}} & \text{if } g(a) = 0. \end{cases}$$

Since a is the only root of f in $\mathbb{C}$, this establishes the Theorem in this case.

Finally, assume $f(X)$ is irreducible quadratic, i.e. with negative discriminant. After completing the square, we may write $f(X) = (X-a)^2 + b^2$ for $a, b \in \mathbb{R}$, $b \neq 0$. Note that the roots of $f(X)$ in $\mathbb{C}$ are precisely $a+bi$ and $a-bi$; in particular, $f(X)$ has no real roots. The Theorem now follows from Lemma 11.2.5(4), using that $g(a+bi) = g(a-bi)$, since $g \in \mathbb{R}[X]$. □

11.3. **Exercises.**

(1) Prove Proposition 11.1.2, Corollary 11.2.3. Complete the proof of Lemma 11.2.5.
(2) Use Hermite's method to determine the number of real roots of the polynomial $f(X) = X^3 - 3X^2 - 2X + 5$ which are larger than $\sqrt[3]{2}$.

Index

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.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued Fields*. Springer, 2005.

[Ger08] Larry Gerstein. *Basic Quadratic Forms*. Graduate Studies in Mathematics. American Mathematical Society, 2008.

[Hat09] Jeffrey Hatley. "Hasse-Minkowski and the Local-to-Global Principle". Available at: `https://www.math.union.edu/~hatleyj/Capstone.pdf`. Apr. 2009.

[Lam05] Tsit Yuen Lam. *Introduction to quadratic forms over fields*. Vol. 67. Graduate Studies in Mathematics. American Mathematical Society, 2005.

[Mil70] John Milnor. "Algebraic K-Theory and Quadratic Forms". In: *Inventiones Mathematicae* 9 (1970), pp. 318–344.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[OVV07] Dmitri Orlov, Alexander Vishik, and Vladimir Voevodsky. "An exact sequence for $K_*^M/2$ with applications to quadratic forms". In: *Annals of Mathematics* 165.1 (2007), pp. 1–13.

[Sch18] Markus Schweighofer. *Real Algebraic Geometry, Positivity and Convexity*. https://www.math.uni-konstanz.de/ schweigh/17/real-alg-geo-16-17.pdf. Lecture notes for course in academic year 2016/2017. 2018.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic.

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