Quadratic Forms and Galois Cohomology

Quadratic Forms

Daniel Echtler

Heinrich-Heine-Universität Düsseldorf

GRK2240 Retreat 2024

Motivation

Let V be a (finite dimensional) real vector space with inner product $\langle \cdot\, , \, \cdot \rangle \colon V \times V \to \mathbb{R}$. Then we can use the inner product to define a norm

$$\begin{aligned} \| \cdot \| \colon V &\longrightarrow \mathbb{R} \\ v &\longmapsto \sqrt{\langle v, v \rangle}. \end{aligned}$$

Moverover, we can reconstruct the inner product from the norm by *polarization*:

$$\langle v, u \rangle = \frac{1}{2}\big(\|v+u\|^2 - \|v\|^2 - \|u\|^2\big).$$

Motivation

Now let K be any field (of char $K \neq 2$) and let V be a K-vector space with symmetric bilinear form $B\colon V \times V \to K$. In this case we can still consider

$$\begin{aligned} q\colon V &\longrightarrow K \\ v &\longmapsto B(v,v). \end{aligned}$$

As before we can reconstruct the bilinear from using polarization:

$$B(v,u) = \frac{1}{2}\big(q(v+u) - q(v) - q(u)\big).$$

Choosing an isomorphism $V \cong K^n$ we can identify B with a symmetric matrix $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{n\times n}(K)$ via $(v,u) \mapsto v^\top A u$. Hence q is given by

$$v \longmapsto \sum_{i,j=1}^{n} a_{i,j} \cdot v_i \cdot v_j.$$

Quadratic Forms

Definition (quadratic form)

Let K be a field of char $K \neq 2$. An *(n-ary) quadratic form* over K is a homogeneous polynomial

$$q = \sum_{i,j=1}^{n} a_{ij} T_i T_j \in K[T_1, \dots, T_n] \qquad \text{with } a_{ij} = a_{ji}$$

of degree 2.
Denote the corresponding symmetric matrix and bilinear form by $M_q = (a_{ij})_{i,j}$ and B_q respectively.
The number n is called the *dimension* and is usually denoted by $\dim q$.

Obviously one of q, M_q and B_q uniquely determines the other two. Thus we sometimes identify quadratic forms with their associated matrix or bilinear form.

Quadratic Forms

Definition (nonsingular quadratic form)

A quadratic form q is called *nonsingular*, if one of the following equivalent statements is true:

- M_q is nonsingular, i.e., $\det(M_q) \neq 0$.
- B_q is non-degenerate, i.e., $\operatorname{rad} B_q = \{x \in K^n \mid \forall_{y \in K^n} \colon B(x, y) = 0\} = \{0\}$.

A quadratic form that is not nonsingular is called *singular*.

Example

- $q = T_1^2 - T_2^2$ is nonsingular as $\det M_q = \det \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -1$.
- $q' = T_1^2 \pm 2T_1T_2 + T_2^2$ is singular as $\det M_{q'} = \det \begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix} = 0$.

Quadratic Forms

Definition (equivalence of quadratic forms)

Two n-ary quadratic forms q, q' are said to be *equivalent* if their associated matricies are congruent, i.e., if there exits an invertible matrix $C \in \mathrm{GL}_n(K)$ such that

$$M_q = C^\top M_{q'} C \quad \text{or equivalently} \quad q(x) = q'(Cx) \quad \text{for all } x \in K^n.$$

Example

Consider the two quadratic forms $q = T_1^2 - T_2^2$ and $q' = T_1 T_2$. They are equivalent as

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^\top \cdot \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Invariants of Quadratic Forms

Question

How do we see whether two (nonsingular) quadratic forms are (not) equivalent?

Answer

Invariants!

Invariants of Quadratic Forms

For two equivalent quadratic forms q, q' there is $C \in \mathrm{GL}_n(K)$ such that

$$M_q = C^\top M_{q'} C$$

and thus we have

$$\det(M_q) = \det(C^\top)\det(M_{q'})\det(C) = \det(C)^2 \det(M_{q'}).$$

So the determinant of two equivalent quadratic forms only differs by a square.

Definition (determinant)

For a nonsingular quadratic form q we define its *determinant (or discriminant)* to be

$$\det(q) = \det(M_q) \cdot (K^*)^2 \in K^*/(K^*)^2.$$

For a singular quadratic form q we sometimes use the convention

$$\det(q) = 0.$$

Invariants of Quadratic Forms

Example

Consider the two quadratic forms $q = T_1^2 + T_2^2$ and $q' = T_1^2 - T_2^2$. Then

$$\det(q) = 1 \cdot (K^*)^2 \qquad \text{and} \qquad \det(q') = -1 \cdot (K^*)^2.$$

Thus for fields where -1 is not a square (e.g. $\mathbb{R}$) these two quadratic forms are *not* equivalent. For fields with $i^2 = -1$ they are, however, equivalent:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^\top \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

Example

The two quadratic forms $q = T_1^2 + T_2^2$ and $q' = -T_1^2 - T_2^2$ have both determinant $1 \cdot (K^*)^2$. However, over $\mathbb{R}$ they are *not* equivalent.

Diagonalization of Quadratic Forms

Theorem

Every n-ary quadratic form q is eqivalent to a diagonal quadratic form, i.e., a quadratic form

$$\langle d_1, \ldots, d_n \rangle := d_1 T_1^2 + \cdots + d_n T_n^2.$$

Sketch of proof.

By writing $K^n = (\mathrm{rad}\, B_q) \oplus W$ and restricting q to W we may assume w.l.o.g. that q is nonsingular. Now let $v \in K^n$ such that $q(v) = d \neq 0$. Then we can decompose

$$K^n = K \cdot v \perp (K \cdot v)^{\perp} \qquad q \cong \langle d \rangle \perp q'.$$

Now precede by induction on $(K \cdot v)^{\perp}$ and q'. □

For diagonal forms it is easy to see that for any $a_i \in K^*$ we have

$$\langle a_1^2 \cdot d_1, \ldots, a_n^2 \cdot d_n \rangle \cong \langle d_1, \ldots, d_n \rangle.$$

Isotropic Forms

Definition (isotropic quadratic form)

A quadratic form q is said to be *isotropic* if there exists a $v \neq 0$ such that $q(v) = 0$. If no such v exists we call q *anisotropic*. A quadratic form is called *totally isotropic* if $q(v) = 0$ for all $v \neq 0$.

Obviously every singular quadratic form is isotropic. Thus we shall focus on nonsingular isotropic forms.

Theorem

Let q be a 2-ary quadratic form. The the following are equivalent:

- *q is nonsingular and isotropic.*
- *q is equivalent to $\langle 1, -1 \rangle$.*

Isotropic Forms

Theorem

Let q be a 2-ary quadratic form. The the following are equivalent:

- *q is nonsingular and isotropic.*
- *q is equivalent to $\langle 1, -1 \rangle$.*

Proof.

If $q \cong \langle 1, -1 \rangle$ it is obviously nonsingular and isotropic. Conversely, let $q \cong \langle a, b \rangle$ with $a, b \neq 0$. Then

$$q \cong \langle a, b \rangle \cong \langle a, -a \rangle \cong aT_1 T_2 \cong \langle 1, -1 \rangle.$$

□

Definition (hyperbolic form)

A quadratic form is called *hyperbolic* if it is equivalent to

$$m \cdot \langle 1, -1 \rangle = (T_1^2 - T_2^2) + \cdots + (T_{2m-1}^2 - T_{2m}^2).$$

The Cancellation and Decomposition Theorem

Theorem (Witt's Cancellation Theorem)

Let q, q_1, q_2 be arbitrary quadratic forms, if $q \perp q_1 \cong q \perp q_2$, then we already have $q_1 \cong q_2$.

Theorem (Witt's Decomposition Theorem)

Let q be a quadratic form. Then q split as an orthogonal sum

$$q \cong q_t \perp q_h \perp q_a,$$

where q_t is totally isotropic, q_h is hyperbolic, and q_a is anisotropic. Moreover, the isometry types of q_t, q_h and q_a is uniquely determined.

Hence the study of (nonsingular) quadratic forms can be reduced to the study of hyperbolic and anisotropic forms.

The Grothendieck-Witt Ring

On the set of equivalence classes of nonsingular quadratic forms $M(K)$ we have two operations:

$$\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_m \rangle = \langle a_1, \ldots, a_1, b_m, \ldots, b_m \rangle$$
$$\langle a_1, \ldots, a_n \rangle \otimes \langle b_1, \ldots, b_m \rangle = \langle a_1 b_1, \ldots, a_1 b_m \ldots, a_n b_1, \ldots, a_n b_m \rangle.$$

This turns $M(K)$ into a commutative semiring. By applying the *Grothendieck group* construction (i.e., adding additive inverses) we obtain a commutative ring.

Definition (Grothendieck-Witt ring)

We define the *Grothendieck-Witt ring* of K to be the commutative ring

$$\mathrm{GW}(K) = \mathrm{Groth}(M(K)).$$

This ring can be used to study both hyperbolic and anisotropic forms at the same time.

The Witt Ring

In order to only study the anisotropic forms we define the *Witt ring*.

Definition (Witt Ring)

The *Witt ring* of K is defined to be the quotient

$$\mathrm{W}(K) := \mathrm{GW}(K)/\mathbb{Z} \cdot [\langle 1, -1 \rangle].$$

Proposition

- *The elements of* $\mathrm{W}(K)$ *are in 1-1-correspondence with the isometry classes of all anisotropic forms.*
- *Two (nonsingular) forms* q, q' *represent the same element in* $\mathrm{W}(K)$ *if and only if* $q_a \cong q'_a$.
- *If* $\dim q = \dim q'$*, then* q *and* q' *represent the same element in* $\mathrm{W}(K)$ *if and only if* $q \cong q'$.

Presentation of the Witt Ring

Proposition

As a commutative ring, the Grothendieck-Witt ring has the presentation

$$\mathrm{GW}(K) = \Big\langle \langle a \rangle, a \in K^* \;\Big|\; \langle 1 \rangle = 1, \quad \langle a \rangle \cdot \langle b \rangle = \langle ab \rangle, \quad \langle a \rangle + \langle b \rangle = \langle a+b \rangle (1 + \langle ab \rangle) \Big\rangle.$$

To obtain a presentation for the Witt ring $\mathrm{W}(K)$ *we add the relation*

$$\langle 1 \rangle + \langle -1 \rangle = 0.$$

Proof of the third relation.

The quadratic form $\langle a \rangle + \langle b \rangle$ can be diagonalized to $\langle a+b, e \rangle$ for some $e \in K^*$. Applying det gives $(a+b)e \equiv ab \equiv (a+b)^2 ab \mod (K^*)^2$. Thus

$$\langle a \rangle + \langle b \rangle \cong \langle a+b, (a+b)ab \rangle = \langle a+b \rangle (1 + \langle ab \rangle).$$

□

The Fundamental Ideal

As $\dim\colon M(K) \to \mathbb{N}$ is a semiring homomorphism we can extend it uniquely to $\dim\colon \mathrm{GW}(K) \to \mathbb{Z}$ by defining

$$\dim(q - q') := \dim(q) - \dim(q').$$

Because $\dim(\langle 1, -1\rangle) = 2$, this induces a morphism $\dim_0\colon \mathrm{W}(K) \to \mathbb{Z}/2\mathbb{Z}$.

Definition (fundamental ideal)

The *fundamental ideal* in $\mathrm{W}(K)$ is defined to be

$$I(K) := \ker(\dim_0\colon \mathrm{W}(K) \to \mathbb{Z}/2\mathbb{Z}).$$

Powers of this ideal are denoted by $I^n(K)$.

Since dim is surjective we have an induced isomorphism

$$W(K)/I(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Pfister Forms

Let $x \in I(K)$. Then there are two quadratic forms q_1, q_2 with $x = q_1 - q_2$. By adding hyperbolic forms we may assume wlog that $\dim(q_1) = \dim(q_2)$. Let $q_1 = \langle a_1, \ldots, a_n \rangle$ and $q_2 = \langle b_1, \ldots, b_n \rangle$, then we obtain

$$x = \sum_{i=1}^{n} -1 + \langle a_i \rangle - \left(\sum_{i=1}^{n} -1 + \langle b_i \rangle \right).$$

Definition (Pfister form)

A *(1-fold) Pfister form* is defined to be $\langle\langle a \rangle\rangle := \langle -1, a \rangle \in I(K)$ for some $a \in K^*$.
More generally an *n-fold Pfister form* is defined to be

$$\langle\langle a_1, \ldots, a_n \rangle\rangle := \bigotimes_{i=1}^{n} \langle -1, a_i \rangle \qquad \text{for some } a_1, \ldots, a_n \in K^*.$$

Corollary

The ideal $I^n(K)$ is additively generated by the n-fold Pfister forms.

The Hauptsatz

Theorem (Arason-Pfister Hauptsatz)

Let q be a positive-dimensional anisotropic form. If $q \in I^n(K)$, then $\dim(q) \geq 2^n$.
Equivalently, if $q \in I^n(K)$ and $\dim(q) < 2^n$, then q is hyperbolic.

Corollary (Krull intersection property)

In the Witt ring $W(K)$ we have

$$\bigcap_{n=0}^{\infty} I^n(K) = 0.$$

Application

If we are able to show inductively that a quadratic form is trivial in every quotient

$$I^n(K)/I^{n+1}(K),$$

then it is already trivial.