Annihilating Polynomials of Excellent Quadratic Forms

Klaas-Tido Rühl

EPFL

GTEM Network - Number Fields, Lattices and Curves
Cetraro, 02 Jun - 06 Jun 2008

Introduction

Already Witt knew that the Witt ring of a field is integral. But only in 1987 did David Lewis introduce specific annihilating polynomials.

He proved that the polynomials

$$P_n := (X - n)(X - n + 2) \cdots (X + n) \in \mathbb{Z}[X], \quad n \in \mathbb{N}_0,$$

annihilate all n-dimensional quadratic forms over an arbitrary field.

This initiated the study of annihilating polynomials of quadratic forms.

Quadratic Forms

Always

- $\mathbb{N}$ does not contain 0. We use $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
- We denote by K a field, $\text{char}(K) \neq 2$.

Quadratic Forms

A quadratic space over K is a tuple (V, b) where

- V is an n-dimensional K-vector space, $n \in \mathbb{N}_0$, and
- $b : V \times V \longrightarrow K$ is a symmetric K-bilinear form.

An n-dimensional quadratic form over K, $n \in \mathbb{N}_0$, is a homogeneous element $\varphi \in K[X_1, \ldots, X_n]$ of degree 2.
We write $\dim(\varphi) = n$.

Note

The dimension is an integral part of the definition of quadratic forms.
For example $X_1^2 \in K[X_1, X_2, X_3]$ can be a quadratic form of dimension 3.

Quadratic Forms

We can consider any n-dimensional quadratic form φ over K as a map

$$\varphi : \; K^n \to K.$$

The bilinear form associated to φ is defined as

$$b_\varphi : \; K^n \times K^n \longrightarrow K, \; (v,w) \longmapsto \frac{1}{2}(\varphi(v+w) - \varphi(v) - \varphi(w)).$$

The tuple (K^n, b_φ) is called quadratic space associated to φ.

The matrix associated to φ is defined as

$$A_\varphi \; := \; (b_\varphi(e_i, e_j))_{i,j=1,\ldots,n},$$

where $\{e_1, \ldots, e_n\}$ is the standard basis of K^n.

Isometries

Definition

Two quadratic spaces (V_1, b_1) and (V_2, b_2) over K are called isometric if there exists a K-vector space isomorphism $T : V_1 \to V_2$ such that

$$b_1(v, w) \ = \ b_2(Tv, Tw) \qquad \forall \ v, w \in V_1.$$

Definition

Two quadratic forms φ and ψ over K are isometric if their associated quadratic spaces are isometric.
We write $\varphi \cong \psi$.

Diagonal Forms

Let $a_1, \ldots, a_n \in K$. We write

$$\langle a_1, \ldots, a_n \rangle \;:=\; a_1 X_1^2 + \cdots + a_n X_n^2 \;\in\; K[X_1, \ldots, X_n].$$

These forms are called diagonal forms.

Theorem

Let φ be an n-dimensional quadratic form over K.
Then there exist $a_1, \ldots, a_n \in K$ such that

$$\varphi \;\cong\; \langle a_1, \ldots, a_n \rangle.$$

We are really only interested in quadratic forms up to isometry.
Hence it suffices to consider only diagonal forms.

Operations

There exists an orthogonal sum of two quadratic forms such that

$$\langle a_1, \dots, a_n \rangle \perp \langle b_1, \dots, b_m \rangle \; = \; \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle.$$

There exists a tensor product of two quadratic forms such that

$$\langle a_1, \dots, a_n \rangle \otimes \langle b_1, \dots, b_m \rangle \; \cong \; \langle a_1 b_1, \dots, a_1 b_m, a_2 b_1, \dots, a_n b_m \rangle.$$

Note

The analogous operations for quadratic spaces are defined as follows

$$\begin{aligned} (V_1, b_1) \perp (V_2, b_2) \quad &:= \quad (V_1 \oplus V_2, b_1 + b_2) \qquad \text{and} \\ (V_1, b_1) \otimes (V_2, b_2) \quad &:= \quad (V_1 \otimes_K V_2, b_1 b_2). \end{aligned}$$

Non-degenerate Forms

Definition

A quadratic form φ is non-degenerate (or regular) if $\det(A_\varphi) \neq 0$.

Henceforth we will only consider non-degenerate forms.

Clear: $\varphi \cong \langle a_1, \ldots, a_n \rangle$ is non-degenerate $\iff$ $a_1, \ldots, a_n \in K^*$.

Definition

The determinant of a quadratic form $\varphi \cong \langle a_1, \ldots, a_n \rangle$ is defined as

$$\det(\varphi) \ := \ a_1 \cdots a_n (K^*)^2 \ \in \ K^*/(K^*)^2.$$

The determinant of a quadratic forms is well-defined, since we consider it in $K^*/(K^*)^2$ instead of in K^*.

Isotropic Forms

Definition

A quadratic form φ over K is called isotropic if there exists $0 \neq v \in K^n$ such that $\varphi(v) = 0$.
Otherwise φ is called anisotropic.

By definition the zero-form over K is anisotropic.
It is clear that every non-degenerate 1-dimensional form over K is anisotropic.

Theorem

Up to isometry there exists only one (non-degenerate) 2-dimensional isotropic form over K,
i.e. the hyperbolic plane $\mathbb{H} := \langle 1, -1 \rangle \cong \langle a, -a \rangle$ for all $a \in K^*$.

Hyperbolic Forms

Let φ be a quadratic form over K.

We use the notation

$$m \times \varphi \;:=\; \underbrace{\varphi \perp \ldots \perp \varphi}_{m\text{-times}}.$$

Definition

A quadratic form φ over K is called hyperbolic if there exists an $m \in \mathbb{N}_0$ such that

$$\varphi \;\cong\; m \times \mathbb{H}.$$

Witt decomposition

Theorem

Let φ be a form over K. There exists a decomposition

$$\varphi \cong \varphi_{\text{an}} \perp (i(\varphi) \times \mathbb{H})$$

such that

- φ_{an} is anisotropic and uniquely determined up to isometry and
- $i(\varphi)$ is uniquely determined.

Definition

The form φ_{an} is called anisotropic kernel of φ,
and $i(\varphi)$ is the Witt index of φ.

The Witt-Grothendieck Ring

The isometry class of a quadratic form φ over K will be denoted by $[\varphi]$.

The isometry classes of quadratic forms over K form a semi-ring $\widehat{W}^+(K)$ with addition

$$[\varphi] + [\psi] \; := \; [\varphi \perp \psi] \, .$$

and multiplication

$$[\varphi] \cdot [\psi] \; := \; [\varphi \otimes \psi] \, .$$

By applying the Grothendieck Construction for semi-groups to $\widehat{W}^+(K)$ we obtain the Witt-Grothendieck Ring $\widehat{W}(K)$.

The Witt-Grothendieck Ring

The elements of $\widehat{W}(K)$ are formal differences

$$[\varphi] - [\psi]$$

and there exists an up to isometry unique anisotropic form χ over K and a unique $m \in \mathbb{N}$ such that

$$[\varphi] - [\psi] \; = \; [\chi] \pm [m \times \mathbb{H}] \, .$$

We extend the notion of dimension to a ring homomorphism

$$\dim([\varphi] - [\psi]) \; := \; \dim(\varphi) - \dim(\psi) \; \in \; \mathbb{Z}.$$

The Witt Ring

Denote by $\mathcal{H}$ the principal ideal of $\widehat{W}(K)$ generated by $[\mathbb{H}]$.
The Witt Ring of K is defined as

$$W(K) := \widehat{W}(K)/\mathcal{H}.$$

If φ is a quadratic form over K, then $\{\varphi\}$ will denote its equivalence class in $W(K)$.
We write $\psi \sim \varphi$ if $\psi \in \{\varphi\}$.

Note

The elements of $W(K)$ classify anisotropic quadratic forms over K.

Example

Let φ be a quadratic form over $\mathbb{R}$.
There exist $r, s \in \mathbb{N}_0$ such that

$$\varphi \cong r \times \langle 1 \rangle \perp s \times \langle -1 \rangle.$$

We have

$$\dim(\varphi) \;=\; r + s \qquad \text{and} \qquad \operatorname{sign}(\varphi) \;=\; r - s,$$

where $\operatorname{sign}(\varphi)$ denotes the signature.
Since $[\langle -1 \rangle]^2 = 1$, it follows that

$$\widehat{W}(\mathbb{R}) \;\cong\; \mathbb{Z}[(\{1, -1\}, \cdot)].$$

Since φ is anisotropic if and only if $r = 0$ or $s = 0$, we obtain

$$W(\mathbb{R}) \;\cong\; \mathbb{Z}.$$

Annihilating Polynomials

Annihilating Polynomials

Let R be a unitary, commutative ring, and let $\iota : \mathbb{Z} \to R$ be the canonical ring homomorphism.

Definition

A polynomial $P = z_n X^n + \cdots + z_1 X + z_0 \in \mathbb{Z}[X]$ is called annihilating polynomial of $x \in R$, if

$$P(x) \ := \ \iota(z_n)x^n + \cdots + \iota(z_1)x + \iota(z_n) \ = \ 0 \ \in \ R.$$

Definition

The annihilating ideal of $x \in R$ is defined as

$$\mathrm{Ann}_x \ := \ \{P \in \mathbb{Z}[X] \mid P(x) = 0\} \ \subset \ \mathbb{Z}[X].$$

Annihilating Polynomials

In our case we have to consider the canonical ring homomorphisms

$$\iota_1 : \quad \mathbb{Z} \longrightarrow \widehat{W}(K) \quad \text{and} \quad \iota_2 : \quad \mathbb{Z} \longrightarrow W(K)$$

defined for $m \in \mathbb{N}$ by

$$m \longmapsto [m \times \langle 1 \rangle] \quad \text{resp.} \quad m \longmapsto \{m \times \langle 1 \rangle\}$$

Usually we will simply write m for its image via ι_1 and ι_2 in $\widehat{W}(K)$ resp. $W(K)$.

Hurrelbrink's method

Let $G := K^*/(K^*)^2$ be the square class group of K.
For $a \in K^*$, denote by $\overline{a}$ its image in G.

There exists a canonical ring homomorphism

$$\pi_1 : \mathbb{Z}[G] \longrightarrow \widehat{W}(K)$$

defined by

$$\overline{a_1} + \cdots + \overline{a_n} \longmapsto [\langle a_1, \ldots, a_n \rangle] .$$

If $\pi : \widehat{W}(K) \to W(K)$ is the canonical projection, then we obtain a canonical homomorphism

$$\pi_2 := \pi \circ \pi_1 : \mathbb{Z}[G] \longrightarrow W(K).$$

Hurrelbrink's method

Let φ be a quadratic form over K, and let $f \in \pi_1^{-1}([\varphi]) \subset \mathbb{Z}[G]$.

If $P \in \mathbb{Z}[X]$ is an annihilating polynomial of f.
$\Longrightarrow$ P is an annihilating polynomial of $[\varphi]$.
$\Longrightarrow$ P is an annihilating polynomial of $\{\varphi\}$.

But Ann_f is easy to calculate.

Hurrelbrink's method

Let $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ be the set of ring homomorphisms $\mathbb{Z}[G] \to \mathbb{Z}$.

The set

$$S_f \;:=\; \{\chi(f) \mid \chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})\}$$

is finite.

Hence we can define

$$P_f \;:=\; \prod_{\chi(f) \in S_f} (X - \chi(f)).$$

Then

$$\mathrm{Ann}_f \;=\; (P_f) \;\subset\; \mathbb{Z}[G].$$

The Quadratic Form Case

In the case of quadratic forms, the situation is considerably more complicated.

Let R be either $\widehat{W}(K)$ or $W(K)$, and let $x \in R$.
Set

$$S_x^{\text{sign}} := \{\chi(x) \mid \chi \in \text{Hom}(R, \mathbb{Z})\} \quad \text{and} \quad Q_x := \prod_{\chi(x) \in S_x^{\text{sign}}} (X - \chi(x)).$$

Theorem

The greatest common divisor of the elements of Ann_x is equal to Q_x.
Furthermore $Q_x(x) \in R$ is a 2-torsion element.

The Quadratic Form Case

Definition

The polynomial Q_x from the previous theorem is called embracing polynomial or signature polynomial.

The name "embracing polynomial" was chosen in view of the fact, that we have $\mathrm{Ann}_x \subset (Q_x)$, and (Q_x) is the unique minimal principal ideal containing Ann_x

The name "signature polynomial" stems from the fact, that $\mathrm{Hom}(W(K), \mathbb{Z})$ is just the set of signature homomorphisms.

The Quadratic Form Case

In general it is difficult to make statements about the gestalt of annihilating polynomials of quadratic forms.

But it is possible to give full sets of generators for the annihilating ideal.

Proposition

There exist monic polynomials $Q_0 = 1, Q_1, \ldots, Q_r \in \mathbb{Z}[X]$ and $k_0, \ldots, k_{r-1}, k_r = 0 \in \mathbb{N}_0$ with

(i) $k_0 > \cdots > k_{r-1} > k_r$ and

(ii) $\deg(Q_0) < \deg(Q_1) < \cdots < \deg(Q_r)$

such that

$$\{2^{k_0} Q_x,\ 2^{k_1} Q_1 Q_x,\ \ldots,\ 2^{k_{r-1}} Q_{r-1} Q_x,\ Q_r Q_x\}$$

forms a full set of generators for Ann_x.

Examples

First Examples

Let φ be a quadratic form over K of dimension n.

- K **Pythagorean.**
  Then $\widehat{W}(K)$ and $W(K)$ are torsion free.
  $\Longrightarrow$ We have $Q_{[\varphi]}([\varphi]) = 0$ and $Q_{\{\varphi\}}(\{\varphi\}) = 0$
  and therefore $\mathrm{Ann}_{[\varphi]} = (Q_{[\varphi]})$ and $\mathrm{Ann}_{\{\varphi\}} = (Q_{\{\varphi\}})$.
- K **not formally real.**
  Then an element of $\widehat{W}(K)$ is torsion if and only if its dimension is 0.
  Furthermore any element of $W(K)$ is torsion.
  $\Longrightarrow$ $Q_\varphi = X - n \in \mathbb{Z}[X]$ and $Q_{\{\varphi\}} = 1$.

The Real Numbers

Let φ be a quadratic form over $\mathbb{R}$ with $n = \dim(\varphi)$.

It is well known, that $\mathrm{Hom}(\widehat{W}(\mathbb{R}), \mathbb{Z}) = \{\dim, \mathrm{sign}\}$ and $\mathrm{Hom}(W(\mathbb{R}), \mathbb{Z}) = \{\mathrm{sign}\}$.

Set $s := \mathrm{sign}(\varphi)$.

Since $\mathbb{R}$ is Pythagorean, we obtain

$$\mathrm{Ann}_{[\varphi]} = \begin{cases} (X - n) & \text{if } s = n, \\ ((X - s)(X - n)) & \text{otherwise,} \end{cases}$$

and

$$\mathrm{Ann}_{\{\varphi\}} = (X - s).$$

Local Fields

Let K be a local field with finite residue field.

It is possible to completely classify the elements of $\widehat{W}(K)$ with the help of the following three invariants.

1. The dimension:
$$\dim : \widehat{W}(K) \longrightarrow \mathbb{Z}.$$
2. The discriminant:
$$d : \widehat{W}(K) \longrightarrow K^*/(K^*)^2, \ [\varphi] \longmapsto (-1)^{\frac{n(n-1)}{2}} \det(\varphi),$$
where n is the dimension of φ.
3. The Clifford invariant (also called Witt invariant):
$$c : \widehat{W}(K) \longrightarrow {}_2\mathrm{Br}(K).$$

Local Fields

With the help of calculations involving these three invariants we can describe the annihilating ideal of any given quadratic form over K.

Proposition

Let φ be a quadratic form over K, $n := \dim(\varphi)$, $\varphi \ncong n \times \langle 1 \rangle$.
Then a complete and minimal set of generators for $\mathrm{Ann}_{[\varphi]} \subset \mathbb{Z}[X]$ is given as follows:

$$\mathrm{Ann}_{[\varphi]} = \begin{cases} (2(X-n), (X-n)^2) & \text{if } d(\varphi) \text{ is a sum of two squares in } K, \\ (4(X-n), (X-n+2)(X-n)) & \text{otherwise.} \end{cases}$$

If $\varphi \cong n \times \langle 1 \rangle$, then $\mathrm{Ann}_{[\varphi]} = (X-n)$.

Remark

Now the previous examples and the Hasse-Minkowski Theorem can be used to obtain a similar result for global fields.

Furthermore it is of course possible to obtain analogous results for $\mathrm{Ann}_{\{\varphi\}}$, where φ is a quadratic form over a local or global field K.

But these results demand for even more case distinctions and do not yield any additional knowledge. Therefore we leave them out here.

Annihilating Polynomials of Excellent Forms

Notation

Two quadratic forms φ and ψ over K are called similar if there exists an $a \in K^*$ such that $\varphi \cong a\psi$.

A quadratic form ψ over K is called a subform of a form φ over K if there exists a form χ over K such that $\varphi \cong \psi \perp \chi$.

Pfister Forms

Definition

A quadratic form φ over K is called a k-fold Pfister form, $k \in \mathbb{N}_0$, if there exist $a_1, \ldots, a_k \in K^*$ such that

$$\varphi \;\cong\; \langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_k \rangle.$$

We write $\langle\langle a_1, \ldots, a_k \rangle\rangle \;:=\; \bigotimes_{i=1}^{k} \langle 1, a_i \rangle$.

Note

A Pfister form φ is isotropic if and only if it is hyperbolic.

In other words: A Pfister form is either anisotropic or hyperbolic.

Annihilating Polynomials of Pfister Forms

We use Hurrelbrink's method.

Let $\varphi \cong b\langle 1, a_1\rangle \otimes \cdots \otimes \langle 1, a_k\rangle$ be similar to a k-fold Pfister form over K, $k \in \mathbb{N}_0$.
Then

$$f \ := \ \overline{b}(1+\overline{a_1})\cdots(1+\overline{a_k}) \in \mathbb{Z}[G]$$

is a preimage of $[\varphi]$ in $\mathbb{Z}[G]$, where $G = {}^{K^*}/(K^*)^2$.

Let $\chi \in \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$. We have

$$\chi(f) \ = \ \begin{cases} 2^k & \text{if } \chi(\overline{a_i}) = 1 \text{ for all } i, \text{ and } \chi(\overline{b}) = 1, \\ -2^k & \text{if } \chi(\overline{a_i}) = 1 \text{ for all } i, \text{ and } \chi(\overline{b}) = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Annihilating Polynomials of Pfister Forms

As a consequence we obtain the following result.

Theorem

For $k \in \mathbb{N}_0$ the polynomial

$$(X - 2^k)X(X + 2^k) = X(X^2 - 2^{2k}) \in \mathbb{Z}[X]$$

annihilates $[\varphi]$ and $\{\varphi\}$,
where φ is similar to a k-fold Pfister form
over any field K.

Pfister Neighbours

Definition

Let τ be a Pfister form over K. A quadratic form φ over K is called Pfister neighbour of τ if

- φ is similar to a subform of τ, and
- $\dim(\varphi) > \frac{1}{2}\dim(\tau)$.

Let φ be a Pfister neighbour of τ.
Then there exists an $a \in K^*$ and a form ψ over K such that

$$a\tau \;\cong\; \varphi \perp \psi.$$

The form ψ is called the complement of φ.

Annihilating Polynomials of Pfister Neighbours

Theorem

Let φ be a Pfister neighbour over K with complement ψ.
Let Q be an annihilating polynomial of $[\psi]$ (resp. $\{\varphi\}$).
Then

$$Q \cdot (X^2 - n^2) \in \mathbb{Z}[X]$$

is an annihilating polynomial of $[\varphi]$ (resp. $\{\varphi\}$).

Excellent Quadratic Forms

Definition

Forms of dimension 0 and 1 are excellent.
If φ is a form over K with $\dim(\varphi) > 1$, then φ is excellent if φ is a Pfister neighbour whose complement is excellent.

Let φ be an excellent form over K.
Then there exists a sequence of forms

$$\varphi = \chi_0,\ \chi_1,\ \ldots, \chi_r$$

such that

- χ_{i-1} is a Pfister neighbour with complement χ_i for $i = 1, \ldots, r$, and
- $\dim(\chi_r) \in \{0, 1\}$.

Excellent Quadratic Forms

Let φ be excellent over K, and let $\chi_0, \ldots, \chi_r$ be the sequence as defined above.

Definition

The form χ_k is called the *k-th complement* of φ.

Annihilating Polynomials of Excellent Forms

Theorem

Let φ be an excellent form over K of dimension n, and let $n = n_0 > \cdots > n_r$ be the dimensions of the higher complements of φ. Then

$$E_n := \begin{cases} X(X^2 - n_{r-1}^2)\cdots(X^2 - n_1^2)(X^2 - n^2) & \text{for } n \text{ even,} \\ (X^2 - 1^2)(X^2 - n_{r-1}^2)\cdots(X^2 - n_1^2)(X^2 - n^2) & \text{for } n \text{ odd,} \end{cases}$$

is an annihilating polynomial of $[\varphi]$ and $\{\varphi\}$.

Remark

There exists a field K such that for any $n \in \mathbb{N}_0$ there exists an excellent form φ over K with $\mathrm{Ann}_{[\varphi]} = \mathrm{Ann}_{\{\varphi\}} = (E_n)$.

The End.