Quadratic forms over $\mathbb{Q}_p$

Kaniuar Bacho

Rheinische Friedrich-Wilhelms-Universität Bonn

WiSe 20/21

Table of contents

We saw in the last talk:

Theorem

Every quadratic module (V, Q) has an orthogonal basis.

We saw in the last talk:

Theorem

Every quadratic module (V, Q) has an orthogonal basis.

Definition

Two orthogonal bases

$$e = (e_1, \ldots, e_n) \text{ and } e' = (e'_1, \ldots, e'_n)$$

of V are called *contiguous* if they have an element in common (i.e. if there exist i and j such that $e_i = e'_j$.)

Reminder: We restricted ourselves to the case V is finite dimensional and $\mathrm{char}(k) \neq 2$.

Lemma

Let (V, Q) be a non-degenerate quadratic module of dimension $n \geq 3$, and let $e = (e_1, ..., e_n)$ and $e' = (e'_1, ..., e'_n)$ be two orthogonal bases of V. Then there exists a finite sequence $e^{(0)}, e^{(1)}, ..., e^{(m)}$ of orthogonal bases of V such that $e^{(0)} = e$ and $e^{(m)} = e'$ and $e^{(i)}$ is contiguous with $e^{(i+1)}$ for $0 \leq i < m$.

Lemma

Let (V, Q) be a non-degenerate quadratic module of dimension $n \geq 3$, and let $e = (e_1, ..., e_n)$ and $e' = (e'_1, ..., e'_n)$ be two orthogonal bases of V. Then there exists a finite sequence $e^{(0)}, e^{(1)}, ..., e^{(m)}$ of orthogonal bases of V such that $e^{(0)} = e$ and $e^{(m)} = e'$ and $e^{(i)}$ is contiguous with $e^{(i+1)}$ for $0 \leq i < m$.

Proof.
Case 1: $\langle e_1, e_1\rangle \cdot \langle e'_1, e'_1\rangle - \langle e_1, e'_1\rangle^2 \neq 0$.
This condition is equivalent to: $P = ke_1 + ke'_1$ is a two dimensional non-degenerate subspace of V.
From talk 4 we know there exist ϵ_2 and ϵ'_2, s.t.

$$P = ke_1 \mathbin{\widehat{\oplus}} k\epsilon_2 \text{ and } P = ke'_1 \mathbin{\widehat{\oplus}} k\epsilon'_2.$$

Let H be the orthogonal complement of P with an orthogonal basis $(e''_3, ..., e''_n)$; since P is non-degenerate, we have $V = H \mathbin{\widehat{\oplus}} P$. Then the following chain of orthogonal bases

$$e \to (e_1, \epsilon_2, e''_3, ..., e''_n) \to (e'_1, \epsilon'_2, e''_3, ..., e''_n) \to e'$$

does the job.

Case 2: $\langle e_1, e_1\rangle \cdot \langle e_2', e_2'\rangle - \langle e_1, e_2'\rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.

Case 2: $\langle e_1, e_1 \rangle \cdot \langle e_2', e_2' \rangle - \langle e_1, e_2' \rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.
Case 3: $\langle e_1, e_1 \rangle \cdot \langle e_i', e_i' \rangle - \langle e_1, e_i' \rangle^2 = 0$ for $i = 1, 2$.
Note that $\langle e_1, e_i' \rangle \neq 0$ for $i = 1, 2$, otherwise e_1 or e_1' would be a non-zero element in $rad(V) = 0$.
First we will prove the following lemma:
There exists $x \in k$ s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane.

Case 2: $\langle e_1, e_1\rangle \cdot \langle e_2', e_2'\rangle - \langle e_1, e_2'\rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.
Case 3: $\langle e_1, e_1\rangle \cdot \langle e_i', e_i'\rangle - \langle e_1, e_i'\rangle^2 = 0$ for $i = 1, 2$.
Note that $\langle e_1, e_i'\rangle \neq 0$ for $i = 1, 2$, otherwise e_1 or e_1' would be a non-zero element in $rad(V) = 0$.
First we will prove the following lemma:
There exists $x \in k$ s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane.
We have $\langle e_x, e_x\rangle = \langle e_1', e_1'\rangle + x^2\langle e_2', e_2'\rangle$. We must take x^2 distinct from $-\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$. Moreover e_x generates with e_1 a non-degenerate plane iff $\langle e_1, e_1\rangle \cdot \langle e_x, e_x\rangle - \langle e_1, e_x\rangle^2 \neq 0$. But the left hand side is $-2x\langle e_1, e_1'\rangle\langle e_1, e_2'\rangle$.
Hence the conditions are equivalent to $x \neq 0$ and $x^2 \neq -\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$.

<u>Case 2:</u> $\langle e_1, e_1\rangle \cdot \langle e_2', e_2'\rangle - \langle e_1, e_2'\rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.
<u>Case 3:</u> $\langle e_1, e_1\rangle \cdot \langle e_i', e_i'\rangle - \langle e_1, e_i'\rangle^2 = 0$ for $i = 1, 2$.
Note that $\langle e_1, e_i'\rangle \neq 0$ for $i = 1, 2$, otherwise e_1 or e_1' would be a non-zero element in $rad(V) = 0$.
First we will prove the following lemma:
There exists $x \in k$ s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane.
We have $\langle e_x, e_x\rangle = \langle e_1', e_1'\rangle + x^2\langle e_2', e_2'\rangle$. We must take x^2 distinct from $-\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$. Moreover e_x generates with e_1 a non-degenerate plane iff $\langle e_1, e_1\rangle \cdot \langle e_x, e_x\rangle - \langle e_1, e_x\rangle^2 \neq 0$. But the left hand side is $-2x\langle e_1, e_1'\rangle\langle e_1, e_2'\rangle$.
Hence the conditions are equivalent to $x \neq 0$ and $x^2 \neq -\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$.
If $|k| \geq 4$, we are done with the lemma.

Case 2: $\langle e_1, e_1\rangle \cdot \langle e_2', e_2'\rangle - \langle e_1, e_2'\rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.
Case 3: $\langle e_1, e_1\rangle \cdot \langle e_i', e_i'\rangle - \langle e_1, e_i'\rangle^2 = 0$ for $i = 1, 2$.
Note that $\langle e_1, e_i'\rangle \neq 0$ for $i = 1, 2$, otherwise e_1 or e_1' would be a non-zero element in $rad(V) = 0$.
First we will prove the following lemma:
There exists $x \in k$ s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane.
We have $\langle e_x, e_x\rangle = \langle e_1', e_1'\rangle + x^2\langle e_2', e_2'\rangle$. We must take x^2 distinct from $-\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$. Moreover e_x generates with e_1 a non-degenerate plane iff $\langle e_1, e_1\rangle \cdot \langle e_x, e_x\rangle - \langle e_1, e_x\rangle^2 \neq 0$. But the left hand side is $-2x\langle e_1, e_1'\rangle\langle e_1, e_2'\rangle$.
Hence the conditions are equivalent to $x \neq 0$ and $x^2 \neq -\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$.
If $|k| \geq 4$, we are done with the lemma.
The case $|k| = 2$ can not appear, since $\mathrm{char}(k) \neq 2$.

Case 2: $\langle e_1, e_1\rangle \cdot \langle e_2', e_2'\rangle - \langle e_1, e_2'\rangle^2 \neq 0$.
Same proof as above, just replace e_1' by e_2'.
Case 3: $\langle e_1, e_1\rangle \cdot \langle e_i', e_i'\rangle - \langle e_1, e_i'\rangle^2 = 0$ for $i = 1, 2$.
Note that $\langle e_1, e_i'\rangle \neq 0$ for $i = 1, 2$, otherwise e_1 or e_1' would be a non-zero element in $rad(V) = 0$.
First we will prove the following lemma:
There exists $x \in k$ s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane.
We have $\langle e_x, e_x\rangle = \langle e_1', e_1'\rangle + x^2\langle e_2', e_2'\rangle$. We must take x^2 distinct from $-\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$. Moreover e_x generates with e_1 a non-degenerate plane iff $\langle e_1, e_1\rangle \cdot \langle e_x, e_x\rangle - \langle e_1, e_x\rangle^2 \neq 0$. But the left hand side is $-2x\langle e_1, e_1'\rangle\langle e_1, e_2'\rangle$.
Hence the conditions are equivalent to $x \neq 0$ and $x^2 \neq -\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle}$.
If $|k| \geq 4$, we are done with the lemma.
The case $|k| = 2$ can not appear, since $\mathrm{char}(k) \neq 2$.
Let us investigate the case $|k| = 3$, so $k = \mathbb{F}_3$. As $\langle e_1, e_i'\rangle \neq 0$ we get $\langle e_1, e_i'\rangle^2 = 1$. So the condition in case 3 is equivalent to $\langle e_1, e_1\rangle \cdot \langle e_i', e_i'\rangle = 1$.
Hence $-\frac{\langle e_1', e_1'\rangle}{\langle e_2', e_2'\rangle} = -1$, so $x = 1$ does the job.

Back to the origin problem, take x s.t. $e_x = e_1' + xe_2'$ is non-isotropic and generates with e_1 a non-degenerate plane. Since e_x is non-isotropic, there exists e_2'' s.t. (e_x, e_2'') is an orthogonal basis of $ke_1' \widehat{\oplus} ke_2'$. Consider the orthogonal basis $e'' = (e_x, e_2'', e_3', ..., e_n')$ of V, which is contiguous to e'. Now we are in case 1 and can relate e to e''. $\square$

We will see that this lemma is important to show the welldefinedness of a new invariant that we will introduce.

Recap the last talks

Let us take a look back at the results, that will be important in this talk.

Recap the last talks

Let us take a look back at the results, that will be important in this talk.

Hilbert symbol

Let k denote $\mathbb{R}$ or $\mathbb{Q}_p$ and $a, b \in k^\times$. Then

$$(a, b) \mapsto \begin{cases} 1, & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a non-trivial solution } (x, y, z) \in k^3; \\ -1, & \text{otherwise.} \end{cases}$$

We saw the following identities:
$(a, b) = (b, a)$, $(a, c^2) = 1$, $(a, b) = (a, -ab)$, $(a, bc) = (a, b)(a, c)$ and the Hilbert symbol is non-degenerate (i.e. if $(a, b) = 1$ for all b, then a is a square in $k^\times$).

Recap the last talks

Solutions of quadratic forms

Let $g = g(x_1, ..., x_{n-1})$ be a non-degenerate quadratic form and let $a \in k^\times$. TFAE

(i) The form g represents a.

(ii) We have $g \sim h \dotplus ax_{n-1}^2$, where h is a form in $n-2$ variables.

(iii) The form $f = g \dot{-} ax_n^2$ represents 0.

Solutions of quadratic forms

Let g and h be non-degenerate forms of rank ≥ 1 and $f = g \dot{-} h$. TFAE

(i) The form f represents 0.

(ii) There exists $a \in k^\times$ which is represented by g and h.

(iii) There exists $a \in k^\times$ s.t. $g \dot{-} az^2$ and $h \dot{-} az^2$ represents 0.

Hasse invariant

From now on we will fix a prime number p, $k = \mathbb{Q}_p$ and assume that all quadratic modules are non-degenerate.
We already defined the discriminant $d(Q)$ of a quadratic module (V, Q) of rank n. It is an element in $k^\times / k^{\times 2}$; let $e = (e_1, ..., e_n)$ be an orthogonal basis of V, then $a_i := \langle e_i, e_i \rangle$ and $d(Q) = a_1 \cdots a_n$ (in $k^\times / k^{\times 2}$).

Definition

Now define $\epsilon(e) = \prod_{i<j} (a_i, a_j) \in \{-1, +1\}$ to be the *Hasse invariant* of (V, Q).

Theorem

The number $\epsilon(e)$ does not depend on the choice of the orthogonal basis e.

Proof. If $n = 1$, we have $\epsilon(e) = 1$.

Hasse invariant

From now on we will fix a prime number p, $k = \mathbb{Q}_p$ and assume that all quadratic modules are non-degenerate.
We already defined the discriminant $d(Q)$ of a quadratic module (V, Q) of rank n. It is an element in $k^\times/k^{\times 2}$; let $e = (e_1, ..., e_n)$ be an orthogonal basis of V, then $a_i := \langle e_i, e_i \rangle$ and $d(Q) = a_1 \cdots a_n$ (in $k^\times/k^{\times 2}$).

Definition

Now define $\epsilon(e) = \prod_{i<j} (a_i, a_j) \in \{-1, +1\}$ to be the *Hasse invariant* of (V, Q).

Theorem

The number $\epsilon(e)$ does not depend on the choice of the orthogonal basis e.

Proof. If $n = 1$, we have $\epsilon(e) = 1$.
If $n = 2$, then $\epsilon(e) = 1$ iff $(a_1, a_2) = 1$ iff $Z^2 - a_1X^2 - a_2Y^2$ represents 0 iff $a_1X^2 + a_2Y^2$ represents 1 iff there is a $v \in V$, s.t. $Q(v) = 1$.

Hasse invariant

But the last condition is independent of the choice of an orthogonal basis, hence the result.

Hasse invariant

But the last condition is independent of the choice of an orthogonal basis, hence the result.
For $n \geq 3$ we will use induction on n and use our lemma in the first part of the talk. It suffices to prove $\epsilon(e) = \epsilon(e')$, when e and e' are contiguous. By the symmetry of the Hilbert symbol $\epsilon(e)$ does not change if we permute e_1 with other basis elements. So we can suppose $e' = (e'_1, ..., e'_n)$ with $e_1 = e'_1$. Write $a'_i = \langle e'_i, e'_i \rangle$, then $a'_1 = a_1$. We get the following equation chain: $\epsilon(e) = (a_1, a_2 \cdots a_n) \cdot \prod_{2 \leq i < j} (a_i, a_j) = (a_1, d(Q)a_1) \cdot \prod_{2 \leq i < j} (a_i, a_j)$. Similarly $\epsilon(e') = (a_1, d(Q)a_1) \cdot \prod_{2 \leq i < j} (a'_i, a'_j)$. Now apply the induction hypothesis to the orthogonal complement of e_1 and e'_1 to get $\prod_{2 \leq i < j} (a_i, a_j) = \prod_{2 \leq i < j} (a'_i, a'_j)$. □

From now on we will write $\epsilon(Q)$ instead of $\epsilon(e)$.

Hasse invariant

Lemma

a) The number of elements in the $\mathbb{F}_2$-vector space $k^\times/k^{\times 2}$ is 2^r with $r = 2$ if $p \neq 2$ and $r = 3$ if $p = 2$.
b) If $a \in k^\times/k^{\times 2}$ and $\epsilon = \pm 1$, let $H_a^\epsilon = \{x \in k^\times/k^{\times 2} \mid (x, a) = \epsilon\}$. If $a = 1$, then H_a^1 has 2^r elements and $H_a^{-1} = \emptyset$. If $a \neq 1$, then H_a^ϵ has 2^{r-1} elements.
c) Let $a, a' \in k^\times/k^{\times 2}$ and $\epsilon, \epsilon' = \pm 1$; assume H_a^ϵ and $H_{a'}^{\epsilon'}$ are non-empty. Then $H_a^\epsilon \cap H_{a'}^{\epsilon'} = \emptyset$ iff $a = a'$ and $\epsilon = -\epsilon'$.

Proof.
a) This follows immediate from talk 2, where we proved $k^\times/k^{\times 2} \simeq (\mathbb{F}_2)^r$.

b) The case $a = 1$ is trivial. Assume $a \neq 1$, then by degeneracy the homomorphism $b \mapsto (a, b)$ carries $k^\times/k^{\times 2}$ onto $\{-1, +1\}$ with kernel H_a^1 of dimension $r - 1$.

Hasse invariant

Lemma

a) The number of elements in the $\mathbb{F}_2$-vector space $k^\times/k^{\times 2}$ is 2^r with $r = 2$ if $p \neq 2$ and $r = 3$ if $p = 2$.
b) If $a \in k^\times/k^{\times 2}$ and $\epsilon = \pm 1$, let $H_a^\epsilon = \{x \in k^\times/k^{\times 2} \mid (x,a) = \epsilon\}$. If $a = 1$, then H_a^1 has 2^r elements and $H_a^{-1} = \emptyset$. If $a \neq 1$, then H_a^ϵ has 2^{r-1} elements.
c) Let $a, a' \in k^\times/k^{\times 2}$ and $\epsilon, \epsilon' = \pm 1$; assume H_a^ϵ and $H_{a'}^{\epsilon'}$ are non-empty. Then $H_a^\epsilon \cap H_{a'}^{\epsilon'} = \emptyset$ iff $a = a'$ and $\epsilon = -\epsilon'$.

Proof. c) The if direction ($\Longleftarrow$) is clear. We will show the only if direction. The conditions imply with part b) that $a \neq 1 \neq a'$ and both have 2^{r-1} elements.
Because of $k^\times/k^{\times 2} = H_a^\epsilon \dot\cup H_a^{-\epsilon}$, we conclude $H_a^\epsilon \cap H_{a'}^{\epsilon'} = \emptyset$ implies $H_{a'}^{\epsilon'} = H_a^{-\epsilon}$ and $H_a^\epsilon = H_{a'}^{-\epsilon'}$. We get $H_a^1 = H_{a'}^1$ and so $(x,a) = (x,a')$ for all $x \in k^\times/k^{\times 2}$. Hence $(x,aa') = (x,a)(x,a') = (x,a)^2 = 1$, by degeneracy we get $aa' = 1$, hence $a = a'$ in $k^\times/k^{\times 2}$. $\square$

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times/k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

Before proving the theorem, let us indicate a consequence of it: let $a \in k^\times/k^{\times 2}$ and $f_a := f \dot{-} aZ^2$. We know that f_a represents 0 iff f represents a.
Moreover $d(f_a) = -ad$ and $\epsilon(f_a) = (-a, d)\epsilon$.
By applying the theorem to f_a we get the following corollary.

Hasse invariant

Corollary

Let $a \in k^\times/k^{\times 2}$. Then f represents a iff
(i) $n = 1$ and $a = d$,
(ii) $n = 2$ and $(a, -d) = \epsilon$,
(iii) $n = 3$ and either $a \neq -d$ or $a = -d$ and $(-1, -d) = \epsilon$,
(iv) $n \geq 4$.

Proof. f represents a iff f_a represents 0. Now apply the theorem and rewrite the conditions in terms of $d(f)$ and $\epsilon(f)$ instead of $d(f_a)$ and $\epsilon(f_a)$. □

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times/k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

Proof. Write $f \sim a_1 X_1^2 + \ldots + a_n X_n^2$. We will prove the theorem by case distinction regarding the rank n.
(i) Assume $n = 2$. Then f represents 0 iff $-a_1/a_2$ is a square in $k^\times/k^{\times 2}$ iff $-a_1 a_2 = -d$ is a square iff $-d = 1$ in $k^\times/k^{\times 2}$.
(ii) Assume $n = 3$, then f represents 0 iff $-a_3 f \sim -a_3 a_1 X_1^2 - a_3 a_2 X_2^2 - X_3^2$ represents 0. By the definition of the Hilbert symbol this is equivalent to $(-a_3 a_1, -a_3 a_2) = 1$. Expanding this leads to

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times / k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

$1 = (-a_3 a_1, -a_3 a_2) = (-1,-1)(-1,a_1)(-1,a_2)(a_3,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)$
Now use $(a_3, a_3) = (a_3, -a_3 a_3) = (a_3, -1) = (-1, a_3)$ to get
$1 = (-1,-1)(-1, a_1 a_2 a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) = (-1,-d)\epsilon$, hence
$\epsilon = (-1, -d)$.
(iii) Assume $n = 4$, then f represents 0 iff there exists and element $x \in k^\times / k^{\times 2}$ which is represented by the two forms $a_1 X_1^2 + a_2 X_2^2$ and $-a_3 X_3^2 - a_4 X_4^2$.

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times / k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

By case (ii) of the corollary above, such an x is characterized by the conditions $(x, -a_1 a_2) = (a_1, a_2)$ and $(x, -a_3 a_4) = (-a_3, -a_4)$.
Write $a = -a_1 a_2$, $b = (a_1, a_2)$, $a' = -a_3 a_4$ and $b' = (-a_3, -a_4)$.
Then $a_1 \in H_a^b$ and $-a_3 \in H_{a'}^{b'}$.
Now f does not represent 0 iff $H_a^b \cap H_{a'}^{b'} = \emptyset$ iff $a = a'$ and $b = -b'$ iff $a_1 a_2 = a_3 a_4$ and $(a_1, a_2) = -(-a_3, -a_4)$. The first condition is equivalent to $d = 1$. Write ϵ out with the definition and use the above relations with the Hilbert symbol identities to get $\epsilon = -(-1, -1)$. Hence the desired result.

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times / k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

(iv) Assume $n \geq 5$. It is sufficient to consider $n = 5$, since a solution for $n \geq 6$ is by setting the variables $X_6, \ldots, X_n$ all to 0 and plug in the solution for $n = 5$. By using part (ii) of the above corollary, we see that a form of rank 2 represents at least 2^{r-1} elements of $k^\times / k^{\times 2}$, and the same is true for forms of rank ≥ 2 (by setting all other variables to zero). Since $2^{r-1} \geq 2$, f represents at least one element $a \in k^\times / k^{\times 2}$ distinct from d.

Hasse invariant

Let f be a quadratic form of rank n with $d = d(f)$ and $\epsilon = \epsilon(f)$.

Theorem

The quadratic form f represents 0 iff
(i) $n = 2$ and $d = -1$ (in $k^\times/k^{\times 2}$),
(ii) $n = 3$ and $(-1, -d) = \epsilon$,
(iii) $n = 4$ and either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$,
(iv) $n \geq 5$ (in particular all forms in at least 5 variables represent 0).

We have $f \sim aX^2 + g$, where g is a form of rank 4. The discriminant of g is equal to $d/a \neq 1$. By part (iii) g represents 0, the same is then true for f, and we are done. $\square$

Artin's conjecture

We saw that all quadratic forms in 5 variables over $\mathbb{Q}_p$ represent 0.
Emil Artin conjectured the following:
All homogeneous polynomials of degree d over $\mathbb{Q}_p$ in at least $d^2 + 1$ variables have a non-trivial zero.
We solved the case $d = 2$.

Artin's conjecture

We saw that all quadratic forms in 5 variables over $\mathbb{Q}_p$ represent 0.
Emil Artin conjectured the following:
All homogeneous polynomials of degree d over $\mathbb{Q}_p$ in at least d^2+1 variables have a non-trivial zero.
We solved the case $d=2$.
The case $d=3$ was also solved 1955.

Artin's conjecture

We saw that all quadratic forms in 5 variables over $\mathbb{Q}_p$ represent 0.
Emil Artin conjectured the following:
All homogeneous polynomials of degree d over $\mathbb{Q}_p$ in at least $d^2 + 1$ variables have a non-trivial zero.
We solved the case $d = 2$.
The case $d = 3$ was also solved 1955.
But 1966 G. Terjanian gave a counter-example for $d = 4$ over $\mathbb{Q}_2$ in 18 variables (take a look at ,,J.P. Serre - A course into arithmetic, page 38-39" for a construction).

Artin's conjecture

We saw that all quadratic forms in 5 variables over $\mathbb{Q}_p$ represent 0.
Emil Artin conjectured the following:
All homogeneous polynomials of degree d over $\mathbb{Q}_p$ in at least $d^2 + 1$ variables have a non-trivial zero.
We solved the case $d = 2$.
The case $d = 3$ was also solved 1955.
But 1966 G. Terjanian gave a counter-example for $d = 4$ over $\mathbb{Q}_2$ in 18 variables (take a look at ,,J.P. Serre - A course into arithmetic, page 38-39" for a construction).
But one knows that Artin's conjecture is *almost true*: for a fixed degree d, it holds for all prime number p except a finite number. However, even for $d = 4$, one does not know how to determine the set of exceptional prime numbers.

Classification of quadratic forms over $\mathbb{Q}_p$

Proposition (Classification of quadratic forms over $\mathbb{Q}_p$)

Two quadratic forms over k are equivalent iff they have the same rank, same discriminant and same Hasse invariant.

Proof. The only if direction ($\Longrightarrow$) is clear. We will prove the other direction via induction on the rank n. The case $n = 0$ is trivial. The statement that f represents $a \in k^\times / k^{\times 2}$ is only dependent on the discriminant and the Hasse invariant by our corollary. Hence f and g represent the same elements. Take an element a which is represented by f and g. This allows us to write $f \sim aZ^2 \dotplus f'$ and $g \sim aZ^2 \dotplus g'$, where f' and g' are forms of rank $n - 1$. One has $d(f') = 1/a \cdot d(f) = 1/a \cdot d(g) = d(g')$ and $\epsilon(f') = \epsilon(f)(a, d(f')) = \epsilon(g)(a, d(g')) = \epsilon(g')$. So f' and g' have the same invariants and are equivalent by induction hypothesis. Hence $f \sim g$. □

Classification of quadratic forms over $\mathbb{R}$

From linear algebra the classification of symmetric bilinear forms over $\mathbb{R}$ is known as *Sylvester's law of inertia*, where a non-degenerate quadratic form f of rank n can be written as $f \sim X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2$ with $r + s = n$ and r respectively s are uniquely determined.
In fact *Sylvester's law of inertia* is more general, than the above version; the general case is valid for all quadratic forms and not just non-degenerated forms.
With the tools from the last talk the above version should be provable.

Thank you for your attention! Do you have any questions?