

Classification of Quadratic Forms over \mathbb{Q}

Shubin Xue

Beijing Institute of Technology

2025-09-11

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Notations

- K : an arbitrary field with $\text{Char } K \neq 2$.
- X, Y, Z : variables.
- $\mathbb{V} = \{v : v \in \mathbb{V}\} = \{p : \text{prime number}\} \cup \{\infty\}$.
- \mathbb{Q}_v : completion of \mathbb{Q}
 - $\mathbb{Q}_\infty = \mathbb{R}$
 - \mathbb{Q}_p : with respect to the p -adic valuation.

Quadratic Forms

- $f(\vec{X}) = \sum_{i,j=1}^n a_{ij}X_iX_j$ is a quadratic form
 - $a_{ij} = a_{ji} \in K$.
 - $\vec{X} = (X_1, \dots, X_n) \in K^n$
- The matrix $A_f = (a_{ij})$ associated with f is symmetric.
- The pair (K^n, f) is a quadratic space.
 - $f \sim g$: $\exists P \in GL(n, K)$ s.t. $A_f = P^T A_g P$.
 - $f \sim g \iff (K^n, f) \cong (K^n, g)$.

Classification of Quadratic Forms over \mathbb{Q} ?

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Background (17-18th Century)

f represents $a \in K$: $\exists x \in K^n \setminus \{0\}$ s.t. $f(x) = a$.

Theorem (Fermat's Two-Square Theorem)

An odd prime p can be represented as the sum of two squares if and only if $p \equiv 1 \pmod{4}$.

Theorem (Gauss's Three-Square Theorem)

A natural number can be represented as a sum of three squares if and only if it is not of the form $4^a(8b - 1)$ for integers $a \geq 0$, $b > 0$.

Theorem (Lagrange's Four Square Theorem)

Every natural number can be represented as the sum of at most four squares.

Background (19-20th Century)

Remark

Equivalent quadratic forms represent exactly the same set of numbers.

Theorem (Hasse-Minkowski)

f represents 0 over \mathbb{Q} iff it represents 0 over all \mathbb{Q}_v .

Representation of Numbers

$f(X_1, \dots, X_n)$ and $g(X_1, \dots, X_m)$

- $f \oplus g = f(X_1, \dots, X_n) + g(X_{n+1}, \dots, X_{n+m})$

Proposition

Let $a \in K^\times$. The following are equivalent:

- f represents a
- $f \sim f_1 \oplus aZ^2$ where f_1 is of rank $\text{rank } f - 1$.
- $f_a = f \oplus -aZ^2$ represents 0.

Corollary (Hasse-Minkowski Theorem)

f represents $a \in \mathbb{Q}^\times$ over \mathbb{Q} iff it represents a over all \mathbb{Q}_v .

- Apply the Hasse-Minkowski Theorem to $f_a = f \oplus -aZ^2$.

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Decomposing Quadratic Spaces

Theorem (Witt's Cancellation)

$f_1 \oplus g_1 \sim f_2 \oplus g_2$ and $g_1 \sim g_2$ implies $f_1 \sim f_2$.

- (V, Q) : A quadratic space.
- (U, Q) and (W, Q) : Isometric subspaces.

$$\begin{array}{ccc} V & \xrightarrow{\cong} & V \\ \text{Lift} \downarrow & & \downarrow \\ U & \xrightarrow{\cong} & W \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{\cong} & V \\ \text{Restrict} \downarrow & & \downarrow \\ U^\perp & \xrightarrow{\cong} & W^\perp \end{array}$$

Figure: Witt's Cancellation Theorem

$$f \sim g \text{ over } \mathbb{Q}$$

Theorem (Hasse-Minkowski)

Two non-degenerate quadratic forms of rank n over \mathbb{Q} are equivalent iff they are equivalent over each \mathbb{Q}_v .

- Suppose $f \sim g$ over \mathbb{Q}_v for all v , the numbers represented by both f and g over \mathbb{Q}_v is the same.
- By the Hasse-Minkowski Theorem, the numbers represented by both f and g over \mathbb{Q} is also the same.
- Take $a \in \mathbb{Q}$ represented by both f and g .
- $f \sim aZ^2 \oplus f_1$ over \mathbb{Q} and \mathbb{Q}_v . Similarly for g .
- By Witt's cancellation, we have $f_1 \sim g_1$ over \mathbb{Q}_v for all $v \in \mathbb{V}$.
- By induction on rank n , $f_1 \sim g_1$ over \mathbb{Q} , thus $f \sim g$ over \mathbb{Q} .

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

General Ideas over K

- Reduced Form: $f \sim \sum_{i=1}^n a_i X_i^2$, where $a_i \in K^\times / (K^\times)^2$.
 - Invariant rank: non-degenerate.
 - Symmetric matrices: diagonal.
 - $\sum a_i b_i^2 X_i^2 \sim \sum a_i X_i^2$: square-free.
- If $f \sim g$, $\det(A_f) = \det(P^T A_g P) = \det(A_g) \det(P)^2$
 - Invariant discriminant: $d = \det(A)$ in $K^\times / (K^\times)^2$.
- $\mathbb{R}^\times / (\mathbb{R}^\times)^2 \cong \{1, -1\}$.
- $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong K_4 = \{1, a, p, ap\}$ ($p \neq 2$).
- $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

- Invariants:

- Rank: $\text{rank } f = n$.
- Signature: $(r, s) := (\# \text{positive eigenvalues}, \# \text{negative eigenvalues})$.

Theorem (Sylvester's Law of Inertia)

Let $f = \sum_{i,j=1}^n a_{ij} X_i X_j$ be a quadratic form of rank n over \mathbb{R} . Then

$$f \sim X_1^2 + X_2^2 + \cdots + X_r^2 - X_{r+1}^2 - \cdots - X_{r+s}^2.$$

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Binary Quadratic Forms over \mathbb{Q}_p for $p \neq 2$

Theorem (Classification of Binary Quadratic Forms over \mathbb{Q}_p for $p \neq 2$)

Two binary quadratic forms over \mathbb{Q}_p for $p \neq 2$ are equivalent if and only if they have the same discriminant d and a common represented number a .

- Take a represented by f .
- $f \sim f_1 \oplus aZ^2$ where $\text{rank } f_1 = 1$.
- Then $f_1 = adX^2$. Thus f is determined.

Binary Quadratic Forms over \mathbb{Q}_p for $p \neq 2$

- Entry: the discriminant of $\alpha X^2 + \beta Y^2$
- a : same color, same equivalent class
 - mutually distinct if colored black
- \boxed{a} : boxed quadratic forms don't represent 1

$\alpha \backslash \beta$	1	a	p	ap
1	1	a	p	ap
a		1	\boxed{ap}	\boxed{p}
p			1	\boxed{a}
ap				1

(a) $p \equiv 1 \pmod{4}$

$\alpha \backslash \beta$	1	a	p	ap
1	1	a	p	ap
a		1	\boxed{ap}	\boxed{p}
p			1	a
ap				1

(b) $p \equiv 3 \pmod{4}$

Table: Classification of binary quadratic forms over \mathbb{Q}_p for $p \neq 2$

Hilbert Symbol

$f = aX^2 + bY^2$ represents 1

\iff

$Z^2 - aX^2 - bY^2$ represents 0.

- Hilbert symbol:

$$(a, b) = \begin{cases} 1 & Z^2 - aX^2 - bY^2 \text{ represents } 0, \\ -1 & \text{Otherwise.} \end{cases}$$

Computation of Hilbert Symbol

(\cdot, \cdot)	1	a	p	ap
1	1	1	1	1
a		1	-1	-1
p			1	-1
ap				1

(a) $p \equiv 1 \pmod{4}$

(\cdot, \cdot)	1	a	p	ap
1	1	1	p	ap
a		1	-1	-1
p			-1	1
ap				-1

(b) $p \equiv 3 \pmod{4}$

Table: Hilbert Symbol of \mathbb{Q}_p for $p \neq 2$

- Hilbert symbol is a symmetric non-degenerate bilinear form.

Hasse Invariant

- $f = a_1X_1^2 + \cdots + a_nX_n^2$.
- Hasse invariant: $\varepsilon(f) = \prod_{i < j} (a_i, a_j)$
- $f_1 = a_2X_2^2 + \cdots + a_nX_n^2$.
- $d(f) = \prod_{i=1}^n a_i = a_1 \prod_{i=2}^n a_i = a_1 d(f_1)$.
- $\varepsilon(f) = \prod_{1 \leq i < j \leq n} (a_i, a_j) = \varepsilon(f_1) \cdot (a_1, a_2 \cdots a_n) = \varepsilon(f_1) \cdot (a_1, a_1 d(f))$.

Representation of Numbers over \mathbb{Q}_p

f represents 0 over \mathbb{Q}_p iff:

- For $n = 2$: $d = -1$;
- For $n = 3$: $(-1, -d) = \varepsilon$;
- For $n = 4$: $d \neq 1$ or $d = 1$ and $\varepsilon = (-1, -1)$;
- For $n \geq 5$: no conditions.

By applying the result to $f_a = f \oplus -aZ^2$, we obtain:

f represents $a \in \mathbb{Q}_p^\times$ iff:

- For $n = 1$: $a = d$;
- For $n = 2$: $(a, -d) = \varepsilon$;
- For $n = 3$: $a \neq d$ or $a = d$ and $\varepsilon = (-1, -d)$;
- For $n \geq 4$: no conditions.

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

$$f \sim g \text{ over } \mathbb{Q}_p$$

Theorem

Two non-degenerate quadratic forms of rank n over \mathbb{Q}_p are equivalent iff they have the same discriminant d and Hasse invariant ε .

- f, g have same d and ε , thus there exists $a \in \mathbb{Q}_p^\times$ which both represented by f and g .
- Then $f \sim f_1 \oplus aZ^2$, where f_1 is of rank $n - 1$. Similarly for g .
- d and ε of f_1 can be determined:
 - $d(f_1) = a \cdot d(f) = a \cdot d(g) = d(g_1)$
 - $\varepsilon(f_1) = \varepsilon(f) \cdot (a, ad(f)) = \varepsilon(g) \cdot (a, ad(g)) = \varepsilon(g_1)$
- Thus f_1, g_1 share the same d and ε . QED by induction.

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Classification of Quadratic Forms over \mathbb{Q}_p

Fix (d, ε) , all possible quadratic forms over \mathbb{Q}_p :

- $n = 1$: $f = dX^2$
- $n = 2$: $f = aX^2 + adY^2$, for
 - $a \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$
- $n \geq 3$: $f = aX_1^2 + bX_2^2 + abdX_3^2 + \sum_{i>3} X_i^2$, for
 - $a : a \neq -d$
 - $b : (b, -ad) \cdot (a, -d) = \varepsilon$

Classification of Quadratic Forms over \mathbb{Q}

Theorem (Product Formula)

$(a, b)_v = 1$ for almost all $v \in \mathbb{V}$ and $\prod_{v \in \mathbb{V}} (a, b)_v = 1$

The invariants d_v and ε_v satisfy the following relations:

- $\varepsilon_v = 1$ for almost $v \in \mathbb{V}$, and $\prod_{v \in \mathbb{V}} \varepsilon_v = 1$.
- $\varepsilon_v = 1$ if $n = 1$ and if $n = 2$ and if the image d_v of d in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ is equal to -1 .
- $r, s \geq 0$ and $r + s = \text{rank}$.
- $d_\infty = (-1)^s$
- $\varepsilon_\infty = (-1)^{s(s-1)/2}$

Table of Contents

1 Classification and Representation

- Some History
- From Global to Local

2 Quadratic Forms over \mathbb{Q}_v

- General Ideas over Arbitrary K
- Classification of Quadratic Forms over \mathbb{R}
- Invariants that Determine the Representation over \mathbb{Q}_p
- Classification of Quadratic Forms over \mathbb{Q}_p

3 Classification Results

- Classification Results
- Hasse-Minkowski Theorem

Theorem (Hasse-Minkowski)

f represents 0 over \mathbb{Q} iff it represents 0 over \mathbb{R} and all \mathbb{Q}_p .

- $n = 2$: Fermat's Two-Square Theorem.
- $n = 3$: Gauss's Three-Square Theorem.
- $n = 4$: Lagrange's Four-Square Theorem.
- $n \geq 5$: Mathematical induction.