

# Classification of Quadratic Forms over $\mathbb{Q}$

sun123zxy

2025-04-16<sup>1</sup>

---

<sup>1</sup>Last modified on 2025-09-01.

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

- References relied on heavily:
  - J.P. Serre “A Course in Arithmetic” [Ser73]
  - Shiva Chidambaram, MIT18.782 Introduction to Arithmetic Geometry (Spring 2023) [Lecture Notes](#)
  - Arushi Gupta, Participant Papers of The University of Chicago Mathematics REU 2018, [The  \$p\$ -adic Integers, Analytically and Algebraically](#)
- May serve as a guidance of the first part of [Ser73]
- Assume familiarity with quadratic residues and basic knowledge of  $p$ -adic numbers
- Skip most of the proofs
- Apology in advance for potential mistakes

# Notations

- We denote by  $K$  an arbitrary field. All fields are assumed to be of characteristic  $\neq 2$ .
- $\nu_p : \mathbb{Q}_p \rightarrow \mathbb{Z}$  being the  $p$ -adic valuation.
- $\left(\frac{a}{p}\right)$  being the Legendre symbol.  $a$  is understood as  $p^{-\nu_p(a)}a \bmod p$  if  $a \in \mathbb{Q}_p$ . Define this similarly in  $\mathbb{F}_q$ .
- Let  $f \oplus g$  denote the direct sum of two quadratic forms  $f$  and  $g$ .

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Review: Quadratic Forms over $\mathbb{R}$

- A quadratic form  $f : V \rightarrow K$  may be identified by a symmetric matrix  $A \in M_n(K)$  by  $f(v) = v^T A v$ .

Their equivalence is defined by *congruence*:

$$A \sim B \iff A = Q^T B Q.$$

- Real symmetric matrices may be diagonalized orthogonally.
- Scale each eigenvalue by multiplying a square. Only their sign matters.
  - the *rank*  $n$ , an invariant
  - the *signature*  $(r, s) := (\# \text{positive eigenvalues}, \# \text{negative eigenvalues})$ .
- Same rank and signature implies the equivalence.
- Sylvester's law of inertia: signature is also an invariant.

# Some Refinement

On an arbitrary field  $K$ :

- All symmetric matrix is equivalent to a diagonal one.
  - Pick a non-isotropic vector  $v$  (exists when the form is nonzero), its orthogonal complement is a hyperplane and does not include  $v$ . Change basis and do the induction.
- The rank is always an invariant. We may (and we shall always) reduce to classify the non-degenerate quadratic forms of rank  $n$ .
- The squares  $(K^\times)^2$  give us the ability to scale. Knowledge of the distribution of diagonal elements in  $K^\times/(K^\times)^2$  suffices to show the equivalence<sup>2</sup>.
  - $\mathbb{C}^\times/(\mathbb{C}^\times)^2 \cong \{1\}$ , suffices to classify by the rank.
  - $\mathbb{R}^\times/(\mathbb{R}^\times)^2 \cong \{1, -1\}$ , signature is also needed.
  - $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 \cong \{1, a\}$ , where  $a \in \mathbb{F}_q$  is a quadratic nonresidue.
  - For  $\mathbb{Q}_p$  and  $\mathbb{Q}$ ?

---

<sup>2</sup>Though working in the refined structure  $\{0\} \cup K^\times/(K^\times)^2$  is probably a better idea if one wishes to deal with the degenerate case in a uniform manner.



# Another Example: Quadratic Forms over $\mathbb{F}_q$

We classify the non-degenerate quadratic forms of rank  $n$ .

- Refined signature: counting nonzero quadratic residues and nonresidues. It may serve as a sufficient criterion for equivalence.
- But it's not an invariant.  $aX^2 + aY^2 \sim X^2 + Y^2$  over  $\mathbb{F}_q$ .
  - Do a change of basis  $X = sU + tV$  and  $Y = tU - sV$ . If we require  $aU^2 + aV^2 = X^2 + Y^2$ , then  $s^2 + t^2 = a$ .
  - It always has a nonzero solution in  $\mathbb{F}_q$ :  $s^2$  and  $a - t^2$  have both  $(q+1)/2$  possible values, thus must reach a common value.
- The *discriminant*  $d := \left( \frac{\det(A)}{q} \right) \in \mathbb{F}_q^\times / (\mathbb{F}_q^\times)^2$  is an invariant and reveals the parity of the signature. It classifies the non-degenerate quadratic forms over  $\mathbb{F}_q$ .

Insight: Existence of nonzero solutions to the equation  $aX^2 + bY^2 = Z^2$  in  $K$  seems to be of great importance.

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Quadratic Spaces

The structure of a quadratic space, i.e. vector space equipped with a symmetric bilinear form, is much more subtle than its positive-definite counterpart over  $\mathbb{R}$  or  $\mathbb{C}$ . For example, for a non-degenerate quadratic space  $V$  and a subspace  $U$  of  $V$  ([Ser73] p. 28, chap. 4, sec. 1.2):

- $U \cap U^\perp = \text{rad}(U)$ ,  $\dim U + \dim U^\perp = \dim V$ ,  $(U^\perp)^\perp = U$
- $U \oplus U^\perp = V$  iff  $U + U^\perp = V$  iff  $\text{rad}(U) = 0$
- It's much harder to show that an orthogonal basis of  $U$  expands to an orthogonal basis of  $V$ .

# Structure of Quadratic Spaces

We mention some results here without details.

Theorem (Witt ([Ser73] p. 31, chap. 4, sec. 1.5, theorem 3))

*Every injective metric-preserving map from a subspace  $U$  of a quadratic space  $V$  to another quadratic space  $W$  may be extended to a metric-preserving map from  $V$  to  $W$ .*

Theorem (Witt's cancellation ([Ser73] p. 34, chap. 4, sec. 1.6, theorem 4))

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

Theorem (Witt's decomposition)

*Every quadratic space  $V$  is a direct sum of:  $\text{rad}(V)$ , an anisotropic quadratic space (i.e. its nonzero vectors has nonzero norms) and a split quadratic space (i.e.  $U = U^\perp$ , full of hyperbolas)*

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Another Invariant: The Range

On an arbitrary field  $K$ , we say that a quadratic form  $f$  *represents*  $a \in K$  if there exists a nonzero  $v \in V$  such that  $f(v) = a$ .

- The range of  $f$ ,  $\text{Im } f$ , is an invariant.
- It may be viewed in  $\{0\} \cup K^\times / (K^\times)^2$ .
- Is it complete?

# Insights from the Range

Proposition (([Ser73] p. 33, chap. 4, sec. 1.6, corollary 1))

Let  $a \in K^\times$ . TFAE:

- $f$  represents  $a$
  - $f \sim g \oplus (Z \mapsto aZ^2)$  where  $g$  is of rank  $\text{rk } f - 1$ .
  - $f \oplus (Z \mapsto -aZ^2)$  represents 0.
- 
- Insight from line 3: To understand the range, it suffices to examine when a quadratic form represents 0.
  - Insight from line 2 (*the common represented element method*): Say  $f_1, f_2$  are nonzero and represent a common  $a \in K^\times$ . Reducing  $Z \mapsto aZ^2$ , if only  $g_1$  and  $g_2$  also share a common represented element...

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$



# Insights from the Range

- Sadly, the range is not always a complete invariant.
  - Otherwise all indefinite quadratic forms over  $\mathbb{R}$  are equivalent, absurd.
- But we shall show that when  $K = \mathbb{Q}_p$  and moreover  $K = \mathbb{Q}$ , it plays a subtle role in the classification of quadratic forms. This requires a more precise characterization of the range.
- In fact, if only there are some simple invariants that can fully determine the range...

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Global and Local Equivalence

- Fact: Field extensions preserve the equivalence of quadratic forms.
  - Example: Equivalence classes are finer over  $\mathbb{R}$  than those over  $\mathbb{C}$ .
- $\mathbb{Q} \hookrightarrow \mathbb{R}$ , thus the rank and the signature are invariants. But we need more information to classify.
- Other field extension of  $\mathbb{Q}$ ?  $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$

Theorem (Hasse-Minkowski ([Ser73] p. 41, chap. 4, sec. 3.1, theorem 8))

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

- To gain more invariants for  $\mathbb{Q}$  (especially those related to the range), let's classify quadratic forms over  $\mathbb{Q}_p$  first.

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Structure of $\mathbb{Q}_p^\times$

- $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$  by collecting common powers of  $p$
- $\mathbb{Z}_p^\times \cong \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p)$  by  $a \mapsto a \bmod p$ 
  - It splits by the explicit construction of a primitive root of order  $p$ , via Hensel's lemma / Teichmüller lift  $\lim_{n \rightarrow \infty} g^{p^n}$ , where  $g$  is a primitive root of  $\mathbb{F}_p^\times$ .

# Structure of $1 + p\mathbb{Z}_p$ and the log / exp map

For  $p \neq 2$ ,  $\alpha \geq 1$  or  $p = 2$ ,  $\alpha \geq 2$ :

$$1 + p^\alpha \mathbb{Z}_p \cong (p^\alpha \mathbb{Z}_p, +) \cong (\mathbb{Z}_p, +)$$
$$1 + p^\alpha a \mapsto \log(1 + p^\alpha a)$$

For  $p = 2$ ,  $\alpha = 1$ ,



$$1 + 2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z} \times (1 + 4\mathbb{Z}_2)$$

- by  $1 + 2a \mapsto a \bmod 2$
- It splits by the explicit construction of a primitive root of order 2:  
 $(-1, -1, \dots) = \sum_{n=0}^{+\infty} 2^n.$
- $(1 + 4\mathbb{Z}_2) \cong (4\mathbb{Z}_2, +) \cong (\mathbb{Z}_2, +)$  by the log map
- Thus

$$1 + 2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}_2, +)$$



# Quadratic residues of $\mathbb{Q}_p$

For  $p \neq 2$ :

- $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{F}_p^\times \times (\mathbb{Z}_p, +)$
- 2 is a unit in  $\mathbb{Z}_p$ . Thus  $a \in (\mathbb{Q}_p^\times)^2$  iff  $\nu_p(a) \bmod 2 = 0$  and  $a \bmod p \in \mathbb{F}_p^\times$  is a quadratic residue.
- $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , generated by  $p$  and  $a$ , where  $a \bmod p$  is a quadratic nonresidue.

For  $p = 2$ :

- $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}_2, +)$
- Quadratic residues of  $(\mathbb{Z}_2, +)$  are  $(2\mathbb{Z}_2, +)$ , which pull back to  $1 + 8\mathbb{Z}_2$ .
- $a \in (\mathbb{Q}_2^\times)^2$  iff  $\nu_2(a) \bmod 2 = 0$  and  $a \bmod 8 \equiv 1$ .
- $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , generated by 2, 3 and 5.

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# The Hilbert Symbol

The Hilbert symbol over  $\mathbb{Q}_p$  is defined as:

$$\langle a, b \rangle := \begin{cases} 1 & \text{if } aX^2 + bY^2 = Z^2 \text{ has a nonzero solution in } \mathbb{Q}_p \\ -1 & \text{otherwise} \end{cases}$$

The symbol may also be viewed in  $\{0\} \cup \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$  or even more simply in  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$  when working with non-degenerate forms.<sup>3</sup>

---

<sup>3</sup>Lots of the resources, even [Ser73], switch between these three views without enough warning. Sadly we shall also commit this usual mild sin (and have already done to other innocent invariants such as the discriminant...)

# Properties of the Hilbert Symbol

- $\langle a, -a \rangle = 1$
- $\langle a, b \rangle = \langle b, a \rangle$  (symmetric)
- If  $\langle a_2, b \rangle = 1$ , then  $\langle a_1 a_2, b \rangle = \langle a_1, b \rangle$ 
  - In fact,  $\langle a_1 a_2, b \rangle = \langle a_1, b \rangle \langle a_2, b \rangle$  (multiplicatively bilinear)
- $\langle a, b \rangle = 1$  for all  $b$  iff  $a \in \mathbb{Q}_p^2$  (nondegenerate)
- the Hilbert symbol is a non-degenerate symmetric bilinear form of the  $\mathbb{F}_2$ -vector space  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - This is a non-trivial result and is said to be, to some extent, a generalization of the law of quadratic reciprocity in local class field theory.
  - To show above over  $\mathbb{Q}_p$ , we develop an explicit formula for the Hilbert symbol.

# The Explicit Formula of the Hilbert Symbol

Theorem ([Ser73] p. 20, chap. 3, sec. 1.2, theorem 1))

Say  $a = p^\alpha u$  and  $b = p^\beta v$  are  $p$ -adic numbers where  $u, v \in \mathbb{Z}_p^\times$ , then

$$\langle a, b \rangle = (-1)^{\alpha \cdot \beta \cdot \frac{p-1}{2}} \left( \frac{u}{p} \right)^\beta \left( \frac{v}{p} \right)^\alpha \text{ if } p \neq 2$$

We omit the case  $p = 2$ . It's a tedious modification of the above formula.

$\langle \cdot, \cdot \rangle$	1	$a$	$p$	$ap$
1	1	1	1	1
$a$		1	-1	-1
$p$			$\epsilon$	$-\epsilon$
$ap$				$\epsilon$

Table: Hilbert symbol over  $\mathbb{Q}_{p \neq 2}$ ,  $\epsilon := (-1)^{(p-1)/2}$

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Prelude: Classifying Binary Quadratic Forms over $\mathbb{Q}_p$

In the following table:

- 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 do not represent 1 ( $\langle \alpha, \beta \rangle = -1$ )

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

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

$\alpha \setminus \beta$	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 nondegenerate binary quadratic forms over  $\mathbb{Q}_p$ ,  $p \neq 2$

# The Hasse Invariant

Recall that we have reduced to work with non-degenerate diagonalized quadratic forms of rank  $n$ . Recall that the discriminant

$$d(f) = a_1 a_2 \dots a_n \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$$

is an invariant.

- Define the *Hasse invariant*  $\varepsilon(f) := \prod_{1 \leq i < j \leq n} \langle a_i, a_j \rangle$
- It is an invariant:

$$\varepsilon(f) = \prod_{1 \leq i < j \leq n} \langle a_i, a_j \rangle = \varepsilon(f_1) \prod_{2 \leq j \leq n} \langle a_1, a_j \rangle = \varepsilon(f_1) \cdot \langle a_1, a_1 d(f) \rangle$$

Thus  $\varepsilon$  is preserved under *contiguous* change of orthogonal bases (fixes one of the vector of the basis)

- For  $n \geq 3$ , orthogonal bases are transitive under contiguous change ([Ser73] p. 30, sec. 4.1.4, theorem 2)



# $d$ and $\varepsilon$ Determine the Range

Theorem ([Ser73] p. 36, chap. 4, sec. 2.2, theorem 6))

*For a non-degenerate quadratic form  $f$  of rank  $n$  over  $\mathbb{Q}_p$ , the range of  $f$  is determined by the discriminant  $d := d(f)$  and the Hasse invariant  $\varepsilon := \varepsilon(f)$ .*

*Or, in detail,  $f$  represents 0 iff:*

- *For  $n = 2$ :  $d = -1$*
- *For  $n = 3$ :  $\langle -1, -d \rangle = \varepsilon$*
- *For  $n = 4$ :  $d \neq 1$  or  $d = 1$  and  $\varepsilon = \langle -1, -1 \rangle$*
- *For  $n = 5$ : no conditions*

Recall that  $f$  represents  $a \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$  iff  $f \oplus (Z \mapsto -aZ^2)$  represents 0, thus above fully characterizes the range.

# Table of Contents

## 1 First Attempts and General Approaches

- Foreword
- Notations
- Example: Quadratic Forms over  $\mathbb{R}$  and  $\mathbb{F}_q$ 
  - Review: Quadratic Forms over  $\mathbb{R}$
  - Some Refinement
  - Another Example: Quadratic Forms over  $\mathbb{F}_q$
- Quadratic Spaces
  - Quadratic Spaces
  - Structure of Quadratic Spaces
- The Common Represented Element Method
  - Another Invariant: The Range
  - Insights from the Range
- Insights from the Range

## 2 Global and Local Equivalence

- Global and Local Equivalence

## 3 Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$

- Structure of  $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ 
  - Structure of  $\mathbb{Q}_p^\times$

# Classification of Quadratic Forms over $\mathbb{Q}_p$

Theorem ([Ser73] p. 39, chap. 4, sec. 2.3, theorem 7))

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

- $f, g$  have same  $d$  and  $\varepsilon$ , thus have the same range. Say they both represent  $a \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ .
- Then  $f \sim f_1 \oplus (Z \mapsto aZ^2)$ , where  $f_1$  is of rank  $n - 1$ .
- $d$  and  $\varepsilon$  of  $f_1$  can be determined:
  - $d(f_1) = ad(f)$
  - $\varepsilon(f_1) = \varepsilon(f) \cdot (a, ad(f))$  (shown when discussing the invariance of  $\varepsilon$ )
- The same for  $g$ . Thus  $f_1, g_1$  share the same  $d$  and  $\varepsilon$  (thus also their range). QED by induction.

# Classification of Quadratic Forms over $\mathbb{Q}$

Theorem ([Ser73] p. 39, chap. 4, sec. 2.3, theorem 7))

*Two non-degenerate quadratic forms of rank  $n$  over  $\mathbb{Q}$  are equivalent iff they are equivalent over  $\mathbb{R}$  and over each  $\mathbb{Q}_p$ .*

- Say  $f, g$  are equivalent over each local field ( $\mathbb{Q}_p$  and  $\mathbb{R}$ ), thus they share the same range locally.
- By Hasse-Minkowski theorem, they also share the same range globally over  $\mathbb{Q}$ .
- Then  $f \sim f_1 \oplus (Z \mapsto aZ^2)$  globally, where  $f_1$  is of rank  $n - 1$ . The same for  $g$ .
- $f_1 \sim g_1$  locally by Witt's cancellation theorem. QED by induction.

# Problem Remains

- Proof of the Hasse-Minkowski theorem
  - essentially needs some understanding of the global property of the Hilbert symbol, which we have not discussed (cf. [Ser73])
- Refine the theory for degenerate quadratic forms (relatively easy)
- Enumerate all the equivalence classes of quadratic forms over  $\mathbb{Q}_p$  and  $\mathbb{Q}$  (cf. [Ser73])
- To what extent can we use the common represented element method to classify quadratic forms over other fields?
- For which fields, the range of a quadratic form is a complete invariant? (At least  $\mathbb{R}$  fails.  $\mathbb{Q}$ ,  $\mathbb{Q}_p$ ?)
- What can we say about  $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ ?
- Classification of quadratic forms over commutative rings (e.g.  $\mathbb{Z}$ ,  $\mathbb{Z}/m\mathbb{Z}$ )

- [Ser73] Jean-Pierre Serre. *A Course in Arithmetic*. Vol. 7. Graduate Texts in Mathematics. New York, NY: Springer, 1973. ISBN: 978-0-387-90041-4 978-1-4684-9884-4. DOI: [10.1007/978-1-4684-9884-4](https://doi.org/10.1007/978-1-4684-9884-4).