Classification of Quadratic Forms over $\mathbb{Q}$[1]

Shubin Xue

Beijing Institute of Technology

2025-09-11[2]

[1]Xinyu Zhong contributed equally to this report

[2]Last modified on 2025-08-13.

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Notations

- We denote by K an arbitrary field of characteristic $\neq 2$.
- X, Y, Z are used as variables.
- $\left(\dfrac{a}{p}\right)$ is the Legendre symbol.
- We will often denote by the same letter an element and its class modulo.

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

What is a Quadratic Form/Quadratic Space?

Definition (Quadratic Space)

Let V be a vector space (finite-dimensional) over a field K of characteristic $\neq 2$. A function $Q : V \to K$ is called quadratic form on V satisfying:

- $Q(\lambda v) = \lambda^2 Q(v)$ *for all* $\lambda \in K$, $v \in V$,
- *The function* $B_Q(u, v) = Q(u + v) - Q(u) - Q(v)$ *is a symmetric bilinear form on* V.

A quadratic space is such a pair (V, Q).

- Put $x \cdot y = \frac{1}{2} B_Q(x, y)$. One has $Q(x) = x \cdot x$.
- Given a basis $\{e_1, \ldots, e_n\}$ of V, the quadratic form Q can be associated with a symmetric matrix $A = (a_{ij})$ where $a_{ij} = e_i \cdot e_j$.

$$\text{If } x = \sum_{i=1}^{n} x_i e_i \in V, \text{ then } Q(x) = \sum_{i,j=1}^{n} a_{ij} x_i x_j.$$

Translations

Let us consider quadratic forms in a more familiar form:

- $f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ is a quadratic form in n variables over K, where $a_{ij} = a_{ji}$.
- The pair (K^n, f) is a quadratic space.
- The matrix $A = (a_{ij})$ is associated with f.
- Let $f(X_1, \cdots, X_n)$ and $g(X_1, \cdots, X_m)$ be two quadratic forms, we denote $f \oplus g$ the quadratic form

$$f(X_1, \cdots, X_n) + g(X_{n+1}, \cdots, X_{n+m})$$

in $n + m$ variables.

Invariant: Discriminant

Change the basis $\{e_i\}$ to another basis $\{e'_i\}$; the associated symmetric matrix A transforms as $A' = PAP^T$.

- Two quadratic forms are equivalent if their matrices are congruent under such a transformation. *(Denoted as $f \sim g$)*
- We know that any symmetric matrix can always be diagonalized by a congruence transformation.
- Without loss of generality, assume quadratic forms are of the shape

$$f \sim \sum_{i=1}^{n} a_i X_i^2$$

  And $A' = PAP^T$ give us: $\det(A) = \det(A')\det(P)^2$.
- This means the image of $\det(A)$ in $K^\times / K^{\times 2}$ is a invariant, it's called discriminant of Q, and denoted by $d(Q)$ or simply d.

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

The case over $\mathbb{R}$

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*

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

where r *and* s *are non-negative integers, and* $r+s=n$*, the pair* (r,s) *is called signature of* f*.*

By diagonalizing via congruence and factoring out squares on the diagonal, we see that the only invariants for classifying real quadratic forms are:

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

The *rank* and *signature* are invariants.

General Ideas

On an arbitrary field K:

- The rank is always an invariants. Hence we may (and we shall always) reduce to classify the non-degenerate quadratic forms of $\operatorname{rank} n$.
- Two quadratic forms $f = \sum_{i \neq j} a_{ij} X_i X_j$ and $f' = \sum_{i \neq j} a'_{ij} X_i X_j$ satisfy: there exist $t_{ij} \in {K^{\times}}^2$ s.t. $a_{ij} = t_{ij} a'_{ij}$, then $f \sim f'$.
- The distribution of diagonal elements in $K^{\times}/(K^{\times})^2$ suffices to show the equivalence.
  - $\mathbb{C}^{\times}/(\mathbb{C}^{\times})^2 \cong \{1\}$, 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 $a \in \mathbb{F}_q$ isn't a square.
  - For $\mathbb{Q}_p$ and $\mathbb{Q}$?

Case over $\mathbb{F}_q$

- Following the above discussion, we might hope that the number of squares appearing on the diagonal would serve as a sufficient criterion for equivalence. However, this is not the case.
- Consider the non-degenerate quadratic form of rank 2 in 2 variables over $\mathbb{F}_q$ with a quadratic nonresidue a,

$$f_1 = aX^2 + aY^2 \sim f_2 = X^2 + Y^2$$

  - Do a change of basis: $X = sX' + tY'$ and $Y = tX' - sY'$. If we requier $aX'^2 + aY'^2 = X^2 + Y^2$, then $s^2 + t^2 = a$. Then we must focus on the existence of solution of eqation $s^2 + t^2 = a$.
  - s^2 and $a - t^2$ have both $(q+1)/2$ possible values, the pigeonhole principle implies the eqation has a nonzero solution.
- The discriminant $d(f_1) = d(f_2) = 1 \in \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ is an invariant for classifying quadratic forms.

Hilbert Symbol

The existence of nonzero solutions to the equation $aX^2 + bY^2 = Z^2$ in K^3 seems to be of great importance.

Definition (Hilbert symbol)

Let $a, b \in K^\times$:

$$(a,b)_K = \begin{cases} 1 & \text{if } Z^2 - aX^2 - bY^2 = 0 \text{ has a nontrivial solution in } K^3, \\ -1 & \text{if } Z^2 - aX^2 - bY^2 = 0 \text{ has no nontrivial solution in } K^3. \end{cases}$$

The number $(a,b)_K$ is called the Hilbert symbol of a and b relative to K. (When there is no ambiguity, the subscript is often omitted.)

- The symbol may also be viewed in $K^\times/(K^\times)^2$ when working with non-degenerate forms.

The Hilbert Symbol over $\mathbb{Q}_p$

From now on, we always assume $K = \mathbb{Q}_p$ for a prime p:

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

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

$$(a,b) = (-1)^{\frac{u-1}{2}\frac{v-1}{2}+\alpha\frac{v^2-1}{8}+\beta\frac{u^2-1}{8}} \quad \text{if } p = 2$$

- This means that Hilbert symbol is a symmetric non-degenerate bilinear form.

Product Formula of Hilbert Symbol

Let $\mathbb{V} = \mathbb{P} \cup \{\infty\}$, and $\mathbb{Q}_\infty = \mathbb{R}$. If $a, b \in \mathbb{Q}^\times$, $(a, b)_v$ denotes the Hilbert symbol of their images in $\mathbb{Q}_v$ for all $v \in \mathbb{V}$.

Proposition (Product formula)

If $a, b \in \mathbb{Q}^\times$, we have $(a, b)_v = 1$ for almost all $v \in \mathbb{V}$ and

$$\prod_{v \in \mathbb{V}} (a, b)_v = 1.$$

- We have seen that the Hilbert symbol works for rank 2, but how do we generalize to rank > 2?
- Let $\varepsilon(f) = \prod_{i<j} (a_i, a_j)$, which is called the Hasse invariant of f.

Two Invariants

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.
- Recall that the *Hasse invariant*

  $$\varepsilon(f) := \prod_{1 \le i < j \le n} (a_i, a_j)$$

  is also an invariant.
- If $f = a_1 X_1^2 \oplus f_1$ where $f_1 = a_2 X_2^2 + \cdots + a_n X_n^2$, then we have:

$$d(f) = \prod_{i=1}^{n} a_i = a_1 \prod_{i=2}^{n} a_i = a_1 d(f_1).$$

$$\varepsilon(f) = \prod_{1 \le i < j \le n} (a_i, a_j) = \varepsilon(f_1) \cdot (a_1, a_2 \cdots a_n) = \varepsilon(f_1) \cdot (a_1, a_1 d(f))$$

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Decomposition of Quadratic Forms

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

- It may be viewed in $\{0\} \cup K^\times/(K^\times)^2$.

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

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

- *f represents a*
- *$f \sim g \oplus aZ^2$ where g is of rank $\operatorname{rank} f - 1$.*
- *$f \oplus -aZ^2$ represents 0.*

- To check if a can be represented by f, it suffices to examine when a quadratic form represents 0.
- Suppose f_1 and f_2 can both represent some $a \in K^\times$, then we hope to reduce their rank and use induction in subsequent proofs.

When does a quadratic form represent 0, a ($a \in K^\times$)?

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

f represents 0 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 Theorem to $f_a = f \oplus -aZ^2$, we obtain:

Corollary (([Ser73] p. 37, chap. 4, sec. 2.2, corollary to themrem 6))

f represents $a \in K^\times / K^\times$ 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.*

Conditions for decomposing quadratic forms

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.

- If a quadratic space (V, Q) has two isometric subspaces U and W, then by Witt's theorem, the isometry can be extended to an automorphism of V. By restricting this automorphism to $U^{\perp}$, we see that $U^{\perp}$ and $W^{\perp}$ are also isometric. The results about quadratic spaces can be translated into results about quadratic forms:

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 $f_1 \sim f_2$.

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Quadratic Forms $f \sim g$ 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 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:
  - $d(f_1) = ad(f) = ad(g) = d(g_1)$
  - $\varepsilon(f_1) = \varepsilon(f) \cdot (a, ad(f)) = \varepsilon(g) \cdot (a, ad(g)) = \varepsilon(g_1)$
- Thus f_1, g_1 share the same d and ε. QED by induction.

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

The invariants d and ε are not independent; they satisfy the following relations:

- For $n = 1$: $\varepsilon = 1$;
- For $n = 2$: $d \neq -1$ or $\varepsilon = 1$;
- For $n \geq 3$: no conditions.

Skeleton of Proof:

- $n = 1$: $f = aX^2$ has $\varepsilon = 1$ and $d = a$ is arbitrary.
- $n = 2$: $f = aX^2 + bY^2$ has $\varepsilon = (a, b) = (a, -ab)$. If $d = ab = -1$, then $\varepsilon = 1$. Conversely:
  - if $d = -1$, $\varepsilon = 1$: take $f = X^2 - Y^2$
  - if $d \neq -1$, since the Hilbert symbol is non-degenerate, there exists $a \in \mathbb{Q}_p^\times$ such that $(a, -d) = \varepsilon$. Take $f = aX^2 + adY^2$.
  - *(when $d = -1$, $f = X^2 - Y^2 = aX^2 + adY^2$)*
- $n = 3$: Choose $a \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ and $a \neq d$. There exsits form g of rank 2 s.t. $d(g) = ad, \varepsilon(g) = \varepsilon(a, -d)$. The form $f = g \oplus aZ^2$ works.
- $n > 3$: Take $f = g(X_1, X_2, X_3) \oplus X^2 \oplus \cdots \oplus X_n^2$.

Table of Contents

1. Motivation and Introduction
    - Quadratic Forms and Quadratic Spaces over Field.
    - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
    - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
    - Quadratic Forms over $\mathbb{Q}_p$
    - Quadratic Forms over $\mathbb{Q}$
3. Appendix
    - Lemmas Required for the Proof
    - Proof of Hasse-Minkowski Theorem

Quadratic Forms $f \sim g$ over $\mathbb{Q}$

Theorem (Hasse-Minkowski)

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

Theorem (([Ser73] p. 44, chap. 4, sec. 3.3, theorem 9))

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, then there exists $a \in \mathbb{Q}$ represented by both f and g.
- Thus $f \sim aZ^2 \oplus f_1$, $g \sim aZ^2 \oplus g_1$, where $\operatorname{rank} f_1 = \operatorname{rank} g_1 = n - 1$.
- By Witt's cancellation theorem, 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 $\mathbb{Q}$.

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

Proposition (Conclusion over $\mathbb{Q}$)

The invariants d_v and ε_v are not independent; they 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* $r + s = \mathrm{rank}$.
- $d_\infty = (-1)^s$
- $\varepsilon_\infty = (-1)^{s(s-1)/2}$

Let d, $(\varepsilon_v)_{v \in \mathbb{V}}$, *and* (r, s) *vertify the relations above, then there exists a quadratic form of rank* n *over* $\mathbb{Q}$ *having for invariants* d, $(\varepsilon_v)_{v \in \mathbb{V}}$, *and* (r, s).

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Lemmas

Lemma

Let $f_i \in \mathbb{Z}_p[X_1, \cdots, X_m]$ be homogeneous polynomials with p-adic integer coefficents. TFAE:

- *The f_i have a non trivial common zero in $(\mathbb{Q}_p)^m$*
- *The f_i have a common primitive zero(i.e. solution $(z, x, y) \not\equiv (0, 0, 0) (\operatorname{mod} p)$) in $(\mathbb{Z}_p)^m$*
- *For all $n > 1$, the f_i have a common primitive zero in $(\mathbb{Z}/p^n\mathbb{Z})^m$.*

Lemma

Let $a, b \in K^\times$ and let $K_b = K(\sqrt{b})$. For $(a, b) = 1 \iff a \in N(K_b^\times)$ of norms of elements of $K_b^\times$.

Lemmas

Lemma

Let $f = g \oplus -h$, TFAE:

- *f represents 0*
- *There exists $a \in K^\times$ which is represented by g and h.*

Theorem

Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^\times$ and let $(\varepsilon_{i,v})_{i\in I, v\in\mathbb{V}}$ be a family of numbers equal to ± 1. In order that there exists $x \in \mathbb{Q}\times$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in \mathbb{V}$ iff the following conditions be satisfied:

- *Almost all the $\varepsilon_{i,v} = 1$*
- *$\prod_{v\in\mathbb{V}} \varepsilon_{i,v} = 1$ for all $i \in I$*
- *For all $v \in \mathbb{V}$ there exists $x_v \in \mathbb{Q}_p^\times$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in I$.*

Lemmas

Theorem (Approximation Theorem)

Let $S \subseteq \mathbb{V}$ be a finite set. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense.

Lemma

All quadratic forms in at least 3 variavles over $\mathbb{F}_q$ have a non trivial zero.

Lemma

Suppose $p \neq 2$. Let f be a quadratic form with coefficients in $\mathbb{Z}_p$ whose discriminant $\det(\mathrm{a_{ij}})$ is invertible. Let $a \in \mathbb{Z}_p$, every primitive solution of the equation $f(x) \equiv a (\bmod p)$ lifts to a true solutons.

Table of Contents

1. Motivation and Introduction
   - Quadratic Forms and Quadratic Spaces over Field.
   - Review: Classification of Quadratic Forms over $\mathbb{R}$ and $\mathbb{F}_q$
   - Representing numbers by quadratic forms
2. Quadratic Forms over $\mathbb{Q}_p$ and $\mathbb{Q}$
   - Quadratic Forms over $\mathbb{Q}_p$
   - Quadratic Forms over $\mathbb{Q}$
3. Appendix
   - Lemmas Required for the Proof
   - Proof of Hasse-Minkowski Theorem

Proof

Theorem (Hasse-Minkowski)

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

- The necessity is trivial. W.L.O.G., $f = \sum_{i=1}^{n} a_i X_i^2$, $a_i \in \mathbb{Q}^\times$. By replacing f by $a_1 f$, we can soppose $a_i = 1$
- $n = 2$: Suppose $f = X_1^2 - aX_2^2$
    - f_∞ represents 0 implies $a > 0$. Let $a = \prod_{p \text{ prime}} p^{\nu_p(a)}$.
    - f_v represents 0 implies that $\nu_p(a)$ is even. Then a is a square, f represents 0 over $\mathbb{Q}$.

Proof

- $n = 3$: Suppose $f = X_1^2 - aX_2^2 - bX_3^2$, we can assume a, b are square-free and $|a| \leq |b|$. Proceed by induction on $m = |a| + |b|$.
- If $m = 2$, then $f = X_1^2 \pm X_2^2 \pm X_3^2$.
  - f_∞ represents 0 implies $f \neq X_1^2 + X_2^2 + X_3^2$.
  - In other cases, f represents 0 by $f(1, 1, 0)$.
- If $m > 2$, then $b \geq 2$, let $b = \pm p_1 \cdots p_k$.
- We need to show a is a square modulo p_i for all i.

Proof

- It is obvious if $a \equiv 0 \pmod{p_i}$.
- Otherwise, a is a p_i-adic unit.
- By hypothesis, $f = X_1^2 - aX_2^2 - bX_3^2$ represents 0, i.e. $z^2 - ax^2 - by^2$ has a nontrivial zero in $(\mathbb{Q}_{p_i})^3$.
- By the lemma, $z^2 - ax^2 - by^2$ has a primitive zero (z, x, y) in $(\mathbb{Z}_{p_i})^3$.
- We have $z^2 - ax^2 \equiv 0 \pmod{p_i}$.
- If $x \equiv 0 \pmod{p_i}$, then $z \equiv 0 \pmod{p_i}$.
- Then $p_i^2 \mid by^2 = z^2 - ax^2$, but $\nu_{p_i}(b) = 1$ implies $y \equiv 0 \pmod{p_i}$.
- Thus $(z, x, y) \equiv (0, 0, 0) \pmod{p_i}$, which is a contradiction, hence $x \not\equiv 0 \pmod{p_i}$.
- Moreover, $a = \left(\frac{z}{x}\right)^2$ is a square modulo p_i.
- Since $\mathbb{Z}/b\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i\mathbb{Z}$, a is a square modulo b.

Proof

- There exist t, b' integers such that $t^2 = a + bb'$.
- We can choose t such that $|t| \leq |\frac{b}{2}|$. $bb' = t^2 - a$ is a norm from $K(\sqrt{a})$ where $K = \mathbb{Q}$ or $\mathbb{Q}_p$.
- By above lemma $(a, bb') = 1$, hence $(a, b) = 1 \iff (a, b') = 1$.
- That means $f = X_1^2 - aX_2^2 - bX_3^2$ represents 0 iff $f' = X_1^2 - aX_2^2 - b'X_3^2$ represents 0.
- $|b'| = |\frac{t^2-a}{b}| \leq |\frac{t^2}{b}| + |\frac{a}{b}| \leq \frac{|b|}{4} + 1 \leq |b|$.
- Write $b' = u^2 b''$, where b'' is square-free. We have $|b''| \leq |b|$.
- The inductive hypothesis applies to $f'' = X_1^2 - aX_2^2 - b''X_3^2$, so it represents 0, and the same is true for f.

Proof

- $n = 4$: Suppose $f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. There exists $a \in K^\times$ which is represented by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$.
  - $(x_v, -ab)_v = (a, b)_v$ and $(x_v, -cd)_v = (c, d)_v$ for all $v \in \mathbb{V}$
  - By above theorem there exists $x \in \mathbb{Q}^\times$ s.t. $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$ for all $v \in \mathbb{V}$
  - This means $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$ represents x in $\mathbb{Q}_p$
  - i.e. $aX^2 + bY^2 - xZ^2$ represents 0 in all $\mathbb{Q}_v$ also $\mathbb{Q}$, and the same argument applied to $cX_3^2 + dX_4^2$, the fact that f represents 0 in $\mathbb{Q}$ follows from this.

Proof

- $n \geq 5$: we use induction on n. Suppose $f = h \oplus -g$ with $h = a_1X_1^2 + a_2X_2^2$, $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$.
- Let $S = \{p \in \mathbb{V} \mid \nu_p(a_i) \neq 0, i \geq 3\} \cup \{2, \infty\}$, it is a finite set.
- Let $v \in S$, f_v represents 0, so there exists $a_v \in \mathbb{Q}_v^\times$ which is represented by both h and g in $\mathbb{Q}_v$.
- That is, there exist $x_1^{(v)}, x_2^{(v)} \in \mathbb{Q}_v$ such that $h(x_1^{(v)}, x_2^{(v)}) = a_v$, and $x_3^{(v)}, \ldots, x_n^{(v)} \in \mathbb{Q}_v$ such that $g(x_3^{(v)}, \ldots, x_n^{(v)}) = a_v$.
- The set $\mathbb{Q}_v^{\times 2}$ is open in $\mathbb{Q}_v^\times$, so $\prod a_v Q_v^{\times 2}$ is also open in $\prod_{v \in S} \mathbb{Q}_v^\times$, and h is a continuous map.

Proof

- By the Approximation Theorem, there exists $a \in \mathbb{Q}^\times$ such that $a \in a_v Q_v^{\times 2}$ for all $v \in S$.
- Thus, $(x_1, x_2) \in (\mathbb{Q})^2$ s.t. $h(x_1, x_2) = a$, and $a/a_v \in \mathbb{Q}^{\times^2}$ for all $v \in S$.
- Consider $f_1 = aZ^2 \oplus -g$.
  - if $v \in S$, g represents a_v, also a since $a/a_v \in \mathbb{Q}^{\times^2}$.
  - if $v \notin S$, the coeffients are v-adic units, the $d(g)$ is also a unit. And because $v \neq 2$, we have $\varepsilon(g) = 1$.
- By above lemma, there exist a solution, and it lifts a true solution.
- In all case we see f_1 represents 0 in $\mathbb{Q}_v$, and $\operatorname{rank} f_1 = n - 1$.
- By inductive hypothesis: f_1 represents 0 in $\mathbb{Q}$. i.e. g represents a, and h represents a.
- The proof is complete.

References I

[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.