# REPRESENTATION, EQUIVALENCE, AND CLASSIFICATION OF QUADRATIC FORMS

SIMON LAPOINTE[†]

## 1. Introduction

A historically important problem in number theory is representation of numbers by quadratic forms. Let $k$ be a field, $(f, k^n)$ a quadratic module and $a$ an element of $k$. We say $f$ *represents* $a$ if there exists an element $x$ of $k^n$ such that $f(x) = a$. Given a quadratic module, we can ask which elements of $k$ are represented by $f$. This problem is completely solved by building criteria to determine when $f$ (or certain forms derived from it) represents 0. In other words, knowing when an arbitrary quadratic form represents 0 completely resolves the question. A related variation of this problem is to classify quadratic forms up to equivalence, where two forms are equivalent if they differ by a linear change of variables.

From now on, assume $k$ is a global field, i.e. an algebraic number field or a finite extension of a rational function field of positive characteristic. Let $V$ be the set of places of $k$, and for $v$ in $V$, denote $k_v$ the completion of $k$ at the place $v$. The Hasse–Minkowski theorem answers the question raised above in full. It says that a quadratic form represents 0 over $k$ if and only if it represents 0 over every completion $k_v$ of $k$. The forward direction is obvious, through the injection

$$k \hookrightarrow k_v.$$

The converse requires a lot more work and the present is concerned with providing a self-contained proof for the case $k = \mathbb{Q}$, as well as providing necessary and sufficient conditions to classify quadratic forms over $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$, and $\mathbb{C}$, as well as indefinite forms of determinant ±1 over $\mathbb{Z}$.

An arbitrary algebraic variety is said to *satisfy the Hasse principle* if the converse of the above holds, i.e. local solutions everywhere imply a global solution. The Hasse–Minkowski theorem can then be rephrased as: quadratic forms over global fields satisfy the Hasse principle. We present an explicit counterexample of a curve of degree greater than two violating the Hasse principle. The sections on the Hasse–Minkowski theorem and its preliminaries closely follow the material in [Ser73].

We use notational conventions from [Ser73]. All rings are integral domains and commutative. We denote fields by $k$ and rings by $R$. The dual of an $R$-module $V$ is denoted $V^* := \mathrm{Hom}_R(V, R)$. Quadratic forms are nondegenerate. We write $\mathbb{Q}_\infty = \mathbb{R}$.

I would like to thank Prof. Patrick Allen for his patience and guidance through this project. It was a pleasure to learn about this area of number theory, and this project could not have been completed without him.

[†] Department of Mathematics and Statistics, McGill University.

## 2. Preliminaries

2.1. **$p$-adic Fields.** This is a concise introduction to $p$-adic numbers. We start with valuations.

**Definition 2.1.** A valuation on an integral domain $R$ is a function $\nu : R \to \mathbb{Z} \cup \{\infty\}$ such that

(1) $\nu(a) = \infty \iff a = 0$
(2) $\nu(ab) = \nu(a) + \nu(b)$
(3) $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$

Fix a prime $p$. We define the *$p$-adic valuation* $\nu_p$ on $\mathbb{Z}$ as follows: for $x$ in $\mathbb{Z}$ and $x = p^n u$, where $p$ does not divide $u$, we have

$$\nu_p(x) = n.$$

This valuation induces the $p$-adic topology on $\mathbb{Z}$ through the $p$-adic metric:

$$d(x, y) = e^{-\nu_p(x-y)}.$$

This topology is said to *nonarchimedean* since for $x, y, z \in \mathbb{Z}$,

$$d(x, z) \leq \sup\{d(x, y), d(y, z)\}$$

This metric can be extended to $\mathbb{Q}$ by $\nu_p(x/y) = \nu_p(x) - \nu_p(y)$. The $p$-adic rationals can be constructed in two equivalent ways. If $\mathbb{Z}_p$ (respectively $\mathbb{Q}_p$) is the metric completion of $\mathbb{Z}$ (resp. $\mathbb{Q}$), then $\mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Q}_p$ canonically.

By a theorem of Ostrowski [Ost16], all nontrivial absolute values on $\mathbb{Z}$ are equivalent to either the euclidean absolute value $|\cdot|$ or to the $p$-adic absolute value $e^{-\nu_p}$ for some $p$. Hence, the metric completions of $\mathbb{Q}$ are $\mathbb{R}$ and $\mathbb{Q}_p$, for $p$ prime.

Here are a few facts about the $p$-adic integers and $p$-adic numbers. Units in $\mathbb{Z}_p$ are precisely those elements not divisible by $p$. Both rings are complete with respect to the $p$-adic metric. The integers $\mathbb{Z}$ (respectively $\mathbb{Q}$) are dense in $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$). The $p$-adic integers and the set of squares form open sets in $\mathbb{Q}_p$. Every element of $\mathbb{Q}_p$ can be written as $p^n u$, where $n$ is an integer and $u$ is invertible in $\mathbb{Z}_p$. The ring $\mathbb{Z}_p$ is precisely those $p^n u$ such that $n \geq 0$. The ring $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ has cardinality $2^r$, where $r = 3$ for $p = 2$ and $r = 2$ for $p \neq 2$.

There are two main analytics tools used in Hasse–Minkowski. The first is density of $\mathbb{Q}$ into $\mathbb{Q}_p$, so that every element of $\mathbb{Q}_p$ is a Cauchy sequence of rational numbers (considered as elements of the $p$-adics). The second is an analogue of Newton's method in $p$-adic analysis, Hensel's lemma.

**Theorem 2.2.** *Let $f$ be a polynomial in $\mathbb{Z}_p$ and $f'$ its derivative. Let $x \in \mathbb{Z}$, $n, k \in \mathbb{Z}$ be such that $0 \leq 2k < n$, $f(x) \equiv 0 \mod p^n$, and $\nu_p(f'(x)) = k$. Then, there exists $y \in \mathbb{Z}$ such that*

$$f(y) \equiv 0 \mod p^{n+1}, \quad \nu_p(f'(y)) = k, \quad y \equiv x \mod p^{n-k}$$

*Proof.* Write $y = x + p^{n-k} z$ with $z$ a $p$-adic integer. We will show we can choose $z$ so that it satisfies the conclusion of the lemma. By Taylor's formula, expand $f(y)$ as

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} a$$

for some $a$ in $\mathbb{Z}$. By hypothesis, we have $f(x) = p^n b$ and $f'(x) = p^k c$ for $b$ in $\mathbb{Z}_p$ and $c$ a $p$-adic unit. Hence, we can choose $z$ such that

$$b + zc \equiv 0 \mod p.$$

Hence, we get

$$f(y) = p^n(b + zc) + p^{2n-2k}a \equiv 0 \mod p^{n+1},$$

as $n > 2k$ and hence $2n - 2k > n$. Applying Taylor's formula to $f'(y)$, we get that $f'(y) \equiv p^k c \mod p^{n-k}$, so $\nu_p\left(f'(y)\right) = k$. □

**Corollary 2.3.** *Let $f$ be a polynomial in $\mathbb{Z}_p$ and $f'$ its derivative. Let $x \in \mathbb{Z}$ be such that $f(x) \equiv 0 \mod p^n$ for some $n > 0$, and $\nu_p\left(f'(x)\right) = k$ with $0 \leq 2k < n$. Then, $f$ has a $p$-adic zero.*

*Proof.* Use Theorem 2.2 to get a sequence of roots of $f$ modulo higher powers of $p$. These form a Cauchy sequence in $\mathbb{Z}_p$, and by completeness, we get existence of a root of $f$ in $\mathbb{Z}_p$. □

There is also a multivariable version of Theorem 2.2.

**Theorem 2.4.** *Let $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ and $j$ an integer with $0 \leq j \leq m$. Suppose $0 < 2k < n$ and*

$$f(x) \equiv 0 \mod p^n \quad \textit{and} \quad \nu_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

*Then, there exists $y \in (\mathbb{Z}_p)^m$ such that $f(y) = 0$ where $y \equiv x \mod p^{n-k}$.*

*Proof.* See [Ser73, Chapter II, Theorem 1]. □

**Corollary 2.5.** *Let $p$ be an odd prime. Let $f(X) = \sum a_{ij}X_iX_j$ be a homogeneous quadratic polynomial with coefficients $a_{ij} = a_{ji}$ in $\mathbb{Z}_p$ and $\det(a_{ij})$ invertible. Every primitive root of $f$ lifts to a true solution.*

*Proof.* By Proposition 2.4, it suffices to show one of the partial derivatives is nonzero modulo $p$. We have

$$\frac{\partial f}{\partial X_i} = 2\sum_{i,j} a_{ij}X_j,$$

and as $\det(a_{ij}) \not\equiv 0 \mod p$ and $x$ not divisible by $p$, one of the partial derivatives is $\not\equiv 0 \mod p$. □

An algebraic tool that will be used later is the Legendre symbol.

**Definition 2.6.** Let $p > 2$ be a prime and let $x \in \mathbb{F}_p$. The Legendre symbol of $x$ in $\mathbb{F}_p$, denoted $\left(\frac{x}{p}\right)$, is defined as

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{0, \pm 1\}$$

Note that whenever $x$ is nonzero, so is its Legendre symbol.

The Legendre symbol is useful since it detects squares, i.e.

**Proposition 2.7.** *Let $f : \mathbb{F}_p \to \mathbb{F}_p$ be the map $x \mapsto x^2$. Then,*

$$f(\mathbb{F}_p^*) = \left\{x \in \mathbb{F}_p : \left(\frac{x}{p}\right) = 1\right\}.$$

*Proof.* If $x = y^2$ is a square, then $\left(\frac{x}{p}\right) = \left(\frac{y^2}{p}\right) = y^{p-1} = 1$, where the last equality follows from Lagrange's theorem. Conversely, suppose $\left(\frac{x}{p}\right) = 1$ and fix an algebraic closure $\bar{\mathbb{F}}_p$ and pick a square root of $x$, say $y$. We need to show that $y \in \mathbb{F}_p$. We have $x^{\frac{p-1}{2}} = y^{p-1} = 1$ and so $y \in \mathbb{F}_p$, as this field is the precisely the set of fixed points of the map $x \mapsto x^{p-1}$ in the algebraic closure. □

Note that the Legendre symbol is multiplicative, and that the subgroup of squares in $\mathbb{F}_p^*$ has index 2.

### 2.2. Hilbert Symbol.

In this section, $k$ is either $\mathbb{R}$ or $\mathbb{Q}_p$ for some $p$.

**Definition 2.8.** Let $a, b \in k^*$. The Hilbert symbol of $a$ and $b$, denoted $(a, b)$, is defined as

$$(a,b) = \begin{cases} 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nonzero solution in } k \\ -1 & \text{otherwise} \end{cases}$$

We will need two functions $\epsilon, \omega : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, defined as

$$\epsilon(n) = \frac{n-1}{2} \mod 2$$
$$\omega(n) = \frac{n^2-1}{8} \mod 2$$

**Theorem 2.9.** *If $k = \mathbb{R}$, we have $(a, b) = 1$ if and only if at least one of $a, b$ is $> 0$. If $k = \mathbb{Q}_p$, $a = p^n\alpha$, and $b = p^m\beta$ with $\alpha, \beta \in \mathbb{Z}_p^\times$, then*

$$(a,b) = (-1)^{nm\epsilon(p)} \left(\frac{\alpha}{p}\right)^m \left(\frac{\beta}{p}\right)^n \quad \textit{if } p \neq 2$$
$$(a,b) = (-1)^{\epsilon(\alpha)\epsilon(\beta)+n\omega(\beta)+m\omega(\alpha)} \quad \textit{if } p = 2$$

*In the equations above, $\alpha$ and $\beta$ denote their respective image modulo $p$.*

*Proof.* See [Ser73, Chapter III, Theorem 1]. □

From Definition 2.8 and Theorem 2.9, we infer the following properties:

1. $(aa', b) = (a, b)(a', b)$ (bilinearity)
2. $(a, b) = (b, a)$ and $(a, c^2) = 1$
3. $(a, -a) = (a, 1 - a) = 1$
4. $(a, b) = (a, -ab) = (a, (1 - a)b)$
5. $(a, a) = (-1, a)$

It will be useful later to note that the Hilbert symbol is a nondegenerate bilinear form from $k^*/k^{*2}$ to $\{\pm 1\}$. The Hilbert symbol is closely tied to the group of norms of quadratic field extension.

**Proposition 2.10.** *Let $a, b$ be nonzero elements of $k$. Then, $(a, b) = 1$ if and only if $a$ is the norm of a nonzero element of $k(\sqrt{b})$.*

*Proof.* For the forward direction, if $b$ is a square, we are done ($a$ is its own norm). Otherwise, $z^2 - ax^2 - by^2$ has a solution with $(x, y, z) \neq 0$ and $x \neq 0$. The norm of

$$\frac{z}{x} + \sqrt{b}\frac{y}{x}$$

is $a$. Conversely, if $b$ is a square, we have $(a, b) = 1$. Otherwise, if $a$ is the norm of an element $z + \sqrt{b}y$ in $k(\sqrt{b})$, then $a = z^2 - by^2$ so $z^2 - ax^2 - by^2$ has a nontrivial solution and $(a, b) = 1$. □

From Theorem 2.9, we can derive a global result relating Hilbert symbols across different fields. Let $V$ be the union of all primes and $\{\infty\}$. Furthermore, for $a, b \in \mathbb{Q}^*$ and $v \in V$, let $(a, b)_v$ be the Hilbert symbol of $a, b$ in $\mathbb{Q}_v$.

**Theorem 2.11.** *Let $a, b \in \mathbb{Q}^*$. We have $(a, b)_v$ for all but finitely many $v$ and*

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

*Proof.* See [Ser73, Chapter III, Theorem 3]. □

In particular, Theorem 2.11 implies that if $(a, b)_v = 1$ for all $v \in V$ *except at most one*, say $w \in V$, then $(a, b)_w = 1$.

Finally, we present conditions for existence of rational $x$ with given Hilbert symbols.

**Theorem 2.12.** *Let $I$ be an index set and let $(a_i)$ be a family of nonzero rationals and $(\epsilon_{i,v})$ be a numbers equal to $\pm 1$ with $v \in V$. There exists a nonzero rational $x$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I$ and $v \in V$, if and only if*

1. *All but finitely many $\epsilon_{i,v}$ are equal to 1.*
2. *For all $i \in I$ we have $\prod_{v \in V} \epsilon_{i,v} = 1$.*
3. *For all $v \in V$, there is a nonzero $x_v \in \mathbb{Q}_v$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.*

*Proof.* See [Ser73, Chapter III, Theorem 4]. □

2.3. **Quadratic Forms.** We discuss definitions and basic facts about quadratic forms. Fields considered below have characteristic not equal to 2. Let $V$ be a finitely generated $R$-module (for the current discussion, usually a vector space).

**Definition 2.13.** A quadratic form of rank $n$ over $R$ is a homogeneous polynomial of the form

$$f(x) = \sum_{i,j} a_{ij} x_i x_j,$$

where $a_{ij} = a_{ji}$. Associated to this polynomial is a unique symmetric matrix $A$ defined by the coefficients $a_{ij}$. The pair $(V, f)$ is called a quadratic module.

Importantly, a quadratic form satisfies $f(ax) = a^2 f(x)$, for all $a \in R$. An example of a quadratic form is $7x^2 - 3xy + 4y^2$, with matrix

$$A = \begin{bmatrix} 7 & -\frac{3}{2} \\ -\frac{3}{2} & 4 \end{bmatrix}.$$

From now on, unless otherwise specified, we work with $R = k$ a field. We will also use $f$ and $A$ interchangeably, depending on which object we need. Quadratic forms are partitioned into equivalence classes. The equivalence class of $A$ is defined as:

$$\left\{ B^T A B : B \in \mathrm{GL}_n(k) \right\},$$

i.e. quadratic forms equivalent to $f$ are those which differ from $f$ by a linear change of variables. If $f$ and $g$ are equivalent, we write $f \sim g$. An invariant associated to $f$ is the *discriminant* of $f$, denoted $\mathrm{Disc}(f)$, and defined by $\mathrm{Disc}(f) = \det A$. It is defined up to a square in $k$ since $\det X = \det X^T$. The squarefree determinant and the rank of a form are invariants of its equivalence class. These invariants will play an important role in classification of quadratic forms later on. For each quadratic form there is an associated symmetric bilinear form $\langle x, y\rangle$. For $x, y$ in $V$, it is defined by

$$\langle x, y\rangle = \frac{1}{2}\left[f(x+y) - f(x) - f(y))\right].$$

Conversely, for each symmetric bilinear form $\langle x, y\rangle$ we have a quadratic form defined by

$$f(x) = \langle x, x\rangle$$

This simplifies the study of quadratic forms as it reduces it to the study of bilinear forms, which can be analysed using linear algebra. From now on, we have $(V, f)$ a quadratic module with associated matrix $A$ and bilinear form $\langle\cdot,\cdot\rangle$. A quadratic form is said to be *nondegenerate* if, for every $x \in V$, there is some $y \in V$ such that $\langle x, y\rangle \neq 0$. An equivalent criterion uses the discriminant: $f$ is nondegenerate if and only if $\mathrm{Disc}(f) \neq 0$. Let $q_V : V \to V^*$ the map sending an element $x \in V$ to the bilinear form $B(x, y)$. Then, $f$ is nondegenerate if and only if $q_V$ is an isomorphism.

An element $x \in V$ such that $f(x) = 0$ is called *isotropic*. Let $S$ be a subset fo $V$. Then,

$$S^0 := \{x \in V : B(x, y) = 0 \text{ for all } y \in S\}$$

is called the *orthogonal complement* of $S$.

We will now show that $f$ representing 0 implies $f(V) = k$.

**Definition 2.14.** A quadratic module of dimension 2 with basis consisting of isotropic vectors $x, y$ such that $\langle x, y\rangle \neq 0$ is called a hyperbolic plane.

By rescaling $y$, we can suppose that $\langle x, y\rangle = 1$. The quadratic form associated with a hyperbolic plane is $X^2 - Y^2$. A hyperbolic plane has discriminant $-1$.

**Lemma 2.15.** *Let $x$ be a nonzero isotropic element of a quadratic module. There is a hyperbolic plane of $V$ containing $x$.*

*Proof.* By nondegeneracy, there is $y \in V$ such that $\langle x, y\rangle = 1$. Then, $z = 2y - f(y)x$ is such that $f(z) = 0$ and $\langle z, x\rangle \neq 0$. Hence, $U = kx + kz$ is a hyperbolic plane. □

**Proposition 2.16.** *If $(V, f)$ contains an isotropic element, $f$ represents all of $k$.*

*Proof.* If $(V, f)$ contains an isotropic element $x$, it contains a hyperbolic plane generated by, say, $x$ and $y$. Furthermore, we can assume $\langle x, y\rangle = 1$. Let $a$ be any element of $k$. Then,

$$f\left(x + \frac{a}{2}y\right) = a.$$

□

As the above fact relies on the existence of inverse elements, it does not hold for general integral quadratic forms. Next, it is interesting (and useful) to note that every quadratic form over $k$ is equivalent to a diagonal form, i.e. every quadratic module has an orthogonal basis.

**Proposition 2.17.** *If $(V, f)$ is a quadratic module, then $V$ has an orthogonal basis.*

*Proof.* Induction on $\dim V$. The case $\dim V = 0$ is trivial. Suppose $\dim V = n$. If $V$ is isotropic then every basis is orthogonal (expand $f(e_i + e_j) = 0$). Otherwise, pick $e$ such that $\langle e, e\rangle \neq 0$ and let $H := (ke)^0$. We have the decomposition $V = ke \oplus H$. The second summand has dimension $n - 1$ and so by the inductive hypothesis it has an orthogonal basis $\{e_1, \cdots, e_{n-1}\}$, so $\{e, e_1, \cdots, e_{n-1}\}$ is an orthogonal basis for $V$. □

Whenever a form $f$ represents $a \in k^*$, it is equivalent to a useful decomposition.

**Proposition 2.18.** *Let $f$ be a form of rank $n$ and let $a$ be an element of $k^*$. The following are equivalent:*

1. *$f$ represents $a$.*
2. *$f \sim g + aZ^2$ where the rank of $g$ is $n - 1$.*
3. *$g := f - aZ^2$ represents 0.*

*Proof.* Clearly $2 \Rightarrow 1 \Rightarrow 3$. For $1 \Rightarrow 2$, suppose $x \in V$ is such that $f(x) = a$. Then, $V = kx \oplus (kx)^0$, so $f \sim aZ^2 + g$, where $P$ is the form associated to $(kx)^0$. It remains to show $3 \Rightarrow 1$. Suppose $g$ has a nontrivial isotropic element $(x_1, \cdots, x_n, z)$. Either $z = 0$ so $f$ represents 0 and thus $a$ by proposition 1, or $z \neq 0$ and $f[(x_1/z, \cdots, x_n/z)] = a$. □

We have a cancellation law for quadratic forms.

**Proposition 2.19.** *Let $f = g + h$ and $f' = g' + h'$ be nondegenerate quadratic modules. If $f \sim f'$ and $g \sim g'$, then $h \sim h'$.*

*Proof.* See [Ser73, Chapter IV, Theorem 4]. □

2.4. **Invariants.** The most efficient way of classifying quadratic forms over a field is to obtain a criterion differentiating between equivalence classes. In particular, we can define invariants associated to equivalence classes which completely answer the classification question.

We have already seen two invariants. First, for a form $f$, the rank $n$ is an invariant. Another is the discriminant of the form (modulo squares in $k$). We also have a new invariant for real quadratic forms, the *signature*. We first present a result (see [Syl52] for original proof).

**Proposition 2.20.** *(Sylvester's Law of Inertia) Two real symmetric matrices $A$ and $B$ have the same number of positive, negative and zero eigenvalues if and only if they are congruent, i.e.*

$$A = SBS^T$$

*for some invertible matrix $S$.*

**Proposition 2.21.** *Let $f$ be a real quadratic form of rank $n$. Then, $f$ is equivalent to a diagonal form*

$$\pm X_1^2 \pm X_2^2 \pm \cdots \pm X_n^2.$$

*If $r$ denotes the number of 1's and $s$ the number of $-1$'s, then $(r, s)$ is an invariant associated to the class of $f$, and is called the signature of $f$.*

*Proof.* We first show that such a diagonal form exists. By Proposition 2.17, $f$ is equivalent to a diagonal form

$$a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2,$$

where $a_i \neq 0$ for all $i$. This form has associated matrix $A = \operatorname{diag}(a_1, a_2, \ldots, a_n)$. Let

$$X = \operatorname{diag}\left(\frac{1}{\sqrt{|a_1|}}, \frac{1}{\sqrt{|a_2|}}, \cdots, \frac{1}{\sqrt{|a_n|}}\right).$$

The form $A$ is equivalent to $X^TAX$, which has the desired property. Signature is a well-defined invariant by Proposition 2.20. □

In $\mathbb{R}$, every nonnegative element has a well defined square root. Over $\mathbb{C}$, however, every element has a square root, so every quadratic form is equivalent to $\operatorname{diag}(1, 1, \ldots, 1)$, and so there is only one equivalence class of forms for a given rank.

Note that the rank of a real quadratic form is $r(f) = r + s$. A form is said to be *definite* if either $r = 0$ or $s = 0$. Otherwise, it is said to be *indefinite.* the signature completely classifies quadratic forms over $\mathbb{R}$, since if two forms have the same signature, they are equivalent to the same diagonal form and thus to each other.

From the signature, we can also define the *torsion* of $f$ as $\tau(f) = r - s$. This will come in handy when classifying forms over $\mathbb{Z}$ later on.

Suppose $f$ is equivalent to $a_1X_1^2 + a_2X_2^2 + \cdots + a_nX_n^2$. Another invariant is $\epsilon(f)$:

$$\epsilon(f) = \prod_{i<j}(a_i, a_j).$$

It does not depend on the choice of basis for $V$ and is therefore an invariant attached to $f$.

We therefore have four invariants:

(1) The rank $r(f)$.
(2) The discriminant $\operatorname{disc}(f) = \det A$.
(3) For real quadratic forms, the signature $(r, s)$.
(4) The invariant defined by the diagonal form, $\epsilon(f) = \prod_{i<j}(a_i, a_j)$.

## 3. Representation and Equivalence

3.1. **Representation of Elements by Quadratic Forms.** The conditions for a real quadratic form to represent elements of $\mathbb{R}$ are simple.

**Proposition 3.1.** *Let $f$ be a real quadratic form. If $f$ is definite, it represents every $x > 0$ or every $x < 0$. If it is indefinite, it represents all of $\mathbb{R}$.*

*Proof.* For $x \neq 0$, the image of the map $x \mapsto x^2$ is the positive reals. For definite $f$, if $s = 0$, then $f \sim X_1^2 + \cdots + X_n^2$, so it represents the positive reals. Similarly, if $r = 0$, then $f$ represents the negative reals. If $f$ is indefinite, it represents 0 and thus all of $\mathbb{R}$. □

If there is risk of ambiguity, we denote the invariants of a form $f$ as: $d_f$ for the discriminant, $\epsilon_f$ for the $\epsilon$-invariant. For forms over $k = \mathbb{Q}_p$, we need a technical lemma. Recall the following fact from section 2: $S := \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ has cardinality $2^r$, where $r = 3$ for $p = 2$ and $r = 2$ for $p \neq 2$.

**Lemma 3.2.** *Let $a, a' \in S$, $\epsilon, \epsilon' = \pm 1$, and $H_a^\epsilon$ be the set of those $x \in S$ such that $(a, x) = \epsilon$. If $a = 1$, $|H_a^1| = 2^r$ and if $a \neq 1$, $|H_a^\epsilon| = 2^{r-1}$. Furthermore, $H_a^\epsilon$ and $H_{a'}^{\epsilon'}$ are nonempty and disjoint if and only if $a = a'$ and $\epsilon = -\epsilon'$.*

*Proof.* If $a = 1$, then $(a, x) = 1$ for all $x \in S$, so $|H_a^1| = 2^r$. Otherwise, the map $S \to \{\pm 1\}$ defined by $x \mapsto (a, x)$ is a surjective homomorphism (by nondegeneracy and bilinearity, respectively). It has kernel $H_a^1$, which has index 2 in $S$, hence the result.

For the second part of the lemma, suppose $H_a^\epsilon$ and $H_a^{\epsilon'}$ are nonempty and disjoint. Both sets must have cardinality $2^{r-1}$, and $H_a^1 \cap H_{a'}^1 \neq \emptyset$ (e.g. 1 is in both). Hence, $H_a^{-1} \cap H_{a'}^{-1} \neq \emptyset$ and so $\epsilon \neq \epsilon'$, or in other words $\epsilon = -\epsilon'$. To show $a = a'$, we argue by contradiction. Suppose $a \neq a'$. By nondegeneracy, we can find $x \in S$ such that $(x, aa') = (x, a)(x, a') = -1$. If $x \in H_a^\epsilon \cap H_{a'}^{\epsilon'}$, we get a contradiction. Else, $x$ is in $H_a^{-\epsilon} \cap H_{a'}^{-\epsilon'}$ and since the $H_a^\epsilon$'s partition $S$, we have $H_a^\epsilon \cap H_{a'}^{\epsilon'} \neq \emptyset$. In all cases, we get a contradiction.

For the converse, we can assume without loss of generality that $\epsilon = 1 = -\epsilon'$. Since $a = a' \neq 1$, $H_a^\epsilon$ and $H_a^{\epsilon'}$ are obviously disjoint, and are nonempty by nondegeneracy of the Hilbert symbol. □

We can now state the main result of this section.

**Theorem 3.3.** *Let $f$ be a rank $n$ quadratic form over $\mathbb{Q}_p$ with discriminant $d$ and invariant $\epsilon$. This form represents 0 if and only if:*

1. *$n = 2$ and $d = -1$,*
2. *$n = 3$ and $(-1, -d) = \epsilon$,*
3. *$n = 4$ and either $d \neq 1$ or $d = 1$ and $(-1, -1) = \epsilon$,*
4. *$n \geq 5$.*

Recall from Proposition 2.18 that a form $g$ represents $a \in k^*$ if and only if $g - aZ^2$ represents 0. By the theorem, if $g = a_1X_1^2 + a_2X_2^2$ has rank 2, this happens if and only if $(-1, -ad_g) = \epsilon_g(a_1, -a)(a_2, -a)$, which is equivalent to

$$(-1, a)(-1, -d_g) = \epsilon_g(d_g, -a) \Rightarrow (-d_g, a) = \epsilon_g$$

We now prove the theorem.

*Proof.* ($n = 2$) A form $a_1X_1^2 + a_2X_2^2$ in two variables represents 0 if and only if $-a_1/a_2 = 1$ in $S$ (i.e. is a square), if and only if $-a_1/a_2 = -a_1a_2 = -d = 1$, or $d = -1$.

($n = 3$) A form $f = a_1X_1^2 + a_2X_2^2 + a_3X_3^2$ represents 0 if and only if $a_3f = a_1a_3X_1^2 + a_2a_3X_2^2 + X_3^2$ represents 0. Hence, we can assume $a_3 = 1$ and work with the form $a_1X_1^2 + a_2X_2^2 + X_3^2$. By the definition of the Hilbert symbol, this form represents 0 if and only if

$$(-a_1a_3, -a_2a_3) = 1,$$

Expanding all of $(-a_1a_3, -a_2a_3)$,

$$(-a_1a_3, -a_2a_3) = (-1, -1)(-1, a_2)(-1, a_1)(a_1, a_2)(a_1, a_3)(a_2, a_3)(a_3, a_3).$$

Using the fact that $(a, a) = (a, -1)$ we find that

$$(-1, -d)(a_1, a_2)(a_1, a_3)(a_2, a_3) = 1,$$

which is precisely $(-1, -d)\epsilon = 1$, or $(-1, -d) = \epsilon$.

($n = 4$) A form $a_1x_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2$ represents 0 if and only if there is some $a \in k$ such that both $a_1x_1^2 + a_2X_2^2$ and $-a_3X_3^2 - a_4X_4^2$ represent $a$. By the remark below the statement of the theorem, such an $a$ satisfies

$$(a, -a_1a_2) = (a_1, a_2) \text{ and } (a, -a_3a_4) = (-a_3, -a_4)$$

Let $A$ be those $a$ in $S$ such that $a$ satisfies the first condition and $B$ the set of element satisfying the second condition. Then, the rank 4 form represents 0 if and only if $A \cap B \neq \emptyset$. Note that $A$ and $B$ are nonempty, as $a_1 \in A$ and $-a_3 \in B$, for example. Thus, by the lemma above, $A$ and $B$ have empty intersection if and only if

$$a_1 a_2 = a_3 a_4 \text{ and } (a_1, a_2) = -(-a_3, -a_4)$$

The first equality implies $d = 1$. We have, from the definition of $\epsilon$ and the two equalities above,

$$\begin{aligned}\epsilon &= (a_1, a_2)(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)(a_3, a_4) \\ &= (a_1, a_2)(a_1, a_3a_4)(a_2, a_3a_4)(a_3, a_4) \\ &= (a_1, a_2)(a_3a_4, a_3a_4)(a_3, a_4) \\ &= (a_1, a_2)(a_3, a_4)(-1, a_3a_4) = -(-1, -1),\end{aligned}$$

where the last equality follows from the second condition. Hence, we have $A \cap B$ if and only if either $d \neq 1$ or $d = 1$ and $\epsilon = (-1, -1)$.

($n \geq 5$) By the remark stated below the theorem, we see that at least $2^{r-1}$ elements of $S$ are represented by an arbitrary forms of rank 2, and so the same is true for a form of rank 5. Since $2^{r-1} \geq 2$ for all primes, a form $f$ of rank 5 represents an element of $S$ distinct from $d_f$. Hence,

$$f \sim g + aZ^2,$$

where $g$ is a form of rank 4. We have $d_f = d_g a$, which implies $d_g = d_f a \neq 1$, and so $g$ represents 0. We therefore have that $f$ represents 0. □

As we will see later, the induction step in the proof of the Hasse–Minkowksi theorem starts at rank 5. This is because all forms of rank 5 and above over $\mathbb{Q}_p$ satisfy the condition for forms of rank 4 to represent 0.

Implied by Proposition 2.18 and Theorem 3.3 is the following corollary.

**Corollary 3.4.** *Let $a \in \mathbb{Q}_p^*$. A quadratic form $f$ represents $a$ if and only if*

(1) $n = 1$ *and* $a = d$ *(in $S$),*
(2) $n = 2$ *and* $(a, -d) = \epsilon$,
(3) $n = 3$ *and either* $a \neq -d$ *or* $a = -d$ *and* $(-1, -d) = \epsilon$,
(4) $n \geq 4$.

*Proof.* Apply Theorem 3.3 to the form $g = f - aZ^2$, which has invariants $d_g = d_f a$ and $\epsilon_g = (a, d_f)\epsilon_f$. □

### 3.2. **Hasse–Minkowski theorem.** We come to the main result.

**Theorem 3.5.** *A quadratic form $f$ over the rationals represents 0 in $\mathbb{Q}$ if and only if $f_v$ represents 0 in $\mathbb{Q}_v$ for all $v$.*

*Proof.* The forward direction is trivial, as $\mathbb{Q}$ is a subfield of $\mathbb{Q}_v$ for all $v$. We assume, without loss of generality, that $f$ is in monic diagonal form, i.e. that $a_1 = 1$. The proof proceeds by induction on the rank, with base cases $n = 2$, $n = 3$, and $n = 4$.

($n = 2$) We have $f = X_1^2 - aX_2^2$, and since $f_\infty$ represents 0, we have $a > 0$. Furthermore, since $f_v$ represents 0 in all $p$-adic fields, $a$ is a square in all such fields. In particular, $\nu_p(a)$ is even for all $p$. Decompose $a$ in prime factors as

$$a = \prod_p p^{\nu_p(a)},$$

which shows $a$ is a square in $\mathbb{Q}$, and so $f$ represents 0.

($n = 3$) This proof is due to Legendre. We have $f = X_1^2 - aX_2^2 - bX_3^2$. We assume $a$ and $b$ are squarefree and that $|b| \geq |a|$. We use induction on $m := |b| + |a|$. If $m = 2$, then $a = \pm 1$ and $b = \pm 1$. We can't have $a = b = -1$ since $f_\infty$ represents 0. In all other cases, $f$ represents 0. For the induction step, suppose $m > 2$. We have $|b| \geq 2$, and suppose its prime decomposition is $b = \pm p_1 \cdots p_n$. We show $a$ is a square mod $p_i$ for all $i$. If $a \equiv 0 \mod p_i$, we are done. Otherwise, by multiplying by an appropriate power of $p_i$, we can find a primitive triple $(x, y, z)$ of $p_i$-adics such that $z^2 - ax^2 - by^2 = 0$. We have

$$z^2 - ax^2 \equiv 0 \mod p_i.$$

If $x \equiv 0 \mod p_i$, then $z \equiv 0 \mod p_i$ and so reducing the original equation mod $p_i^2$ tells us that $by^2 \equiv 0 \mod p_i^2$ and since $b$ is squarefree we have $y \equiv 0 \mod p_i$, contradicting the fact $(x, y, z)$ is primitive. Hence $x \not\equiv 0 \mod p_i$, and $a$ is a square mod $p_i$. By the chinese remainder theorem, $a$ is also a square modulo $b$. We therefore have

$$bb' = t^2 - a$$

where we choose $t$ such that $|t| \leq |b|/2$. The integer $bb'$ is a norm of $k(\sqrt{a})$ where $k$ is the field of rationals or the $p$-adics. By Proposition 2.10 and expanding $(bb', a) = 1$, $f$ represents 0 in $\mathbb{Q}$ and $\mathbb{Q}_p$ if and only if

$$f' = X_1^2 - aX_2^2 - b'X_3^2$$

represents 0 in $\mathbb{Q}$ and $\mathbb{Q}_v$. Hence, $f'$ represents 0 in all $\mathbb{Q}_v$. Denote $b''$ the squarefree part of $b'$. We have

$$|b''| \leq |b'| = \left|\frac{t^2 - a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|$$

and by the induction hypothesis the form $f'' = X_1^2 - aX_2^2 - b''X_3^2$ represents 0 in $\mathbb{Q}$. It is equivalent to $f'$ and thus to $f$, and so $f$ represents 0 in $\mathbb{Q}$.

($n = 4$) Split the quadratic form in two rank 2 forms as

$$aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2).$$

As $f_v$ represents 0 for all $v$, there is some nonzero $x_v$ (possibly depending on $v$) represented by both rank 2 forms above. By Corollary 3.4, this is true if and only if

$$(x_v, -ab)_v = (a, b)_v \text{ and } (x_v, -cd)_v = (c, d)_v.$$

Applying Theorem 2.11 and Theorem 2.12, we obtain the existence of a nonzero rational $x$ represented by both rank 2 forms. Hence,

$$aX_1^2 + bX_2^2 - xZ^2$$

represents 0 in $\mathbb{Q}_v$ for all $v$ and by the case $n = 3$ it represents 0 in $\mathbb{Q}$. The same argument applies to $cX_3^2 + dX_4^2 - xZ^2$, so both rank 2 forms represent $x$ and thus 0 over $\mathbb{Q}$.

($n \geq 5$) This is the induction step. Write the form $a_1X_1^2 + \cdots + a_nX_n^2$ as the sum of a rank 2 form $g$ and a rank $n-2$ form $h$:

$$f = g - h.$$

Let $S$ be the subset of $V$ containing $\infty, 2$, and all primes $p$ such that $v_p(a_i) \neq 0$ for some $i \geq 3$. This set is finite. Let $v \in S$. There is some nonzero $a_v$ represented by both $g_v$ and $h_v$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_v$ (and in any finite product of such fields), we can choose a pair of rationals $(x_1, x_2)$ such that $a = g(x_1, x_2)$ has the property that $a/a_v$ is arbitrarily close to 1 for all $v \in S$. Since the set of squares is open in $\mathbb{Q}_v$, $x_1, x_2$ can be chosen such that $a/a_v$ is a square. Consider the form

$$h_1 = aZ^2 - h.$$

If $v \in S$, since $h$ represents $a_v$, it also represents $a$ so $h_1$ represents 0. Otherwise, the coefficients of $h$ are $v$-adic units, so $d_h$ considered in $\mathbb{Q}_v$ is as well. As $v \neq 2$, we have $\epsilon_h = 1$ (the Hilbert symbol is trivial on units, away from places $2, \infty$ by Theorem 2.9) and so by Corollary 3.4, $h_1$ represents 0. The rank of $h_1$ is $n - 1$ so by the inductive hypothesis it represents 0 over $\mathbb{Q}$. This implies $h$ represents $a$ over $\mathbb{Q}$, and since $g$ represents $a$, $f$ represents 0 over $\mathbb{Q}$. We are done. □

As we will see later, this result need not hold for cubic forms or general curves. We now present a few corollaries.

**Corollary 3.6.** *A quadratic form of rank $\geq 5$ represents 0 over $\mathbb{Q}$ if and only if it is indefinite.*

*Proof.* By Theorem 3.5, such a form represents 0 over $\mathbb{Q}$ if and only if it represents 0 over $\mathbb{Q}_v$ for all $v$. A form of rank $\geq 5$ represent 0 over $\mathbb{Q}_p$ and represents 0 over $\mathbb{R}$ if and only if it is indefinite, hence the result. □

**Corollary 3.7.** *A quadratic form $f$ represents $a$ in $\mathbb{Q}$ if and only if it does in $\mathbb{Q}_v$ for all $v$.*

*Proof.* Apply Theorem 3.5 to the form $f - aZ^2$. □

Corollary 3.7 answers in full the question asked in the introduction (representation of an element of $\mathbb{Q}$). The result is computationally remarkable, since it reduces an *a priori* infinite problem (testing all rational $n$-tuples) to a finite computation of invariants (invariants in $\mathbb{Q}_v$).

**Corollary 3.8.** *Suppose $f$ has rank 3 (resp. rank 4 and discriminant 1). If $f$ represents 0 in all $\mathbb{Q}_v$ except at most one, then it represents 0 over $\mathbb{Q}$.*

*Proof.* By Theorem 3.3, a form $f$ of rank 3 represents 0 in $\mathbb{Q}_v$ if and only if

$$(-1, -d)_v = \epsilon_v.$$

Both sides of the equation satisfy the product formula of Theorem 2.11. Hence, if this equation is true for all but one $v$, it is true for all $v$, and $f$ represents 0 in $\mathbb{Q}$ by Theorem 3.5. For rank 4 and $d = 1$, replace the above equation by $(-1, -1)_v = \epsilon_v$ and use the same argument. □

### 3.3. **Equivalence of Forms.**

We answer the question of classification raised in the introduction.

**Theorem 3.9.** *Let $f$ and $f'$ be two rational quadratic forms. They are equivalent over $\mathbb{Q}$ if and only if they are equivalent over $\mathbb{Q}_v$ for all $v$.*

*Proof.* The forward direction is obvious. For the converse, we use induction on the rank $n$. The statement is clearly true for $n = 0$. For the induction step, suppose $f$ and $f'$ are equivalent over all $\mathbb{Q}_v$, and that $f$ represents some nonzero rational $a$. By equivalence of forms, $f$ and $f'$ have the same invariants. Hence, $f'$ represents $a$ and we have

$$f \sim aZ^2 + g \quad \text{and} \quad f' \sim aZ^2 + g'$$

By Proposition 2.19, we have $g \sim g'$ over all $\mathbb{Q}_v$ and by the inductive hypothesis, $g \sim g'$ over $\mathbb{Q}$ and thus $f \sim f'$ over $\mathbb{Q}$. □

## 4. Integral Quadratic Forms

Following [Ser73], we present a classification of indefinite integral forms of discriminant ±1. We denote by $E$ a free abelian group of rank $n$, which we endow with a symmetric bilinear form, thereby making it a quadratic module over $\mathbb{Z}$. In this section, two quadratic modules $(E_1, f_1)$ and $(E_2, f_2)$ are *isomorphic* if $E_1 \cong E_2$ as $\mathbb{Z}$-modules and $f_1 \sim f_2$.

From now on, we work with quadratic modules $(E, f)$ over $\mathbb{Z}$, where $f$ has discriminant ±1. We often refer to $E$ as a module or as a quadratic form interchangeably, where $f$ is implied or clear from the context.

### 4.1. **Basics and Invariants.**

We have already introduced rank, signature, torsion, and discriminant. These all apply to integral forms. Recall that if the signature of a form $f$ is $(r, s)$, the torsion is $\tau_f = r - s$ and the rank is $\mathrm{rk}_f = r + s$. Note that $\tau_f \equiv \mathrm{rk}_f \mod 2$, and that a form is definite if and only if $|\tau_f| = \mathrm{rk}_f$. The matrix associated to $f$ is a symmetric element $A = (a_{ij})$ of $\mathrm{GL}_n(\mathbb{Z})$. Hence, its polynomial form is

$$f(x) = \sum_i a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j .$$

The equivalence class of $A$ is defined in the same way as before, with change-of-basis matrices being elements of $\mathrm{GL}_n(\mathbb{Z})$. A form $f$ which is zero when reduced modulo 2 is said to be of Type II. Otherwise, it is of Type I. In other words, $f$ is of Type II if and only if diagonal terms of its associated matrix are all even. For example, $2x^2 - 6xy - 4y^2$ is of Type II and $4x^2 + 2xy - y^2$ is of Type I.

Recall from Section 2 that given a quadratic module $(E, f)$ with associated bilinear form $\langle x, y\rangle$, $f$ has invertible determinant (in $\mathbb{Z}$, ±1) if and only if $x \mapsto \langle x, y\rangle$ is an isomorphism $E \to E^*$. Let $\bar{E} := E/2E$, the reduction of $E$ modulo 2. The bilinear form $\langle x, y\rangle$ on $E$ defines a bilinear form $\overline{\langle \bar{x}, \bar{y}\rangle}$ on $\bar{E}$. Furthermore, $\overline{\langle \cdot, \cdot\rangle}$ gives rise to a quadratic form $\overline{\langle \bar{x}, \bar{x}\rangle}$ of discriminant $\pm 1 = 1$. This quadratic form is linear, since $x^2 = x \mod 2$ for all $x$:

$$\overline{\langle \bar{x} + \bar{y}, \bar{x} + \bar{y}\rangle} = \overline{\langle \bar{x}, \bar{x}\rangle} + \overline{\langle \bar{y}, \bar{y}\rangle} + 2\overline{\langle \bar{x}, \bar{y}\rangle} = \overline{\langle \bar{x}, \bar{x}\rangle} + \overline{\langle \bar{y}, \bar{y}\rangle},$$

and is therefore an element of the dual of $\bar{E}$. Since $\overline{\langle \bar{x}, \bar{x}\rangle}$ has discriminant ±1, we have an isomorphism $\bar{E} \to \bar{E}^*$ and hence an element $\bar{u}$ of $\bar{E}$ such that

$$\overline{\langle \bar{u}, \bar{x}\rangle} \equiv \overline{\langle \bar{x}, \bar{x}\rangle} \mod 2$$

for all $\bar{x} \in \bar{E}$. Lifting $\bar{u}$ to $E$ (this lifting is unique modulo 2), we get $u$ such that $\langle u, x\rangle \equiv \langle x, x\rangle \mod 2$. Then,

$$\langle u + 2x, u + 2x\rangle = \langle u, u\rangle + 4\left(\langle u, x\rangle + \langle x, x\rangle\right) \equiv \langle u, u\rangle \mod 8,$$

So the integer $\sigma_E = \langle u, u\rangle \mod 8$ is an invariant of the quadratic module $(E, f)$.

The direct sum of two quadratic modules $(E_1, f_1)$ and $(E_2, f_2)$, denoted $E_1 \oplus E_2$, is defined as the direct sum of $E_1$ and $E_2$ as $\mathbb{Z}$-modules endowed with the bilinear form

$$\langle x_1 + x_2, y_1 + y_2\rangle = \langle x_1, x_2\rangle + \langle y_1, y_2\rangle .$$

Hence, the quadratic form associated with the direct sum is

$$\langle x_1 + x_2, x_1 + x_2\rangle = f_1(x_1) + f_2(x_2).$$

Invariants are well-behaved with respect to direct sums. If $E = E_1 \oplus E_2$, then

(1) $\mathrm{rk}_E = \mathrm{rk}_{E_1} + \mathrm{rk}_{E_2}$
(2) $\tau_E = \tau_{E_1} + \tau_{E_2}$
(3) $\sigma_E = \sigma_{E_1} + \sigma_{E_2}$
(4) $\mathrm{disc}_E = \mathrm{disc}_{E_1} \cdot \mathrm{disc}_{E_2}$

4.2. **Examples.** Let us look at some examples. Denote by $I_+$ (respectively $I_-$) the $\mathbb{Z}$-module $\mathbb{Z}$ with the bilinear form $\langle x, y\rangle = xy$ (resp. $\langle x, y\rangle = -xy$). It has quadratic form $x^2$ (resp. $-x^2$). The invariants associated to a direct sum of the form

$$rI_+ \oplus sI_-$$

are $\mathrm{rk} = r + s$, $\tau = r - s$, $\sigma = r - s \mod 8$, and $\mathrm{disc} = (-1)^s$.

Denote by $U$ the $\mathbb{Z}$-module $\mathbb{Z}^2$ defined by the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

It has associated quadratic form $2xy$. Its invariants are $\mathrm{rk} = 2$, $\tau = 0$, $\sigma = 0$, and $\mathrm{disc} = -1$.

Let $S := \mathbb{Z}^8 \cup (\mathbb{Z} + 1/2)^8$. Define

$$\Gamma_8 = \left\{ (x_i) \in S : \sum_i x_i \equiv 0 \mod 2 \right\}$$

and equip this $\mathbb{Z}$-module with the quadratic form $f$ defined by the identity matrix of rank 8. By design, this form is of Type II, as $\sum_i x_i^2 = \sum_i x_i$ modulo 2. Its invariants are $\mathrm{rk} = 8$, $\tau = 8$, $\sigma = 0$, and $\mathrm{disc} = 1$.

4.3. **Type I Forms.** We prove that a Type I form is equivalent to $rI_+ \oplus sI_-$ for some $r, s$.

First, we need a result about indefinite forms in general.

**Theorem 4.1.** *Let $E$ be an indefinite form. Then, $E$ represents 0 over $\mathbb{Z}$.*

*Proof.* Multiplying by a suitable integer, it is sufficient to show that $E$ represents 0 over $\mathbb{Q}$. We consider $E$ as a rational quadratic form.

($\mathrm{rk} = 2$) $E$ has discriminant $\pm 1$, and its signature is $(1, -1)$ so $E \sim X_1^2 - X_2^2$, which represents 0 over $\mathbb{Q}$.

($\mathrm{rk} = 3$) Consider $E = \sum a_{ij} X_i X_j$, where $a_{ij} \in \mathbb{Z}$. By the Chevalley–Warning theorem, $E$ has a solution mod $p$ for every $p$ except perhaps $p = 2$. By Corollary 2.5, this solution lifts to a $p$-adic solution. The form $E$ represents 0 in $\mathbb{R}$ since it is indefinite, and in $\mathbb{Q}_p$ for every $p$ except perhaps 2, so by Corollary 3.8, $E$ represents 0 in $\mathbb{Q}$.

($\mathrm{rk} = 4$) The same argument as rank 3 shows $E$ represents 0 in $\mathbb{R}$ and in every $\mathbb{Q}_p$ except perhaps $p = 2$. If $E$ has $\mathrm{disc} = 1$, then by Corollary 3.8, $E$ represents 0 over $\mathbb{Q}$. If $\mathrm{disc} = -1$, then by Theorems 3.3 and 3.5, $E$ represents 0 over $\mathbb{Q}$.

($\mathrm{rk} \geq 5$) Every form $E$ in 5 or more variables represents 0 over $\mathbb{Q}_p$ for every $p$. Since $E$ is indefinite, it represents 0 over $\mathbb{R}$. By Theorem 3.5, $E$ represents 0 over $\mathbb{Q}$. □

We now state a few lemmas. Let $F$ be a submodule of $E$, and $F'$ the submodule of elements orthogonal to $F$.

**Lemma 4.2.** *The quadratic form $F$ induced by $E$ has discriminant $\pm 1$ if and only if $E = F \oplus F'$.*

*Proof.* See [Ser73, Chapter V, Lemma 1]. □

**Lemma 4.3.** *Let $x \in E$ be such that $f(x) = \pm 1$. Then, if $D = \mathbb{Z}x$, we have $E = D \oplus D'$.*

*Proof.* Apply Lemma 4.2 to $F = D$. □

An element $x$ of $E$ is indivisible if it is not contained in a submodule $nE$ for $n \geq 2$, or equivalently, if its coordinates are pairwise coprime.

**Lemma 4.4.** *If $x \in E$ is indivisible, there exists $y$ such that $\langle x, y\rangle = 1$.*

*Proof.* Consider the linear form $f : E \to \mathbb{Z}$ defined by $y \mapsto \langle x, y\rangle$. Since $E$ has discriminant $\pm 1$, the form defines an isomorphism on the dual $\mathrm{Hom}(E, \mathbb{Z})$. As $x$ is indivisible, $f$ is indivisible, i.e. it is not a multiple of another form. We conclude that $f$ is surjective and hence there exists $y$ such that $\langle x, y\rangle = 1$. □

**Lemma 4.5.** *Let $f$ be an indefinite Type I quadratic form of rank $n$. Then , there exists a form $F$ of rank $n - 2$ such that*

$$E \cong I_+ \oplus I_- \oplus F.$$

*Proof.* By Theorem 4.1, $E$ contains an isotropic element. Dividing by an appropriate integer, we can assume $x$ is indivisible. Hence, by Lemma 4.4, there exists $y$ such that $\langle x, y\rangle = 1$. Furthermore, we can choose $y$ such that $\langle y, y\rangle$ is odd. Indeed, if $\langle y, y\rangle$ is even, we can find $t$ such that $\langle t, t\rangle$ is odd (as $E$ is Type I). We put $y' = t + ky$ with $k = 1 - \langle x, t\rangle$. We have $\langle x, y'\rangle = 1$ and $\langle y', y'\rangle = \langle t, t\rangle$ mod 2, so $\langle y', y'\rangle$ is odd. Hence, suppose $\langle y, y\rangle = 2m + 1$. Define $e_1 = y - mx$ and $e_2 = y - (m + 1)x$. We have $\langle e_1, e_1\rangle = 1$, $\langle e_2, e_2\rangle = -1$ and $\langle e_1, e_2\rangle = 0$, so the submodule generated by $(e_1, e_2)$ is isomorphic to $I_+ \oplus I_-$. By Lemma 4.2, we have

$$E \cong I_+ \oplus I_- \oplus F,$$

where $F$ has rank $n - 2$. □

**Theorem 4.6.** *Let $E$ be an indefinite Type I quadratic form. There exist natural numbers $r, s$ such that*

$$E \cong rI_+ \oplus sI_-$$

*Proof.* We use induction on the rank $n$. Suppose $E$ satisfies the hypothesis of the theorem. By Lemma 4.5, we have $E \cong I_+ \oplus I_- \oplus F$. If $n = 2$, we have $F = 0$ and we are done. Otherwise, $F \neq 0$ and one of $I_+ \oplus F$ or $I_- \oplus F$ is indefinite. Say the first one is indefinite. Since $I_+$ is Type I and has rank 1, $I_+ \oplus F$ is Type I and has rank $n - 1$. By the induction hypothesis, this module is isomorphic to some $aI_+ \oplus bI_-$ and so $E \cong aI_+ \oplus (b + 1)I_-$. The other case is similar. We are done. □

### 4.4. **Type II Forms.**

We prove that a Type II form is equivalent to $pU \oplus q\Gamma_8$, for some natural numbers $p, q$. First, a few lemmas.

**Lemma 4.7.** *Let $E$ be an indefinite Type II quadratic form of rank $n$. There exists a form $F$ of rank $n - 2$ such that $E \cong U \oplus F$.*

*Proof.* Choose an indivisible isotropic element $x$ of $E$. Choose $y$ such that $\langle x, y\rangle = 1$. If $\langle y, y\rangle = 2m$, replace $y$ by $y - mx$ to get a $y$ such that $\langle y, y\rangle = 0$. The submodule of $E$ generated by $x, y$ is isomorphic to $U$ and by Lemma 4.2, we have $E = U \oplus U'$. Hence, $U' = F$. □

**Lemma 4.8.** *Let $F_1$ and $F_2$ be indefinite Type II quadratic forms and suppose $I_+ \oplus I_- \oplus F_1 \cong I_+ \oplus I_- \oplus F_2$. Then, $U \oplus F_1 \cong U \oplus F_2$.*

*Proof.* See [Ser73, Chapter V, Lemma 6]. □

**Theorem 4.9.** *Let $E$ be an indefinite Type II quadratic form with $\tau_E \geq 0$. There exist natural numbers $p, q$ such that*

$$E \cong pU \oplus q\Gamma_8$$

*Proof.* First, suppose $E_1$ and $E_2$ have the same rank and torsion. We have $E_1 \cong U \oplus F_1$ and $E_2 \cong U \oplus F_2$. The $F_i$'s have the same rank and torsion and are of Type II. The modules $I_+ \oplus I_- \oplus F_1$ and $I_+ \oplus I_- \oplus F_2$ have the same rank and torsion and are both of Type I. Hence, by Theorem 4.6, they are isomorphic. By Lemma 4.8, the $E_i$'s are isomorphic. To prove the theorem, let

$$q = \frac{\tau_E}{8} \quad \text{and} \quad p = \frac{1}{2}\left(\mathrm{rk}_E - \tau_E\right)$$

and apply the result from the beginning of the proof to $E$ and $pU \oplus q\Gamma_8$. □

In the case $\tau_E \leq 0$, one can apply Theorem 4.9 to $-E$, obtained by multiplying the quadratic form by $-1$. We have now classified indefinite integral quadratic forms of discriminant ±1.

## 5. Counterexamples to the Hasse Principle

5.1. **Known Results.** A famous counterexample due to Selmer shows that the Hasse principle need not hold for cubic forms. Indeed,

$$3x^3 + 4y^3 + 5z^3$$

has solutions in all $\mathbb{Q}_v$ but not in $\mathbb{Q}$ (see [Sel51]). However, Roger Heath-Brown showed in [HB07] that every cubic form over the rationals in $\geq 14$ variables represents 0. Hence, the Hasse principle holds (trivially) for cubic forms in $\geq 14$ variables. It is known that some results which hold for quadratic forms do not hold in general. For example, Theorem 3.5 cannot be extended for forms of certain degrees. In [FS76], Fujiwara and Sudo present counterexamples for forms of degree $5 + 10n$.

5.2. **Algorithm and Explicit Counterexample.** There exists an algorithm producing a curve violating the Hasse principle, given a global field [Poo10]. The same author proves that given a number field $k$, one can construct a Châtelet surface violating the Hasse principle [Poo09].

The curve algorithm is presented in [Poo10]. We present an explicit counterexample for the case $k = \mathbb{Q}$. For a curve $E$, write $E(k)$ for the set of $k$-rational points and $\kappa(E)$ for the function field of $E$. We start with the rank 1 elliptic curve $E$, defined by $y^2 + y = x^3 - x^2$ over $\mathbb{Q}$. Its integral points are $\{y_1, y_2, y_3, y_4\} = \{(0, 0), (0, -1), (1, 0), (1, -1)\}$. The group $E(\mathbb{Q})$ has order 5. Let

$P$ be a nonintegral point $(x_0, y_0)$ on $E(\bar{\mathbb{Q}})$ such that $y_0^2+y_0 = x_0^3-x_0^2 = 4$. Consider the infinite-dimensional $\mathbb{F}_2-$vector space $V := \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We have

$$V \cong \bigoplus_{\mathbb{N}} \mathbb{Z}/2\mathbb{Z},$$

where one $\mathbb{Z}/2\mathbb{Z}$ comes from $\pm 1$ and the others are associated to prime numbers. Let $p, q$ be distinct odd primes such that at least one of $p, q, pq$ is congruent to 1 modulo 8 (so that it is a square in $\mathbb{Q}_2$). Images of $p, q$ in $V$ are $\mathbb{F}_2-$independent. The set $S$ of places where $p, q, pq$ are all nonsquares is finite. In our case, $S = \{p, q\}$. Let $c := 1 + 8npq$, and choose $n$ so that $c$ is a square at all places in $S$ and $w(c)$ is odd for at least one place $w$ outside of $S$. In particular, $c$ is not a rational square. Using polynomial interpolation, we can find a rational function $f$ in two variables such that $f$ has a simple pole at $P$ and $f(y_1) = p, f(y_2) = q, f(y_3) = pq, f(y_4) = c$. Explicitly, $f$ is of the form

$$f(X,Y) = \frac{p(Y+1)(1-X) + qY(X-1) + pqX(Y+1) - cXY}{(Y^2+Y-4)},$$

We then construct the curve whose function function field is $\kappa(E)(\sqrt{f})$, namely

$$Y^2 + Y = X^3 - X^2$$

$$Z^2 = f(X,Y).$$

This is an affine model for a curve violating the Hasse principle. The image of $f$ at integral points of $Y^2 + Y = X^3 - X^2$ is never a rational square, hence this curve has no rational points. However, for every $\mathbb{Q}_v$, at least one of $p, q, pq, c$ is a square, so the curve has a $v$-adic zero for all $v$.

5.3. **Going Further.** Birch's theorem, first proved in 1957 in [Bir57], shows that given an odd positive integer $d$, there exists an positive integer $N(d)$ such that all forms of degree $d$ in more than $N(d)$ variables represent 0. These forms then satisfy the Hasse principle. In this context, we would have $N(2) = 0$ (even though 2 is not odd), which is precisely Theorem 3.5. Furthermore, combining the cubic form in [Sel51] and the result of [HB07], we get that $3 \leq N(3) \leq 13$.

## References

[Bir57] B. J. Birch. Homogeneous forms of odd degree in a large number of variables. *Mathematika*, 4(2):102–105, 1957.

[FS76] Masahiko Fujiwara and Masaki Sudo. Some forms of odd degree for which the hasse principle fails. *Pacific J. Math.*, 67(1):161–169, 1976.

[HB07] D. R. Heath-Brown. Cubic forms in 14 variables. *Invent. Math.*, 170(1):199–230, 2007.

[Ost16] Alexander Ostrowski. ber einige Lsungen der Funktionalgleichung $\psi$(x)·$\psi$(x)=$\psi$(xy). *Acta Mathematica*, 41(none):271 – 284, 1916.

[Poo09] Bjorn Poonen. Existence of rational points on smooth projective varieties. *J. Eur. Math. Soc. (JEMS)*, 11(3):529–543, 2009.

[Poo10] B. Poonen. Curves over every global field violating the local-global principle. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 377(Issledovaniya po Teorii Chisel. 10):141–147, 243–244, 2010.

[Sel51] Ernst S. Selmer. The Diophantine Equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85(none):203 – 362, 1951.

[Ser73] J.-P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[Syl52] J.J. Sylvester. Xix. a demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 4(23):138–142, 1852.