QUADRATIC FORMS OVER $\mathbb{Q}_p$ AND OVER $\mathbb{Q}$

HUA-CHIEH LI

Introduction

In this very short note, we will study general properties of quadratic forms over fields. Our objective is to classify quadratic forms over the field of rational numbers, *i.e.,* the Hasse-Minkowski theorem.

We begin with a brief review of some basic properties of bilinear and quadratic forms. We also include some properties of Hilbert symbol which are needed. Finally we study quadratic forms over $\mathbb{Q}_p$ and then over $\mathbb{Q}$.

For reading this note some basic knowledge of linear algebra [1] is needed and the reader is also required to have an elementary knowledge of the p-adic rational numbers $\mathbb{Q}_p$. Our main reference is Serre [3, Chapter 4]. However, we recommend Kitaoka [2] for further reading.

1. Bilinear and Quadratic Forms

1.1. **Bilinear Forms.** First recall the general notion of a bilinear form.

Definition 1.1. Let V be a vector space over a field k. A function from the set $V \times V$ to k is called a *bilinear form* on V if

(1) $H(cv_1 + v_2, w) = cH(v_1, w) + H(v_2, w)$ for $v_1, v_2, w \in V$ and $c \in k$.
(2) $H(v, cw_1 + w_2) = cH(v, w_1) + H(v, w_2)$ for $v, w_1, w_2 \in V$ and $c \in k$.

We now list several properties possessed by all bilinear forms:

(1) For any fixed $w \in V$, functions L_w, $R_w : V \to k$ defined by $L_w(v) = H(w, v)$ and $R_w(v) = H(v, w)$ are linear.
(2) $H(0, v) = H(v, 0) = 0$, for all $v \in V$.
(3) If $v_1, v_2, w_1, w_2 \in V$, then

$$H(v_1 + v_2, w_1 + w_2) = H(v_1, w_1) + H(v_1, w_2) + H(v_2, w_1) + H(v_2, w_2).$$

Let V be an n-dimensional vector space with basis $\beta = \{v_1, v_2, \ldots, v_n\}$. For any bilinear form H on V we can associate with H an $n \times n$ matrix A whose entry in row i column j is defined by $a_{ij} = H(v_i, v_j)$.

The matrix A above is called the *matrix representation* of H with respect to the basis β.

Fixing a basis for V, we can therefore define a one-to-one correspondence between the set of bilinear forms on V to the set of $n \times n$ matrices with entries in k.

Let γ be another basis of V and let U be the change of coordinate matrix changing γ-coordinates to β-coordinates. Then it is easy to check that U^tAU is the matrix representation of H with respect to the basis γ. Therefore, we have the following definition:

Definition 1.2. Two matrices A and B are said to be *congruent* if there exists an invertible matrix U such that $B = U^tAU$.

It is easily seen that congruence is an equivalence relation.

1.2. **Symmetric Bilinear Forms.**

Definition 1.3. A bilinear form H on a vector space V is called *symmetric* if $H(v,w) = H(w,v)$ for all $v, w \in V$.

As the name suggests, symmetric bilinear forms corresponds to symmetric matrices.

Given two symmetric bilinear forms H_1 and H_2 on vector spaces V_1 and V_2, respectively, a linear map $h : V_1 \to V_2$ such that $H_2(h(v), h(w)) = H_1(v,w)$ for all $v, w \in V_1$ is called a *metric morphism* of (V_1, H_1) into (V_2, H_2).

Like the diagonalization problem for linear operators, there is an analogous diagonalization problem for bilinear forms.

Definition 1.4. A bilinear form H on V is called *diagonalizable* if there exists a basis β for V such the matrix representation of H with respect to the basis β is a diagonal matrix.

It is clear that a diagonalizable bilinear form is symmetric. Unfortunately, the converse is not true, as illustrated by the following example.

Example 1.5. Let $k = \mathbb{F}_2$ and $V = \mathbb{F}_2^2$ with the standard basis β. Let $H : V \times V \to \mathbb{F}_2$ be the symmetric bilinear form represented by the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

with respect to β. We will assume that H is diagonalizable and obtain a contradiction.

Suppose that H is diagonalizable. Then there exists an invertible matrix U such that $B = U^t A U$ is a diagonal matrix. Since U is invertible, $\operatorname{rank}(A) = \operatorname{rank}(B) = 2$. Thus,

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Suppose that

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We have

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ac + ac & bc + ad \\ bc + ad & bd + bd \end{pmatrix}.$$

However, $ac + ac = bd + bd = 0$ in $\mathbb{F}_2$. We conclude that $1 = 0$ in $\mathbb{F}_2$, a contradiction. Consequently, H is not diagonalizable.

The bilinear form of Example 1.5 is an anomaly. Its failure to be diagonalizable stems from the fact that the scalar field $\mathbb{F}_2$ is of characteristic 2. As we will see, for the field of characteristic other than 2, the diagonalizable bilinear forms are those that are symmetric. Prior to prove this, we must establish the following lemma.

Lemma 1.6. *Let H be a nontrivial symmetric bilinear form on a vector space V over a field k not of characteristic 2. Then there exists an element $v \in V$ such that $H(v,v) \neq 0$.*

Proof. Since H is nontrivial, there exist $u, w \in V$ such that $H(u,w) \neq 0$. If $H(u,u) \neq 0$ or $H(w,w) \neq 0$, there is nothing to prove. Otherwise, suppose that $H(u,u) = H(w,w) = 0$. Setting $v = u + w$, we have $H(v,v) = 2H(u,w) \neq 0$. □

Definition 1.7. An element v of a symmetric bilinear form H on V is called *isotropic* if $H(v,v) = 0$. A subspace W of V is called a *isotropic subspace* if all its elements are isotropic.

Lemma 1.6 above, tell us that for a nontrivial symmetric bilinear form on a vector space over a filed not of characteristic 2, there must exist a non-isotropic element.

Theorem 1.8. *Let V be a finite dimensional vector space over a field k not of characteristic 2. Then every symmetric bilinear form on V is diagonalizable.*

Proof. We use mathematical induction on $n = \dim(V)$. If $n = 1$, then every bilinear form is diagonalizable. Suppose that the theorem is valid for vector spaces of dimension less than n for some fixed integer $n > 1$. If H is the trivial bilinear form, then certainly H is diagonalizable. Suppose then H is nontrivial and symmetric. By Lemma 1.6, there exists an element $v \in V$ such that $H(v, v) \neq 0$. Consider the linear map $L : V \to k$, $L(w) = H(v, w)$, for all $w \in V$. Since L is nontrivial ($L(v) = H(v, v) \neq 0$), we have $\dim(\ker(L)) = n - 1$. The restriction of H to $\ker(L)$ is obviously a symmetric bilinear form on a vector space of dimension $n - 1$. thus by the induction hypothesis there exists a basis $\{v_1, v_2, \ldots, v_{n-1}\}$ for $\ker(L)$ such that $H(v_i, v_j) = 0$ for $1 \leq i \neq j \leq n - 1$. Set $v_n = v$. Then $\{v_1, v_2, \ldots, v_n\}$ is a basis for V. In addition $H(v_i, v_n) = H(v_n, v_i) = 0$ for $i = 1, 2 \ldots, n - 1$. We conclude that H is diagonalizable. □

1.3. **Quadratic Forms.** Associated with symmetric bilinear forms are functions called quadratic forms.

Definition 1.9. Let V be a vector space over a field k. A function $Q : V \to k$ is called a *quadratic form* on V if:

(1) $Q(cv) = c^2 Q(v)$, for $c \in k$ and $v \in V$.
(2) The function $(v, w) \mapsto Q(v + w) - Q(v) - Q(w)$ is a bilinear form.

Such a pair (V, Q) is called a *quadratic space*.

If the field k is not of characteristic 2, there is a one-to-one correspondence between symmetric bilinear forms and quadratic forms. In this case, for a given symmetric bilinear form H, we get a quadratic form Q given by $Q(v) = H(v, v)$ and for a given quadratic form Q, we have a bilinear form H defined by

$$H(v, w) = \frac{1}{2}\big(Q(v + w) - Q(v) - Q(w)\big).$$

In the rest of this note, we limit ourselves to the case where k is not of characteristic 2, unless we specify. Also, for a given quadratic form Q, we will write H for the correspondent symmetric bilinear form without any further comment, and *vice versa*.

The determinant of the matrix representation of H is determined up to multiplication by an element of k^{*2}; it is called the *discriminant* of Q and denoted by $\mathrm{disc}(Q)$.

Let $\beta = \{v_1, v_2, \ldots, v_n\}$ be a basis of V and let $A = (a_{ij})$ be the matrix representation of H with respect to β. If $v = \sum x_i v_i$, then

$$Q(v) = H(v, v) = \sum_{i,j} a_{ij} x_i x_j,$$

which shows that Q is a quadratic form in $x_1, \ldots, x_n$ in the usual sense. Conversely, let $f(x) = \sum_{i=1}^{n} a_{ii} x_i^2 + 2 \sum_{i<j} a_{ij} x_i x_j$ be a quadratic form in n variables over k; we put $a_{ij} = a_{ji}$ if $i > j$ so that the matrix $A = (a_{ij})$ is symmetric. We can consider f as a quadratic form on the space k^n. As before, we have the following definition:

Definition 1.10. Two quadratic forms f_1 and f_2 are called *equivalent* if the corresponding matrix are congruent. In this case, we write $f_1 \sim f_2$.

2. Orthogonality and Witt's Theorem

2.1. **Orthogonality.** Let Q be a quadratic form on V. Two elements v, $w \in V$ are called *orthogonal* (denoted $v \perp w$) if $H(v,w) = 0$. The set of elements in V orthogonal to a subset S of V is denoted by $S^\perp$; it is a vector subspace of V. Two subspace V_1 and V_2 of V are said to be *orthogonal* if $V_1 \subseteq V_2^\perp$. In this case, if $v_1 \in V_1$ and $v_2 \in V_2$, we have $Q(v_1+v_2) = Q(v_1)+Q(v_2)+2H(v_1,v_2) = Q(v_1)+Q(v_2)$.

Definition 2.1. Let $V_1, \ldots, V_m$ be vector subspace of V. One says that V is the *orthogonal direct sum* of the V_i if they are pairwise orthogonal and if V is the direct sum of them. One writes then:

$$V = V_1 \boxplus \cdots \boxplus V_m.$$

Suppose that V is the orthogonal direct sum of the V_i. If $v \in V$ has for components $v_i \in V_i$, by the argument above, we have

$$Q(v) = Q(v_1 + \cdots + v_m) = Q(v_1) + \cdots + Q(v_m).$$

Conversely if Q_i is a family of quadratic forms on V_i, the formula above endows $V = V_1 \oplus \cdots \oplus V_m$ with a quadratic form Q, call the *direct sum* of the Q_i, and one has $V = V_1 \boxplus \cdots \boxplus V_m$.

Let $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_m)$ be two quadratic forms; we will denote $f \boxplus g$ the quadratic form $f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_{n+m})$ in $n+m$ variables. This operation corresponds to that of orthogonal sum. We write similarly $f \boxminus g$ for $f \boxplus (-g)$. Using this notation, we can rewrite Theorem 1.8 as the following theorem:

Theorem 2.2. *Let f be a quadratic forms in n variables. There exists $a_1, \ldots, a_n \in k$ such that $f \sim a_1 x_1^2 + \cdots + a_n x_n^2$.*

For a subspace W of V, the orthogonal complement of W itself is called the radical of W and denoted by $\mathrm{rad}(W)$; *i.e.*, $\mathrm{rad}(W) = W \cap W^\perp$. In particular, $\mathrm{rad}(V) = V^\perp$. Its codimension is called the rank of Q. If $V^\perp = 0$ we say that Q is *nondegenerate*; this is equivalent to saying that the discriminant of Q is not 0.

Let W be a vector subspace of V and let $W^* = \mathrm{Hom}_k(W, k)$. For each $v \in V$, we associate to a linear form $H_v : W \to k$ by $H_v(w) = H(v,w)$ for all $w \in W$. This gives us a linear map $q_W : V \to W^*$ ($v \mapsto H_v$). The kernel of q_W is $W^\perp$. In particular we see that Q is nondegenerate if and only if $q_V : V \to V^*$ is an isomorphism.

Proposition 2.3. *Suppose that (V,Q) is nondegenerate. Then:*

(1) *All metric isomorphisms of V into a quadratic space (V',Q') are injective.*
(2) *For all vector subspace W of V, we have*

$$(W^\perp)^\perp = W, \quad \dim W + \dim W^\perp = \dim V, \quad \mathrm{rad}(W) = \mathrm{rad}(W^\perp).$$

In particular, the quadratic module W is nondegenerate if and only if $W^\perp$ is nondegenerate, in which case $V = W \boxplus W^\perp$.
(3) *If V is the orthogonal direct sum of two subspaces, they are nondegenerate and each of them is orthogonal to the other.*

Proof. (1) If $h : V \to V'$ is a metric morphism and if $h(v) = 0$, we have $H(v,w) = H'(h(v), h(w)) = 0$ for all $w \in V$; this implies that $v = 0$ because (V,Q) is nondegenerate.

(2) Composing the isomorphism $q_V : V \to V^*$ with the canonical surjection $V^* \to W^*$, the homomorphism $q_W : V \to W^*$ is surjective with kernel equal to $W^\perp$. Hence $\dim V = \dim W^* + \dim W^\perp = \dim W + \dim W^\perp$. Similarly, $\dim V = \dim W^\perp + \dim(W^\perp)^\perp$; since W is contained in $(W^\perp)^\perp$, we have $W = (W^\perp)^\perp$. Because $\mathrm{rad}(W) = W \cap W^\perp$, this implies that $\mathrm{rad}(W) = \mathrm{rad}(W^\perp)$ and the last assertion of (2) follows easily.

(3) If $V = W_1 \boxplus W_2$, then $W_1 \subseteq W_2^\perp$ and $W_2 \subseteq W_1^\perp$. By (2), we have $\dim W_1 = \dim W_2^\perp$ and hence $W_1 = W_2^\perp$ and similarly $W_2 = W_1^\perp$. This implies that $\mathrm{rad}(W_1) = W_1 \cap W_1^\perp = W_1 \cap W_2 = 0$ and similarly $\mathrm{rad}(W_2) = 0$.

□

We remark that in Proposition 2.3, the nondegenerate assumption of (V, Q) is essential. Recall that an element v of V is called isotropic if $Q(v) = 0$. Suppose that v_0 is not isotropic. In the induction process for proving Theorem 1.8, we use the fact that $V = kv_0 \boxplus W$, where W is the orthogonal complement of kv_0. When (V, Q) is degenerate, though $\dim(W) = \dim(V) - 1$, we have $W \subsetneq (W^\perp)^\perp$ and (W, Q) is degenerate, even (kv_0, Q) is nondegenerate.

2.2. **Witt's Theorem.** Let $(V, Q)$and (V', Q') be two nondegenerate quadratic spaces; let W be a subspace of V, and let $s : W \to V'$ be an injective metric morphism of W into V'. we try to extend s to a subspace larger than W and if possible to all of V. We begin with the case where W is degenerate.

Lemma 2.4. *Let $(V, Q)$and (V', Q') be two nondegenerate quadratic spaces; let W be a subspace of V, and let $s : W \to V'$ be an injective metric morphism of W into V'. If W is degenerate, we can extend s to an injective metric morphism $s_1 : W_1 \to V'$ where W_1 contains W as a hyperplane.*

Proof. Since W is degenerate, there exists $\mathbf{0} \neq w_0 \in \mathrm{rad}(W)$. Let l be a linear map on W such that $l(w_0) = 1$. We can extend l to a linear map on V and since V is nondegenerate, there exists $v_0 \in V$ such that $l(w) = H(v_0, w)$ for all $w \in W$. Let $w_1 = v_0 - \frac{1}{2}Q(v_0)w_0$. We also have

$$H(w_1, w) = H(v_0, w) - \frac{1}{2}Q(v_0)H(w_0, w) = l(w), \forall\, w \in W.$$

Since, $H(w_1, w_0) = l(w_0) = 1 \neq 0$, we have that $w_1 \notin W$. Moreover, we have

$$H(w_1, w_1) = H(v_0, v_0) - Q(v_0)H(v_0, w_0) = Q(v_0) - Q(v_0)l(w_0) = 0.$$

The space $W_1 = W \oplus kw_1$ contains W as a hyperplane.

On the other hand, let $W' = s(W)$, $w_0' = s(w_0)$ and $l' = l \circ s^{-1}$. We have that $w_0' \in \mathrm{rad}(W')$. By the same argument above, there exists $w_1' \in V' \setminus W'$ such that $H'(w_1', w_1') = 0$ and $l'(w') = H'(w_1', w')$, for all $w' \in W'$. The linear map $s_1 : W_1 \to V'$ which coincides with s on W and carries w_1 onto w_1' is an injective metric morphism because

$$H'(s_1(w_1), s_1(w)) = l \circ s^{-1}(s(w)) = l(w) = H(w_1, w), \quad \forall w \in W$$

and

$$H'(s_1(w_1), s_1(w_1)) = H'(w_1', w_1') = 0 = H(w_1, w_1).$$

□

Theorem 2.5 (Witt)**.** *If (V, Q) and (V', Q') are metric isomorphic and nondegenerate, every injective metric morphism $s : W \to V'$ of a subspace W of V can be extended to a metric isomorphism of V onto V'.*

Proof. By applying Lemma 2.4, we are reduced to the case where W is nondegenerate. we argue then by induction on $\dim W$.

Let $\iota : V \to V'$ be an metric isomorphism. If $\dim W = 1$, W is generated by a non-isotropic element w and hence $s(w)$ is also non-isotropic. One can choose $\varepsilon = \pm 1$ such that $w + \varepsilon\iota^{-1}(s(w))$ is not isotropic; otherwise, we would have

$$Q(w+\iota^{-1}(s(w))) = Q(w)+2H(w,\iota^{-1}(s(w)))+Q(\iota^{-1}(s(w))) = 2Q(w)+2H(w,\iota^{-1}(s(w))) = 0$$

and

$$Q(w-\iota^{-1}(s(w))) = Q(w)-2H(w,\iota^{-1}(s(w)))+Q(\iota^{-1}(s(w))) = 2Q(w)-2H(w,\iota^{-1}(s(w))) = 0$$

which would imply $Q(w) = 0$. Choose such an ε and let $w_0 = w + \varepsilon\iota^{-1}(s(w))$. Since ι is a metric homomorphism, $\iota(w_0)$ is also not isotropic. Let W_1 be the orthogonal complement of w_0; we have $V = kw_0 \boxplus W_1$ and $V' = k\iota(w_0) \boxplus \iota(W_1)$. Let $\sigma : V \to V'$ be the isomorphism which maps w_0 to $\varepsilon\iota(w_0)$ and maps w_1 to $-\varepsilon\iota(w_1)$ for all $w_1 \in W_1$. It is clear that σ is a metric isomorphism. Since

$$H(w - \varepsilon\iota^{-1}(s(w)), w + \varepsilon\iota^{-1}(s(w))) = Q(w) - Q(\varepsilon\iota^{-1}(s(w))) = Q(w) - Q(w) = 0,$$

$w - \varepsilon\iota^{-1}(s(w))$ is contained in W_1 and we have

$$\sigma(w - \varepsilon\iota^{-1}(s(w))) = -\varepsilon\iota(w - \varepsilon\iota^{-1}(s(w))) = -\varepsilon\iota(w) + s(w)$$

and

$$\sigma(w + \varepsilon\iota^{-1}(s(w))) = \varepsilon\iota(w + \varepsilon\iota^{-1}(s(w))) = \varepsilon\iota(w) + s(w).$$

This implies that $\sigma(w) = s(w)$; thus σ extends s.

If $\dim W > 1$, we decompose W in the form $W_1 \boxplus W_2$, with W_1, $W_2 \neq 0$. By the inductive hypothesis, the restriction s_1 of s to W_1 extends to an metric isomorphism $\sigma_1 : V \to V'$. Note that $V = W_1 \boxplus W_1^\perp$ and $V' = s(W_1) \boxplus s(W_1)^\perp$. The restriction of σ_1 to $W_1^\perp$ gives a metric isomorphism from $W_1^\perp$ to $s(W_1)^\perp$ and the metric morphism s carries W_2 into the orthogonal complement $s(W_1)^\perp$ of $s(W_1)$ in V'; by induction hypothesis, because $W_2 \subseteq W_1^\perp$, the restriction of s to W_2 extends to a metric isomorphism $\sigma_2 : W_1^\perp \to s(W_1)^\perp$. The isomorphism $\sigma : V \to V'$ which is σ_1 on W_1 and σ_2 on $W_1^\perp$ is a metric isomorphism and hence has the desired property. □

Given two metric isomorphic subspaces of a nondegenerate quadratic space, one extends a metric isomorphism between the two subspaces to an automorphism of the space and restricts it to the orthogonal complements. Hence these two isomorphic subspaces have metric isomorphic orthogonal complements. Therefore, Witt's theorem gives the following *cancellation theorem*:

Theorem 2.6. *Let $f_1 = g_1 \boxplus h_1$ and $f_2 = g_2 \boxplus h_2$ be two nondegenerate quadratic forms. If $f_1 \sim f_2$ and $g_1 \sim g_2$, one has $h_1 \sim h_2$.*

2.3. **Representation of an Element of k.** We say that a form $f(x_1, \ldots, x_n)$ represents an element a of k if there exists $(c_1, \ldots, c_n) \in k^n$, $(c_1, \ldots, c_n) \neq \mathbf{0}$, such that $f(c_1, \ldots, c_n) = a$. In particular f represents 0 if and only if the corresponding quadratic space contains a non-zero isotropic element. We also remark that if $f \sim g$, then f represents a if and only if g represents a.

Definition 2.7. A 2-dimensional quadratic space having a basis formed of two isotropic element v_1 and v_2 such that $H(v_1, v_2) \neq 0$ is called a *hyperbolic plane*.

Equivalently, a quadratic form $f(x_1, x_2)$ in two variables is called *hyperbolic* if we have $f \sim x_1 x_2$.

After multiplying v_2 by $1/H(v_1, v_2)$, we can suppose that $H(v_1, v_2) = 1$. Hence the matrix representation of the hyperbolic quadratic form is simply $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; its discriminant is -1. In particular, it is nondegenerate. A hyperbolic quadratic form is important because it represents every element of k. In fact, if $a \in k$, then

$$Q(v_1 + \frac{a}{2} v_2) = Q(v_1) + aH(v_1, v_2) + \frac{a^2}{4} Q(v_2) = a.$$

Proposition 2.8. *Let v be a non-zero isotropic element of a nondegenerate quadratic space (V, Q). Then there exists a subspace W of V which contains v and which is a hyperbolic plane. Moreover, one has $Q(V) = k$.*

Proof. Since V is nondegenerate, there exists $v' \in V$ such that $H(v, v') = 1$. Consider the element $w = v' - \frac{1}{2} Q(v') v$. We have

$$Q(w) = Q(v') - Q(v') H(v, v') + \frac{1}{4} Q(v')^2 Q(v) = 0$$

and

$$H(v, w) = H(v, v') - \frac{1}{2} Q(v') Q(v) = 1.$$

The subspace $W = kv \oplus kw$ has the desired property. Since $V = W \boxplus W^{\perp}$ (Proposition 2.3 (2)) and W is hyperbolic, we have $Q(V) = k$. □

Corollary 2.9. *If f is nondegenerate, then $f \sim g_1 \boxplus \cdots \boxplus g_m \boxplus h$ where g_i are hyperbolic and h does not represent 0. This decomposition is unique up to equivalence.*

Proof. If f represents 0, by Proposition 2.8 one has $f \sim g_1 \boxplus g$ where g_1 is hyperbolic. Since hyperbolic quadratic form is nondegenerate, by Proposition 2.3 (2) g is also nondegenerate. Using this process inductively, the existence is proved. The uniqueness follows from Theorem 2.6. □

Corollary 2.10. *Let $g(x_1, \ldots, x_{n-1})$ be a nondegenerate quadratic form and let $a \in k^*$. The following properties are equivalent:*

(1) *g represents a.*
(2) *One has $g \sim h(x_1, \ldots, x_{n-2}) + ax_{n-1}^2$.*
(3) *The form $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) - ax_n^2$ represents 0.*

Proof. If g represents a, the quadratic space V corresponding to g contains an element v such that $Q(v) = a \neq 0$; if W is the orthogonal complement to v, we have $V = kv \boxplus W$, hence $g \sim h \boxplus ax^2$ where h denotes the quadratic form attached to a basis of W. Hence (1) $\Rightarrow$ (2).

The implication (2) $\Rightarrow$ (3) follows from the fact that $f \sim h \boxplus ax^2 \boxminus ay^2$, and $h(0, \ldots, 0) + a \cdot 1^2 - a \cdot 1^2 = 0$.

Finally, if the form $g(c_1, \ldots, c_{n-1}) - ac_n^2 = 0$ with $(c_1, \ldots, c_n) \neq \mathbf{0}$, we have either $c_n = 0$ in which case g represents 0 and hence by Proposition 2.8 also represents a, or $c_n \neq 0$ in which case $g(c_1/c_n, \ldots, c_{n-1}/c_n) = a$. Hence (3) $\Rightarrow$ (1).

□

Corollary 2.11. *Let g and h be two nondegenerate forms of rank ≥ 1, and let $f = g \boxplus h$. the following properties are equivalent:*

(1) *f represents 0.*
(2) *There exists $a \in k^*$ which is represented by g and by h.*
(3) *There exists $a \in k^*$ such that $g \boxplus ax^2$ and $h \boxplus ax^2$ represent 0.*

Proof. Let us first show (1) $\Rightarrow$ (2). f represents 0 is equivalent to $a = g(c_1, \ldots, c_n) = h(d_1, \ldots, d_m)$ with $(c_1, \ldots, c_n, d_1, \ldots, d_m) \neq \mathbf{0}$. If $a \neq 0$, then (2) is verified. If $a = 0$, then either $(c_1, \ldots, c_n) \neq \mathbf{0}$ or $(d_1, \ldots, d_m) \neq \mathbf{0}$. Let us say $(c_1, \ldots, c_n) \neq \mathbf{0}$ for example. Then g represents 0, thus all elements of k (Proposition 2.8). In particular, all non-zero values taken by h can be represented by g.

(2) $\Rightarrow$ (3) followsfrom Corollary 2.10 ((1) $\Rightarrow$ (3)).

Suppose that $g \boxplus ax^2$ and $h \boxplus ax^2$ represent 0. Then by Corollary 2.10 ((3) $\Rightarrow$ (1)), there exist $(c_1, \ldots, c_n) \neq \mathbf{0}$ and $(d_1, \ldots, d_m) \neq \mathbf{0}$ such that $g(c_1, \ldots, c_n) = h(d_1, \ldots, d_m) = a$. Hence $f(c_1, \ldots, c_n, d_1, \ldots, d_m) = 0$. This shows (3) $\Rightarrow$ (1). □

2.4. **Orthogonal Basis.** We already know that every quadratic space has an orthogonal basis. Given two orthogonal bases , there is a special chain of orthogonal bases relating these two bases.

Definition 2.12. Two orthogonal bases $\mathbf{e} = \{v_1, \ldots, v_n\}$ and $\mathbf{e}' = \{v'_1, \ldots, v'_n\}$ of V are called *contiguous* if there exist i and j such that $v_i = v'_j$.

Theorem 2.13. *Let (V, Q) be a nondegenerate quadratic space of dimension ≥ 3, and let $\mathbf{e} = \{v_1, \ldots, v_n\}$ and $\mathbf{e}' = \{v'_1, \ldots, v'_n\}$ be two orthogonal bases of V. There exists a finite sequence $\mathbf{e}^{(0)}$, $\mathbf{e}^{(1)}$,…,$\mathbf{e}^{(m)}$ of orthogonal bases of V such that $\mathbf{e}^{(0)} = \mathbf{e}$, $\mathbf{e}^{(m)} = \mathbf{e}'$ and $\mathbf{e}^{(i)}$ is contiguous with $\mathbf{e}^{(i+1)}$ for $0 \leq i < m$.*

Proof. We show first the case that there exist $v_i \in \mathbf{e}$ and $v'_j \in \mathbf{e}'$ such that the plane $P = kv_i + kv'_j$ is nondegenerate. Let us say for example $v_i = v_1$ and $v'_j = v'_1$. Since P is nondegenerate and v_1, v'_1 are non-isotropic, there exist w_2 and $w'_2 \in V$ such that $P = kv_1 \boxplus kw_2 = kv'_1 \boxplus kw'_2$ and $V = P \boxplus P^\perp$ (see Proposition 2.3). Let $v''_3, \ldots, v''_n$ be an orthogonal basis of $P^\perp$. One can then relate $\mathbf{e}$ to $\mathbf{e}'$ by means of the chain

$$\mathbf{e} \to (v_1, w_2, v''_3, \ldots, v''_n) \to (v'_1, w'_2, v''_3, \ldots, v''_n) \to \mathbf{e}',$$

hence the theorem in this case.

We now proceed to the case that $kv_i + kv'_j$ is degenerate for all i, j. In this case, we show first that there exists $x \in k^*$ such that $v = v'_1 + xv'_2$ is non-isotropic and generates with v_1 a nondegenerate plane.

We have $Q(v) = Q(v'_1) + x^2 Q(v'_2)$; we must take $x^2 \neq -Q(v'_1)/Q(v'_2)$. Moreover, for v to generate with v_1 a nondegenerate plane, it is necessary and sufficient that $Q(v_1)Q(v) - H(v_1, v)^2 \neq 0$; by the hypothesis that $kv_1 + kv'_i$ for $i = 1, 2$ is degenerate (*i.e.*, $Q(v_1)Q(v'_i) - H(v_1, v'_i)^2 = 0$ for $i = 1, 2$) this is equivalent to $-2xH(v_1, v'_1)H(v_1, v'_2) \neq 0$. Because $Q(v_1)$, $Q(v'_1)$ and $Q(v'_2)$ are not 0, we have that $H(v_1, v'_1) \neq 0$ and $H(v_1, v'_2) \neq 0$. Combining this, we see that we must have $x \neq 0$ and $x^2 \neq -Q(v'_1)/Q(v'_2)$. This eliminates at most three values of x; if k has at least 4 elements, we can find one such x. There remains the case $k = \mathbb{F}_3$. But, then, all non-zero squares are equal to 1 and $H(v_1, v'_i) \neq 0$ implies that $Q(v'_1) = Q(v'_2)$. Hence it is sufficient to take $x = 1$.

This being so, let us choose such a v. Since $v \in kv_1' + kv_2'$ is not isotropic, there exists w such that $kv_1' + kv_2' = kv \boxplus kw$. Let us put $\mathbf{e}'' = (v, w, v_3', \dots, v_n')$; it is an orthogonal basis of V. Since $kv_1 + kv$ is nondegenerate, the proof of the first case shows that one can relate $\mathbf{e}$ to $\mathbf{e}''$ by a chain of contiguous bases; since $\mathbf{e}''$ and $\mathbf{e}'$ are contiguous, the theorem follows. □

3. Examples

In this section, we introduce some examples of symmetric bilinear forms. It only serves as a brief review of some preliminary results. Most results are just mentioned without proof. For detail we refer to [3, Chapters 1–3].

3.1. **Hilbert Symbol.** In this subsection, k denotes either $\mathbb{R}$ or $\mathbb{Q}_p$.

Let $a, b \in k^*$. We put:

$$(a,b) = \begin{cases} 1 & \text{if the quadratic form } z^2 - ax^2 - by^2 \text{ represents } 0, \\ -1 & \text{otherwise.} \end{cases}$$

The number $(a,b) = \pm 1$ is called the *Hilbert symbol* of a and b relative to k. It is clear that (a,b) does not change when a and b are multiplied by squares; thus the Hilbert symbol defined a map from $k^*/k^{*2} \times k^*/k^{*2}$ into $\{1, -1\}$.

We list some basic formulas of (a,b).

Proposition 3.1. *The Hilbert symbol satisfies the formulas:*

(1) $(a,b) = (b,a)$ *and* $(a,c^2) = 1$.
(2) $(a,-a) = 1$ *and* $(a,1-a) = 1$.
(3) $(a,b) = (a,-ab) = (a,(1-a)b)$. *In particular,* $(a,a) = (a,-1)$.
(4) $(aa',b) = (a,b)(a',b)$.
(5) *If a and b are p-adic units, we have*

$$(a,b) = \begin{cases} 1 & \text{if } p \neq 2, \\ (-1)^{(a-1)(b-1)/4} & \text{if } p = 2. \end{cases}$$

We can consider k^*/k^{*2} as a vector space over $\mathbb{F}_2$. Proposition 3.1 tell us that the Hilbert symbol is a symmetric bilinear form on k^*/k^{*2}.

Theorem 3.2. *The Hilbert symbol is a nondegenerate bilinear form on the $\mathbb{F}_2$-vector space k^*/k^{*2}.*

When $k = \mathbb{Q}_p$, recall that the number of elements in the $\mathbb{F}_2$ vector space k^*/k^{*2} is 2^r with

$$r = \begin{cases} 3 & \text{if } p = 2, \\ 2 & \text{otherwise.} \end{cases}$$

If $a \in k^*/k^{*2}$ and $\varepsilon = \pm 1$, let $H_a^\varepsilon = \{x \in k^*/k^{*2} \mid (x,a) = \varepsilon\}$.

Proposition 3.3. *For $k = \mathbb{Q}_p$, H_a^ε has the following properties:*

(1) *If $a = 1$ in k^*/k^{*2}, H_a^1 has 2^r elements and $H_a^{-1} = \varnothing$. If $a \neq 1$ in k^*/k^{*2}, H_a^ε has 2^{r-1} elements.*
(2) *Let $a, a' \in k^*/k^{*2}$ and $\varepsilon, \varepsilon' = \pm 1$; assume that H_a^ε and $H_{a'}^{\varepsilon'}$ are nonempty. For $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \varnothing$, it is necessary and sufficient that $a = a'$ and $\varepsilon = -\varepsilon'$.*

Proof. The case $a = 1$ is trivial; of the case $a \neq 1$ in k^*/k^{*2}, by Theorem 3.2, the homomorphism $b \mapsto (a, b)$ carries k^*/k^{*2} onto $\{1, -1\}$. Hence its kernel H_a^1 has dimension $r - 1$, thus 2^{r-1} elements; its complement H_a^{-1} has $2^r - 2^{r-1} = 2^{r-1}$ elements.

Finally, if H_a^ε and $H_{a'}^{\varepsilon'}$ are nonempty and disjoint, we must have $a, a' \neq 1$ in k^*/k^{*2}. Therefore, they have necessarily 2^{r-1} elements each and are complementary to one another. Since $1 \in H_a^1 \cap H_{a'}^1$, we have $H_a^1 = H_{a'}^1$, thus $(x, a) = (x, a')$ for all $x \in k^*/k^{*2}$. Again, by Theorem 3.2, this implies that $a = a'$ and hence $\varepsilon = -\varepsilon'$. The converse is trivial. □

The field $\mathbb{Q}$ embeds as a subfield into each of the fields $\mathbb{Q}_p$ and $\mathbb{R}$. We denote by $\mathcal{V}$ the union of the set of prime numbers and the symbol ∞, and we put $\mathbb{Q}_\infty = \mathbb{R}$. Hence $\mathbb{Q}$ is dense in $\mathbb{Q}_\nu$ for all $\nu \in \mathcal{V}$.

If $a, b \in \mathbb{Q}^*$, $(a, b)_\nu$ denotes the Hilbert symbol of their images in $\mathbb{Q}_\nu$. We have the following important global property of Hilbert symbol, which is essentially equivalent to the quadratic reciprocity law.

Theorem 3.4 (Hilbert Product Formula)**.** *If $a, b \in \mathbb{Q}^*$, we have $(a, b)_\nu = 1$ for almost all $\nu \in \mathcal{V}$ and*

$$\prod_{\nu \in \mathcal{V}} (a, b)_\nu = 1.$$

Conversely, given $a \in \mathbb{Q}^*$ and $(\varepsilon_\nu)_{\nu \in \mathcal{V}}$ with $\varepsilon_\nu = \pm 1$. Suppose that almost all the $\varepsilon_\nu = 1$, $\prod_{\nu \in \mathcal{V}} \varepsilon_\nu = 1$ and for every $\nu \in \mathcal{V}$ there exists $x_\nu \in \mathbb{Q}_\nu^*$ such that $(a, x_\nu)_\nu = \varepsilon_\nu$. Then there exists $b \in \mathbb{Q}^*$ such that $(a, b)_\nu = \varepsilon_\nu$. Moreover, we have the following theorem.

Theorem 3.5. *Let $a_1, \ldots, a_m$ be elements in $\mathbb{Q}^*$ and let $(\varepsilon_{1,\nu})_{\nu \in \mathcal{V}}, \ldots, (\varepsilon_{m,\nu})_{\nu \in \mathcal{V}}$ be a family of numbers equal to ± 1. In order that there exists $b \in \mathbb{Q}^*$ such that $(a_i, b)_\nu = \varepsilon_{i,\nu}$ for $i = 1, \ldots, m$ and $\nu \in \mathcal{V}$, it is necessary and sufficient that the following conditions be satisfied:*

(1) *Almost all the $\varepsilon_{i,\nu} = 1$.*
(2) *For $i = 1, \ldots, m$, we have $\prod_{\nu \in \mathcal{V}} \varepsilon_{i,\nu} = 1$.*
(3) *For $\nu \in \mathcal{V}$ there exists $x_\nu \in \mathbb{Q}_\nu^*$ such that $(a_i, x_\nu)_\nu = \varepsilon_{i,\nu}$ for all $i = 1, \ldots, m$.*

3.2. **The Norms and Quadratic Forms over Finite Fields.** Let K be a quadratic extension of k; then the *norm* N and the *trace* Tr from K to k are defined by $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ and $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$, where $\overline{\alpha}$ denotes the conjugate of α over k.

For $\alpha, \beta \in K$,

$$\mathrm{Tr}(\alpha\overline{\beta}) = \mathrm{N}(\alpha + \beta) - \mathrm{N}(\alpha) - \mathrm{N}(\beta)$$

is clear. If $\mathrm{N}(\alpha) = 0$ for $\alpha \in K$, then $\alpha = 0$ holds; hence every nonzero elements is non-isotropic. Moreover, if $\alpha \neq 0$, then $\mathrm{Tr}(\alpha\overline{\alpha}) = 2\mathrm{N}(\alpha) \neq 0$ ($\mathrm{char}(k) \neq 2$); thus, N is a nondegenerate quadratic form on K.

We remark that for $\alpha, \beta \in K$, $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. This property is very useful. For example, if a is not a square in k, considering the field $K = k(\sqrt{a})$, then b is represented by the form $f = x^2 - ay^2$ if and only if $b \in \mathrm{N}(K)$. Hence, if b and $c \in k^*$ are represented by f, then bc and b/c both are represented by f.

Now, we restrict to the case k is a finite field. In this case, K is the unique quadratic extension of k and it is well known that the norm and the trace from K to k are surjective. Hence, we know that (K, N) is a nondegenerate quadratic space which represents k^* (even when $\mathrm{char}(k) = 2$). Though K is of dimension 2 over k, it is important to know that (K, N) is not a hyperbolic plane, since there is no nonzero isotropic element.

Proposition 3.6. *Let (V, Q) be a 2-dimensional quadratic space over a finite field k without any nonzero isotropic element. Then (V, Q) is metric isomorphic to (K, N), and hence (V, Q) is nondegenerate and represents k^*.*

Proof. Given a basis v_1, v_2 of V, we have

$$Q(xv_1 + v_2) = Q(v_1)x^2 + H(v_1, v_2)x + Q(v_2) \neq 0, \quad \forall\, x \in k.$$

Hence, there exists $\alpha \in K \setminus k$ such that

$$Q(v_1)x_1^2 + H(v_1, v_2)x_1x_2 + Q(v_2)x_2^2 = Q(v_1)(x_1 - \alpha x_2)(x_1 - \overline{\alpha}x_2) = Q(v_1)\mathrm{N}(x_1 - \alpha x_2).$$

By the ontoness, there exists $\beta \in K$ such that $\mathrm{N}(\beta) = Q(v_1)$. The mapping $h : V \to K$ sending $x_1v_1 + x_2v_2$ to $\beta(x_1 - \alpha x_2)$ is a metric isomorphism because

$$\mathrm{N}(h(x_1v_1 + x_2v_2)) = \mathrm{N}(\beta(x_1 - \alpha x_2)) = \mathrm{N}(\beta)\mathrm{N}(x_1 - \alpha x_2) = Q(x_1v_1 + x_2v_2).$$

□

Corollary 3.7. *A nondegenerate 2-dimensional quadratic space over a finite field k is metric isomorphic to a hyperbolic plane or to (K, N).*

Proof. If there exists a nonzero isotropic element, then Proposition 2.8 implies that it is a hyperbolic plane. Hence, Proposition 3.6 yields the corollary. □

We have proved that every nontrivial quadratic space over a field of characteristic not equal to 2 has a non-isotropic element. Our next corollary is interesting and is true even for the case $\mathrm{char}(k) = 2$.

Corollary 3.8. *A quadratic space (V, Q) over a finite field of rank > 2 has a nonzero isotropic element.*

Proof. Suppose that there is no nonzero isotropic element. Take a 2-dimensional subspace W; then by Proposition 3.6, (W, Q) is metric isomorphic to (K, N). Thus, (W, Q) is nondegenerate and Q represents k^* in W. By Proposition 2.3, we have $W^\perp \neq \{0\}$ (because $\dim(W^\perp) > 3 - 2$); thus, there exists a nonzero $v \in W^\perp$. Since v is not isotropic, $Q(v) \in k^*$ and hence, there exists $w \in W$ such that $Q(w) = -Q(v)$. Thus $Q(v+w) = Q(v)+Q(w) = 0$. Since (W, Q) is nondegenerate, $W \cap W^\perp = \{0\}$. Thus $v + w$ is a nonzero isotropic element which contradicts to our assumption. □

From this corollary, a quadratic form over a finite field k of rank ≥ 3 must represents 0. Also from Propositions 2.8 and 3.6, a rank 2 quadratic form over a finite field k represents all elements of k^*.

Proposition 3.9. *Let k be a finite field and let a denote an element of k^* which is not a square. Every nondegenerate quadratic form of rank n over k is equivalent to*

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \quad \text{or} \quad x_1^2 + \cdots + x_{n-1}^2 + ax_n^2,$$

depending on whether its discriminant is a square or not.

Proof. This is clear if $n = 1$. If $n \geq 2$, then the argument above shows that the form f represents 1. This is thus equivalent to $x^2 \boxplus g$ where g is a form of rank $n-1$ (*c.f.* Corollary 2.10). One applies the inductive hypothesis to g. □

Corollary 3.10. *For two nondegenerate quadratic forms over a finite field k to be equivalent, it is necessary and sufficient that they have same rank and same discriminant in k^*/k^{*2}.*

4. Quadratic Forms over Local Fields

In this section, we discuss quadratic forms over the field $\mathbb{Q}_p$ of p-adic numbers and the field $\mathbb{R}$ of real numbers.

4.1. **Quadratic Forms over $\mathbb{Q}_p$.** In this subsection, all quadratic forms are nondegenerate.

Let (V, Q) be a quadratic space of rank n. Recall that if $\mathbf{e} = \{v_1, \ldots, v_n\}$ is an orthogonal basis of V and if we put $a_i = Q(v_i)$, we have its discriminant

$$d(Q) = a_1 \cdots a_n \quad \text{in } \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}.$$

$d(Q)$ is an invariant of Q in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. There is another invariant $\varepsilon(\mathbf{e})$ which is defined by

$$\varepsilon(\mathbf{e}) = \prod_{i<j} (a_i, a_j)$$

where (a, b) is the Hilbert symbol. One has $\varepsilon(\mathbf{e}) = \pm 1$. We need to show that $\varepsilon(\mathbf{e})$ is independent of the choice of the orthogonal basis.

Theorem 4.1. *For any two orthogonal bases $\mathbf{e}, \mathbf{e}'$ of V, $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e}')$.*

Proof. If $n = 1$, one has $\varepsilon(\mathbf{e}) = 1$ by definition. If $n = 2$, $f \sim a_1 x_1^2 + a_2 x_2^2$. One has $\varepsilon(\mathbf{e}) = 1$ if and only if $z^2 - a_1 x_1^2 - a_2 x_2^2$ represents 0, that is equivalent to say (by Corollary 2.10) that f represents 1 an this condition does not depend on $\mathbf{e}$.

For $n \geq 3$ we use induction on n. By Theorem 2.13, it suffices to prove that $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e}')$ when $\mathbf{e}$ and $\mathbf{e}'$ are contiguous. By the symmetry of the Hilbert symbol, we can suppose that $\mathbf{e}' = \{v_1', \ldots, v_n'\}$ with $v_1' = v_1$. If we put $a_i' = Q(v_i')$, then $a_1' = a_1$. One can write $\varepsilon(\mathbf{e})$ in the form

$$\varepsilon(\mathbf{e}) = (a_1, a_2 \cdots a_n) \prod_{2 \leq i < j} (a_i, a_j) = (a_1, -d(Q)) \prod_{2 \leq i < j} (a_i, a_j),$$

and similarly

$$\varepsilon(\mathbf{e}') = (a_1, -d(Q)) \prod_{2 \leq i < j} (a_i', a_j').$$

Apply the inductive hypothesis to the orthogonal complement of v_1, the desired result follows. □

We therefore write from now on $\varepsilon(Q)$ instead of $\varepsilon(\mathbf{e})$ and call it the *Hasse invariant* of Q.

Let now f be a quadratic form of rank n. Let $d = d(f)$ and $\varepsilon = \varepsilon(f)$ be its discriminant and Hasse invariant, respectively.

Theorem 4.2. *For f to represent 0 it is necessary and sufficient that:*

(1) *$n = 2$ and $d = -1$ in k^*/k^{*2},*
(2) *$n = 3$ and $(-1, -d) = \varepsilon$,*
(3) *$n = 4$ and either $d \neq 1$ in k^*/k^{*2} or $d = 1$ in k^*/k^{*2} and $\varepsilon = (-1, -1)$,*
(4) *$n \geq 5$.*

Before proving the theorem, let us indicate a consequence of it: let $a \in k^*/k^{*2}$ and $g = f \boxplus az^2$. By Corollary 2.10, g represents 0 if and only if f represents a. On the other hand, $d(g) = -ad(f)$ and $\varepsilon(g) = (-a, d(f))\varepsilon(f)$. By applying Theorem 4.2 to g and taking into account the above formulas, we obtain:

Corollary 4.3. *Let $a \in k^*/k^{*2}$. In order that f represents a it is necessary and sufficient that:*

(1) $n = 1$ *and* $a = d$ *in* k^*/k^{*2},
(2) $n = 2$ *and* $(a, -d) = \varepsilon$,
(3) $n = 3$ *and either* $a \neq -d$ *in* k^*/k^{*2} *or* $a = -d$ *in* k^*/k^{*2} *and* $(-1, -d) = \varepsilon$,
(4) $n \geq 4$.

Proof of Corollary 4.3. If the rank of f is 1 , we have the rank of g is 2. Since in this case, g represents 0 if and only if $d(g) = -1$; this is equivalent to $ad(f) = 1$, *i.e.,* $d = d(f) = a$.

For $n = 2$, we have g represents 0 if and only if

$$(-1, d)(a, d)\varepsilon = (-a, d)\varepsilon = \varepsilon(g) = (-1, -d(g)) = (-1, ad) = (-1, a)(-1, d).$$

This is equivalent to $\varepsilon = (a, d)(a, -1) = (a, -d)$.

$-ad = d(g) \neq 1$ in k^*/k^{*2} is equivalent to $a \neq -d$ in k^*/k^{*2}. $d(g) = 1$ in k^*/k^{*2} and $(-a, d)\varepsilon = \varepsilon(g) = (-1, -1)$ is equivalent to $a = -d$ in k^*/k^{*2} and by Proposition 3.1 (3),

$$\varepsilon = (-a, d)(-1, -1) = (d, d)(-1, -1) = (-1, d)(-1, -1) = (-1, -d).$$

This proves the case for $n = 3$.

□

Proof of Theorem 4.2. We write f in the form $f \sim a_1x_1^2 + \cdots a_nx_n^2$.

(1) The case $n = 2$: The form f represents 0 if and only if $-a_1/a_2 = 1$ in k^*/k^{*2}; but $-a_1/a_2 = -a_1a_2 = -d$ in k^*/k^{*2}. This means that $d = -1$ in k^*/k^{*2}.
(2) The case $n = 3$: f represents 0 if and only if

$$-a_3 f \sim -a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$$

represents 0. Now by the definition of Hilbert symbol $-a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$ represents 0 if and only if $(-a_3a_1, -a_3a_2) = 1$. By the bilinear property of Hilbert symbol, we have the expansion

$$\begin{aligned}
1 &= (-a_3a_1, -a_3a_2) \\
&= (-1,-1)(-1,a_3)(-1,a_2)(a_3,-1)(a_3,a_3)(a_3,a_2)(a_1,-1)(a_1,a_3)(a_1,a_2) \\
&= (-1,-1)(-1,a_1)(-1,a_2)(a_3,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) \\
&= (-1,-1)(-1,a_1)(-1,a_2)(-1,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) \quad \text{(Proposition 3.1)} \\
&= (-1,-1)(-1,d)\,\varepsilon.
\end{aligned}$$

i.e., $(-1, -d) = \varepsilon$.

(3) The case $n = 4$: By Corollary 2.11, f represents 0 if and only if there exists an element $a \in k^*/k^{*2}$ which is represented by $a_1x_1^2 + a_2x_2^2$ and $-a_3x_3^2 - a_4x_4^2$. Since we already proved the case $n = 3$ we can apply case (2) ($n = 2$) of Corollary 4.3. Thus such an a is characterized by the conditions

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

Denote $\varepsilon_1 = (a_1, a_2)$ and $\varepsilon_2 = (-a_3, -a_4)$. In order that f does not represent 0, it is necessary and sufficient that $H^{\epsilon_1}_{-a_1a_2} \cap H^{\varepsilon_2}_{-a_3a_4} = \varnothing$. By Proposition 3.1 (3), $a_1 \in H^{\varepsilon_1}_{-a_1a_2}$ and $-a_3 \in H^{\varepsilon_2}_{-a_3a_4}$ and hence $H^{\varepsilon_1}_{-a_1a_2}$ and $H^{\varepsilon_2}_{-a_3a_4}$ are nonempty. Therefore, by Proposition 3.3 (2), $H^{\varepsilon_1}_{-a_1a_2} \cap H^{\varepsilon_2}_{-a_3a_4} = \varnothing$ is thus equivalent to $a_1a_2 = a_3a_4$ in k^*/k^{*2}

and $(a_1, a_2) = -(-a_3, -a_4)$. The first condition means that $d = 1$ in k^*/k^{*2}. If it is fulfilled, one has

$$\begin{aligned}
\varepsilon &= (a_1, a_2)(a_3, a_4)(a_1, a_3)(a_2, a_3)(a_1, a_4)(a_2, a_4) \\
&= (a_1, a_2)(a_3, a_4)(a_1a_2, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4) \\
&= (a_1, a_2)(a_3, a_4)(-1, a_3a_4) \quad \text{(Proposition 3.1)} \\
&= (a_1, a_2)(a_3, a_4)(-1, a_3)(-1, a_4) \\
&= (a_1, a_2)(a_3, -a_4)(-1, -a_4)(-1, -1) \\
&= (a_1, a_2)(-a_3, -a_4)(-1, -1).
\end{aligned}$$

Hence the second condition can be written $\varepsilon = -(-1, -1)$, from which the result follows.

(4) The case $n \geq 5$: It is sufficient to treat the case $n = 5$. By Corollary 2.11, f represents 0 if and only if there exists an element $a \in k^*/k^{*2}$ which is represented by $f_1 = a_1x_1^2 + a_2x_2^2$ and $f_2 = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2$. By the case $n = 2$, if $a_1a_2 = -1$ in k^*/k^{*2}, f_1 represents 0 and hence by Proposition 2.8, f_1 represents all elements of k. In particular, all non-zero values taken by f_2 can be represented by f_1. On the other hand, if $a_1a_2 \neq -1$ in k^*/k^{*2}, by using Proposition 3.3 and case (2) ($n = 2$) of Corollary 4.3, there are $2^{r-1} \geq 2$ elements in k^*/k^{*2} which can be represented by f_1. We can choose such a a so that $a \neq a_3a_4a_5$ in k^*/k^{*2} and hence by case (3)($n = 3$) of Corollary 4.3 (which can be proved by using case (3) ($n = 3$) above), a is represented by f_2 and the proof is complete.

□

To end this subsection, we give a classification of quadratic forms over $\mathbb{Q}_p$.

Theorem 4.4. *Two quadrate forms over k are equivalent if and only if they have the same rank, same discriminant and same Hasse invariant.*

Proof. That two equivalent forms have the same rank, discriminant and Hasse invariant follows from the definitions and Theorem 4.1. The converse is proved by induction on the rank n of two forms f and g considered. Corollary 4.3 shows that f and g represent the same elements of k^*/k^{*2}. One can thus find $a \in k^*$ which is represented at the same time by f and by g; by Corollary 2.10, this allows one to write:

$$f \sim ax^2 \boxplus f_1 \quad \text{and} \quad g \sim ax^2 \boxplus g_1,$$

where f_1 and g_1 are forms of rank $n-1$. One has $ad(f_1) = d(f) = d(g) = ad(g_1)$ which shows that $d(f_1) = d(g_1)$. One also has $\varepsilon(f_1)(a, d(f_1)) = \varepsilon(f) = \varepsilon(g) = \varepsilon(g_1)(a, d(g_1))$ which shows that $\varepsilon(f_1) = \varepsilon(g_1)$. In view of the inductive hypothesis, we have $f_1 \sim g_1$, hence $f \sim g$. □

Corollary 4.5. *Up to equivalence, there exists a unique quadratic form of rank 4 which does not represent 0; it is the form $z^2 - ax^2 - by^2 + abt^2$ with $(a, b) = -1$.*

Proof. By Theorem 4.2, such a form is characterized by $d(f) = 1$ and $\varepsilon(f) = -(-1, -1)$ and a simple computation shows that $z^2 - ax^2 - by^2 + abt^2$ has these properties. The uniqueness follows from Theorem 4.4. □

Proposition 4.6. *Let $n \geq 1$, $d \in k^*/k^{*2}$ and $\varepsilon = \pm 1$. In order that there exists a quadratic form f of rank n such that $d(f) = d$ and $\varepsilon(f) = \varepsilon$, it is necessary and sufficient that $n = 1$, $\varepsilon = 1$; or $n = 2$, $d \neq -1$ in k^*/k^{*2}; or $n = 2$, $\varepsilon = 1$; or $n \geq 3$.*

Proof. The case $n = 1$ is trivial. If $n = 2$, one has $f \sim ax^2 + by^2$ and $d(f) = ab = -1$ in k^*/k^{*2} implies $\varepsilon(f) = (a, b) = (a, -ab) = 1$. Thus, we must have either $d(f) \neq -1$ in k^*/k^{*2} or $\varepsilon(f) = 1$. Conversely, if $d \neq -1$ in k^*/k^{*2}, there exists $a \in k^*$ such that $(a, -d) = \varepsilon$ and we take $f = ax^2 + ady^2$ so that $d(f) = a^2 d = d$ in k^*/k^{*2} and $\varepsilon(f) = (a, ad) = (a, -d) = \varepsilon$; for $f = x^2 - y^2$, we have $d(f) = -1$ and $\varepsilon(f) = 1$.

If $n = 3$, we can choose $a \in k^*/k^{*2}$ such that $a \neq -d$ (*i.e.*, $ad \neq -1$) in k^*/k^{*2}. By what we have just seen, there exists a form g of rank 2 such that $d(g) = ad$ and $\varepsilon(g) = \varepsilon(a, -d)$. The form $f = az^2 \boxplus g$ has $d(f) = ad(g) = d$ in k^*/k^{*2} and $\varepsilon(f) = (a, d(g))\varepsilon(g) = (a, -d)^2\varepsilon = \varepsilon$. The case $n \geq 4$ is reduced to the case $n = 3$ by taking $f = g(x_1, x_2, x_3) + x_4^2 + \cdots + x_n^2$ where g is a form of rank 3 of given d and ε. □

Corollary 4.7. *The number of equivalent classes of quadratic forms of rank n over $\mathbb{Q}_p$ for $p \neq 2$ is equal to 4 if $n = 1$, to 7 if $n = 2$ and to 8 if $n \geq 3$; for $p = 2$ is equal to 8 if $n = 1$, to 15 if $n = 2$ and to 16 if $n \geq 3$.*

Proof. For $p \neq 2$, k^*/k^{*2} has 4 elements and for $p = 2$, k^*/k^{*2} has 8 elements. Since ε can take 2 values, our result follows easily from Proposition 4.6. □

4.2. **Quadratic Forms over $\mathbb{R}$.** Let f ba a quadratic form of rank n over the field $\mathbb{R}$ of real numbers. We know that $\mathbb{R}^*/\mathbb{R}^{*2} = \{\pm 1\}$ and hence f is equivalent to $x_1 + \cdots + x_r^2 - y_1^2 - \cdots y_s^2$, where r and s are two nonnegative integers such that $r + s = n$.

Theorem 4.8 (Sylvester's Law of Inertia)**.** *Let (V, Q) be a real nondegenerate quadratic space of rank n. The number r and s are independent of the orthogonal basis of V.*

Proof. Suppose that $\mathbf{e} = \{v_1, \ldots, v_r, v_{r+1}, \ldots, v_n\}$ and $\mathbf{e}' = \{v_1', \ldots, v_{r'}', v_{r'+1}', \ldots, v_n'\}$ are two orthogonal bases with $Q(v_i) > 0$ (*resp.* $Q(v_{i'}') > 0$) for $1 \leq i \leq r$ (*resp.* $1 \leq i' \leq r'$) and $Q(v_j) < 0$ (*resp.* $Q(v_{j'}) < 0$) for $r < j \leq n$ (*resp.* $r' < j' \leq n$).

We suppose that $r \neq r'$ and arrive at a contradiction. Without loss of generality assume that $r < r'$. Let $l : V \to \mathbb{R}^{n+r-r'}$ be the mapping defined by

$$l(v) = (H(v, v_1), \ldots, H(v, v_r), H(v, v_{r'+1}'), \ldots, H(v, v_n')).$$

It is easy to check that l is linear and $\dim(l(V)) \leq n + r - r'$. Hence $\dim(\mathrm{Ker}(l)) \geq r' - r > 0$. Therefore, there exist a nonzero $v_0 \in \mathrm{Ker}(l)$. It follows that $H(v_0, v_i) = 0$ for $i \leq r$ and $H(v_0, v_j') = 0$ for $r' < j \leq n$. Hence we have

$$v_0 = \sum_{i=r+1}^{n} a_i v_i = \sum_{j=1}^{r'} b_j v_j'.$$

Thus

$$Q(v_0) = \sum_{i=r+1}^{n} a_i^2 Q(v_i) \geq 0 \quad \text{and} \quad Q(v_0) = \sum_{j=1}^{r'} b_j^2 Q(v_j') \leq 0.$$

So we have $a_i = b_j = 0$ which contradict to that v_0 is nonzero. □

From Sylvester's law of inertia, the pair (r, s) depends only on f; it is called the *signature* of f. We say that f is definite if $r = 0$ or $s = 0$, *i.e.*, if f does not change sign; otherwise, we say that f is *indefinite*. Only indefinite real quadratic form represents 0.

We can see easily that $d(f) = (-1)^s$ in $\mathbb{R}^*/\mathbb{R}^{*2}$. The Hasse invariant $\varepsilon(f)$ is defined as in the case of $\mathbb{Q}_p$; due to the fact that $(-1, -1) = -1$, we have $\varepsilon(f) = (-1)^{s(s-1)/2}$.

Though the representation of elements in $\mathbb{R}$ of a quadratic form can be directly derived, it is interested to know that parts (1), (2), (3) of Theorem 4.2 and Corollary 4.3 are valid for $\mathbb{R}$ (indeed their proofs use only the nondegeneracy of the Hilbert symbol). However, part (4) does not extend (indeed, in the proof we use the fact that the number of H_a^ε is ≥ 2 which is not true for $\mathbb{R}$).

5. Quadratic Forms over $\mathbb{Q}$

All quadratic forms considered in this section have coefficients in $\mathbb{Q}$ and are nondegenerate.

5.1. **Invariants of a Quadratic Form.** We denote by $\mathcal{V}$ the union of the set of prime numbers and the symbol ∞, and we put $\mathbb{Q}_\infty = \mathbb{R}$.

Let $f \sim a_1x_1^2 + \cdots + a_nx_n^2$ be a quadratic form of rank n. We associate to it the following invariants:

(1) The discriminant $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ equal to $a_1 \cdots a_n$.

(2) Let $\nu \in \mathcal{V}$. The injection $\mathbb{Q} \to \mathbb{Q}_\nu$ allows one to view f as a quadratic form f_ν over $\mathbb{Q}_\nu$. The discriminant and Hasse invariant of f_ν will be denoted by $d_\nu(f)$ and $\varepsilon_\nu(f)$, respectively. It is clear that $d_\nu(f)$ is the image of $d(f)$ by $\mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$ and we have

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

The product formula (Theorem 3.4) gives the relation

$$\prod_{\nu \in \mathcal{V}} \varepsilon_\nu(f) = 1.$$

(3) The signature (r, s) of the real quadratic form f is another invariant of f.

$d_\nu(f)$, $\varepsilon_\nu(f)$ and (r, s) are sometimes called the *local invariants* of f.

5.2. **Hasse-Minkowski Theorem.** Hasse-Minkowski theorem is mainly concerning about representation of a ration number by a quadratic form. It says that f has a "global" zero if and only if f has everywhere a "local" zero.

Theorem 5.1 (Hasse-Minkowski)**.** *In order that f represent 0, it is necessary and sufficient that for all $\nu \in \mathcal{V}$, the form f_ν represents 0.*

Proof. The necessity is trivial. In order to see the sufficiency, we write $f = a_1x_1^2 + \cdots + a_nx_n^2$ with $a_i \in \mathbb{Q}^*$. Replacing f by a_1f, one can moreover suppose that $a_1 = 1$; being free to multiply by squares, we can assume that a_i are square free integers (*i.e.*, $\nu_p(a_i)$ is equal to 0 or 1 for all prime numbers p).

(1) The case $n = 2$: We have $f \sim x_1^2 - ax_2^2$. Since f_∞ represents 0, $a > 0$. If we write $a = \prod_p p^{\nu_p(a)}$, the fact that f_p represents 0 shows that a is a square in $\mathbb{Q}_p$, hence $\nu_p(a) = 0$. From this follows that $a = 1$ and $f \sim x_1^2 - x_2^2$ represents 0.

(2) The case $n = 3$ (Legendre): We have $f \sim x_1^2 - ax_2^2 - bx_3^2$. We assume that $|a| \leq |b|$ and use induction on the integer $m = |a| + |b|$. If $m = 2$, we have $f \sim x_1^2 \pm x_2^2 \pm x_3^2$; the case of $x_1^2 + x_2^2 + x_3^2$ is excluded because f_∞ represents 0; in other cases, f represents 0.

Suppose now that $m > 2$. For every $p \mid b$, we are going to prove that a is a square modulo p. This is obvious if $a \equiv 0 \pmod{p}$. Otherwise, by hypothesis there exists $(\alpha, \beta, \gamma) \in \mathbb{Z}_p^3$ such that $\gamma^2 - a\alpha^2 - b\beta^2 = 0$ and (α, β, γ) is *primitive* (*i.e.*, at least one of α, β or γ is a p-adic unit). If $p \mid \alpha$, then $p \mid \gamma$ and hence $p^2 \mid b\beta^2$. Since $p^2 \nmid b$, this implies that $p \mid \beta$ and contrary to the fact that (α, β, γ) is primitive. Thus, we have $p \nmid \alpha$, which shows that $a \equiv (\gamma/\alpha)^2 \pmod{p}$. Since b is square free, by Chinese remainder theorem, we see that a is a square modulo b. There exist thus integers u and b' such that $u^2 = a + bb'$ and (by substituting u by $u + \lambda b$) we can always choose u such that $|u| \leq |b|/2$. $u^2 - a \cdot 1^2 - bb' \cdot 1^2$ shows that $(a, bb')_\nu = 1$ for all $\nu \in \mathcal{V}$. Combining this with the assumption $(a, b)_\nu = 1$, $\forall\, \nu \in \mathcal{V}$, we have that $(a, b')_\nu = 1$, $\forall\, \nu \in \mathcal{V}$. This shows that $g = x_1^2 - ax_2^2 - b'x_3^2$ represents 0 in each of the $\mathbb{Q}_\nu$. But we have

$$|b'| = \left|\frac{u^2 - a}{b}\right| \leq \frac{|b|}{4} + \frac{|a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|. \quad \text{(because } |b| \geq 2)$$

Write b' in the form $b''\lambda^2$ with b'', λ integers and b'' square free; we have *a fortiori* $|b''| < |b|$. The induction hypothesis applies thus to the form $x_1^2 - ax_2^2 - b''x_3^2$ which is equivalent to g and hence g represents 0 in $\mathbb{Q}$. Suppose that $(\alpha, \beta, \gamma) \in \mathbb{Q}^3$ such that $\gamma^2 - a\alpha^2 - b'\beta^2 = 0$. If $\beta = 0$, we have a is a square in $\mathbb{Q}$ and hence $f \sim x_1^2 - ax_2^2 - bx_3^2$ represents 0; otherwise we have that $b' = (\gamma/\beta) - a(\alpha/\beta)^2$ and this shows that b' is a norm of the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$. Since $bb' = u^2 - a$ is also a norm of the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$, this implies that b is a norm of the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$. Therefore, $b = \zeta^2 - a\eta^2$ for $\zeta, \eta \in \mathbb{Q}$, thus $x_1^2 - ax_2^2 - bx_3^2$ represents 0.

(3) The case $n = 4$: Write $f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$. For every $\nu \in \mathcal{V}$, since f_ν represents 0, Corollary 2.11 shows that there exists α_ν which is represented both by $ax_1^2 + bx_2^2$ and by $cx_3^2 + dx_4^2$. By part (2) of Corollary 4.3, this is equivalent to saying that

$$(\alpha_\nu, -ab)_\nu = (a, b)_\nu \quad \text{and} \quad (\alpha_\nu, -cd)_\nu = (c, d)_\nu \ \forall\, \nu \in \mathcal{V}.$$

Since $\prod_{\nu\in\mathcal{V}}(a, b)_\nu = \prod_{\nu\in\mathcal{V}}(c, d)_\nu = 1$, we can apply Theorem 3.5 and obtain from it the existence of $\alpha \in \mathbb{Q}^*$ such that

$$(\alpha, -ab)_\nu = (a, b)_\nu \quad \text{and} \quad (\alpha, -cd)_\nu = (c, d)_\nu \ \forall\, \nu \in \mathcal{V}.$$

This shows that both $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$ represent α in each of the $\mathbb{Q}_\nu$ and hence $ax_1^2 + bx_2^2 - \alpha z^2$ and $cx_3^2 + dx_4^2 - \alpha z^2$ in each of the $\mathbb{Q}_\nu$ (Corollary 2.10). By what we have just proved (the case of $n = 3$), $ax_1^2 + bx_2^2 - \alpha z^2$ and $cx_3^2 + dx_4^2 - \alpha z^2$ both represent 0 in $\mathbb{Q}$ and hence α is represented in $\mathbb{Q}$ by $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$; the fact that f represents 0 follows from this.

(4) The case $n \geq 5$: We use induction on n. We write f in the form

$$f = h \boxminus g \quad \text{with} \quad h = a_1x_1^2 + a_2x_2^2,\ g = -(a_3x_3^2 + \cdots + a_nx_n^2).$$

Let S be a subset of $\mathcal{V}$ consisting of ∞, 2 and the primes p such that $\nu_p(a_i) \neq 0$ for one $i \geq 3$.; it is a finite set. For $\nu \in S$, since f_ν represents 0, there exist $\alpha_\nu \in \mathbb{Q}_\nu^*$ and

$x_i^\nu \in \mathbb{Q}_\nu$, $i = 1, \dots, n$ such that

$$h(x_1^\nu, x_2^\nu) = \alpha_\nu = g(x_3^\nu, \dots, x_n^\nu).$$

Consider h as a mapping from $\prod_{\nu\in S} Q_\nu^2 \to \prod_{\nu\in S} Q_\nu$. Let

$$U_\nu = \begin{cases} 1 + p\mathbb{Z}_p & \text{if } \nu = p \neq 2, \\ 1 + 8\mathbb{Z}_2 & \text{if } \nu = 2, \\ \mathbb{R}^+ & \text{if } \nu = \infty. \end{cases}$$

Because h is continuous and U_ν is a open set of $\mathbb{Q}_\nu^*$, the pre-image of h of the open neighborhood $(\dots, \alpha_\nu U_\nu, \dots)$ is also an open set. By the "approximation theorem" (*i.e.*, $\mathbb{Q}$ is dense in $\prod_{\nu\in S} \mathbb{Q}_\nu$), there exists $(\beta, \gamma) \in \mathbb{Q}^2$ such that the image of (β, γ) in $\prod_{\nu\in S} Q_\nu^2$ is in the pre-image. Thus if $h(\beta, \gamma) = \alpha$, then $\alpha \in \alpha_\nu U_\nu$ for every $\nu \in S$. If $\nu \in S$, g represents $\alpha_\nu \in \mathbb{Q}_\nu$, thus also α because $U_\nu \subset \mathbb{Q}_\nu^{*\,2}$ (this can be shown by using Hensel's Lemma); hence $f_1 = \alpha z^2 - g$ represents 0 in $\mathbb{Q}_\nu$. If $\nu \notin S$, the coefficients of g are ν-adic units; the same is true of $d_\nu(g)$, and because $\nu \neq 2$, we have $\varepsilon_\nu(g) = 1$ (recall that $(a, b)_\nu = 1$ if a, b are ν-adic units). For $n > 5$ the rank of g is ≥ 4 and for $n = 5$, the rank of g is 3; in this case $(-1, -d_\nu(g)) = 1 = \varepsilon_\nu(g)$. By Corollary 4.3, g represents α in $\mathbb{Q}_\nu$, and hence f_1 represents 0 in $\mathbb{Q}_\nu$. In all cases, since the rank of f_1 is $n - 1$, the inductive hypothesis shows that f_1 represents 0 in $\mathbb{Q}$, *i.e.*, g represents α in $\mathbb{Q}$; since we have chosen α such that h represents α in $\mathbb{Q}$, f represents 0 in $\mathbb{Q}$ and the proof is complete.

□

Corollary 5.2. *Let $a \in \mathbb{Q}^*$. In order that f represents a in $\mathbb{Q}$, it is necessary and sufficient that it does in each of the $\mathbb{Q}_\nu$.*

Proof. Applying Theorem 5.1 to the form $g = az^2 \boxminus f$, we have that g represents 0 in $\mathbb{Q}$ if and only if g represents 0 in each of $\mathbb{Q}_\nu$. By Corollary 2.10, our result follows.

□

Corollary 5.3 (Meyer)**.** *A quadratic form of rank ≥ 5 represents 0 if and only if it is indefinite.*

Proof. Indeed, it represents 0 in $\mathbb{R}$ and by Theorem 4.2, such a form represents 0 in each of the $\mathbb{Q}_p$. □

Corollary 5.4. *Let n be the rank of f. Suppose that*

(1) *$n = 2$ and f represents 0 in almost all the $\mathbb{Q}_\nu$;*
(2) *$n = 3$ and f represents 0 in all the $\mathbb{Q}_\nu$ except at most one;*
(3) *$n = 4$, $d(f) = 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*\,2}$ and f represents 0 in all the $\mathbb{Q}_\nu$ except at most one.*

Then f represents 0 in $\mathbb{Q}$.

Proof. For $n = 2$, by Theorem 4.2, f represents 0 in $\mathbb{Q}$ if and only if $-d(f)$ is in $\mathbb{Q}_\nu^{*\,2}$ for every $\mathbb{Q}_\nu$. One can show, by means of the "Dirichlet theorem" that if $-d(f)$ is not a square in $\mathbb{Q}$, then there are infinitely many p such that $-d(f)$ is not a square in $\mathbb{Q}_p$.

For $n = 3$, f represents 0 in $\mathbb{Q}$ if and only if $(-1, -d(f))_\nu = \varepsilon_\nu(f)$ for every $\nu \in \mathcal{V}$. But the two families $\varepsilon_\nu(f)$ and $(-1, -d(f))_\nu$ satisfy the product formula (Theorem 3.4). From this, it is impossible that there is only one $\nu \in \mathcal{V}$ such that $(-1, -d(f))_\nu \neq \varepsilon_\nu(f)$ and hence f represents 0.

For $n = 4$ and $d(f) = 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$, we have that f represents 0 in $\mathbb{Q}$ if and only if $(-1,-1)_\nu = \varepsilon_\nu(f)$ for every $\nu \in \mathcal{V}$. We argue in the same as in the case $n = 3$.

□

5.3. **Classification.**

Theorem 5.5. *Let f and g be two quadratic forms over $\mathbb{Q}$. For f and g to be equivalent over $\mathbb{Q}$ it is necessary and sufficient that f and g are equivalent over each $\mathbb{Q}_\nu$.*

Proof. The necessity is trivial. To prove the sufficiency, we use induction on the rank n of f and g. For the case $n = 0$ there is nothing to prove. Otherwise, consider any $a \in \mathbb{Q}^*$ which is represented by f in $\mathbb{Q}$ and hence in each $\mathbb{Q}_\nu$. Since $f \sim g$ over each $\mathbb{Q}_\nu$, a is also represented by g in each $\mathbb{Q}_\nu$ and hence by Corollary 5.2, a is represented by g over $\mathbb{Q}$. Thus we have $f \sim az^2 \boxplus f_1$ and $g \sim az^2 \boxplus g_1$. Again, since $f \sim g$ over each $\mathbb{Q}_\nu$, we have $f_1 \sim g_1$ over each $\mathbb{Q}_\nu$. The induction hypothesis then shows that $f_1 \sim g_1$ over $\mathbb{Q}$, hence $f \sim g$ over $\mathbb{Q}$. □

Let f and g be two quadratic form over $\mathbb{Q}$. By Theorem 4.4, $f \sim g$ over $\mathbb{Q}_p$ if and only if they have the same rank, $d_p(f) = d_p(g)$ and $\varepsilon_p(f) = \varepsilon_p(g)$. Also, by Theorem 4.8, $f \sim g$ in $\mathbb{R}$ if and only if they have the same signatures. Combining these with Theorem 5.5, we have the following corollary.

Corollary 5.6. *Let (r,s) and (r',s') be the signatures of the two quadratic forms f and g over $\mathbb{Q}$, respectively. For f and g to be equivalent it is necessary and sufficient that one has*

$$d(f) = d(g), \quad (r,s) = (r',s') \quad \text{and} \quad \varepsilon_\nu(f) = \varepsilon_\nu(g), \forall\, \nu \in \mathcal{V}.$$

Proof. Indeed, since $d(f)$ and $d(g)$ are in $\mathbb{Q}$, $d(f) = d(g)$ if and only if $d_p(f) = d_p(g)$ for every p. □

The invariants $d = d(f)$, $\varepsilon_\nu = \varepsilon_\nu(f)$ and (r,s) are not arbitrary. They satisfy the following relations:

(1) $\varepsilon_\nu = 1$ for almost all $\nu \in \mathcal{V}$ and $\prod_{\nu\in\mathcal{V}} \varepsilon_\nu = 1$,
(2) if $n = 1$, then $\varepsilon_\nu = 1$ for all $\nu \in \mathcal{V}$ (by definition),
(3) if $n = 2$ and the image $-d_\nu$ of $-d$ in $\mathbb{Q}_\nu^*$ is a square, then $\varepsilon_\nu = 1$ (because if $f \sim ax^2 + by^2$, then $\varepsilon_\nu = (a,b)_\nu = (a,-d)_\nu = 1$),
(4) $r, s \geq 0$ and $r + s = n$,
(5) $d_\infty = (-1)^s$,
(6) $\varepsilon_\infty = (-1)^{s(s-1)/2}$ (because $(-1,-1)_\infty = -1$).

Proposition 5.7. *Let d, $(\varepsilon_\nu)_{\nu\in\mathcal{V}}$ and (r,s) satisfy the relations (1) to (6) above. Then there exists a quadratic form of rank n over $\mathbb{Q}$ having $d(f) = d$, $\varepsilon_\nu(f) = \varepsilon_\nu$ and signature (r,s).*

Proof. The case $n = 1$ is trivial.

Suppose that $n = 2$. For $\nu \in \mathcal{V}$, if $-d_\nu \in \mathbb{Q}_\nu^{*2}$, by condition (3), for any $a_\nu \in \mathbb{Q}_\nu^*$, we have $(a_\nu, -d)_\nu = 1 = \varepsilon_\nu$; if $-d_\nu \notin \mathbb{Q}_\nu^{*2}$, then by the nondegeneracy of the Hilbert symbol, there exists $a_\nu \in \mathbb{Q}_\nu^*$ such that $(a_\nu, -d)_\nu = \varepsilon_\nu$. From this and condition (1), follows the existence of $a \in \mathbb{Q}^*$ such that $(a,-d)_\nu = \varepsilon_\nu$ for all $\nu \in \mathcal{V}$ (*c.f.* Theorem 3.5). The form $ax^2 + ady^2$ works.

Suppose that $n = 3$. Let $\mathcal{S}$ be the set of $\nu \in \mathcal{V}$ such that $(-d,-1)_\nu = -\varepsilon_\nu$. $\mathcal{S}$ is a finite set. Indeed, by condition (1) there are only finitely many $\nu \in \mathcal{V}$ such that $-\varepsilon_\nu = 1$, so that there are only finitely many $\nu \in \mathcal{V}$ such that $-\varepsilon_\nu = (-d,-1)_\nu = 1$; similarly, there are only

finitely many $\nu \in \mathcal{V}$ such that $(-d,-1)_\nu = -\varepsilon_\nu = -1$ (Theorem 3.4). If $\nu \in \mathcal{S}$, choose $c_\nu \neq -d_\nu$ in $\mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$. Since Q_ν^{*2} is an open set of $\mathbb{Q}_\nu^*$ (recall that $U_\nu \subseteq \mathbb{Q}_\nu^{*2}$ is open in $\mathbb{Q}_\nu^*$), using the approximation theorem, there exists $c \in \mathbb{Q}^*$ such that $c = c_\nu$ in $\mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$, for every $\nu \in \mathcal{S}$. Let $d' = cd$ and let $\varepsilon'_\nu = (c,-d)_\nu\varepsilon_\nu$, $\forall\, \nu \in \mathcal{V}$. Since $(c,-d)_\nu = 1$ for almost all $\nu \in \mathcal{V}$ and $\prod_{\nu\in\mathcal{V}}(c,-d)_\nu = 1$ (Theorem 3.4), $(\varepsilon'_\nu)_{\nu\in\mathcal{V}}$ satisfies condition (1). Also, if the image $-d'_\nu$ of $-d'$ in $\mathbb{Q}_\nu^*$ is a square (*i.e.*, $c_\nu = -d_\nu$ in $\mathbb{Q}_\nu^*/\mathbb{Q}_\nu^{*2}$), then $\nu \notin \mathcal{S}$ and hence, $(-d,-1)_\nu \neq -\varepsilon_\nu$ (*i.e.*, $(-d,-1)_\nu = \varepsilon_\nu$); thus,

$$\varepsilon'_\nu = (c,-d)_\nu\varepsilon_\nu = (cd,-d)_\nu\varepsilon_\nu = (-1,-d)_\nu\varepsilon_\nu = 1.$$

Hence, from what we have just proved (using only conditions (1) and (3)) follows the existence of a form g of rank 2 such that

$$d(g) = d' = cd \quad \text{and} \quad \varepsilon_\nu(g) = \varepsilon'_\nu = (c,-d)_\nu\varepsilon_\nu,\ \forall\, \nu \in \mathcal{V}.$$

The form $f = cz^2 \boxplus g$ then has $d(f) = cd(g) = c^2d = d$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ and

$$\varepsilon_\nu(f) = (c, d(g))_\nu\varepsilon_\nu(g) = (c,cd)_\nu(c,-d)_\nu\varepsilon_\nu = (c,-d)_\nu^2\varepsilon_\nu = \varepsilon_\nu.$$

When $n \geq 4$, we use induction on n. Suppose first that $r \geq 1$. Because d_∞ and ε_∞ depend only on s, using the induction hypothesis, we obtain a form g of rank $n-1$ which has for invariants $d(g) = d$, $(\varepsilon_\nu(g))_{\nu\in\mathcal{V}} = (\varepsilon_\nu)_{\nu\in\mathcal{V}}$ and signature $(r-1,s)$; the form $x^2 \boxplus g$ is then a form of rank n with desired invariants. When $r = 0$ (*i.e.*, $s = n$) we consider $d' = -d$ and $\varepsilon'_\nu = \varepsilon_\nu(-1,-d)_\nu$ for all $\nu \in \mathcal{V}$. We have $(\varepsilon'_\nu)_{\nu\in\mathcal{V}}$ satisfies condition (1), the image d' in $\mathbb{R}^*/\mathbb{R}^{*2}$ is $-d = (-1)\cdot(-1)^n = (-1)^{n-1}$ and

$$\varepsilon'_\infty = \varepsilon_\infty(-1,-d)_\infty = (-1)^{n(n-1)/2}\cdot(-1)^{n-1} = (-1)^{(n-1)(n-2)/2}.$$

These are conditions (5) and (6) for $s = n-1$. By the inductive hypothesis, we obtain a form h of rank $n-1$ having for invariants $d(h) = d' = -d$, $\varepsilon_\nu(h) = \varepsilon'_\nu = \varepsilon_\nu(-1,-d)_\nu$ and signature $(0,n-1)$; the form $f = -z^2 \boxplus h$ has $d(f) = -d(h) = d$,

$$\varepsilon_\nu(f) = (-1, d(h))_\nu\varepsilon_\nu(h) = (-1,-d)_\nu(-1,-d)_\nu\varepsilon_\nu = \varepsilon_\nu$$

and signature $(0,n)$. □

Note that in this proof, for $n \leq 3$ we do not need to consider the signature of the form. Indeed, d_∞ and ε_∞ is equivalent to that of the class of s modulo 4 and hence, when $n \leq 3$, d_∞ and ε_∞ determinate s uniquely.

5.4. **Sums of Three Squares.** Let n be a positive integer. We say that n is the sum of 3 squares if n is representable over the ring $\mathbb{Z}$ by the quadratic form $x_1^2 + x_2^2 + x_3^2$, *i.e.* there exist integers n_1, n_2 and n_3 such that $n = n_1^2 + n_2^2 + n_3^2$.

Lemma 5.8. *Let $a \in \mathbb{Q}^*$. In order that a be represented in $\mathbb{Q}$ by the form $f = x_1^2 + x_2^2 + x_3^2$ it is necessary and sufficient that $a > 0$ and that $-a$ is not a square in $\mathbb{Q}_2$*

Proof. By Corollary 5.2, we have to represent a by f in $\mathbb{R}$ and in all $\mathbb{Q}_p$. The case of $\mathbb{R}$ gives the positivity condition. On the other hand, we have the local invariants $d_p(f) = 1$ and $\varepsilon_p(f) = 1$ for all prime p. If $p \neq 2$, we have $(-1,-d(f))_p = (-1,-1)_p = 1 = \varepsilon_p(f)$; Corollary 4.3 thus shows that a is represented by f in $\mathbb{Q}_p$. if $p = 2$, we have $(-1,-d(f))_2 = (-1,-1) = -1 \neq \varepsilon_2(f)$; Again, Corollary 4.3 shows that a is represented by f in $\mathbb{Q}_2$ if and only if $a \neq -1$ in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, *i.e.*, if $-a$ is not a square in $\mathbb{Q}_2$. □

Now we must pass from representations in $\mathbb{Q}$ to representations in $\mathbb{Z}$. Note that for every $(a_1, a_2, a_3) \in \mathbb{Q}^3$, we can choose $(m_1, m_2, m_3) \in \mathbb{Z}^3$ such that $|a_i - m_i| \leq 1/2$ for $i = 1, 2, 3$; we have $(a_1 - m_2)^2 + (a_2 - m_2)^2 + (a_3 - m_3)^2 \leq 3/4 < 1$. Hence, we can apply the following Lemma.

Lemma 5.9 (Davenport-Cassels). *Let f be a positive definite quadratic form of rank r with integer coefficients. Suppose that for every $(a_1, \ldots, a_r) \in \mathbb{Q}^r$ there exists $(m_1, \ldots, m_r) \in \mathbb{Z}^r$ such that $f(a_1 - m_1, \ldots, a_r - m_r) < 1$. If $n \in \mathbb{Z}$ is represented by f in $\mathbb{Q}$, then n is represented by f in $\mathbb{Z}$.*

Proof. Let H be the symmetric bilinear form corresponding to f; thus, we have $H(v, v) = f(v)$. Let $n \in \mathbb{Z}$ be represented by f in $\mathbb{Q}$. There exists an integer $t > 0$ such that $t^2 n = f(\alpha_1, \ldots, \alpha_r)$ with $v = (\alpha_1, \ldots, \alpha_r) \in \mathbb{Z}^r$. Choose t in such a way that it is minimum; we claim that $t = 1$.

By the hypothesis, there exists $w = (m_1, \ldots, m_r) \in \mathbb{Z}^r$ such that

$$(\frac{\alpha_1}{t}, \ldots, \frac{\alpha_r}{t}) = (m_1, \ldots, m_r) + (\beta_1, \ldots, \beta_r), \quad \text{with } f(\beta_1, \ldots, \beta_r) < 1.$$

If $f(\beta_1, \ldots, \beta_r) = 0$, we have $(\beta_1, \ldots, \beta_r) = (0, \ldots, 0)$ because f is positive definite. Hence $(\alpha_1/t, \ldots, \alpha_r/t) \in \mathbb{Z}^r$. Because of the minimality of t, this implies that $t = 1$.

Assume now that $f(\beta_1, \ldots, \beta_r) \neq 0$ and put

$$a = f(w) - n, \quad \text{and} \quad b = 2(nt - H(v, w)).$$

We also put

$$t' = at + b \quad \text{and} \quad v' = av + bw.$$

It is clear that $a, b, t' \in \mathbb{Z}$, $v' \in \mathbb{Z}^r$ and

$$f(v') = a^2 f(v) + 2abH(v, w) + b^2 f(w) = a^2 t^2 n + ab(2nt - b) + b^2(n + a) = t'^2 n.$$

Moreover,

$$\begin{aligned} tt' &= at^2 + bt = t^2 f(w) - nt^2 + 2nt^2 - 2tH(v, w) \\ &= t^2 f(w) - 2tH(v, w) + f(v) \\ &= f(tw - v) \\ &= t^2 f(\beta_1, \ldots, \beta_r) \end{aligned}$$

Hence, $t' = tf(\beta_1, \ldots, \beta_r)$; since $0 < f(\beta_1, \ldots, \beta_r) < 1$, we have $0 < t' < t$. This contradicts the minimality of t and concludes the proof of the lemma. □

Using generalized Hensel's lemma, we know that a positive integer n of the form $4^\alpha(8\beta - 1)$ is equivalent to say that $-n$ is a square in $\mathbb{Q}_2^*$. Combining this with Lemma 5.8 and Lemma 5.9, we have the following theorem.

Theorem 5.10 (Gauss). *In order that a positive integer be a sum of three squares it is necessary and sufficient that it is not of the form $4^\alpha(8\beta - 1)$ with $\alpha, \beta \in \mathbb{N}$.*

A positive integer n is a sum of four squares if there exist integers $n_1, \ldots, n_4$ such that $n = n_1^2 + \cdots + n_4^2$.

Corollary 5.11 (Largrange). *Every positive integer is a sum of four squares.*

Proof. We write n in the form $4^\alpha m$ where $4 \nmid m$. m is not a sum of three squares only when $m \equiv -1 \pmod 8$, but in this case $m-1$ is a sum of three squares and hence m is a sum of four squares; the same holds for n. □

A number is called *triangular* if it is of the form $m(m+1)/2$ with $m \in \mathbb{Z}$.

Corollary 5.12 (Gauss)**.** *Every positive integers is a sum of three triangular numbers.*

Proof. Given a positive integer m, by applying Theorem 5.10 to the number $8m+3$, there exist $n_1, n_2, n_3 \in \mathbb{Z}$ such that $n_1^2 + n_2^2 + n_3^2 = 8m+3$. The only squares modulo 8 is $0, 1, 4$ Hence we have that $n_i = 2m_i + 1$ for $i = 1, 2, 3$. We have

$$\sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} = \frac{1}{8}\left(\sum_{i=1}^{3}(2m_i+1)^2 - 3\right) = \frac{1}{8}(8m+3-3) = m.$$

□

References

[1] S. Friedberg, A. Insel & L. Spence, *Linear Algebra*, 2nd ed., Prentice-Hall, New Jersey, 1992.
[2] Y. Kitaoka, *Arithmetic of Quadratic Forms*, Cambridge University Press, Cambridge, 1993.
[3] J-P. Serre, *A Course in Arithmetic*, GTM 7, Springer-Verlag, Berlin and New York, 1973.

Department of Mathematics, National Taiwan Normal University
E-mail address: li@math.ntnu.edu.tw