PAIRS OF QUADRATIC FORMS OVER COMPLETE DISCRETELY VALUED FIELDS

DAVID B. LEEP and NANDITA SAHAJPAL

Communicated by Alexandru Zaharescu

Let F be a complete discretely valued field with residue field $\overline{F}$, $\operatorname{char} F \neq 2$. We express the u-invariant of F for one quadratic form, $u(F)$, and a pair of quadratic forms, $u_2(F)$, in terms of the u-invariants of $\overline{F}$ for one quadratic form and a pair of quadratic forms, respectively. It is well known that $u(F) = 2u(\overline{F})$. We give a new and simpler proof of this result that includes the case $\operatorname{char} \overline{F} = 2$. It is also known that $u_2(F) = 2u_2(\overline{F})$ when F is a p-adic field. We extend this result to an arbitrary complete discretely valued field F with $\operatorname{char} F \neq 2$. This paper gives a self-contained exposition of this material.

AMS 2020 Subject Classification: 11E08, 11D72, 12J25, 11D79.

Key words: pairs of quadratic forms, complete discretely valued field, u-invariant, nonsingular zero, Hensel's lemma.

1. INTRODUCTION

It was proved in [3], with a simplified proof given in [2], that a system of two quadratic forms in at least 9 variables with coefficients in a p-adic field F always has a nontrivial common zero over F. The main result of this paper is to prove an analogous result (Theorem 1.2) that holds for an arbitrary complete discretely valued field F with $\operatorname{char} F \neq 2$.

The classical u-invariant of a field F, $u(F)$, is the supremum of all integers n such that there exists an anisotropic quadratic form in n variables with coefficients in F. More generally, $u_r(F)$ is defined as the supremum of all integers n such that there is an anisotropic system $\mathcal{S} = \{f_1, \ldots, f_r\}$ of r quadratic forms in n variables with coefficients in F. Thus, $u_1(F) = u(F)$.

For any system of homogeneous forms $f_1, \ldots, f_r \in F[X_1, \ldots, X_n]$, we say that $a \in F^n$ is a nontrivial zero of the system if $f_i(a) = 0$, $1 \leq i \leq r$, and $a \neq (0, \ldots, 0)$. A system of homogeneous forms $f_1, \ldots, f_r$ is anisotropic over F if there is no nontrivial common zero of these forms defined over F, and is isotropic over F if there is a nontrivial common zero of these forms over F.

It is of great interest to compute $u_r(F)$ and, if possible, to express $u_r(F)$ in terms of $u(F)$. For example, the following general result is known.

REV. ROUMAINE MATH. PURES APPL. **71** (2026), *1-2*, 31–54
doi: 10.59277/RRMPA.2026.31.54

Proposition 1.1 ([10, Proposition 2.1, Theorem 2.6]). *For any field F and any integer $r \geq 1$, we have*

$$ru(F) \leq u_r(F) \leq \frac{r(r+1)}{2}u(F). \tag{1.1}$$

In particular, for $r = 2$, we have that

$$2u(F) \leq u_2(F) \leq 3u(F). \tag{1.2}$$

If F is a field such that $u(F) = 4$ (thus, any quadratic form over F in at least 5 variables is isotropic), then for $r = 2$, Proposition 1.1 implies that $8 \leq u_2(F) \leq 12$. There are fields with $u(F) = 4$ and $u_2(F) = 12$. See [10, Proposition 3.5].

If F is a p-adic field (defined in Definition 1.11) and $r = 2$, then a better bound than the one in Proposition 1.1 holds because $u(F) = 4$ by [8, Chapter VI, Theorem 2.12, p. 158]) and as mentioned above, in [3] and [2] it was proved that $u_2(F) = 8$.

A p-adic field is an example of a complete discretely valued field (defined in Definition 1.11). Suppose that F is a complete discretely valued field with residue field $\overline{F}$ and assume that $\operatorname{char} F \neq 2$. It is also of great interest to express $u_r(F)$ in terms of $u_r(\overline{F})$. We always have $u_r(F) \geq 2u_r(\overline{F})$ for all $r \geq 1$ by [10, Proposition 3.3]. See also Lemma 2.4 for a proof. If $r = 1$ and $\operatorname{char} \overline{F} \neq 2$, then $u(F) = 2u(\overline{F})$. See [8, Chapter VI, Corollary 1.10, p. 149] for a proof. The same result holds if $r = 1$ and $\operatorname{char} \overline{F} = 2$, but the proof is more difficult. See [8, Chapter VI, Theorem 2.12, p. 158] for the case when $\overline{F}$ is a finite field with $\operatorname{char} \overline{F} = 2$ (that is, when F is a dyadic p-adic field), and [12] and [1] for the case when $\overline{F}$ is arbitrary with $\operatorname{char} \overline{F} = 2$. For the case $r = 1$, we give a simpler proof in Theorem 4.3 that handles both cases for $\operatorname{char} \overline{F}$ at the same time.

The main result in this paper is Theorem 1.2 where the case $r = 2$ is considered. If F is a p-adic field, then it is known that $u(\overline{F}) = 2$ and $u_2(\overline{F}) = 4$. Thus, the result in [3] and [2] for a p-adic field F proves that $u_2(F) = 2u_2(\overline{F}) = 2 \cdot 4 = 8$. In this paper, we extend the theorem in [3] and [2] to the following theorem.

Theorem 1.2 (Main Theorem). *Let F be a complete discretely valued field with* $\operatorname{char} F \neq 2$. *Let $\overline{F}$ be the residue field of F and assume $u(\overline{F}) < \infty$. Then*

$$u_2(F) = 2u_2(\overline{F}). \tag{1.3}$$

Our proof closely follows the ideas in [2] although an important modification of the proof needs to be made at the end. Our proof also includes many details that were left out of the proof in [2]. For example, in Section 5,

we study an invariant of two quadratic forms that was introduced in [2]. The main properties of this important invariant were not proved in [2]. We provide complete proofs in Theorem 5.1. In this paper, we give a careful exposition of the necessary background material in quadratic forms so that, in the end, we have a self-contained exposition of this material.

We now give some definitions, terminology, and concepts that are used in this paper.

Let F be a field and let $f = \sum_{1\le i\le j\le n} a_{ij}X_iX_j \in F[X_1,\dots,X_n]$ be a quadratic form. Let $M_f = (b_{ij})$ denote the $n\times n$ symmetric matrix given by

$$b_{ij} = \begin{cases} 2a_{ii} & \text{if } i = j,\\ a_{ij} & \text{if } i < j, \end{cases} \text{ and } b_{ij} = b_{ji} \text{ if } i > j.$$

Let F^n denote the F-vector space of n-dimensional column vectors. For a column vector $v = (c_1,\dots,c_n)^t \in F^n$, let $f(v) = f(c_1,\dots,c_n)$. The symmetric bilinear form associated to f is

$$B_f : F^n \times F^n \to F$$

given by $B_f(v,w) = f(v+w) - f(v) - f(w)$ for $v,w \in F^n$. It easily follows that $B_f(v,v) = 2f(v)$ for $v \in F^n$ because $f(v+v) = f(2v) = 4f(v)$.

Let $w = (d_1,\dots,d_n)^t \in F^n$. We have $B_f(v,w) = v^tM_fw$ because

$$\begin{aligned} B_f(v,w) &= f(v+w) - f(v) - f(w)\\ &= \sum_{1\le i\le j\le n} a_{ij}(c_i+d_i)(c_j+d_j) - \sum_{1\le i\le j\le n} a_{ij}c_ic_j - \sum_{1\le i\le j\le n} a_{ij}d_id_j\\ &= \sum_{1\le i\le j\le n} a_{ij}(c_id_j + c_jd_i)\\ &= \sum_{i=1}^{n} 2a_{ii}c_id_i + \sum_{1\le i<j\le n} a_{ij}(c_id_j + c_jd_i)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} b_{ij}c_id_j = v^tM_fw. \end{aligned}$$

We let $e_1,\dots,e_n$ denote the standard basis of the vector space F^n over a field F. Note that $B_f(e_i,e_j) = e_i^tM_fe_j = b_{ij}$ for all i,j. Thus if $i<j$, we have $B_f(e_i,e_j) = a_{ij}$. We also have $f(e_i) = a_{ii}$. It follows by induction that

$$\begin{aligned} f(X_1e_1 + \cdots + X_ne_n) &= \sum_{i=1}^{n} f(e_i)X_i^2 + \sum_{1\le i<j\le n} B_f(e_i,e_j)X_iX_j\\ &= \sum_{1\le i\le j\le n} a_{ij}X_iX_j = f. \end{aligned}$$

If $f \in F[X_1, \ldots, X_n]$ is a quadratic form and $T : F^n \to F^n$ is an invertible linear transformation over F, let $f_T(x) = f(Tx)$.

Then $M_{f_T} = T^t M_f T$. If $R : F^n \to F^n$ is another invertible linear transformation over F, then $f_{TR} = (f_T)_R$ because

$$(f_T)_R(X) = f_T(RX) = f(TRX) = f_{TR}(X).$$

Definition 1.3 (Radical of a quadratic form). Let $f \in F[X_1, \ldots, X_n]$ be a quadratic form with associated symmetric bilinear form B_f.

1. The radical of B_f, written $\mathrm{rad}(B_f)$, is defined by
$$\big\{v \in F^n \mid B_f(v, F^n) = 0\big\}.$$

2. The radical of f, written $\mathrm{rad}(f)$, is defined by
$$\big\{v \in F^n \mid B_f(v, F^n) = 0 = f(v)\big\}.$$

Note that $\mathrm{rad}(f) \subseteq \mathrm{rad}(B_f)$. If $\mathrm{char}\, F \neq 2$, then $\mathrm{rad}(f) = \mathrm{rad}(B_f)$ because if $v \in \mathrm{rad}(B_f)$ then $0 = B_f(v, v) = 2f(v)$, and thus $f(v) = 0$. If $\mathrm{char}\, F = 2$ and $v, w \in \mathrm{rad}(f)$, then $f(v + w) = f(v) + f(w) + B_f(v, w) = 0$. It is now straightforward to verify that $\mathrm{rad}(f)$, $\mathrm{rad}(B_f)$ are each subspaces of F^n.

Definition 1.4 (Order of a quadratic form). Let $f \in F[X_1, \ldots, X_n]$ be a quadratic form.

1. The order of f, written $o(f)$, is defined by
$$o(f) = n - \dim\big(\mathrm{rad}(f)\big).$$

2. A form f is degenerate if $o(f) < n$ and nondegenerate if $o(f) = n$.

Definition 1.5 (Radical and order of a pair of quadratic forms). Let $f, g \in F[X_1, \ldots, X_n]$ be quadratic forms.

1. The radical of f, g, written $\mathrm{rad}(f, g)$, is defined by
$$\mathrm{rad}(f, g) = \mathrm{rad}(f) \cap \mathrm{rad}(g).$$

2. The order of f, g, written $o(f, g)$, is defined by
$$o(f, g) = n - \dim\big(\mathrm{rad}(f, g)\big).$$

3. A pair $\{f, g\}$ is degenerate if $o(f, g) < n$, and is nondegenerate if $o(f, g) = n$.

Lemma 1.6. *Let $f, g \in F[X_1, \ldots, X_n]$ be quadratic forms.*

1. *If* $\operatorname{char} F \neq 2$, *then* f *is degenerate if and only if* $\det(M_f) = 0$.

2. *Suppose that* $o(f) = m < n$. *Then there exists an invertible linear transformation* $T : F^n \to F^n$ *such that* $f_T(X) \in F[X_1, \dots, X_m]$, *and* f *is isotropic over* F.

3. *Suppose that* $o(f, g) = m < n$. *Then there exists an invertible linear transformation* $T : F^n \to F^n$ *such that* $f_T(X), g_T(X) \in F[X_1, \dots, X_m]$, *and* f, g *is isotropic over* F.

Proof. (1) Since $\operatorname{char} F \neq 2$, we have $\operatorname{rad}(f) = \operatorname{rad}(B_f)$. Therefore, f is degenerate if and only if $\operatorname{rad}(f) \neq 0$, if and only if $\operatorname{rad}(B_f) \neq 0$. We have $\operatorname{rad}(B_f) \neq 0$ if and only if M_f has rank $< n$, if and only if $\det(M_f) = 0$.

(2) Let $\{w_1, \dots, w_s\}$ be a basis of $\operatorname{rad}(f)$ and let $\{v_1, \dots, v_m, w_1, \dots, w_s\}$ be a basis of F^n, where $m + s = n$. Let $T : F^n \to F^n$ be the invertible linear transformation defined by $T(e_i) = v_i$, $1 \leq i \leq m$, and $T(e_{m+j}) = w_j$ for $1 \leq j \leq s$. Then

$$f_T = f(X_1 v_1 + \cdots + X_m v_m + X_{m+1} w_1 + \cdots + X_n w_s) = f(X_1 v_1 + \cdots + X_m v_m)$$

because $B_f(v_i, w_j) = f(w_j) = 0$ for all i, j. Since $f(w_s) = 0$, f is isotropic over F.

(3) We start with a basis of $\operatorname{rad}(f, g)$ and then the proof is similar to the proof of (2). □

Let F^{alg} denote the algebraic closure of the field F.

Definition 1.7 (Nonsingular zero). Let $f, g \in F[X_1, \dots, X_n]$ be quadratic forms:

1. A vector $v \in F^n$ is a nonsingular zero of f if $f(v) = 0$ and $v \notin \operatorname{rad}(B_f)$, and is a singular zero if $v \in \operatorname{rad}(B_f)$.

2. A vector v is a nonsingular common zero of the pair f, g if $f(v) = g(v) = 0$ and the linear maps $B_f(v, \cdot), B_g(v, \cdot) : F^n \to F$ are linearly independent over F, and is a singular common zero otherwise.

3. We say that f, g is a nonsingular pair of quadratic forms if every nontrivial common zero of f, g defined over F^{alg} is a nonsingular zero.

Lemma 1.8. *Let* $f, g \in F[X_1, \dots, X_n]$ *be quadratic forms:*

1. *A vector* $v \in F^n$ *is a nonsingular zero of* f *if and only if* $f(v) = 0$ *and*

$$\frac{\partial f}{\partial X}(v) = \left(\frac{\partial f}{\partial X_1}(v), \dots, \frac{\partial f}{\partial X_n}(v) \right)$$

is not the zero vector.

2. *A vector v is a nonsingular common zero of f, g if and only if $f(v) = g(v) = 0$ and the vectors*

$$\frac{\partial f}{\partial X}(v),\ \frac{\partial g}{\partial X}(v)$$

are linearly independent over F.

Proof. Suppose that $f = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j$ with each $a_{ij} \in F$. Let $M_f = (b_{ij})$ denote the $n \times n$ symmetric matrix associated to f.

(1) Let $v = c_1 e_1 + \cdots + c_n e_n = (c_1, \ldots, c_n)^t$, where each $c_i \in F$. Since $B_f(e_i, e_j) = b_{ij}$ for all i, j and $b_{ii} = 2a_{ii}$, we have

$$B_f(e_i, v) = e_i^t M_f v = \sum_{j=1}^{n} b_{ij} c_j = \frac{\partial f}{\partial X_i}(v).$$

We have $v \notin \mathrm{rad}(B_f)$ if and only if $B_f(e_i, v) \neq 0$ for some i, if and only if $(\frac{\partial f}{\partial X_1}(v), \ldots, \frac{\partial f}{\partial X_n}(v))$ is not the zero vector.

(2) The linear maps $B_f(v, \cdot), B_g(v, \cdot) : F^n \to F$ are linearly dependent over F if and only if there exist $\lambda, \mu \in F$, not both zero, such that

$$B_{\lambda f + \mu g}(v, \cdot) : F^n \to F$$

is the zero map, if and only if $v \in \mathrm{rad}(B_{\lambda f + \mu g})$, if and only if

$$\lambda \frac{\partial f}{\partial X}(v) + \mu \frac{\partial g}{\partial X}(v) = 0,$$

that is, the vectors $\frac{\partial f}{\partial X}(v)$, $\frac{\partial g}{\partial X}(v)$ are linearly dependent over F. □

We now give the basic terminology of fields with a non-archimedean valuation. Let $\mathbb{Z}$ denote the ring of integers.

Definition 1.9 (Discretely valued field). A field F is a discretely valued field if there is a surjective valuation

$$\nu : F \to \mathbb{Z} \cup \{\infty\}.$$

That is, ν is surjective and

1. $\nu(a) = \infty$ if and only if $a = 0$,
2. $\nu(ab) = \nu(a) + \nu(b)$, for all $a, b \in F$,
3. $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$, for all $a, b \in F$.

We assume that the symbol ∞ satisfies the statements $n < \infty$ for all $n \in \mathbb{Z}$, and $\infty + \infty = \infty + n = \infty$ for all $n \in \mathbb{Z}$.

Definition 1.10 (Valuation ring). Let (F, ν) be a discretely valued field. The valuation ring of F is the subring of F defined by

$$\mathcal{O} = \big\{a \in F : \nu(a) \geq 0\big\}.$$

The valuation ring $\mathcal{O}$ of F has the following properties:

1. The fraction field of $\mathcal{O}$ is F.

2. $\mathcal{O}$ has a unique maximal ideal

$$\mathfrak{m} = \big\{a \in F : \nu(a) \geq 1\big\}$$

that is generated by any element $\pi \in F$ such that $\nu(\pi) = 1$. Such an element π is determined up to multiplication by a unit in $\mathcal{O}$ and is called a uniformizer of $\mathcal{O}$, or of F.

3. The group of units of the valuation ring $\mathcal{O}$ is given by

$$\begin{aligned}\mathcal{O}^\times &= \{a \in \mathcal{O} : a \notin \mathfrak{m}\} \\ &= \{a \in F : \nu(a) = 0\},\end{aligned}$$

and every nonzero element $a \in F$ can be written uniquely in the form

$$a = \mu\pi^{\nu(a)},$$

where $\mu \in \mathcal{O}^\times$ and π is a fixed uniformizer.

4. The valuation ring $\mathcal{O}$ is a principal ideal domain.

5. The field $\overline{F} := \mathcal{O}/\mathfrak{m}$ is called the residue field of $\mathcal{O}$ relative to the valuation ν, and the projection of $\mathcal{O}$ onto $\overline{F}$ is expressed as

$$a \in \mathcal{O} \mapsto \overline{a} = a + \mathfrak{m}.$$

Let (F, ν) be a discretely valued field. For a fixed real number c greater than 1, we define

$$d(a, b) = c^{-\nu(a-b)}, \quad a, b \in F. \tag{1.4}$$

This gives a metric on F relative to the discrete valuation ν. Any two real numbers c, c' greater than one induce the same metric topology.

Definition 1.11 (Complete discretely valued field). The pair (F, ν) is a complete discretely valued field if F is complete with respect to ν. That is, every Cauchy sequence in F converges to an element in F with respect to the metric defined in (1.4).

A p-adic field is a complete discretely valued field whose residue field is a finite field.

Definition 1.12. A function $U : \mathcal{O}^n \to \mathcal{O}^n$ is a unimodular transformation if U is an $\mathcal{O}$-module isomorphism, which is the same as requiring that $\det(U) \in \mathcal{O}^\times$.

A unimodular transformation $U : \mathcal{O}^n \to \mathcal{O}^n$ extends uniquely to an invertible linear transformation $F^n \to F^n$.

For any invertible linear transformation $S : \overline{F}^n \to \overline{F}^n$ there is a unimodular transformation $U : \mathcal{O}^n \to \mathcal{O}^n$ such that $\overline{U} = S$. The existence of such a linear transformation U is straightforward. Since

$$\overline{\det(U)} = \det(\overline{U}) = \det(S) \neq 0$$

in $\overline{F}$, it follows that $\det(U) \in \mathcal{O}^\times$ and thus U is a unimodular transformation.

Examples. Let R be a principal ideal domain and let K be its field of fractions. Let π be a prime element of R. Every nonzero element $a \in R$ can be written $a = \pi^m b$ where $m \in \mathbb{Z}_{\geq 0}$, $b \in R$, and $\pi \nmid b$ in R. Then every nonzero element $a \in K$ can be written $a = \pi^m \cdot \frac{b}{c}$ where $m \in \mathbb{Z}$ is uniquely determined, $b, c \in R$, and $\pi \nmid bc$. Define $\nu : K \to \mathbb{Z} \cup \{\infty\}$ by $\nu(0) = \infty$ and $\nu(a) = m$. Then ν is a discrete valuation on K with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m} = (\pi)$. The valuation ring $\mathcal{O}$ of (K, ν) is the localization of R at the maximal ideal $\mathfrak{m}$. Let F be the completion of K with respect to the metric d induced by ν. The valuation $\nu : K \to \mathbb{Z} \cup \{\infty\}$ extends to a discrete valuation $\nu : F \to \mathbb{Z} \cup \{\infty\}$ and thus the metric d also extends to a metric on F.

More generally, let R be a Dedekind domain with field of fractions K and let P be a nonzero prime ideal of R. For any nonzero $a \in R$, we can write the ideal $(a) = P^m I$ where I is an ideal in R with $m \in \mathbb{Z}_{\geq 0}$ and $P \nmid I$. This gives a valuation $\nu : R \to \mathbb{Z} \cup \{\infty\}$ where $\nu(a) = m$. This valuation extends to a valuation $\nu : K \to \mathbb{Z} \cup \{\infty\}$. The localization of R at P, R_P, is the valuation ring $\mathcal{O}$.

Let k be a field, let $R = k[t]$, and let $K = k(t)$ be the field of fractions of R. Then R is a principal ideal domain. Let $\pi = t$. The completion F of K is denoted by $k((t))$, and its valuation ring is denoted by $k[[t]]$, the ring of formal power series with coefficients in k. The residue field $\overline{F}$ of F is $k[[t]]/(t) \cong k$. In this case, we have $\operatorname{char} F = \operatorname{char} \overline{F}$.

Let $\mathbb{Z}$ be the ring of integers with field of fractions $\mathbb{Q}$. Let p be a prime number. The completion of $\mathbb{Q}$ with respect to the valuation determined by p as above is denoted by $\mathbb{Q}_p$ and its valuation ring is denoted by $\mathbb{Z}_p$. The residue field of $(\mathbb{Q}_p, \nu)$ is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, the finite field with p elements. In this case, we have $\operatorname{char} F \neq \operatorname{char} \overline{F}$.

2. PRELIMINARY RESULTS

LEMMA 2.1 ([2, Lemma 1]). *Let $f \in F[X_1, \ldots, X_n]$ be a quadratic form that has a nonsingular zero in F^n. Then the set of nonsingular zeros of f in F^n does not lie in a proper linear subspace of F^n.*

Proof. Let W be a linear subspace of F^n such that $\dim(W) = n-1$. We show that f has a nonsingular zero $v \in F^n$ with $v \notin W$. There exists a nonzero linear form $M(X_1, \ldots, X_n) = \sum_{i=1}^n c_i X_i$ with each $c_i \in F$ such that

$$W = \big\{(x_1, \ldots, x_n) \in F^n \mid M(x_1, \ldots, x_n) = 0\big\}.$$

By hypothesis, f has a nonsingular zero in F^n, which, after an invertible linear transformation, we may assume is $e_1 = (1, 0, \ldots, 0)$. Then f can be written in the form

$$f = X_1 L(X_2, \ldots, X_n) + q(X_2, \ldots, X_n),$$

where $n \geq 2$ and $L(X_2, \ldots, X_n) = \sum_{i=2}^n b_i X_i$ with each $b_i \in F$. If $L = 0$, then $f = q(X_2, \ldots, X_n)$ and e_1 would be a singular zero. Thus $L \neq 0$ and some $b_i \neq 0$.

If $e_1 \notin W$, then the proof is finished. Suppose that $e_1 \in W$. Then $c_1 = 0$, and $M(X_1, \ldots, X_n) = M(0, X_2, \ldots, X_n)$. We show at the end that there exist $d_i \in F$, $2 \leq i \leq n$, such that $L(d_2, \ldots, d_n) \neq 0$ and $M(0, d_2, \ldots, d_n) \neq 0$.

Let

$$v = \left(\frac{-q(d_2, \ldots, d_n)}{L(d_2, \ldots, d_n)}, d_2, \ldots, d_n\right).$$

Then $f(v) = 0$ and $\frac{\partial f}{\partial x_1}(v) = L(d_2, \ldots, d_n) \neq 0$, showing that v is a nonsingular zero of f such that $M(v) = M(0, d_2, \ldots, d_n) \neq 0$. Thus $v \notin W$.

We now show that there exist $d_i \in F$, $2 \leq i \leq n$, such that $\sum_{i=2}^n b_i d_i \neq 0$ and $\sum_{i=2}^n c_i d_i \neq 0$. Let $w = (b_2, \ldots, b_n)$ and $y = (c_2, \ldots, c_n)$. Then w and y are each nonzero. If w, y are linearly dependent, then find $d_i \in F$ such that $\sum_{i=2}^n b_i d_i = 1$. Since w, y are linearly dependent and $y \neq 0$, it follows that $\sum_{i=2}^n c_i d_i \neq 0$. If w, y are linearly independent, then $n \geq 3$ and it follows from linear algebra that we can solve over F the system of linear equations

$$\sum_{i=2}^n b_i X_i = \sum_{i=2}^n c_i X_i = 1. \qquad \square$$

LEMMA 2.2. *Let F be a field and let $f \in F[X_1, \ldots, X_n]$ be a quadratic form such that $o(f) \geq u(F) + 1$. Then f has a nonsingular zero in F^n.*

Proof. There exists an invertible linear transformation of F^n, letting us assume that $f \in F[X_1, \ldots, X_m]$ where $m = o(f)$. Then f has a nontrivial zero

in F^m because $m \geq u(F)+1$. After an invertible linear transformation of F^m, we can assume that $f(e_1) = 0$. Then f can be written as

$$f = X_1 L(X_2, \ldots, X_m) + q(X_2, \ldots, X_m),$$

where L is a linear form and q is a quadratic form, each with coefficients in F. The linear form $L = c_2X_2 + \cdots + c_mX_m \neq 0$ because $o(f) = m$. We can assume that $c_2 \neq 0$. Then e_1 is a nonsingular zero of f because $\frac{\partial f}{\partial X_2}(e_1) = c_2 \neq 0$. □

LEMMA 2.3. *Let $f, g \in F[X_1, \ldots, X_n]$ be quadratic forms and assume that $o(f, g) \geq u_2(F)+1$ and $o(h) \geq u(F)+1$ for every $h = \lambda f + \mu g$ where $\lambda, \mu \in F$, not both zero. Then f, g have a nonsingular zero in F^n.*

Proof. By Lemma 1.6 (3), there exists an invertible linear transformation of F^n letting us assume that $f, g \in F[X_1, \ldots, X_m]$ where $m = o(f, g)$. Then f, g have a nontrivial common zero in F^m because $m \geq u_2(F) + 1$. After an invertible linear transformation of F^m, we assume that $f(e_1) = g(e_1) = 0$. Then f, g can be written as

$$f = X_1 L(X_2, \ldots, X_m) + q_1(X_2, \ldots, X_m),$$

$$g = X_1 M(X_2, \ldots, X_m) + q_2(X_2, \ldots, X_m),$$

where L, M are linear forms and q_1, q_2 are quadratic forms, each with coefficients in F.

The linear forms L, M are not both zero because $o(f, g) = m$. We can assume that $L \neq 0$. If L, M are linearly independent, then e_1 is a nonsingular zero of f, g. Suppose that L, M are linearly dependent. Then there exist $\lambda, \mu \in F$, not both zero, such that $\lambda L + \mu M = 0$. Then $\mu \neq 0$. Let $h = \lambda f + \mu g$. Then $h = h(X_2, \ldots, X_m) = \lambda q_1 + \mu q_2$.

The hypothesis implies that $o(h) \geq u(F) + 1$ and thus h has a nonsingular zero $(a_2, \ldots, a_m) \in F^m$ such that $L(a_2, \ldots, a_m) \neq 0$ by Lemma 2.2 and Lemma 2.1. Let

$$a_1 = \frac{-q_1(a_2, \ldots, a_m)}{L(a_2, \ldots, a_m)}.$$

Then $v := (a_1, \ldots, a_m)$ is a nonsingular zero of f, h because $\frac{\partial f}{\partial X}(v), \frac{\partial h}{\partial X}(v)$ are linearly independent. (Note that $\frac{\partial f}{\partial X_1}(v) = L(a_2, \ldots, a_m) \neq 0$, $\frac{\partial h}{\partial X_1}(v) = 0$, and $\frac{\partial h}{\partial X_i}(v) \neq 0$ for some $i \geq 2$.) Thus v is also a nonsingular zero of f, g because $\mu \neq 0$. □

We need the following result only for $r = 1, 2$. We prove the result for all $r \geq 1$ as it hardly requires any extra work.

LEMMA 2.4 ([10, Proposition 3.3]). *Let $(F, \nu, \mathcal{O}, \mathfrak{m}, \pi, \overline{F})$ be a discretely valued field with residue field $\overline{F}$. Then $u_r(F) \geq 2u_r(\overline{F})$ for all $r \geq 1$.*

Proof. Let $f_1, \dots, f_r \in \mathcal{O}[X_1, \dots, X_n]$ be a system of quadratic forms such that $\overline{f_1}, \dots, \overline{f_r}$ is an anisotropic system over $\overline{F}$. Let

$$g_i = f_i(X_1, \dots, X_n) + \pi f_i(X_{n+1}, \dots, X_{2n}),$$

where $1 \le i \le r$. Then $g_1, \dots, g_r$ is a system of r quadratic forms in $2n$ variables with coefficients in F. We show that $g_1, \dots, g_r$ is an anisotropic system of quadratic forms defined over F. This shows that $u_r(F) \ge 2u_r(\overline{F})$.

Suppose that $g_i(a_1, \dots, a_{2n}) = 0$, $1 \le i \le r$, and each $a_j \in F$, not all zero. We can multiply each a_j by an appropriate nonzero element in F so that we can assume each $a_j \in \mathcal{O}$ with $\pi \nmid a_j$ for at least one j. This gives $f_i(a_1, \dots, a_n) \equiv g_i(a_1, \dots, a_{2n}) \equiv 0 \bmod \pi$, $1 \le i \le r$. Since $\overline{f_1}, \dots, \overline{f_r}$ is an anisotropic system over $\overline{F}$, it follows that $\overline{a_j} = 0$, $1 \le j \le n$, which implies that $\pi \mid a_j$, $1 \le j \le n$. Then $\pi^2 \mid f_i(a_1, \dots, a_n) = -\pi f_i(a_{n+1}, \dots, a_{2n})$, $1 \le i \le r$. Thus $\pi \mid f_i(a_{n+1}, \dots, a_{2n})$, $1 \le i \le r$. For the same reason, it follows that $\pi \mid a_j$, $n+1 \le j \le 2n$, a contradiction. □

3. HENSEL'S LEMMA FOR ONE AND TWO QUADRATIC FORMS

In this section, we prove Hensel's lemma for one quadratic form and a pair of quadratic forms. We give a detailed proof for a pair of quadratic forms in Lemma 3.2. The proof for one quadratic form is easier and involves only a part of the proof of Lemma 3.2.

Suppose that (F, ν) is a complete discretely valued field. If

$$f = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j$$

is a quadratic form with coefficients $a_{ij} \in \mathcal{O}$, then

$$\bar{f} = \sum_{1 \le i \le j \le n} (a_{ij} + \mathfrak{m}) X_i X_j$$

is a quadratic form with coefficients $a_{ij} + \mathfrak{m} \in \overline{F}$.

Definition 3.1 (Primitive vector). We say that a vector $(a_1, \dots, a_n) \in \mathcal{O}^n$ is primitive if there exists at least one i such that $a_i \in \mathcal{O}^\times$.

Lemma 3.2. *Let $(F, \nu, \mathcal{O}, \mathfrak{m}, \pi, \overline{F})$ be a complete discretely valued field. Let $f, g \in \mathcal{O}[X_1, \dots, X_n]$ be quadratic forms. If $\bar{f}, \bar{g}$ have a nonsingular common zero in the residue field $\overline{F}$, then f, g have a common primitive zero in $\mathcal{O}$.*

Proof. For $\ell \ge 1$, we construct a sequence $(v^{(\ell)})$ of primitive vectors in $\mathcal{O}^n$ such that

(i) $f(v^{(\ell)}) \equiv g(v^{(\ell)}) \equiv 0 \mod \mathfrak{m}^{\ell}$;

(ii) $v^{(\ell)} \equiv v^{(\ell-1)} \mod \mathfrak{m}^{\ell-1}$.

Condition (ii) implies that the sequence is a Cauchy sequence in $\mathcal{O}^n$. Since $\mathcal{O}$ is complete, this sequence converges in $\mathcal{O}^n$. Let $v = \lim_{\ell\to\infty} v^{(\ell)}$. Since $v^{(1)}$ is a primitive vector, condition (ii) implies that v is a primitive vector in $\mathcal{O}^n$. Since f, g are continuous over $\mathcal{O}$, condition (i) implies that

$$f(v) = f(\lim_{\ell\to\infty} v^{(\ell)}) = \lim_{\ell\to\infty} f(v^{(\ell)}) = 0.$$

Similarly, $g(v) = 0$. We now construct such a sequence. The hypothesis implies that there exists a primitive vector $v^{(1)} \in \mathcal{O}^n$ such that $\overline{v^{(1)}}$ is a nonsingular common zero of $\bar{f}$ and $\bar{g}$ in $\overline{F}$. Thus, condition (i) is satisfied for $\ell = 1$ and condition (ii) is satisfied vacuously for $\ell = 1$. Suppose that $\ell \geq 1$ and that we have constructed $v^{(\ell)}$ satisfying conditions (i) and (ii). To construct $v^{(\ell+1)}$, we find $w = (b_1, \ldots, b_n) \in \mathcal{O}^n$ such that

$$v^{(\ell+1)} = v^{(\ell)} + \pi^{\ell} w.$$

Then,

$$f(v^{(\ell+1)}) = f(v^{(\ell)} + \pi^{\ell} w) \equiv f(v^{(\ell)}) + \pi^{\ell}\left(\sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(v^{(\ell)}) \cdot b_j\right) \mod \mathfrak{m}^{\ell+1},$$

with a similar equation for g. We want to choose w such that

$$f(v^{(\ell+1)}) \equiv g(v^{(\ell+1)}) \equiv 0 \mod \mathfrak{m}^{\ell+1}.$$

Condition (i) implies that π^{ℓ} divides

$$f(v^{(\ell)}) + \pi^{\ell}\left(\sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(v^{(\ell)}) \cdot b_j\right),$$

and similarly for g. Thus, we want to choose $w \in \mathcal{O}^n$ such that

$$\pi^{-\ell} f(v^{(\ell)}) + \left(\sum_{j=1}^{n} \frac{\partial f}{\partial X_j}(v^{(\ell)}) \cdot b_j\right) \equiv 0 \mod \mathfrak{m},$$

and

$$\pi^{-\ell} g(v^{(\ell)}) + \left(\sum_{j=1}^{n} \frac{\partial g}{\partial X_j}(v^{(\ell)}) \cdot b_j\right) \equiv 0 \mod \mathfrak{m}.$$

This is a system of two linear equations over $\overline{F}$ in the variables $b_1, \ldots, b_n$ whose coefficient matrix over $\overline{F}$ is given by

$$\begin{pmatrix} \frac{\partial \bar{f}}{\partial X_1}(\overline{v^{(\ell)}}) & \cdots & \frac{\partial \bar{f}}{\partial X_n}(\overline{v^{(\ell)}}) \\ \\ \frac{\partial \bar{g}}{\partial X_1}(\overline{v^{(\ell)}}) & \cdots & \frac{\partial \bar{g}}{\partial X_n}(\overline{v^{(\ell)}}) \end{pmatrix}. \tag{3.1}$$

Since $\overline{v^{(1)}}$ is a nonsingular common zero of $\bar{f}, \bar{g}$ over $\overline{F}$ and $v^{(\ell)} \equiv v^{(1)} \mod \pi$, we have

$$\frac{\partial f}{\partial X_j}(v^{(\ell)}) \equiv \frac{\partial f}{\partial X_j}(v^{(1)}) \mod \mathfrak{m}$$

and

$$\frac{\partial g}{\partial X_j}(v^{(\ell)}) \equiv \frac{\partial g}{\partial X_j}(v^{(1)}) \mod \mathfrak{m},$$

and thus $\overline{v^{(\ell)}}$ is also a nonsingular zero of $\bar{f}, \bar{g}$. Hence the vectors $\frac{\partial \overline{f}}{\partial X}(\overline{v^{(\ell)}})$, $\frac{\partial \overline{g}}{\partial X}(\overline{v^{(\ell)}})$ are linearly independent over $\overline{F}$.

Thus the matrix in (3.1) has rank 2, and so the system of two linear equations has at least one solution in $\overline{F}^n$. Hence, we can choose $w \in \mathcal{O}^n$ to be any inverse image of that solution. This completes the proof of the lemma. □

By restricting to one of the quadratic forms in the proof of Lemma 3.2, a similar proof gives the following result for one quadratic form.

LEMMA 3.3. *Let $(F, \nu, \mathcal{O}, \mathfrak{m}, \pi, \overline{F})$ be a complete discretely valued field. Let $f \in \mathcal{O}[X_1, \ldots, X_n]$ be a quadratic form. If $\bar{f}$ has a nonsingular zero in the residue field $\overline{F}$, then f has a primitive zero in $\mathcal{O}^n$.*

4. ONE QUADRATIC FORM

It was stated in the Introduction that if $\operatorname{char} F \neq 2$ and F is a complete discretely valued field with residue field $\overline{F}$, then $u(F) = 2u(\overline{F})$. If $\operatorname{char} \overline{F} \neq 2$, this is relatively easy to prove and a proof appears in [8], as already noted. The case when $\operatorname{char} \overline{F} = 2$ has traditionally been considered much more difficult to prove. When $\overline{F}$ is a finite field with $\operatorname{char} \overline{F} = 2$, then a somewhat complicated proof is given in [8, Chapter 6]. We give a much easier proof in this section when $\operatorname{char}(F) \neq 2$ and $\overline{F}$ is arbitrary. If $\operatorname{char} F = 2$, then more work is required. See references [1] and [11].

LEMMA 4.1. *Let F be a field and let $f \in F[X_1, \ldots, X_n]$ be a quadratic form. Let $\mathscr{I}(f) = \det(M_f)$ where M_f is the symmetric matrix associated with the quadratic form f. Then $\mathscr{I}(f)$ is a polynomial in the coefficients of f such that for $a \in F$ and an invertible linear transformation $T : F^n \to F^n$,*

$$\mathscr{I}(af_T) = a^n \det(T)^2 \mathscr{I}(f).$$

If F is a discretely valued field and $f \in \mathcal{O}[X_1, \ldots, X_n]$, then $\mathscr{I}(f) \in \mathcal{O}$.

Proof. It is clear that $\mathscr{I}(f)$ is a polynomial in the coefficients of f, and

$$\mathscr{I}(af_T) = \det(M_{af_T}) = \det(aM_{f_T}) = a^n \det(T^t M_f T)$$

$$= a^n \det(T)^2 \det(M_f) = a^n \det(T)^2 \mathscr{I}(f).$$

The last statement of Lemma 4.1 holds because $\mathscr{I}(f)$ is a polynomial in the coefficients of f. $\square$

LEMMA 4.2. *Let F be a field with* $\operatorname{char} F \neq 2$ *and let $f \in F[X_1, \ldots, X_n]$ be a quadratic form. Then, the following statements hold:*

1. *$\mathscr{I}(f) = 0$ if and only if f is degenerate.*

2. *If f is degenerate, then f has a nontrivial zero in F^n.*

Proof. We have that $\mathscr{I}(f) = 0$ if and only if $\det(M_f) = 0$, if and only if f is degenerate, by Lemma 1.6 (1). If f is degenerate, then f has a nontrivial zero in F^n by Lemma 1.6 (2). $\square$

THEOREM 4.3. *Let $(F, \nu, \mathcal{O}, \mathfrak{m}, \pi, \overline{F})$ be a complete discretely valued field with* $\operatorname{char} F \neq 2$. *Then $u(F) = 2u(\overline{F})$.*

Proof. We have $u(F) \geq 2u(\overline{F})$ by Lemma 2.4. We now prove that $u(F) \leq 2u(\overline{F})$.

Let $f \in F[X_1, \ldots, X_n]$ be a quadratic form with $n \geq 2u(\overline{F}) + 1$. If $\mathscr{I}(f) = 0$, then since $\operatorname{char} F \neq 2$, Lemma 4.2 implies that f has a nontrivial zero in F^n. Now assume that $\mathscr{I}(f) \neq 0$. Since F is the fraction field of $\mathcal{O}$, without loss of generality, we may assume that $f \in \mathcal{O}[X_1, \ldots, X_n]$ and hence $\mathscr{I}(f) \in \mathcal{O}$ by Lemma 4.1. Define

$$A := \left\{ f' = a f_T \;\middle|\; \begin{array}{c} f' \in \mathcal{O}[X_1, \ldots, X_n] \\ T : F^n \to F^n \text{ is an invertible linear transformation,} \\ a \in F \text{ with } a \neq 0 \end{array} \right\}.$$

Certainly, A is nonempty because $f \in A$ (with $a = 1$ and T equal to the identity transformation). Lemma 4.1 implies that $\mathscr{I}(f') \in \mathcal{O}$ and $\mathscr{I}(f') \neq 0$ for any $f' \in A$. For any $f' \in A$, f' is isotropic over F if and only if f is isotropic over F. Since $\nu[\mathscr{I}(f')] \geq 0$ when $f' \in A$, there exists $f' \in A$ for which $\nu[\mathscr{I}(f')]$ is minimal. Assume without loss of generality that $f \in A$ is such that $\nu[\mathscr{I}(f)]$ is minimal.

We now show that $o(\bar{f}) \geq u(\overline{F}) + 1$. Let $o(\bar{f}) = m$. By Lemma 1.6 (2), there is an invertible linear map $S : \overline{F}^n \to \overline{F}^n$ such that $\overline{f}_S \in \overline{F}[X_1, \ldots, X_m]$. As pointed out in a comment after Definition 1.12, S lifts to a unimodular map $U : \mathcal{O}^n \to \mathcal{O}^n$. Since $\overline{U} = S$, we have $\overline{f_U} = \overline{f}_S \in \overline{F}[X_1, \ldots X_m]$. It follows that

$$f_U(X_1, \ldots, X_n) = f_1(X_1, \ldots, X_m) + \pi f_2(X_1, \ldots, X_n),$$

where $f_1, f_2 \in \mathcal{O}[X_1, \ldots, X_n]$ are quadratic forms.

Define a linear transformation $R : F^n \to F^n$ by

$$\begin{aligned} e_i &\mapsto \pi e_i, \quad 1 \le i \le m \\ e_i &\mapsto e_i, \quad m < i \le n. \end{aligned}$$

Then

$$\begin{aligned} f_{UR}(X_1, \dots, X_n) &= f_1(\pi X_1, \dots, \pi X_m) + \pi f_2(\pi X_1, \dots, \pi X_m, X_{m+1}, \dots, X_n) \\ &= \pi^2 f_1(X_1, \dots, X_m) + \pi f_2(\pi X_1, \dots, \pi X_m, X_{m+1}, \dots, X_n). \end{aligned}$$

Then $UR : F^n \to F^n$ is an invertible linear transformation and $\pi^{-1} f_{UR} \in A$. Since $\det(U) \in \mathcal{O}^\times$ and $\det(R) = \pi^m$, minimality of $\nu[\mathscr{I}(f)]$ implies that

$$\begin{aligned} \nu\big[\mathscr{I}(\pi^{-1} f_{UR})\big] &= \nu\big[(\pi^{-1})^n (\det(UR))^2 \mathscr{I}(f)\big] \\ &= -n + 2m + \nu\big[\mathscr{I}(f)\big] \\ &\ge \nu\big[\mathscr{I}(f)\big]. \end{aligned}$$

Thus $2m - n \ge 0$, which implies that

$$2m \ge n \ge 2u(\overline{F}) + 1.$$

Since m is an integer, we have that $o(\bar{f}) = m \ge u(\overline{F}) + 1$. Lemma 2.2 implies that $\bar{f}$ has a nonsingular zero over $\overline{F}$. Then Lemma 3.3 implies that f has a primitive zero in $\mathcal{O}^n$. $\square$

5. AN INVARIANT OF TWO QUADRATIC FORMS

Let R be an integral domain and let F be its fraction field. Assume that $\operatorname{char} F \ne 2$. In this section, we define an invariant $\mathscr{I}(f, g)$ associated to a pair of quadratic forms $f, g \in F[X_1, \dots, X_n]$.

Let $f, g \in F[X_1, \dots, X_n]$ be quadratic forms, and let M_f, M_g be the symmetric matrices associated with the forms f, g, respectively. For variables X, Y, let

$$P(X, Y) = \det(XM_g - YM_f).$$

If $P(X, Y) \ne 0$, then $P(X, Y)$ is a homogeneous polynomial of degree n, so

$$P(X, Y) = \prod_{i=1}^{n} (\lambda_i X - \mu_i Y),$$

where $\lambda_i, \mu_i \in F^{\mathrm{alg}}$ and $(\lambda_i, \mu_i) \ne (0, 0)$, $1 \le i \le n$.

By unique factorization in $F^{\mathrm{alg}}[X, Y]$, the linear factors $\lambda_i X - \mu_i Y$ are uniquely determined up to multiplication by a nonzero element in F^{alg}.

If $P(X,Y)$ is identically zero, then we define $\mathscr{I}(f,g)=0$. If $P(X,Y)$ is not identically zero, then we define

$$\mathscr{I}(f,g)=\prod_{1\le i<j\le n}(\lambda_i\mu_j-\lambda_j\mu_i)^2. \tag{5.1}$$

We now show that this expression is well defined. Suppose that (λ_i,μ_i) is replaced by $(c_i\lambda_i,c_i\mu_i)$ where $c_i\in F^{\text{alg}}$ is nonzero, $1\le i\le n$, and $\prod_{i=1}^n c_i=1$. Then

$$\begin{aligned}\prod_{1\le i<j\le n}\big((c_i\lambda_i)(c_j\mu_j)-(c_j\lambda_j)(c_i\mu_i)\big)^2&=\prod_{1\le i<j\le n}(c_ic_j)^2\prod_{1\le i<j\le n}(\lambda_i\mu_j-\lambda_j\mu_i)^2\\&=\prod_{i=1}^n c_i^{2(n-1)}\prod_{1\le i<j\le n}(\lambda_i\mu_j-\lambda_j\mu_i)^2\\&=\prod_{1\le i<j\le n}(\lambda_i\mu_j-\lambda_j\mu_i)^2.\end{aligned}$$

A version of the following theorem was stated without proof in [2].

THEOREM 5.1. *Let $f,g\in F[X_1,\dots,X_n]$ be quadratic forms. Then the following statements about $\mathscr{I}(f,g)$ hold:*

1. *If $a,b,c,d\in F$ and $T:F^n\to F^n$ is an an invertible linear transformation, then*

$$\mathscr{I}(af_T+bg_T,cf_T+dg_T)=(ad-bc)^{n(n-1)}\det(T)^{4(n-1)}\mathscr{I}(f,g).$$

2. *If $f,g\in R[X_1,\dots,X_n]$, then $\mathscr{I}(f,g)\in R$.*

3. *Suppose that $f=\sum_{1\le i\le j\le n}a_{ij}X_iX_j$ and $g=\sum_{1\le i\le j\le n}b_{ij}X_iX_j$. Let*

$$\hat{f}=\sum_{1\le i\le j\le n}t_{ij}X_iX_j,\ \ \hat{g}=\sum_{1\le i\le j\le n}t'_{ij}X_iX_j,$$

where $\{t_{ij}\}$ and $\{t'_{ij}\}$ are variables (algebraically independent elements). Let $h=\mathscr{I}(\hat{f},\hat{g})\in\mathbb{Z}[\{t_{ij}\},\{t'_{ij}\}]$, by (2).

Then $\mathscr{I}(f,g)=h(\{a_{ij},\},\{b_{ij}\})$. In particular, $\mathscr{I}(f,g)$ is a homogeneous polynomial of degree $2n(n-1)$ in the coefficients of f and g.

Proof. (1) First we show that $\mathscr{I}(f_T,g_T)=\det(T)^{4(n-1)}\mathscr{I}(f,g)$.

$$\begin{aligned}\det(XM_{g_T}-YM_{f_T})&=\det(XT^tM_gT-YT^tM_fT)=\det\big(T^t(XM_g-YM_f)T\big)\\&=\det(T)^2\det(XM_g-YM_f)=\det(T)^2P(X,Y)\\&=\det(T)^2\prod_{i=1}^n(\lambda_iX-\mu_iY).\end{aligned}$$

To compute $\mathscr{I}(f_T, g_T)$, we replace λ_1 with $\lambda_1' = \det(T)^2\lambda_1$ and μ_1 with $\mu_1' = \det(T)^2\mu_1$. Since $\lambda_1'\mu_j - \lambda_j\mu_1' = \det(T)^2(\lambda_1\mu_j - \lambda_j\mu_1)$, this gives

$$\mathscr{I}(f_T, g_T) = \det(T)^{4(n-1)}\mathscr{I}(f, g).$$

We now show that

$$\mathscr{I}(af + bg, cf + dg) = (ad - bc)^{n(n-1)}\mathscr{I}(f, g)$$

for $a, b, c, d \in F$.

$$\begin{aligned}\det(XM_{cf+dg} - YM_{af+bg}) &= \det\big(X(cM_f + dM_g) - Y(aM_f + bM_g)\big)\\ &= \det\big((cX - aY)M_f - (-dX + bY)M_g\big)\\ &= \prod_{i=1}^{n}\big(\lambda_i(cX - aY) - \mu_i(-dX + bY)\big)\\ &= \prod_{i=1}^{n}\big((c\lambda_i + d\mu_i)X - (a\lambda_i + b\mu_i)Y\big).\end{aligned}$$

This gives

$$\begin{aligned}&\mathscr{I}(af + bg, cf + dg)\\ &\quad= \prod_{1\le i<j\le n}\big((c\lambda_i + d\mu_i)(a\lambda_j + b\mu_j) - (c\lambda_j + d\mu_j)(a\lambda_i + b\mu_i)\big)^2\\ &\quad= \prod_{1\le i<j\le n}\big(-(ad - bc)(\lambda_i\mu_j - \lambda_j\mu_i)\big)^2 = \prod_{1\le i<j\le n}(ad - bc)^2(\lambda_i\mu_j - \lambda_j\mu_i)^2\\ &\quad= (ad - bc)^{n(n-1)}\mathscr{I}(f, g).\end{aligned}$$

(2) Suppose that $f, g \in R[X_1, \dots, X_n]$. Then $P(X, Y) \in R[X, Y]$. If $P(X, Y) = 0$, then $\mathscr{I}(f, g) = 0 \in R$. Now assume that $P(X, Y) \neq 0$. Then

$$P(X, Y) = \prod_{i=1}^{n}(\lambda_i X - \mu_i Y) \in R[X, Y]$$

is a homogeneous polynomial of degree n with $\lambda_i, \mu_i \in F^{\mathrm{alg}}$ and $(\lambda_i, \mu_i) \neq (0, 0)$, $1 \le i \le n$.

If either λ_i is zero for more than one i or μ_i is zero for more than one i, then (5.1) implies that $\mathscr{I}(f, g) = 0$. Thus, without loss of generality, we may assume that at least $n - 1$ λ_i's and at least $n - 1$ μ_i's are nonzero.

Case 1: Suppose that λ_i is nonzero for each i, $1 \le i \le n$. We have

$$P(X, Y) = \prod_{i=1}^{n}(\lambda_i X - \mu_i Y).$$

Let $t_i = \dfrac{\mu_i}{\lambda_i}$ and let $\alpha_n = \prod_{i=1}^{n} \lambda_i \in R$. Then $\alpha_n \neq 0$. Let

$$p(X) = P(X,1) = \prod_{i=1}^{n}(\lambda_i X - \mu_i) = \alpha_n X^n + \cdots + \alpha_0 = \alpha_n \prod_{i=1}^{n}(X - t_i).$$

Then $p(X) \in R[X]$ is polynomial of degree n. Let $p'(X) = \sum_{i=0}^{n-1} \beta_i X^i \in R[X]$ denote the derivative of p with respect to X. By [9, Proposition 8.5, p. 204], the resultant of p, p' is

$$\operatorname{Res}(p,p') = (-1)^{n(n-1)/2}\alpha_n D\big(p(X)\big), \tag{5.2}$$

where

$$D\big(p(X)\big) = \alpha_n^{2n-2} \prod_{1\le i<j\le n} (t_i - t_j)^2. \tag{5.3}$$

By the definition of the resultant in [9, p. 200], $\operatorname{Res}(p,p')$ is the determinant of the $(2n-1)\times(2n-1)$ matrix A_{2n-1} (5.4) whose entries are determined by the coefficients of p and p'. This implies that $\operatorname{Res}(p,p') \in R$.

(5.4)

$$A_{2n-1} = \begin{pmatrix}
\alpha_n & \alpha_{n-1} & \dots & \alpha_0 & & & & \\
 & \alpha_n & \alpha_{n-1} & \dots & \alpha_0 & & & \\
 & & & & \dots & & & \\
 & & & & \alpha_n & \alpha_{n-1} & \dots & \alpha_0 \\
\beta_{n-1} & \beta_{n-2} & \dots & \beta_0 & & & & \\
 & \beta_{n-1} & \beta_{n-2} & \dots & \beta_0 & & & \\
 & & & & \dots & & & \\
 & & & & \beta_{n-1} & \beta_{n-2} & \dots & \beta_0
\end{pmatrix}.$$

The first $n-1$ rows of the matrix A_{2n-1} in (5.4) involve α's, the last n rows involve β's, and the blank spaces are filled with zeros. Note that the first column of A_{2n-1} is divisible by α_n in R because $\beta_{n-1} = n\alpha_n$. Therefore, $\operatorname{Res}(p,p')$ is also divisible by α_n in R. Using (5.3) and (5.2), this implies that

$$\alpha_n^{2n-2} \prod_{1\le i<j\le n} (t_i - t_j)^2 = D\big(p(X)\big) = (-1)^{n(n-1)/2}\alpha_n^{-1} \operatorname{Res}(p,p') \in R.$$

Next, since $\alpha_n = \prod_{i=1}^{n} \lambda_i$ we note that

$$\begin{aligned}
\alpha_n^{2n-2} \prod_{1\le i<j\le n} (t_i - t_j)^2 &= \left(\prod_{i=1}^{n} \lambda_i\right)^{2n-2} \prod_{1\le i<j\le n} \left(\frac{\mu_i}{\lambda_i} - \frac{\mu_j}{\lambda_j}\right)^2 \\
&= \left(\prod_{1\le i<j\le n} \lambda_i\lambda_j\right)^{2} \prod_{1\le i<j\le n} \left(\frac{\mu_i}{\lambda_i} - \frac{\mu_j}{\lambda_j}\right)^2
\end{aligned}$$

$$= \prod_{1\le i<j\le n} (\lambda_i\mu_j - \lambda_j\mu_i)^2 = \mathscr{I}(f,g).$$

Therefore, $\mathscr{I}(f,g) \in R$.

Case 2: Suppose that $\lambda_n = 0$. Then we can assume that $\mu_n = -1$. Then

$$P(X,Y) = Y\prod_{i=1}^{n-1}(\lambda_i X - \mu_i Y).$$

Let $P_1(X,Y) = \prod_{i=1}^{n-1}(\lambda_i X - \mu_i Y)$. Then $P_1(X,Y) \in R[X,Y]$. Since $\lambda_i \neq 0$, $1 \le i \le n-1$, the proof of case 1 shows that $\prod_{1\le i<j\le n-1}(\lambda_i\mu_j - \lambda_j\mu_i)^2 \in R$. Since $\prod_{i=1}^{n-1}\lambda_i \in R$, and $\lambda_n = 0$, $\mu_n = -1$, we have

$$\mathscr{I}(f,g) = \prod_{1\le i<j\le n} (\lambda_i\mu_j - \lambda_j\mu_i)^2 = \prod_{i=1}^{n-1}(-\lambda_i)^2 \prod_{1\le i<j\le n-1} (\lambda_i\mu_j - \lambda_j\mu_i)^2 \in R.$$

(3) Let $R = \mathbb{Z}[\{t_{ij}\},\{t'_{ij}\}]$. By (2), $h = \mathscr{I}(\hat{f},\hat{g}) \in R$. Thus $\mathscr{I}(f,g) = h(\{a_{ij}\},\{b_{ij}\})$. We have $\mathscr{I}(tf,tg) = t^{2n(n-1)}\mathscr{I}(f,g)$ by applying (1) with $(a,b,c,d) = (t,0,0,t)$. Thus, $\mathscr{I}(f,g)$ is a homogeneous polynomial of degree $2n(n-1)$ in the coefficients of f and g. □

6. **PROOF OF THE MAIN THEOREM**

In this section, we make the following assumptions on F and $\overline{F}$:

- (F,ν) is a complete discretely valued field with $\mathrm{char}(F) \neq 2$;
- $u(\overline{F}) < \infty$.

The second assumption implies that $u_2(\overline{F})$ is finite by Proposition 1.1.

Proof of the Main Theorem: We have $u_2(F) \ge 2u_2(\overline{F})$ by Lemma 2.4. We now prove that $u_2(F) \le 2u_2(\overline{F})$.

Let $f,g \in F[X_1,\dots,X_n]$ be quadratic forms with $n \ge 2u_2(\overline{F}) + 1$. We show that f,g have a primitive common zero in F^n. Without loss of generality, we may assume that $f,g \in \mathcal{O}[X_1,\dots,X_n]$ and so $\mathscr{I}(f,g) \in \mathcal{O}$ by Theorem 5.1 (2).

First assume that $\mathscr{I}(f,g) \neq 0$. Define

$$A := \left\{ (f',\, g') = (af_T + bg_T,\, cf_T + dg_T) \;\middle|\; \begin{array}{c} f',g' \in \mathcal{O}[X_1,\dots,X_n] \\ T : F^n \to F^n \text{ is an invertible} \\ \text{linear transformation,} \\ a,b,c,d \in F \text{ so that } ad-bc \neq 0 \end{array} \right\}.$$

By Theorem 5.1 (1), we see that $\mathscr{I}(f',g') \neq 0$, for any $(f',g') \in A$. Note that

- For any $(f', g') \in A$, there is a bijection between the common zeros of (f', g') and (f, g).
- There exists a pair (f', g') for which $\nu[\mathscr{I}(f', g')]$ is minimal.

Assume without loss of generality that (f, g) is a pair such that $\nu[\mathscr{I}(f, g)]$ is minimal. We claim that

(i) $o(\bar{f}, \bar{g}) \geq u_2(\overline{F}) + 1$, and

(ii) if $\bar{\mu}, \bar{\lambda} \in \overline{F}$, not both zero, then $o(\bar{\mu}\bar{f} - \bar{\lambda}\bar{g}) \geq u(\overline{F}) + 1$.

Proof of (i). Let $o(\bar{f}, \bar{g}) = m$. By Lemma 1.6 (3), there is a unimodular transformation $U : \mathcal{O}^n \to \mathcal{O}^n$ such that $\bar{f}_U, \bar{g}_U \in \overline{F}[X_1, \ldots, X_m]$. Define a linear transformation $R : F^n \to F^n$ by

$$e_i \mapsto \pi e_i, \quad 1 \leq i \leq m$$
$$e_i \mapsto e_i, \quad m < i \leq n.$$

Arguments from the proof of Theorem 4.3 show that $(\pi^{-1} f_{UR}, \pi^{-1} g_{UR}) \in A$. Since $\det(U) \in \mathcal{O}^\times$ and $\det(R) = \pi^m$, the minimality of $\nu[\mathscr{I}(f, g)]$ implies that

$$\begin{aligned}
\nu\big[\mathscr{I}(\pi^{-1} f_{UR}, \pi^{-1} g_{UR})\big] &= \nu\big[(\pi^{-2})^{n(n-1)} (\det(UR))^{4(n-1)} \mathscr{I}(f, g)\big] \\
&= -2n(n-1) + 4m(n-1) + \nu\big[\mathscr{I}(f, g)\big] \\
&= (4m - 2n)(n-1) + \nu\big[\mathscr{I}(f, g)\big] \\
&\geq \nu\big[\mathscr{I}(f, g)\big],
\end{aligned}$$

which implies that $4m - 2n \geq 0$. Then

$$2m \geq n \geq 2u_2(\overline{F}) + 1.$$

Since m is an integer, we have that $m \geq u_2(\overline{F}) + 1$, as claimed. □

Proof of (ii). Let $h = \mu f - \lambda g$, where $\mu, \lambda \in \mathcal{O}$ and $\bar{\mu}, \bar{\lambda}$ are not both zero. Let $o(\bar{h}) = m$ and first assume that $\lambda \in \mathcal{O}^\times$ so that $\bar{\lambda} \neq 0$ in $\overline{F}$. By Lemma 1.6 (2), there is a unimodular transformation $U : \mathcal{O}^n \to \mathcal{O}^n$ such that $\bar{h}_U \in \overline{F}[X_1, \ldots, X_m]$. Define a linear transformation $R : F^n \to F^n$ by

$$e_i \mapsto \pi e_i, \quad 1 \leq i \leq m$$
$$e_i \mapsto e_i, \quad m < i \leq n.$$

Then $\pi^{-1} h_{UR} \in \mathcal{O}[X_1, \ldots, X_n]$, and $(f_{UR}, \pi^{-1} h_{UR}) \in A$ because

$$\pi^{-1} h_{UR} = \pi^{-1} \mu f_{UR} - \pi^{-1} \lambda g_{UR}.$$

Since $\lambda \in \mathcal{O}^\times$, $\det(UR) = \pi^m$ times a unit in $\mathcal{O}$, and $\nu[\mathscr{I}(f, g)]$ is minimal, we apply Theorem 5.1 (1) with

$$(a, b, c, d) = (1, 0, \mu\pi^{-1}, -\lambda\pi^{-1})$$

and $ad - bc = -\lambda\pi^{-1}$ to obtain

$$\begin{aligned}\nu\big[\mathscr{I}(f_{UR},\, \pi^{-1}h_{UR})\big] &= \nu\big[(-\lambda\pi^{-1})^{n(n-1)}(\det(UR))^{4(n-1)}\mathscr{I}(f,h)\big]\\ &= -n(n-1) + 4m(n-1) + \nu\big[\mathscr{I}(f,h)\big]\\ &= (4m-n)(n-1) + \nu\big[(-\lambda)^{n(n-1)}\mathscr{I}(f,g)\big]\\ &= (4m-n)(n-1) + \nu\big[\mathscr{I}(f,g)\big]\\ &\geq \nu\big[\mathscr{I}(f,g)\big],\end{aligned}$$

which implies that $4m - n \geq 0$. Since $u_2(\overline{F}) \geq 2u(\overline{F})$ by Proposition 1.1, this gives

$$4m \geq n \geq 2u_2(\overline{F}) + 1 \geq 4u(\overline{F}) + 1.$$

Since m is an integer, we have that $m \geq u(\overline{F}) + 1$, as claimed. If $\bar{\mu} \neq 0$ in $\overline{F}$, then a similar proof works using the pair h, g. □

By (i) and (ii), Lemma 2.3 implies that $\bar{f}, \bar{g}$ have a nonsingular zero over $\overline{F}$. Then Lemma 3.2 implies that f, g have a primitive common zero in $\mathcal{O}^n$.

Now assume that $\mathscr{I}(f,g) = 0$. We now show that there exists a sequence $f^{(J)}, g^{(J)}$ of pairs of quadratic forms in $\mathcal{O}[X_1, \ldots, X_n]$ with $\mathscr{I}(f^{(J)}, g^{(J)}) \neq 0$ that converges to f, g as $J \to \infty$.

We define $f^{(J)}$ and $g^{(J)}$ such that

$$f^{(J)} = f + \pi^J \sum_{i=1}^{n} X_i^2 \text{ and } g^{(J)} = g + \pi^J \sum_{i=1}^{n} d_i X_i^2,$$

where $d_1, \ldots, d_n \in \mathcal{O}$ are distinct. Then

$$M_{f^{(J)}} = M_f + 2\pi^J I_n \text{ and } M_{g^{(J)}} = M_g + 2\pi^J D,$$

where I_n is the $n \times n$ identity matrix and D is the $n \times n$ diagonal matrix with diagonal entries $d_1, \ldots, d_n$. Then $\lim_{J\to\infty} f^{(J)} = f, \lim_{J\to\infty} g^{(J)} = g$.

Let $P(X,Y) = \det(2XD - 2YI_n) = \prod_{i=1}^{n}(2d_iX - 2Y)$. Then by (5.1)

$$\mathscr{I}\left(\sum_{i=1}^{n} X_i^2, \sum_{i=1}^{n} d_i X_i^2\right) = 2^{n(n-1)} \prod_{1\leq i<j\leq n} (d_i - d_j)^2 \neq 0.$$

Then,

$$\mathscr{I}\left(f + \alpha\sum_{i=1}^{n} X_i^2, g + \alpha\sum_{i=1}^{n} d_i X_i^2\right) \in \mathcal{O}[\alpha], \tag{6.1}$$

where α is a variable, by Theorem 5.1 (3). It is a nonzero polynomial because the coefficient of the highest power of α, $\alpha^{2n(n-1)}$ by Theorem 5.1 (3), is

$$\mathscr{I}\left(\sum_{i=1}^{n} X_i^2, \sum_{i=1}^{n} d_i X_i^2\right) \neq 0.$$

Therefore, we can find a sufficiently large N such that $\alpha = \pi^J$ is not a root of (6.1) for all $J \geq N$. This implies that for all $J \geq N$, $\mathscr{I}(f^{(J)}, g^{(J)}) \neq 0$. Therefore, by the first part, each pair of quadratic forms $f^{(J)}, g^{(J)}$, $J \geq N$, has a primitive zero $v^{(J)} \in \mathcal{O}^n$.

Since $f \equiv f^{(J)} \bmod \pi^J$ and $g \equiv g^{(J)} \bmod \pi^J$, it follows for $J \geq N$ that

$$f(v^{(J)}) \equiv 0 \bmod \pi^J,\ g(v^{(J)}) \equiv 0 \bmod \pi^J.$$

Then by either [6, Proposition 5.24, p. 67] or [5], there exists $v \in \mathcal{O}^n$ such that v is a primitive common zero of f and g. This completes the proof of Theorem 1.2. (See the next section for additional explanation for the existence of v.)

7. COMMENTS ON THE PROOF OF THE MAIN THEOREM

It is worthwhile to clarify the last part of the proof of Theorem 1.2 at the end of Section 6. The proof depends on an important idea of finding zeros of a sequence of systems of polynomials and proving that the zeros converge to a zero of the original system.

Let $(F, \nu, \mathcal{O}, \mathfrak{m}, \pi, \overline{F})$ be a complete discretely valued field and suppose that $S = \{f_1, \ldots, f_r\}$ is a system of polynomials in $F[X_1, \ldots, X_n]$. For every $j \geq 1$, let $\mathcal{S}^{(j)} = \{f_1^{(j)}, \ldots, f_r^{(j)}\}$ be a system of polynomials in $F[X_1, \ldots, X_n]$.

We write $\lim_{j\to\infty} f_i^{(j)} = f_i$ if the sequence of coefficients of each monomial in $f_i^{(j)}$ converges to the coefficient of the corresponding monomial in f_i. We write $\lim_{j\to\infty} \mathcal{S}^{(j)} = \mathcal{S}$ if $\lim_{j\to\infty} f_i^{(j)} = f_i$, $1 \leq i \leq r$.

Let $v \in F^n$, and for each $j \geq 1$ let $v^{(j)} \in F^n$. We write $\mathcal{S}^{(j)}(v^{(j)}) = 0$ if $f_i^{(j)}(v^{(j)}) = 0$, $1 \leq i \leq r$. Similarly, we write $\mathcal{S}(v) = 0$ if $f_i(v) = 0$, $1 \leq i \leq r$.

Now assume for each $j \geq 1$ that $f_1^{(j)}, \ldots, f_r^{(j)} \in \mathcal{O}[X_1, \ldots, X_n]$ and assume that $f_1, \ldots, f_r \in \mathcal{O}[X_1, \ldots, X_n]$. Suppose that for each $j \geq 1$ there exists $v^{(j)} \in \mathcal{O}^n$ such that $\mathcal{S}^{(j)}(v^{(j)}) = 0$, and suppose that $\lim_{j\to\infty} \mathcal{S}^{(j)} = \mathcal{S}$. Then it follows from [5] that there exists $v \in \mathcal{O}^n$ such that $\mathcal{S}(v) = 0$. This is the result that was used at the end of Section 6.

The theorem in [5] is not easy to prove at this time. We now explain this assertion and give some background.

First consider the case in [2] where F is a p-adic field and thus $\overline{F}$ is a finite field. Since $\overline{F}$ is finite, the metric topology on $\mathcal{O}$ induced by the valuation is compact. We give $\mathcal{O}^n$ the product topology. Then $\mathcal{O}^n$ is compact and so every infinite subset of $\mathcal{O}^n$ contains a convergent subsequence. Since each $v^{(j)} \in \mathcal{O}^n$, the sequence $v^{(j)}$ contains a convergent subsequence. If this

subsequence converges to $v \in \mathcal{O}^n$, then since $\lim_{j\to\infty} \mathcal{S}^{(j)} = \mathcal{S}$, the continuity of the polynomials on the compact set $\mathcal{O}^n$ implies that $\mathcal{S}(v) = 0$.

Now we remove the assumption that $\overline{F}$ is a finite field. Greenberg proved in [5] (and discussed in [6, Proposition 5.24, p. 67]) that the conclusion is still valid, but the proof is much more difficult.

If $\operatorname{char} F = 0$, then Kneser gave an elementary proof in [7]. In fact, Kneser's proof is valid under the weaker assumption that F is the fraction field of a Henselian discrete valuation ring R.

Greenberg's theorem (with no assumption on $\operatorname{char} F$) is valid under the weaker assumption that F is the fraction field of a Henselian discrete valuation ring R with the additional property that if R^* is the completion of R and F^* is the fraction field of R^* then F^* is separable over F.

The hypotheses of both Kneser's theorem and Greenberg's theorem are satisfied by complete discretely valued fields because a complete discrete valuation ring is also Henselian (see [4], p. 86).

8. THE CASE OF CHARACTERISTIC 2

Let (F, ν) be a complete discretely valued field with residue field $\overline{F}$ and assume that $\operatorname{char} F = 2$. For example, let $F = k((t))$ where k is a field with $\operatorname{char} k = 2$, and thus $k = \overline{F}$. Then $u_2(F)$ has not yet been computed.

In [11], the condition that (F, ν) is complete was relaxed to assume only that (F, ν) is a Henselian field. In this case, computing $u(F)$ for just one quadratic form is much more difficult when $\operatorname{char} F = 2$. Very good results were obtained in [11] but the precise value of $u(F)$ was not calculated. The computation of $u_2(F)$ in this case is presumably more difficult.

Acknowledgments. We are very grateful to the referee for making many suggestions to improve the exposition.

REFERENCES

[1] R. Baeza, *Comparing u-invariants of fields of characteristic* 2. Bol. Soc. Brasil. Mat. **13** (1982), *1*, 105–114.

[2] B.J. Birch, D.J. Lewis, and T.G. Murphy, *Simultaneous quadratic forms*. Amer. J. Math. **84** (1962), 110–115.

[3] V.B. Dem'yanov, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes* (in Russian). Izv. Akad. Nauk SSSR Ser. Mat **20** (1956), 307–324. English translation. Amer. Math. Soc. Transl. **52** (1966), 75–94.

[4] A.J. Engler and A. Prestel, *Valued Fields*. Springer Monogr. Math., Springer, Berlin, 2005.

[5] M.J. Greenberg, *Rational points in Henselian discrete valuation rings.* Inst. Hautes Études Sci. Publ. Math. **31** (1966), 59–64.

[6] M.J. Greenberg, *Lectures on Forms in Many Variables.* W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[7] M. Kneser, *Konstruktive Lösung p-adischer Gleichungssysteme* (in German). Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **5** (1978), 67–69.

[8] T.Y. Lam, *Introduction to Quadratic Forms over Fields.* Grad. Stud. Math. 67, American Mathematical Society, Providence, RI, 2005.

[9] S. Lang, *Algebra.* Grad. Texts in Math. 211, Springer, New York, NY, 2002.

[10] D.B. Leep, *Systems of quadratic forms.* J. Reine Angew. Math. **350** (1984), 109–116.

[11] P. Mammone, R. Moresi, and A.R. Wadsworth, *u-invariants of fields of characteristic* 2. Math. Z. **208** (1991), *3*, 335–347.

[12] T.A. Springer, *Quadratic forms over fields with a discrete valuation,* I. *Equivalence classes of definite forms.* Nederl. Akad. Wetensch. Proc. Ser. A. **58** (1955), 352–362.

Received 21 June 2024

David B. Leep
Department of Mathematics,
University of Kentucky,
Lexington, Kentucky, 40506, USA
leep@uky.edu

Nandita Sahajpal
Department of Data, Media, and Design,
Nevada State University,
Henderson, Nevada, 89002, USA
nandita.sahajpal@nevadastate.edu