2024

Pairs of Quadratic Forms over p-Adic Fields

John Hall
University of Kentucky, johnhall93@live.com
Author ORCID Identifier:
https://orcid.org/0009-0004-1353-3241
Digital Object Identifier: https://doi.org/10.13023/etd.2024.128

John Hall, Student

Dr. David Leep, Major Professor

Dr. Ben Braun, Director of Graduate Studies

Pairs of Quadratic Forms over p-Adic Fields

DISSERTATION

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the College of Arts and Sciences at the University of Kentucky

By
John R. Hall
Lexington, Kentucky

Director: Dr. David Leep, Professor of Mathematics
Lexington, Kentucky
2024

https://orcid.org/0009-0004-1353-3241

ABSTRACT OF DISSERTATION

Pairs of Quadratic Forms over p-Adic Fields

Given two quadratic forms Q_1, Q_2 over a p-adic field K in n variables, we consider the pencil $\mathcal{P}_K(Q_1, Q_2)$, which contains all nontrivial K-linear combinations of Q_1 and Q_2. We define D to be the maximal dimension of a subspace in K^n on which Q_1 and Q_2 both vanish. We define H to be the maximal number of hyperbolic planes that a form in $\mathcal{P}_K(Q_1, Q_2)$ splits off over K. We will determine which values for (D, H) are possible for a nonsingular pair of quadratic forms over a p-adic field K.

KEYWORDS: algebra, number theory, quadratic forms, p-adic fields, finite fields

John R. Hall

May 1, 2024

Pairs of Quadratic Forms over p-Adic Fields

By
John R. Hall

Dr. David Leep
Director of Dissertation

Dr. Ben Braun
Director of Graduate Studies

May 1, 2024
Date

ACKNOWLEDGMENTS

I would like to thank my family for their support.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1 Introduction

Let $Q_1, Q_2 \in K[X_1, \ldots, X_n]$ be quadratic forms defined over a field K. We begin by stating a few of the main definitions. We define $\mathcal{P}_K(Q_1, Q_2)$ to be the set of nontrivial K-linear combinations of Q_1 and Q_2. We call $\mathcal{P}_K(Q_1, Q_2)$ the K-pencil of Q_1 and Q_2. We define $D = D_K(Q_1, Q_2)$ to be the maximal dimension of a subspace in K^n on which Q_1 and Q_2 both vanish. We define $H = H_K(Q_1, Q_2)$ to be the maximal number of hyperbolic planes that a form in $\mathcal{P}_K(Q_1, Q_2)$ splits off over K. We say that the pair $\{Q_1, Q_2\}$ is nonsingular if the projective variety $\mathcal{V} : Q_1 = Q_2 = 0$ is nonsingular. We will elaborate on the definition of nonsingularilty and the definitions of D and H in chapter 2.

In chapter 2, we will show that if K is a p-adic field, and the pair $\{Q_1, Q_2\}$ is nonsingular, then the following inequalities hold:

$$\frac{n-8}{2} \leqslant D \leqslant H \leqslant \frac{n}{2}$$

and

$$\frac{n-4}{2} \leqslant H \leqslant \frac{n}{2}.$$

In Theorem 2.2.11, we will show that $D < \frac{n}{2}$. Thus $\frac{n-8}{2} \leqslant D \leqslant \frac{n-1}{2}$. These inequalities lead us to ask what pairs of (D, H) are possible for a nonsingular pair of quadratic forms over a p-adic field? Answering this question is the purpose of this paper. We will refer to this problem as the (D, H) problem over p-adic fields.

The motivation for the definitions of D and H came from a paper by Heath-Brown. Heath-Brown [7, Thm 1] proved the Hasse principle for nonsingular pairs of quadratic forms in 8 variables defined over number fields. A major part of his proof was solving a local problem over p-adic fields [7, Thm 2]. Using our D and H notation, Heath-Brown's [7, Thm 2] implies that if $Q_1, Q_2 \in K[X_1, \ldots, X_8]$ is a nonsingular pair of quadratic forms defined over a p-adic field K, $D_K(Q_1, Q_2) \geqslant 1$, and the size of residue field is $\geqslant 32$, then $H_K(Q_1, Q_2) \geqslant 3$. Therefore, Heath-Brown's result implies that the pairs $(D \geqslant 1, H = 2)$ are impossible provided the size of the residue field is $\geqslant 32$. Our original goal was to generalize [7, Thm 2] to nonsingular pairs in n variables. Studying how [7, Thm 2] would generalize to nonsingular pairs in n variables is what led us to consider the (D, H) problem.

The tables on the next page show the pairs of (D, H) that are possible and not possible. The tables include links to the theorems where we prove that the corresponding (D, H) values are possible or not possible. There are four open cases in the tables. For these open cases, we do not know if there exists a nonsingular pair of quadratic forms with the corresponding D and H values. We are currently working on solving these open cases.

n: the number of variables
k: the residue field of the p-adic field
$|k|$: the cardinality of the residue field
✓: there is an example with the corresponding (D, H) values

Table 1.1: (D, H) values for n even

n even			
$D\backslash H$	$\frac{n-4}{2}$	$\frac{n-2}{2}$	$\frac{n}{2}$
$\frac{n-8}{2}$, $n = 10$	open	✓Thm 9.4.3	✓Thm 9.4.1
$\frac{n-8}{2}$, $n \geqslant 8$, $n \neq 10$	✓Thm 9.4.4	✓Thm 9.4.2	✓Thm 9.4.1
$\frac{n-6}{2}$, $n = 6$, $\lvert k\rvert \geqslant 4$	No examples Thm 11.2.2	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-6}{2}$, $n = 6$, $\lvert k\rvert < 4$	open	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-6}{2}$, $n = 8$, $\lvert k\rvert \geqslant 4$	No examples Thm 11.2.3	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-6}{2}$, $n = 8$, $\lvert k\rvert < 4$	open	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-6}{2}$, $n = 12$	✓Thm 9.3.4	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-6}{2}$ $n \geqslant 10$, $n \neq 12$	✓Thm 9.3.3	✓Thm 9.3.2	✓Thm 9.3.1
$\frac{n-4}{2}$, $n = 4$	No examples Thm 2.2.14	✓Thm 9.2.2	✓Thm 9.2.1
$\frac{n-4}{2}$, $n = 6$	No examples Thm 2.2.14	✓Thm 9.2.3	✓Thm 9.2.1
$\frac{n-4}{2}$, $n = 8$	No examples Thm 2.2.14	✓Thm 9.2.2	✓Thm 9.2.1
$\frac{n-4}{2}$, $n = 10$	No examples Thm 2.3.15	✓Thm 9.2.4	✓Thm 9.2.1
$\frac{n-4}{2}$, $n = 14$	✓Thm 9.2.10	✓Thm 9.2.2	✓Thm 9.2.1
$\frac{n-4}{2}$, $n \geqslant 12$, $n \neq 14$	✓Thm 9.2.5	✓Thm 9.2.2	✓Thm 9.2.1
$\frac{n-2}{2}$, $n = 2$	No examples	No examples Thm 2.2.14	✓Thm 9.1.1
$\frac{n-2}{2}$, $n = 4$	No examples	No examples Thm 2.3.15	✓Thm 9.1.1
$\frac{n-2}{2}$, $n \geqslant 6$	No examples	✓Thm 9.1.2	✓Thm 9.1.1

Table 1.2: (D, H) values for n odd

n odd		
$D\backslash H$	$\frac{n-3}{2}$	$\frac{n-1}{2}$
$\frac{n-7}{2}$, $n = 9$	✓Thm 10.4.3	✓Thm 10.4.1
$\frac{n-7}{2}$, $n = 7$, $n \geqslant 11$	✓Thm 10.4.2	✓Thm 10.4.1
$\frac{n-5}{2}$, $n = 5$, $\lvert k\rvert \geqslant 4$	No examples Thm 11.1.1	✓Thm 10.3.1
$\frac{n-5}{2}$, $n = 5$, $\lvert k\rvert < 4$	open	✓Thm 10.3.1
$\frac{n-5}{2}$, $n \geqslant 7$	✓Thm 10.3.2	✓Thm 10.3.1
$\frac{n-3}{2}$, $n = 3, 5$	No examples Thm 2.2.14	✓Thm 10.2.1
$\frac{n-3}{2}$, $n = 7$	No examples Thm 2.3.15	✓Thm 10.2.1
$\frac{n-3}{2}$ $n \geqslant 9$	✓Thm 10.2.2	✓Thm 10.2.1
$\frac{n-1}{2}$ $n \geqslant 1$	No examples	✓Thm 10.1.1

We will now describe our plan of attack for solving the (D, H) problem over p-adic fields. In chapter 2, we will prove some preliminary results about quadratic forms and establish some results about the D and H values for pairs of quadratic forms. In chapter 3, we will construct an important example that will be used in various places throughout the paper. Every example in the above tables is required to be a nonsingular pair. In general, it can be difficult to determine whether a pair of quadratic forms is nonsingular. To get around this difficulty, we will establish in chapter 4 a process by which we can make a pair of integral quadratic forms nonsingular by adjusting their coefficients.

Most of the examples in the above tables will be constructed in the following way. We will define two types of pairs of quadratic forms: type $\mathcal{A}$ and type $\mathcal{B}$. Most of the examples in the tables are built using these two types of pairs. Chapter 5 contains the definitions of type $\mathcal{A}$ and type $\mathcal{B}$ pairs along with some fundamental results. Most of our type $\mathcal{A}$ and type $\mathcal{B}$ pairs are constructed by first considering a suitable pair of quadratic forms over the residue field of the p-adic field. The type $\mathcal{A}$ and $\mathcal{B}$ pairs are then obtained by lifting the residue field pair up to the ring of integers in a particular way. The residue field pairs are constructed in chapter 7; these constructions are done over arbitrary finite fields.

In chapter 8, we will construct all the type $\mathcal{A}$ and type $\mathcal{B}$ pairs that we need; as previously mentioned, most of these will be obtained by lifting residue field pairs from chapter 7 to the ring of integers. Then, in chapters 9 and 10, we will use the type $\mathcal{A}$ and type $\mathcal{B}$ pairs to construct most of the examples in the tables.

As shown in the tables, there are pairs of (D, H) for which no examples exist. In particular, we see from the tables that there are no examples for the cases where $(n = 5, D = 0, H = 1)$, $(n = 6, D = 0, H = 1)$, and $(n = 8, D = 1, H = 2)$, provided $|k| \geqslant 3$. Chapter 11 deals with proving that no examples exist for these three cases. Our proof of Theorem 11.1.1 in chapter 11 follows the method that Heath-Brown used in [7, Theorem 2].

Throughout this paper, we will make use of various results that are not directly related to the (D, H) problem; for example, certain results from basic quadratic form theory. In order for this to be a self-contained document, we provide proofs and references of these various results in the appendices.

Chapter 2 Definitions, Preliminary Results, and Notation

2.1 Quadratic Form Theory

In this section, we discuss basic definitions and results from quadratic form theory. The reader who is familiar with quadratic form theory may wish to skip this section and start with section 2.2.

Let V be a vector space over a field k with $\dim(V) = n < \infty$. Let k^{alg} denote the algebraic closure of k.

Definition 2.1.1. *A map $f : V \to k$ is said to be quadratic map if*

1. *$f(cv) = c^2 f(v)$ for all $c \in k$ and $v \in V$, and*
2. *the map $B_f : V \times V \to k$ given by $B_f(v, w) = f(v + w) - f(v) - f(w)$ is bilinear over k.*

Note that B_f is symmetric. We call B_f the symmetric bilinear form associated to f. We may also refer to the pair (f, V) as a quadratic module.

Definition 2.1.2. *A quadratic form is a polynomial $q \in k[x_1, \ldots, x_n]$ that can be written as*

$$q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

where each $a_{ij} \in k$.

We can regard a quadratic form $q \in k[x_1, \ldots, x_n]$ as a map from k^n to k. With some work, one can show that $q : k^n \to k$ is quadratic map. On the other hand, given a quadratic map $f : V \to k$, we can associate to f a quadratic form in $k[x_1, \ldots, x_n]$ as follows. Let $A = \{\alpha_1, \ldots, \alpha_n\}$ be a k-basis of V. Given $(x_1, \ldots, x_n) \in k^n$, we have

$$f(x_1\alpha_1 + \cdots + x_n\alpha_n) = \sum_{i=1}^{n} f(\alpha_i)x_i^2 + \sum_{1 \leqslant i < j \leqslant n} B_f(\alpha_i, \alpha_j)x_i x_j. \tag{2.1.1}$$

This formula can be proved by induction on n. Note that the right-hand side of equation 2.1.1 is a quadratic form over k in the variables $x_1, \ldots, x_n$.

Definition 2.1.3. *Given a quadratic map $f : V \to k$, and a k-basis $A = \{\alpha_1, \ldots, \alpha_n\}$ of V, we define the quadratic form associated to f with respect to the basis A as*

$$\sum_{i=1}^{n} f(\alpha_i)x_i^2 + \sum_{1 \leqslant i < j \leqslant n} B_f(\alpha_i, \alpha_j)x_i x_j.$$

Definition 2.1.4. *A quadratic form $q \in k[x_1, \ldots, x_n]$ is said to be isotropic over k if there exist a nonzero $v \in k^n$ such that $q(v) = 0$. We say q is anisotropic over k if q does not have any nontrivial zeros in k^n.*

Let $M_f = M_f^{(A)}$ denote the $n \times n$ matrix given by $(M_f)_{ij} = B_f(\alpha_i, \alpha_j)$; that is, the (i, j) entry of M_f is $B_f(\alpha_i, \alpha_j)$. Since B_f is symmetric, we see that M_f is a symmetric matrix. We call M_f the symmetric matrix of f with respect to the basis A. Note that M_f is the symmetric matrix of the bilinear form B_f with respect to the basis A.

Let $S = \{e_1, \ldots, e_n\}$ denote the standard basis for k^n and let $q \in k[x_1, \ldots, x_n]$ be a quadratic form. We will compute the matrix $M_q^{(S)}$. Write

$$q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

where $a_{ij} \in k$. Note that $q(e_i) = a_{ii}$ and $q(e_i + e_j) = a_{ij} + a_{ii} + a_{jj}$. Observe that

$$B_q(e_i, e_i) = q(2e_i) - 2q(e_i) = 4q(e_i) - 2q(e_i) = 2q(e_i) = 2a_{ii},$$

and for $i \neq j$, we have

$$B_q(e_i, e_j) = q(e_i + e_j) - q(e_i) - q(e_j) = (a_{ij} + a_{ii} + a_{jj}) - a_{ii} - a_{jj} = a_{ij}.$$

Therefore, the matrix $M_q = M_q^{(S)}$ is given by

$$(M_q)_{ij} = \begin{cases} a_{ij} & i < j \\ 2a_{ij} & i = j \\ a_{ji} & i > j. \end{cases}$$

Often, this will be our preferred matrix to use when dealing with quadratic forms. We therefore establish the following definition.

Definition 2.1.5. *For a quadratic form $q \in k[x_1, \ldots, x_n]$ with*

$$q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

we let $M(q) = M_q$ denote the matrix of q, where

$$(M_q)_{ij} = \begin{cases} a_{ij} & i < j \\ 2a_{ij} & i = j \\ a_{ji} & i > j. \end{cases}$$

Thus M_q is the matrix of q with respect to the standard basis of k^n.

For example, suppose $q(x, y) = x^2 + xy + y^2$. Then

$$M_q = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Suppose A_1 and A_2 are bases of V over k. For a quadratic map $f : V \to k$, let $M_1 = M_f^{(A_1)}$ and $M_2 = M_f^{(A_2)}$. Thus M_i is the matrix of B_f with respect to the basis A_i. With some work, it can be shown that there exists an invertible matrix $U \in \mathrm{GL}_n(k)$ such that $M_1 = U^t M_2 U$, where U^t denotes the transpose. It follows that $\det(M_1) = \det(U)^2 \det(M_2)$. We therefore define the determinant of f as $\det(M_1)$, hence the determinant of f is unique up to a square. We regard $\det(f)$ as an element of k/k^2, where k^2 denotes the set of squares in k.

Definition 2.1.6. *Let $f : V \to k$ be a quadratic map. Let A be a k-basis of V, and $M_f = M_f^{(A)}$. We define the determinant of f as follows:*

$$det(f) = det(M_f).$$

We regard $det(f)$ as an element of k/k^2.

In the case where $f = q \in k[x_1, \ldots, x_n]$ is a quadratic form, we can use the matrix M_q from definition 2.1.5 to compute $\det(q)$.

Definition 2.1.7. *For a quadratic form $q \in k[x_1, \ldots, x_n]$ with*

$$q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

we define the determinant of q as

$$det(q) = det(M_q),$$

where M_q is the matrix of q as defined in Definition 2.1.5.

Unless stated otherwise, will always use the matrix M_q from Definition 2.1.5 when computing the determinant of a quadratic form.

Lemma 2.1.8. *Let k be any field and let $n \geqslant 1$ be odd. Suppose A is an $n \times n$ symmetric matrix over k such that the (i, i) entry is $2a_{ii}$, and for $i \neq j$, the (i, j) entry is a_{ij}. There exists a polynomial $h \in \mathbb{Z}[x_{ij}]$ of degree n such that $det(A) = 2h(a_{ij})$.*

Proof. We go by induction on n. The case $n = 1$ is clear. For $n \geqslant 3$, assume by induction that the result holds for $n-2$. Suppose the entries $a_{12}, a_{13}, \ldots, a_{1n}$ are each divisible by 2. Then every entry in row 1 of A is divisible by 2. We can therefore factor out 2 from row 1, leaving us with a new matrix A'. Thus $\det(A) = 2\det(A')$, and we can express $\det(A') = h(a_{ij})$ for some polynomial $h \in \mathbb{Z}[x_{ij}]$ of degree n, as desired.

On the other hand, suppose at least one of the entries $a_{12}, a_{13}, \ldots, a_{1n}$ is not divisible by 2. To keep A symmetric, every row operation will be followed by an analogous column operation, and vice versa. By performing column and row operations, we can assume that $a_{12} = a_{21}$ is not divisible by 2. Then by performing column and row operations, we can assume that $a_{i1} = a_{1i} = 0$ for $i \geqslant 3$ and $a_{i2} = a_{2i} = 0$ for $i \geqslant 3$. Let B denote this new matrix. Thus B is a symmetric block diagonal matrix. We have

$$\det(A) = \det(B) = (4a_{11}a_{22} - a_{12}^2)\det(C),$$

where C is some $(n-2) \times (n-2)$ matrix. By induction, $\det(C) = 2h'(a_{ij})$ for some $h' \in \mathbb{Z}[x_{ij}]$ of degree $n-2$. Then $\det(A) = 2(4a_{11}a_{22} - a_{12}^2)h'(a_{ij})$. Take $h = (4x_{11}x_{22} - x_{12}^2)h'(x_{ij})$. Then h has degree n and $\det(A) = 2h(a_{ij})$, as desired. □

Let $f : V \to k$ be quadratic map. Assume $\text{char}(k) = 2$ and $\dim(V) = n$ is odd. Then the matrix of f with respect to any k-basis $\{\alpha_1, \ldots, \alpha_n\}$ of V is a symmetric $n \times n$ matrix. The diagonal entries are $2f(\alpha_i) = 0$. Lemma 2.1.8 implies that $\det(f)$ is divisible by 2. So for $\text{char}(k) = 2$, the determinant will be zero. In this scenario, we can formally divide $\det(f)$ by 2; doing so gives us what we call the half-determinant.

Definition 2.1.9. *Let k be a field with $char(k) = 2$. Let $f : V \to k$ be a quadratic map with $dim(V) = n$ odd. We define the half-determinant of f, denoted $det_{\frac{1}{2}}(f)$, as follows:*

$$det_{\frac{1}{2}}(f) = \frac{1}{2} det(f).$$

Let $f : V \to k$ be a quadratic map.

Definition 2.1.10. *We define*

$$rad(B_f) = \{v \in V \mid B_f(v, w) = 0 \text{ for all } w \in V\}.$$

We call $rad(B_f)$ the radical of the bilinear form B_f.

Definition 2.1.11. *We define*

$$rad(f) = \{v \in V \mid f(v) = 0 \text{ and } v \in rad(B_f)\}.$$

We call $rad(f)$ the radical of f.

Definition 2.1.12. *We define the order and rank of $f : V \to k$ as follows.*

$$ord(f) = order(f) = dim(V) - dim(rad(f).$$

$$rk(f) = rank(f) = dim(V) - dim(rad(B_f)).$$

Note that $\text{rad}(q) \subseteq \text{rad}(B_q)$. Thus $\text{rank}(q) \leqslant \text{order}(q) \leqslant \dim(V) = n$. Observe that if $v \in \text{rad}(B_f)$, then

$$0 = B_f(v, v) = 2f(v).$$

Therefore, if $\text{char}(k) \neq 2$, then $f(v) = 0$ and $v \in \text{rad}(f)$. It follows that for $\text{char}(k) \neq 2$, $\text{rad}(f) = \text{rad}(B_f)$ and $\text{order}(f) = \text{rank}(f)$.

We also note that $\text{rank}(f)$ equals the rank of the bilinear form B_f. Therefore, the rank of f equals the rank of the matrix of the bilinear form B_f:

$$\text{rank}(f) = \text{rank}(M_f).$$

It follows that $\text{rank}(f) = n$ if and only if $\det(M_f) \neq 0$.

Definition 2.1.13. *We say a quadratic map $f : V \to k$ is nondegenerate if $rad(f) = 0$. We say B_f is nondegenerate if $rad(B_f) = 0$.*

From the definitions, $\text{order}(f) = n$ if and only if f is nondegenerate, and $\text{rank}(f) = n$ if and only if B_f is nondegenerate.

Lemma 2.1.14. *Let $q : V \to k$ be a quadratic map.*

1. *If char$(k) \neq 2$, then order$(q) = n$ if and only if det$(q) \neq 0$.*
2. *If char$(k) = 2$, n is even, and k is perfect, then order$(q) = n$ if and only if det$(q) \neq 0$.*
3. *If char$(k) = 2$, n is odd, and k is perfect, then order$(q) = n$ if and only if det$_{\frac{1}{2}}(q) \neq 0$*

Proof. For proof, see Lemma $B.1.5$ in the appendix. □

Definition 2.1.15. *Let $f : V \to k$ be a quadratic map. A vector $v \in V$ is said to be a singular zero of f if $f(v) = 0$ and $v \in rad(f)$. We say v is a nonsingular zero of f if $f(v) = 0$ and $v \notin rad(f)$.*

Let V be a vector space over k of dimension n. Let $A = \{\alpha_1, \ldots, \alpha_n\} \subset V$ be a k-basis for V. Let $v, w \in V$ and let $y, z \in k^n$ denote the coordinates of v, w, respectively, with respect to the basis A. Thus, if $y = (y_i)$ and $z = (z_i)$, then $v = \sum_{i=1}^n y_i\alpha_i$ and $w = \sum_{i=1}^n y_i\alpha_i$. With some work, we obtain

$$B_f(v, w) = y^t M_f z. \tag{2.1.2}$$

Given a quadratic form $q \in k[x_1, \ldots, x_n]$, we define

$$\nabla q = (q_{x_1}, q_{x_2}, \ldots, q_{x_n}),$$

where q_{x_i} is the partial derivative of q with respect to x_i. Thus $q_{x_i} \in k[x_1, \ldots, x_n]$ is a linear form. For $u \in k^n$, we define

$$\nabla q(u) = (q_{x_1}(u), q_{x_2}(u), \ldots, q_{x_n}(u)).$$

Lemma 2.1.16. *Let $f : V \to k$ be a quadratic map. Let A be a k-basis of V. For $v, w \in V$, let $y, z \in k^n$ denote the coordinates of v, w, respectively, with respect to the basis A. Let $q \in k[X_1, \ldots, X_n]$ denote the quadratic form associated to f with respect to A. Then*

$$B_f(v, w) = y \cdot \nabla q(z),$$

where $y \cdot \nabla q(z)$ denotes the dot product of y and $\nabla q(z)$.

Proof. We will show that

$$f(v + w) = f(v) + f(w) + y \cdot \nabla q(z).$$

Write $y = (y_i)$ and $z = (z_i)$. Let

$$q = \left(\sum_{i=1}^n a_i X_i^2\right) + \left(\sum_{1 \leqslant i < j \leqslant n} a_{ij} X_i X_j\right),$$

where $a_i, a_{ij} \in k$. Note $f(v+w) = q(y+z)$, $f(v) = q(y)$, and $f(w) = q(z)$. We have

$$\begin{aligned} q(y+z) &= \left(\sum_{i=1}^{n} a_i(y_i+z_i)^2\right) + \left(\sum_{1\leqslant i<j\leqslant n} a_{ij}(y_i+z_i)(y_j+z_j)\right). \\ &= q(y)+q(z)+\left(\sum_{i=1}^{n} a_i 2y_i z_i\right) + \left(\sum_{1\leqslant i<j\leqslant n} a_{ij}(y_i z_j + y_j z_i)\right). \end{aligned}$$

To finish, observe that

$$\begin{aligned} &\left(\sum_{i=1}^{n} a_i 2y_i z_i\right) + \left(\sum_{1\leqslant i<j\leqslant n} a_{ij}(y_i z_j + y_j z_i)\right) \\ &= y \cdot (2a_1 z_1, \ldots, 2a_n z_n) \\ &+ y_1(a_{12}z_2 + a_{13}z_3 + \cdots + a_{1n}z_n) \\ &+ y_2(a_{12}z_1 + a_{23}z_3 + \cdots + a_{2n}z_n) \\ &\vdots \\ &+ y_n(a_{1n}z_1 + a_{2n}z_2 + \cdots + a_{n-1,n}z_{n-1}) \\ &= y \cdot \nabla q(z). \end{aligned}$$

□

Since B_f is symmetric, we have $B_f(v,w) = B_f(w,v)$. Combining this fact with equation 2.1.2 and Lemma 2.1.16 gives us the following identities.

$$B_f(v,w) = y^t M_f z = y \cdot \nabla q(z) = \nabla q(y) \cdot z = z^t M_f y = B_f(w,v).$$

The next lemma relates singular zeros to partial derivatives.

Lemma 2.1.17. *Let $f : V \to k$ be a quadratic map. Let A be a k-basis of V. For $v \in V$, let $y \in k^n$ denote the coordinates of v with respect to A. Let $q \in k[x_1, \ldots, x_n]$ be the quadratic form associated to f with respect to A. Then v is a nonsingular zero of f if and only if $q(y) = 0$ and $\nabla q(y) \neq 0$.*

Proof. Suppose v is a nonsingular zero of f. Then $f(v) = 0$ and $v \notin \operatorname{rad}(B_f)$. Then there exists $w \in V$ such that $B_f(v,w) \neq 0$. Let $z \in k^n$ denote the coordinates of w with respect to A. We have $B_f(v,w) = \nabla q(y) \cdot z$. Thus $\nabla q(y) \neq 0$.

Conversely, suppose $q(y) = 0$ and $\nabla q(y) \neq 0$. Write $\nabla q(y) = (c_1, \ldots, c_n)$, where each $c_i \in k$. Since $\nabla q(y) \neq 0$, there exists $1 \leqslant j \leqslant n$ such that $c_j \neq 0$. Let $e_j \in k^n$ denote the j^{th} standard basis vector of k^n. Note that $e_j \cdot \nabla q(y) = c_j$. Let $u \in V$ be the vector whose coordinates respect to A are e_j. We have

$$B_f(u,v) = e_j \cdot \nabla q(y) = c_j \neq 0.$$

Thus $v \notin \operatorname{rad}(B_q)$ and so v is a nonsingular zero of f. □

Lemma 2.1.18. *Let $f : V \to k$ be a quadratic map. If f is nondegenerate, then every nontrivial zero of f is nonsingular.*

Proof. Suppose v is a singular zero of f. Let q be the quadratic form associated to f with respect to a basis A. Let $y \in k^n$ denote the coordinates of v with respect to A. Lemma 2.1.17 implies that $\nabla q(y) = 0$. Let $w \in V$ and $z \in k^n$ denote the coordinates of w with respect to A. We have

$$B_f(v, w) = \nabla q(y) \cdot z = 0.$$

Therefore, $v \in \text{rad}(B_f)$. Since $f(v) = 0$, $v \in \text{rad}(f)$ as well. Because f is nondegenerate, $\text{rad}(f) = 0$, hence $v = 0$. $\square$

Definition 2.1.19. *Let $f : V \to k$ be a quadratic map. Suppose $V_1, \ldots, V_j \subseteq V$ are subspaces such that $V = V_1 \oplus \cdots \oplus V_j$ and $B_f(V_i, V_t) = 0$ for $i \neq t$. Then we say V is the orthogonal direct sum of $V_1, \ldots, V_j$ with respect to f, and we write*

$$V = V_1 \widehat{\oplus}_f \cdots \widehat{\oplus}_f V_j.$$

If f is clear from context, we may also write

$$V = V_1 \widehat{\oplus} \cdots \widehat{\oplus} V_j.$$

Definition 2.1.20. *Let $f : V \to k$ be a quadratic map. A subspace $\mathbb{H} \subseteq V$ is said to be hyperbolic if the following conditions are satisfied.*

1. *$dim(\mathbb{H}) = 2$.*

2. *$\mathbb{H} = span(v, w)$, where $v, w \in V$ with $f(v) = f(w) = 0$.*

3. *$B_f(v, w) \neq 0$.*

The quadratic form associated to $g = f|_{\mathbb{H}}$ with respect to the basis $\{v, w\}$ is

$$f(v)X^2 + B_f(v, w)XY + f(w)Y^2 = B_f(v, w)XY.$$

Moreover, B_g is nondegenerate.

Definition 2.1.21. *We say a quadratic map $f : V \to k$ splits off j hyperbolic planes over k if there exist subspaces $\mathbb{H}_1, \ldots, \mathbb{H}_j, V_0 \subseteq V$ such that*

$$V = \mathbb{H}_1 \widehat{\oplus} \cdots \widehat{\oplus} \mathbb{H}_j \widehat{\oplus} V_0,$$

where the $\mathbb{H}_i$ are hyperbolic.

Definition 2.1.22. *Let $f, g \in R[X_1, \ldots, X_n]$ be quadratic forms over a ring R. We say that f and g are equivalent over R if there exists an invertible matrix $T \in GL_n(R)$ such that $f(TX) = g(X)$, where $X = (X_1, \ldots, X_n)$. If f and g are equivalent over R, then we write $f \sim_R g$ or $f \sim g$ when the underlying ring is clear.*

In terms of quadratic forms, Definition 2.1.21 translates to the following.

Definition 2.1.23. *We say a quadratic form $q \in k[X_1, \ldots, X_n]$ splits off j hyperbolic planes over k if there exists $T \in GL_n(k)$ such that*

$$q(TX) = X_1X_2 + X_3X_4 + \cdots + X_{2j-1}X_{2j} + q_0(X_{2j+1}, \ldots, X_n)$$

where $X = (X_1, \ldots, X_n)$ and q_0 is some quadratic form over k.

Definition 2.1.24. *Let $Q_1, Q_2 \in k[X_1, \ldots, X_n]$ be quadratic forms. An element $x \in (k^{alg})^n$ is said to be singular common zero of $\{Q_1, Q_2\}$ if $Q_1(x) = Q_2(x) = 0$ and the $2 \times n$ matrix*

$$\begin{bmatrix} \nabla Q_1(x) \\ \nabla Q_2(x) \end{bmatrix} = \begin{bmatrix} \frac{\partial Q_1}{\partial X_1}(x) & \frac{\partial Q_1}{\partial X_2}(x) & \cdots & \frac{\partial Q_1}{\partial X_n}(x) \\ \frac{\partial Q_2}{\partial X_1}(x) & \frac{\partial Q_2}{\partial X_2}(x) & \cdots & \frac{\partial Q_2}{\partial X_n}(x) \end{bmatrix}$$

has rank < 2.

Definition 2.1.25. *Let $Q_1, Q_2 \in k[X_1, \ldots, X_n]$ be quadratic forms. We say that the pair $\{Q_1, Q_2\}$ is nonsingular over k if Q_1 and Q_2 do not have any nontrivial singular common zeros defined over k^{alg}.*

From Definitions 2.1.24 and 2.1.25, we see that a pair $Q_1, Q_2 \in k[X_1, \ldots, X_n]$ is nonsingular if and only if for each nonzero $x \in (k^{\text{alg}})^n$ such that $Q_1(x) = Q_2(x) = 0$, the matrix

$$\begin{bmatrix} \nabla Q_1(x) \\ \nabla Q_2(x) \end{bmatrix} = \begin{bmatrix} \frac{\partial Q_1}{\partial X_1}(x) & \frac{\partial Q_1}{\partial X_2}(x) & \cdots & \frac{\partial Q_1}{\partial X_n}(x) \\ \frac{\partial Q_2}{\partial X_1}(x) & \frac{\partial Q_2}{\partial X_2}(x) & \cdots & \frac{\partial Q_2}{\partial X_n}(x) \end{bmatrix}$$

has rank 2.

Lemma 2.1.26. *Let k be a field with char$(k) \neq 2$ and $|k| \geqslant n$. Let $Q_1, Q_2 \in k[x_1, \ldots, x_n]$ be quadratic forms. Suppose that no form in $\mathcal{P}_k(Q_1, Q_2)$ has order n. Then Q_1, Q_2 has a singular nontrivial common zero defined over k.*

Proof. Suppose order$(Q_1) = m < n$. If $m = 0$, then $Q_1 = 0$. Since order$(Q_2) < n$, rad$(Q_2) \neq 0$ in which case Q_2 has a nontrivial zero. This nontrivial zero is a nontrivial singular zero of the pair Q_1, Q_2.

Suppose $m \neq 0$. Then we can write $Q_1(x_1, \ldots, x_n) = Q_1'(x_1, \ldots, x_m)$, where Q_1' has order m. Since char$(k) \neq 2$, rank$(Q_1') = m$, hence det$(Q_1') \neq 0$. Let $g(\lambda, \mu) =$ det$(\lambda Q_1 + \mu Q_2)$. Then $g(\lambda, \mu) = 0$ for all $\lambda, \mu \in k$. Either $g = 0$ or g is a homogeneous form of degree n. Since $|k| \geqslant n$, then $g = 0$. Then the coefficient of λ^m in g is 0. The coefficient of λ^m in g is

$$\det(Q_1')\det(\mu Q_2(0, \ldots, 0, x_{m+1}, \ldots, x_n)).$$

Since this equals zero, with $\det(Q_1') \neq 0$, we deduce that

$$\det(\mu Q_2(0, \ldots, 0, x_{m+1}, \ldots, x_n)) = 0.$$

Then $Q_2(0, \ldots, 0, x_{m+1}, \ldots, x_n)$ has order $< n - m$. It follows that $\text{rad}(Q_2(0, \ldots, 0, x_{m+1}, \ldots, x_n)) \neq 0$, in which case $Q_2(0, \ldots, 0, x_{m+1}, \ldots, x_n)$ has a nontrivial zero $(0, \ldots, 0, c_{m+1}, \ldots, c_n)$ over k. Then $(0, \ldots, 0, c_{m+1}, \ldots, c_n)$ is a nontrivial singular zero over k of Q_1, Q_2.

□

Let $f, g \in K[x_1, \ldots, x_n]$ be quadratic forms. Let $h = \det(\lambda f + \mu g)$. Then $h \in K[\lambda, \mu]$ and either $h = 0$ or h is a homogeneous form of degree n. If h is nonzero, then h factors over K^{alg} into a product of linear factors.

Theorem 2.1.27. *Let K be a field with char$(K) \neq 2$. Let $f, g \in K[X_1, \ldots, X_n]$ be quadratic forms. Let $h = det(\lambda f + \mu g)$.*

1. *If $\{f, g\}$ is a nonsingular pair, then every form in $\mathcal{P}_{K^{alg}}(f, g)$ has rank either n or $n - 1$. (The converse does not hold.)*
2. *If h has distinct linear factors over K^{alg}, then $\{f, g\}$ is a nonsingular pair. (The converse holds.)*
3. *If $\{f, g\}$ has a nontrivial singular zero defined over K, then some form in $\mathcal{P}_K(f, g)$ has rank $\leqslant n - 1$.*

Proof. See [8, Proposition 2.1, p.13] or [14, Propositions 7.2 and 7.3]. □

Lemma 2.1.28. *Let K be a field with characteristic of K not equal to 2. Let $f, g : K^n \to K$ be quadratic maps with associated symmetric bilinear forms $B_f, B_g : K \times K \to K$. Assume that f, g is a nonsingular pair. Suppose that $\mathcal{P}_K(f, g)$ contains a form having order $n - 1$. Then there is a basis of K^n such that when f and g are written with respect to this basis then*

$$f = f_1(x_1, \ldots, x_{n-1}) + ax_n^2$$

$$g = g_1(x_1, \ldots, x_{n-1}) + bx_n^2$$

where $f_1, g_1 : K^{n-1} \to K$ are quadratic maps and $a, b \in K$.

Proof. Without loss of generality, f has order $n - 1$. There is a basis $\{v_1, \ldots, v_n\}$ of K^n such that $\text{rad}(f) = \text{span}_K(v_n)$.

Suppose that $g(v_n) = 0$. Then v_n would be a nontrivial singular zero of f, g, which is excluded. Thus $g(v_n) \neq 0$, and since $\text{char}(K) \neq 2$, we have $B_g(v_n, v_n) \neq 0$.

Let V be the orthogonal complement of v_n with respect to B_g. Thus $K^n = V \oplus (K \cdot v_n)$ and $B_g(V, v_n) = 0$. For example, a basis of V is given by $\{w_1, \ldots, w_{n-1}\}$ where $w_i = v_i - c_i v_n$ with $c_i = B_g(v_i, v_n)/B_g(v_n, v_n)$.

If f, g are written with respect to the basis $w_1, \ldots, w_{n-1}, v_n$, then since $v_n \in \text{rad}(f)$, and $B_g(V, v_n) = 0$, we have

$$f = f_1(x_1, \ldots, x_{n-1})$$

and

$$g = g_1(x_1, \ldots, x_{n-1}) + cx_n^2$$

for some $c \in K^\times$. Note that $c \neq 0$ because otherwise v_n would be a singular zero of f, g. □

2.2 $D_K(f,g)$ and $H_K(f,g)$

Let K be a field. Let $Q, f, g \in K[X_1, \ldots, X_n]$ be quadratic forms. For $1 \leqslant i \leqslant n$, let e_i denote the standard basis vectors of K^n.

Definition 2.2.1. *Let $D_K(Q)$ denote the largest integer such that Q vanishes on a subspace in K^n of dimension $D_K(Q)$.*

For example, if $Q = X_1X_2$, then Q vanishes on $\text{span}_K(e_1) \subset K^2$, where $e_1 = (1,0)$. Note that Q does not vanish on a 2-dimensional space in K^2. Therefore, $D_K(Q) = 1$.

Definition 2.2.2. *Let $D = D_K(f,g)$ denote the largest integer such that f and g both vanish on a subspace in K^n of dimension D.*

Thus, if we let S be the set of subspaces in K^n, then

$$D_K(f,g) = \max\{\dim(U) \mid U \in S \text{ and } f(U) = g(U) = 0\}.$$

For example, if $f = X_1^2$ and $g = X_1X_2$, then f and g both vanish on $\text{span}_K(e_2) \subset K^2$, where $e_2 = (0,1)$. Thus $D_K(f,g) = 1$. On the other hand, if $f = X_1^2$ and $g = X_2^2$, then $D_K(f,g) = 0$.

Definition 2.2.3. *Let $H_K(Q)$ denote the largest integer such that Q splits off $H_K(Q)$ hyperbolic planes over K.*

For example, if $Q = X_1^2 + X_1X_2 + X_3^2$, then after an invertible linear change of variables, we see that $Q \sim X_1X_2 + X_3^2$. Thus $H_K(Q) = 1$.

Definition 2.2.4. *We define $H_K(f,g) = \max\{H_K(Q) \mid Q \in \mathcal{P}_K(f,g)\}$.*

Lemma 2.2.5. *For any field K, and for any quadratic forms $Q, f, g \in K[X_1, \ldots, X_n]$, we have*

1. *$D_K(f,g) \leqslant max\{D_K(f), D_K(g)\}$.*
2. *$2H_K(Q) \leqslant n$.*
3. *$H_K(Q) \leqslant D_K(Q)$.*

Proof. Statements (1) and (2) are clear from the definitions. As for (3), by definition, Q splits off $h = H_K(Q)$ hyperbolic planes over K. So after an invertible linear change of variables, we can assume $Q = X_1X_2 + \cdots + X_{2h-1}X_{2h} + Q_0(X_{2h+1}, \ldots, X_n)$ for some quadratic form Q_0 over K. Observe that Q vanishes on $\text{span}_K(e_2, e_4, \ldots, e_{2h})$, a subspace of dimension h. Thus $h = H_K(Q) \leqslant D_K(Q)$. □

Lemma 2.2.6. *Let $Q \in K[X_1, \ldots, X_n]$ be a quadratic form over a field K. Let $j = order(Q)$. Then $D_K(Q) = H_K(Q) + n - j$. In particular, if Q has order n, then $D_K(Q) = H_K(Q) \leqslant \frac{n}{2}$.*

Proof. If Q has order n, then Theorem $B.1.1$ implies that Q splits off $D_K(Q)$ hyperbolic planes. Thus $D_K(Q) \leqslant H_K(Q)$. On the other hand, since Q splits off $H_K(Q)$ hyperbolic planes, Q vanishes on a subspace of dimension $H_K(Q)$, hence $H_K(Q) \leqslant D_K(Q)$. This proves the case where Q has order n.

Suppose $\text{order}(Q) = j < n$. Then there is an invertible linear change of variables over K so that $Q = Q'(X_1, \ldots, X_j)$, where Q' has order j. It follows that $D_K(Q) = D_K(Q') + n - j$. By our special case above, $D_K(Q') = H_K(Q')$. Since $H_K(Q') = H_K(Q)$, we obtain $D_K(Q) = H_K(Q) + n - j$. □

Lemma 2.2.7. *Let K be a field with char$(K) \neq 2$ and let $f, g \in K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms. Assume $|K| \geqslant n$. Then $D_K(f, g) \leqslant H_K(f, g)$.*

Proof. Lemma 2.1.26 implies that there exists $Q \in \mathcal{P}_K(f, g)$ such that $\text{order}(Q) = n$. Note $D_K(Q) \geqslant D_K(f, g)$. Theorem $B.1.1$ implies that Q splits off at least $D_K(f, g)$ hyperbolic planes over K. Thus $D_K(f, g) \leqslant H_K(Q) \leqslant H_K(f, g)$. □

Theorem 2.2.8 (Amer's Theorem)**.** *Let K be an arbitrary field. Let $Q_1, Q_2 \in K[X_1, \ldots, X_n]$ be quadratic forms. Then Q_1 and Q_2 both vanish on an i-dimensional space over K if and only if $Q_1 + tQ_2$ vanishes on an i-dimensional space over $K(t)$.*

Proof. Amer proved the case where $\text{char}(K) \neq 2$ [1]. Leep gave a proof that was independent of the characteristic of the field [11]. □

Lemma 2.2.9. *Let K be a field and $n \geqslant 1$. If char$(K) = 2$, then assume n is even. Suppose $f, g \in K[X_1, \ldots, X_n]$ are quadratic forms with rank$(f) = n$ or rank$(g) = n$.*

1. *$\{f, g\}$ vanishes on a j-dimensional space over K if and only if $f + tg$ splits off at least j hyperbolic planes over $K(t)$.*

2. *$D_K(f, g) = H_{K(t)}(f + tg)$.*

Proof.

1. Note $\det(f + tg)$ is a polynomial in t; the constant term is $\det(f)$, and the coefficient of t^n is $\det(g)$. Since $\text{rank}(f) = n$ or $\text{rank}(g) = n$, then either $\det(f) \neq 0$ or $\det(g) \neq 0$, respectively. In either case, $\det(f + tg)$ is a nonzero polynomial in t; that is, $\det(f + tg) \neq 0$ in $K(t)$. Thus $f + tg$ has rank n over $K(t)$. By Amer's theorem (Theorem 2.2.8), $\{f, g\}$ vanishes on a j-dimensional space over K if and only if $f + tg$ vanishes on a j-dimensional space over $K(t)$. Since $f + tg$ has rank n over $K(t)$, we conclude from Theorem $B.1.1$ that $f + tg$ vanishes on a j-dimensional space if and only if $f + tg$ splits off at least j hyperbolic planes over $K(t)$.

2. Since $\{f, g\}$ vanishes on a subspace over K of dimension $D_K(f, g)$, statement (1) implies that $f + tg$ splits off at least $D_K(f, g)$ hyperbolic planes over $K(t)$, hence $H_{K(t)}(f + tg) \geqslant D_K(f, g)$. On the other hand, since $f + tg$ splits off at least $H_{K(t)}(f + tg)$ hyperbolic planes over $K(t)$, statement (1) implies that $\{f, g\}$

vanishes on a subspace over K of dimension $H_{K(t)}(f+tg)$. Thus $H_{K(t)}(f+tg) \leqslant D_K(f,g)$ and so $D_K(f,g) = H_{K(t)}(f+tg)$.

□

Theorem 2.2.10. *Let K be an infinite field with char$(K) \neq 2$. Let $Q_1, Q_2 \in K[X_1, \ldots, X_n]$ be linearly independent quadratic forms in $n \geqslant 2$ variables. Suppose rad$(Q_1) \cap$ rad$(Q_2) = 0$. Then there are infinitely forms in $\mathcal{P}_K(Q_1, Q_2)$ that split off at least 1 hyperbolic plane. In particular, $H_K(Q_1, Q_2) \geqslant 1$.*

Proof. First, we will show that there is a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off at least one 1 hyperbolic plane. We begin by considering the case where every form in $\mathcal{P}_K(Q_1, Q_2)$ has order $< n$. Then Lemma 2.1.26 implies that Q_1 and Q_2 have a nontrivial singular common zero over K, say $x \in K^n$. By a change of variable, we can assume $x = e_1$, the first standard basis vector in K^n. Then

$$Q_1 = X_1 L_1(X_2, \ldots, X_n) + Q_3(X_2, \ldots, X_n)$$

and

$$Q_2 = X_1 L_2(X_2, \ldots, X_n) + Q_4(X_2, \ldots, X_n)$$

for some linear forms L_1, L_2 and some quadratic forms Q_3, Q_4, all defined over K. Since $\mathrm{rad}(Q_1) \cap \mathrm{rad}(Q_2) = 0$, we know that not both L_1 and L_2 can be zero. Without loss of generality, assume $L_1 \neq 0$. Then e_1 is a nonsingular zero of Q_1. Therefore, Theorem B.1.1 implies that Q_1 splits off at least one hyperbolic plane over K, as desired.

Now, assume that $\mathcal{P}_K(Q_1, Q_2)$ contains at least one form of order n (i.e. rank n since $\mathrm{char}(K) \neq 2$). Let $F(\lambda, \mu) = \det(\lambda Q_1 + \mu Q_2)$. Then $F(\lambda, \mu)$ is a homogeneous form of degree n in λ, μ over K. Since there is a form in $\mathcal{P}_K(Q_1, Q_2)$ of rank n, we know $F(\lambda, \mu)$ is a nonzero homogeneous form. Therefore, there are only finitely many forms in $\mathcal{P}_K(Q_1, Q_2)$ that have rank $< n$. If a form in $\mathcal{P}_K(Q_1, Q_2)$ has rank n, then its radical is zero. On the other hand, if a form in $\mathcal{P}_K(Q_1, Q_2)$ has rank $< n$, then its radical is a proper, nonempty subset of K^n. Therefore, there are only finitely many nontrivial radicals (i.e. radicals that are proper, nonempty subsets of K^n). Let $R_1, \ldots, R_j$ denote the nontrivial radicals. Because K is an infinite field, the union of finitely many proper subspaces of K^n is also a proper subset. Thus, $R = R_1 \cup \cdots \cup R_j$ is a proper subset of K^n. Choose an element $p \in K^n \backslash R$. Then $p \neq \vec{0}$. By taking an appropriate linear combination of Q_1 and Q_2, we can find a form Q in the pencil $\mathcal{P}_K(Q_1, Q_2)$ that vanishes at p. Note that since Q_1 and Q_2 are linearly independent, we know $Q \neq 0$. Then p will be a nontrivial zero of Q that is not in the radical of Q, in which case Q will split off at least one hyperbolic plane. This shows that there is a form in the pencil $\mathcal{P}_K(Q_1, Q_2)$ that splits off at least 1 hyperbolic plane.

Next, we will show that there are infinitely forms in $\mathcal{P}_K(Q_1, Q_2)$ that split off at least 1 hyperbolic plane. Suppose there are m forms in $\mathcal{P}_K(Q_1, Q_2)$ that split off at least 1 hyperbolic plane, let's say $G_1, \ldots, G_m$. Each of the radicals $R_1, \ldots, R_j$ lies in a subspace of dimension $n-1$, and this subspace is given by the zeros of a nonzero linear form. That is, there exist nonzero linear forms $L_1, \dots, L_j$ such that

$$R_i = \{x \in K^n \mid L_i(x) = 0\}.$$

Let $S = L_1 \cdots L_j G_1 \cdots G_m$. Thus, S is a nonzero homogeneous form of degree $j + 2m$ over K. Because K is an infinite field, we can find a vector $p' \in K^n$ such that $S(p') \neq 0$. Consequently, none of the linear forms $L_1, \dots, L_j$ vanish at p', and none of the quadratic forms $G_1, \dots, G_m$ vanish at p'. By taking an approprate linear combination of Q_1 and Q_2, we can a find a form Q' in the pencil $\mathcal{P}_K(Q_1, Q_2)$ that vanishes at p'. Because p' is not a zero of any of the linear forms $L_1, \dots, L_j$, we know that p' is not in the radical of Q'. Therefore Q' splits off at least one hyperbolic plane. Because p' is not a zero of any of the quadratic forms $G_1, \dots, G_m$, it follows that Q' is not a multiple of any of $G_1, \dots, G_m$. Therefore, $G_1, G_2, \dots, G_m, Q'$ are all distinct forms in $\mathcal{P}_K(Q_1, Q_2)$. This proves that there are infinitely forms in $\mathcal{P}_K(Q_1, Q_2)$ that split off at least 1 hyperbolic plane. □

Theorem 2.2.11. *Let K be a field. Suppose $f, g \in K[X_1, \dots, X_n]$ are quadratic forms such that $\{f, g\}$ is nonsingular. Then $D_K(f, g) < \frac{n}{2}$.*

Proof. For sake of contradiction, assume $D_K(f, g) \geqslant \frac{n}{2}$. Let $W \subset K^n$ be a subspace of dimension $D_K(f, g)$ where f and g both vanish. There exist $\lambda_0, \mu_0 \in K^{\mathrm{alg}}$, not both zero, such that $\det(\lambda_0 f + \mu_0 g) = 0$. Let $h = \lambda_0 f + \mu_0 g$. From Lemma 2.1.14, we know $\mathrm{order}(h) < n$.

Suppose $v \in W$ is a nonzero singular zero of h. By Lemma 2.1.17, we have $\nabla h(v) = 0$. Therefore,

$$0 = \nabla h(v) = \lambda_0 \nabla f(v) + \mu_0 \nabla g(v).$$

This proves that the matrix $\begin{bmatrix} \nabla f(v) \\ \nabla g(v) \end{bmatrix}$ has rank < 2, hence v is a singular zero of $\{f, g\}$. According to Definition 2.1.25, this is contrary to the pair $\{f, g\}$ being nonsingular.

Therefore, every nonzero element of W is a nonsingular zero of h. Then Lemma B.1.1 implies that h splits off $\dim(W) \geqslant \frac{n}{2}$ hyperbolic planes. Then $\mathrm{order}(h) \geqslant 2\dim(W) \geqslant n$. This is contrary to $\mathrm{order}(h) < n$.

□

Remark: For $\mathrm{char}(K) \neq 2$ and $|K| \geqslant n$, we can give another proof of Theorem 2.2.11 as follows. Since $\{f, g\}$ is nonsingular, Lemma 2.1.26 implies that $\mathcal{P}_K(f, g)$ contains a form of order n. Without loss of generality, assume g has order n. By Amer's Theorem, if f, g both vanish on a subspace of dimension $n/2$, then $f + tg$ vanishes on a subspace of dimension $n/2$ over $K(t)$. Since g has order n over K, the form $f + tg$ has order n over $K(t)$. Lemma B.1.1 then implies that $f + tg$ splits off $n/2$ hyperbolic planes over $K(t)$. This implies that $\det(f + tg)$ has a repeated linear factor. According to Theorem 2.1.27, this is contrary to $\{f, g\}$ being a nonsingular pair.

Theorem 2.2.12 is due to David Leep.

Theorem 2.2.12. *Let K be a field. Let $\{f, g\}$ be a pair of linearly independent quadratic forms defined over K in n variables. Suppose that $\{f, g\}$ vanishes on a subspace W of K^n with* $\dim(W) = m$. *Assume that every form in $\mathcal{P}_K(f, g)$ has rank n.*

If $n \geqslant 3m + 1$, then there exist $\lambda, \mu \in K$, not both zero, such that $\lambda f + \mu g$ splits off $m + 1$ hyperbolic planes.

Proof. Let $\{e_1, \ldots, e_n\}$ be the standard basis of K^n. We can assume that $W = \operatorname{Span}(e_1, \ldots, e_m)$. Then

$$f = \sum_{i=1}^{m} x_i L_i(x_{m+1}, \ldots, x_n) + Q(x_{m+1}, \ldots, x_n)$$

$$g = \sum_{i=1}^{m} x_i L_i'(x_{m+1}, \ldots, x_n) + Q'(x_{m+1}, \ldots, x_n),$$

where L_i, L_i' are linear forms and Q, Q' are quadratic forms.

Note that there are $2m$ linear forms L_i, L_i', and each linear form is in terms of $n - m$ variables. Since $n - m > 2m$, we can perform an invertible linear change of variables so that $L_i, L_i' \in K[x_{m+1}, \ldots, x_{3m}]$. Therefore

$$f = \sum_{i=1}^{m} x_i L_i(x_{m+1}, \ldots, x_{3m}) + Q(x_{m+1}, \ldots, x_n),$$

and

$$g = \sum_{i=1}^{m} x_i L_i'(x_{m+1}, \ldots, x_{3m}) + Q'(x_{m+1}, \ldots, x_n).$$

There exist $\lambda, \mu \in K$, not both zero, such that the coefficient of x_n^2 in $\lambda f - \mu g$ is zero. Since $n - 1 \geqslant 3m$, we can set $x_{m+1} = \cdots = x_{3m} = \cdots = x_{n-1} = 0$ in $\lambda f - \mu g$ and let $h = (\lambda f - \mu g)(x_1, \ldots, x_m, 0, \ldots, 0, x_n)$. Since the coefficient of x_n^2 in $\lambda f - \mu g$ is zero, it follows that $h = (\lambda f - \mu g)(x_1, \ldots, x_m, 0, \ldots, 0, x_n) = 0$. Thus $\lambda f - \mu g$ vanishes on a subspace of dimension $m + 1$. Since $\lambda f - \mu g$ has rank n, it follows that $\lambda f - \mu g$ splits off $m + 1$ hyperbolic planes. □

Remark: In Theorem 2.2.12, if there are forms in $\mathcal{P}_K(f, g)$ that have rank $< n$, then it is possible for the result to fail. For example, let $N(X, Y) \in K[X, Y]$ be anisotropic of rank 2, and let $f, g \in K[X_1, \ldots, X_4]$ be given by

$$f = X_1 X_2 + X_2^2 + N(X_3, X_4),$$

and

$$g = X_1 X_2.$$

Then g has rank 2, and $(1,0,0,0)$ is a common zero of $\{f,g\}$. Thus $\{f,g\}$ vanish on a subspace of dimension 1, and the inequality $n \geqslant 3m+1$ is satisfied for $n=4$ and $m=1$. Let $\lambda, \mu \in K$, not both zero. Observe

$$\lambda f + \mu g = X_2((\lambda+\mu)X_1 + \lambda X_2) + \lambda N(X_3, X_4).$$

If $\lambda+\mu = 0$, then $\lambda f + \mu g$ does not split off 2 hyperbolic planes over K. If $\lambda + \mu \neq 0$, then we can perform the change of variable

$$X_1' = (\lambda+\mu)X_1 + \lambda X_2.$$

Doing so yields

$$\lambda f + \mu g = X_1' X_2 + \lambda N(X_3, X_4),$$

and this form does not split off 2 hyperbolic planes. Thus, there are no forms in $\mathcal{P}_K(f,g)$ that split off 2 hyperbolic planes.

Theorem 2.2.13. *Let K be a field. If char$(K) = 2$, then assume K is perfect. Assume that K is an infinite field (or a field with at least $2n$ elements). Let $f, g \in K[x_1, \ldots, x_n]$ be quadratic forms that satisfy the following three properties.*

1. *$\mathcal{P}_K(f,g)$ contains a form of order n.*
2. *Every form in $\mathcal{P}_K(f,g)$ has order $\geqslant n-1$.*
3. *$\{f,g\}$ vanishes on a subspace W of K^n with dim$(W) = m$.*

If $n \geqslant 3m+2$, then there exist $\lambda, \mu \in K$, not both zero, such that $\lambda f + \mu g$ splits off $m+1$ hyperbolic planes.

Proof. Let $\{e_1, \ldots, e_n\}$ be the standard basis of K^n. By an invertible linear change of variables, we can assume that $\{f,g\}$ vanish on $W = \text{Span}(e_1, \ldots, e_m)$. Then

$$f = \sum_{i=1}^{m} x_i L_i(x_{m+1}, \ldots, x_n) + Q(x_{m+1}, \ldots, x_n)$$

$$g = \sum_{i=1}^{m} x_i L_i'(x_{m+1}, \ldots, x_n) + Q'(x_{m+1}, \ldots, x_n),$$

where L_i, L_i' are linear forms and Q, Q' are quadratic forms.

Note that there are $2m$ linear forms L_i, L_i', and each linear form is in terms of $n-m$ variables. Since $n - m > 2m$, we can perform an invertible linear change of variables so that $L_i, L_i' \in K[x_{m+1}, \ldots, x_{3m}]$. Therefore

$$\begin{aligned} f &= \sum_{i=1}^{m} x_i L_i(x_{m+1}, \ldots, x_{3m}) + Q(x_{m+1}, \ldots, x_n). \\ g &= \sum_{i=1}^{m} x_i L_i'(x_{m+1}, \ldots, x_{3m}) + Q'(x_{m+1}, \ldots, x_n). \end{aligned} \tag{2.2.1}$$

If n is even, then let $P = \det(\lambda f + \mu g)$, and if n is odd, then let $P = \det_{\frac{1}{2}}(\lambda f + \mu g)$. In either case, P is a homogeneous form of degree n in the variables λ, μ. For $\lambda_0, \mu_0 \in K$, Lemma 2.1.14 implies that $\lambda_0 f + \mu_0 g$ has order n if and only if $P(\lambda_0, \mu_0) \neq 0$. Therefore, since $\mathcal{P}_K(f, g)$ contains a form of order n, we deduce that P is nonzero. As a nonzero homogeneous form of degree n, P has at most n distinct linear factors. Therefore, there are at most n forms in $\mathcal{P}_K(f, g)$ that have order $< n$.

Let $h_1, \ldots, h_j$ be the forms in the K-pencil of f and g such that $\text{order}(h_i) < n$. Thus $j \leqslant n$. Let $h_i = \lambda_i f + \mu_i g$, for $1 \leqslant i \leqslant j$. Let

$$f_1(x_{3m+1}, \ldots, x_n) = f(0, \ldots, 0, x_{3m+1}, \ldots, x_n),$$

and

$$g_1(x_{3m+1}, \ldots, x_n) = g(0, \ldots, 0, x_{3m+1}, \ldots, x_n).$$

Then f_1 and g_1 are quadratic forms in $n - 3m \geqslant 2$ variables. Let $S = \prod_{i=1}^{j}(\lambda_i f_1 + \mu_i g_1)$.

Suppose first that S is a nonzero polynomial. Since S is a homogeneous form with $\deg(S) = 2j$, and $|K| \geqslant 2n \geqslant 2j$, there exists $v \in K^{n-3m} = \text{Span}(e_{3m+1}, \ldots, e_n)$ such that $S(v) \neq 0$. There exist $\lambda, \mu \in K$, not both zero, such that $(\lambda f_1 + \mu g_1)(v) = 0$. Since $(\lambda f_1 + \mu g_1)(v) = 0$ and $S(v) \neq 0$, we deduce that $(\lambda, \mu) \neq (\lambda_i, \mu_i)$ for $1 \leqslant i \leqslant j$. It follows that $h := \lambda f + \mu g$ has order n. Note h vanishes on $\text{Span}(e_1, \ldots, e_m, v)$. Lemma B.1.1 implies that h splits off $m + 1$ hyperbolic planes.

Now suppose that S is the zero polynomial. Then some $\lambda_i f_1 + \mu_i g_1$ is the zero polynomial. Let $h = \lambda_i f + \mu_i g$. Then $h(0, \ldots, 0, x_{3m+1}, x_{3m+2}, \ldots, x_n) = 0$. This, together with equation 2.2.1, implies that h vanishes whenever $x_{m+1} = x_{m+2} = \cdots = x_{3m} = 0$. Thus, h vanishes on a subspace in K^n of dimension $n - 3m \geqslant m + 2$.

If h has order n, then Theorem B.1.1 implies that h splits off at least $m + 2$ hyperbolic planes, which is sufficient.

Suppose h has order $n - 1$. We can perform a change of variables so that $h = h'(x_1, \ldots, x_{n-1})$, where h' is a quadratic form of order $n-1$ over K. Let $W_1 \subset K^n$ be a subspace of dimension $m+2$ on which h vanishes. Let $W_2 = \{(a_1, a_2, \ldots, a_{n-1}, 0) \mid a_i \in K\}$. Thus W_2 is a subspace in K^n of dimension $n-1$. It follows that $\dim(W_1 \cap W_2) \geqslant m + 1$. Thus h' vanishes on $W_1 \cap W_2$. Theorem B.1.1 implies that h' splits off at least $m + 1$ hyperbolic planes over K.

□

Theorem 2.2.14. *Suppose $\{f, g\}$ is a nonsingular pair of quadratic forms in n variables over a field K.*

1. *If $n = 2$ and $D_K(f, g) = 0$, then $H_K(f, g) = 1$.*

2. *If $n = 3$ and $D_K(f, g) = 0$, then $H_K(f, g) = 1$.*

3. *If $n = 4$ and $D_K(f, g) = 0$, then $H_K(f, g) \geqslant 1$.*

4. *If $n = 5$ and $D_K(f, g) = 1$, then $H_K(f, g) \geqslant 2$. Therefore, the case $D = H = \frac{n-3}{2}$ is impossible for $n = 5$.*

5. *If $n = 6$ and $D_K(f, g) = 1$, then $H_K(f, g) \geqslant 2$. Therefore, the case $D = H = \frac{n-4}{2}$ is impossible for $n = 6$.*

6. *If $n = 8$ and $D_K(f, g) = 2$, then $H_K(f, g) \geqslant 3$. Therefore, the case $D = H = \frac{n-4}{2}$ is impossible for $n = 8$.*

Proof. Suppose $\{f, g\}$ is a nonsingular pair over K in $n \geqslant 2$ variables. Theorem 2.2.10 implies that there is always a form in $\mathcal{P}_K(f, g)$ that splits off at least one hyperbolic plane. This proves (1), (2), and (3). Alternately, Theorem 2.2.13 implies (1), (2), and (3) as well. Further, Theorem 2.2.13 also implies (4), (5), and (6). □

Lemma 2.2.15. *Let F be any field and let $Q \in F[X_1, \ldots, X_n]$ be a quadratic form. If Q is anisotropic over F, then Q is anisotropic over $F(t)$.*

Proof. For sake of contradiction, suppose $Q(x_1, \ldots, x_n) = 0$, where $x_i \in F(t)$, not all zero. By multiplying $(x_1, \ldots, x_n)$ by a suitable polynomial in t, we can assume that each $x_i \in F[t]$. Then, by multiplying $(x_1, \ldots, x_n)$ by a suitable power of t, we can assume that not all x_i are divisible by t.

Note that $Q(x_1, \ldots, x_n)$ is a polynomial in t. Let $c_1, \ldots, c_n \in F$ denote the constant terms of $x_1, \ldots, x_n$, respectively. Then the constant term of $Q(x_1, \ldots, x_n)$ is $Q(c_1, \ldots, c_n)$. Thus $Q(c_1, \ldots, c_n) = 0$. Since Q is anisotropic over F, we see that each $c_i = 0$. It follows that each x_i is divisible by t, a contradiction. □

2.3 Quadratic Forms over p-Adic Fields

For this section, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. Thus k is a finite field. Let K^{alg} denote the algebraic closure of K. For $1 \leqslant i \leqslant n$, let $e_i \in K^n$ denote the i^{th} standard basis vector of K^n.

Let $\mathfrak{m}$ be the unique maximal ideal of $\mathcal{O}_K$ and suppose that $\mathfrak{m} = (\pi)$. Thus $k = \mathcal{O}_K/(\pi)$. Let $v : K \to \mathbb{Z} \cup \{\infty\}$ denote the p-adic valuation. Assume $v(\pi) = 1$.

If $A \in \mathcal{O}_K$, let $\overline{A}$ denote the image of A in k. If $Q \in \mathcal{O}_K[X_1, \ldots, X_n]$ is a quadratic form, then let $\overline{Q} \in k[X_1, \ldots, X_n]$ denote the quadratic form obtained by reducing the coefficients modulo π. Thus, if $Q = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} X_i X_j$, then $\overline{Q} = \sum_{1 \leqslant i \leqslant j \leqslant n} \overline{a_{ij}} X_i X_j$.

Given two quadratic forms $Q_1 \in K[X_1, \ldots, X_n]$ and $Q_2 \in K[X_1, \ldots, X_m]$, we let $Q_1 \perp Q_2$ denote the orthogonal direct sum of Q_1 and Q_2. The form $Q_1 \perp Q_2$ is obtained by adding together Q_1 and Q_2 but making their variables disjoint. Thus

$Q_1 \perp Q_2$ is a form in $n+m$ variables. For example, if $Q_1 = X_1X_2$ and $Q_2 = X_1^2$, then one may regard $Q_1 \perp Q_2$ as $X_1X_2 + X_3^2$.

By Chevalley's Theorem, any quadratic form over a finite field in at least 3 variables is isotropic. Since the residue field k is a finite field, Lemma $B.2.5$ implies that there exists a unique (up to equivalence) anisotropic quadratic form $n(X,Y) \in k[X,Y]$. Therefore, if we let $N \in \mathcal{O}_K[X,Y]$ be any lift of n, then $\overline{N}$ is anisotropic over k.

Lemma 2.3.1. *Let $N_1 \in \mathcal{O}_K[X_1,\dots,X_{n_1}]$ and $N_2 \in \mathcal{O}_K[Y_1,\dots,Y_{n_2}]$ be quadratic forms such that $\overline{N_1}$ and $\overline{N_2}$ are anisotropic over k (thus $n_1, n_2 \leqslant 2$). Suppose Q is a quadratic form over $\mathcal{O}_K$ in the variables X_i, Y_j such that $Q \equiv N_1 + \pi N_2 \bmod \pi^2$. Then Q is anisotropic over K.*

Proof. Suppose $v = (x_1,\dots,x_{n_1},y_1,\dots,y_{n_2}) \in K^{n_1+n_2}$ is a nontrivial zero of Q. By multipling v by a sufficient power of π, we can assume that each $x_i, y_j \in \mathcal{O}_K$, not all divisible by π. We have $Q = N_1 + \pi N_2 + \pi^2 Q_0$, where Q_0 is some quadratic form over $\mathcal{O}_K$ in the variables X_i, Y_j. Note that

$$N_1(x_1,\dots,x_{n_1}) + \pi N_2(y_1,\dots,y_{n_2}) + \pi^2 Q_0(v) = 0$$

We must have $\pi \mid N_1(x_1,\dots,x_{n_1})$. Thus $\pi \mid x_1,\dots,x_{n_1}$ since $\overline{N_1}$ is anisotropic. Then $\pi^2 \mid N_1(x_1,\dots,x_{n_1})$. It follows that $\pi \mid N_2(y_1,\dots,y_{n_2})$. As before, this implies $\pi \mid y_1,\dots,y_{n_2}$, which is a contradiction. Therefore Q is anisotropic over K. □

Lemma 2.3.2. *Suppose $Q \in \mathcal{O}_K[X_1,\dots,X_n]$ is a quadratic form such that $Q = N(X_1,\dots,X_m) + \pi G(X_{m+1},\dots,X_n)$, where G and N are quadratic forms over $\mathcal{O}_K$ with $\overline{N}$ anisotropic over k. Then $D_K(Q) \leqslant D_k(\overline{G})$. In particular, Q splits off at most $D_k(\overline{G})$ hyperbolic planes.*

Proof. Suppose that Q vanishes on a subspace $U \subseteq K^n$ of dimension d. We will show that $d \leqslant D_k(\overline{G})$. By Theorem $C.0.1$, we arrange for $U = \operatorname{span}_K(v_1,\dots,v_d)$, where $v_i \in (\mathcal{O}_K)^n$ are linearly independent modulo π. Write $v_i = (a_{i1}, a_{i2},\dots,a_{in})$, where $a_{ij} \in \mathcal{O}_K$. Since $Q(v_i) = 0$, we have

$$0 = N(a_{i1},\dots,a_{im}) + \pi G(a_{i,m+1},\dots,a_{in}).$$

Thus $\pi \mid N(a_{i1},\dots,a_{im})$, hence π divides the first m coordinates of each v_i. Let w_i' denote the projection of v_i onto the first m coordinates. Thus $\pi \mid w_i'$ and so $\pi^2 \mid N(w_i')$. Let v_i' denote the projection of v_i onto the last $n-m$ coordinates. Since $v_1,\dots,v_d$ are linearly independent modulo π, we deduce that $v_1',\dots,v_n'$ are linearly independent modulo π. Let

$$U' = \{b_1v_1' + \dots + b_dv_d' \mid b_i \in \mathcal{O}_K\}.$$

Then $\overline{U'}$ is a subspace over k of dimension d. Since $\pi^2 \mid N(w_i')$, and $Q(U) = 0$, we deduce that $\pi \mid G(U')$. Thus $d \leqslant D_k(\overline{G})$. □

Lemma 2.3.3. *Suppose $Q \in \mathcal{O}_K[X_1, \ldots, X_n]$ is a quadratic form such that $Q = G(X_1, \ldots, X_m) + \pi N(X_{m+1}, \ldots, X_n)$, where G and N are quadratic forms over $\mathcal{O}_K$ with $\overline{N}$ anisotropic over k. Then $D_K(Q) \leqslant D_k(\overline{G})$. In particular, Q splits off at most $D_k(\overline{G})$ hyperbolic planes.*

Proof. Let T be the $n \times n$ diagonal matrix given by

$$T = \text{diag}(\pi, \pi, \ldots, \pi, 1, 1, \ldots, 1),$$

where the first m entries are π's and the last $n - m$ entries are ones. Let $Q' = \pi^{-1}Q(TX)$, where $X = (X_1, \ldots, X_n)$. Then

$$Q' = \pi G(X_1, \ldots, X_m) + N(X_{m+1}, \ldots, X_n).$$

Thus, Lemma 2.3.2 implies that $D_K(Q') \leqslant D_k(\overline{G})$. The same is true for Q. □

Lemma 2.3.4. *Let $N_1, N_2 \in \mathcal{O}_K[X, Y]$ be quadratic forms such that $\overline{N_1}$ and $\overline{N_2}$ are anisotropic of order 2 over k. Suppose $Q \in \mathcal{O}_K[X_1, \ldots, X_4]$ is a quadratic form such that $Q \equiv N_1(X_1, X_2) + N(X_3, X_4) \bmod \pi$. Then Q splits off 2 hyperbolic planes over $\mathcal{O}_K$.*

Proof. By Lemma $B.2.6$, $\overline{Q} = \overline{N_1}(X_1, X_2) + \overline{N_2}(X_3, X_4)$ splits off 2 hyperbolic planes over k. By Lemma $A.1.2$, it follows that $\overline{Q}$ splits off 2 hyperbolic planes over $\mathcal{O}_K$. □

Lemma 2.3.5. *Let $Q(X_1, \ldots, X_n)$ be a quadratic form over K in $n = 2m$ variables of rank n. If $\det(Q) = (-1)^m a$, where $a \in K$ is a nonsquare, then Q splits off exactly $\frac{n-2}{2}$ hyperbolic planes.*

Proof. Since Q has rank n, Q splits off at least $\frac{n-4}{2} = m - 2$ hyperbolic planes:

$$Q = X_1X_2 + \cdots + X_{n-5}X_{n-4} + Q'(X_{n-3}, X_{n-2}, X_{n-1}, X_n).$$

This implies that

$$(-1)^{m-2}\det(Q') = \det(Q) = (-1)^m a.$$

So $\det(Q') = a$, hence Q' has a nonsquare determinant. As a form in four variables over a p-adic field whose determinant is not a square, we know Q' splits off a hyperbolic plane, hence Q splits off at least $m - 1$ hyperbolic planes. To show that Q splits off exactly $m - 1$ hyperbolic planes, note that

$$Q = X_1X_2 + \cdots + X_{2m-3}X_{2m-2} + Q''(X_{2m-1}, X_{2m}),$$

where

$$\det(Q'') = (-1)^{m-1}\det(Q) = (-1)^{m-1}(-1)^m a = -a.$$

Since a is a nonsquare, this shows that Q'' is not hyperbolic. □

Proof. We can write $Q_1 = X_1X_2 + \cdots + X_{2h_1-1}X_{2h_1} + Q_1'(X_{2h_1+1}, \ldots, X_{n_1})$, where Q_1' is either zero or is anisotropic modulo π. Likewise, we can write $Q_2 = Y_1Y_2 + \cdots + Y_{2h_2-1}Y_{2h_2} + Q_2'(Y_{2h_2+1}, \ldots, Y_{n_2})$, where Q_2' is either zero or is anisotropic modulo π. By Lemma 2.3.1, the form $Q_1' \perp \pi Q_2'$ is anisotropic over K. Thus $Q_1 \perp \pi Q_2$ splits off exactly $h_1 + h_2$ hyperbolic planes over K. □

Lemma 2.3.6 (Hensel's Lemma)**.** *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be quadratic forms. If $\{\overline{Q_1}, \overline{Q_2}\}$ have a common nonsingular zero over k, then $\{Q_1, Q_2\}$ have a common nonsingular zero over K.*

Proof. See [4, Lemma 6, p.113]. □

The symbol $u(K)$ denotes the u-invariant of K, which is defined as the largest integer n such that there exists a quadratic form $Q \in K[x_1, \ldots, x_n]$ having no nontrivial zero defined over K.

We let $u_2(K)$ denote the largest integer n such that there exists a pair of quadratic forms $f, g \in K[x_1, \ldots, x_n]$ having no nontrivial common zero defined over K.

Lemma 2.3.7. *Let K be a p-adic field. The following statements hold.*

1. $u(K) = 4$.
2. $u(K(t)) = 8$.
3. $u_2(K) = 8$.

Proof. For a proof of $u(K) = 4$, see [9, Theorem 2.12, p.158]. Parimala and Suresh [16] proved $u(K(t)) = 8$ for the case where the characteristic of the residue field of K is not 2. Then Leep [12] gave a proof of $u(K(t)) = 8$ that was independent of the characteristic of the residue field. Demyanov was the first to prove $u_2(K) = 8$; Birch, Lewis, and Murphy gave a simpler proof [4, Theorem 1, p.113]. □

Corollary 2.3.8. *Let K be a p-adic field and let Q be a quadratic form over $K(t)$ in $n \geqslant 8$ variables. Then Q vanishes on a subspace over $K(t)$ of dimension at least $\frac{n-8}{2}$.*

Proof. We go by induction on n. If $n = 8$, then there is nothing to prove. If $n = 9$, then Lemma 2.3.7 implies that $u(K(t)) = 8$, hence Q has a common nontrivial zero and the result follows. Now suppose $n \geqslant 10$, and assume by induction that the result holds for quadratic forms over $K(t)$ that have $< n$ variables. Given $Q \in (K(t))[X_1, \ldots, X_n]$, we consider the cases where Q has rank n and rank $< n$ separately.

First, suppose Q has rank n. Since $u(K(t)) = 8$, we see that Q has a common nontrivial zero. Thus Theorem $B.1.1$ implies that Q splits off a hyperbolic plane over $K(t)$. This means there is an invertible linear change of variable over $K(t)$ so that

$$Q = Q_0(X_1, \ldots, X_{n-2}) + X_{n-1}X_n$$

where Q_0 is some quadratic form over $K(t)$. By induction, Q_0 vanishes on a subspace over $K(t)$ of dimension at least $\frac{n-10}{2}$. It follows that Q vanishes on a subspace over $K(t)$ of dimension at least $\frac{n-8}{2}$.

Next, suppose Q has rank $j < n$. Then there is an invertible linear change of variable over $K(t)$ so that $Q = Q'(X_1, \ldots, X_j)$. By induction, Q' vanishes on a subspace over $K(t)$ of dimension at least $\frac{j-8}{2}$. It follows that Q vanishes on a subspace over $K(t)$ of dimension at least

$$\frac{j-8}{2} + n - j = \frac{2n-j-8}{2} \geqslant \frac{n-8}{2}.$$

□

Corollary 2.3.9. *Let K be a p-adic field and let $f, g \in K[X_1, \dots, X_n]$ be quadratic forms in $n \geqslant 8$ variables. Then $D_K(f, g) \geqslant \frac{n-8}{2}$.*

Proof. By Theorem 2.2.8, it is sufficient to show that $Q_1 + tQ_2$ vanishes on a subspace over $K(t)$ of dimension $\geqslant \frac{n-8}{2}$. This follows from Corollary 2.3.8. □

Corollary 2.3.10. *Let K be a p-adic field. Let $Q \in K[X_1, \dots, X_n]$ be a quadratic form of rank n. Then $H_K(Q) = D_K(Q) \geqslant \frac{n-4}{2}$.*

Proof. We know from Lemma 2.3.7 that $u(K) = 4$. This, together with Theorem B.1.1, implies that $H_K(Q) \geqslant \frac{n-4}{2}$. Lemma 2.2.6 implies that $H_K(Q) = D_K(Q)$. □

Lemma 2.3.11. *Let K be a p-adic field and $\{f, g\}$ be a nonsingular pair of quadratic forms over K in n variables. Then*

$$\frac{n-8}{2} \leqslant D_K(f, g) \leqslant H_K(f, g) \leqslant \frac{n}{2},$$

and

$$\frac{n-4}{2} \leqslant H_K(f, g) \leqslant \frac{n}{2}.$$

Proof. Since K is a p-adic field, we know $\mathrm{char}(K) \neq 2$ and K is infinite. Since $\{f, g\}$ is nonsingular, Lemma 2.2.7 implies that $D_K(f, g) \leqslant H_K(f, g)$. Corollary 2.3.9 implies that $D_K(f, g) \geqslant \frac{n-8}{2}$. Lemma 2.2.5 implies that $H_K(f, g) \leqslant \frac{n}{2}$.

Since $\{f, g\}$ is nonsingular, Lemma 2.1.26 implies that $\mathcal{P}_K(f, g)$ contains a form Q of rank n. Corollary 2.3.10 then implies that Q splits off at least $\frac{n-4}{2}$ hyperbolic planes over K, hence $H_K(f, g) \geqslant \frac{n-4}{2}$. □

Thus, for a p-adic field K and a nonsingular pair of quadratic forms f, g in n variables defined over K, we ask what values $(D_K(f, g), H_K(f, g))$ can occur? We already showed in Lemma 2.2.14 that certain pairs of $(D_K(f, g), H_K(f, g))$ are impossible; note that the results in Lemma 2.2.14 were over arbitrary fields. Also, in Theorem 2.2.11, we showed that $D_K(f, g) < \frac{n}{2}$ for a nonsingular pair of quadratic forms over any field. In Lemma 2.3.15, we will prove that there are no examples of nonsingular pairs of quadratic forms over p-adic fields with $(n = 4, D = 1, H = 1)$, $(n = 7, D = 2, H = 2)$, and $(n = 10, D = 3, H = 3)$. First, we will need to prove the following lemmas. The proof of Lemma 2.3.12 is due to David Leep.

Lemma 2.3.12. *Let K be a p-adic field. Let $f, g \in K[X_1, \dots, X_n]$ be a nonsingular pair of quadratic forms with $n \geqslant 2$. Suppose $\mathcal{P}_K(f, g)$ contains a form of rank $n-1$ that splits off m hyperbolic planes over K, with $0 \leqslant m \leqslant \frac{n-2}{2}$. Then $H_K(f, g) \geqslant m+1$.*

Proof. Without loss of generality, assume f has order $n-1$ and splits off m hyperbolic planes over K. By an invertible linear change of variable, we can assume

$$\begin{aligned} f &= Q_1(X_1, \ldots, X_{n-1}) \\ g &= Q_2(X_1, \ldots, X_{n-1}) + X_n L(X_1, \ldots, X_{n-1}) + bX_n^2 \end{aligned} \tag{2.3.1}$$

for suitable quadratic forms Q_1, Q_2, a linear form L, and some $b \in K$. Since f has order $n-1$, the form Q_1 has order $n-1$. Since $\{f, g\}$ is nonsingular, $b \neq 0$; otherwise, e_n would be a nonsingular common zero of f and g.

Claim: By a change of variable, we can assume that $L = 0$.

Proof of Claim. To prove the claim, let $F, G : K^n \to K$ be quadratic maps such that for $(x_1, \ldots, x_n) \in K^n$, we have $F(x_1e_1 + \cdots + x_ne_n) = f(x_1, \ldots, x_n)$ and $G(x_1e_1 + \cdots + x_ne_n) = g(x_1, \ldots, x_n)$. Thus, f and g are the quadratic forms associated to F and G with respect to the standard basis of K^n. Note that $B_g(e_n, e_n) = 2g(e_n) \neq 0$. For each $1 \leqslant i \leqslant n-1$, let $c_i = \frac{-B_g(e_i, e_n)}{B_g(e_n, e_n)}$. Consider the basis

$$S = \{e_1 + c_1e_n, \ldots, e_{n-1} + c_{n-1}e_n, e_n\}.$$

Let f', g' be the quadratic forms associated to F, G with respect to this new basis. Notice that $f' = f$. By our choice of c_i, the form g' has the shape

$$g = Q_2'(X_1, \ldots, X_{n-1}) + b'X_n^2$$

for some quadratic form Q_2' and some $b' \in K$. This allows us, in effect, to assume that $L = 0$ in equation 2.3.1. This proves the claim. ☐

Since $f = Q_1(X_1, \ldots, X_{n-1})$ splits off m hyperbolic planes, we can perform an invertible linear change of variables over K involving only the variables $X_1, \ldots, X_{n-1}$ so that

$$\begin{aligned} f &= X_1X_2 + X_3X_4 + \cdots + X_{2m-1}X_{2m} + Q_1'(X_{2m+1}, \ldots, X_{n-1}) \\ g &= Q_2'(X_1, \ldots, X_{n-1}) + bX_n^2 \end{aligned}$$

for some quadratic forms Q_1' and Q_2' over K. Since f has order $n-1$, the form Q_1' is nondegenerate (i.e. has order $n-1-2m$). By multiplying f and g by a sufficient power of π, we can assume Q_1' and Q_2' have coefficients in $\mathcal{O}_K$ and $b \in \mathcal{O}_K$. Let

$$f_0 = X_1X_2 + X_3X_4 + \cdots + X_{2m-1}X_{2m} + Q_1'(X_{2m+1}, \ldots, X_{n-1}).$$

Since f_0 has order $n-1$, Theorem $E.0.2$ implies that there exists a positive integer N depending on f_0 such that if a quadratic form $q \in \mathcal{O}_K[X_1, \ldots, X_{n-1}]$ is congruent to f_0 modulo π^N, then f_0 and q will be equivalent over $\mathcal{O}_K$. Consequently, for any $d \in \mathcal{O}_K$, the form $f_0 + \pi^N dQ_2'$ is equivalent to f_0 over $\mathcal{O}_K$. Let

$$d = -\frac{Q_1'(\pi^N b, \ldots, \pi^N b)}{\pi^N b}.$$

Then $d \in \mathcal{O}_K$. Consider $f + \pi^N dg$. After an invertible linear change of variable involving only the variables $X_1, \ldots, X_{n-1}$, we can write

$$f + d\pi^N g = X_1X_2 + X_3X_4 + \cdots + X_{2m-1}X_{2m} + \\ + Q_1'(X_{2m+1}, \ldots, X_{n-1}) + d\pi^N bX_n^2.$$

Notice that $(\pi^N b, \pi^N b, \ldots, \pi^N b, 1) \in K^{n-2m}$ is an isotropic vector of $Q_1'(X_{2m+1}, \ldots, X_{n-1}) + d\pi^N bX_n^2$. Since $Q_1' + d\pi^N bX_n^2$ is isotropic of order $n - 2m$, Theorem $B.1.1$ implies that it splits off at least one hyperbolic plane, in which case $f + d\pi^N g$ splits off at least $m + 1$ hyperbolic planes. This completes the proof. □

The proof of Lemma 2.3.13 is due to David Leep.

Lemma 2.3.13. *Let K be a p-adic field. Let $f, g \in K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms in $n \geqslant 2$ variables. Suppose $\mathcal{P}_K(f, g)$ contains a form of order $< n$. If $\{f, g\}$ vanish on a subspace over K of dimension $m \leqslant \frac{n-2}{2}$, then $\mathcal{P}_K(f, g)$ contains a form that splits off at least $m + 1$ hyperbolic planes. Therefore, if $D_K(f, g) \geqslant m$, then $H_K(f, g) \geqslant m + 1$.*

Proof. Note that since $\{f, g\}$ is a nonsingular pair, Theorem 2.1.27 implies that every form in $\mathcal{P}_K(f, g)$ has order $\geqslant n - 1$. By hypothesis, there is a form in $\mathcal{P}_K(f, g)$ of order $< n$. Therefore, $\mathcal{P}_K(f, g)$ contains a form of order $n - 1$, and we may apply Lemma 2.1.28, which implies that there is an invertible linear change of variables over K so that

$$f = Q_1(X_1, \ldots, X_{n-1}) + aX_n^2$$
$$g = Q_2(X_1, \ldots, X_{n-1}) + bX_n^2$$

for some quadratic forms Q_1, Q_2 over K and some $a, b \in K$. Since $\{f, g\}$ is nonsingular, not both a and b can be zero. Without loss of generality, assume $b \neq 0$. By adding a multiple of g to f, we can assume $a = 0$. We therefore have

$$f = Q_1(X_1, \ldots, X_{n-1}).$$
$$g = Q_2(X_1, \ldots, X_{n-1}) + bX_n^2.$$

Next, we will show that Q_1 vanishes on a subspace in K^{n-1} of dimension m. By hypothesis, $\{f, g\}$ vanish on a subspace $U \subset K^n$ of dimension m. Suppose $U = \text{span}(v_1, \ldots, v_m)$, where $v_i \in K^n$ are linearly independent, $1 \leqslant i \leqslant m$. For each $1 \leqslant i \leqslant m$, let $v_i' \in K^{n-1}$ denote the projection of v_i onto the first $n - 1$ coordinates. Note that Q_1 vanishes on $\text{span}(v_1', \ldots, v_m')$. For sake of contradiction, assume that $v_1', \ldots, v_m'$ are linearly dependent over K. Then there exists a nonzero vector $v \in \text{span}(v_1, \ldots, v_m)$ such that $v = (0, \ldots, 0, c)$, where $c \in K$ is nonzero. But notice that v is a singular common zero of $\{f, g\}$, a contradiction. Therefore, $v_1', \ldots, v_m'$ are linearly inedpendent, and we deduce that Q_1 vanishes on subspace in K^{n-1} of dimension m, namely the space $\text{span}(v_1', \ldots, v_m')$.

Since Q_1 has order $n - 1$ and vanishes on a subspace in K^{n-1} of dimension m, Theorem $B.1.1$ implies that Q_1 splits off m hyperbolic planes over K. Then Lemma 2.3.12 implies that $H_K(f, g) \geqslant m + 1$, as desired. □

We can now prove a version of Lemma 2.2.12 that holds for nonsingular pairs of quadratic forms over p-adic fields.

Lemma 2.3.14. *Let K be a p-adic field. Let $f, g \in K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms in $n \geqslant 2$ variables. If $\{f, g\}$ vanish on a subspace over K of dimension m and $n \geqslant 3m+1$, then $\mathcal{P}_K(f,g)$ contains a form that splits off at least $m+1$ hyperbolic planes. Therefore, if $D_K(f,g) \geqslant m$, then $H_K(f,g) \geqslant m+1$ provided $n \geqslant 3m+1$.*

Proof. If $\mathcal{P}_K(f,g)$ contains a form of order $< n$, then Lemma 2.3.13 proves the result. If every form in $\mathcal{P}_K(f,g)$ order n, then Lemma 2.2.12 proves the result. □

Lemma 2.3.14 tells us that there no examples exist for the following pairs of $(D_K(f,g), H_K(f,g))$.

Theorem 2.3.15. *Suppose $\{f, g\}$ is a nonsingular pair of quadratic forms in n variables over a p-adic field K.*

1. *If $n = 4$ and $D_K(f,g) = 1$, then $H_K(f,g) \geqslant 2$. Therefore, the case $D = H = \frac{n-2}{2}$ is impossible for $n = 4$.*
2. *If $n = 7$ and $D_K(f,g) = 2$, then $H_K(f,g) = 3$. Therefore, the case $D = H = \frac{n-3}{2}$ is impossible for $n = 7$.*
3. *If $n = 10$ and $D_K(f,g) = 3$, then $H_K(f,g) \geqslant 4$. Therefore, the case $D = H = \frac{n-4}{2}$ is impossible for $n = 10$.*

Proof. Apply Lemma 2.3.14 with $(n = 4, m = 1)$, $(n = 7, m = 2)$, and $(n = 10, m = 3)$. □

Lemma 2.3.16. *Let $f, g \in \mathcal{O}_K[X_1, \ldots, X_n]$ be quadratic forms. Then $D_K(f,g) \leqslant D_k(\overline{f}, \overline{g})$.*

Proof. Let $U \subset K^n$ be a subspace where $f(U) = g(U) = 0$ and $\dim(U) = D_K(f,g)$. By Theorem C.0.1, there exists a basis for U, say $w_1, \ldots, w_t$, $t = D_K(f,g)$, such that each w_i has coordinates in $\mathcal{O}_K$ and $w_1, \ldots, w_t$ are linearly independent over k. For each i, we have $f(w_i) = g(w_i) = 0$, hence $\overline{f}(\overline{w_i}) = \overline{g}(\overline{w_i}) = 0$. Thus $\{\overline{f}, \overline{g}\}$ vanish on a subspace over k of dimension $D_K(f,g)$. This implies that $D_K(f,g) \leqslant D_k(\overline{f}, \overline{g})$. □

Lemma 2.3.17. *Let $f_1, g_1 \in \mathcal{O}_K[X_1, \ldots, X_\ell]$ be quadratic forms and let $f_2, g_2 \in \mathcal{O}_K[X_{\ell+1}, \ldots, X_n]$ be quadratic forms. Let $f = f_1 \perp \pi f_2$ and $g = g_1 \perp \pi g_2$. Then*

$$D_K(f_1, g_1) + D_K(f_2, g_2) \leqslant D_K(f,g) \leqslant D_k(\overline{f_1}, \overline{g_1}) + D_k(\overline{f_2}, \overline{g_2}).$$

Proof. It's clear that $D_K(f_1, g_1) + D_K(f_2, g_2) \leqslant D_K(f,g)$. For the other inequality, let $m = D_K(f,g)$, $m_1 = D_k(\overline{f_1}, \overline{g_1})$, and $m_2 = D_k(\overline{f_2}, \overline{g_2})$. We will show $m \leqslant m_1 + m_2$. Let $W \subseteq K^n$ be a subspace with $\dim(W) = m$ such that $f(W) = g(W) = 0$. Theorem C.0.1 implies that there exists a basis $\{y_1, \ldots, y_m\}$ of W such that each $y_i \in (\mathcal{O}_K)^n$

and $\{y_1, \ldots, y_m\}$ are linearly independent modulo π.

Let $y'_1, \ldots, y'_m$ be the projection of the vectors $y_1, \ldots, y_m$ onto the first ℓ coordinates, respectively. Thus each $y'_i \in K^\ell$. Let $y''_1, \ldots, y''_m$ be the projection of the vectors $y_1, \ldots, y_m$ onto the last $n - \ell$ coordinates. Thus each $y''_i \in K^{n-\ell}$.

Let $W_1 = \mathrm{span}_K(y'_1, \ldots, y'_m)$ and let $W_2 = \mathrm{span}_K(y''_1, \ldots, y''_m)$. Thus $W_1 \subseteq K^\ell$ and $W_2 \subseteq K^{n-\ell}$. Since $f(W) = g(W) = 0$, it follows that after reducing modulo π, we get $\overline{f_1}(\overline{W_1}) = \overline{g_1}(\overline{W_1}) = 0$. Thus $\dim(\overline{W_1}) \leqslant m_1$.

Let $j = \dim(\overline{W_1})$. Thus $j \leqslant m_1$. By relabeling appropriately, we can assume that $\{\overline{y'_1}, \ldots, \overline{y'_j}\}$ is a basis of $\overline{W_1}$. We can assume that $\overline{y'_{j+1}} = \overline{y'_{j+2}} = \cdots = \overline{y'_m} = 0$; that is, $\pi \mid y'_{j+1}, \ldots, y'_m$. In other words, the first ℓ coordinates of $y_{j+1}, \ldots, y_m$ are each divisible by π. This, combined with the fact that $y_1, \ldots, y_m$ are linearly independent modulo π, implies that $\{y''_{j+1}, \ldots, y''_m\}$ are linearly independent modulo π, hence $\dim(\overline{W_2}) = n - j$.

Since $\pi \mid y'_{j+1}, \ldots, y'_m$, and $f(W) = g(W) = 0$, we get that $f_2(\overline{W_2}) = g_2(\overline{W_2}) = 0$. Thus

$$n - j = \dim(\overline{W_2}) \leqslant D_K(\overline{f_2}, \overline{g_2}) = m_2.$$

The inequalities $j \leqslant m_1$ and $m - j \leqslant m_2$ imply that $m \leqslant m_1 + m_2$.

□

Remark: why were we able to assume $\pi \mid y'_i$ for $j + 1 \leqslant i \leqslant m$? Because $\{\overline{y'_1}, \ldots, \overline{y'_j}\}$ are linearly independent over k, for each $j + 1 \leqslant i \leqslant m$, there exist $c_{i1}, \ldots, c_{ij} \in k$ such that

$$c_{i1}\overline{y'_1} + \cdots + c_{ij}\overline{y'_j} + \overline{y_i} = 0.$$

This translates to scalars $d_{i1}, \ldots, d_{ij} \in \mathcal{O}_K$ such that

$$d_{i1}y'_1 + \cdots + d_{ij}y'_j + y'_i \equiv 0 \bmod \pi.$$

Therefore, for each $j + 1 \leqslant i \leqslant m$, we can replace y_i with $z_i = d_{i1}y_1 + \cdots + d_{ij}y_j + y_i$. Because $y_1, \ldots, y_m$ are linearly independent modulo π, the same is true for $y_1, \ldots, y_j, z_{j+1}, \ldots, z_m$. This allows us in effect to assume that $y'_i \equiv 0 \bmod \pi$ for each $j + 1 \leqslant i \leqslant m$.

Corollary 2.3.18. *Let $f_1, g_1 \in \mathcal{O}_K[X_1, \ldots, X_\ell]$ be quadratic forms and let $f_2, g_2 \in \mathcal{O}_K[X_{\ell+1}, \ldots, X_n]$ be quadratic forms. Let $f = f_1 \perp \pi f_2$ and $g = g_1 \perp \pi g_2$. If $D_K(f_i, g_i) = D_k(\overline{f_i}, \overline{g_i})$ for $i = 1, 2$, then $D_K(f, g) = D_K(f_1, g_1) + D_K(f_2, g_2)$.*

Proof. This follows from Lemma 2.3.17. □

Chapter 3 Pairs of Forms in $n = 2m + 1$ Variables: An Important Example

In this chapter, we begin by proving Theorem 3.0.1, which is a result that holds over arbitrary communitive rings with identity 1.

Theorem 3.0.1. *Let R be a communitive ring with identity 1. Let $m \geqslant 0$ and $n = 2m + 1$. For each $m + 1 \leqslant i \leqslant 2m + 1$, let a_i and b_i be elements of R. Let $f, g \in R[X_1, \ldots, X_n]$ be the quadratic forms*

$$f = X_1X_{m+1} + X_2X_{m+2} + \cdots + X_mX_{2m} + \sum_{i=m+1}^{2m+1} a_iX_i^2.$$

$$g = X_1X_{m+2} + X_2X_{m+3} + \cdots + X_mX_{2m+1} + \sum_{i=m+1}^{2m+1} b_iX_i^2.$$

Then

$$\begin{aligned} det(\lambda f + \mu g) &= 2(-1)^m(a_{1+m}\lambda\mu^{2m} + b_{1+m}\mu^{2m+1}) \\ &\quad + 2(-1)^m(a_{2+m}\lambda^3\mu^{2m-2} + b_{2+m}\lambda^2\mu^{2m-1}) \\ &\quad \vdots \\ &\quad + 2(-1)^m(a_{2m+1}\lambda^{2m+1} + b_{2m+1}\lambda^{2m}\mu). \end{aligned}$$

Proof. We go by induction on m. For $m = 0$, we have $f = a_1X_1^2$ and $g = b_1X_1^2$. Thus $\det(\lambda f + \mu g) = 2(a_1\lambda + b_1\mu)$.

For $m \geqslant 1$, assume by induction that the result holds for $m - 1$. Let $A = (a_{i,j})$ denote the $(2m + 1) \times (2m + 1)$ matrix of $\lambda f + \mu g$. Notice that column $2m + 1$ of A contains only two nonzero terms, namely $a_{m,2m+1} = \mu$ and $a_{2m+1,2m+1} = 2(a_{2m+1}\lambda + b_{2m+1}\mu)$. Given $1 \leqslant i \leqslant j \leqslant 2m + 1$, let $A_{i,j}$ denote the $(2m) \times (2m)$ matrix obtain by deleting row i and column j of A. Performing cofactor expansion along column $2m + 1$ yields

$$\begin{aligned} \det(A) &= (-1)^{m+1}\mu\det(A_{m,2m+1}) \\ &\quad + 2(a_{2m+1}\lambda + b_{2m+1}\mu)\det(A_{2m+1,2m+1}). \end{aligned} \tag{3.0.1}$$

Claim: $\det(A_{2m+1,2m+1}) = (-1)^m\lambda^{2m}$.

Proof of Claim. We know $A_{2m+1,2m+1}$ is obtain by deleting row $2m + 1$ and column $2m + 1$ from A. This corresponds to deleting the monomials X_mX_{2m+1} and X_{2m+1}^2 from $\lambda f + \mu g$. Therefore, by letting

$$f_0 = X_1X_{m+1} + X_2X_{m+2} + \cdots + X_{m-1}X_{2m-1} + X_mX_{2m} + \sum_{i=m+1}^{2m} a_iX_i^2,$$

$$g_0 = X_1X_{m+2} + X_2X_{m+3} + \cdots + X_{m-1}X_{2m} + \sum_{i=m+1}^{2m} b_iX_i^2,$$

we see that $\det(A_{2m+1,2m+1}) = \det(\lambda f_0 + \mu g_0)$. Write $A_{2m+1,2m+1} = (c_{i,j})_{1\leqslant i,j\leqslant 2m}$. Then

$$\det(\lambda f_0 + \mu g_0) = \sum_{\sigma\in S_{2m}} \operatorname{sgn}(\sigma) \prod_{i=1}^{2m} c_{i,\sigma(i)}.$$

Let $\tau \in S_{2m}$ be a permutation such that $\prod_{i=1}^{2m} c_{i,\tau(i)} \neq 0$. Suppose (y,z) is a 2-cycle in τ, where $y \in \{2,\ldots,m\}$ and $z = y+m$. Thus $\tau(y) = y+m$ and $\tau(y+m) = y$. Consider the monomials

$$X_{y-1}X_{y-1+m} \quad (\text{in } f_0),$$

and

$$X_{y-1}X_{y+m} \quad (\text{in } g_0).$$

These are the only monomials in f_0 and g_0 that contain the variable X_{y-1}. Therefore, $\tau(y-1) \in \{y-1+m, y+m\}$ and either $\tau(y-1+m) = y-1$ or $\tau(y+m) = y-1$. Since $\tau(y) = y+m$ and $\tau(y+m) = y$, we deduce that $\tau(y-1) = y-1+m$ and $\tau(y-1+m) = y-1$. Thus $(y-1, y-1+m) = (y-1, z-1)$ is a 2-cycle.

With that in mind, notice that if $\tau \in S_{2m}$ satisfies $\prod_{i=1}^{2m} c_{i,\tau(i)} \neq 0$, then $\tau(m) = 2m$ and $\tau(2m) = m$ since $X_m X_{2m}$ is the only monomial in $\lambda f_0 + \mu g_0$ that contains the variable X_m. Therefore $(m, 2m)$ is a 2-cycle. Iterating our previous calculation, we obtain the following 2-cycles in τ:

$$(m,2m)(m-1,2m-1)\cdots(2,2+m)(1,1+m).$$

This is the disjoint cycle decomposition of τ, hence τ is the only permutation in S_{2m} that satisfies $\prod_{i=1}^{2m} c_{i,\tau(i)} \neq 0$. Since the sign of 2-cycle is -1, and $\operatorname{sgn} : S_{2m} \to \{-1,1\}$ is a group homomorphism, we see that $\operatorname{sgn}(\tau) = (-1)^m$. We conclude that

$$\begin{aligned}\det(\lambda f_0 + \mu g_0) &= \sum_{\sigma\in S_{2m}} \operatorname{sgn}(\sigma) \prod_{i=1}^{2m} c_{i,\sigma(i)}.\\ &= (-1)^m \prod_{i=1}^{2m} c_{i,\tau(i)}.\\ &= (-1)^m (c_{1,m+1})^2 (c_{2,m+2})^2 \cdots + (c_{m,2m})^2.\\ &= (-1)^m \lambda^{2m}.\end{aligned}$$

This completes of the proof of the claim. □

Combining our claim with equation 3.0.1 yield

$$\begin{aligned}\det(A) &= (-1)^{m+1}\mu\det(A_{m,2m+1})\\ &\quad + 2(-1)^m(a_{2m+1}\lambda^{2m+1} + b_{2m+1}\lambda^{2m}\mu).\end{aligned} \tag{3.0.2}$$

It remains to determine $\det(A_{m,2m+1})$. Let $A' = A_{m,2m+1}$, hence A' is a $(2m)\times(2m)$ matrix. Write $A' = (a'_{ij})_{1\leqslant i,j\leqslant 2m}$. Row $2m+1$ of matrix A has only two nonzero entries, namely $a_{2m+1,m} = \mu$ and $a_{2m+1,2m+1} = 2(a_{2m+1}\lambda + b_{2m+1}\mu)$. Therefore, row

$2m$ of $A' = (a'_{i,j})$ has only one nonzero entry, namely $a'_{2m,m} = \mu$. We perform cofactor expansion on A' along row $2m$; doing so yields

$$\det(A_{m,2m+1}) = \det(A') = (-1)^{3m}\mu\det(A'_{2m,m}) = (-1)^{m}\mu\det(A'_{2m,m}), \tag{3.0.3}$$

where $A'_{2m,m}$ is obtain by deleting rows $2m$ and m of matrix A'. Thus $A'_{2m,m}$ is a $(2m-1)\times(2m-1)$ matrix. Since $a'_{2m,m} = \mu$ was originally the entry $a_{2m+1,m} = \mu$ in A, we observe that deleting row $2m$ and column m in A' corresponds to deleting row $2m+1$ and column m in A. In total, we see that $A'_{2m,m}$ is obtained by deleting rows m, $2m+1$ and columns m, $2m+1$ in matrix A. This in turn corresponds to deleting the monomials X_mX_{2m+1}, X_mX_{2m}, $X_{m-1}X_{2m}$, and X_{2m+1}^2 in $\lambda f + \mu g$. Therefore, by letting

$$f' = X_1X_m + X_2X_{m+1} + \cdots + X_{m-1}X_{2m-2} + \sum_{i=m+1}^{2m} a_iX_{i-1}^2,$$

$$g' = X_1X_{m+1} + X_2X_{m+3} + \cdots + X_{m-1}X_{2m-1} + \sum_{i=m+1}^{2m} b_iX_{i-1}^2,$$

we see that $\det(A'_{2m,m}) = \det(\lambda f' + \mu g')$. To see why the subscript for X_{i-1}^2 is correct, note that for $i \geqslant m+1$, the (i,i) entry in our original matrix A is $a_i\lambda + b_i\mu$. When we delete column m, the entry $a_i\lambda + b_i\mu$ is now in column $i-1$ of the matrix $A'_{2m,m}$, hence it corresponds to the variable X_{i-1}.

By induction, we have

$$\begin{aligned}\det(A'_{2m,m}) &= 2(-1)^{m-1}(a_{1+m}\lambda\mu^{2m-2} + b_{1+m}\mu^{2m-1})\\ &\quad + 2(-1)^{m-1}(a_{2+m}\lambda^3\mu^{2m-4} + b_{2+m}\lambda^2\mu^{2m-3})\\ &\quad \vdots\\ &\quad + 2(-1)^{m-1}(a_{2m}\lambda^{2m-1} + b_{2m}\lambda^{2m-2}\mu).\end{aligned} \tag{3.0.4}$$

Combining equations 3.0.3 and 3.0.4 yield

$$\begin{aligned}\det(A_{m,2m+1}) &= -2(a_{1+m}\lambda\mu^{2m-1} + b_{1+m}\mu^{2m})\\ &\quad - 2(a_{2+m}\lambda^3\mu^{2m-3} + b_{2+m}\lambda^2\mu^{2m-2})\\ &\quad \vdots\\ &\quad - 2(a_{2m}\lambda^{2m-1}\mu + b_{2m}\lambda^{2m-2}\mu^2).\end{aligned} \tag{3.0.5}$$

Combining equations 3.0.2 and 3.0.5 yield

$$\begin{aligned}\det(A) &= 2(-1)^{m}(a_{1+m}\lambda\mu^{2m} + b_{1+m}\mu^{2m+1})\\ &\quad + 2(-1)^{m}(a_{2+m}\lambda^3\mu^{2m-2} + b_{2+m}\lambda^2\mu^{2m-1})\\ &\quad \vdots\\ &\quad + 2(-1)^{m}(a_{2m}\lambda^{2m-1}\mu^2 + b_{2m}\lambda^{2m-2}\mu^3)\\ &\quad + 2(-1)^{m}(a_{2m+1}\lambda^{2m+1} + b_{2m+1}\lambda^{2m}\mu).\end{aligned} \tag{3.0.6}$$

□

For any field F, we let $e_1, \ldots, e_n$ denote the standard basis vectors in F^n.

Corollary 3.0.2. *Let R be a commutative ring with identity 1. Let F be a field containing R. Let $m \geqslant 0$ and $n = 2m+1$. Let $P(\lambda, \mu) \in R[\lambda, \mu]$ denote a homogeneous form of degree n in the variables λ, μ. Then there exist quadratic forms $f, g \in R[X_1, \ldots, X_n]$ such that $\{f, g\}$ vanish on $span_F(e_1, \ldots, e_m)$ and $det(\lambda f + \mu g) = 2(-1)^m P(\lambda, \mu)$.*

Proof. We can write $P(\lambda, \mu)$ in the following way:

$$\begin{aligned} P(\lambda, \mu) = {} & a_{1+m}\lambda\mu^{2m} + b_{1+m}\mu^{2m+1} \\ & + a_{2+m}\lambda^3\mu^{2m-2} + b_{2+m}\lambda^2\mu^{2m-1} \\ & \vdots \\ & + a_{2m}\lambda^{2m-1}\mu^2 + b_{2m}\lambda^{2m-2}\mu^3 \\ & + a_{2m+1}\lambda^{2m+1} + b_{2m+1}\lambda^{2m}\mu, \end{aligned}$$

where $a_i, b_i \in R$. Let f and g be as in Theorem 3.0.1. Then $\{f, g\}$ vanish on $\mathrm{span}_F(e_1, \ldots, e_m)$ and $\det(\lambda f + \mu g) = 2(-1)^m P(\lambda, \mu)$. □

Chapter 4 A Method for Producing Nonsingular Pairs over p-Adic Fields

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We will use the same notation given at the beginning of section 2.3.

Our goal in this chapter is to show how we can adjust the coefficients of a pair of quadratic forms in $\mathcal{O}_K[X_1, \ldots, X_n]$ modulo a power of π so that the pair becomes nonsingular. We begin with Lemmas 4.0.1 and 4.0.2. Lemma 4.0.1 is essentially Gauss's lemma, and Lemma 4.0.2 is a simple generalization of [5, Lemma 2.1, p.2].

Lemma 4.0.1. *Let $g(x) \in k[x]$ be a monic polynomial that is irreducible over k. Let $G(x) \in \mathcal{O}_K[x]$ be a monic polynomial such that the reduction of G modulo π is g, $\deg(G) = \deg(g)$, and with the convention that 0 lifts to 0. Then the nonzero coefficients of G are units in $\mathcal{O}_K$, and G is irreducible over K.*

Proof. Since 0 lifts to 0, the nonzero coefficient of G are units in $\mathcal{O}_K$. To prove that G is irreducible over K, we go by contrapositive. Assume G is reducible over K. We will show g is reducible over k. Write $G(x) = A(x)B(x)$, where $A(x), B(x) \in K[x]$, $\deg(A) \geqslant 1$, and $\deg(B) = 1$. By multiplying both sides of this equation by a sufficient positive power of π, we can assume $A(x), B(x) \in \mathcal{O}_K[x]$. Upon doing this, we obtain a new equation: $\pi^N G(x) = A_1(x)B_1(x)$, where $N \geqslant 0$, and $A_1(x), B_1(x) \in \mathcal{O}_K[x]$ with $\deg(A_1) = \deg(A) \geqslant 1$ and $\deg(B_1) = \deg(B) \geqslant 1$. If $N = 0$, then reducing modulo π gives a nontrivial factorization of $g(x)$.

Assume $N \geqslant 1$. Then reducing modulo π gives $0 = a_1(x)b_1(x)$, where $\overline{A_1(x)} = a_1(x)$ and $\overline{B_1(x)} = b_1(x)$. Since $k[x]$ is an integral domain, at least one of either $a_1(x)$ or $b_1(x)$ is zero. Without loss of generality, suppose $a_1(x) = 0$. Then $\pi \mid A_1(x)$. We can then cancel a factor of π from $\pi^N G(x) = A_1(x)B_1(x)$ to obtain $\pi^{N-1}G(x) = A_1'(x)B_1(x)$, where $A_1'(x) \in \mathcal{O}_K[x]$ with $\pi A_1(x) = A_1'(x)$, hence $\deg(A_1') = \deg(A_1) \geqslant 1$. If $N - 1 = 0$, then as before, reducing modulo π gives a nontrivial factorization of $g(x)$. If $N - 1 > 0$, then we may repeat this process again. The process terminates once all the factors of π are canceled, which in turn gives us a nontrivial factorization of $g(x)$. □

Lemma 4.0.2 (Chakri, Leep)**.** *Let S be a ring such that $\mathcal{O}_K \subseteq S$. Suppose $h \in S[X_1, \ldots, X_n]$ is a nonzero polynomial, and let $b_1, \ldots, b_n \in \mathcal{O}_K$. Let j be a positive integer. Then there exist $a_1, \ldots, a_n \in \mathcal{O}_K$ such that $h(a_1, \ldots, a_n) \neq 0$ and $a_i \equiv b_i \bmod \pi^j$, $1 \leqslant i \leqslant n$.*

Proof. The proof is essentially identical to [5, Lemma 2.1, p.2]. Note that in [5, Lemma 2.1, p.2], they use R to denote the ring of integers, and they use k to denote the p-adic field. □

Lemma 4.0.3. *Let $L_1, \ldots, L_t \in K^{alg}[\lambda, \mu]$ be a finite collection (possibly empty) of linear forms such that for $i \neq j$, L_i and L_j and not multiplies of each other. Let*

$n \geqslant 1$ be a positive integer and d be an integer such that $0 \leqslant d \leqslant \frac{n-1}{2}$. There exist quadratic forms $f, g \in K[X_1, \ldots, X_n]$ with the following properties.

1. *$\{f, g\}$ is nonsingular.*
2. *For each $1 \leqslant i \leqslant t$, $L_i \nmid$ det$(\lambda f + \mu g)$.*
3. *$\{f, g\}$ vanish on span$_K(e_1, \ldots, e_d)$ (if $d = 0$ then we simply assert that $\{f, g\}$ vanish on the zero space.)*

Proof. First, consider the case where $n \geqslant 1$ is odd. Write $n = 2m+1$ for some $m \geqslant 0$. Since K is a infinite field, we can choose $P(\lambda, \mu) \in K[\lambda, \mu]$ to be a homogeneous form of degree n in the variables λ, μ such that $P(\lambda, \mu)$ has distinct linear factors and $L_i \nmid P$ for each $1 \leqslant i \leqslant t$.

By Corollary 3.0.1, there exist quadratic forms $f, g \in K[X_1, \ldots, X_n]$ such that $\{f, g\}$ vanish on $\text{span}_K(e_1, \ldots, e_m)$ and

$$\det(\lambda f + \mu g) = 2(-1)^m P(\lambda, \mu).$$

Since $P(\lambda, \mu)$ has distinct linear factors, Theorem 2.1.27 implies that $\{f, g\}$ is nonsingular. Statement (2) follows from our choice of P. Statement (3) follows from the fact that $d \leqslant \frac{n-1}{2}$ and $m = \frac{n-1}{2}$.

Suppose $n \geqslant 2$ is even. Write $n - 1 = 2m' + 1$ for some $m' \geqslant 0$. Since n is even, $d \leqslant \frac{n-2}{2}$. Since K is an infinite field, we can choose $P'(\lambda, \mu) \in K[\lambda, \mu]$ to be a homogeneous form of degree $n-1$ in the variables λ, μ such that $P'(\lambda, \mu)$ has distinct linear factors and $L_i \nmid P'$ for each $1 \leqslant i \leqslant t$.

By Corollary 3.0.1, there exist quadratic forms $f', g' \in K[X_1, \ldots, X_{n-1}]$ such that $\{f', g'\}$ vanish on $\text{span}_K(e_1, \ldots, e_{m'})$ and

$$\det(\lambda f' + \mu g') = 2(-1)^{m'} P'(\lambda, \mu).$$

Since K is infinite, we can choose $a, b \in K$, not both zero, so that $L' = a\lambda + b\mu$ does not divide $P'(\lambda, \mu)$ and L' is not a multiple of L_i, $1 \leqslant i \leqslant t$. Take $f = f' + aX_n^2$ and $g = g' + bX_n^2$. Theorem 2.1.27 implies that $\{f, g\}$ is nonsingular. Statement (2) follows from our choice of P', a, and b. Statement (3) follows from the fact that $d \leqslant \frac{n-2}{2}$ and $m' = \frac{n-2}{2}$. ☐

Let $n \geqslant 1$ be a positive integer and d be an integer such that $0 \leqslant d \leqslant \frac{n-1}{2}$. Let

$$U = \{(i, j) \mid 1 \leqslant i \leqslant j \leqslant n \text{ and } j \geqslant d + 1\}. \tag{4.0.1}$$

For each $(i, j) \in U$, let t_{ij} and t'_{ij} be indeterminants (i.e. variables). Let F, G be the quadratic forms defined by

$$\begin{aligned} F = F_{t_{ij}} &= \sum_{(i,j) \in U} t_{ij} X_i X_j. \\ G = G_{t'_{ij}} &= \sum_{(i,j) \in U} t'_{ij} X_i X_j. \end{aligned} \tag{4.0.2}$$

In general, for a subring $R \subseteq K$, a pair of quadratic forms $f, g \in R[X_1, \ldots, X_n]$ vanish on the subspace $\text{span}_K(e_1, \ldots, e_d)$ if and only if there exist $s_{ij}, s'_{ij} \in R$ so that $f = F_{s_{it}}$ and $g = G_{s'_{ij}}$.

Lemma 4.0.4. *Let U, F, and G be as above. Let $L_1, \ldots, L_t \in K^{alg}[\lambda, \mu]$ be a finite collection (possibley empty) of linear forms such that for $i \neq j$, L_i and L_j are not multiples of each other.*

There exists a nonzero polynomial $h = h(t_{ij}, t'_{ij}) \in K^{alg}[\{t_{ij}, t'_{ij}\}]$ with the property that if $s_{ij}, s'_{ij} \in K$ and $h(s_{ij}, s'_{ij}) \neq 0$, then the pair $\{F_{s_{ij}}, G_{s'_{ij}}\}$ is nonsingular, and $L_m \nmid det(\lambda F_{s_{ij}} + \mu G_{s'_{ij}})$ for each $1 \leqslant m \leqslant t$.

Proof. Note that $\det(\lambda F + \mu G) \in (\mathbb{Z}[\{t_{ij}, t'_{ij}\}])[\lambda, \mu]$ is a homogeneous form. Let $P(\lambda, \mu) = \det(\lambda F + \mu G) L_1 L_2 \cdots L_t$. Then $P(\lambda, \mu)$ is a homogeneous form in λ, μ. Let

$$\begin{aligned} h &= \text{disc}(P(\lambda, \mu)) \\ &= \text{disc}(\det(\lambda F + \mu G) L_1 L_2 \cdots L_t). \end{aligned} \tag{4.0.3}$$

By Theorem $D.1.3$, h is a polynomial over $\mathbb{Z}$ in the coefficients of $P(\lambda, \mu)$. In particular, since $\det(\lambda F + \mu G)$ has coefficients in $\mathbb{Z}[\{t_{ij}, t'_{ij}\}]$, and the L_i have coefficients in K^{alg}, we deduce that h is a polynomial over K^{alg} in the variables $\{t_{ij}, t'_{ij}\}$. To express this, we write $h = h(t_{ij}, t'_{ij})$.

Next, we will show that h is a nonzero polynomial. By Lemma 4.0.3, there exist quadratic forms $f_0, g_0 \in K[X_1, \ldots, X_n]$ such that $\{f_0, g_0\}$ vanish on $\text{span}_K(e_1, \ldots, e_d)$, $\{f_0, g_0\}$ is nonsingular, and $L_m \nmid \det(\lambda f_0 + \mu g_0)$, $1 \leqslant m \leqslant t$. Since $\{f_0, g_0\}$ vanish on $\text{span}_K(e_1, \ldots, e_d)$, we can write f_0 and g_0 in the following way:

$$f_0 = \sum_{(i,j) \in U} c_{ij} X_i X_j$$

$$g_0 = \sum_{(i,j) \in U} d_{ij} X_i X_j$$

for suitable $c_{ij}, d_{ij} \in K$. Notice that $F_{c_{ij}} = f_0$ and $G_{d_{ij}} = g_0$. Observe that

$$h(c_{ij}, d_{ij}) = \text{disc}(\det(\lambda f_0 + \mu g_0) L_1 L_2 \cdots L_t).$$

Since $\{f_0, g_0\}$ is nonsingular, Theorem 2.1.27 implies that $\det(\lambda f_0 + \mu g_0)$ has no repeated linear factors. It follows that the homogeneous form $\det(\lambda f_0 + \mu g_0) L_1 L_2 \cdots L_t$ has no repeated linear factors. Lemma $D.1.2$ then implies that $h(c_{ij}, d_{ij}) \neq 0$. Thus h is a nonzero polynomial.

Likewise, for $s_{ij}, s'_{ij} \in K$, if $h(s_{ij}, s'_{ij}) \neq 0$, then the pair $\{F_{s_{ij}}, G_{s'_{ij}}\}$ is a nonsingular pair of quadratic over K such that $L_m \nmid \det(\lambda F_{s_{ij}} + \mu G_{s'_{ij}})$ for each $1 \leqslant m \leqslant t$.

□

Lemma 4.0.5. *Let $L_1, \dots, L_t \in K^{alg}[\lambda, \mu]$ be a finite collection (possibly empty) of linear forms such that for $i \neq j$, L_i and L_j and not multiplies of each other.*

Let $n \geqslant 1$ be a positive integer and d be an integer such that $0 \leqslant d \leqslant \frac{n-1}{2}$. Let $f, g \in \mathcal{O}_K[X_1, \dots, X_n]$ be quadratic forms. Suppose $\{f, g\}$ vanish on $span_K(e_1, \dots, e_d)$ (if $d = 0$ then we simply assert that $\{f, g\}$ vanish on the zero space.)

Let $j \geqslant 1$ be a positive integer. We can adjust the coefficients of f and g modulo π^j so that

1. *$\{f, g\}$ is nonsingular,*
2. *$L_i \nmid det(\lambda f + \mu g)$ for each $1 \leqslant i \leqslant t$, and*
3. *the pair $\{f, g\}$ still vanishes on $span_K(e_1, \dots, e_d)$.*

Proof. We will show that there exist quadratic forms $f', g' \in \mathcal{O}_K[X_1, \dots, X_n]$ such that $f' \equiv f \bmod \pi^j$, $g' \equiv g \bmod \pi^j$, and f', g' satisfy properties (1), (2), and (3).

Since $\{f, g\}$ vanish on $\text{span}_K(e_1, \dots, e_d)$, we can write f and g in the shape of equation 4.0.2:

$$f = \sum_{(i,j) \in U} a_{ij} X_i X_j$$
$$g = \sum_{(i,j) \in U} b_{ij} X_i X_j$$

for appropriate $a_{ij}, b_{ij} \in \mathcal{O}_K$. Let $h = h(t_{ij}, t'_{ij})$ be as Lemma 4.0.4. Since h is a nonzero polynomial over K^{alg}, Lemma 4.0.2 implies that for each $(i, j) \in U$, there exist $a'_{ij}, b'_{ij} \in \mathcal{O}_K$ such that $a'_{ij} \equiv a_{ij} \bmod \pi^j$, $b'_{ij} \equiv b_{ij} \bmod \pi^j$, and $h(a'_{ij}, b'_{ij}) \neq 0$. Let

$$f' = \sum_{(i,j) \in U} a'_{ij} X_i X_j.$$
$$g' = \sum_{(i,j) \in U} b'_{ij} X_i X_j.$$

Then $f' \equiv f \bmod \pi^j$ and $g' \equiv g \bmod \pi^j$. Since $h(a'_{ij}, b'_{ij}) \neq 0$, we know that $\{f', g'\}$ is nonsingular and $L_i \nmid \det(\lambda f' + \mu g')$ for each $1 \leqslant i \leqslant t$. By our definition of U in equation 4.0.1, we know $\{f', g'\}$ vanish on $\text{span}_K(e_1, \dots, e_d)$.

□

Using Lemma 4.0.5, we obtain the following result.

Lemma 4.0.6. *Let $L_1, \dots, L_t \in K^{alg}[\lambda, \mu]$ be a finite collection (possibly empty) of linear forms such that for $i \neq j$, L_i and L_j and not multiplies of each other.*

Let $n \geqslant 1$ and let $q_1, q_2 \in k[X_1, \dots, X_n]$ be quadratic forms. Suppose that $\{q_1, q_2\}$ vanish on a subspace over k of dimension d, where $0 \leqslant d \leqslant \frac{n-1}{2}$. There exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \dots, X_n]$ that satisfy the following properties.

1. $\overline{Q_1} = q_1$ *and* $\overline{Q_2} = q_2$.

2. $\{Q_1, Q_2\}$ *is nonsingular.*

3. $L_i \nmid det(\lambda Q_1 + \mu Q_2)$ *for each* $1 \leqslant i \leqslant t$

4. $D_K(Q_1, Q_2) \geqslant d$*; in particular,* $\{Q_1, Q_2\}$ *vanish on* $span_K(e_1, \ldots, e_d)$.

Proof. By a change of variables, we can assume that q_1 and q_2 both vanish on $\text{span}_k(e_1, \ldots, e_d)$. Therefore, we can express q_1 and q_2 in the following way:

$$q_1 = \sum_{i=1}^{d} X_i \ell_i(X_{d+1}, \ldots, X_n) + q_3(X_{d+1}, \ldots, X_n)$$

$$q_2 = \sum_{i=1}^{d} X_i s_i(X_{d+1}, \ldots, X_n) + q_4(X_{d+1}, \ldots, X_n)$$

for suitable linear forms ℓ_i, s_i and quadratic forms q_3, q_4, all defined over k. Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be lifts of q_1, q_2, respectively, such that 0 lifts to 0. Therefore, Q_1 and Q_2 have the shape

$$Q_1 = \sum_{i=1}^{d} X_i S_i(X_{d+1}, \ldots, X_n) + Q_3(X_{d+1}, \ldots, X_n)$$

$$Q_2 = \sum_{i=1}^{d} X_i T_i(X_{d+1}, \ldots, X_n) + Q_4(X_{d+1}, \ldots, X_n)$$

for suitable linear forms S_i, T_i and quadratic forms Q_3, Q_4, all defined over $\mathcal{O}_K$. In particular, we see that $\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \ldots, e_d)$. Since $0 \leqslant d \leqslant \frac{n-1}{2}$, we can apply Lemma 4.0.5 to the pair $\{Q_1, Q_2\}$ (in the lemma, we use $j = 1$). According to Lemma 4.0.5, we can adjust the coefficients of Q_1 and Q_2 modulo π so that $\{Q_1, Q_2\}$ is nonsingular, and the pair $\{Q_1, Q_2\}$ still vanishes on $\text{span}_K(e_1, \ldots, e_d)$. Thus $D_K(Q_1, Q_2) \geqslant d$. □

Chapter 5 Definition and Properties of Type $\mathcal{A}$ and $\mathcal{B}$ Pairs

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We will use the same notation given at the beginning of section 2.3.

Definition 5.0.1 (Type $\mathcal{A}$). *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be quadratic forms. The pair $\{Q_1, Q_2\}$ is said to be type $\mathcal{A}$ if there exist nonnegative integers d and h such that the following properties hold.*

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = d$.*
3. *$\{Q_1, Q_2\}$ vanish on $span_K(e_1, \ldots, e_d)$.*
4. *For every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there is an invertible linear change of variable over $\mathcal{O}_K$ so that*

$$\lambda Q_1 + \mu Q_2 = X_1X_2 + \cdots + X_{2h-1}X_{2h} + N(X_{2h+1}, \ldots, X_n)$$

   where $N \in \mathcal{O}_K[X_{2h+1}, \ldots, X_n]$ is a quadratic form such that $\overline{N}$ is anisotropic over k. Therefore, $H_K(Q_1, Q_2) = h$.

We will write $Q_i = Q_i(n, \mathcal{A}, d, h)$ to denote a type $\mathcal{A}$ pair.

Definition 5.0.2 (Type $\mathcal{B}$). *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be quadratic forms. The pair $\{Q_1, Q_2\}$ is said to be type $\mathcal{B}$ if there exist nonnegative integers d and h such that the following properties hold.*

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = d$.*
3. *$\{Q_1, Q_2\}$ vanish on $span_K(e_1, \ldots, e_d)$.*
4. *$H_k(\overline{Q_1}, \overline{Q_2}) = H_k(\overline{Q_1}) = h$.*
5. *For every $q \in \mathcal{P}_k(\overline{Q_1}, \overline{Q_2})$, $D_k(q) \leqslant h$.*

We will write $Q_i = Q_i(n, \mathcal{B}, d, h)$ to denote a type $\mathcal{B}$ pair.

Lemma 5.0.3. *Every type $\mathcal{A}$ pair is also a type $\mathcal{B}$ pair.*

Proof. Property (4) of Definition 5.0.1 implies that every form in $\mathcal{P}_k(q_1, q_2)$ has order n and splits off exactly h hyperbolic planes over k. This implies properties (4) and (5) of Definition 5.0.2. $\square$

Lemma 5.0.4. *Let $Q_i = Q_i(n, \mathcal{T}, d, h)$, $1 \leqslant i \leqslant 2$, where $\mathcal{T} \in \{\mathcal{A}, \mathcal{B}\}$, be a type $\mathcal{A}$ (or type $\mathcal{B}$) pair. Let $L_1, \ldots, L_t \in K^{alg}$ be a finite collection (possibly empty) of linear forms. We can adjust the coefficients of Q_1 and Q_2 modulo π so that $L_i \nmid det(\lambda Q_1 + \mu Q_2)$ and so that the pair $\{Q_1, Q_2\}$ remains a type $\mathcal{A}$ (or type $\mathcal{B}$) pair with the same values for d and h.*

Proof. By Lemma 4.0.5 with $j = 1$, we can adjust the coefficients of Q_1 and Q_2 modulo π so that $\{Q_1, Q_2\}$ remains nonsingular, $L_i \nmid \det(\lambda Q_1 + \mu Q_2)$ for each $1 \leqslant i \leqslant t$, and the pair $\{Q_1, Q_2\}$ still vanishes on $\text{span}_K(e_1, \ldots, e_d)$. Having $\{Q_1, Q_2\}$ still vanish on $\text{span}_K(Q_1, Q_2)$ implies that $D_K(Q_1, Q_2) \geqslant d$. On the other hand, since we adjusted the coefficients of Q_1 and Q_2 modulo π, we know that $D_k(q_1, q_2)$ is still equal to d. By Lemma 2.3.16, $D_K(Q_1, Q_2) \leqslant D_k(q_1, q_2) = d$. Thus $D_K(Q_1, Q_2) = D_k(q_1, q_2) = d$. Adjusting the coefficients modulo π does not affect property (4) of Definition 5.0.1 or properties (4) and (5) of Definition 5.0.2. $\square$

Lemma 5.0.5. *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms (not necessarily type $\mathcal{A}$ or $\mathcal{B}$). Let $Q'_i = Q'_i(n, \mathcal{T}, d, h)$, $1 \leqslant i \leqslant 2$, where $\mathcal{T} \in \{\mathcal{A}, \mathcal{B}\}$, be a type $\mathcal{A}$ (or type $\mathcal{B}$) pair. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. Then the coefficients of Q'_1 and Q'_2 can be adjusted modulo π so that the pair $\{f, g\}$ is nonsingular and so that the pair $\{Q'_1, Q'_2\}$ remains a type $\mathcal{A}$ (or type $\mathcal{B}$) pair with the same values for d and h.*

Proof. Since $\{Q'_1, Q'_2\}$ is nonsingular, Theorem 2.2.11 implies that $0 \leqslant d' \leqslant \frac{n'-1}{2}$. Since $\{Q_1, Q_2\}$ is nonsingular, Theorem 2.1.27 implies that $\det(\lambda Q_1 + \mu Q_2)$ has distinct linear factors. Suppose $L_1, \ldots, L_n \in K^{\text{alg}}$ are the linear factors in $\det(\lambda Q_1 + \mu Q_2)$. By Lemma 5.0.4, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $L_i \nmid \det(\lambda Q'_1 + \mu Q'_2)$, $1 \leqslant i \leqslant n$, and so that the pair $\{Q'_1, Q'_2\}$ remains a type $\mathcal{A}$ (or type $\mathcal{B}$) pair. It follows that $\det(\lambda f + \mu g)$ has no repeated linear factors, hence Theorem 2.1.27 implies that $\{f, g\}$ is nonsingular. $\square$

Lemma 5.0.6. *Let $Q_i = Q_i(n, \mathcal{A}, d, h)$, $1 \leqslant i \leqslant 2$, be a type $\mathcal{A}$ pair, and let $Q'_i = Q'_i(n', \mathcal{T}, d', h')$, $1 \leqslant i \leqslant 2$, where $\mathcal{T} \in \{\mathcal{A}, \mathcal{B}\}$, be a type $\mathcal{A}$ or $\mathcal{B}$ pair. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. Then the coefficients of Q'_1 and Q'_2 can be adjusted modulo π so that*

1. *$\{f, g\}$ is nonsingular,*
2. *$D_K(f, g) = d + d'$, and*
3. *$H_K(f, g) = h + h'$.*

Proof. By Lemma 5.0.3, every type $\mathcal{A}$ pair is also a type $\mathcal{B}$ pair. So without loss of generality, we can assume $\mathcal{T} = \mathcal{B}$.

(1) By Lemma 5.0.5, we can adjust the coefficients of Q'_1, Q'_2 modulo π so that $\{f, g\}$ is nonsingular and so that properties (1) - (5) in Definition 5.0.2 are preserved.

(2) Corollary 2.3.18 implies that $D_K(f,g) = d + d'$.

(3) By Definition 5.0.2, $H_k(q_1', q_2') = H_K(q_1') = h'$. By Lemma A.1.2, Q_1' splits off h' hyperbolic planes over $\mathcal{O}_K$. By Definition 5.0.1, the form Q_1 splits off h hyperbolic planes over $\mathcal{O}_K$. Therefore, f splits off $h + h'$ hyperbolic planes over $\mathcal{O}_K$, hence $H_K(f,g) \geqslant h + h'$.

To prove that $H_K(f,g) \leqslant h + h'$, it is sufficient to show that for every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, the form $\lambda f + \mu g$ splits off at most $h + h'$ hyperbolic planes. By Definition 5.0.1, we can perform an invertible linear change of variable over $\mathcal{O}_K$ so that

$$\lambda f + \mu g = X_1X_2 + \cdots + X_{2h-1}X_{2h} + N(X_{2h+1}, \ldots, X_n) \perp \pi(\lambda Q_1' + \mu Q_2').$$

Let $Q_0 = N(X_{2h+1}, \ldots, X_n) \perp \pi(\lambda Q_1' + \mu Q_2')$. By Lemma 2.3.2,

$$D_K(Q_0) \leqslant D_k(\overline{\lambda Q_1' + \mu Q_2'}).$$

By Definition 5.0.2,

$$D_k(\overline{\lambda Q_1' + \mu Q_2'}) \leqslant h'.$$

Therefore, Q_0 vanishes on a subspace over K of dimension at most h'. This proves that $\lambda f + \mu g$ splits off at most $h + h'$ hyperbolic planes. □

Lemma 5.0.7. *Let $Q_i = Q_i(n, \mathcal{B}, d, h)$, $1 \leqslant i \leqslant 2$, be a type $\mathcal{B}$ pair, and let $Q_i' = Q_i'(n', \mathcal{B}, d', h')$, $1 \leqslant i \leqslant 2$, be a type $\mathcal{B}$ pair. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. Suppose that $h + h' = \begin{cases} \frac{n+n'}{2} & \text{if } n+n' \text{ is even} \\ \frac{n+n'-1}{2} & \text{if } n+n' \text{ is odd.} \end{cases}$ Then the coefficients of Q_1' and Q_2' can be adjusted modulo π so that*

1. *$\{f, g\}$ is nonsingular,*
2. *$D_K(f,g) = d + d'$, and*
3. *$H_K(f,g) = h + h'$.*

Proof. (1) By Lemma 5.0.5, we can adjust the coefficients of Q_1', Q_2' modulo π so that $\{f, g\}$ is nonsingular and so that properties (1) - (5) in Definition 5.0.2 are preserved.

(2) Corollary 2.3.18 implies that $D_K(f,g) = d + d'$.

(3) Since $H_k(q_1) = h$ and $H_k(q_1') = h'$, Lemma A.1.2 implies that Q_1 splits off h hyperbolic planes and Q_2' splits off h' hyperbolic planes. Therefore, f splits off $h + h'$ hyperbolic planes, hence $H_K(f,g) \geqslant h + h'$. Since $h + h' = \begin{cases} \frac{n+n'}{2} & \text{if } n+n' \text{ is even} \\ \frac{n+n'-1}{2} & \text{if } n+n' \text{ is odd,} \end{cases}$ we deduce that $H_K(f,g) = h + h'$. □

Let F be a field and let K/F be an algebraic extension with $[K:F]=m$, $m \geqslant 1$. Let V be a finite dimensional vector space over K with $\dim_K(V)=t$. Then V is a vector space over F with $\dim_F(V)=mt$.

Let $s: K \to F$ be a nonzero F-linear map. That is, $s: K \to F$ is a nonzero linear transformation of F-vector spaces.

Let $Q: V \to K$ be a quadratic map. Thus

1. $Q(av)=a^2Q(v)$ for all $a \in K$ and $v \in V$.
2. $B_Q: V \times V \to K$ defined by $B_Q(v,w)=Q(v+w)-Q(v)-Q(w)$ for all $v,w \in V$ is a symmetric bilinear form.

This gives $B_Q(v,v)=Q(2v)-Q(v)-Q(v)=2Q(v)$ for all $v \in V$.

Define $s_*(Q): V \to F$ by $s_*(Q)(v)=s(Q(v))$ for all $v \in V$. We now show that $s_*(Q)$ is a quadratic map.

$$s_*(Q)(av)=s(Q(av))=s(a^2Q(v))=a^2s(Q(v))=a^2s_*(Q)(v).$$

$$\begin{aligned} B_{s_*(Q)}(v,w) &= s_*(Q)(v+w)-s_*(Q)(v)-s_*(Q)(w) \\ &= s(Q(v+w))-s(Q(v))-s(Q(w)) \\ &= s(Q(v+w)-Q(v)-Q(w))=s(B_Q(v,w)). \end{aligned}$$

Since s is a linear transformation, it follows easily that $B_{s_*(Q)}$ is a symmetric bilinear form.

Note that $s_*(Q)$ is a quadratic map corresponding to a quadratic form of dimension mt, which is $\dim_F(V)$.

Lemma 6.0.1. *Suppose $q \in K[X_1,\ldots,X_n]$ is a quadratic form and $s: K \to F$ be a nonzero F-linear map. Let $h=s_*(q)$. If b_q is nondegenerate, then $b_h=s_*(b_q)$ is also nondegenerate.*

Proof. We are assuming that b_q is nondegenerate. Therefore, there exists $(v,w) \in K \times K$ such that $b_q(v,w) \neq 0$. Since we are assuming that s is nonzero, there exists $a \in K$ such that $s(a) \neq 0$. Choose $c \in K$ so that $cb_q(v,w)=b_q(cv,w)=a$. Then $b_h(cv,w)=s_*(b_q(cv,w)) \neq 0$. This proves that b_h is nondegenerate. □

Lemma 6.0.2. *Suppose $q \in K[X_1,\ldots,X_n]$ is a quadratic form such that b_q is nondegenerate. Suppose $K=F(\theta)$ with $[K:F]=m>1$. Let $s: K \to F$ be a nonzero F-linear map, $f=s_*(q)$, and $g=s_*(\theta q)$. Then for every $\lambda,\mu \in F$, not both zero, the form $h=\lambda f+\mu g$ is nondegenerate. In particular, b_h is nondegenerate.*

Proof. Let $h = \lambda f + \mu g$. Observe that

$$\begin{aligned} h = \lambda f + \mu g &= \lambda s_*(q) + \mu s_*(\theta q). \\ &= s_*(\lambda q + \mu \theta q). \\ &= s_*((\lambda + \mu\theta)q). \end{aligned}$$

Since $m > 1$, we know that $\theta \notin F$. Thus $\lambda + \mu\theta \neq 0$. Because b_q is nondegenerate, we get that $b_{(\lambda+\mu\theta)q}$ is nondegenerate. Thus, Lemma 6.0.1 implies that b_h is nondegenerate, hence h is nondegenerate. □

Lemma 6.0.3. *Let F be an arbitrary field and let $n \geqslant 2$. Assume that F has a finite simple extension of degree n. There exist quadratic forms $h_1,\ h_2 \in F[X_1, \ldots, X_{2n}]$ such that*

1. *every form in the pencil $\mathcal{P}_F(h_1, h_2)$ splits off n hyperbolic planes, and*
2. *$D_F(h_1, h_2) = n$.*

Proof. Let $L = F(\theta)$ be a finite simple extension of degree n. Thus

$$L = \mathrm{span}_F(1, \theta, \ldots, \theta^{n-1}).$$

Let $q(X, Y) \in L[X, Y]$ be the quadratic form $q = XY$. Let $s : L \to F$ be a nonzero F-linear map. Take $h_1 = s_*(q)$ and $h_2 = s_*(\theta q)$. Then h_1 and h_2 are quadratic maps from $L^2 \to F$ of dimension $2n$. Observe that h_1 and h_2 both vanish on the subspace

$$U = \mathrm{span}_F\Big((1, 0), (\theta, 0), \ldots, (\theta^{n-1}, 0)\Big) \subset L^2.$$

Note that $\dim_F(U) = n$. Thus $D_F(h_1, h_2) \geqslant n$.

Next, we will show that every form in $\mathcal{P}_F(h_1, h_2)$ splits off n hyperbolic planes. Since $n \geqslant 2$, we deduce that $\theta \notin F$. It follows that $\lambda + \mu\theta \neq 0$ for all $\lambda, \mu \in F$, not both zero. Note $\lambda h_1 + \mu h_2 = s_*((\lambda + \mu\theta)q)$. Since $\lambda + \mu\theta \neq 0$, and q has rank 2, we deduce that $(\lambda + \mu\theta)q$ also has rank 2. Then Lemma 6.0.1 implies that $\lambda h_1 + \mu h_2$ has rank $2n$. Since h_1 and h_2 both vanish on U, the form $\lambda h_1 + \mu h_2$ also vanishes on U. Then Theorem B.1.1 implies that $\lambda h_1 + \mu h_2$ splits off n hyperbolic planes. This proves (1). In particular, every form$\mathcal{P}_F(h_1, h_2)$ has rank n. Thus, if $D_F(h_1, h_2) > n$, then Theorem B.1.1 would imply that every form in $\mathcal{P}_F(h_1, h_2)$ splits off $> n$ hyperbolic planes, which is note true. Thus $D_F(h_1, h_2) = n$, which proves (1). □

Let F be a field and let K/F be an algebraic extension with $[K : F] = m$, $m \geqslant 2$.

Recall that if $a_1, \ldots, a_n \in K^\times$, then $\langle a_1, \ldots, a_n \rangle$ denotes the quadratic form $a_1 x_1^2 + \cdots + a_n x_n^2$. From definitions 2.1.5 and 2.1.7, we get that

$$\det(\langle a_1, \ldots, a_n \rangle) = 2^n a_1 \cdots a_n.$$

In terms of quadratic maps, let $V = K^n$ and let $e_1, \ldots, e_n$ denote the standard basis of K^n. Define $Q : V \to K$ by setting $Q(e_i) = a_i$, $1 \leqslant i \leqslant n$, and $b_Q(e_i, e_j) = 0$ for all $i \neq j$.

Suppose that $K = F(\theta)$ for some $\theta \in K$. (If K/F is a separable extension, then this is always possible.) Let $j \in F[x]$ be the minimal polynomial satisfied by θ. Thus j is monic, irreducible, and $j(\theta) = 0$. Let $J(\lambda, \mu)$ denote the homogenization of j. It follows that

$$N_{K/F}(x - \theta) = j(x), \;\; N_{K/F}(\lambda - \mu\theta) = J(\lambda, \mu).$$

Let $s : K \to F$ be a nonzero F-linear map. Let $\beta \in K^\times$ and let

$$f = s_*(\langle \beta \rangle), \;\; g = s_*(\langle \beta\theta \rangle).$$

Then

$$\lambda f - \mu g = \lambda s_*(\langle \beta \rangle) - \mu s_*(\langle \beta\theta \rangle) = s_*(\langle \lambda\beta - \mu\beta\theta \rangle) = s_*(\beta\langle \lambda - \mu\theta \rangle).$$

We note that $\lambda - \mu\theta \neq 0$ for every $\lambda, \mu \in F$, not both zero, because $[F(\theta) : F] = m \geqslant 2$ and thus $1, \theta$ are linearly independent over F.

[17, Theorem 5.12, p. 51] implies that

$$\begin{aligned}
\det(\lambda f - \mu g) &= \det(s_*(\beta\langle \lambda - \mu\theta \rangle)) \\
&= \det(s_*(\langle 1 \rangle)) N_{K/F}(\det(\beta\langle \lambda - \mu\theta \rangle) \\
&= \det(s_*(\langle 1 \rangle)) N_{K/F}(2\beta(\lambda - \mu\theta)) \\
&= \det(s_*(\langle 1 \rangle)) N_{K/F}(2\beta) N_{K/F}(\lambda - \mu\theta) \\
&= 2^m \det(s_*(\langle 1 \rangle)) N_{K/F}(\beta) J(\lambda, \mu).
\end{aligned}$$

Since $[K : F] = [F(\theta) : F] = m$, it follows that $\{1, \theta, \ldots, \theta^{m-1}\}$ is an F-basis of K. Define the F-linear map $s : K \to F$ by

$$s(1) = \cdots = s(\theta^{m-2}) = 0, \;\; s(\theta^{m-1}) = 1.$$

Then [2, Lemma 2.3] implies that

$$\det(s_*(\langle 1 \rangle) = \begin{cases} 2^m(-1)^\ell & \text{if } m = 2\ell \\ 2^m(-1)^\ell & \text{if } m = 2\ell + 1. \end{cases}$$

We summarize the above results with the following theorem.

Theorem 6.0.4. *For any field F, let $K = F(\theta)$ be an extension of F of degree $m \geqslant 2$. Let $j(x) \in F[x]$ be the minimal polynomial of θ.*
Let $J(\lambda, \mu)$ denote the homogenization of $j(x)$.
Define the linear map $s : K \to F$ by $s(1) = s(\theta) = \cdots = s(\theta^{m-2}) = 0$ and $s(\theta^{m-1}) = 1$.

For the quadratic maps $f = s_*(\langle\beta\rangle)$ and $g = s_*(\langle\beta\theta\rangle)$, we have

$$det(\lambda f - \mu g) = 2^m det(s_*(\langle 1\rangle)) N_{K/F}(\beta) J(\lambda, \mu),$$

where

$$\det(s_*(\langle 1\rangle) = \begin{cases} 2^m(-1)^\ell & \text{if } m = 2\ell \\ 2^m(-1)^\ell & \text{if } m = 2\ell + 1. \end{cases}$$

In the next theorem, we find subspaces where the quadratic maps f and g vanish.

Theorem 6.0.5. *Assume that $K = F(\theta)$, $[K : F] = m \geqslant 2$, and define the F-linear map $s : K \to F$ by $s(1) = \cdots = s(\theta^{m-2}) = 0$, $s(\theta^{m-1}) = 1$.*

Let $f = s_*(\langle 1\rangle)$, $g = s_*(\langle\theta\rangle)$, and $h = s_*(\langle\theta^2\rangle)$. The following statements hold.

1. *f vanishes on* $\begin{cases} Span(1, \theta, \dots, \theta^{\frac{m-2}{2}}) & \text{if } m \text{ is even} \\ Span(1, \theta, \dots, \theta^{\frac{m-3}{2}}) & \text{if } m \text{ is odd.} \end{cases}$

2. *g vanishes on* $\begin{cases} Span(1, \theta, \dots, \theta^{\frac{m-4}{2}}) & \text{if } m \text{ is even, } m \geqslant 4, \\ Span(1, \theta, \dots, \theta^{\frac{m-3}{2}}) & \text{if } m \text{ is odd.} \end{cases}$

3. *h vanishes on* $\begin{cases} Span(1, \theta, \dots, \theta^{\frac{m-4}{2}}) & \text{if } m \text{ is even, } m \geqslant 4, \\ Span(1, \theta, \dots, \theta^{\frac{m-5}{2}}) & \text{if } m \text{ is odd, } m \geqslant 5. \end{cases}$

Proof. Let $\beta \in K$, and let $q = s_*(\langle\beta\rangle)$. Observe that

$$\begin{aligned} B_q(\theta^i, \theta^j) &= q(\theta^i + \theta^j) - q(\theta^i) - q(\theta^j). \\ &= s(\beta(\theta^i + \theta^j)^2) - s(\beta\theta^{2i}) - s(\beta\theta^{2j}). \\ &= s(2\beta\theta^{i+j}). \\ &= 2s(\beta\theta^{i+j}) \end{aligned}$$

For (1), take $\beta = 1$, and note that $s(\theta^{i+j}) = 0$ whenever $i + j \leqslant m - 2$.

For (2), take $\beta = \theta$, and note that $s(\theta^{i+j+1}) = 0$ whenever $i + j \leqslant m - 3$.

For (3), take $\beta = \theta^2$, and note that $s(\theta^{i+j+2}) = 0$ whenever $i + j \leqslant m - 4$. □

Chapter 7 Pairs of Quadratic Forms over Finite Fields

Our goal for this chapter to build examples of pairs of quadratic forms over finite fields.

Lemma 7.0.1. *Let k be a finite field and $n \geqslant 2$ be even. There exist quadratic forms $f, g \in k[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. *There are no forms in $\mathcal{P}_k(f,g)$ that vanish on a subspace over k of dimension $\frac{n+2}{2}$.*
2. $D_k(f,g) = \begin{cases} 0 & \text{if } n = 2 \\ \frac{n}{2} & \text{if } n \geqslant 4. \end{cases}$
3. $H_k(f,g) = H_k(f) = \frac{n}{2}$.
4. *If $n \geqslant 4$, then every form in $\mathcal{P}_k(f,g)$ splits off $\frac{n}{2}$ hyperbolic planes, hence every form in $\mathcal{P}_k(f,g)$ has rank n.*

Proof. For $n = 2$, let $f = X_1X_2$ and let $g \in k[X_1, X_2]$ be anisotropic. Then $D_k(f,g) = 0$, and $H_k(f,g) = H_k(f) = 1$. Also, note that f, g are linearly independent.

If there exist $\lambda, \mu \in k$, not both zero, such that $\lambda f + \mu g$ vanishes on a subspace over k of dimension 2, then $\lambda f + \mu g$ would vanish on k^2, hence $\lambda f + \mu g = 0$. This, however, is contrary to f, g being linearly independent. This completes the proof for $n = 2$.

For $n \geqslant 4$, note that as a finite field, k has a simple extension of degree $\frac{n}{2}$. Thus, Lemma 6.0.3 implies that there exist quadratic forms $f, g \in k[X_1, \ldots, X_n]$ such that $D_k(f,g) = \frac{n}{2}$ and every form in $\mathcal{P}_k(f,g)$ splits off $\frac{n}{2}$ hyperbolic planes. This implies that every form in $\mathcal{P}_k(f,g)$ has rank n. Theorem $B.1.1$ implies that there are no forms in $\mathcal{P}_k(f,g)$ that vanish on a subspace over k of dimension $\frac{n+2}{2}$. □

Recall from Definition 2.2.1 that $D_k(q)$ denotes the maximal dimension of a subspace in k^n on which q vanishes.

Lemma 7.0.2. *Let k be a finite field and $n \geqslant 2$ be even. There exist quadratic forms $f, g \in k[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. $D_k(f,g) = \frac{n-2}{2}$.
2. $H_k(f,g) = H_k(f) = \frac{n}{2}$.
3. $D_k(q) \leqslant \frac{n}{2}$ *for all* $q \in \mathcal{P}_k(f,g)$.

Proof. Let $n(X,Y) \in k[X,Y]$ be an anisotropic quadratic form. Lemma 7.0.1 provides an example for $n = 2$. We will do $n = 4$ last. For $n \geqslant 6$, let $q_1, q_2 \in k[X_1, \ldots, X_{n-2}]$ be as in Lemma 7.0.1. Take $f = q_1 + X_{n-1}X_n$ and $g = q_2 + n(X_{n-1}, X_n)$. Then $H_k(f,g) = H_k(f) = \frac{n}{2}$. Lemma 7.0.1 implies that $D_k(q_1,q_2) = \frac{n-2}{2}$. Thus $D_k(f,g) \geqslant \frac{n-2}{2}$. Note that g has order n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes. Thus, Theorem B.1.1 implies that g can not vanish on a subspace over k of dimension $\frac{n}{2}$, in which case $D_k(f,g) = \frac{n-2}{2}$. As for (1), Lemma 7.0.1 implies that every form in $\mathcal{P}_k(q_1,q_2)$ has order $n-2$. It follows that every form in $\mathcal{P}_k(f,g)$ has order $\geqslant n-1$. Then Lemma 2.2.6 implies that every form in $\mathcal{P}_k(f,g)$ vanishes on a subspace of dimension at most $\frac{n}{2}$, as desired.

For $n = 4$, consider

$$f = X_1X_2 + X_3X_4.$$

$$g = X_1X_3 + n(X_2, X_4).$$

Then $H_k(f,g) = H_k(f) = 2$. Note that $\{f,g\}$ both vanish on $\operatorname{span}(e_1)$, hence $D_k(f,g) \geqslant 1$. Since g has order 4 and splits off exactly 1 hyperbolic plane, we know from Theorem B.1.1 that g can not vanish on a two-dimensional subspace over k. Thus $D_k(f,g) = 1$. As for (1), we will show that every form in $\mathcal{P}_k(f,g)$ has order $\geqslant 3$. Then Lemma 2.2.6 implies (1).

Consider $\lambda f + \mu g$, where $\lambda, \mu \in k$, not both zero. If $\lambda = 0$, then $\mu \neq 0$ and this form has order 4. Assume $\lambda \neq 0$. We can multiply by λ^{-1}, so we consider the form $f + \mu' g$, where $\mu' = \lambda^{-1}\mu$. Observe that

$$f + \mu' g = X_1(X_2 + \mu' X_3) + X_3X_4 + \mu' n(X_2, X_4).$$

Apply the change of variables given by

$$Y_2 = X_2 + \mu' X_3$$

$$Y_i = X_i \qquad i \neq 2$$

to obtain

$$f + \mu' g = Y_1Y_2 + Y_3Y_4 + \mu' n(Y_2 - \mu' Y_3, Y_4).$$

We can write $\mu' n(Y_2 - \mu' Y_3, Y_4) = Y_2 \ell(Y_2, Y_3, Y_4) + \mu' n(-\mu' Y_3, Y_4)$ for some linear form ℓ over k. Apply the change of variable where Y_1 is replaced with $Y_1 - \ell(Y_2, Y_3, Y_4)$ to obtain

$$f + \mu' g = Y_1Y_2 + Y_3Y_4 + \mu' n(-\mu' Y_3, Y_4).$$

If $\mu' = 0$, then this form has order 4. If $\mu' \neq 0$, then observe that the coefficient of Y_4^2 in $\mu' n(\mu' Y_3, Y_4)$ is nonzero because n is anisotropic. It follows that $Y_3Y_4 + \mu' n(\mu' Y_3, Y_4)$ has order $\geqslant 1$, hence $f + \mu' g$ has order $\geqslant 3$. $\square$

Theorem 7.0.3. *Let $n \geqslant 6$ be even with $n \neq 8$. Let k be a finite field. There exist quadratic forms $f, g \in k[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. *$D_k(f,g) = \frac{n-2}{2}$.*

2. *Every form in $\mathcal{P}_k(f,g)$ has rank n.*

3. *$H_K(f,g) = \frac{n-2}{2}$; moreover, if $q \in \mathcal{P}_k(f,g)$, then q splits off exactly $\frac{n-2}{2}$ hyperbolic planes; that is,*

$$q = X_1X_2 + \cdots + X_{n-3}X_{n-2} + q_0(X_{n-1}, X_n),$$

where q_0 is anisotropic of rank 2 over k.

First, we will show that if Theorem 7.0.3 holds when $n \geqslant 6$ with $n \equiv 2 \bmod 4$, then the theorem holds when $n \geqslant 12$ with $n \equiv 0 \bmod 4$.

Lemma 7.0.4. *Assume Theorem* 7.0.3 *holds when $n \geqslant 6$ with $n \equiv 2 \bmod 4$. Then Theorem* 7.0.3 *holds when $n \geqslant 12$ with $n \equiv 0 \bmod 4$.*

Proof. Since $n \geqslant 12$ with $n \equiv 0 \bmod 4$, we get that $n-6 \geqslant 6$ and $n-6 \equiv 2 \bmod 4$. Let $f_0, g_0 \in k[X_1, \ldots, X_{n-6}]$ be quadratic forms satisfying Theorem 7.0.3. Thus, $\{f_0, g_0\}$ satisfy the following properties.

(i) $D_k(\overline{f_0}, \overline{g_0}) = \frac{n-8}{2}$.

(ii) For every $\lambda, \mu \in k$, not both zero, there is an invertible change of variable over k so that

$$\lambda f_0 + \mu g_0 = X_1X_2 + \cdots + X_{n-9}X_{n-8} + q_0(X_{n-7}, X_{n-6}),$$

where q_0 is anisotropic of rank 2 over k.

Let $q_1, q_2 \in k[X_{n-5}, \ldots, X_n]$ be as in Lemma 6.0.3; note that this Lemma can be applied since as a finite field, k has a finite simple extension of degree 3. From Lemma 6.0.3, we see that

(iii) $D_k(q_1, q_2) = 3$, and

(iv) every form in $\mathcal{P}_k(q_1, q_2)$ splits off 3 hyperbolic planes over k.

Let $f, g \in k[X_1, \ldots, X_n]$ be defined by

$$f = f_0 + q_1,$$

and

$$g = g_0 + q_2.$$

Properties (i) and (iii) imply that $D_k(f,g) \geqslant \frac{n-8}{2} + 3 = \frac{n-2}{2}$. Further, notice that properties (ii) and (iv) imply that every form in $\mathcal{P}_k(f,g)$ has rank n over k and splits off exactly $\frac{n-2}{2}$ hyperbolic planes over k, hence $H_k(f,g) = \frac{n-2}{2}$.

Notice that if $D_k(f,g) \geqslant \frac{n}{2}$, then every form in $\mathcal{P}_k(f,g)$ would vanish on a subspace of dimension $\frac{n}{2}$. Since every form in $\mathcal{P}_k(f,g)$ has rank n, Theorem B.1.1 implies that every form in $\mathcal{P}_k(f,g)$ would split off $\frac{n}{2}$ hyperbolic planes, a contradiction. Therefore, $D_k(f,g) = \frac{n-2}{2}$.

□

To prove Theorem 7.0.3 when $n \geqslant 6$ with $n \equiv 2 \bmod 4$, we consider the cases $\mathrm{char}(k) \neq 2$ and $\mathrm{char}(k) = 2$ separately.

Lemma 7.0.5. *Let k be a finite field of characteristic not 2. Let $n \geqslant 6$ with $n \equiv 2 \bmod 4$. There exist quadratic forms $f, g \in k[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. $D_k(f,g) = \frac{n-2}{2}$.
2. *Every form in $\mathcal{P}_k(f,g)$ has rank n.*
3. $H_K(f,g) = \frac{n-2}{2}$*; moreover, if $q \in \mathcal{P}_K(f,g)$, then q splits off exactly $\frac{n-2}{2}$ hyperbolic planes; that is,*

$$q = X_1X_2 + \cdots + X_{n-3}X_{n-2} + q_0(X_{n-1}, X_n),$$

where q_0 is anisotropic of rank 2 over k.

Proof. We can write $n = 2m$, where $m \geqslant 3$ is odd. Since k is a finite field, there exists a simple extension ℓ/k of degree m. Write $\ell = k(\theta)$, where $\theta \in \ell$. Since $m > 1$, we know $\theta \notin k$. Let $j(x) \in k[x]$ denote the minimal polynomial of θ over k. Let $J(\lambda, \mu)$ denote the homogenization of $j(x)$. Note that as a k-vector space, $\ell = \mathrm{span}_k(1, \theta, \ldots, \theta^{m-1})$. Define the linear map $s : \ell \to k$ by

$$s(1) = s(\theta) = \cdots = s(\theta^{m-2}) = 0 \qquad s(\theta^{m-1}) = 1.$$

Let $d \in k^\times$ be a nonsquare, which is possible since $|k| \geqslant 3$ and $\mathrm{char}(k) \neq 2$. Let $\beta = -d$.

Consider the following quadratic forms.

$$f_1 = s_*(\langle 1 \rangle) \qquad f_2 = s_*(\langle \beta \rangle)$$

$$g_1 = s_*(\langle \theta \rangle) \qquad g_2 = s_*(\langle \beta\theta \rangle).$$

Let $f = f_1 \perp f_2$ and $g = g_1 \perp g_2$. By Theorem 6.0.4, f and g are quadratic forms in $2m$ variables over k such that

$$\begin{aligned} \det(\lambda f - \mu g) &= 2^n \det(s_*(\langle 1 \rangle))^2 N_{\ell/k}(1) N_{\ell/k}(\beta) J(\lambda, \mu)^2 \\ &= 2^n (-1)^m d^m J(\lambda, \mu)^2. \end{aligned}$$

Since $j(x)$ is irreducible over k, we know $j(x)$ has no roots in k. Thus, if $\lambda, \mu \in k$, not both zero, then $J(\lambda, \mu) \neq 0$. It follows that for $\lambda, \mu \in k$, not both zero, $\det(\lambda f - \mu g) \neq 0$. This proves (2). To prove (3), note that since $m \geqslant 3$ is odd, we can write $d^m = d(d^2)^{\frac{m-1}{2}}$. It follows that $\det(\lambda f - \mu g) \in d(k^\times)^2$. Lemma $B.2.1$ implies (3).

To prove (1), let $U = \operatorname{span}_k(1, \theta, \dots, \theta^{\frac{m-3}{2}})$. By Theorem 6.0.5, $\{f_1, g_1\}$ vanishes on U. Note that since $\beta \in k$ and s is k-linear, we have $s_*(\beta) = \beta s_*(\langle 1 \rangle)$ and $s_*(\langle \beta\theta \rangle) = \beta s_*(\langle \theta \rangle)$. Then Theorem 6.0.5 implies that $\{f_2, g_2\}$ also vanishes on U. It follows that $\{f, g\}$ vanishes on a subspace of k^n of dimension $\frac{m-1}{2} + \frac{m-1}{2} = m - 1 = \frac{n-2}{2}$. Thus $D_k(f, g) \geqslant \frac{n-2}{2}$. By Lemma 2.2.7, $D_k(f, g) \leqslant H_K(f, g) = \frac{n-2}{2}$. Thus $D_k(f, g) = \frac{n-2}{2}$. □

Our goal now is to prove Lemma 7.0.5 for finite fields of characteristic 2.

Let k be a finite field of characteristic 2, and let ℓ/k be a finite extension. Let $\operatorname{tr} : \ell \to k$ be the trace map. Note that tr is a k-linear map. Since k is finite field, the extension ℓ/k is a separable extension. Then tr is a nonzero k-linear map. Recall that the Arf invariant is defined for quadratic forms over a finite field in an even number of variables when the associated symmetric bilinear form is nondegenerate. For a binary form $cX^2 + dXY + eY^2$ with $d \neq 0$, we have $\operatorname{Arf}(cX^2 + dXY + eY^2) = \frac{ce}{d^2}$. We have the following theorem.

Theorem 7.0.6. *$\operatorname{Arf}(s_*(q)) = \operatorname{tr}(\operatorname{Arf}(q))$.*

Proof. See [3, Lemma 2.3 (ii) and Corollary 2.6] and [19, Proposition 2.4]. □

Now assume that m, the degree of the extension ℓ/k, is odd and $\geqslant 3$. Since ℓ/k is separable, there exists $\theta \in \ell$ such that $\ell = k(\theta)$ (every finite exension of a perfect field is separable.) Note that as k-vector space, $\ell = \operatorname{span}_k(1, \theta, \dots, \theta^{m-1})$. Let $s : \ell \to k$ be the k-linear map defined by

$$s(1) = s(\theta) = \cdots = s(\theta^{m-2}) = 0 \text{ and } s(\theta^{m-1}) = 1.$$

Lemma 7.0.7. *Let $b \in \ell$ and $q_1 = X^2 + XY + bY^2$. Let $q_2 = \theta q_1 = \theta X^2 + \theta XY + \theta b Y^2$. Let $f = s_*(q_1)$ and $g = s_*(q_2)$, hence f and g are quadratic forms with coefficients in k in $n = 2m$ variables. The quadratic forms f and g both vanish on a subspace of k^n of dimension $\frac{n-2}{2}$.*

Proof. Consider the subspace

$$W = \operatorname{span}_k(1, \theta, \dots, \theta^{\frac{m-3}{2}}) \oplus \operatorname{span}_k(1, \theta, \dots, \theta^{\frac{m-3}{2}}) \subset \ell^2.$$

Thus $\dim_k(W) = m - 1$. We will show that f and g both vanish on W. Suppose $\{w_1, \dots, w_{m-1}\}$ is a k-basis for W. Let $x_1, \dots, x_{m-1} \in k$ and $w = x_1 w_1 + \cdots + x_{m-1} w_{m-1}$. Then

$$f(w) = \sum_{i=1}^{m-1} f(w_i) x_i^2 + \sum_{1 \leqslant i < j \leqslant m-1} b_f(w_i, w_j) x_i x_j,$$

and

$$g(w) = \sum_{i=1}^{m-1} g(w_i)x_i^2 + \sum_{1 \leqslant i < j \leqslant m-1} b_g(w_i, w_j)x_i x_j.$$

Therefore, to show that f and g both vanish on W, it is enough to show that $f(w_i) = g(w_i) = 0$ for each $1 \leqslant i \leqslant m-1$, and $b_f(w_i, w_j) = b_g(w_i, w_j) = 0$ for each $1 \leqslant i < j \leqslant m-1$.

To that end, we first choose a basis for W. We will use the basis

$$\{(1,0), (\theta, 0), \ldots, (\theta^{\frac{m-3}{2}}, 0), (0,1), (0,\theta), \ldots, (0, \theta^{\frac{m-3}{2}})\}.$$

Recall $q_1 = X^2 + XY + bY^2$, $f = s_*(q_1)$, and $g = s_*(\theta q_1)$. For $0 \leqslant i \leqslant \frac{m-3}{2}$, observe that

$$f(\theta^i, 0) = s(q_1(\theta^i, 0)) = s(\theta^{2i}),$$
$$f(0, \theta^i) = s(q_1(0, \theta^i)) = bs(\theta^{2i}),$$
$$g(\theta^i, 0) = s(\theta q_1(\theta^i, 0)) = s(\theta^{2i+1}),$$

and

$$g(0, \theta^i) = s(\theta q_1(0, \theta^i)) = bs(\theta^{2i+1}).$$

Since $2i \leqslant 2i+1 \leqslant m-2$, we have $s(\theta^{2i}) = s(\theta^{2i+1}) = 0$. We have shown that f and g both vanish on the basis vectors of W.

Now we consider b_f and b_g. Let $0 \leqslant i, j \leqslant \frac{m-3}{2}$, we already showed that $f(0, \theta^i) = f(\theta^i, 0) = g(\theta^i, 0) = g(0, \theta^i) = 0$. It follows that

$$\begin{aligned} b_f((0, \theta^i), (0, \theta^j)) &= f((0, \theta^i + \theta^j)). \\ &= s(q_1(0, \theta^i + \theta^j)). \\ &= bs(\theta^i + \theta^j)^2. \\ &= bs(\theta^{2i}) + bs(\theta^{2j}). \\ &= 0. \end{aligned}$$

Likewise, $b_g((0, \theta^i), (0, \theta^j)) = bs(\theta^{2i+1}) + bs(\theta^{2j+1}) = 0$. Similarly, we have

$$\begin{aligned} b_f((0, \theta^i), (\theta^j, 0)) &= f(\theta^j, \theta^i). \\ &= s(\theta^{2j} + \theta^{i+j} + b\theta^{2j}). \\ &= s(\theta^{2j}) + s(\theta^{i+j}) + bs(\theta^{2j}). \\ &= 0. \end{aligned}$$

Likewise, $b_g((0, \theta^i), (\theta^j, 0)) = s(\theta^{2j+1}) + s(\theta^{i+j+1}) + bs(\theta^{2j+1}) = 0$.

We have

$$\begin{aligned} b_f((\theta^i,0),(\theta^j,0)) &= f(\theta^i+\theta^j,0). \\ &= s((\theta^i+\theta^j)^2). \\ &= s(\theta^{2i}+\theta^{2j}). \\ &= s(\theta^{2i})+s(\theta^{2j}). \\ &= 0. \end{aligned}$$

Likewise, $b_g((\theta^i,0),(\theta^j,0)) = s(\theta^{2i+1}) + s(\theta^{2j}+1) = 0$.

Finally, we have

$$\begin{aligned} b_f((\theta^i,0),(0,\theta^j)) &= f(\theta^i,\theta^j). \\ &= s(\theta^{2i}+\theta^{i+j}+b\theta^{2j}). \\ &= s(\theta^{2i})+s(\theta^{i+j})+bs(\theta^{2j}). \\ &= 0. \end{aligned}$$

Likewise, $b_g((\theta^i,0),(0,\theta^j)) = s(\theta^{2i+1}) + s(\theta^{i+j+1}) + bs(\theta^{2j+1}) = 0$. This completes the proof of (1).

□

We are ready to prove a version of Lemma 7.0.5 for finite fields of characteristic 2.

Lemma 7.0.8. *Let k be a finite field of characteristic 2. Let $n \geqslant 6$ be even with $n \equiv 2 \bmod 4$. There exist quadratic forms $f, g \in k[X_1, \dots, X_n]$ that have the following properties.*

1. *f and g both vanish on a subspace of k^n of dimension $\frac{n-2}{2}$.*
2. *For every $\lambda, \mu \in k$, not both zero, let $h = \lambda f + \mu g$. Then b_h is nondegenerate; in particular, h is nondegenerate.*
3. *Every form in the pencil $\mathcal{P}_k(f,g)$ splits off exactly $m-1$ hyperbolic planes with a two-dimensional anisotropic binary form left over. Thus $H_k(f,g) = m-1 = \frac{n-2}{2}$, where $n = 2m$.*
4. *$D_k(f,g) = m-1 = \frac{n-2}{2}$, where $n = 2m$.*

Proof. Let $f = s_*(q_1)$ and $g = s_*(\theta q_1)$ be as in Lemma 7.0.7, hence $q_1 = X^2 + XY + bY^2$ where $b \in \ell$. Then Lemma 7.0.7 implies property (1). Lemma 6.0.2 implies property (2). To prove properties (3) and (4), we will choose a specific value for b.

We let $\wp(k)$ denote the Artin-Schreier subgroup of k. Thus $\wp(k) = \{a + a^2 \mid a \in k\}$ and $[k : \wp(k)] = 2$. Having $[k : \wp(k)] = 2$ implies that $\wp(k)$ is a proper subgroup of

k. Then there exists $b \in k$ such that $b \notin \wp(k)$. Thus $x^2 + x + b$ is irreducible over k. Since m is odd, $x^2 + x + b$ is also irreducible over ℓ (proof: suppose r is a root of $x^2 + x + b$. Then $[k(r) : k] = 2$, and since m is odd, this implies that $k(r) \nsubseteq \ell$, hence $x^2 + x + b$ has no roots in ℓ.)

Let $h = \lambda f + \mu g$. Since b_h is nondegenerate, we can take the Arf invariant of h. We will show that $\mathrm{Arf}(h) = b \notin \wp(k)$, which will prove (3). Observe

$$\begin{aligned}
\mathrm{Arf}(\lambda f + \mu g) &= \mathrm{Arf}(s_*((\lambda + \mu\theta)q_1)). \\
&= \mathrm{tr}(\mathrm{Arf}((\lambda + \mu\theta)q_1)). \\
&= \mathrm{tr}(\mathrm{Arf}((\lambda + \mu\theta)X^2 + (\lambda + \mu\theta)XY + (\lambda + \mu\theta)bY^2)). \\
&= \mathrm{tr}\left(\frac{(\lambda + \mu\theta)^2 b}{(\lambda + \mu\theta)^2}\right). \\
&= \mathrm{tr}(b). \\
&= mb. \\
&= b.
\end{aligned}$$

In the last equality, we used the fact that since $\mathrm{ch}(k) = 2$, and m is odd, $m = 1$ in the field k. Because $b \notin \wp(k)$, we get that for every $\lambda, \mu \in k$, not both zero, $\lambda f + \mu g$ is an orthogonal sum of $m - 1$ hyperbolic planes and an anisotropic binary form of dimension 2. This proves (3).

Finally, to prove (4), note that if $D_k(f, g) = \frac{n}{2}$, then every form in the pencil $\mathcal{P}_k(f, g)$ would vanish on a subspace of dimension $\frac{n}{2}$. From (2), we know that there is a form in the pencil $\mathcal{P}_k(f, g)$ that is nondegenerate (in fact every form is nondegenerate.) Theorem $B.1.1$ would then imply that there is a form in the pencil that splits off $\frac{n}{2}$ hyperbolic planes, which would be contrary to property (3).

□

Lemma 7.0.9. *Let k be a finite field of characteristic not 2. There exist quadratic forms $f, g \in k[x_1, x_2, x_3, x_4]$ such that the following conditions hold.*

1. *$\lambda f + \mu g$ has rank 4 for every $\lambda, \mu \in k$, not both zero.*
2. *If $q \in \mathcal{P}_k(f, g)$, then there is an invertible change of variable over k so that*

$$q = x_1 x_2 + n(x_3, x_4),$$

where $n(x_3, x_4)$ is anisotropic of rank 2 over k. Thus $H_k(f, g) = 1$.

3. *$D_k(f, g) = 0$.*

Proof. Let $k = F_q$ be the finite field with q elements, where q is odd since $\mathrm{char}(k) \neq 2$. Let $d \in \mathbb{F}_q^\times$ be a nonsquare. Then $\mathbb{F}_q^\times = (\mathbb{F}_q^\times)^2 \cup d(\mathbb{F}_q^\times)^2$. We can write $d = s^2 + t^2$, where $s, t \in \mathbb{F}_q$. Since d is a nonsquare, it follows that s, t are both nonzero.

Let

$$\begin{aligned} f &= \quad 2x_1x_2 + sx_3^2 + 2tx_3x_4 - sx_4^2 \\ g &= x_1^2 + dx_2^2 + \quad dx_3^2 + dx_4^2. \end{aligned}$$

Then

$$\begin{aligned} \det(\lambda f + \mu g) &= \det \begin{pmatrix} \mu & \lambda \\ \lambda & d\mu \end{pmatrix} \det \begin{pmatrix} d\mu + s\lambda & t\lambda \\ t\lambda & d\mu - s\lambda \end{pmatrix} \\ &= (d\mu^2 - \lambda^2)(d^2\mu^2 - s^2\lambda^2 - t^2\lambda^2) \\ &= (-1)(\lambda^2 - d\mu^2)(d^2\mu^2 - d\lambda^2) \\ &= (-1)(\lambda^2 - d\mu^2)(-d)(\lambda^2 - d\mu^2) \\ &= d(\lambda^2 - d\mu^2)^2. \end{aligned}$$

This calculation shows that for every $\lambda, \mu \in \mathbb{F}_q$, not both zero, $\lambda f + \mu g$ has rank 4 and nonsquare determinant d because $\lambda^2 - d\mu^2 \neq 0$ if λ, μ are not both zero.

To prove (3), let $q \in \mathcal{P}_{\mathbb{F}_q}(f, g)$. Then q has rank 4, and by Chevalley-Warning, q is isotropic. Thus q splits off at least 1 hyperbolic plane:

$$q = x_1x_2 + n(x_3, x_4),$$

where $n = n(x_3, x_4)$ has rank 2. Note $\det(n) = -\det(q) \in -d(\mathbb{F}_q)^\times$. This implies that n is anisotropic. This proves (3).

By Theorem B.1.1, there are no forms in $\mathcal{P}_k(f, g)$ that vanish on a 2-dimensional space over k, hence $D_k(f, g) \neq 2$. Theorem 2.2.12 implies that $D_k(f, g) \neq 1$. Thus $D_k(f, g) = 0$.

□

Lemma 7.0.10. *Let k be a finite field of characteristic 2. There exist quadratic forms $f, g \in k[x_1, x_2, x_3, x_4]$ such that the following conditions hold.*

1. *$\lambda f + \mu g$ has rank 4 for every $\lambda, \mu \in k$, not both zero.*
2. *If $q \in \mathcal{P}_k(f, g)$, then there is an invertible change of variable over k so that*

$$q = x_1x_2 + n(x_3, x_4),$$

where $n(x_3, x_4)$ is anisotropic of rank 2 over k. Thus $H_k(f, g) = 1$.

3. *$D_k(f, g) = 0$.*

Proof. Let $\ell = k(\theta)$ be an extension of k of degree 2. Thus $[\ell : k] = 2$. Let $s : \ell \to k$ be a nonzero k-linear map. Let $\beta \in \ell$ such that $\beta \notin \wp(\ell)$. Consider the quadratic form $q(x, y) = x^2 + xy + \beta y^2 \in \ell[x, y]$. Note that $\det(q) = -1 \neq 0$, hence the associated symmetric bilinear form b_q is nondegenerate. Take $f = s_*(q)$ and $g = s_*(\theta q)$. Then

Lemma 6.0.2 implies that for every $\lambda, \mu \in k$, not both zero, the form $h = \lambda f + \mu g$ is nondegenerate; in particular, b_h is nondegenerate. This proves (1). We can take the Arf invariant of h. Observe that

$$\begin{aligned}
\operatorname{Arf}(\lambda f + \mu g) &= \operatorname{Arf}(s_*((\lambda + \mu\theta)q)). \\
&= \operatorname{tr}(\operatorname{Arf}((\lambda + \mu\theta)q)). \\
&= \operatorname{tr}(\operatorname{Arf}((\lambda + \mu\theta)x^2 + (\lambda + \mu\theta)xy + (\lambda + \mu\theta)\beta y^2)). \\
&= \operatorname{tr}\left(\frac{(\lambda + \mu\theta)^2\beta}{(\lambda + \mu\theta)^2}\right). \\
&= \operatorname{tr}(\beta).
\end{aligned}$$

Lemma $F.2.1$ implies that since $\beta \notin \wp(\ell)$, we get $\operatorname{tr}(\beta) \notin \wp(k)$. This, combined with the fact that $\lambda f + \mu g$ has rank 4, implies that every form in the pencil $\mathcal{P}_K(f, g)$ splits off exactly 1 hyperbolic plane. This implies (2).

According to Theorem 2.2.12, if $D_k(f, g) = 1$, there would be a form in the pencil $\mathcal{P}_k(f, g)$ that splits off 2 hyperbolic planes, a contradiction. Likewise, Theorem $B.1.1$ implies that if $D_k(f, g) = 2$, then there would be a form in the pencil $\mathcal{P}_k(f, g)$ that splits off 2 hyperbolic planes, a contradiction. Thus $D_k(f, g) = 0$, which proves (3). □

For convienience, we combine Lemmas 7.0.9 and 7.0.10 to get the following.

Lemma 7.0.11. *Let k be a finite field. There exist quadratic forms $f, g \in k[x_1, x_2, x_3, x_4]$ such that the following conditions hold.*

1. *$\lambda f + \mu g$ has rank 4 for every $\lambda, \mu \in k$, not both zero.*
2. *If $q \in \mathcal{P}_k(f, g)$, then there is an invertible change of variable over k so that*

$$q = x_1x_2 + n(x_3, x_4),$$

   where $n(x_3, x_4)$ is anisotropic of rank 2 over k. Thus $H_k(f, g) = 1$.

3. *$D_k(f, g) = 0$.*

Proof. Lemma 7.0.9 proves the case where $\operatorname{char}(k) \neq 2$, and Lemma 7.0.10 proves the case where $\operatorname{char}(k) = 2$. □

Lemma 7.0.12. *Let k be a finite field. Let $n \geqslant 4$ be even with $n \neq 6$. There exist quadratic forms $f, g \in k[x_1, \ldots, x_n]$ such that the following conditions hold.*

1. *$D_k(f, g) = \frac{n-4}{2}$.*
2. *Every form in $\mathcal{P}_k(f, g)$ has order n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes over k. Thus $H_k(f, g) = \frac{n-2}{2}$.*

Proof. Let $q_3, q_4 \in k[X_1, \dots, X_4]$ be as in Lemma 7.0.11. Since $n - 4 \neq 2$, we can let $q_5, q_6 \in k[X_5, \dots, X_n]$ be as in Lemma 7.0.1. Let $q_1, q_2 \in k[X_1, \dots, X_n]$ be given by

$$q_1 = q_3(X_1, \dots, X_4) + q_5(X_5, \dots, X_n).$$

$$q_2 = q_4(X_1, \dots, X_4) + q_6(X_5, \dots, X_n).$$

By Lemma 7.0.11, every form in $\mathcal{P}_k(q_3, q_4)$ has order 4 and splits off exactly 1 hyperbolic plane. By Lemma 7.0.1, every form in $\mathcal{P}_k(q_5, q_6)$ has order $n-4$ and splits off exactly $\frac{n-4}{2}$ hyperbolic planes. Thus, every form in $\mathcal{P}_k(q_1, q_2)$ has order n and splits off eactly $\frac{n-2}{2}$ hyperbolic planes.

We will show that $D_k(q_1, q_2) = \frac{n-4}{2}$. Note that $\text{rank}(q_1) = n$. By Lemma 2.2.9, $D_k(q_1, q_2) = H_{k(t)}(q_1 + tq_2)$. To determine $H_{k(t)}(q_1 + tq_2)$, note that since $D_k(q_3, q_4) = 0$, Amer's Theorem (Theorem 2.2.8) implies that $q_3 + tq_4$ is anisotropic over $k(t)$. On the other hand, we have $D_k(q_5, q_6) = \frac{n-4}{2}$, and q_5 has rank $n-4$ over k. Thus, $q_5 + tq_6$ has rank $n-4$ over $k(t)$ and vanishes on a subspace over $k(t)$ of dimension $\frac{n-4}{2}$. Thus, Theorem $B.1.1$ implies that $q_5 + tq_6$ splits off $\frac{n-4}{2}$ hyperbolic planes over $k(t)$. Hence $q_1 + tq_2$ splits off exactly $\frac{n-4}{2}$ hyperbolic planes over $k(t)$ and so $D_k(q_1, q_2) = \frac{n-4}{2}$. □

Lemma 7.0.13. *Let k be a finite field. Let $n \geqslant 6$ be even with $n \neq 8$. There exist quadratic forms $f, g \in k[x_1, \dots, x_n]$ such that the following conditions hold.*

1. $D_k(f, g) = \frac{n-4}{2}$.
2. $H_k(f, g) = H_k(f) = \frac{n}{2}$.
3. *For every $q \in \mathcal{P}_k(f, g)$, we have $D_k(q) \leqslant \frac{n}{2}$.*

Proof. Note that $n - 2 \geqslant 4$ and $n - 2 \neq 6$. Thus, by Lemma 7.0.12, there exist quadratic forms $q_1, q_2 \in k[x_1, \dots, x_{n-2}]$ such that $D_k(q_1, q_2) = \frac{n-6}{2}$, and every form in $\mathcal{P}_k(q_1, q_2)$ has order $n-2$ and splits off exactly $\frac{n-4}{2}$ hyperbolic planes. Let $N(x_{n-1}, x_n)$ be an anisotropic quadratic form over k. Let

$$f = q_1(x_1, \dots, x_{n-2}) + N(x_{n-1}, x_n).$$
$$g = q_2(x_1, \dots, x_{n-2}).$$

By a change of variables, we can assume $q_1 = x_1x_2 + \cdots + x_{n-5}x_{n-4} + N'(x_{n-3}, x_{n-2})$, where N' is anisotropic over k. By Lemma $B.2.6$, $N'(x_{n-3}, x_{n-2}) + N(x_{n-1}, x_n)$ splits off 2 hyperbolic planes. It follows that $H_k(f, g) = H_k(f) = \frac{n}{2}$, which proves (2).

Observe that every form in $\mathcal{P}_k(f, g)$ either has order n and splits off $\frac{n}{2}$ hyperbolic planes or has order $n-2$ and splits off exactly $\frac{n-4}{2}$ hyperbolic planes. It follows that every form in $\mathcal{P}_k(f, g)$ vanishes on a subspace in k^n of dimension at most $\frac{n}{2}$, which proves (3).

It remains to prove that $D_k(f, g) = \frac{n-4}{2}$. By Lemma $B.2.13$, $D_k(f, g) \geqslant \frac{n-4}{2}$. For sake of contradiction, assume that $D_k(f, g) \geqslant \frac{n-2}{2}$. Then $\{f, g\}$ vanish on a subspace U in k^n of dimension $\frac{n-2}{2}$. Suppose $U = \text{span}_k(v_1, \ldots, v_d)$, where $d = \frac{n-2}{2}$ and $v_1, \ldots, v_d \in k^n$ are linearly independent. For each $1 \leqslant i \leqslant n$, let w_i denote the projection of v_i onto the first $n-2$ coordinates, hence $w_i \in k^{n-2}$.

Suppose $w_1, \ldots, w_d$ are linearly dependent. Then there exist $c_1, \ldots, c_d \in k$, not all zero, such that $\sum_{i=1}^{d} c_i w_i = 0$. Let $v = \sum_{i=1}^{d} c_i v_i$. Then $v = (0, \ldots, 0, a, b)$ for some $a, b \in k$. Since $f(v) = 0$, and N is anisotropic, we deduce that $a = b = 0$. Thus $v = 0$, which is contrary to $v_1, \ldots, v_d$ being linearly independent.

Therefore, $w_1, \ldots, w_d$ are linearly independent. Note that g vanishes on the subspace $\text{span}_k(w_1, \ldots, w_d)$. Thus g vanishes on a subspace in k^{n-2} of dimension $d = \frac{n-2}{2}$. Then Theorem $B.1.1$ implies that g splits off $\frac{n-2}{2}$ hyperbolic planes, a contradiction. We conclude that $D_k(f, g) = \frac{n-4}{2}$, as desired.

□

Results in this chapter shed some light on the relationship between $D_k(f, g)$ and $H_k(f, g)$ for pairs of quadratic forms $\{f, g\}$ defined over a finite field k. It could be of interest to investigate this relationship further. It is not exactly clear what additional properties one should require of the pair $\{f, g\}$. Should one require the pair to be nonsingular, as we have done for the p-adic field case? This could be addressed in a future project.

Chapter 8 Existence of Type $\mathcal{A}$ and $\mathcal{B}$ Pairs

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We will use the same notation given at the beginning of section 2.3.

In this chapter, we will prove the existence of various type $\mathcal{A}$ and type $\mathcal{B}$ pairs. Refer to Definitions 5.0.1 and 5.0.2 for the definitions of type $\mathcal{A}$ and type $\mathcal{B}$ pairs. The strategy is to start with a pair of forms over the residue field and then lift the pair up to the ring of integers.

8.1 Odd Number of Variables

Lemma 8.1.1. *Let $m \geqslant 0$ and $n = 2m + 1$. There exist quadratic forms $F, G \in \mathcal{O}_K[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. *The pair $\{F, G\}$ is nonsingular; moreover, $det(\lambda F + \mu G)$ is an irreducible form over K of degree n in λ, μ.*
2. $D_K(F, G) = D_k(\overline{F}, \overline{G}) = \frac{n-1}{2}$.
3. *$\{F, G\}$ vanish on $span_K(e_1, \ldots, e_{\frac{n-1}{2}})$.*
4. *$H_K(F, G) = H_k(\overline{F}, \overline{G}) = \frac{n-1}{2}$; moreover, for every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there is an invertible linear change of variable over $\mathcal{O}_K$ so that*

$$\lambda F + \mu G = X_1 X_2 + \cdots + X_{n-2} X_{n-1} + a X_n^2,$$

where $a \in \mathcal{O}_K$ is a unit.

5. *Every form in $\mathcal{P}_k(\overline{F}, \overline{G})$ has order n.*

Proof. Since k is a finite field, there exists a finite simple extension of k of degree n,. Suppose $\ell = k(\theta)$ is a finite simple extension of k and let $p(x) \in k[x]$ denote the minimal polynomial of θ. Thus $p(x)$ is monic and irreducible over k of degree n. Let $P(x) \in \mathcal{O}_K[x]$ be a lift of $p(x)$ such that 0 lifts to 0 and 1 lifts to 1. Lemma 4.0.1 implies that $P(x)$ is irreducible over K. Let $P(\lambda, \mu)$ denote the homogenization of $P(x)$; for instance, say $P(\lambda, \mu) = \lambda^n P(\lambda^{-1}\mu)$. Then $P(\lambda, \mu) \in \mathcal{O}_K[\lambda, \mu]$ is irreducible over K, and $P(\lambda, \mu)$ is homogeneous of degree n in λ, μ. It follows that $P(\lambda, \mu)$ has the following shape:

$$\begin{aligned} P(\lambda, \mu) = {} & a_{1+m}\lambda\mu^{2m} + b_{1+m}\mu^{2m+1} \\ & + a_{2+m}\lambda^3\mu^{2m-2} + b_{2+m}\lambda^2\mu^{2m-1} \\ & \vdots \\ & + a_{2m}\lambda^{2m-1}\mu^2 + b_{2m}\lambda^{2m-2}\mu^3 \\ & + a_{2m+1}\lambda^{2m+1} + b_{2m+1}\lambda^{2m}\mu, \end{aligned}$$

where each $a_i, b_i \in \mathcal{O}_K$ for $1 + m \leqslant i \leqslant 2m + 1$. Let $F, G \in \mathcal{O}_K[X_1, \dots, X_n]$ be the quadratic forms given by

$$\begin{aligned} F &= X_1X_{m+1} + X_2X_{m+2} + \cdots + X_mX_{2m} + \sum_{i=m+1}^{2m+1} a_iX_i^2. \\ G &= X_1X_{m+2} + X_2X_{m+3} + \cdots + X_mX_{2m+1} + \sum_{i=m+1}^{2m+1} b_iX_i^2. \end{aligned} \tag{8.1.1}$$

Theorem 3.0.1 implies that $\det(\lambda F + \mu G) = 2(-1)^m P(\lambda, \mu)$. Since $P(\lambda, \mu)$ is irreducible over K, and $\mathrm{char}(K) \neq 2$, we deduce that $\det(\lambda F + \mu G)$ has no repeated linear factors. Thus Theorem 2.1.27 implies that $\{F, G\}$ is a nonsingular pair, which proves (1).

Equation 8.1.1 implies that F and G both vanish on $\mathrm{span}_K(e_1, \dots, e_m) \subset K^n$, where $m = \frac{n-1}{2}$. Hence $D_K(F, G) \geqslant \frac{n-1}{2}$. Since $\{F, G\}$ is a nonsingular pair, Lemma 2.3.11 implies $D_K(F, G) \leqslant \frac{n-1}{2}$. Thus $D_K(F, G) = \frac{n-1}{2}$, which proves (2).

To prove (3), let $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π.

Claim: $\overline{\lambda F + \mu G}$ is nondegenerate; i.e., has order n.

First, we explain why (3) follows from the claim. Observe that if $\overline{\lambda F + \mu G}$ is nondegenerate, then there is an invertible linear change of variable over k so that

$$\overline{\lambda F + \mu G} = X_1X_2 + \cdots + X_{n-2}X_{n-1} + a'X_n^2,$$

where $a' \in k$ is nonzero. Lemma A.1.2 then implies (3).

To prove the claim, note that since $p(x)$ is irreducible over k, we see that $p(x)$ has no roots over k. It follows that $\pi \nmid P(\lambda, \mu)$. For $\mathrm{char}(k) \neq 2$, we deduce that $\det(\overline{\lambda F + \mu G}) \neq 0$, hence $\overline{\lambda F + \mu G}$ is nondegenerate. For $\mathrm{char}(k) = 2$, we see that $\det_{/2}(\overline{\lambda F + \mu G}) \neq 0$, hence $\overline{\lambda F + \mu G}$ is nondegenerate by [15, Prop 3.1, p.397].

Since $\mathcal{P}_k(\overline{F}, \overline{G})$ is nondegenerate, we deduce that every form in $\mathcal{P}_k(\overline{F}, \overline{G})$ has order n, which proves (4). □

Lemma 8.1.2. *Let $n \geqslant 1$ be odd. There exists a type $\mathcal{A}$ pair of quadratic forms in n variables with $d = h = \frac{n-1}{2}$.*

Proof. The pair $\{F, G\}$ from Lemma 8.1.1 satisfies Definition 5.0.1 with $d = h = \frac{n-1}{2}$. □

Lemma 8.1.3. *There exist quadratic forms $J_1, J_2 \in \mathcal{O}_K[X, Y, Z]$ that satisfy the following properties.*

1. $D_K(J_1, J_2) = D_k(\overline{J_1}, \overline{J_2}) = 0$.

2. *For $\lambda, \mu \in \mathcal{O}_K$, if λ is a unit, then there is an invertible linear change of variables over $\mathcal{O}_K$ so that*
$$\lambda J_1 + \mu J_2 = XY + eZ^2,$$
where e is some unit in $\mathcal{O}_K$.

3. *$J_2 \in \mathcal{O}_K[X, Y]$ and $\overline{J_2}$ is anisotropic of rank 2 over k.*

4. *For each $q \in \mathcal{P}_k(\overline{J_1}, \overline{J_2})$, we have $D_k(q) = 1$.*

Proof. Note that properties (2) and (3) imply (4).

Note that by Lemma 2.3.16, $D_K(J_1, J_2) \leqslant D_k(\overline{J_1}, \overline{J_2})$. So to prove (1), it is sufficient to show that $D_k(\overline{J_1}, \overline{J_2}) = 0$.

First, consider the case where $\text{char}(k) \neq 2$. Let $d \in k$ so that $d \neq 0$ and d is a nonsquare in k. Let $q_1(X, Y) = XY$ and $q_2(X, Y) = X^2 + dY^2$. Let $\lambda, \mu \in k$, not both zero. Observe that $\lambda q_1 + \mu q_2 = \mu X^2 + \lambda XY + d\mu Y^2$; therefore, the matrix of $q_1 + \mu q_2$ is
$$\begin{bmatrix} 2\mu & \lambda \\ \lambda & 2d\mu \end{bmatrix}.$$
It follows that $\det(\lambda q_1 + \mu q_2) = 4d\mu^2 - \lambda^2$. Since d is a nonsquare in k, we see that $\det(q_1 + \mu q_2)$ is an anisotropic quadratic form in the variables λ, μ over k. It follows that every form in the pencil $\mathcal{P}_k(q_1, q_2)$ has rank 2. Since q_1 and q_2 do not share any common factors, Lemma B.2.10 implies that there is a form $q_2'(X, Y) \in \mathcal{P}_k(q_1, q_2)$ such that $q_2'(X, Y)$ is anisotropic of rank 2 over k. There exists $q_1' \in \mathcal{P}_k(q_1, q_2)$ such that $\mathcal{P}_k(q_1, q_2) = \mathcal{P}_k(q_1', q_2')$.

Let $J_1(X, Y, Z) = Q_1'(X, Y) + Z^2$ and $J_2(X, Y, Z) = Q_2'(X, Y)$, where Q_1' and Q_2' are lifts of q_1' and q_2' to $\mathcal{O}_K[X, Y]$, respectively. Since $\overline{Q_2'}$ is anisotropic of rank 2, we see that $D_k(\overline{J_1}, \overline{J_2}) = 0$. Since every form in $\mathcal{P}_k(\overline{Q_1'}, \overline{Q_2'})$ has rank 2 over k, we conclude that every form in $\mathcal{P}_k(\overline{J_1}, \overline{J_2})$ has rank 2 or 3 over k and that $\overline{J_2}$ is the only form in $\mathcal{P}_k(\overline{J_1}, \overline{J_2})$ that has rank 2. Thus, if $\lambda, \mu \in \mathcal{O}_K$, with λ a unit, then $\text{rank}(\overline{\lambda J_1 + \mu J_2}) = 3$. By Chevalley-Warning, this form is isotropic. Then Theorem B.1.1 implies that $\overline{\lambda J_1 + \mu J_2} = XY + e'Z^2$, where $e' \in k$ is nonzero. Lemma A.1.2 gives us $\lambda J_1 + \mu J_2 = XY + eZ^2$, where e is a unit.

Now, suppose $\text{char}(k) = 2$. Let $c \in k$ be chosen so that $c \notin \wp(k)$. Let $j_1, j_2 \in k[X, Y, Z]$ be the quadratic forms
$$j_1 = XY + X^2 + c^3 Z^2,$$
and
$$j_2 = YZ + Y^2 + cZ^2.$$
Let $c' \in \mathcal{O}_K$ be so that $\overline{c'} = c$. Take
$$J_1 = XY + X^2 + (c')^3 Z^2,$$

and

$$J_2 = YZ + Y^2 + c'Z^2.$$

Thus $\overline{J_1} = j_1$ and $\overline{J_2} = j_2$. Notice that $YZ + Y^2 + cZ^2$ is anisotropic of rank 2 since its Arf invariant is c. Thus, if $j_2(x, y, z) = 0$, then $y = z = 0$. It follows that $D_k(j_1, j_2) = 0$.

Let $\lambda, \mu \in k$, not both zero. Let $j = \lambda j_1 + \mu j_2$. According to [15, Prop 3.1, p. 397], if the half-determinant of j is nonzero, then j is nondegenerate (that is, j has no singular zeros). We proceed by showing that if $\lambda \neq 0$, then the half-determinant of j is nonzero. Let $\lambda', \mu' \in \mathcal{O}_K$ be lifts of λ, μ, respectively. We have

$$\det{}_{/2}(\lambda j_1 + \mu j_2) = \overline{\frac{1}{2}\det(\lambda' J_1 + \mu' J_2)}.$$

Notice

$$\lambda' J_1 + \mu' J_2 = \lambda' XY + \lambda' X^2 + \mu' YZ + \mu' Y^2 + (\lambda'(c')^3 + c'\mu')Z^2.$$

Then the matrix of $\lambda' J_1 + \mu' J_2$ is

$$\begin{bmatrix} 2\lambda' & \lambda' & 0 \\ \lambda' & 2\mu' & \mu' \\ 0 & \mu' & 2((c')^3\lambda' + c'\mu') \end{bmatrix}.$$

It follows that

$$\det(\lambda' J_1 + \mu' J_2) = 2\lambda'\Big(4\mu'((c')^3\lambda' + c'\mu') - (\mu')^2\Big) - 2(\lambda')^2\Big((c')^3\lambda' + c'\mu'\Big).$$

$$\frac{1}{2}\det(\lambda' J_1 + \mu' J_2) = \lambda'\Big(4\mu'((c')^3\lambda' + c'\mu') - (\mu')^2\Big) - (\lambda')^2\Big((c')^3\lambda' + c'\mu'\Big).$$

Therefore,

$$\overline{\frac{1}{2}\det(\lambda' J_1 + \mu' J_2)} = \lambda\mu^2 + \lambda^2(c^3\lambda + c\mu).$$

$$= \lambda\Big(\mu^2 + c^3\lambda^2 + c\lambda\mu\Big).$$

The Arf invariant of $\mu^2 + c^3\lambda^2 + c\lambda\mu$ is $\frac{c^3}{c^2} = c \notin \wp(k)$; therefore, $\mu^2 + c^3\lambda^2 + c\lambda\mu$ is an anisotropic quadratic form in the variables λ, μ over k. It follows that the half-determinant of j is zero if and only if $\lambda = 0$. Thus, if $\lambda, \mu \in \mathcal{O}_K$, with λ a unit, then $\overline{\lambda J_1 + \mu J_2}$ is nondegenerate. By Chevalley-Warning, $\overline{\lambda J_1 + \mu J_2}$ is isotropic, hence this form vanishes on a one-dimensional subspace U over k. Every nonzero element of U is a nonsingular zero, hence Theorem B.1.1 implies that $\overline{\lambda J_1 + \mu J_2}$ splits off 1 hyperbolic plane, hence $\overline{\lambda J_1 + \mu J_2} = XY + e'Z^2$, where $e' \in k$. Since this form is nondegenerate, $e' \neq 0$. Lemma A.1.2 then gives us $\lambda J_1 + \mu J_2 = XY + eZ^2$, where e is a unit. This completes the proof.

□

Lemma 8.1.4. *There exists a type $\mathcal{B}$ pair of quadratic forms in $n = 3$ variables with $d = 0$ and $h = 1$.*

Proof. The pair $\{J_1, J_2\}$ from Lemma 8.1.3 satifies Definition 5.0.2 with $n = 3$, $d = 0$, and $h = 1$. □

8.2 Even Number of Variables

Lemma 8.2.1. *Let $n \geqslant 2$ be even. There exists a type $\mathcal{B}$ pair of quadratic forms in n variables with $d = \frac{n-2}{2}$ and $h = \frac{n}{2}$.*

That is, for $n \geqslant 2$ even, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ that satisfy the following properties.

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-2}{2}$.*
3. *$\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \ldots, e_{\frac{n-2}{2}})$.*
4. *$H_k(q_1, q_2) = H_k(q_1) = \frac{n}{2}$.*
5. *For every $q \in \mathcal{P}_k(q_1, q_2)$, $D_k(q) \leqslant \frac{n}{2}$.*

Proof. Let $q_1, q_2 \in k[X_1, \ldots, X_n]$ be as in Lemma 7.0.2. By Lemma 4.0.6, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ such that $\overline{Q_i} = q_i$, $\{Q_1, Q_2\}$ is nonsingular, and $\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \ldots, e_{\frac{n-2}{2}})$. Hence $D_K(Q_1, Q_2) \geqslant \frac{n-2}{2}$. Since $\{Q_1, Q_2\}$ is nonsingular, Theorem 2.2.11 implies that $D_K(Q_1, Q_2) < \frac{n}{2}$. Thus $D_K(Q_1, Q_2) = D_k(q_1, q_2) = \frac{n-2}{2}$. Properties (4) and (5) follow from Lemma 7.0.2. □

Lemma 8.2.2. *The pair $Q_i = Q_i(n, \mathcal{A}, \frac{n-2}{2}, \frac{n-2}{2})$ exist for $n \geqslant 6$ even, $n \neq 8$. That is, for $n \geqslant 6$ even with $n \neq 8$, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ that satisfy the following properties.*

1. *$\{Q_1, Q_2\}$ is a nonsingular pair over K.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-2}{2}$.*
3. *$\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \ldots, e_{\frac{n-2}{2}})$.*
4. *For every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there is an invertible linear change of variable over $\mathcal{O}_K$ so that*

$$\lambda Q_1 + \mu Q_2 = X_1X_2 + \cdots + X_{n-3}X_{n-2} + N(X_{n-1}, X_n),$$

where $\overline{N}$ is anisotropic of over k.

Proof. Let $q_1, q_2 \in k[X_1, \dots, X_n]$ be as Lemma 7.0.3. Thus $D_k(q_1, q_2) = \frac{n-2}{2}$ and every form in $\mathcal{P}_k(q_1, q_2)$ has rank n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes. By Lemma 4.0.6 with $d = \frac{n-2}{2}$, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \dots, X_n]$ such that $\overline{Q_i} = q_i$, $\{Q_1, Q_2\}$ is nonsingular, and $\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \dots, e_{\frac{n-2}{2}})$. Thus $D_K(Q_1, Q_2) \geqslant \frac{n-2}{2}$.

Since $\{Q_1, Q_2\}$ is nonsingular, Theorem 2.2.11 implies that $D_K(Q_1, Q_2) < \frac{n}{2}$. Thus $D_K(Q_1, Q_2) = \frac{n-2}{2} = D_K(q_1, q_2)$.

Since every form in $\mathcal{P}_k(q_1, q_2)$ has rank n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes, Lemma $A.1.2$ implies that for every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there is an invertible linear change of variables over $\mathcal{O}_K$ so that

$$\lambda Q_1 + \mu Q_2 = X_1 X_2 + \cdots + X_{n-3} X_{n-2} + N(X_{n-1}, X_n),$$

where $N \in \mathcal{O}_K[X_{n-1}, X_n]$ is a quadratic form such that $\overline{N}$ is anisotropic over k. Therefore, the pair $\{Q_1, Q_2\}$ is type $\mathcal{A}$ with $d = h = \frac{n-2}{2}$. $\square$

Lemma 8.2.3. *Let $n \geqslant 4$ be even with $n \neq 6$. There exists a type $\mathcal{A}$ pair of quadratic forms in n variables with $d = \frac{n-4}{2}$ and $h = \frac{n-2}{2}$.*

That is, for $n \geqslant 4$ even, $n \neq 6$, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \dots, X_n]$ that satisfy the following properties.

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-4}{2}$.*
3. *$\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \dots, e_{\frac{n-4}{2}})$.*
4. *For every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there exists an invertible linear change of variables over $\mathcal{O}_K$ so that*

   $$\lambda Q_1 + \mu Q_2 = X_1 X_2 + X_3 X_4 + \cdots + X_{n-3} X_{n-2} + N(X_{n-1}, X_n),$$

   where $\overline{N}$ is anisotropic over k.

Proof. Since $n \geqslant 4$ and $n \neq 6$, Lemma 7.0.12 implies that there exist quadratic forms $q_1, q_2 \in k[X_1, \dots, X_n]$ such that $D_k(q_1, q_2) = \frac{n-4}{2}$, and every form in $\mathcal{P}_k(q_1, q_2)$ has order n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes. By Lemma 4.0.6, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \dots, X_n]$ that satisfy the following properties.

1. $\overline{Q_1} = q_1$ and $\overline{Q_2} = q_2$.
2. $\{Q_1, Q_2\}$ is nonsingular.
3. $D_K(Q_1, Q_2) \geqslant \frac{n-4}{2}$; in particular, $\{Q_1, Q_2\}$ vanish on $\text{span}_K(e_1, \dots, e_{\frac{n-4}{2}})$.

By Lemma 2.3.16, $D_K(Q_1, Q_2) \leqslant D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-4}{2}$. Thus $D_K(Q_1, Q_2) = D_K(\overline{Q_1}, \overline{Q_2}) = \frac{n-4}{2}$. Since every form in $\mathcal{P}_k(q_1, q_2)$ has order n and splits off exactly $\frac{n-2}{2}$ hyperbolic planes over k, statement (2) of Lemma A.1.2 implies that for every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there exists an invertible linear change of variables over $\mathcal{O}_K$ so that

$$\lambda Q_1 + \mu Q_2 = X_1X_2 + X_3X_4 + \cdots + X_{n-3}X_{n-2} + N(X_{n-1}, X_n),$$

where $\overline{N}$ is anisotropic over k.

□

Lemma 8.2.4. *Let $n \geqslant 6$ be even with $n \neq 8$. There exists a type $\mathcal{B}$ pair of quadratic forms in n variables with $d = \frac{n-4}{2}$ and $h = \frac{n}{2}$.*

That is, for $n \geqslant 6$ even with $n \neq 8$, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ that satisfy the following properties.

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-4}{2}$.*
3. *$\{Q_1, Q_2\}$ vanish on span$_K(e_1, \ldots, e_{\frac{n-4}{2}})$.*
4. *$H_k(\overline{Q_1}, \overline{Q_2}) = H_k(\overline{Q_1}) = \frac{n}{2}$.*
5. *For every $q \in \mathcal{P}_k(\overline{Q_1}, \overline{Q_2})$, $D_k(q) \leqslant \frac{n}{2}$.*

Proof. Since $n \geqslant 6$ and $n \neq 8$, Lemma 7.0.13 implies that there exist quadratic forms $q_1, q_2 \in k[X_1, \ldots, X_n]$ with the following properties.

(i) $D_k(q_1, q_2) = \frac{n-4}{2}$.

(ii) $H_k(q_1, q_2) = H_k(q_1) = \frac{n}{2}$.

(iii) For every $q \in \mathcal{P}_k(q_1, q_2)$, $D_k(q) \leqslant \frac{n}{2}$.

By Lemma 4.0.6, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ such that $\overline{Q_i} = q_i$, $1 \leqslant i \leqslant 2$, $\{Q_1, Q_2\}$ is nonsingular, and $\{Q_1, Q_2\}$ vanish on the subspace span$_K(e_1, \ldots, e_{\frac{n-4}{2}})$. Thus $D_K(Q_1, Q_2) \geqslant \frac{n-4}{2}$. By Lemma 2.3.16, $D_K(Q_1, Q_2) \leqslant D_k(\overline{Q_1}, \overline{Q_2}) = \frac{n-4}{2}$. Thus $D_K(Q_1, Q_2) = \frac{n-4}{2}$. □

Lemma 8.2.5. *There exists a type $\mathcal{B}$ pair of quadratic forms in $n = 4$ variables with $d = 0$ and $h = 2$.*

That is, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_4]$ that satisfy the following properties.

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = D_k(\overline{Q_1}, \overline{Q_2}) = 0$.*

3. *$H_k(\overline{Q_1}, \overline{Q_2}) = H_k(\overline{Q_1}) = 2$.*

4. *For every $q \in \mathcal{P}_k(\overline{Q_1}, \overline{Q_2})$, $D_k(q) \leqslant 2$.*

Proof. Let $n(X,Y) \in k[X,Y]$ be an anisotropic quadratic form over k. Let $q_1 = n(X_1, X_2) + n(X_3, X_4)$ and $q_2 = n(X_1, X_2)$. If (x_1, x_2, x_3, x_4) is a common zero of q_1 and q_2 over k, then $q_2(x) = n(x_1, x_2) = 0$ implies that $x_1 = x_2 = 0$. Then $q_1(x) = n(x_3, x_4) = 0$ implies that $x_3 = x_4 = 0$. Thus $D_k(q_1, q_2) = 0$.

By Lemma B.2.6, q_1 splits off 2 hyperbolic planes. Thus $H_k(q_1, q_2) = H_k(q_1) = 2$. To prove (4), let $a, b \in k$, not both zero, and let $q = aq_1 + bq_2$. If $a = -b$, then $q = an(X_3, X_4)$. Since n is ansotropic, the form $q = an(X_3, X_4)$ can not vanish on a 3-dimensional subapce in k^4. If $a \neq -b$, then $q = (a+b)n(X_1, X_2) + an(X_3, X_4)$. If $a \neq 0$, then q has order 4, in which case q can not vanish on a subspace in k^4 of dimension 3. If $a = 0$, then $b \neq 0$ and $q = bn(X_1, X_2)$. As before, q can not vanish on a subsapce in k^4 of dimension 3. Thus, $D_k(q) \leqslant 2$ for all $q \in \mathcal{P}_k(q_1, q_2)$.

Lemma 4.0.6 implies that there exist quadratic forms Q_1, $Q_2 \in \mathcal{O}_K[X_1, \ldots, X_4]$ such that $\overline{Q_i} = q_i$ and $\{Q_1, Q_2\}$ is nonsingular. By Lemma 2.3.16, $D_K(Q_1, Q_2) \leqslant D_k(q_1, q_2) = 0$, hence $D_K(Q_1, Q_2) = D_k(q_1, q_2) = 0$. □

Chapter 9 n even

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We will use the same notation given at the beginning of section 2.3.

9.1 $D = \frac{n-2}{2}$

Theorem 9.1.1. *Let $n \geqslant 2$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-2}{2}$.*
3. *$H_K(f, g) = \frac{n}{2}$.*

Proof. Lemma 8.2.1 provides an example. □

Theorem 9.1.2. *Let $n \geqslant 6$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-2}{2}$.*
3. *$H_K(f, g) = \frac{n-2}{2}$.*

Theorem 2.2.14 *implies that there are no examples of quadratic forms satisfying these conditions for $n = 2$. Theorem* 2.3.15 *implies that there are no examples of quadratic forms satisfying these conditions for $n = 4$.*

Proof. Lemma 8.2.2 provides an example when $n \geqslant 6$ with $n \neq 8$.

Suppose $n = 8$. By Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(5, \mathcal{A}, 2, 2)$, $1 \leqslant i \leqslant 2$. Likewise, by Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q'_i = Q'_i(3, \mathcal{A}, 1, 1)$, $1 \leqslant i \leqslant 2$.

Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. Then Lemma 5.0.6 implies that we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = 2 + 1 = 3$, and $H_K(f, g) = 2 + 1 = 3$.

□

9.2 $D = \frac{n-4}{2}$

Theorem 9.2.1. *Let $n \geqslant 4$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-4}{2}$.*
3. *$H_K(f, g) = \frac{n}{2}$.*

Proof. By Lemma 8.2.1, there exist type $\mathcal{B}$ pairs $Q_i = Q_i(n-2, \mathcal{B}, \frac{n-4}{2}, \frac{n-2}{2})$, $1 \leqslant i \leqslant 2$, and $Q'_i = Q'_i(2, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. Lemma 5.0.7 implies that the coefficients of Q'_1 and Q'_2 can be adjusted modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-4}{2} + 1 = \frac{n-2}{2}$, and $H_K(f, g) = \frac{n-2}{2} + 1 = \frac{n}{2}$. ☐

Theorem 9.2.2. *Let $n \geqslant 4$ be even with $n \neq 6, 10$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-4}{2}$.*
3. *$H_K(f, g) = \frac{n-2}{2}$.*

Proof. If $n = 4$, then Lemma 8.2.3 provides an example.

Assume $n \geqslant 8$ and $n \neq 10$. Thus $n-2 \geqslant 6$ and $n-2 \neq 8$. By Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-2, \mathcal{A}, \frac{n-4}{2}, \frac{n-4}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q'_i = Q'_i(2, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-4}{2} + 0 = \frac{n-4}{2}$, and $H_K(f, g) = \frac{n-4}{2} + 1 = \frac{n-2}{2}$. ☐

Theorem 9.2.3. *Let $n = 6$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-4}{2} = 1$.*
3. *$H_K(f, g) = \frac{n-2}{2} = 2$.*

Proof. By Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(3, \mathcal{A}, 1, 1)$, $1 \leqslant i \leqslant 2$. By Lemma 8.1.4, there exists a type $\mathcal{B}$ pair $Q'_i = Q'_i(3, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = 1 + 0 = 1$, and $H_K(f, g) = 1 + 1 = 2$. ☐

Theorem 9.2.4. *Let $n = 10$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. $\{f, g\}$ *is nonsingular.*

2. $D_K(f, g) = \frac{n-4}{2} = 3.$

3. $H_K(f, g) = \frac{n-2}{2} = 4.$

Proof. By Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(6, \mathcal{A}, 2, 2)$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(4, \mathcal{B}, 1, 2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = 2 + 1 = 3$, and $H_K(f, g) = 2 + 2 = 4$. □

Theorem 9.2.5. *Let $n \geqslant 12$ be even with $n \neq 14$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. $\{f, g\}$ *is nonsingular.*

2. $D_K(f, g) = \frac{n-4}{2}.$

3. $H_K(f, g) = \frac{n-4}{2}.$

Proof. Note that $n - 6 \geqslant 6$ and $n - 6 \neq 8$. Thus, by Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n - 6, \mathcal{A}, \frac{n-8}{2}, \frac{n-8}{2})$, $1 \leqslant i \leqslant 2$. Also, by Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i' = Q_i'(6, \mathcal{A}, 2, 2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-8}{2} + 2 = \frac{n-4}{2}$, and $H_K(f, g) = \frac{n-8}{2} + 2 = \frac{n-4}{2}$. □

9.2.1 The Case $n = 14$

In this section, we will prove Theorem 9.2.5 for $n = 14$. We will do this by constructing a family of examples that satisfy Theorem 9.2.5 for $n \geqslant 14$, $n \neq 16$ (see Theorem 9.2.10).

Take $t \geqslant 1$. Suppose $f_1, g_1 \in k[X_1, \ldots, X_t]$ are quadratic forms such that every form in $\mathcal{P}_k(f_1, g_1)$ has order t and splits off $H_k(f_1, g_1)$ hyperbolic planes over k. Let $F_1, G_1 \in \mathcal{O}_K[X_1, \ldots, X_t]$ be quadratic forms such that $\overline{F_1} = f_1$ and $\overline{G_1} = g_1$. Let $N_1, N_2 \in \mathcal{O}_K[X, Y]$ be quadratic forms such that $\overline{N_1}$ and $\overline{N_2}$ are anisotropic over k. Thus each $\overline{N_i}$ has rank 2 over k, hence each N_i has rank 2 over K.

With the above notation, we will prove the following lemma.

Lemma 9.2.6. *Let Q_1, Q_2 be quadratic forms over $\mathcal{O}_K$ in $t + 8$ variables such that*

$$\begin{aligned} Q_1 &\equiv F_1(X_1, \ldots, X_t) + Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3 N_1(Y_3, Y_8) \bmod \pi^4, \\ Q_2 &\equiv G_1(X_1, \ldots, X_t) + Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2(Y_1, Y_4) \bmod \pi^4. \end{aligned} \tag{9.2.1}$$

Then $H_K(Q_1, Q_2) = H_k(f_1, g_1) + 3$. Further, every form in $\mathcal{P}_K(Q_1, Q_2)$ has rank $t + 8$ and splits off exactly $H_k(f_1, g_1) + 3$ hyperbolic planes.

Proof. Let $h = H_k(f_1, g_1)$. Let $\lambda, \mu \in K$, not both zero. We want to show that $\lambda Q_1 + \mu Q_2$ has rank $t+8$ and splits off exactly $h+3$ hyperbolic planes. By multiplying $\lambda Q_1 + \mu Q_2$ by a sufficient power of π, we can assume that $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π.

Case 1. Assume μ is a unit. By multiplying $\lambda Q_1 + \mu Q_2$ by μ^{-1}, it is sufficient to consider $Q = \lambda' Q_1 + Q_2$, where $\lambda' = \lambda\mu^{-1}$. Observe that

$$\begin{aligned} Q \equiv\ & \lambda' F_1 + G_1 + Y_2(\lambda' Y_1 + Y_3) + Y_5(\lambda' Y_4 + Y_6) + Y_7(\lambda' Y_6 + Y_8) \\ & + \lambda' \pi^3 N_1(Y_3, Y_8) + \pi N_2(Y_1, Y_4) \bmod \pi^4. \end{aligned}$$

Since $\overline{\lambda' F_1 + G_1}$ has order t and splits off exactly h hyperbolic planes, Lemma $A.1.2$ implies that there is an invertible linear change of variables over $\mathcal{O}_K$ involving the variables $X_1, \ldots, X_t$ so that

$$\lambda' F_1 + G_1 = X_1X_2 + \cdots + X_{2h-1}X_{2h} + G(X_{2h+1}, \ldots, X_t)$$

where $\overline{G}$ is anisotropic. Thus

$$\begin{aligned} Q \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G(X_{2h+1}, \ldots, X_t) \\ & + Y_2(\lambda' Y_1 + Y_3) + Y_5(\lambda' Y_4 + Y_6) + Y_7(\lambda' Y_6 + Y_8) \\ & + \lambda' \pi^3 N_1(Y_3, Y_8) + \pi N_2(Y_1, Y_4) \bmod \pi^4. \end{aligned}$$

Applying the change of variables given by

$$\begin{aligned} Z_3 &= \lambda' Y_1 + Y_3 \\ Z_6 &= \lambda' Y_4 + Y_6 \\ Z_8 &= \lambda' Y_6 + Y_8 \\ Z_i &= Y_i \qquad i \neq 3, 6, 8 \end{aligned}$$

gives us

$$\begin{aligned} Q \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G(X_{2h+1}, \ldots, X_t) \\ & + Z_2Z_3 + Z_5Z_6 + Z_7Z_8 \\ & + \lambda' \pi^3 N_1(Z_3 - \lambda' Z_1, Z_8 - \lambda' Z_6 + (\lambda')^2 Z_4) + \pi N_2(Z_1, Z_4) \bmod \pi^4. \end{aligned}$$

Thus

$$\begin{aligned} Q \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G(X_{2h+1}, \ldots, X_t) \\ & + Z_2Z_3 + Z_5Z_6 + Z_7Z_8 + \pi N_2(Z_1, Z_4) \bmod \pi^2. \end{aligned}$$

Lemma $A.1.2$ implies that there is an invertible linear change of variables over $\mathcal{O}_K$ so that

$$\begin{aligned} Q =\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} \\ & + Z_2Z_3 + Z_5Z_6 + Z_7Z_8 + Q_0(X_{2h+1}, \ldots, X_t, Z_1, Z_4), \end{aligned}$$

where

$$Q_0(X_{2h+1}, \dots, X_t, Z_1, Z_4) \equiv G(X_{2h+1}, \dots, X_t) + \pi N_2(Z_1, Z_4) \bmod \pi^2.$$

Since $\overline{G}$ and $\overline{N_2}$ are anisotropic over k, Lemma 2.3.1 implies that Q_0 is anisotropic over K, in which case Q has rank $t+8$ and splits off exactly $h+3$ hyperbolic planes.

Case 2. Assume $\pi \mid \mu$. Then λ is a unit. Write $\mu = \pi d$ for some $d \in \mathcal{O}_K$. By multiplying $\lambda Q_1 + \mu Q_2$ by λ^{-1}, it is sufficient to consider $Q' = Q_1 + \pi\mu' Q_2$, where $\mu' = \lambda^{-1} d$. Observe that

$$\begin{aligned} Q' \equiv\ & F_1 + \pi\mu' G_1 + Y_2(Y_1 + \pi\mu' Y_3) + Y_5(Y_4 + \pi\mu' Y_6) + Y_7(Y_6 + \pi\mu' Y_8) \\ & + \pi^3 N_1(Y_3, Y_8) + \pi^2\mu' N_2(Y_1, Y_4) \bmod \pi^4. \end{aligned}$$

Since $\overline{F_1 + \pi\mu' G_1}$ has order t and splits off exactly h hyperbolic planes over k, Lemma $A.1.2$ implies that there is an invertible linear change of variables over $\mathcal{O}_K$ involving $X_1, \dots, X_t$ so that

$$F_1 + \pi\mu' G_1 = X_1X_2 + \cdots + X_{2h-1}X_{2h} + G'(X_{2h+1}, \dots, X_h)$$

where $\overline{G'}$ is anisotropic. Thus

$$\begin{aligned} Q' \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G'(X_{2h+1}, \dots, X_h) \\ & + Y_2(Y_1 + \pi\mu' Y_3) + Y_5(Y_4 + \pi\mu' Y_6) + Y_7(Y_6 + \pi\mu' Y_8) \\ & + \pi^3 N_1(Y_3, Y_8) + \pi^2\mu' N_2(Y_1, Y_4) \bmod \pi^4. \end{aligned}$$

Applying the change of variables given by

$$\begin{aligned} Z_1 &= Y_1 + \pi\mu' Y_3 \\ Z_4 &= Y_4 + \pi\mu' Y_6 \\ Z_6 &= Y_6 + \pi\mu' Y_8 \\ Z_i &= Y_i \qquad i \neq 1, 4, 6 \end{aligned}$$

gives us

$$\begin{aligned} Q' \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G'(X_{2h+1}, \dots, X_h) \\ & + Z_2Z_1 + Z_5Z_4 + Z_7Z_6 \\ & + \pi^3 N_1(Z_3, Z_8) + \pi^2\mu' N_2(Z_1 - \pi\mu' Z_3, Z_4 - \pi\mu' Z_6 + \pi^2(\mu')^2 Z_8)) \bmod \pi^4. \end{aligned}$$

Next, we apply the change of variables where we multiply Z_3 by π^{-1} and multiply Z_8 by π^{-1}. This gives us

$$\begin{aligned} Q' \equiv\ & X_1X_2 + \cdots + X_{2h-1}X_{2h} + G'(X_{2h+1}, \dots, X_t) \\ & + Z_2Z_1 + Z_5Z_4 + Z_7Z_6 \\ & + \pi N_1(Z_3, Z_8) + \pi^2\mu' N_2(Z_1 - \mu' Z_3, Z_4 - \pi\mu' Z_6 + \pi(\mu')^2 Z_8)) \bmod \pi^2. \end{aligned}$$

Note that $N_2(Z_1 - \mu' Z_3, Z_4 - \pi\mu' Z_6 + \pi(\mu')^2 Z_8))$ has coefficients in $\mathcal{O}_K$. We have

$$\begin{aligned} Q' &\equiv X_1X_2 + \cdots + X_{2h-1}X_{2h} + G'(X_{2h+1}, \ldots, X_t) \\ &\quad + Z_2Z_1 + Z_5Z_4 + Z_7Z_6 \\ &\quad + \pi N_1(Z_3, Z_8) \bmod \pi^2. \end{aligned}$$

By Lemma $A.1.2$, there is an invertible linear change of variables over $\mathcal{O}_K$ so that

$$\begin{aligned} Q' &= X_1X_2 + \cdots + X_{2h-1}X_{2h} + Z_2Z_1 + Z_5Z_4 + Z_7Z_6 \\ &\quad Q_0'(X_{2h+1}, \ldots, X_t, Z_3, Z_8) \end{aligned}$$

where

$$Q_0' \equiv G'(X_{2h+1}, \ldots, X_t) + \pi N_1(Z_3, Z_8) \bmod \pi^2.$$

Since $\overline{G'}$ and $\overline{N_1}$ are anisotropic over k, Lemma 2.3.1 implies that Q_0' is anisotropic over K, in which case Q' has rank $t + 8$ and splits off exactly $h + 3$ hyperbolic planes. □

Next, we want to show that the coefficients of N_1 and N_2 can be adjusted modulo π so that the pair $\{J_1, J_2\}$ is nonsingular, where

$$\begin{aligned} J_1 &= Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3 N_1(Y_3, Y_8). \\ J_2 &= Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2(Y_1, Y_4). \end{aligned}$$

The following lemma will help us accomplish this.

Lemma 9.2.7. *Let Q_1', Q_2' be the quadratic forms given below.*

$$\begin{aligned} Q_1' &= Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3\beta_1Y_3Y_8, \\ Q_2' &= Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi\alpha_2Y_1^2 + \pi\gamma_2Y_4^2, \end{aligned}$$

where $\beta_1, \alpha_2, \gamma_2$ are indeterminants. Then $det(\lambda Q_1' + \mu Q_2') = \pi^6\beta_1^2\lambda^8 - 4\pi^2\alpha_2\gamma_2\mu^8$.

Proof. According to Definition 2.1.5, the 8×8 symmetric matrix associated to $\lambda Q_1' + \mu Q_2'$ is given by

$$M = \begin{bmatrix} 2\pi\alpha_2\mu & \lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ \lambda & 0 & \mu & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu & 0 & 0 & 0 & 0 & 0 & \pi^3\beta_1\lambda \\ 0 & 0 & 0 & 2\pi\gamma_2\mu & \lambda & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & 0 & \mu & 0 & 0 \\ 0 & 0 & 0 & 0 & \mu & 0 & \lambda & 0 \\ 0 & 0 & 0 & 0 & 0 & \lambda & 0 & \mu \\ 0 & 0 & \pi^3\beta_1\lambda & 0 & 0 & 0 & \mu & 0 \end{bmatrix}.$$

If we expand along the first row of M, we get

$$\det(M) = 2\pi\alpha_2\mu M_{11} - \lambda M_{12},$$

where M_{11} is the 7×7 matrix obtained by deleting row 1 and column 1 of M, and M_{12} is the 7×7 matrix obtained by deleting row 1 and column 2 of M.

Claim 1: $\det(M_{11}) = -2\pi\gamma_2\mu^7$.

To prove claim 1, expand along the first row of M_{11} to get

$$\det(M_{11}) = -\mu\det(A_6),$$

where A_6 is the resulting 6×6 matrix. We will describe the row/column to expand along at each step. Expand A_6 along its first column to get

$$\det(M_{11}) = (-\mu)(\mu)\det(A_5).$$

Expand A_5 along its last row to get

$$\det(M_{11}) = (-\mu)(\mu)(-\mu)\det(A_4).$$

Expand A_4 along its third row to get

$$\det(M_{11}) = (-\mu)(\mu)(-\mu)(-\mu)\det(A_3).$$

Expand A_3 along its last row to obtain

$$\det(M_{11}) = (-\mu)(\mu)(-\mu)(-\mu)(\mu)\det(A_2).$$

The determinant of 2×2 matrix A_2 is $2\pi\gamma_2\mu^2$. Thus $\det(M_{11}) = -2\pi\gamma_2\mu^7$.

Claim 2: $\det(M_{12}) = -\pi^6\beta_1^2\lambda^7$.

To prove claim 2, expand along the first column of M_{12} to get

$$\det(M_{12}) = \lambda\det(B_6)$$

where B_6 is the resulting 6×6 matrix. We will describe the row/column to expand along at each step. Expand B_6 along its first row to obtain

$$\det(M_{12}) = (\lambda)(-\pi^3\beta_1\lambda)\det(B_5).$$

Expand B_5 along its fourth row to get

$$\det(M_{12}) = (\lambda)(-\pi^3\beta_1\lambda)(-\lambda)\det(B_4).$$

Expand B_4 along its second row to obtain

$$\det(M_{12}) = (\lambda)(-\pi^3\beta_1\lambda)(-\lambda)(-\lambda)\det(B_3).$$

Expand B_3 along its first row to obtain

$$\det(M_{12}) = (\lambda)(-\pi^3\beta_1\lambda)(-\lambda)(-\lambda)(-\lambda)\det(B_2).$$

The determinant of the 2×2 matrix B_2 is $-\pi^3\beta_1\lambda^2$. Thus $\det(M_{12}) = -\pi^6\beta_1^2\lambda^7$.

□

Lemma 9.2.8. *Let J_1, J_2 be the quadratic forms given below.*

$$J_1 = Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3 N_1(Y_3, Y_8).$$
$$J_2 = Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2(Y_1, Y_4).$$

We can adjust the coefficients of N_1 and N_2 modulo π so that $\{J_1, J_2\}$ is nonsingular.

Proof. Suppose $N_1(X,Y) = a_1X^2 + b_1XY + c_1Y^2$ and $N_2(X,Y) = a_2X^2 + b_2XY + c_2Y^2$, where $a_i, b_i, c_i \in \mathcal{O}_K$, $1 \leqslant i \leqslant 2$. Let $\alpha_i, \beta_i, \gamma_i$, $1 \leqslant i \leqslant 2$, be indeterminants. Let

$$\begin{aligned} F &= Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3(\alpha_1Y_3^2 + \beta_1Y_3Y_8 + \gamma_1Y_8^2). \\ G &= Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi(\alpha_2Y_1^2 + \beta_2Y_1Y_4 + \gamma_2Y_4^2). \end{aligned} \tag{9.2.2}$$

Let $P(\lambda, \mu) = \det(\lambda F + \mu G)$. Thus $P(\lambda, \mu)$ is a homogeneous form in the variables λ, μ of degree 8. Let $h = \operatorname{discr}(P(\lambda, \mu))$. Lemma $D.2.5$ implies that h is a polynomial over $\mathcal{O}_K$ in the coefficients of F and G. Thus, h is a polynomial over $\mathcal{O}_K$ in the variables $\alpha_i, \beta_i, \gamma_i$, $1 \leqslant i \leqslant 2$; that is,

$$h \in \mathcal{O}_K[\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2].$$

We want to show that h is a nonzero polynomial. Let F', G' be the quadratic forms obtained by setting $\alpha_1 = \gamma_1 = \beta_2 = 0$ in equation 9.2.2, hence

$$F' = Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3\beta_1Y_3Y_8,$$

$$G' = Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi\alpha_2Y_1^2 + \pi\gamma_2Y_4^2.$$

To show that h is a nonzero polynomial, it is sufficient to find values for $\beta_1, \alpha_2, \gamma_2$ so that $\operatorname{discr}(\det(\lambda F' + \mu G')) \neq 0$. By Lemma $D.1.2$, this amounts to finding values for $\beta_1, \alpha_2, \gamma_2 \in K^{\text{alg}}$ so that $\det(\lambda F' + \mu G')$ has distinct linear factors. Lemma 9.2.7 implies that

$$\det(\lambda F' + \mu G') = \pi^6\beta_1^2\lambda^8 - 4\pi^2\alpha_2\gamma_2\mu^8.$$

Choose $\beta_1, \alpha_2, \gamma_2 \in K^{\text{alg}}$ so that $\det(\lambda F' + \mu G') = \lambda^8 - \mu^8$. Since $\lambda^8 - \mu^8$ has distinct linear factors over K^{alg}, we deduce that h is a nonzero polynomial, as desired.

Since h is nonzero, Lemma 4.0.2 implies that there exist $a_i', b_i', c_i' \in \mathcal{O}_K$, $1 \leqslant i \leqslant 2$ such that h evaluated at a_i', b_i', c_i', $1 \leqslant i \leqslant 2$ is nonzero and so that

$$a_i' \equiv a_i \bmod \pi,$$

$$b_i' \equiv b_i \bmod \pi,$$

$$c_i' \equiv c_i \bmod \pi.$$

Let $N_1'(Y_3, Y_8) = a_1'Y_3^2 + b_1'Y_3Y_8 + c_1'Y_8^2$ and $N_2'(Y_1, Y_4) = a_2'Y_1^2 + b_2'Y_1Y_4 + c_2'Y_4^2$. Thus $N_1' \equiv N_1 \bmod \pi$ and $N_2' \equiv N_2 \bmod \pi$. Let

$$J_1' = Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3N_1'(Y_3, Y_8).$$
$$J_2' = Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2'(Y_1, Y_4).$$

Since h evaluated at a_i', b_i', c_i', $1 \leqslant i \leqslant 2$, is nonzero, we deduce that $\{J_1', J_2'\}$ is a nonsingular pair; this pair is obtained by adjusting the coefficients of N_1 and N_2 modulo π.

□

Lemma 9.2.9. *Let $t \geqslant 1$. Suppose $f_1, g_1 \in k[X_1, \ldots, X_t]$ are quadratic forms such that every form in $\mathcal{P}_k(f_1, g_1)$ has order t and splits off exactly $H_k(f_1, g_1)$ hyperbolic planes over k. Assume $D_k(f_1, g_1) \leqslant \frac{t-1}{2}$. There exist quadratic forms F, G over $\mathcal{O}_K$ in $t+8$ variables that satisfy the following properties.*

1. *$\{F, G\}$ is nonsingular.*
2. *$D_K(F, G) \geqslant D_k(f_1, g_1) + 3$.*
3. *$H_K(F, G) = H_k(f_1, g_1) + 3$.*

Proof. Let J_1, J_2 be as in Lemma 9.2.8; that is,

$$J_1 = Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3 N_1(Y_3, Y_8).$$
$$J_2 = Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2(Y_1, Y_4).$$

By Lemma 9.2.8, we can adjust the coefficients of N_1 and N_2 modulo π so that $\{J_1, J_2\}$ is nonsingular. By Theorem 2.1.27, $\det(\lambda J_1 + \mu J_2)$ has distinct linear factors. Suppose $L_1, \ldots, L_8 \in K^{\text{alg}}[\lambda, \mu]$ are the distinct linear factors of $\det(\lambda J_1 + \mu J_2)$.

Let $d = D_k(f_1, g_1)$. Since $d \leqslant \frac{t-1}{2}$, Lemma 4.0.6 implies that there exist quadratic forms $F_1, G_1 \in \mathcal{O}_K[X_1, \ldots, X_t]$ with the following properties.

1. $\overline{F_1} = f_1$ and $\overline{G_1} = g_1$.
2. $\{F_1, G_1\}$ is nonsingular.
3. $L_i \nmid \det(\lambda F_1 + \mu G_1)$ for each $1 \leqslant i \leqslant 8$.
4. $D_K(F_1, G_1) \geqslant d$.

Let

$$F = F_1(X_1, \ldots, X_t) + J_1(Y_1, \ldots, Y_8).$$
$$G = G_1(X_1, \ldots, X_t) + J_2(Y_1, \ldots, Y_8).$$

Then $\{F, G\}$ is nonsingular. Notice that $\{J_1, J_2\}$ vanish whenever $Y_1 = Y_3 = Y_4 = Y_6 = Y_8 = 0$. Thus, $\{J_1, J_2\}$ vanish on a three-dimensional space over K, hence $D_K(J_1, J_2) \geqslant 3$. We have

$$\begin{aligned} D_K(F, G) &\geqslant D_K(F_1, G_1) + D_K(J_1, J_2) \\ &\geqslant D_k(f_1, g_1) + 3. \end{aligned}$$

Lemma 9.2.6 implies that $H_K(F, G) = H_k(f_1, g_1) + 3$. □

Theorem 9.2.10. *Let $n \geqslant 14$ be even with $n \neq 16$. There exists a pair of quadratic forms $\{F, G\}$ over K in n variables with the following properties:*

1. *$\{F, G\}$ is nonsingular.*
2. *$D_K(F, G) = \frac{n-4}{2}$.*
3. *$H_K(F, G) = \frac{n-4}{2}$.*

Proof. Let $t \geqslant 6$ with $t \neq 8$. Let $f_1, g_1 \in k[X_1, \ldots, X_t]$ be quadratic forms satisfying Theorem 7.0.3. Therefore, $D_k(f_1, g_1) = \frac{t-2}{2}$, every form in $\mathcal{P}_k(f_1, g_1)$ has rank (hence order) t, and every form in $\mathcal{P}_k(f_1, g_1)$ splits off exactly $H_k(f_1, g_1) = \frac{t-2}{2}$ hyperbolic planes.

By Lemma 9.2.9, there exist quadratic form F, G defined over $\mathcal{O}_K$ in $n = t + 8$ variables such that $\{F, G\}$ is nonsingular, $D_K(F, G) \geqslant \frac{t-2}{2}+3$, and $H_K(F, G) = \frac{t-2}{2}+3$. Since $\{F, G\}$ is nonsingular, Lemma 2.3.11 implies that $D_K(F, G) \leqslant H_K(F, G) = \frac{t-2}{2} + 3$. Thus $D_K(F, g) = \frac{t-2}{2} + 3$. Observe that

$$\frac{t-2}{2} + 3 = \frac{t+4}{2} = \frac{n-4}{2}.$$

□

In particular, taking $t = 6$ in Theorem 9.2.10 implies that Theorem 9.2.5 holds for $n = 14$, as desired.

We end this section by giving an alternate proof of Theorem 10.2.2.

Theorem 9.2.11. *Let $n \geqslant 9$ be odd. There exists a pair of quadratic forms $\{F, G\}$ over K in n variables with the following properties:*

1. *$\{F, G\}$ is nonsingular.*
2. *$D_K(F, G) = \frac{n-3}{2}$.*
3. *$H_K(F, G) = \frac{n-3}{2}$.*

Proof. Let $t \geqslant 1$ be odd. Let $F_1, G_1 \in \mathcal{O}_K[X_1, \ldots, X_t]$ be quadratic forms satisfying Lemma 8.1.1. Let $f_1 = \overline{F_1}$ and $g_1 = \overline{G_1}$. Lemma 8.1.1 implies that $D_k(f_1, g_1) = \frac{t-1}{2}$ and every form in $\mathcal{P}_k(f_1, g_1)$ has order t. It follows that every form in $\mathcal{P}_k(f_1, g_1)$ splits off exactly $H_k(f_1, g_1) = \frac{t-1}{2}$ hyperbolic planes.

By Lemma 9.2.9, there exist quadratic form F, G defined over $\mathcal{O}_K$ in $n = t + 8$ variables such that $\{F, G\}$ is nonsingular, $D_K(F, G) \geqslant \frac{t-1}{2}+3$, and $H_K(F, G) = \frac{t-1}{2}+3$. Since $\{F, G\}$ is nonsingular, Lemma 2.3.11 implies that $D_K(F, G) \leqslant H_K(F, G) = \frac{t-1}{2} + 3$. Thus $D_K(F, g) = \frac{t-1}{2} + 3$. Observe that

$$\frac{t-1}{2} + 3 = \frac{t+5}{2} = \frac{n-3}{2}.$$

□

9.3 $D = \frac{n-6}{2}$

Theorem 9.3.1. *Let $n \geqslant 6$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-6}{2}$.*
3. *$H_K(f, g) = \frac{n}{2}$.*

Proof. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q_i = Q_i(n-4, \mathcal{B}, \frac{n-6}{2}, \frac{n-4}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.5, there exists a type $\mathcal{B}$ pair $Q'_i = Q'_i(4, \mathcal{B}, 0, 2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.7, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-6}{2} + 0 = \frac{n-6}{2}$, and $H_K(f, g) = \frac{n-4}{2} + 2 = \frac{n}{2}$. □

Theorem 9.3.2. *Let $n \geqslant 6$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-6}{2}$.*
3. *$H_K(f, g) = \frac{n-2}{2}$.*

Proof. By Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q'_i = Q'_i(n-4, \mathcal{B}, \frac{n-6}{2}, \frac{n-4}{2})$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = 0 + \frac{n-6}{2} = \frac{n-6}{2}$, and $H_K(f, g) = 1 + \frac{n-4}{2} = \frac{n-2}{2}$. □

Theorem 9.3.3. *Let $n \geqslant 10$ be even with $n \neq 12$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-6}{2}$.*
3. *$H_K(f, g) = \frac{n-4}{2}$.*

Proof. Note that $n-4 \geqslant 6$ and $n-4 \neq 8$. Thus, by Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-4, \mathcal{A}, \frac{n-6}{2}, \frac{n-6}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q'_i = Q'_i(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-6}{2} + 0 = \frac{n-6}{2}$, and $H_K(f, g) = \frac{n-6}{2} + 1 = \frac{n-4}{2}$. □

9.3.1 The Case $n = 12$

In this section, our goal is to prove the case where $n = 12$ in Theorem 9.3.3. Therefore, we will prove the following theorem.

Theorem 9.3.4. *There exists a pair of quadratic forms $\{Q_1, Q_2\}$ over K in 12 variables with the following properties:*

1. *$\{Q_1, Q_2\}$ is nonsingular.*
2. *$D_K(Q_1, Q_2) = 3$.*
3. *$H_K(Q_1, Q_2) = 4$.*

We begin the proof now. Throughout this section, let $N_1(X, Y) \in \mathcal{O}_K[X, Y]$ and $N_2(X, Y) \in \mathcal{O}_K[X, Y]$ denote quadratic forms such that $\overline{N_1}$ and $\overline{N_2}$ are anisotropic over k. Let $G_1, G_2 \in \mathcal{O}_K[X_1, \ldots, X_4]$ be a type $\mathcal{A}$ pair of quadratic forms satisfying Lemma 8.2.3; therefore, G_1, G_2 satisfy the following properties.

(P0) $\{G_1, G_2\}$ is nonsingular.

(P1) $D_K(G_1, G_2) = D_k(g_1, g_2) = 0$, where $g_i = \overline{G_i}$.

(P2) For every $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π, there is an invertible linear change of variables over $\mathcal{O}_K$ so that

$$\lambda G_1 + \mu G_2 = X_1X_2 + N(X_3, X_4),$$

where $\overline{N}$ is anisotropic of rank 2 over k. Consequently, $H_K(G_1, G_2) = 1$.

We start with Q_1 and Q_2 given below.

$$\begin{aligned} Q_1 &= G_1(X_1, \ldots, X_4) + X_6X_5 + X_9X_8 + X_{11}X_{10} \\ &\quad + \pi^3 N_1(X_7, X_{12}). \\ Q_2 &= G_2(X_1, \ldots, X_4) + X_6X_7 + X_9X_{10} + X_{11}X_{12} \\ &\quad + \pi N_2(X_5, X_8). \end{aligned} \tag{9.3.1}$$

Let J_1, J_2 be as in Lemma 9.2.8; that is,

$$\begin{aligned} J_1 &= Y_2Y_1 + Y_5Y_4 + Y_7Y_6 + \pi^3 N_1(Y_3, Y_8). \\ J_2 &= Y_2Y_3 + Y_5Y_6 + Y_7Y_8 + \pi N_2(Y_1, Y_4). \end{aligned}$$

By Lemma 9.2.8, we can adjust the coefficients of N_1 and N_2 modulo π so that $\{J_1, J_2\}$ is nonsingular. Observe that

$$\begin{aligned} Q_1 &= G_1(X_1, \ldots, X_4) + J_1(X_5, \ldots, X_{12}). \\ Q_2 &= G_2(X_1, \ldots, X_4) + J_2(X_5, \ldots, X_{12}). \end{aligned}$$

By Lemma 5.0.5, we can adjust the coefficients of G_1 and G_2 modulo π so that the pair $\{Q_1, Q_2\}$ is nonsingular and so that $\{G_1, G_2\}$ remain a type $\mathcal{A}$ pair satisfying properties (P0), (P1), and (P2) above.

Lemma 9.3.5. *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_{12}]$ be as in equation* 9.3.1. *Then $H_K(Q_1, Q_2) = 4$. In particular, every form in $\mathcal{P}_K(Q_1, Q_2)$ has rank 12 and splits off exactly 4 hyperbolic planes over K.*

Proof. This follows from Lemma 9.2.6 with $t = 4$ and $H_k(f_1, g_1) = 1$. □

All that is left is to show that $D_K(Q_1, Q_2) = 3$.

Lemma 9.3.6. *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_{12}]$ be as in equation* 9.3.1. *Then $D_K(Q_1, Q_2) = 3$.*

Proof. For convenience, we restate equation 9.3.1 below:

$$\begin{aligned}
Q_1 &= G_1(X_1, \ldots, X_4) + X_6X_5 + X_9X_8 + X_{11}X_{10} \\
&\quad + \pi^3 N_1(X_7, X_{12}) \\
Q_2 &= G_2(X_1, \ldots, X_4) + X_6X_7 + X_9X_{10} + X_{11}X_{12} \\
&\quad + \pi N_2(X_5, X_8).
\end{aligned}$$

Note that N_1 has rank 2 over K. Property (P2) implies that G_1 has rank 4 over K. Thus Q_1 has rank 12 over K. It follows that $Q_1 + tQ_2$ has rank 12 over $K(t)$. By Lemma 2.2.9, we have $D_K(Q_1, Q_2) = H_{K(t)}(Q_1 + tQ_2)$. Therefore, it is sufficient to show that $Q_1 + tQ_2$ splits off exactly 3 hyperbolic planes over $K(t)$. Observe that

$$\begin{aligned}
Q_1 + tQ_2 = (G_1 + tG_2)(X_1, \ldots, X_4) + X_6(X_5 + tX_7) + X_9(X_8 + tX_{10}) \\
+ X_{11}(X_{10} + tX_{12}) + \pi^3 N_1(X_7, X_{12}) + t\pi N_2(X_5, X_8).
\end{aligned}$$

Consider the following invertible linear change of variables:

$$\begin{aligned}
Y_5 &= X_5 + tX_7 \\
Y_8 &= X_8 + tX_{10} \\
Y_{10} &= X_{10} + tX_{12} \\
Y_i &= X_i \quad i \neq 5, 8, 10.
\end{aligned}$$

Applying this change of variables gives us

$$\begin{aligned}
Q_1 + tQ_2 \sim (G_1 + tG_2)(Y_1, \ldots, Y_4) + Y_6Y_5 + Y_9Y_8 + Y_{11}Y_{10} \\
+ \pi^3 N_1(Y_7, Y_{12}) + t\pi N_2\big(Y_5 - tY_7, Y_8 - tY_{10} + t^2Y_{12}\big),
\end{aligned} \tag{9.3.2}$$

where $\sim$ denotes equivalence over $K(t)$. We can write $t\pi N_2\big(Y_5 - tY_7, Y_8 - tY_{10} + t^2Y_{12}\big)$ in the following way:

$$\begin{aligned}
t\pi N_2\big(Y_5 - tY_7, Y_8 - tY_{10} + t^2Y_{12}\big) &= t^3\pi N_2(-Y_7, tY_{12}) \\
&\quad + Y_5 L_1(Y_5, Y_7, Y_8, Y_{10}, Y_{12}) \\
&\quad + Y_8 L_2(Y_5, Y_7, Y_8, Y_{10}, Y_{12}) \\
&\quad + Y_{10} L_3(Y_5, Y_7, Y_8, Y_{10}, Y_{12}).
\end{aligned}$$

for suitable linear forms $L_i \in (\mathcal{O}_K[t])[Y_5, Y_7, Y_8, Y_{10}, Y_{12}]$, $1 \leqslant i \leqslant 3$. Substituting this into equation 9.3.2 yields

$$\begin{aligned} Q_1 + tQ_2 \sim (G_1 + tG_2)&(Y_1, \ldots, Y_4) + Y_6Y_5 + Y_9Y_8 + Y_{11}Y_{10} \\ &+ \pi^3 N_1(Y_7, Y_{12}) + t^3\pi N_2(-Y_7, tY_{12}) \\ &+ Y_5L_1(Y_5, Y_7, Y_8, Y_{10}, Y_{12}) \\ &+ Y_8L_2(Y_5, Y_7, Y_8, Y_{10}, Y_{12}) \\ &+ Y_{10}L_3(Y_5, Y_7, Y_8, Y_{10}, Y_{12}). \end{aligned} \tag{9.3.3}$$

Consider the following change of variables:

$$\begin{aligned} Z_6 &= Y_6 + L_1(Y_5, Y_7, Y_8, Y_{10}, Y_{12}). \\ Z_9 &= Y_9 + L_2(Y_5, Y_7, Y_8, Y_{10}, Y_{12}). \\ Z_{11} &= Y_{11} + L_3(Y_5, Y_7, Y_8, Y_{10}, Y_{12}). \\ Z_i &= Y_i \quad i \neq 6, 9, 11. \end{aligned} \tag{9.3.4}$$

Note that this change of variables is invertible. Applying this change of variables to equation 9.3.3 gives us

$$\begin{aligned} Q_1 + tQ_2 \sim (G_1 + tG_2)&(Z_1, \ldots, Z_4) + Z_6Z_5 + Z_9Z_8 + Z_{11}Z_{10} \\ &+ \pi^3 N_1(Z_7, Z_{12}) + t^3\pi N_2(-Z_7, tZ_{12}). \end{aligned} \tag{9.3.5}$$

Suppose $N_2(X, Y) = aX^2 + bXY + cY^2$ for some $a, b, c \in \mathcal{O}_K$. Since $\overline{N_2}$ is anisotropic over k, we know $\pi \nmid a$ and $\pi \nmid c$. Substituting this into equation 9.3.5 yields

$$\begin{aligned} Q_1 + tQ_2 \sim (G_1 + tG_2)&(Z_1, \ldots, Z_4) + Z_6Z_5 + Z_9Z_8 + Z_{11}Z_{10} \\ &+ \pi^3 N_1(Z_7, Z_{12}) + t^3\pi\big(aZ_7^2 - btZ_7Z_{12} + ct^2Z_{12}^2\big). \end{aligned} \tag{9.3.6}$$

Let

$$\begin{aligned} Q(Z_1, \ldots, Z_4, Z_7, Z_{12}) = (G_1 + tG_2)&(Z_1, \ldots, Z_4) + \pi^3 N_1(Z_7, Z_{12}) \\ &+ t^3\pi\big(aZ_7^2 - btZ_7Z_{12} + ct^2Z_{12}^2\big). \end{aligned}$$

To finish, we will show that Q is anisotropic over $K(t)$.

For sake of contradiction, suppose $Q(z_1, \ldots, z_4, z_7, z_{12}) = 0$, where $z_i \in K(t)$, not all zero. By multiplying $(z_1, \ldots, z_4, z_7, z_{12})$ by a suitable polynomial in $K[t]$, we can assume that each $z_i \in K[t]$ (i.e. clearing the denominators). Then we can multiply $(z_1, \ldots, z_4, z_7, z_{12})$ by a sufficient power of π so that each $z_i \in \mathcal{O}_K[t]$. Thus, each z_i is a polynomial in t with coefficients in $\mathcal{O}_K$. Let ϵ_i be the minimum valuation of the coefficients of z_i. Let $M = \min(\epsilon_1, \ldots, \epsilon_4, \epsilon_7, \epsilon_{12})$. Multiply $(z_1, \ldots, z_4, z_7, z_{12})$ by π^{-M}. These maneuvers allow us to assume that at least one of the z_i's is not divisible by π.

We have

$$(G_1 + tG_2)(z_1, \ldots, z_4) + \pi^3 N_1(z_7, z_{12}) + t^3\pi\left(az_7^2 - btz_7z_{12} + ct^2z_{12}^2\right) = 0.$$

Thus, $\pi \mid (G_1 + tG_2)(z_1, \ldots, z_4)$. Since $D_k(g_1, g_2) = 0$, Lemma 2.2.8 implies that $g_1 + tg_2$ is anisotropic over $k(t)$. It follows that $\pi \mid z_i$, $1 \leqslant i \leqslant 4$. Write $z_i = \pi z_i'$ for some $z_i' \in \mathcal{O}_K[t]$, $1 \leqslant i \leqslant 4$. We have

$$\pi^2(G_1 + tG_2)(z_1', \ldots, z_4') + \pi^3 N_1(z_7, z_{12}) + t^3\pi\left(az_7^2 - btz_7z_{12} + ct^2z_{12}^2\right) = 0.$$

It follows that

$$\pi \mid az_7^2 - btz_7z_{12} + ct^2z_{12}^2.$$

Let $F(X,Y) = aX^2 - btXY + ct^2Y^2$. Thus $\pi \mid F(z_7, z_{12})$. To finish we will show that

$$\overline{F}(X,Y) = \overline{a}X^2 - \overline{b}tXY + \overline{c}t^2Y^2$$

is anisotropic over $k(t)$. This will complete the proof since having $\overline{F}$ anisotropic over $k(t)$ implies that $\pi \mid z_7, z_{12}$, in which case all the z_i are divisible by π, a contradiction.

Suppose that $\overline{F}(x,y) = 0$ for some $x, y \in k(t)$. We have

$$\overline{a}x^2 - \overline{b}txy + \overline{c}t^2y^2 = 0.$$

Recall that $\pi \nmid a$ and $\pi \nmid c$, hence $\overline{a} \neq 0$ and $\overline{c} \neq 0$. Thus, $t \mid x$. Write $x = tx'$ for some $x' \in k(t)$. Then

$$t^2\left(\overline{a}(x')^2 - \overline{b}x'y + \overline{c}y^2\right) = 0.$$

Thus $\overline{a}(x')^2 - \overline{b}x'y + \overline{c}y^2 = 0$. Recall that $\overline{N_2}(X,Y) = \overline{a}X^2 + \overline{b}XY + \overline{c}Y^2$ is anisotropic over k. Let $N_2'(X,Y) = \overline{a}X^2 - \overline{b}XY + \overline{c}Y^2$. Then N_2' is equivalent over k to $\overline{N_2}$, which can be seen by performing a change of variable where Y is replaced with $-Y$. Thus N_2' is also anisotropic over k. Further, Lemma 2.2.15 implies that N_2' is also anisotropic over $k(t)$. We have $N_2'(x', y) = 0$, hence $x' = y = 0$. This proves that $\overline{F}$ is anisotropic over $k(t)$, as desired.

□

9.4 $D = \frac{n-8}{2}$

Theorem 9.4.1. *Let $n \geqslant 8$ be even. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties.*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-8}{2}$.*
3. *$H_K(f, g) = \frac{n}{2}$.*

Proof. Let $n(X,Y) \in k[X,Y]$ be an anisotropic quadratic form over the residue field k. Let $q_1, q_2 \in k[X_1,\ldots,X_{n-4}]$ be the quadratic forms given below.

$$\begin{aligned} q_1 &= n(X_1,X_2) + n(X_3,X_4) + X_5X_6 + X_7X_8 + \cdots + X_{n-5}X_{n-4}. \\ q_2 &= n(X_1,X_2). \end{aligned}$$

We will show that $D_k(q_1,q_2) = \frac{n-8}{2}$. Suppose $q_1(X) = q_2(X) = 0$ for some $X = (x_1,\ldots,x_{n-4}) \in k^{n-4}$. Then having $q_2(X) = 0$ implies that $x_1 = x_2 = 0$. Note that $q_1(0,0,X_3,\ldots,X_{n-4})$ is a quadratic form in $n-6$ variables of rank $n-6$ that splits off exactly $\frac{n-8}{2}$ hyperbolic planes. Therefore, $q_1(0,0,X_3,\ldots,X_{n-4})$ vanishes on a subspace over k of dimension $\frac{n-8}{2}$. Theorem $B.1.1$ implies that $\frac{n-8}{2}$ is the largest dimension of a subspace over k on which $q_1(0,0,X_3,\ldots,X_{n-4})$ vanishes. Thus $D_k(q_1,q_2) = \frac{n-8}{2}$.

By Lemma 4.0.6, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1,\ldots,X_{n-4}]$ such that $\overline{Q_i} = q_i$, $1 \leqslant i \leqslant 2$, and $\{Q_1,Q_2\}$ is nonsingular. By Lemma 8.2.5, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(4,\mathcal{B},0,2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$.

By Lemma 5.0.5, we can adjust the coefficients of Q_1' and Q_2' modulo π so that the pair $\{f,g\}$ is nonsingular and so that $\{Q_1',Q_2'\}$ remains a type $\mathcal{B}$ pair with $d=0$ and $h=2$.

By Lemma 2.3.17, we have

$$\begin{aligned} D_K(f,g) &\leqslant D_k(\overline{Q_1},\overline{Q_2}) + D_k(\overline{Q_1'},\overline{Q_2'}). \\ &= \frac{n-8}{2} + 0. \\ &= \frac{n-8}{2}. \end{aligned}$$

By Lemma 2.3.11, $D_K(f,g) \geqslant \frac{n-8}{2}$. Thus $D_K(f,g) = \frac{n-8}{2}$.

To show that $H_K(f,g) = \frac{n}{2}$, note that Lemma $B.2.6$ implies that $n(X_1,X_2) + n(X_3,X_4)$ splits off 2 hyperbolic planes over k, hence $q_1 = \overline{Q_1}$ splits off $\frac{n-4}{2}$ hyperbolic planes over k. By Definition 5.0.2, $\overline{Q_1'}$ splits off 2 hyperbolic planes over k. By Lemma $A.1.2$, Q_1 splits off $\frac{n-4}{2}$ hyperbolic planes over $\mathcal{O}_K$ and Q_1' splits off 2 hyperbolic planes over $\mathcal{O}_K$. Therefore, f splits off $\frac{n-4}{2} + 2 = \frac{n}{2}$ hyperbolic planes over $\mathcal{O}_K$, which proves that $H_K(f,g) = \frac{n}{2}$.

□

Theorem 9.4.2. *Let $n \geqslant 8$ be even with $n \neq 10$. There exists a pair of quadratic forms $\{f,g\}$ over K in n variables with the following properties.*

1. *$\{f,g\}$ is nonsingular.*
2. *$D_K(f,g) = \frac{n-8}{2}$.*

3. $H_K(f,g) = \frac{n-2}{2}$.

Proof. Note that $n-4 \geqslant 4$ and $n-4 \neq 6$. Thus, by Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-4, \mathcal{A}, \frac{n-8}{2}, \frac{n-6}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.5, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(4, \mathcal{B}, 0, 2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f,g\}$ is nonsingular, $D_K(f,g) = \frac{n-8}{2} + 0 = \frac{n-8}{2}$, and $H_K(f,g) = \frac{n-6}{2} + 2 = \frac{n-2}{2}$. □

Theorem 9.4.3. *Let $n = 10$. There exists a pair of quadratic forms $\{f,g\}$ over K in n variables with the following properties:*

1. *$\{f,g\}$ is nonsingular.*
2. *$D_K(f,g) = \frac{n-8}{2} = 1$.*
3. *$H_K(f,g) = \frac{n-2}{2} = 4$.*

Proof. By Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.4, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(6, \mathcal{B}, 1, 3)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f,g\}$ is nonsingular, $D_K(f,g) = 0 + 1 = 1$, and $H_K(f,g) = 1 + 3 = 4$. □

Theorem 9.4.4. *Let $n \geqslant 8$ be even with $n \neq 10$. There exists a pair of quadratic forms $\{f,g\}$ over K in n variables with the following properties.*

1. *$\{f,g\}$ is nonsingular.*
2. *$D(f,g) = \frac{n-8}{2}$.*
3. *$H(f,g) = \frac{n-4}{2}$.*

Proof. Note that $n-4 \geqslant 4$ and $n-4 \neq 6$. Thus, by Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-4, \mathcal{A}, \frac{n-8}{2}, \frac{n-6}{2})$, $1 \leqslant i \leqslant 2$. Likewise, by Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i' = Q_i'(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f,g\}$ is nonsingular, $D_K(f,g) = \frac{n-8}{2} + 0 = \frac{n-8}{2}$, and $H_K(f,g) = \frac{n-6}{2} + 1 = \frac{n-4}{2}$. □

Chapter 10 n odd

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We will use the same notation given at the beginning of section 2.3.

10.1 $D = \frac{n-1}{2}$

Theorem 10.1.1. *Let $n \geqslant 1$ be odd. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-1}{2}$.*
3. *$H_K(f, g) = \frac{n-1}{2}$.*

Proof. Lemma 8.1.1 provides an example. □

10.2 $D = \frac{n-3}{2}$

Theorem 10.2.1. *Let $n \geqslant 3$ be odd. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-3}{2}$.*
3. *$H_K(f, g) = \frac{n-1}{2}$.*

Proof. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q_i = Q_i(n-1, \mathcal{B}, \frac{n-3}{2}, \frac{n-1}{2})$, $1 \leqslant i \leqslant 2$. Let $Q'_1 = Q'_2 = X^2$. By checking Definition 5.0.2, it is easy to see that $\{Q'_1, Q'_2\}$ is a type $\mathcal{B}$ pair in one variable with $d = h = 0$; that is, $Q'_i = Q'_i(1, \mathcal{B}, 0, 0)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.7, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-3}{2} + 0 = \frac{n-3}{2}$, and $H_K(f, g) = \frac{n-1}{2} + 0 = \frac{n-1}{2}$. □

Theorem 10.2.2. *Let $n \geqslant 9$ be odd. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-3}{2}$.*
3. *$H_K(f, g) = \frac{n-3}{2}$.*

Theorems 2.2.14 *and* 2.3.15 *imply that there are no examples of quadratic forms with these properties for $n = 3, 5, 7$.*

Proof. First, assume $n = 11$. By Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(6, \mathcal{A}, 2, 2)$, $1 \leqslant i \leqslant 2$. By Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q'_i = Q'_i(5, \mathcal{A}, 2, 2)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = 2 + 2 = 4$, and $H_K(f, g) = 2 + 2 = 4$.

Now assume $n \geqslant 9$ is odd with $n \neq 11$. Then $n-3 \geqslant 6$ is even and $n-3 \neq 8$. Thus, by Lemma 8.2.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-3, \mathcal{A}, \frac{n-5}{2}, \frac{n-5}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q'_i = Q'_i(3, \mathcal{A}, 1, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-5}{2} + 1 = \frac{n-3}{2}$, and $H_K(f, g) = \frac{n-5}{2} + 1 = \frac{n-3}{2}$. □

10.3 $D = \frac{n-5}{2}$

Theorem 10.3.1. *Let $n \geqslant 5$ be odd. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-5}{2}$.*
3. *$H_K(f, g) = \frac{n-1}{2}$.*

Proof. By Lemma 8.2.1, there exists a type $\mathcal{B}$ pair $Q_i = Q_i(n-3, \mathcal{B}, \frac{n-5}{2}, \frac{n-3}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.1.4, there exists a type $\mathcal{B}$ pair $Q'_i = Q'_i(3, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.7, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-5}{2} + 0 = \frac{n-5}{2}$, and $H_K(f, g) = \frac{n-3}{2} + 1 = \frac{n-1}{2}$.

□

Theorem 10.3.2. *Let $n \geqslant 7$ be odd. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables with the following properties:*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-5}{2}$.*
3. *$H_K(f, g) = \frac{n-3}{2}$.*

Proof. By Lemma 8.1.2, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-4, \mathcal{A}, \frac{n-5}{2}\frac{n-5}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q'_i = (4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q'_1$ and $g = Q_2 \perp \pi Q'_2$. By Lemma 5.0.6, we can adjust the coefficients of Q'_1 and Q'_2 modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-5}{2} + 0 = \frac{n-5}{2}$, and $H_K(f, g) = \frac{n-5}{2} + 1 = \frac{n-3}{2}$. □

10.4 $D = \frac{n-7}{2}$

Theorem 10.4.1. *Suppose $n \geqslant 7$ is odd. There exists a pair of quadratic forms $\{f, g\}$ over $\mathcal{O}_K$ in n variables satisfying the following properties.*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-7}{2}$.*
3. *$H_K(f, g) = \frac{n-1}{2}$.*

Proof. Let $n(X, Y) \in k[X, Y]$ be an anisotropic quadratic form over the residue field k. Let $q_1, q_2 \in k[X_1, \ldots, X_{n-4}]$ be the quadratic forms given below.

$$q_1 = n(X_1, X_2) + n(X_3, X_4) + X_5X_6 + X_7X_8 + \cdots + X_{n-4}X_{n-3}.$$
$$q_2 = n(X_1, X_2).$$

We will show that $D_k(q_1, q_2) = \frac{n-7}{2}$. Suppose $q_1(X) = q_2(X) = 0$ for some $X = (x_1, \ldots, x_{n-3}) \in k^{n-3}$. Then having $q_2(X) = 0$ implies that $x_1 = x_2 = 0$. Note that $q_1(0, 0, X_3, \ldots, X_{n-3})$ is a quadratic form in $n-5$ variables of rank $n-5$ that splits off exactly $\frac{n-7}{2}$ hyperbolic planes. Therefore, $q_1(0, 0, X_3, \ldots, X_{n-3})$ vanishes on a subspace over k of dimension $\frac{n-7}{2}$, and Theorem $B.1.1$ implies that this is the largest dimension of a subspace over k on which it vanishes. Thus $D_k(q_1, q_2) = \frac{n-7}{2}$.

By Lemma 4.0.6, there exist quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_{n-3}]$ such that $\overline{Q_i} = q_i$, $1 \leqslant i \leqslant 2$, and $\{Q_1, Q_2\}$ is nonsingular. By Lemma 8.1.4, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(3, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$.

By Lemma 5.0.5, we can adjust the coefficients of Q_1' and Q_2' modulo π so that the pair $\{f, g\}$ is nonsingular and so that $\{Q_1', Q_2'\}$ remains a type $\mathcal{B}$ pair with $d = 0$ and $h = 1$.

By Lemma 2.3.17, we have

$$\begin{aligned} D_K(f, g) &\leqslant D_k(\overline{Q_1}, \overline{Q_2}) + D_k(\overline{Q_1'}, \overline{Q_2'}) \\ &= \frac{n-7}{2} + 0 \\ &= \frac{n-7}{2}. \end{aligned}$$

By Lemma 2.3.11, $D_K(f, g) \geqslant \frac{n-7}{2}$. Thus $D_K(f, g) = \frac{n-7}{2}$.

To show that $H_K(f, g) = \frac{n}{2}$, note that Lemma $B.2.6$ implies that $n(X_1, X_2) + n(X_3, X_4)$ splits off 2 hyperbolic planes over k, hence $q_1 = \overline{Q_1}$ splits off $\frac{n-3}{2}$ hyperbolic planes over k. By Definition 5.0.2, $\overline{Q_1'}$ splits off 1 hyperbolic plane over k. By Lemma $A.1.2$, Q_1 splits off $\frac{n-3}{2}$ hyperbolic planes over $\mathcal{O}_K$, and Q_1' splits off 1 hyperbolic plane over $\mathcal{O}_K$. Therefore, f splits off $\frac{n-3}{2} + 1 = \frac{n-1}{2}$ hyperbolic planes over $\mathcal{O}_K$, which proves that $H_K(f, g) = \frac{n-1}{2}$. □

Theorem 10.4.2. *Suppose n is odd with $n = 7$ or $n \geqslant 11$. There exists a pair of quadratic forms $\{f, g\}$ over K in n variables satisfying the following properties.*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-7}{2}$.*
3. *$H_K(f, g) = \frac{n-3}{2}$.*

Proof. Note that $n-3 \geqslant 4$ is even with $n-3 \neq 6$. Thus, by Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(n-3, \mathcal{A}, \frac{n-7}{2}, \frac{n-5}{2})$, $1 \leqslant i \leqslant 2$. By Lemma 8.1.4, there exists a type $\mathcal{B}$ pair $Q_i' = Q_i'(3, \mathcal{B}, 0, 1)$, $1 \leqslant i \leqslant 2$. Let $f = Q_1 \perp \pi Q_1'$ and $g = Q_2 \perp \pi Q_2'$. By Lemma 5.0.6, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f, g\}$ is nonsingular, $D_K(f, g) = \frac{n-7}{2} + 0 = \frac{n-7}{2}$, and $H_K(f, g) = \frac{n-5}{2} + 1 = \frac{n-3}{2}$. □

Theorem 10.4.3. *There exists a pair of quadratic forms $\{f, g\}$ over $\mathcal{O}_K$ in $n = 9$ variables satisfying the following properties.*

1. *$\{f, g\}$ is nonsingular.*
2. *$D_K(f, g) = \frac{n-7}{2} = 1$.*
3. *$H_K(f, g) = \frac{n-3}{2} = 3$.*

Proof. By Lemma 8.2.3, there exists a type $\mathcal{A}$ pair $Q_i = Q_i(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$. Since $\{Q_1, Q_2\}$ is nonsingular, Theorem 2.1.27 implies that $\det(\lambda Q_1 + \mu Q_2)$ has distinct linear factors. Since $\mathcal{O}_K$ has infinitely many units, we can choose units $a, b \in \mathcal{O}_K$ so that $a\lambda + b\mu$ is not a linear factor in $\det(\lambda Q_1 + \mu Q_2)$. Let $f_1, g_1 \in \mathcal{O}_K[X_1, \ldots, X_5]$ be the quadratic forms given below.

$$f_1 = Q_1(X_1, \ldots, X_4) + aX_5^2.$$
$$g_1 = Q_2(X_1, \ldots, X_4) + bX_5^2.$$

By our choice of a and b, the pair $\{f_1, g_1\}$ is nonsingular.

We will show that $D_k(\overline{f_1}, \overline{g_1}) = 1$. Since $\{f_1, g_1\}$ have 5 variables, Lemma B.2.9 implies that $D_k(\overline{f_1}, \overline{g_1}) \geqslant 1$. For sake of contradiction, suppose $\{\overline{f_1}, \overline{g_1}\}$ vanish on a two-dimensional subspace over k, say $\text{span}_k(v, w)$, where $v, w \in k^5$ are linearly independent. Since $D_k(\overline{Q_1}, \overline{Q_2}) = 0$, we know that the fifth coordinate of v and the fifth coordinate of w can not both be zero. Without loss of generality, assume the fifth coordinate of v is nonzero. We can choose $c \in k$ so that the fifth coordinate of $x = cv+w$ is zero. Since $\{v, w\}$ are linearly independent, $x \neq 0$. Since $\overline{f_1}(x) = \overline{g_1}(x) = 0$, it follows that $\overline{Q_1}(x) = \overline{Q_2}(x) = 0$. This is contrary to $D_k(\overline{Q_1}, \overline{Q_2}) = 0$.

Thus, $D_k(\overline{f_1}, \overline{g_1}) = 1$. Next, we will show that for each $q \in \mathcal{P}_k(\overline{f_1}, \overline{g_1})$, we have $D_k(q) \leqslant 2$. To see this, note that by Lemma 8.2.3, every form in $\mathcal{P}_k(\overline{Q_1}, \overline{Q_2})$ has order 4 and splits off exactly 1 hyperbolic plane over k. It follows that every form in

$\mathcal{P}_k(\overline{f_1}, \overline{f_2})$ either has order 4 and splits off exactly 1 hyperbolic plane, or has order 5 and splits off exactly 2 hyperbolic planes. Thus, Lemma 2.2.6 implies that $D_k(q) \leqslant 2$ for each $q \in \mathcal{P}_k(\overline{f_1}, \overline{g_1})$.

Now, let $Q_i' = Q_i'(4, \mathcal{A}, 0, 1)$, $1 \leqslant i \leqslant 2$, be a type $\mathcal{A}$ pair in four variables as in Lemma 8.2.3. Let

$$f = f_1(X_1, \ldots, X_5) + \pi Q_1'(X_6, \ldots, X_9).$$
$$g = g_1(X_1, \ldots, X_5) + \pi Q_2'(X_6, \ldots, X_9).$$

By Lemma 5.0.5, we can adjust the coefficients of Q_1' and Q_2' modulo π so that $\{f, g\}$ is nonsingular and so that $\{Q_1', Q_2'\}$ remains a type $\mathcal{A}$ pair with $d = 0$ and $h = 1$. By Lemma 2.3.11, we have $D_K(f, g) \geqslant 1$. On other hand, Lemma 2.3.17 implies that

$$\begin{aligned} D_K(f, g) &\leqslant D_k(\overline{f_1}, \overline{g_1}) + D_k(\overline{Q_1'}, \overline{Q_2'}) \\ &= 1 + 0 \\ &= 1. \end{aligned}$$

Thus, $D_K(f, g) = 1$. To show that $H_K(f, g) = 3$, let $\lambda, \mu \in \mathcal{O}_K$, not both divisible by π. Note that by Lemma 8.2.3, there is an invertible linear change of variable over $\mathcal{O}_K$ so that $\lambda Q_1' + \mu Q_2' = X_6X_7 + N(X_8, X_9)$, where $\overline{N}$ is anisotropic over k. Thus

$$\lambda f + \mu g = G(X_1, \ldots, X_5) + \pi N(X_9, X_{10}) + \pi X_6 X_7,$$

where $G = \lambda f_1 + \mu g_1$. We proved above that $D_k(\overline{G}) \leqslant 2$. Lemma 2.3.3 implies that $G + \pi N$ splits off at most $D_k(\overline{G}) \leqslant 2$ hyperbolic planes. Thus $\lambda f + \mu g$ splits off at most 3 hyperbolic planes, hence $H_K(f, g) \leqslant 3$. Lemma 2.3.11 implies that $H_K(f, g) \geqslant 3$. We conclude that $H_K(f, g) = 3$. □

For this chapter, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. We use the same notation given at the beginning of section 2.3.

11.1 $n = 5$

Our goal for this section is to prove the following theorem.

Theorem 11.1.1. *Let $Q_1, Q_2 \in K[X_1, \ldots, X_5]$ be a nonsingular pair of quadratic forms. If $D_K(Q_1, Q_2) = 0$ and $|k| \geqslant 4$, then $H_K(Q_1, Q_2) = 2$.*

We begin the proof of theorem 11.1.1 now. Our proof will utilize results from appendix A. By multiplying Q_1 and Q_2 by a sufficient power of π, we can assume that Q_1 and Q_2 have coefficients in $\mathcal{O}_K$.

For $i = 1, 2$, let $q_i = \overline{Q_i}$. We define $R = R(q_1, q_2)$ to be the least integer m such that there is a linear transformation $T \in \mathrm{GL}_5(k)$ for which $q_1(TX)$ and $q_2(TX)$ are both functions of $X_1, \ldots, X_m$ alone. Therefore, there is an invertible linear change of variables over k so that $q_i = q_i'(X_1, \ldots, X_R)$ for $i = 1, 2$, where q_i' denote quadratic forms over k. Consequently, every form in $\mathcal{P}_k(q_1, q_2)$ can be expressed using only the variables $X_1, \ldots, X_R$.

We define $r = r(q_1, q_2)$ to be the maximum order a form in $\mathcal{P} = \mathcal{P}_k(q_1, q_2)$; that is,

$$r = r(q_1, q_2) = \max\{\mathrm{order}(q) \mid q \in \mathcal{P}\}.$$

It follows that $r \leqslant R \leqslant 5$.

By Lemma $A.2.4$, we can assume Q_1, Q_2 is a minimized pair. By Lemma $A.3.4$ with $d = 0$ and $n = 5$, we get

$$R = R(q_1, q_2) \geqslant \frac{5+1}{2} + 0 = 3.$$

By Lemma $A.3.3$, we know every form in $\mathcal{P}_k(q_1, q_2)$ has order $\geqslant \frac{5}{4}$, hence $r \geqslant 2$. Further, by Lemma $A.3.2$, any form in $\mathcal{P}_k(q_1, q_2)$ that has order 2 must be anisotropic. Then Lemma $B.2.21$ implies that $r \geqslant 3$. We have shown that

$$3 \leqslant r \leqslant R \leqslant 5.$$

Our proof is divided into cases depending on the possible values for r and R.

Suppose $r = 5$. Then there is a form in $\mathcal{P}_k(q_1, q_2)$ that splits off 2 hyperbolic planes over k. Lemma $A.1.2$ implies that there is a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off 2 hyperbolic planes over K, as desired.

From here on, we assume $3 \leqslant r \leqslant 4$. Next, we consider the case $R = 3$.

11.1.1 $R = 3$

Since $R = 3$, we get $r = 3$ as well. We can put Q_1 and Q_2 into the following shape

$$\begin{aligned} Q_1 &= G_1(X_1, X_2, X_3) + \pi \sum_{j=4}^{5} \Big(X_j L_j^{(1)}(X_1, X_2, X_3) \Big) + \pi H_1(X_4, X_5), \\ Q_2 &= G_2(X_1, X_2, X_3) + \pi \sum_{j=4}^{5} \Big(X_j L_j^{(2)}(X_1, X_2, X_3) \Big) + \pi H_2(X_4, X_5), \end{aligned} \tag{11.1.1}$$

where the G_i and H_i are quadratic forms over $\mathcal{O}_K$ and the $L_j^{(i)}$ are linear forms over $\mathcal{O}_K$. By minimization, Lemma $A.2.7$ implies that $D_k(h_1, h_2) = 0$. We will show that h_1 and h_2 are linearly independent.

Assume for contradiction that h_1 and h_2 are linearly dependent. Then there exist $\alpha_1, \alpha_2 \in \mathcal{O}_K$, not both divisible by π, such that $\alpha_1 H_1 + \alpha_2 H_2 \equiv 0 \bmod \pi$. Without loss of generality, assume α_1 is a unit. Let $U' = \begin{bmatrix} \alpha_1 & \alpha_2 \\ 0 & 1 \end{bmatrix}$. Since $\det(U') = \alpha_1$ is a unit, the pair $(Q_1, Q_2)^{U'}$ is still minimized, but now the form playing the role of H_1 is divisible by π. From these maneuvers, we can assume that $\pi \mid H_1$ in equation 11.1.1. Let $T = \operatorname{diag}(\pi, \pi, \pi, 1, 1)$ and $U = \operatorname{diag}(\pi^{-2}, \pi^{-1})$. Then $(Q_1, Q_2)_T^U$ is integral, but

$$4v(\det(T)) + 5v(\det(U)) = 4(3) + 5(-3) < 0.$$

By Lemma $A.2.5$, this is contrary to Q_1, Q_2 being minimized. Therefore, h_1 and h_2 are linearly independent.

Next, we will show that $D_k(g_1, g_2) = 0$. Suppose $D_k(g_1, g_2) \geqslant 1$. By an invertible linear change of variables over k, we can assume $(0, 0, 1)$ is a common zero of g_1 and g_2. Then g_1 and g_2 both vanish whenever $X_1 = X_2 = 0$. It follows that q_1 and q_2 both vanish on a subspace in k^5 of dimension 3. Then the inequality $n < 2d$ is satisfied for $n = 5$ and $d = 3$, in which case Lemma $A.3.1$ contradicts minimization. Therefore, $D_k(g_1, g_2) = 0$.

Also, by minimization, Lemmas $A.3.3$ and $A.3.2$ imply that every form in $\mathcal{P}_k(g_1, g_2)$ is either anisotropic of order 2 or has order 3. Thus Lemma $B.2.22$ implies that there are exactly $|k| - 1$ pairs $(a, b) \in k^2$, not both zero, for which $ag_1 + bg_2$ is anisotropic of order 2.

On the other hand, since $D_k(h_1, h_2) = 0$ and h_1, h_2 are linearly independent, Lemma $B.2.23$ implies that there are at least $|k|$ pairs $(a, b) \in k^2$, not both zero, for which $ah_1 + bh_2$ is isotropic.

Since $|k| > |k| - 1$, we deduce that there exist $(a, b) \in k^2$, not both zero, for which $ag_1 + bg_2$ has order 3 (and hence splits off 1 hyperbolic plane), and $ah_1 + bh_2$ is isotropic.

Without loss of generality, $b \neq 0$. Let $b' \in \mathcal{O}_K$ be a unit so that $\overline{b'} = b$. By replacing Q_1 with $Q_1 + b'Q_2$, we may assume that g_1 has order 3 and that h_1 is isotropic. We can perform an invertible linear change of variable over k involving X_1, X_2, X_3 so that

$$g_1 = X_1X_2 + dX_3^2$$

for some $d \in k$. Through a change of variable involving X_4, X_5, we can assume $h_1(0,1) = 0$. Since $D_k(h_1, h_2) = 0$, we get $h_2(0,1) \neq 0$. Thus $\pi^2 \mid Q_1(e_5)$ and $\pi^2 \nmid Q_2(e_5)$. We therefore have the following:

1. $Q_1(X_1, X_2, 0, 0, X_5) \equiv X_1X_2 \bmod \pi$.
2. $Q_2(X_1, X_2, 0, 0, X_5) \equiv G_2(X_1, X_2, 0) \bmod \pi$.
3. $\pi^2 \mid Q_1(e_5)$.
4. $\pi^2 \nmid Q_2(e_5)$

Thus Lemma $A.1.6$ implies that there is a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off 2 hyperbolic planes.

11.1.2 $R = 4$

We can write Q_1 and Q_2 in the following way.

$$\begin{aligned} Q_1 &= G_1(X_1, \ldots, X_4) + \pi X_5 L_1(X_1, \ldots, X_4) + \pi a_1 X_5^2, \\ Q_2 &= G_2(X_1, \ldots, X_4) + \pi X_5 L_2(X_1, \ldots, X_4) + \pi a_2 X_5^2, \end{aligned} \tag{11.1.2}$$

where $R = R(g_1, g_2) = 4$ and $r = r(g_1, g_2) \in \{3, 4\}$. If g_1 and g_2 have a nonsingular common zero over k, then by Lemma 2.3.6, the forms G_1 and G_2 would have a common nontrivial zero over K, contrary to $D_K(Q_1, Q_2) = 0$.

Therefore, either g_1 and g_2 have a singular common zero over k, or $D_k(g_1, g_2) = 0$. We will address each of these cases separately.

Case 1. Suppose g_1 and g_2 have a singular common zero over k. Through a change of variable, we can assume $(1, 0, 0, 0)$ is a singular common zero of g_1 and g_2. Then g_1 and g_2 have the shape

$$\begin{aligned} g_1 &= X_1 \ell(X_2, \ldots, X_4) + w_1'(X_2, \ldots, X_4), \\ g_2 &= X_1 \ell'(X_2, \ldots, X_4) + w_2'(X_2, \ldots, X_4), \end{aligned}$$

where ℓ, ℓ' are linear forms over k and w_1', w_2' are quadratic forms over k. Since $R(g_1, g_2) = 4$, we know at least one of either ℓ or ℓ' is nonzero. Since $(1, 0, 0, 0)$ is a singular common zero, we know ℓ and ℓ' are linearly dependent. Without loss of generality, assume the coefficient of X_2 in ℓ is nonzero, and $\ell' = c\ell$ for some $c \in k$. Through a change of variables involving X_2, X_3, X_4, we obtain

$$g_1 = X_1X_2 + w_1(X_2, \dots, X_4),$$
$$g_2 = c'X_1X_2 + w_2(X_2, \dots, X_4),$$

where for $i = 1, 2$, w_i is the image of w_i' under the change of variables. We can write w_1 and w_2 in the following way.

$$w_1 = X_2s_1(X_2, X_3, X_4) + t_1(X_3, X_4),$$
$$w_2 = X_2s_2(X_2, X_3, X_4) + t_2(X_3, X_4),$$

where s_1, s_2 are linear forms over k, and t_1, t_2 are quadratic forms over k. Thus

$$\begin{aligned} g_1 &= X_1X_2 + X_2s_1(X_2, X_3, X_4) + t_1(X_3, X_4). \\ g_2 &= c'X_1X_2 + X_2s_2(X_2, X_3, X_4) + t_2(X_3, X_4). \end{aligned} \tag{11.1.3}$$

Suppose t_1 and t_2 have a common nontrivial zero over k. Through a change of variables involving X_3 and X_4, we can assume $(1, 0)$ is a common zero of t_1 and t_2. Then g_1 and g_2 both vanish whenever $X_2 = X_4 = 0$. It follows that q_1 and q_2 both vanish on a $5 - 2 = 3$ dimensional subspace in k^5. Then $n < 2d$ is satisfied for $n = 5$ and $d = 3$, in which case Lemma $A.3.1$ contradicts minimization.

Therefore, $D_k(t_1, t_2) = 0$. Suppose t_1 and t_2 are linearly dependent over k. Then there exist $\alpha_1, \alpha_2 \in k$, not both zero, such that $\alpha_1 t_1 + \alpha_2 t_2 = 0$. Let $g = \alpha_1 g_1 + \alpha_2 g_2$. Thus

$$g = (\alpha_1 + c'\alpha_2)X_1X_2 + X_2(\alpha_1 s_1 + \alpha_2 s_2).$$
$$g = X_2\ell(X_1, X_2, X_3, X_4)$$

where $\ell = (\alpha_1 + c'\alpha_2)X_1 + (\alpha_1 s_1 + \alpha_2 s_2)$. By Lemma $A.3.3$, g has order $\geqslant \frac{5}{4}$, hence g must have order 2. But then g is isotropic of order 2, contrary to Lemma $A.3.2$.

We have shown that $D_k(t_1, t_2) = 0$ and that t_1 and t_2 are linearly independent over k. Next, consider the following claim.

Claim: There exist $(a, b) \in k^2$, not both zero, for which $a + bc' \neq 0$ and $at_1 + bt_2$ is isotropic.

To prove this claim, notice that there are exactly $|k| - 1$ pairs $(a, b) \in k^2$, not both zero, for which $a + bc' = 0$. On the other hand, since t_1, t_2 are linearly independent with $D_k(t_1, t_2) = 0$, Lemma $B.2.23$ implies that there are at least $|k|$ pairs $(a, b) \in k^2$, not both zero, for which $at_1 + bt_2$ is isotropic. Since $|k| > |k| - 1$, we deduce that there is a pair $(a, b) \in k^2$, not both zero, for which $a + bc' \neq 0$ and $at_1 + bt_2$ is isotropic, as desired.

Without loss of generality, assume $a \neq 0$. Let $g_1' = ag_1 + bg_2$. From equation 11.1.3, we have

$$g_1' = a'X_1X_2 + X_2s'(X_2, X_3, X_4) + t'(X_3, X_4),$$
$$g_2 = c'X_1X_2 + X_2s_2(X_2, X_3, X_4) + t_2(X_3, X_4),$$

where $a' = a + bc'$, $s' = as_1 + bs_2$, and $t' = at_1 + bt_2$. Thus $a' \neq 0$ and t' is isotropic. We rewrite g_1' as

$$g_1' = X_2(a'X_1 + s'(X_2, X_3, X_4)) + t'(X_3, X_4).$$
$$g_2 = c'X_1X_2 + X_2s_2(X_2, X_3, X_4) + t_2(X_3, X_4).$$

Since $a' \neq 0$, we can perform the invertible linear change of variable given by $X_1' = a'X_1 + s'(X_2, X_3, X_4)$. Doing so yields

$$g_1' = X_1'X_2 + t'(X_3, X_4).$$
$$g_2 = (c'/a')(X_1' - s'(X_2, X_3, X_4))X_2 + X_2s_2(X_2, X_3, X_4) + t_2(X_3, X_4).$$

Thus we have

$$g_1' = X_1'X_2 + t'(X_3, X_4)$$
$$g_2 = X_2s(X_1', X_2, X_3, X_4) + t_2(X_3, X_4)$$

for some linear form $s(X_1', X_2, X_3, X_4)$ defined over k. Since t' is isotropic, we can perform an invertible linear change of variables involving only X_3 and X_4 so that $t'(1, 0) = 0$. Then $g_1'(X_1', X_2, X_3, 0) = X_1'X_2$. Since $D_k(t', t_2) = D_k(t_1, t_2) = 0$, we know $t_2(1, 0) \neq 0$, hence $\pi \nmid Q_2(e_3)$. If we let $Q_1' = AQ_1 + BQ_2$, where $A, B \in \mathcal{O}_K$ satisfy $\overline{A} = a$ and $\overline{B} = b$, then we have shown that

$$Q_1'(X_1', X_2, X_3, 0, 0) \equiv X_1'X_2 \bmod \pi$$

and

$$\pi \nmid Q_2(e_3).$$

Thus, Lemma $A.1.5$ implies that there is a form in $\mathcal{P}_K(Q_1', Q_2)$ that splits off 2 hyperbolic planes over K. The same is true for $\mathcal{P}_K(Q_1, Q_2)$.

Case 2. Suppose $D_k(g_1, g_2) = 0$. Note that by Lemma $A.3.3$, every form in $\mathcal{P}_k(g_1, g_2)$ has order $\geqslant 2$. We consider two possibilities.

First, suppose every form in $\mathcal{P}_k(g_1, g_2)$ has order $\geqslant 3$. Then Lemma $B.2.20$ implies that every form in $\mathcal{P}_k(g_1, g_2)$ has order 4 and splits off exactly 1 hyperbolic plane. We work from equation 11.1.2, which we restate below for convenience.

$$Q_1 = G_1(X_1, \ldots, X_4) + \pi X_5L_1(X_1, \ldots, X_4) + \pi a_1X_5^2.$$
$$Q_2 = G_2(X_1, \ldots, X_4) + \pi X_5L_2(X_1, \ldots, X_4) + \pi a_2X_5^2.$$

By minimization, Lemma $A.2.7$ implies that at least one of a_1 or a_2 is a unit. Without loss of generality, assume a_2 is a unit. There exists $c \in \mathcal{O}_K$ so that $\pi \mid a_1 + ca_2$. Let $Q_1' = Q_1 + cQ_2$ and $G_1' = G_1 + cG_2$. Since every form in $\mathcal{P}_k(g_1, g_2)$ has order 4 and splits off exactly 1 hyperbolic plane, we can perform an invertible linear change of variables over k so that $\overline{G_1'} = X_1X_2 + g_0(X_3, X_4)$ for some quadratic form g_0 defined over k. It follows that

1. $Q_1'(X_1, X_2, 0, 0, X_5) \equiv X_1X_2 \bmod \pi$.
2. $Q_2(X_1, X_2, 0, 0, X_5) \equiv G_2(X_1, X_2, 0, 0) \bmod \pi$.
3. $\pi^2 \mid Q_1'(e_5)$.
4. $\pi^2 \nmid Q_2(e_5)$.

Therefore, Lemma $A.1.6$ implies that there is a form in $\mathcal{P}_K(Q_1', Q_2)$ that splits off 2 hyperbolic planes over K. The same is true for the pencil $\mathcal{P}_K(Q_1, Q_2)$.

It remains to consider the case where there is a form of order 2 in $\mathcal{P}_k(g_1, g_2)$. In this case, since $|k| \geqslant 4$ and $D_k(g_1, g_2) = 0$, Lemma $B.2.14$ implies that there is a form in $\mathcal{P}_k(g_1, g_2)$ that splits off 2 hyperbolic planes. Then Lemma $A.1.2$ implies that the same is true for $\mathcal{P}_K(Q_1, Q_2)$, as desired.

11.1.3 $R = 5$

Without loss of generality, we may assume that $\text{order}(q_1) = r = r(q_1, q_2)$. Since $3 \leqslant r \leqslant 4$, we may perform an invertible linear change of variables over k so that $q_1 = q_3(X_1, \ldots, X_4)$, where q_3 is a quadratic form over k of order $r \in \{3, 4\}$. We can write q_2 in the following way:

$$q_2 = q_4(X_1, \ldots, X_4) + X_5\ell(X_1, \ldots, X_5),$$

where q_4 is a quadratic form and ℓ is a linear form, each defined over k.

Suppose $q_2(e_5) \neq 0$. Since q_3 has order $\geqslant 3$, q_3 splits off at least 1 hyperbolic plane over k. We may perform an invertible linear change of variables over k involving the variables $X_1, \ldots, X_4$ so that $q_1 = X_1X_2 + q_0(X_3, X_4)$ for some quadratic form q_0 over k. Then $Q_1(X_1, X_2, 0, 0, X_5) \equiv X_1X_2 \bmod \pi$ and $\pi \nmid Q_2(e_5)$. Thus Lemma $A.1.5$ implies that $H_K(Q_1, Q_2) = 2$, as desired.

So, consider the case where $q_2(e_5) = 0$. Since $R = 5$, we know $\ell \neq 0$. Without loss of generality, assume the coefficient of X_4 in ℓ is nonzero. By an invertible linear change of variables involving $X_1, \ldots, X_4$, we may assume $\ell = X_4$. We have

$$q_1 = q_3(X_1, \ldots, X_4).$$
$$q_2 = q_4(X_1, \ldots, X_4) + X_4X_5.$$

We can rewrite q_3 and q_4 so that

$$q_1 = q_5(X_1, X_2, X_3) + X_4\ell_1(X_1, X_2, X_3, X_4)$$
$$q_2 = q_6(X_1, X_2, X_3) + X_4\ell_2(X_1, X_2, X_3, X_4) + X_4X_5$$

for some quadratic forms q_5, q_6 and some linear forms ℓ_1, ℓ_2, all defined over k. Since q_1 has order $\geqslant 3$, we know $q_5 \neq 0$. Thus q_5 has order $\geqslant 1$. By an invertible linear change of variables involving X_1, X_2, X_3, we may assume that $q_5(1, 0, 0) \neq 0$, hence $\pi \nmid Q_1(e_1)$. There exists $c \in k$ such that the coefficient of X_1^2 in $q_2' = cq_1 + q_2$ is zero. We can write q_2' in the following way:

$$q_2' = X_1\ell_3(X_2, X_3) + q_6'(X_2, X_3) + X_4\ell_4(X_1, \ldots, X_4) + X_4X_5$$

for some linear forms ℓ_3, ℓ_4 and some quadratic form q_6', all defined over k. Apply the invertible linear change of variable where X_5 is replaced with $X_5 - \ell_4(X_1, \ldots, X_4)$ to obtain

$$q_2' = X_1\ell_3(X_2, X_3) + q_6'(X_2, X_3) + X_4X_5.$$

Let $Q_2' = c'Q_1 + Q_2$, where $c' \in \mathcal{O}_K$ satisfies $\overline{c'} = c$. Then

$$Q_2'(X_1, 0, 0, X_4, X_5) \equiv X_4X_5 \bmod \pi$$

and

$$\pi \nmid Q_1(e_1).$$

Thus Lemma $A.1.5$ implies that $H_K(Q_1, Q_2) = 2$, as desired. This completes the proof of Theorem 11.1.1.

11.2 $n = 6, 8$

Let $Q_1, Q_2 \in K[x_1, \ldots, x_n]$ be quadratic forms over a p-adic field K. We consider the following conditions.

Condition A: If $\{Q_1, Q_2\}$ is a nonsingular pair, $n = 5$, and $D_K(Q_1, Q_2) = 0$, then $H_K(Q_1, Q_2) = 2$.

Condition B: If $\{Q_1, Q_2\}$ is a nonsingular pair, $n = 6$, and $D_K(Q_1, Q_2) = 0$, then $H_K(Q_1, Q_2) \geqslant 2$.

Condition C: If $\{Q_1, Q_2\}$ is a nonsingular pair, $n = 8$, and $D_K(Q_1, Q_2) = 1$, then $H_K(Q_1, Q_2) \geqslant 3$.

Theorem 11.2.1. *Let $Q_1, Q_2 \in K[x_1, \ldots, x_n]$ be a nonsingular pair of quadratic forms over a p-adic field K.*

1. *If Condition A holds, then Condition B holds.*
2. *If Condition A holds, then Condition C holds.*

Proof. This theorem is due to David Leep. □

Theorem 11.1.1 implies that condition A is true provided $|k| \geqslant 4$. Therefore, Theorem 11.2.1 implies that conditions B and C are also true provided $|k| \geqslant 4$. This gives us the following two theorems.

Theorem 11.2.2. *Let $Q_1, Q_2 \in K[X_1, \ldots, X_6]$ be a nonsingular pair of forms. If $D_K(Q_1, Q_2) = 0$ and $|k| \geqslant 4$, then $H_K(Q_1, Q_2) \geqslant 2$.*

Theorem 11.2.3. *Let $Q_1, Q_2 \in K[X_1, \ldots, X_8]$ be a nonsingular pair of forms. If $D_K(Q_1, Q_2) = 1$ and $|k| \geqslant 4$, then $H_K(Q_1, Q_2) \geqslant 3$.*

Appendix A: Splitting off Hyperbolic Planes, Minimized Pairs, R and r

A.1 Splitting off Hyperbolic Planes

For this section, let K denote a p-adic field with ring of integers $\mathcal{O}_K$ and residue field k. Thus k is a finite field. Let K^{alg} denote the algebraic closure of K. We may also use $\overline{K}$ to denote the algebraic closure of K. For $1 \leqslant i \leqslant n$, let $e_i \in K^n$ denote the i^{th} standard basis vector of K^n.

Lemma A.1.1. *Let M be a matrix over $\mathcal{O}_K$ and I_n be the $n \times n$ identity matrix. If $M \equiv I_n \bmod \pi$, then det(M) is a unit. In particular, M is invertible.*

Proof. We can write $M = I_n + \pi A$ for some $n \times n$ matrix A over $\mathcal{O}_K$. If we compute $\det(M)$ using co-factor expansion, expanding along the first row implies that $\det(M)$ has the form $\det(M) = 1 + \pi a$ for some $a \in \mathcal{O}_K$. Then

$$v(\det(M)) = \min(v(1), v(\pi a)) = v(1) = 0$$

An element of $\mathcal{O}_K$ is a unit if and only if its valuation is zero, hence we have shown that $\det(M)$ is a unit and it follows that M is invertible. $\square$

Lemma A.1.2 is from [7, Lemma 2.2, p. 45], but we have slightly modified the statement of the Lemma from that of Heath-Brown.

Lemma A.1.2. *Let π be a uniformizing element for K and let $Q(X_1, \ldots, X_n) \in \mathcal{O}_K[X]$ be a quadratic form.*

1. *If*

$$Q(X) \equiv X_1X_2 + \cdots + X_{2s-1}X_{2s} + \widetilde{Q}(X_{2s+1}, \ldots, X_n) + \pi \sum_{i=1}^{2s} X_i L_i(X_1, \ldots, X_n) \pmod{\pi^2}$$

for some quadratic form $\widetilde{Q}$ over $\mathcal{O}_K$, then there exists $T \in GL_n(\mathcal{O}_K)$ such that

$$Q(TX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q_0(X_{2s+1}, \ldots, X_n)$$

with $Q_0 \in \mathcal{O}_K[X]$ satisfying $Q_0 \equiv \widetilde{Q} \bmod \pi^2$.

2. Likewise, if

$$Q(X) \equiv X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q'(X_{2s+1}, \ldots, X_n) \bmod \pi,$$

then there exists $T \in GL_n(\mathcal{O}_K)$ such that

$$Q(TX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q_0(X_{2s+1}, \ldots, X_n)$$

with $Q_0 \in \mathcal{O}_K[X]$ satisfying $Q_0 \equiv Q' \bmod \pi$. Thus, if $\overline{Q}$ splits off at least s hyperbolic planes over k, then Q splits off at least s hyperbolic planes over $\mathcal{O}_K$.

Proof. First, we will show that (1) implies (2). Assume

$$Q \equiv X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q'(X_{2s+1}, \ldots, X_n) \bmod \pi$$

for some form $Q' \in \mathcal{O}_K[X]$. This implies that there is some quadratic form $R = R(X_1, \ldots, X_n) \in \mathcal{O}_K[X]$ such that

$$Q = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q'(X_{2s+1}, \ldots, X_n) + \pi R(X_1, \ldots, X_n).$$

We can write

$$R = \sum_{i=1}^{2s} (X_iL_i(X_1, \ldots, X_n)) + Q''(X_{2s+1}, \ldots, X_n).$$

It follows that

$$Q = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q'(X_{2s+1}, \ldots, X_n) + \pi Q''(X_{2s+1}, \ldots, X_n)$$
$$+\pi \sum_{i=1}^{2s} X_iL_i(X_1, \ldots, X_n).$$

Take $\widetilde{Q} = Q' + \pi Q''$. Now Q satisfies the hypothesis (1), in which case there exists $T \in \mathrm{GL}_n(\mathcal{O}_K)$ such that

$$Q(TX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q_0(X_{2s+1}, \ldots, X_n)$$

with $Q_0 \in \mathcal{O}_K[X]$ satisfying $Q_0 \equiv \widetilde{Q} \bmod \pi^2$. In particular, $Q_0 \equiv \widetilde{Q} \bmod \pi$, hence $Q_0 \equiv Q' \bmod \pi$. This proves (2).

Next we prove (1). We closely follow Heath-Brown's proof, but with added steps and more details. We begin by proving the existence of T in the lemma. To accomplish this, we will show inductively that for every positive integer h there is a linear transformation $T_h \in \mathrm{GL}_n(\mathcal{O}_K)$ and linear forms $\mathcal{L}_i^{(h)}(X_1, \ldots, X_n)$ over $\mathcal{O}_K$ such that

$$Q(T_hX) \equiv X_1X_2 + \cdots + X_{2s-1}X_{2s} + \mathcal{Q}_h(X_{2s+1}, \ldots, X_n)$$
$$+\pi^h \sum_{i=1}^{2s} X_i\mathcal{L}_i^{(h)}(X_1, \ldots, X_n) \bmod \pi^{h+1}$$

with $\mathcal{Q}_h \equiv \widetilde{Q} \bmod \pi^2$. From this we let $T = \lim_h T_h$ and $Q_0 = \lim_h \mathcal{Q}_h$, in which case

$$Q(TX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + Q_0(X_{2s+1}, \ldots, X_n)$$

as desired.

The hypothesis implies the case $h = 1$ with $T_1 = \mathrm{id}$, $\mathcal{Q}_1 = \widetilde{Q}$, and $\mathcal{L}_i^{(1)} = L_i$. Assume there exists $T_h \in \mathrm{GL}_n(\mathcal{O}_K)$ such that the above congruence holds. We may reinterpret the above conguence as an equation:

$$Q(T_hX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + \mathcal{Q}_h(X_{2s+1}, \ldots, X_n)$$
$$+\pi^h \sum_{i=1}^{2s} X_i\mathcal{L}_i^{(h)}(X_1, \ldots, X_n) + \pi^{h+1}Y,$$

where Y is a quadratic form in $X_1, \ldots, X_n$. We can write Y in the form $Y = \sum_{i=1}^{2s}(X_iM_i) + N$, where M_i are linear forms in $X_1, \ldots, X_n$ and N is a quadratic form in $X_{2s+1}, \ldots, X_n$. We have

$$Q(T_hX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + \mathcal{Q}_h + \pi^{h+1}N$$
$$+\pi^h \sum_{i=1}^{2s}\left(X_i\mathcal{L}_i^{(h)}\right) + \pi^{h+1}\sum_{i=1}^{2s}(X_iM_i)$$
$$Q(T_hX) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + \mathcal{Q}_h + \pi^{h+1}N$$
$$+\pi^h \sum_{i=1}^{2s}\left(X_i\left(\mathcal{L}_i^{(h)} + \pi M_i\right)\right).$$

Now let $Q_h = \mathcal{Q}_h + \pi^{h+1}N$ and $L_i^{(h)} = \mathcal{L}_i^{(h)} + \pi M_i$. Notice that $Q_h \equiv \mathcal{Q}_h \equiv \widetilde{Q} \bmod \pi^2$ since $2 \leqslant h+1$. Now we obtain

$$Q(T_hX) = \sum_{i=1}^{s}(X_{2i-1}X_{2i}) + Q_h + \pi^h\sum_{i=1}^{2s}\left(X_iL_i^{(h)}\right). \qquad (\star)$$

Let U_h be the linear transformation defined by the following change of variable.

$$X_{2i-1} \mapsto \widetilde{X}_{2i-1} = X_{2i-1} - \pi^h L_{2i}^{(h)}(X_1, \ldots, X_n) \quad (1 \leqslant i \leqslant s).$$
$$X_{2i} \mapsto \widetilde{X}_{2i} = X_{2i} - \pi^h L_{2i-1}^{(h)}(X_1, \ldots, X_n) \quad (1 \leqslant i \leqslant s).$$
$$X_i \mapsto X_i \quad (2s < i \leqslant n).$$

Note that Lemma $A.1.1$ implies that U_h is an invertible linear transformation. Let $\widetilde{L}_i^{(h)}$ denote the image of $L_i^{(h)}$ under the above change of variables. That is, $\widetilde{L}_i^{(h)} = L_i^{(h)}(\widetilde{X}_1, \ldots, \widetilde{X}_{2s}, X_{2s+1}, \ldots, X_n)$. Observe that for $1 \leqslant i \leqslant s$,

$$\widetilde{L}_{2i-1}^{(h)} = L_{2i-1}^{(h)} + \pi^h L'_{2i-1} \quad \text{and} \quad \widetilde{L}_{2i}^{(h)} = L_{2i}^{(h)} + \pi^h L'_{2i}, \qquad (*)$$

where L'_{2i-1} and L'_{2i} are linear forms in the variables $X_1, \ldots, X_n$. Let $T_{h+1} = U_h T_h$. To determine $Q(T_{h+1}X)$ we apply the change of variables to the right-hand side of $(\star)$:

$$Q(T_{h+1}X) = \underbrace{\sum_{i=1}^{s} \widetilde{X}_{2i-1}\widetilde{X}_{2i}}_{(1)} + Q_h + \pi^h \underbrace{\sum_{i=1}^{2s} \widetilde{X}_i \widetilde{L}_i^{(h)}}_{(2)}. \qquad (**)$$

We will deal with the expressions (1) and (2) separately.

(1) We have

$$\widetilde{X}_{2i-1}\widetilde{X}_{2i} = (X_{2i-1} - \pi^h L_{2i}^{(h)})(X_{2i} - \pi^h L_{2i-1}^{(h)}).$$

Therefore

$$\sum_{i=1}^{s} \widetilde{X}_{2i-1}\widetilde{X}_{2i} = \sum_{i=1}^{s} (X_{2i-1}X_{2i}) - \pi^h \sum_{i=1}^{s} \left(X_{2i-1}L_{2i-1}^{(h)} + X_{2i}L_{2i}^{(h)} \right) + \pi^{2h}A,$$

where $A = \sum_{i=1}^{s} L_{2i-1}^{(h)} L_{2i}^{(h)}$. Note that A is a quadratic form in the variables $X_1, \ldots, X_n$.

(2) We have

$$\begin{aligned}
\pi^h \sum_{i=1}^{2s} \widetilde{X}_i \widetilde{L}_i^{(h)} &= \pi^h \sum_{i=1}^{s} \left(\widetilde{X}_{2i-1}\widetilde{L}_{2i-1}^{(h)} + \widetilde{X}_{2i}\widetilde{L}_{2i}^{(h)} \right). \\
&= \pi^h \sum_{i=1}^{s} \left((X_{2i-1} - \pi^h L_{2i}^{(h)})\widetilde{L}_{2i-1}^{(h)} + (X_{2i} - \pi^h L_{2i-1}^{(h)})\widetilde{L}_{2i}^{(h)} \right). \\
&= \pi^h \sum_{i=1}^{s} \left(X_{2i-1}\widetilde{L}_{2i-1}^{(h)} + X_{2i}\widetilde{L}_{2i}^{(h)} \right) - \pi^{2h} \sum_{i=1}^{s} \left(L_{2i}^{(h)}\widetilde{L}_{2i-1}^{(h)} + L_{2i-1}^{(h)}\widetilde{L}_{2i}^{(h)} \right). \\
&= \pi^h \sum_{i=1}^{s} \left(X_{2i-1}\widetilde{L}_{2i-1}^{(h)} + X_{2i}\widetilde{L}_{2i}^{(h)} \right) - \pi^{2h}B,
\end{aligned}$$

where $B = \sum_{i=1}^{s} L_{2i}^{(h)}\widetilde{L}_{2i-1}^{(h)} + L_{2i-1}^{(h)}\widetilde{L}_{2i}^{(h)}$. Note that B is a quadratic form in the variables $X_1, \ldots, X_n$.

Now the right-hand side of $(**)$ becomes

$$\begin{aligned}
&\sum_{i=1}^{s} X_{2i-1}X_{2i} - \pi^h \sum_{i=1}^{s} \left(X_{2i-1}L_{2i-1}^{(h)} + X_{2i}L_{2i}^{(h)} \right) + \pi^{2h}A + Q_h \\
&\qquad + \pi^h \sum_{i=1}^{s} \left(X_{2i-1}\widetilde{L}_{2i-1}^{(h)} + X_{2i}\widetilde{L}_{2i}^{(h)} \right) - \pi^{2h}B. \\
&\qquad = \sum_{i=1}^{s} (X_{2i-1}X_{2i}) + \pi^{2h}(A - B) + Q_h
\end{aligned}$$

$$+\pi^h \sum_{i=1}^{s} \left(X_{2i-1}(\widetilde{L}_{2i-1}^{(h)} - L_{2i-1}^{(h)}) + X_{2i}(\widetilde{L}_{2i}^{(h)} - L_{2i}^{(h)}) \right).$$

Using the equations in $(*)$ yields

$$= \sum_{i=1}^{s} (X_{2i-1}X_{2i}) + \pi^{2h}(A - B) + Q_h$$

$$+\pi^h \sum_{i=1}^{s} \left(X_{2i-1}(\pi^h L'_{2i}) + X_{2i}(\pi^h L'_{2i}) \right).$$

$$= \sum_{i=1}^{s} (X_{2i-1}X_{2i}) + \pi^{2h}(A - B) + Q_h + \pi^{2h}C,$$

where $C = \sum_{i=1}^{s} X_{2i-1}L'_{2i} + X_{2i}L'_{2i}$. Note that C is a quadratic form in the variables $X_1, \ldots, X_n$. We have shown that the right-hand side of $(**)$ is

$$\sum_{i=1}^{s} (X_{2i-1}X_{2i}) + \pi^{2h}(A - B + C) + Q_h. \qquad (***)$$

Note that $(A - B + C)$ is a quadratic form in the variables $X_1, \ldots, X_n$. Therefore, we can write

$$(A - B + C) = \sum_{i=1}^{2s} (X_i R_i) + S(X_{2s+1}, \ldots, X_n),$$

where the R_i are linear forms in $X_1, \ldots, X_n$ and S is a quadratic form in $X_{2s+1}, \ldots, X_n$. Now $(***)$ becomes

$$\sum_{i=1}^{s} (X_{2i-1}X_{2i}) + \pi^{2h} \left(\sum_{i=1}^{2s} (X_i R_i) + S \right) + Q_h.$$

Let $\mathcal{L}_i^{h+1} = \pi^{h-1}R_i$ and $\mathcal{Q}_{h+1} = \pi^{2h}S + Q_h$. Then $\mathcal{Q}_{h+1} \equiv Q_h \equiv \widetilde{Q} \bmod \pi^2$. In conclusion we have shown that

$$Q(T_{h+1}X) = X_1X_2 + \cdots + X_{2s-1}X_{2s} + \mathcal{Q}_{h+1}(X_{2s+1}, \ldots, X_n)$$

$$+\pi^{h+1} \sum_{i=1}^{2s} X_i \mathcal{L}_i^{(h+1)}(X_1, \ldots, X_n).$$

It follows that $Q(T_{h+1}X)$ is congruent to the right-hand of the above equation modulo π^{h+2}, which completes the induction argument.

□

Lemma $A.1.3$ is a generalization of an argument from the proof of Lemma 7.2 on page 58 of [7].

Lemma A.1.3. *Given quadratic forms S_1 and S_2 in k variables over $\mathcal{O}_K$, assume k is odd and*

$$S_1 \equiv X_1X_2 + \cdots + X_{k-2}X_{k-1} \bmod \pi$$

and

$$\pi \nmid S_2(e_k).$$

Then there exist $\lambda \in \mathcal{O}_K$ and a transformation $T \in GL_k(\mathcal{O}_K)$ such that

$$T(e_k) = e_k$$

and

$$(S_1 - \lambda S_2)(TX) = X_1X_2 + \cdots + X_{k-2}X_{k-1}.$$

Moreover, $\lambda \equiv S_1(e_k)(S_2(e_k))^{-1} \bmod \pi^2$.

Proof. We will show that for all positive integers f there exist suitable λ_f and T_f such that

$$(S_1 - \lambda_f S_2)(T_f X) \equiv X_1X_2 + \cdots + X_{2t-1}X_{2t} \bmod \pi^f, \tag{A.1.1}$$

where $t = \frac{k-1}{2}$ and $T_f(e_k) = e_k$. We prove this by induction on f, but before we do, we will explain why this condition is enough to prove the lemma. Let λ_f and T_f be chosen for each $f \geqslant 1$ so that $A.1.1$ holds. Because $\mathcal{O}_K$ is compact, the sequence $\{\lambda_f\}_{f\geqslant 1}$ converges to some $\lambda \in \mathcal{O}_K$. Because $\mathrm{GL}_k(\mathcal{O}_K)$ is compact, the sequence $\{T_f\}_{f\geqslant 1}$ converges to some $T \in \mathrm{GL}_k(\mathcal{O}_K)$. For this λ and T, we see that $A.1.1$ holds for all $f \geqslant 1$. Since $\pi^f \to 0$ as $f \to \infty$, we get $(S_1 - \lambda S_2)(TX) = X_1X_2 + \cdots + X_{2t-1}X_{2t}$, as desired.

Now, to prove $A.1.1$ by induction, first note that the hypothesis of the lemma gives us the case $f = 1$, where $T_1 = \mathrm{id}$ and $\lambda_1 = 0$. Assume now by induction that λ_f and T_f are chosen so that $A.1.1$ holds for $f \geqslant 1$. We will show the corresponding statement holds for $f + 1$.

Let

$$S(X) = (S_1 - \lambda_f S_2)(T_f X). \tag{A.1.2}$$

By induction,

$$S(X) = X_1X_2 + \cdots + X_{2t-1}X_{2t} + \pi^f Q$$

for some quadratic form $Q = Q(X_1, \ldots, X_k)$ over $\mathcal{O}_K$. Note that Q depends on λ_f and T_f, and $2t = k - 1$. We can write Q in the following way

$$Q = S'(X_1, \ldots, X_{2t}) + X_k L(X_1, \ldots, X_{2t}) + cX_k^2.$$

We know Q depends on λ_f and T_f, so in particular, c depends on f. Substituting the above formula for Q into the equation for $S(X)$ gives us

$$\begin{aligned} S(X) = X_1X_2 + \cdots + X_{2t-1}X_{2t} + \pi^f S'(X_1, \ldots, X_{2t}) \\ + \pi^f X_k L(X_1, \ldots, X_{2t}) + \pi^f c X_k^2. \end{aligned} \tag{A.1.3}$$

Define $U(X) = S_2(T_f X)$. We can express $S_2(T_f X)$ in the following way:

$$U(X) = S_2(T_f X) = U_0(X_1, \ldots, X_{2t}) + M(X_1, \ldots, X_{2t})X_k + dX_k^2, \tag{A.1.4}$$

where U_0 is a quadratic form over $\mathcal{O}_K$, M is a linear form over $\mathcal{O}_K$, and $d \in \mathcal{O}_K$. By induction $T_f(e_k) = e_k$. It follows that

$$U(e_k) = S_2(e_k) = d. \tag{A.1.5}$$

By hypothesis, $\pi \nmid d$. We now examine $S - \pi^f cd^{-1}U$, which has coefficients in $\mathcal{O}_K$. By construction, this form has no term in X_k^2; indeed, observe

$$S(e_k) - \pi^f cd^{-1}U(e_k) = \pi^f c - \pi^f c = 0.$$

Define $V(X_1, \ldots, X_{2t}) = (S - \pi^f cd^{-1}U)(X_1, \ldots, X_{2t}, 0)$. Looking at $A.1.3$ and $A.1.4$, togehter with V, we can write

$$\begin{aligned}(S - \pi^f cd^{-1}U)(X) = {} & V(X_1, \ldots, X_{2t}) \\ & + X_k \pi^f (L(X_1, \ldots, X_{2t}) - cd^{-1}M(X_1, \ldots, X_{2t})).\end{aligned} \tag{A.1.6}$$

Again, looking at $A.1.3$ and $A.1.4$, we can write V as

$$\begin{aligned}V(X_1, \ldots, X_{2t}) &= S(X_1, \ldots, X_{2t}, 0) - \pi^f cd^{-1}U(X_1, \ldots, X_{2t}, 0) \\ &= X_1X_2 + \cdots + X_{2t-1}X_{2t} \\ &\quad + \pi^f S'(X_1, \ldots, X_{2t}) - \pi^f cd^{-1}U_0(X_1, \ldots, X_{2t}).\end{aligned}$$

Notice $V \equiv X_1X_2 + \cdots + X_{2t-1}X_{2t} \mod \pi$. Thus Lemma $A.1.2$ implies there is a transformation $T_0 \in \mathrm{GL}_{2t}(\mathcal{O}_K)$ such that

$$V(T_0(X_1, \ldots, X_{2t})) = X_1X_2 + \cdots + X_{2t-1}X_{2t}. \tag{A.1.7}$$

We will extend T_0 to a transformation $T' \in \mathrm{GL}_k(\mathcal{O}_K)$. Define $T' \in \mathrm{GL}_k(\mathcal{O}_K)$ so that

$$T'(x_1, \ldots, x_{2t}, 0) = T_0(x_1, \ldots, x_{2t})$$

and

$$T'(e_k) = e_k.$$

Looking at equation $A.1.6$, we can write $(S - \pi^f cd^{-1}U)(T'X)$ as

$$\begin{aligned}(S - \pi^f cd^{-1}U)(T'X) = {} & V(T_0(X_1, \ldots, X_{2t})) \\ & + X_k \pi^f \big(L(T_0(X_1, \ldots, X_{2t})) - cd^{-1}M(T_0(X_1, \ldots, X_{2t}))\big).\end{aligned} \tag{A.1.8}$$

Let

$$L'(X_1, \ldots, X_{2t}) = L(T_0(X_1, \ldots, X_{2t})) - cd^{-1}M(T_0(X_1, \ldots, X_{2t})).$$

Substituting this, together our expression for V in $A.1.7$, into equation $A.1.8$ yields

$$(S - \pi^f cd^{-1}U)(T'X) = X_1X_2 + \cdots + X_{2t-1}X_{2t} + X_k \pi^f L'(X_1, \ldots, X_{2t}). \tag{A.1.9}$$

Suppose $L' = \sum_{i=1}^{2t} a_i X_i$. Let $\gamma_{2i} = -a_{2i-1}$ and $\gamma_{2i-1} = -a_{2i}$ for $1 \leqslant i \leqslant t$. Consider the change in variables given by

$$X_i \to X_i + \pi^f \gamma_i X_k \qquad 1 \leqslant i \leqslant 2t.$$

Notice what happens when we apply this change in variables to the monomial $X_{2i-1}X_{2i}$:

$$\begin{aligned} X_{2i-1}X_{2i} &\to (X_{2i-1} + \pi^f \gamma_{2i-1} X_k)(X_{2i} + \pi^f \gamma_{2i} X_k) \\ &= X_{2i-1}X_{2i} + \pi^f \gamma_{2i} X_{2i-1} X_k + \pi^f \gamma_{2i-1} X_{2i} X_k + \pi^{2f} \gamma_{2i-1}\gamma_{2i} X_k^2. \\ &= X_{2i-1}X_{2i} - \pi^f a_{2i-1} X_{2i-1} X_k - \pi^f a_{2i} X_{2i} X_k + \pi^{2f} \gamma_{2i-1}\gamma_{2i} X_k^2. \end{aligned}$$

Observe that $\pi^f a_{2i-1} X_{2i-1} X_k$ and $\pi^f a_{2i} X_{2i} X_k$ are terms in $X_k \pi^f L'$. Therefore, applying this change in variables to $A.1.9$ will make $X_k \pi^f L(X_1, \ldots, X_{2t})$ vanish, leaving us with a form of the shape

$$(S - \pi^f c d^{-1})(T'X) = X_1X_2 + \cdots + X_{2t-1}X_{2t} + \pi^{2f} c' X_k^2 \qquad \text{(A.1.10)}$$

for some $c' \in \mathcal{O}_K$. Using equations $A.1.2$ and $A.1.4$, we can write the left-hand side of equation $A.1.10$ as

$$\begin{aligned} (S - \pi^f c d^{-1} U)(T'X) &= S(T'X) - \pi^f c d^{-1} U(T'X). \\ &= (S_1 - \lambda_f S_2)(T_f T' X) - \pi^f c d^{-1} S_2(T_f T' X). \\ &= (S_1 - (\lambda_f + \pi^f c d^{-1}) S_2)(T_f T' X). \end{aligned}$$

Since $T_f(e_k) = T'(e_k) = e_k$, we see $(T_f T')(e_k) = e_k$. Let

$$T_{f+1} = T_f T' \quad \text{and} \quad \lambda_{f+1} = \lambda_f + \pi^f c d^{-1}.$$

Since $f \geqslant 1$, we have $2f > f$. Substituting the above into the left-hand side of equation $A.1.10$ yields

$$\begin{aligned} (S_1 - \lambda_{f+1} S_2)(T_{f+1} X) &= X_1X_2 + \cdots + X_{2t-1}X_{2t} + \pi^{2f} c' X_k^2. \\ &\equiv X_1X_2 + \cdots + X_{2t-1}X_{2t} \bmod \pi^{f+1}. \end{aligned}$$

This completes the induction argument. To finish, we will show that

$$\lambda \equiv S_1(e_k)(S_2(e_k))^{-1} \bmod \pi^2.$$

Since $\lambda_{f+1} = \lambda_f + \pi^f c d^{-1}$, we get $\lambda_{f+1} \equiv \lambda_f \bmod \pi^f$. Therefore,

$$\lambda_f \equiv \lambda_{f-1} \bmod \pi^{f-1}.$$

$$\lambda_{f-1} \equiv \lambda_{f-2} \bmod \pi^{f-2}.$$

$$\vdots$$

$$\lambda_3 \equiv \lambda_2 \bmod \pi^2.$$

Thus, for all $f \geqslant 2$, $\lambda_f \equiv \lambda_2 \bmod \pi^2$. Since λ is the limit of the Cauchy sequence $\{\lambda_f\}_{f\geqslant 1}$, we obtain $\lambda \equiv \lambda_2 \bmod \pi^2$. We will show that $\lambda_2 = S_1(e_k)(S_2(e_k))^{-1}$.

We know $\lambda_2 = \lambda_1 + \pi c d^{-1}$, where c is as in equation $A.1.3$ with $f = 1$, and from equation $A.1.5$, we know $d = S_2(e_k)$. From equation $A.1.3$, we see that πc is the coefficient of X_k^2 in $S(X)$; that is, $S(e_k) = \pi c$. From equation $A.1.2$, we see that $S(X) = (S_1 - \lambda_1 S_2)(T_1 X)$. From the beginning of the proof, we established that $\lambda_1 = 0$ and $T_1 = \text{id}$. Therefore, $S(X) = S_1(X)$, and so $\pi c = S(e_k) = S_1(e_k)$. We conclude that

$$\lambda_2 = \lambda_1 + \pi c d^{-1} = S_1(e_k)(S_2(e_k))^{-1}.$$

□

Lemma A.1.4. *Let $n \geqslant 5$ be odd and $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be quadratic forms. Suppose that*

1. *$Q_1(X_1, \ldots, X_{n-2}, 0, 0) \equiv X_1X_2 + \cdots + X_{n-4}X_{n-3} \bmod \pi$, and*
2. *$\pi \nmid Q_2(e_{n-2})$.*

Then there exists $\lambda \in \mathcal{O}_K$ such that $(Q_1 - \lambda Q_2)(X)$ vanishes on a subspace over K of dimension $\frac{n-1}{2}$. Moreover, $\lambda \equiv Q_1(e_{n-2})(Q_2(e_{n-2}))^{-1} \bmod \pi^2$.

Proof. Let $S_i(X_1, \ldots, X_{n-2}) = Q_i(X_1, \ldots, X_{n-2}, 0, 0)$. Then S_1 and S_2 satisfy the hypothesis of Lemma $A.1.3$ with $k = n-2$. According to the lemma, there exist $\lambda \in \mathcal{O}_K$ and $T' \in \mathrm{GL}_{n-2}(\mathcal{O}_K)$ such that

$$(S_1 - \lambda S_2)(T'(X_1, \ldots, X_{n-2})) = X_1X_2 + \cdots + X_{n-4}X_{n-3},$$

with $T'(e_{n-2}) = e_{n-2}$, and $\lambda \equiv S_1(e_{n-2})(S_2(e_{n-2}))^{-1} \bmod \pi^2$. Thus

$$\lambda \equiv Q_1(e_{n-2})(Q_2(e_{n-2}))^{-1} \bmod \pi^2.$$

Extend T' to an invertible matrix matrix $T \in \mathrm{GL}_n(\mathcal{O}_K)$ in the following way: for $1 \leqslant i \leqslant n-2$, let $T(e_i) = T'(e_i)$, and for $n-1 \leqslant j \leqslant n$, let $T(e_j) = e_j$. We have

$$(Q_1 - \lambda Q_2)(X) = (S_1 - \lambda S_2)(X_1, \ldots, X_{n-2}) + X_{n-1}L_1(X) + X_nL_2(X),$$

where L_1, L_2 are linear forms over $\mathcal{O}_K$ with $X = (X_1, \ldots, X_n)$. It follows that

$$(Q_1 - \lambda Q_2)(TX) = X_1X_2 + \cdots + X_{n-4}X_{n-3} + X_{n-1}L_1'(X) + X_nL_2'(X),$$

where $L_1'(X) = L_1(TX)$ and $L_2'(X) = L_2(TX)$. Notice that $(Q_1 - \lambda Q_2)(TX)$ vanishes whenever the following $\frac{n+1}{2}$ variables all equal zero:

$$X_1 = X_3 = \cdots X_{n-4} = X_{n-1} + X_n = 0.$$

Therefore, $(Q_1 - \lambda Q_2)(TX)$ vanishes on a subspace over K of dimension $n - \frac{n+1}{2} = \frac{n-1}{2}$. Since T is invertible, the same is true for $(Q_1 - \lambda Q_2)(X)$. □

Lemma A.1.5. *Let $n \geqslant 5$ be odd and $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms. Suppose that*

1. $Q_1(X_1, \ldots, X_{n-2}, 0, 0) \equiv X_1X_2 + \cdots + X_{n-4}X_{n-3} \bmod \pi$, *and*
2. $\pi \nmid Q_2(e_{n-2})$.

Then there exists a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off $\frac{n-1}{2}$ hyperbolic planes over K.

Proof. By Lemma A.1.4, there exists a form $Q \in \mathcal{P}_K(Q_1, Q_2)$ that vanishes on a subspace over K of dimension $\frac{n-1}{2}$. Since $\{Q_1, Q_2\}$ is nonsingular, Theorem 2.1.27 implies that every form in $\mathcal{P}_K(Q_1, Q_2)$ either has rank $n-1$ or n over K. If Q has rank n, then Theorem B.1.1 implies that Q splits off $\frac{n-1}{2}$ hyperbolic planes over K. If Q has rank $n-1$, then after an invertible linear change of variables, we can assume $Q = Q'(X_1, \ldots, X_{n-1})$, where Q' is a quadratic form over K of rank $n-1$. Since Q vanishes on a subspace over K of dimension $\frac{n-1}{2}$, the form Q' vanishes on a subspace over K of dimension $\frac{n-3}{2}$. By applying Lemma 2.3.12 with $m = \frac{n-3}{2}$, we conclude that there is a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off $m + 1 = \frac{n-1}{2}$ hyperbolic planes over K. ☐

For any matrices $U \in \mathrm{GL}_2(K)$ and $T \in \mathrm{GL}_n(K)$ we define actions on pairs of quadratic forms Q_1, Q_2 by setting

$$(Q_1, Q_2)^U = (U_{11}Q_1 + U_{12}Q_2, U_{21}Q_1 + U_{22}Q_2)$$

and

$$(Q_1(X), Q_2(X))_T = (Q_1(TX), Q_2(TX)).$$

This notation is also introduced in section A.2. In particular, Lemma A.2.1 implies that the K-pencil generated by (Q_1, Q_2) contains a form which splits off j hyperbolic planes if and only if the same is true for the K-pencil generated by $(Q_1, Q_2)^U_T$. We will use this fact in the next few lemmas. The reader can verify that there is no circular logic being used.

Lemma A.1.6. *Let $n \geqslant 5$ be odd and $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be a nonsingular pair of quadratic forms. Suppose that*

1. $Q_1(X_1, \ldots, X_{n-2}, 0, 0) \equiv X_1X_2 + \cdots + X_{n-4}X_{n-3} \bmod \pi$,
2. $Q_2(X_1, \ldots, X_{n-2}, 0, 0) \equiv Q_2'(X_1, \ldots, X_{n-3}) \bmod \pi$ *for some quadratic form Q_2'*,
3. $\pi^2 \mid Q_1(e_{n-2})$, *and*
4. $\pi^2 \nmid Q_2(e_{n-2})$.

Then there exists a form in $\mathcal{P}_K(Q_1, Q_2)$ that splits off $\frac{n-1}{2}$ hyperbolic planes.

Proof. We can write Q_1 and Q_2 in the following way:

$$Q_1 = Q_1(X_1, \ldots, X_{n-2}, 0, 0) + X_{n-1}S_1(X) + X_n S_1'(X),$$

$$Q_2 = Q_2(X_1, \ldots, X_{n-2}, 0, 0) + X_{n-1}S_2(X) + X_n S_2'(X),$$

where $X = (X_1, \ldots, X_n)$, and S_i, S_i' are linear forms over $\mathcal{O}_K$. Conditions (1) and (2) imply that

$$\begin{aligned} Q_1(X_1, \ldots, X_{n-2}, 0, 0) &= X_1X_2 + \cdots + X_{n-4}X_{n-3} \\ &\quad + \pi H_1(X_1, \ldots, X_{n-2}), \\ Q_2(X_1, \ldots, X_{n-2}, 0, 0) &= Q_2'(X_1, \ldots, X_{n-3}) \\ &\quad + \pi H_2(X_1, \ldots, X_{n-2}), \end{aligned} \tag{A.1.11}$$

for some quadratic forms H_1, H_2 over $\mathcal{O}_K$. Note $Q_1(e_{n-2}) = \pi H_1(e_{n-2})$. Condition (3) then implies that $\pi \mid H_1(e_{n-2})$, so we write $H_1(e_{n-2}) = \pi c$ for some $c \in \mathcal{O}_K$. Likewise, we have $Q_2(e_{n-2}) = \pi H_2(e_{n-2})$, so condition (4) implies that $H_2(e_{n-2}) = d$ for some unit d. We can write H_1 and H_2 in the following way:

$$\begin{aligned} H_1 &= H_1'(X_1, \ldots, X_{n-3}) + X_{n-2}L(X_1, \ldots, X_{n-3}) + \pi c X_{n-2}^2, \\ H_2 &= H_2'(X_1, \ldots, X_{n-3}) + X_{n-2}L'(X_1, \ldots, X_{n-3}) + d X_{n-2}^2, \end{aligned} \tag{A.1.12}$$

where H_1', H_2' are quadratic forms over $\mathcal{O}_K$ and L, L' are linear forms over $\mathcal{O}_K$. We now have the following formulas for Q_1 and Q_2.

$$\begin{aligned} Q_1 &= X_1X_2 + \cdots + X_{n-4}X_{n-3} + \pi H_1'(X_1, \ldots, X_{n-3}) \\ &\quad + \pi X_{n-2}L(X_1, \ldots, X_{n-3}) + \pi^2 c X_{n-2}^2 \\ &\quad + X_{n-1}S_1(X) + X_n S_1'(X). \\ Q_2 &= Q_2'(X_1, \ldots, X_{n-3}) + \pi H_2'(X_1, \ldots, X_{n-3}) \\ &\quad + \pi X_{n-2}L'(X_1, \ldots, X_{n-3}) + \pi d X_{n-2}^2 \\ &\quad + X_{n-1}S_2(X) + X_n S_2'(X). \end{aligned} \tag{A.1.13}$$

Set

$$T = \mathrm{diag}(\pi, \pi, \ldots, \pi, 1, \pi^3, \pi^3),$$

and

$$U = \mathrm{diag}(\pi^{-2}, \pi^{-1}).$$

Let $(V_1, V_2) = (Q_1, Q_2)_T^U$. Then

$$\begin{aligned} V_1 &\equiv X_1X_2 + \cdots + X_{n-4}X_{n-3} \\ &\quad + X_{n-2}L(X_1, \ldots, X_{n-3}) + cX_{n-2}^2 \bmod \pi. \\ V_2 &\equiv dX_{n-2}^2 \bmod \pi. \end{aligned} \tag{A.1.14}$$

For each $1 \leqslant i \leqslant n-3$, there exist $c_i \in \mathcal{O}_K$ so that a change of variable of the type

$$X_i' = X_i + c_i X_{n-2} \qquad 1 \leqslant i \leqslant n-3$$

gives us

$$V_1 \equiv X_1'X_2' + \cdots + X_{n-4}'X_{n-3}' + c'X_{n-2}^2 \bmod \pi$$

for some $c' \in \mathcal{O}_K$. This change of variable leaves $V_2 \equiv dX_{n-2}^2 \bmod \pi$. Let $t = -d^{-1}c'$ and $V_1' = V_1 + tV_2$. Then

$$V_1' \equiv X_1'X_2' + \cdots + X_{n-4}'X_{n-3}' \bmod \pi.$$

Now V_1', V_2 satisfy the hypothesis of Lemma $A.1.5$, in which case Lemma $A.1.5$ implies that there exists a form in $\mathcal{P}_K(V_1', V_2)$ that splits off $\frac{n-1}{2}$ hyperbolic planes over K. Lemma $A.2.1$ implies that since $\mathcal{P}_K(V_1', V_2)$ contains a form which splits off $\frac{n-1}{2}$ hyperbolic planes, the same is true for $\mathcal{P}_K(Q_1, Q_2)$.

□

A.2 Minimized Pairs

We will describe the v-adic minimization process due to Birch, Lewis, and Murphy [4].

Let K be a p-adic field, $\mathcal{O}_K$ the ring of integers, and k the residue field. Let π be a uniformizing element for K. Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be the valuation map, with $v(\pi) = 1$.

We define

$$F(x, y; Q_1, Q_2) = F(x, y) = \det(xQ_1 + yQ_2).$$

We assume the variety $Q_1 = Q_2 = 0$ is nonsingular, so that Lemma 2.1.27 implies that $F(x, y)$ does not vanish identically and has no repeated factors. Consider $\operatorname{disc}(F(x, y))$ where $\operatorname{disc}(F(x, y))$ is the discriminant of $F(x, y)$, as defined in definition $D.1.1$. From definition $D.2.2$, we have

$$\operatorname{disc}(F) = \Delta(Q_1, Q_2),$$

where $\Delta(Q_1, Q_2)$ is as in definition $D.2.1$.

If the forms Q_1 and Q_2 are defined over $\mathcal{O}_K$, then Proposition $D.2.4$ implies that $\Delta(Q_1, Q_2) \in \mathcal{O}_K$. For any matrices $U \in \mathrm{GL}_2(K)$ and $T \in \mathrm{GL}_n(K)$ we define actions on pairs of quadratic forms Q_1, Q_2 by setting

$$(Q_1, Q_2)^U = (U_{11}Q_1 + U_{12}Q_2, U_{21}Q_1 + U_{22}Q_2)$$

and

$$(Q_1(X), Q_2(X))_T = (Q_1(TX), Q_2(TX)).$$

Given a quadratic form $Q \in K[X_1, \ldots, X_n]$, we define

$$\nabla Q = (Q_{X_1}, Q_{X_2}, \ldots, Q_{X_n}),$$

where Q_{X_i} is the partial derivative of Q with respect to X_i. Thus $Q_{X_i} \in K[X_1, \ldots, X_n]$ is a linear form. For $u \in K^n$, we define

$$\nabla Q(u) = (Q_{X_1}(u), Q_{X_2}(u), \ldots, Q_{X_n}(u)).$$

Thus, by Definition 2.1.25, a pair $Q_1, Q_2 \in K[X_1, \ldots, X_n]$ is nonsingular if and only if for each nonzero $x \in (K^{\mathrm{alg}})^n$ such that $Q_1(x) = Q_2(x) = 0$, the matrix

$$\begin{bmatrix} \nabla Q_1(x) \\ \nabla Q_2(x) \end{bmatrix} = \begin{bmatrix} \frac{\partial Q_1}{\partial X_1}(x) & \frac{\partial Q_1}{\partial X_2}(x) & \cdots & \frac{\partial Q_1}{\partial X_n}(x) \\ \frac{\partial Q_2}{\partial X_1}(x) & \frac{\partial Q_2}{\partial X_2}(x) & \cdots & \frac{\partial Q_2}{\partial X_n}(x) \end{bmatrix}$$

has rank 2.

Lemma A.2.1. *Given two quadratic forms $Q_1, Q_2 \in F[X_1, \ldots, X_n]$ defined over a field F, we have the following:*

(1) The variety $Q_1 = Q_2 = 0$ is nonsingular if and only if the same is true for the forms $(Q_1, Q_2)_T^U$.

(2) Q_1, Q_2 both vanish on a subspace over F of dimension i if and only if the same is true for $(Q_1, Q_2)_T^U$.

(3) The pencil defined over F by Q_1, Q_2 contains a form which splits off t hyperbolic planes if and only if the same is true for the forms $(Q_1, Q_2)_T^U$.

Proof. (1) We prove (1) first. We handle the actions of U and T separately. We begin with $(Q_1, Q_2)^U$. Let $Q_1'(X) = U_{11}Q_1(X) + U_{12}Q_2(X)$ and $Q_2'(X) = U_{21}Q_1(X) + U_{22}Q_2(X)$. Observe that

$$\begin{bmatrix} Q_1'(X) \\ Q_2'(X) \end{bmatrix} = \begin{bmatrix} U_{11}Q_1(X) + U_{12}Q_2(X) \\ U_{21}Q_1(X) + U_{22}Q_2(X) \end{bmatrix} = \begin{bmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{bmatrix} \begin{bmatrix} Q_1(X) \\ Q_2(X) \end{bmatrix}.$$

Since U is invertible, we see that $Q_i'(x) = 0$ if and only if $Q_i(x) = 0$ for $i = 1, 2$. Given such a point x, observe that

$$\begin{bmatrix} \nabla Q_1'(x) \\ \nabla Q_2'(x) \end{bmatrix} = \begin{bmatrix} U_{11}\nabla Q_1(x) + U_{12}\nabla Q_2(x) \\ U_{21}\nabla Q_1(x) + U_{22}\nabla Q_2(x) \end{bmatrix} = \begin{bmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{bmatrix} \begin{bmatrix} \nabla Q_1(x) \\ \nabla Q_2(x) \end{bmatrix}.$$

Since U is invertible, we see that $\begin{bmatrix} \nabla Q_1'(x) \\ \nabla Q_2'(x) \end{bmatrix}$ has rank 2 if and only if $\begin{bmatrix} \nabla Q_1(x) \\ \nabla Q_2(x) \end{bmatrix}$ has rank 2. We conclude that $Q_1 = Q_2 = 0$ is nonsingular if and only if the same is true for $(Q_1, Q_2)^U$.

As for $(Q_1, Q_2)_T$ we note that if x is a singular common zero of $Q_1(X)$ and $Q_2(X)$, then $T^{-1}x$ is a singular common zero of $Q_1(TX)$ and $Q_2(TX)$. We deduce that (Q_1, Q_2) is nonsingular if and only if the same is true for $(Q_1, Q_2)_T$.

(2) Now we prove (2). Let $S \subseteq F^n$ be an i-dimensional space for which Q_1, Q_2 vanish on. Then $(Q_1, Q_2)^U$ also vanishes on S. Conversely, assume that $(Q_1, Q_2)^U$ vanishes on an i-dimensional space $S' \subseteq k^n$. Let $x \in S'$. Since x is a common zero of $(Q_1, Q_2)^U$, we have that

$$U \begin{bmatrix} Q_1(x) \\ Q_2(x) \end{bmatrix} = \vec{0}.$$

Since U is invertible, this implies $Q_1(x) = Q_2(x) = 0$, hence the pair (Q_1, Q_2) vanishes on S' too. We have shown that (Q_1, Q_2) vanishes on an i-dimensional space if and only if the same is true for $(Q_1, Q_2)^U$.

On the other hand, since T is invertible, T maps the space S isomorphically onto another space of of the same dimension. Therefore, (Q_1, Q_2) vanish on an i-dimensional space if and only if the same is true for $(Q_1, Q_2)_T$.

(3) Finally, we prove (3). Since T is invertible, every form in (Q_1, Q_2) is equivalent to some form in $(Q_1, Q_2)_T$, and vice versa. Thus the pencil (Q_1, Q_2) contains a form which splits off t hyperbolic planes if and only if the same is true for $(Q_1, Q_2)_T$. To prove the analogous statement for $(Q_1, Q_2)^U$, it suffices to show that the pencil (Q_1, Q_2) and $(Q_1, Q_2)^U$ are the same.

To that end, let $Q_1' = U_{11}Q_1 + U_{12}Q_2$ and $Q_2' = U_{21}Q_1 + U_{22}Q_2$. We will show $(Q_1, Q_2) = (Q_1', Q_2')$. Note $(Q_1', Q_2') \subseteq (Q_1, Q_2)$. On the other hand, if $aQ_1 + bQ_2 \in (Q_1, Q_2)$, then we want values for x and y such that

$$\begin{aligned} aQ_1 + bQ_2 &= xQ_1' + yQ_2'. \\ &= x(U_{11}Q_1 + U_{12}Q_2) + y(U_{21}Q_1 + U_{22}Q_2). \\ &= (xU_{11} + yU_{21})Q_1 + (xU_{12} + yU_{22})Q_2. \end{aligned} \tag{$***$}$$

Since U is invertible, the matrix equation

$$U^t \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} U_{11} & U_{21} \\ U_{12} & U_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

is solvable, in which case we find values for x and y satisfying $(***)$.

□

Definition A.2.2. *Two quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ are said to be minimized if there are no matrices $U \in GL_2(K)$ and $T \in GL_n(K)$ such that $(Q_1, Q_2)_T^U$ is integral and*

$$|\Delta(Q_1, Q_2)_T^U|_v > |\Delta(Q_1, Q_2)|_v \tag{1}$$

where $|\cdot|_v$ is the v-adic absolute value: $|a|_v = c^{v(a)}$ where $0 < c < 1$. Thus the above inequality states that

$$c^{v(\Delta(Q_1,Q_2)_T^U)} > c^{v(\Delta(Q_1,Q_2))}$$

which in turn is true if and only if

$$v(\Delta(Q_1, Q_2)_T^U) < v(\Delta(Q_1, Q_2)). \tag{2}$$

Our next lemma shows that there always exist matrices U and T for which $(Q_1, Q_2)_T^U$ is minimized.

Lemma A.2.3. *Given a nonsingular pair of quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$, there exist matrices U and T for which $(Q_1, Q_2)_T^U$ is minimized.*

Proof. If Q_1, Q_2 is already minimized, then take $U = \mathrm{id}_{2\times 2}$ and $T = \mathrm{id}_{n\times n}$. Otherwise, if Q_1, Q_2 is not minimized, then there exist matrices U' and T' such that $(Q_1, Q_2)_{T'}^{U'}$ is integral and U' and T' satisfy (2):

$$v(\Delta(Q_1, Q_2)_{T'}^{U'}) < v(\Delta(Q_1, Q_2)).$$

If $(Q_1, Q_2)_{T'}^{U'}$ is minimized, then we are done. Otherwise, there exists U'' and T'' such that the action of U'' and T'' on $(Q_1, Q_2)_{T'}^{U'}$ yields a pair of integral forms and

$$v(\Delta(Q_1, Q_2)_{T'T''}^{U'U''}) < v(\Delta(Q_1, Q_2)_{T'}^{U'}) < v(\Delta(Q_1, Q_2)). \tag{A.2.1}$$

Again, if $(Q_1, Q_2)_{T'T''}^{U'U''}$ is minimized, then we're done. Otherwise, we may continue this process. Ultimately, as we continue to repeat this process, we obtain pairs (U_i, T_i) such that $\Delta(Q_1, Q_2)_{T_i}^{U_i}$ is integral and

$$\cdots < v(\Delta(Q_1, Q_2)_{T_i}^{U_i}) < v(\Delta(Q_1, Q_2)_{T_{i-1}}^{U_{i-1}}) < \cdots < v(\Delta(Q_1, Q_2)).$$

By Proposition $D.2.4$, each of the terms $\Delta(Q_1, Q_2)_{T_i}^{U_i}$ belong in $\mathcal{O}_K$, in which case

$$v(\Delta(Q_1, Q_2)_{T_i}^{U_i}) \in \mathbb{Z}_{\geqslant 0}.$$

Further, we are assuming that Q_1, Q_2 is a nonsingular pair, and this implies that $\Delta(Q_1, Q_2) \neq 0$. Thus $v(\Delta(Q_1, Q_2))$ is a positive integer. By Lemma $A.2.1$, the pairs $(Q_1, Q_2)_{T_i}^{U_i}$ are also nonsginular, hence $v(\Delta(Q_1, Q_2)_{T_i}^{U_i}$ are also positive integers. In conclusion, we have shown that $A.2.1$ above represents a decreasing sequence of positive integers. Thus, the sequence

$$\{v(\Delta(Q_1, Q_2)_{T_i}^{U_i})\}_{i \geqslant 1}$$

eventually terminates, leaving us with a pair of matrices U and T for which $(Q_1, Q_2)_T^U$ is minimized. □

Lemma A.2.4. *Suppose $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ are quadratic forms. There exist matrices U and T for which $(Q_1, Q_2)_T^U$ is minimized, and so that*

1. *(Q_1, Q_2) is nonsingular if and only if $(Q_1, Q_2)_T^U$ is nonsingular.*
2. *(Q_1, Q_2) vanishes on an i-dimensional space over K if and only the same is true for $(Q_1, Q_2)_T^U$.*
3. *$\mathcal{P}_K(Q_1, Q_2)$ contains a form which splits off t hyperbolic planes if and only if the same is true for the pencil generated by $(Q_1, Q_2)_T^U$.*

Proof. By Lemma $A.2.3$, there exist matrices U and T for which $(Q_1, Q_2)_T^U$ is minimized. By Lemma $A.2.1$, the pair (Q_1, Q_2) is nonsingular, vanishes on an i-dimensional space, and $\mathcal{P}_K(Q_1, Q_2)$ contains a form which splits off t hyperbolic planes if and only if the same is true for $(Q_1, Q_2)_T^U$. □

Lemma A.2.5. *If the pair $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ is minimized, then there are no matrices $U \in GL_2(K)$ and $T \in GL_n(K)$ for which $(Q_1, Q_2)_T^U$ are integral and such that*

$$4v(det(T)) + nv(det(U)) < 0. \tag{A.2.2}$$

Proof. Corollary $D.2.3$ gives

$$\Delta((Q_1, Q_2)_T^U) = (\det(U))^{n(n-1)}(\det(T))^{4(n-1)}\Delta(Q_1, Q_2).$$

Using this formula, we see from inequality (2) of definition $A.2.2$ that an equivalent condition for a pair of integral forms Q_1, Q_2 to be minimized is that there are no matrices $U \in \mathrm{GL}_2(K)$ and $T \in \mathrm{GL}_n(K)$ for which $(Q_1, Q_2)_T^U$ are integral and such that

$$\begin{aligned} v(\Delta(Q_1, Q_2)_T^U) &< v(\Delta(Q_1, Q_2)). \\ v(\det(U)^{n(n-1)}) + v(\det(T)^{4(n-1)}) + v(\Delta(Q_1, Q_2)) &< v(\Delta(Q_1, Q_2)). \\ v(\det(U)^{n(n-1)}) + v(\det(T)^{4(n-1)}) &< 0. \\ n(n-1)v(\det(U)) + 4(n-1)v(\det(T)) &< 0. \\ nv(\det(U)) + 4v(\det(T) &< 0. \end{aligned}$$

□

Lemma A.2.6. *If*

$$|det(U)|_v^n |det(T)|_n^4 = 1$$

or equivalently

$$nv(det\ U) + 4v(det\ T) = 0$$

and Q_1, Q_2 is a pair of minimized forms, then $(Q_1, Q_2)_T^U$ will also be minimized provided $(Q_1, Q_2)_T^U$ is integral.

Proof. Suppose $(Q_1, Q_2)_T^U$ is not minimized. Then there exists U', T' such that $(Q_1, Q_2)_{T'T}^{U'U}$ is integral and

$$|\det(U')|_v^n |\det(T')|_v^4 > 1.$$

This gives

$$|\det(U'U)|_v^n |\det(T'T)|_v^4 = |\det(U')|_v^n |\det(T')|_v^4 > 1$$

since $|\det(U)|_v^n |\det(T)|_n^4 = 1$. This is contrary to our assumption that (Q_1, Q_2) is minimized. □

Lemma $A.2.7$ is a simple generalization of [7, Lemma 4.3, p.54].

Lemma A.2.7. *Suppose that Q_1, Q_2, are quadratic forms over $\mathcal{O}_K$ in n variables and that $R(q_1, q_2) = R \leqslant n - 1$. Assume Q_1, Q_2 take the shape*

$$\begin{aligned} Q_i(X_1, \ldots, X_n) = G_i(X_1, \ldots, X_R) + \pi \sum_{j=1}^{R} X_j L_j^{(i)}(X_{R+1}, \ldots, X_n) \\ + \pi H_i(X_{R+1}, \ldots, X_n) \end{aligned} \tag{A.2.3}$$

for $i = 1, 2$ with appropriate quadratic forms G_i, H_i and linear forms $L_j^{(i)}$, all defined over $\mathcal{O}_K$. If $\overline{H}_1$ and $\overline{H}_2$ have a common nontrivial zero over k, then the pair Q_1, Q_2 is not minimized.

Proof. We can make a change of variables among $X_{R+1}, \ldots, X_n$ so that

$$\overline{H}_1(0, \ldots, 0, 1) = \overline{H}_2(0, \ldots, 0, 1) = 0.$$

One then sets $T = \operatorname{diag}(\pi, \ldots, \pi, 1)$, where the multiplicity of π is $n - 1$, and $U = \operatorname{diag}(\pi^{-2}, \pi^{-2})$. Then $(Q_1, Q_2)_T^U$ are integral and we have

$$nv(\det(U)) + 4v(\det(T)) = -4n + 4(n - 1) = -4 < 0$$

so that inequality $A.2.2$ is satisfied, hence Q_1, Q_2 is not a minimized pair. □

A.3 Bounds on R and r

The definitions of R and r that we give here are the same as what was given in section 11.1. Given quadratic forms $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$, for $i = 1, 2$, let $q_i = \overline{Q_i}$. We define $R = R(q_1, q_2)$ to be the least integer m such that there is a linear transformation $T \in \mathrm{GL}_n(k)$ for which $q_1(TX)$ and $q_2(TX)$ are both functions of $X_1, \ldots, X_m$ alone, where $X = (X_1, \ldots, X_n)$. Therefore, there is an invertible linear change of variables over k so that $q_i = q_i'(X_1, \ldots, X_R)$ for $i = 1, 2$, where q_i' denote quadratic forms over k. Consequently, every form in $\mathcal{P}_k(q_1, q_2)$ can be expressed using only the variables $X_1, \ldots, X_R$.

We define $r = r(q_1, q_2)$ to be the maximum order a form in $\mathcal{P} = \mathcal{P}_k(q_1, q_2)$; that is,

$$r = r(q_1, q_2) = \max\{\operatorname{order}(q) \mid q \in \mathcal{P}\}.$$

It follows that $r \leqslant R \leqslant n$.

This is a simple generalization of [7, Lemma 4.2, p. 54].

Lemma A.3.1. *Suppose Q_1, Q_2 are quadratic forms over $\mathcal{O}_K$ in n variables. Assume that q_1 and q_2 both vanish on a subspace in k^n of dimension d. Assume further that $n < 2d$. Then Q_1, Q_2 is not minimized.*

Proof. By an invertible linear change of variables over k, we can assume q_1 and q_2 both vanish on $\operatorname{span}_k(e_1, \ldots, e_d)$. Therefore

$$q_1 = \sum_{i=1}^{d} X_i \ell_i(X_{d+1}, \ldots, X_n) + q_3(X_{d+1}, \ldots, X_n)$$

$$q_2 = \sum_{i=1}^{d} X_i \ell_i'(X_{d+1}, \ldots, X_n) + q_4(X_{d+1}, \ldots, X_n)$$

for some linear forms ℓ_i, ℓ_i', $1 \leqslant i \leqslant d$, and some quadratic forms q_3, q_4, all defined over k. It follows that

$$Q_1 \equiv \sum_{i=1}^{d} X_i L_i(X_{d+1}, \ldots, X_n) + Q_3(X_{d+1}, \ldots, X_n) \bmod \pi$$

$$Q_2 \equiv \sum_{i=1}^{d} X_i L_i'(X_{d+1}, \ldots, X_n) + Q_4(X_{d+1}, \ldots, X_n) \bmod \pi$$

for some linear forms L_i, L_i', $1 \leqslant i \leqslant d$, and some quadratic forms Q_3, Q_4, all defined over $\mathcal{O}_K$. Let

$$T = \operatorname{diag}(1, \ldots, 1, \pi, \ldots, \pi)$$

where the first d entries are 1's and the last $n-d$ entries are π's. Let $U = \operatorname{diag}(\pi^{-1}, \pi^{-1})$. Then $(Q_1, Q_2)_T^U$ is an integral pair. Observe that

$$\begin{aligned} &nv(\det(U)) + 4v(\det(T)) \\ &= nv(\pi^{-2}) + 4v(\pi^{n-d}). \\ &= -2n + 4(n-d). \\ &= 2n - 4d \end{aligned}$$

We see that $2n - 4d < 0$ since $n < 2d$. We conclude from Lemma $A.2.5$ that Q_1, Q_2 is not a minimized pair. □

Lemma A.3.2. *Let $Q_1, Q_2 \in \mathcal{O}_K[X_1, \ldots, X_n]$ be a minimized pair of quadratic forms with $n \geqslant 5$. If there is a form in $\mathcal{P}_k(q_1, q_2)$ of order 2, then it must be anisotropic of order 2.*

Proof. Suppose there is a form in $\mathcal{P}_k(q_1, q_2)$ that is isotropic of order 2. By changing the generators of the pencil $\mathcal{P}_k(q_1, q_2)$, we can assume q_1 is isotropic of order 2. Through a change of variable, we can assume $q_1 = X_1X_2$. Let $T = \operatorname{diag}(\pi, 1, \ldots, 1)$ and $U = \operatorname{diag}(\pi^{-1}, 1)$. Then $(Q_1, Q_2)_T^U$ is an integral pair, but

$$4v(\det(T)) + nv(\det(U)) = 4 - n < 0.$$

According to Lemma $A.2.5$, this contradicts the minimization of Q_1 and Q_2. □

Lemma A.3.3. *Let Q_1 and Q_2 be a minimized pair of quadratic forms in n variables defined over $\mathcal{O}_K$. Then every form in $\mathcal{P}_k(q_1, q_2)$ has order $\geqslant \frac{n}{4}$, hence $r(q_1, q_2) \geqslant \frac{n}{4}$.*

Proof. Suppose there is a form in $\mathcal{P}_k(q_1, q_2)$ of order j. By changing the generators of $\mathcal{P}_k(q_1, q_2)$, we can assume $\operatorname{order}(q_1) = j$. Through a change of variable, we get $q_1(X_1, \ldots, X_n) = q_1'(X_1, \ldots, X_j)$ for some quadratic form q'. Let

$$T = \operatorname{diag}(\pi, \ldots, \pi, 1, \ldots, 1),$$

where the first j diagonal entries are π's, and the last $n-j$ diagonal entries are ones. Let $U = \operatorname{diag}(\pi^{-1}, 1)$. Then $(Q_1, Q_2)_T^U$ is an integral pair. By minimization, Lemma $A.2.5$ implies that

$$4v(\det(T)) + nv(\det(U)) \geqslant 0.$$

That is, $4j - n \geqslant 0$, hence $j \geqslant \frac{n}{4}$. □

The next lemma shows the role that $D_K(Q_1, Q_2)$ plays in finding a lower bound on R.

Lemma A.3.4. *Suppose Q_1 and Q_2 are a minimized pair over $\mathcal{O}_K$ in n variables and Q_1, Q_2 both vanish on a subspace of dimension d over K. Then*

$$R(q_1, q_2) \geqslant \begin{cases} \frac{n}{2} + d & \text{if } n \text{ is even} \\ \frac{n+1}{2} + d & \text{if } n \text{ is odd.} \end{cases}$$

Proof. For $i = 1, 2$, we can write Q_i in the following way:

$$\begin{aligned} Q_i &= G_i(X_1, \ldots, X_R) \\ &\quad + \pi \sum_{j=1}^{R} \left(X_j L_j^{(i)}(X_{R+1}, \ldots, X_n) \right) + \pi H_i(X_{R+1}, \ldots, X_n), \end{aligned} \tag{A.3.1}$$

where G_i, H_i are integral quadratic forms and the $L_j^{(i)}$ are integral linear forms. For $i = 1, 2$, let $g_i = \overline{G_i}$. Note $q_i(X_1, \ldots, X_n) = g_i(X_1, \ldots, X_R)$. By hypothesis, Q_1 and Q_2 vanish on a subspace $S \subseteq K^n$ of dimension d. Let $v_1, \ldots, v_d$ be a K-basis for S. By Lemma $C.0.1$, we can assume $v_1, \ldots, v_d$ have coordinates in $\mathcal{O}_K$ and are linearly independent modulo π.

For each $1 \leqslant i \leqslant d$, let $v_i' \in (\mathcal{O}_K)^R$ denote the projection of v_i onto the first R coordinates. Assume that $v_1', \ldots, v_d'$ are linearly dependent modulo π. Then there exist $a_1, \ldots, a_d \in \mathcal{O}_k$, not all divisible by π, such that the first R coordinates of $w = a_1 v_1 + \cdots + a_d v_d$ are divisible by π. Since $v_1, \ldots, v_d$ are linearly independent modulo π, it follows that the remaining $n - R$ coordinates of w can not all be divisible by π; that is, if $w = (w_1, \ldots, w_n)$, then $(w_{R+1}, \ldots, w_n) \not\equiv 0 \bmod \pi$. Since $Q_i(w_1, \ldots, w_n) = 0$, we get that π divides $H_i(w_{R+1}, \ldots, w_n)$. Since $(w_{R+1}, \ldots, w_n) \not\equiv 0 \bmod \pi$, we deduce that h_1 and h_2 have a common nontrivial zero over k. According to Lemma $A.2.7$, this is contrary to Q_1 and Q_2 being minimized.

Therefore, $v_1', \ldots, v_d'$ are linearly independent modulo π.
Let $S' = \mathrm{span}_{\mathcal{O}_K}(v_1', \ldots, v_d')$. Since $Q_1(S) = Q_2(S) = 0$, we see that $\pi \mid G_1(S')$ and $\pi \mid G_2(S')$. Let $\overline{S'} = \mathrm{span}_k(\overline{v_1'}, \ldots, \overline{v_d'})$. Then $\overline{S'}$ is a subspace of k^R of dimension d, and $g_1(\overline{S'}) = g_2(\overline{S'}) = 0$. Through an invertible change of variable over k, we can assume that $\overline{S'} = \mathrm{span}_k(e_1, \ldots, e_d)$. Thus g_1 and g_2 have the shape

$$g_i = \sum_{j=1}^{d} \left(X_j m_j^{(i)}(X_{d+1}, \ldots, X_R) \right) + w_i(X_{d+1}, \ldots, X_R),$$

where the $m_j^{(i)}$ are linear forms over k and the w_i are quadratic forms over k. This implies that Q_1 and Q_2 have the following shape

$$\begin{aligned} Q_i = &\sum_{j=1}^{d} \left(X_j M_j^{(i)}(X_{d+1}, \ldots, X_R) \right) + W_i(X_{d+1}, \ldots, X_R) \\ &+ \pi U_i(X_1, \ldots, X_R) \\ &+ \pi \sum_{j=1}^{R} \left(X_j L_j^{(i)}(X_{R+1}, \ldots, X_n) \right) + \pi H_i(X_{R+1}, \ldots, X_n), \end{aligned} \tag{A.3.2}$$

where the $M_J^{(i)}$ are linear forms over $\mathcal{O}_K$ and the U_i, W_i are quadratic forms over $\mathcal{O}_K$. Let T be the $n \times n$ diagonal matrix defined by

$$T = \mathrm{diag}(1, 1, \ldots, 1, \pi, \pi, \ldots, \pi, 1, \ldots, 1),$$

where the first d entries are ones, and there are $(R-d)$ π's. Thus $v(\det(T)) = R - d$. Let $U = \mathrm{diag}(\pi^{-1}, \pi^{-1})$. Then the pair $(Q_1, Q_2)_T^U$ is integral. Since (Q_1, Q_2) is a minimized pair, Lemma $A.2.5$ implies that

$$\begin{aligned} 4v(\det(T)) + nv(\det(U)) &\geqslant 0. \\ 4(R-d) - 2n &\geqslant 0. \\ R - d &\geqslant \frac{n}{2}. \\ R &\geqslant \frac{n}{2} + d. \end{aligned}$$

It follows that

$$R \geqslant \begin{cases} \frac{n}{2} + d & \text{if } n \text{ is even} \\ \frac{n+1}{2} + d & \text{if } n \text{ is odd.} \end{cases}$$

□

Appendix B: Quadratic Form Theory

Let k be any field and let V be a finite dimensional vector space over k. For a quadratic map $f : V \to k$ and a subspace $W \subseteq V$, we define

$$W^{\perp} = \{w \in V \mid B_f(w, V) = 0\}.$$

That is, $W^{\perp}$ consists of the all the vectors $w \in V$ such that $B_f(w, v) = 0$ for all $v \in V$.

Lemma B.0.1. *Let $q : V \to k$ be a quadratic map, and let $W \subseteq V$ be any subspace. If B_q is nondegenerate, then $dim(W^{\perp}) = dim(V) - dim(W)$.*

Proof. Let $V^* = \operatorname{Hom}_k(V, k)$, and $W^* = \operatorname{Hom}_k(W, k)$. Thus V^* is the dual space of V and W^* is the dual space of W. Consider the map $\varphi : V \to V^*$ defined by

$$(\varphi(v))(v') = B_q(v, v') \qquad v, v' \in V.$$

Since B_q is bilinear over k, the map φ is k-linear. We will show φ is injective. Suppose $v \in \ker(\varphi)$. Let $v' \in V$. Then $B_q(v', v) = 0$, hence $v \in \operatorname{rad}(B_q)$. Since B_q is nondegenerate, $\operatorname{rad}(B_q) = 0$, hence $v = 0$ and so φ is injective.

By rank-nullity,

$$\dim(V) = \dim(\operatorname{im}(\varphi)) + \dim(\ker(\varphi)).$$

Since φ is injective, $\dim(\operatorname{im}(\varphi)) = \dim(V)$. Since $\dim(V) = \dim(V^*)$, we obtain $\dim(\operatorname{im}(\varphi)) = \dim(V^*)$. Thus $\operatorname{im}(\varphi) = V^*$, hence φ is surjective. Therefore φ is an isomorphism.

For any linear map $f \in V^*$, let $f|_W$ denote the restriction of f to W, hence $f|_W \in W^*$. The map from V^* to W^* given by $\pi : f \mapsto f|_W$ is surjective, which we prove now. Let $g \in W^*$. For any basis β_1 of W, extend to a basis β for V: $\beta = \beta_1 \cup \beta_2$. Let $f \in V^*$ be defined by letting $f(v) = g(v)$ for all $v \in \beta_1$ and $f(v) = 0$ for all $v \in \beta_2$. Then $f|_W = g$, hence $V^* \xrightarrow{\pi} W^*$ is surjective.

Our results give us the following exact sequence

$$0 \to V \xrightarrow{\varphi} V^* \xrightarrow{\pi} W^* \to 0.$$

Applying rank-nullity to $\pi \circ \varphi$ gives

$$\dim(V) = \dim(\operatorname{im}(\pi \circ \varphi)) + \dim(\ker(\pi \circ \varphi)).$$

$$n = \dim(W^*) + \dim(\ker(\pi \circ \varphi)).$$

$$n - \dim(W) = \dim(\ker(\pi \circ \varphi)).$$

We will be done once we show that $\dim(\ker(\pi \circ \varphi)) = \dim(W^\perp)$. The map $\pi \circ \varphi$ is given by

$$(\pi \circ \varphi)(v) = \pi(\varphi(v)) = \varphi(v)|_W.$$

If $\varphi(v)|_W$ is the zero map, then $B_Q(v, w) = 0$ for all $w \in W$. Thus $v \in W^\perp$. We conclude that $\ker(\pi \circ \varphi) = W^\perp$, in which case $\dim(\ker(\pi \circ \varphi)) = \dim(W^\perp)$.

□

Lemma B.0.2. *Let $q : V \to k$ be a quadratic map. If $W \subset V$ is a subspace where every nonzero element of W is a nonsingular zero of q, then dim$(W^\perp) = n -$ dim(W).*

Proof. Since every nonzero element of W is a nonsingular zero of q, we have $W \cap \text{rad}(B_q) = 0$. Since V is a finite dimensional vector space, there exists a subspace $V_0 \subset V$ such that V_0 is maximal with respect to containing W and such that $V_0 \cap \text{rad}(B_q) = 0$. We will show that $V = V_0 \oplus \text{rad}(B_q)$. We already know $V_0 \cap \text{rad}(B_q) = 0$, so it remains show that $V = V_0 + \text{rad}(B_q)$. Let $v \in V$. If $v \in V_0 + \text{rad}(B_q)$, we are done. Otherwise, $v \notin V_0 + \text{rad}(B_q)$. Then consider $V_0 \oplus kv$. We will show that $(V_0 \oplus kv) \cap \text{rad}(B_q) = 0$.

To that end, let $w \in (V_0 \oplus kv) \cap \text{rad}(B_q)$. Then $w \in \text{rad}(B_q)$, and $w = v_0 + \lambda v$ for some $v_0 \in V_0$ and some $\lambda \in k$. Thus

$$\lambda v = -v_0 + w \in V_0 + \text{rad}(B_q).$$

Since $v \notin V_0 + \text{rad}(B_q)$, we must have $\lambda = 0$. Then $w = v_0$, and $w \in \text{rad}(B_q)$, so $v_0 \in \text{rad}(B_q)$. But $V_0 \cap \text{rad}(B_q) = 0$, hence $v_0 = 0$. This proves that $w = 0$ and so $(V_0 \oplus kv) \cap \text{rad}(B_q) = 0$.

However, having $(V_0 \oplus kv) \cap \text{rad}(B_q) = 0$ is contrary to the maximality of V_0. We therefore conclude that $V = V_0 \oplus \text{rad}(B_q)$. This implies that $B_{q|_{V_0}}$ is nondegenerate, which we prove now. Suppose $y \in \text{rad}(B_{q|_{V_0}})$. Then $y \in V_0$, and $B_q(y, V_0) = 0$. For any $z \in V$, we can write $z = z_0 + z_1$, where $z_0 \in V_0$ and $z_1 \in \text{rad}(B_q)$. Thus $B_q(y, z) = B_q(y, z_0) + B_q(y, z_1) = 0 + 0 = 0$, which implies $y \in \text{rad}(B_q)$. Thus $y = 0$ since $V_0 \cap \text{rad}(B_q) = 0$. This proves that $B_{q|_{V_0}}$ is nondegenerate.

Because $B_{q|_{V_0}}$ is nondegenerate, and $W \subseteq V_0$ is a subspace, Lemma $B.0.1$ implies that

$$\dim(W^\perp_{V_0}) = \dim(V_0) - \dim(W), \tag{B.0.1}$$

where $W^\perp_{V_0} = \{x \in V_0 \mid B_q(x, W) = 0\}$. Since $V = V_0 \oplus \text{rad}(B_q)$, every element of V can be written as $v_0 + v_1$, where $v_0 \in V_0$ and $v_1 \in \text{rad}(B_q)$. Consider the projection map $\pi : W^\perp \to V_0$ given by

$$\pi(v_0 + v_1) = v_0 \qquad v_0 + v_1 \in W^\perp.$$

We will compute the kernal and image of π. It is clear that $\ker(\pi) = \text{rad}(B_q)$ (note that $\text{rad}(B_q) \subseteq W^{\perp}$). As for the image of π, observe that if $y = y_0 + y_1 \in W^{\perp}$, with $y_0 \in V_0$ and $y_1 \in \text{rad}(B_q)$, then $\pi(y) = y_0$. We claim $y_0 \in W^{\perp}_{V_0}$. Let $z \in W$ and observe that

$$B_q(y_0, z) = B_q(y - y_1, z) = B_q(y, z) - B_q(y_1, z) = 0$$

because $y \in W^{\perp}$ and $y_1 \in \text{rad}(B_q)$. Thus $y_0 \in W^{\perp}_{V_0}$, which shows that $\text{im}(\pi) \subseteq W^{\perp}_{V_0}$. For the reverse inclusion, observe that $W^{\perp}_{V_0} \subseteq V_0$ and $W^{\perp}_{V_0} \subseteq W^{\perp}$. These two inclusions imply that $\pi(W^{\perp}_{V_0}) = W^{\perp}_{V_0}$, hence $W^{\perp}_{V_0} \subseteq \text{im}(\pi)$. Thus $\text{im}(\pi) = W^{\perp}_{V_0}$.

We have shown that the kernal of π is $\text{rad}(B_q)$, and the image of π is $W^{\perp}_{V_0}$. By rank-nullity,

$$\dim(W^{\perp}) = \dim(W^{\perp}_{V_0}) + \dim(\text{rad}(B_q)).$$

$$\dim(W_{V_0})^{\perp} = \dim(W^{\perp}) - \dim(\text{rad}(B_q)).$$

Substituting this formula into equation $B.0.1$ gives

$$\dim(W^{\perp}) - \dim(\text{rad}(B_q)) = \dim(V_0) - \dim(W).$$

$$\dim(W^{\perp}) = \dim(V_0) + \dim(\text{rad}(B_q)) - \dim(W).$$

$$\dim(W^{\perp}) = n - \dim(W).$$

□

B.1 Orthogonal Decomposition and Hyperbolic Planes

Theorem B.1.1. *Let $q : V \to k$ be a quadratic map with dim$(V) = n$. The following statements are true.*

1. *If q vanishes on an m-dimensional subspace U of V, where every nonzero element of U is a nonsingular zero of q, then q splits off at least dim(U) hyperbolic planes.*

2. *If order$(q) = n$ and W is any subspace of V where $q(W) = 0$, then q splits off at least dim(W) hyperbolic planes.*

Proof. Assume that q has order n and $q(W) = 0$ for some subspace W of V. Definition 2.1.13 implies that q is nondegenerate. Therefore, Lemma 2.1.18 implies that every nonzero element of W is a nonsingular zero of q. For this reason, we see that (1) implies (2).

To prove (1), we induct on m. The result is trivial for $m = 0$. Let $m \geqslant 1$, and assume by induction that the result is true when $\dim(U) < m$.

Let U be an m-dimensional subspace of V where every nonzero element of U is a nonsingular zero of q. Write $U = U' \oplus kv$, where U' is an $(m-1)$-dimensional space. Thus $U' \subsetneq U$. We will show that $U^{\perp} \subsetneq (U')^{\perp}$. By inclusion-reversing, since $U' \subset U$, we get $U^\perp \subset (U')^\perp$. Since every nontrivial zero of q is nonsingular, Lemma $B.0.2$ implies that

$$\dim(U^\perp) = n - \dim(U) < n - \dim(U') = \dim((U')^\perp).$$

This proves that $U^\perp \subsetneq (U')^\perp$.

Therefore, there exists $w \in (U')^\perp$ with $w \notin U^\perp$. Since $w \notin U^\perp$, there exists nonzero $v \in U$ such that $B_q(v, w) \neq 0$. By scaling v, we can assume $B_q(v, w) = 1$. Let $w' = w - cv$, where $c = q(w)$. Note that

$$q(w') = q(w - cv) = B_q(w, -cv) + q(w) + q(-cv) = -c + q(w) = 0.$$

Thus $q(w') = 0$, $q(v) = 0$, and $B_q(v, w') = B_q(v, w - cv) = 1 \neq 0$. We deduce that the subspace $Y = \text{span}(v, w')$ is hyperbolic. Therefore, q restricted to Y splits off 1 hyperbolic plane.

In particular, $B_{q|_Y}$ is nondegenerate, so by Lemma $B.0.1$, $\dim(Y^\perp) = n - \dim(Y)$. Moreover, $Y \cap Y^\perp = \text{rad}(B_{q|_Y})$, and since $B_{q|_Y}$ is nondegenerate, we have $Y \cap Y^\perp = 0$. Therefore,

$$\dim(Y \oplus Y^\perp) = \dim(Y) + \dim(Y^\perp) = \dim(Y) + (n - \dim(Y)) = n.$$

This proves that $V = Y \hat{\oplus} Y^\perp$.

Since $v \in U$, $q(v) = 0$; likewise, since $U' \subsetneq U$, we get $q(U') = 0$. Thus $B_q(v, U') = 0$. Further, $B_q(w, U') = 0$ because $w \in (U')^\perp$. Because $w' = w - cv$, it follows that $B_q(w', U') = 0$ also. Having $B_q(v, U') = B_q(w', U') = 0$ implies that $v, w' \in (U')^\perp$. Since $Y = \text{span}(v, w')$, we get $Y \subseteq (U')^\perp$, hence $U' \subseteq Y^\perp$ by inclusion reversing. By induction, q restricted to $Y^\perp$ splits off at least $\dim(U') = m - 1$ hyperbolic planes and so q splits off at least m hyperbolic planes.

□

Theorem B.1.2. *Let V be a vector space over a field F with $\dim(V) = n < \infty$. Let $q : V \to F$ be a quadratic map. There exist subspaces $V_1, \ldots, V_j \subseteq V$ such that*

$$V = V_1 \hat{\oplus} \cdots \hat{\oplus} V_j \hat{\oplus} rad(B_q),$$

where each $V_i = span(v_i, w_i)$ with $B_q(v_i, w_i) \neq 0$.

Proof. We go by induction on n. If $n = 0$, then $V = \text{rad}(B_q) = 0$. Assume by induction that the result holds for quadratic modules (V, q) such that $\dim(V) < n$, where $n \geqslant 1$.

For $\dim(V) = n$, if $\text{rad}(B_q) = V$, then we are done. Otherwise, we choose a subspace $V' \subset V$ such that $V = V' \oplus \text{rad}(B_q)$ and $\dim(V') \geqslant 1$. Thus $\dim(V) = \dim(V') + \dim(B_q)$ and $V' \cap \text{rad}(B_q) = 0$. Since $V' \cap \text{rad}(B_q) = 0$, we see that

$q|_{V'}$ is nondegenerate. Let $v_1 \in V'$ be nonzero. Then $v_1 \notin \mathrm{rad}(B_q)$. There exists $w_1 \in V'$ such that $B_q(v_1, w_1) \neq 0$. Let $V_1 = \mathrm{span}(v_1, w_1)$. Let $S = V_1^{\perp} \cap V'$, hence $S = \{x \in V' \mid B_q(x, V_1) = 0\}$. Since $q|_{V'}$ is nondegenerate, Lemma $B.0.1$ implies that $\dim(S) = \dim(V') - \dim(V_1)$.

We will show that $V_1 \cap S = 0$. Suppose $x \in V_1 \cap S$. For any $v \in V$, we can write $v = z_1 + z_2$, where $z_1 \in V'$ and $z_2 \in \mathrm{rad}(B_q)$. Observe that

$$B_q(x, v) = B_q(x, z_1) + B_q(x, z_2).$$

Since $x \in S$, $B_q(x, z_1) = 0$. Because $z_2 \in \mathrm{rad}(B_q)$, $B_q(x, z_2) = 0$. Thus $x \in \mathrm{rad}(B_q)$. Since $x \in V_1 \subset V'$, we deduce that $x \in V' \cap \mathrm{rad}(B_q) = 0$, hence $x = 0$. We have shown that $V_1 \cap S = 0$.

Since $\dim(V') = \dim(V_1) + \dim(S)$ and $V_1 \cap S = 0$, it follows that $V' = V_1 \oplus S$. Then

$$V = V_1 \oplus S \oplus \mathrm{rad}(B_q).$$

Let $W = S \oplus \mathrm{rad}(B_q)$. Note that $B_q(V_1, W) = 0$ and $V = V_1 \oplus W$, with $\dim(W) < n$. Applying induction to W yields

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_j \oplus \mathrm{rad}(B_{q|_W}).$$

We will be done once we show that $\mathrm{rad}(B_{q|_W}) = \mathrm{rad}(B_q)$.

To that end, suppose $w \in \mathrm{rad}(B_{q|_W})$. Then

$$B_q(w, V) = B_q(w, V_1 \oplus W) = B_q(w, V_1) + B_q(w, W).$$

Since $B_q(V_1, W) = 0$, we get $B_q(w, V_1) = 0$. Since $w \in \mathrm{rad}(B_{q|_W})$, we get $B_q(w, W) = 0$. Thus $B_q(w, V) = 0$ and so $w \in \mathrm{rad}(B_q)$. On the other hand, suppose $y \in \mathrm{rad}(B_q)$. Then $B_q(y, W) = 0$, and since $W = S \oplus \mathrm{rad}(B_q)$, we get that $\mathrm{rad}(B_q) \subset W$, hence $y \in W$. Then $y \in \mathrm{rad}(B_{q|_W})$. We have shown that $\mathrm{rad}(B_{q|_W}) = \mathrm{rad}(B_q)$. This completes the proof. $\square$

Lemma B.1.3. *Let $q : V \to k$ be a quadratic map with char$(k) = 2$ and dim$(V) = n$. There exists a k-basis of V for which the quadratic form associated to q with respect to this basis has the shape*

$$Q_1(X_1, X_2) + \cdots + Q_j(X_{2j-1}, X_{2j}) + q(d_{2j+1})X_{2j+1}^2 + \cdots + q(d_n)X_n^2,$$

where rank$(Q_i) = 2$, $n - 2j =$ dim(rad(B_q)), and $\{d_{2j+1}, \ldots, d_n\}$ is a k-basis for rad(B_q).

Proof. By Lemma $B.1.2$, there exist subspaces $V_1, \ldots, V_j \subseteq V$ such that

$$V = V_1 \hat{\oplus} \cdots \hat{\oplus} V_j \hat{\oplus} \mathrm{rad}(B_q),$$

where each $V_i = \text{span}(v_i, w_i)$ with $B_q(v_i, w_i) \neq 0$. Having $B_q(v_i, w_i) \neq 0$ implies that for $\text{char}(k) = 2$, v_i, w_i are linearly independent, for if $v_i = \lambda w_i$ for some $\lambda \in k$, then $B_q(v_i, w_i) = \lambda B_q(w_i, w_i) = \lambda 2q(w_i) = 0$.

Let $Q_i(X_{2i-1}, X_{2i})$ be the quadratic form associated to $q|_{V_i}$ with respect to the basis $\{v_i, w_i\}$. Then

$$q(v_i)X_{2i-1}^2 + B_q(v_i, w_i)X_{2i-1}X_{2i} + q(w_i)X_{2i}^2.$$

Thus, $\det(Q_i) = 4q(v_i)q(w_i) - B_q(v_i, w_i) = B_q(v_i, w_i) \neq 0$. It follows that $\text{rank}(Q_i) = 2$.

From Lemma B.1.2, $\dim(\text{rad}(B_q)) = n - (\sum_{i=1}^{j} \dim(V_i)) = n - 2j$. Let

$$\{d_{2j+1}, \ldots, d_n\}$$

be a k-basis for $\text{rad}(B_q)$. The quadratic form associated to q with respect to the basis $\{v_1, w_1, \ldots, v_j, w_j, d_{2j+1}, \ldots, d_n\}$ is given by

$$Q_1(X_1, X_2) + \cdots + Q_j(X_{2j-1}, X_{2j}) + q(d_{2j+1})X_{2j+1}^2 + \cdots + q(d_n)X_n^2.$$

□

Lemma B.1.4. *Let $q : V \to k$ be a quadratic map with k perfect. If dim(rad(B_q)) $\geqslant 2$, then dim(rad(q)) $\geqslant 1$.*

Proof. Let $v, w \in \text{rad}(B_h)$ be linearly independent. Let $a, b \in k$, not both zero. Note that $q(av + bw) = a^2q(v) + b^2q(w)$. Since k is a perfect field, every element of k is a square. We may therefore choose $a, b \in k$, not both zero, such that $q(av + bw) = 0$. Then $av + bw \in \text{rad}(q)$. Since v, w are linearly independent, and not both a, b are zero, we get that $av + bw \neq 0$. Thus $\dim(\text{rad}(q)) \geqslant 1$. □

Lemma B.1.5. *Let $q : V \to k$ be a quadratic map.*

1. *If char(k) $\neq 2$, then order(q) $= n$ if and only if det(q) $\neq 0$.*
2. *If char(k) $= 2$, n is even, and k is perfect, then order(q) $= n$ if and only if det(q) $\neq 0$.*
3. *If char(k) $= 2$, n is odd, and k is perfect, then order(q) $= n$ if and only if det$_{\frac{1}{2}}$(q) $\neq 0$*

Proof. We begin the observation that for both $\text{char}(k) \neq 2$ and $\text{char}(k) = 2$, if $\det(q) = n$, then $\text{rank}(q) = n$, hence $\text{order}(q) = n$.

For $\text{char}(k) \neq 2$, $\text{order}(q) = \text{rank}(q)$, and $\text{rank}(q) = n$ if and only if $\det(q) \neq 0$. This proves (1).

Assume $\mathrm{char}(k) = 2$. By Lemma $B.1.3$, there exists a k-basis of V such that the quadratic form associated to q with respect to this basis is

$$Q_1(X_1, X_2) + \cdots + Q_j(X_{2j-1}, X_{2j}) + q(d_{2j+1})X_{2j+1}^2 + \cdots + q(d_n)X_n^2,$$

where $\mathrm{rank}(Q_i) = 2$, $n - 2j = \dim(\mathrm{rad}(B_q))$, and $\{d_{2j+1}, \ldots, d_n\}$ is a k-basis for $\mathrm{rad}(B_q)$. Observe that

$$\det(q) = \det(Q_1) \cdots \det(Q_j) 2^{n-2j} q(d_{2j+1}) \cdots q(d_n). \tag{B.1.1}$$

Since $\mathrm{rank}(Q_i) = 2$, we have $\det(Q_i) \neq 0$.

For (2), we suppose n is even and k is perfect. On the one hand, our observation at the beginning of the of proof implies that if $\det(q) \neq 0$, then $\mathrm{order}(q) = n$. For an alternate argument, equation $B.1.1$ implies that if $\det(q) \neq 0$, then $0 = n - 2j = \dim(\mathrm{rad}(B_q))$. Since $\mathrm{rad}(q) \subseteq \mathrm{rad}(B_q)$, we obtain $\dim(\mathrm{rad}(q)) = 0$, hence $\mathrm{order}(q) = n$.

Conversely, suppose $\mathrm{order}(q) = n$. Then $\mathrm{rad}(q) = 0$ and so Lemma $B.1.4$ implies that $n - 2j = \dim(\mathrm{rad}(B_q)) \leqslant 1$. Since n is even, $n - 2j = \dim(\mathrm{rad}(B_q)) = 0$, hence equation $B.1.1$ implies that $\det(q) = \det(Q_1) \cdots \det(Q_j) \neq 0$. This proves (2).

For (3), we suppose n is odd and k is perfect. If $\det_{\frac{1}{2}}(q) \neq 0$, then $1 = n - 2j = \dim(\mathrm{rad}(B_q))$. Thus $\mathrm{rad}(B_q) = \mathrm{span}(d_{2j+1})$. Also, since $\det_{\frac{1}{2}}(q) \neq 0$, we have $q(d_{2j+1}) \neq 0$. Thus, $\mathrm{rad}(q) = \mathrm{rad}(q) \cap \mathrm{rad}(B_q) = 0$, hence $\mathrm{order}(q) = n$.

Conversely, suppose $\mathrm{order}(q) = n$. Then $\mathrm{rad}(q) = 0$ and so Lemma $B.1.4$ implies that $n - 2j = \dim(\mathrm{rad}(B_q) \leqslant 1$. Since n is odd, we get $n - 2j = \dim(\mathrm{rad}(B_q)) = 1$. Then equation $B.1.1$ implies that $\det_{\frac{1}{2}}(q) = \det(Q_1) \cdots \det(Q_j) \neq 0$.

□

Lemma B.1.6. *Let $q : V \to k$ be a quadratic map with char(k) $\neq 2$ and dim(V) $= n$. There exists a k-basis of V for which the quadratic form associated to q with respect to this basis is given by*

$$a_1 X_1^2 + \cdots + a_n X_n^2,$$

where each $a_i \in k$.

Proof. By Lemma $B.1.2$, there exist subspaces $V_1, \ldots, V_j \subseteq V$ such that

$$V = V_1 \widehat{\oplus} \cdots \widehat{\oplus} V_j \widehat{\oplus} \mathrm{rad}(B_q),$$

where each $V_i = \mathrm{span}(v_i, w_i)$ with $B_q(v_i, w_i) \neq 0$. Suppose $\{z_1, \ldots, z_t\}$ is a k-basis for $\mathrm{rad}(B_q)$, hence $t = \dim(\mathrm{rad}(B_q))$. Then the quadratic form associated to $q|_{\mathrm{rad}(B_q)}$ with respect to this basis is a diagonal form.

As for $q|_{V_i}$, note that if $\dim(V_i) = 1$, then the quadratic associated to $q|_{V_i}$ is a 1-dimensional form, as desired. Suppose $\dim(V_i) = 2$. We consider two cases.

Case 1. Suppose $q(v_i) = q(w_i) = 0$. Then the quadratic form associated to $q|_{V_i}$ is the hyperbolic plane aXY, $a = B_q(v_i, w_i) \neq 0$. Then aXY is equivalent to XY. For $\mathrm{char}(k) \neq 2$, XY is equivalent to the diagonal form $X^2 - Y^2$; to see this, start with $X^2 - Y^2$, and write $X^2 - Y^2 = (X - Y)(X + Y)$. The change of variable given by $X' = X - Y$ and $Y' = X + Y$ is invertible because the matrix $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ has determinant -2. This change of variable transforms $X^2 - Y^2$ into the hyperbolic plane $X'Y'$.

Case 2. Without loss of generality, suppose $q(v_i) \neq 0$. Let $a \in k$, yet to be chosen. Observe that

$$\begin{aligned} B_q(v_i, v_i + aw_i) &= B_q(v_i, v_i) + aB_q(v_i, w_i). \\ &= 2q(v_i) + aB_q(v_i, w_i). \end{aligned}$$

Let $b = B_q(v_i, w_i)$ and let $a = -2b^{-1}q(v_i)$. Then $a \neq 0$, $B_q(v_i, v_i + aw_i) = 0$, and $\{v_i, v_i + aw_i\}$ is a k-basis for V_i. It follows that the quadratic form associated to $q|_{V_i}$ with respect to the basis $\{v_i, v_i + aw_i\}$ is a diagonal form.

□

Lemma B.1.7. *Let $q : V \to k$ be a quadratic map over an arbitrary field k. Assume $\dim(V) = n \geqslant 2$, and let $A = \{a_1, \ldots, a_n\}$ be a k-basis of V. Let $M_q = (m_{ij})$ be the matrix of B_q with respect to A; thus $m_{ij} = B_q(a_i, a_j)$. Fix $1 \leqslant t \leqslant n - 1$, and for each $1 \leqslant i \leqslant n$, let $R_i = (m_{i1}, \ldots, m_{it})$.*

Let $U = span(a_1, \ldots, a_t)$. For each $j \in \{t + 1, \ldots, n\}$, suppose there exist elements $c_{1j}, \ldots, c_{tj} \in k$ such that

$$c_{1j}R_1 + c_{2j}R_2 + \cdots + c_{tj}R_t = -R_j. \tag{B.1.2}$$

Let $a'_j = a_j + \sum_{s=1}^{t} c_{sj}a_i$. Then $span(a'_{t+1}, a'_{t+2}, \ldots, a'_n) \subseteq U^{\perp}$. Thus

$$V = span(a_1, \ldots, a_t) \widehat{\oplus} span(a'_{t+1}, \ldots, a'_n).$$

Proof. To show $\mathrm{span}(a'_{t+1}, a'_{t+2}, \ldots, a'_n) \subseteq U^{\perp}$, it is sufficient to prove that for each $t + 1 \leqslant j \leqslant n$, $B_q(a_i, a'_j) = 0$ for all $1 \leqslant i \leqslant t$. Equation $B.1.2$ implies that for each $1 \leqslant i \leqslant t$,

$$c_{1j}m_{1i} + c_{2j}m_{2i} + \cdots + c_{tj}m_{ti} = -m_{ji}.$$

Since $M_q = (m_{ij})$ is a symmetric matrix, we get

$$c_{1j}m_{i1} + c_{2j}m_{i2} + \cdots + c_{tj}m_{it} = -m_{ij}.$$

$$\sum_{s=1}^{t} c_{sj} m_{is} = -m_{ij}.$$

$$\sum_{s=1}^{t} c_{sj} B_q(a_i, a_s) = -B_q(a_i, a_j).$$

It follows that

$$\begin{aligned} B_q(a_i, a'_j) &= B_q(a_i, a_j) + B_q(a_i, \sum_{s=1}^{t} c_{sj} a_s). \\ &= B_q(a_i, a_j) + \sum_{s=1}^{t} c_{sj} B_q(a_i, a_s). \\ &= 0. \end{aligned}$$

To prove $V = \text{span}(a_1, \ldots, a_t) \widehat{\oplus} \text{span}(a'_{t+1}, \ldots, a'_n)$, let $W = \text{span}(a_1, \ldots, a_t) + \text{span}(a'_{t+1}, \ldots, a'_n)$. Note that $a_1, \ldots, a_t \in W$. For $t+1 \leqslant j \leqslant n$, we have

$$a_j = -\left(\sum_{s=1}^{t} c_{sj} a_i\right) + a'_j.$$

Thus each $a_j \in W$. Then $A \subset W$ and so $V = W$.

$\square$

Lemma B.1.8. *Let k be any field and $q \in k[X_1, \ldots, X_n]$ be a quadratic form with $n \geqslant 2$. Let $e_i \in k^n$ denote the i^{th} standard basis vector of k^n. Let $f : k^n \to k$ be the quadratic map associated to q with respect to the standard basis $\{e_1, \ldots, e_n\}$. Fix $1 \leqslant t \leqslant n-1$, and let $g(X_1, \ldots, X_t) = q(X_1, \ldots, X_t, 0, \ldots, 0)$.*

Suppose g has rank t over k. Then there exist $e'_{t+1}, \ldots, e'_n \in k^n$ with the following properties.

1. *$k^n = span(e_1, \ldots, e_t) \widehat{\oplus} span(e'_{t+1}, \ldots, e'_n)$.*
2. *For $t+1 \leqslant j \leqslant n$, $e'_j = e_j + \sum_{s=1}^{t} c_{sj} e_s$ for some $c_{sj} \in k$.*
3. *The quadratic form q' associated to f with respect to the basis*

   $$\{e_1, \ldots, e_t, e'_{t+1}, \ldots, e'_n\}$$

   has the shape

   $$q' = g(X_1, \ldots, X_t) + h(X_{t+1}, \ldots, X_n),$$

   where $h \in k[X_{t+1}, \ldots, X_n]$ is some quadratic form.
4. *$det(q) = det(q')$.*

Proof. Let $M_q = (m_{ij})$ denote the matrix of q with respect to the standard basis of k^n. Let M_g denote the matrix of g with respect to the standard basis of k^t. Since g has rank t, the rows of M_g are linearly independent. Note that the upper $t \times t$ block of M_q is the matrix M_g. For each $1 \leqslant i \leqslant n$, let $R_i = (m_{i1}, \ldots, m_{it})$. Note that for $1 \leqslant i \leqslant t$, R_i is the i^{th} row of M_g; thus $R_1, \ldots, R_t$ are linearly independent. Then $\operatorname{span}(R_1, \ldots, R_t) = k^t$. It follows that for each $j \in \{t+1, \ldots, n\}$, there exist $c_{1j}, \ldots, c_{tj} \in k$ such that

$$c_{1j}R_1 + c_{2j}R_2 + \cdots + c_{tj}R_t = -R_j.$$

Let $U = \operatorname{span}(e_1, \ldots, e_t)$, and for each $t+1 \leqslant j \leqslant n$, let $e'_j = e_j + \sum_{s=1}^{t} c_{sj}e_s$. Then Lemma $B.1.7$ implies that $\operatorname{span}(e'_{t+1}, \ldots, e'_n) \subseteq U^{\perp}$, and

$$k^n = \operatorname{span}(e_1, \ldots, e_t)\widehat{\oplus}\operatorname{span}(e'_{t+1}, \ldots, e'_n).$$

With respect to the basis

$$\{e_1, \ldots, e_t, e'_{t+1}, \ldots, e'_n\},$$

q has the shape

$$q = g(X_1, \ldots, X_t) + h(X_{t+1}, \ldots, X_n),$$

where $h \in k[X_{t+1}, \ldots, X_n]$ is some quadratic form. Note that the change of basis matrix between the two bases is a triangular matrix with ones along the diagonal, hence the determinant of the change of basis matrix is 1. Thus $\det(q) = \det(q')$. $\square$

Lemma B.1.9. *Let $n \geqslant 2$ and let $q_1, q_2 \in k[X_1, \ldots, X_n]$ be quadratic forms over a field k. Fix $1 \leqslant t \leqslant n-1$. Suppose that q_1 and q_2 satisfy the following shape:*

$$q_1 = g(X_1, \ldots, X_t) + \sum_{i=1}^{t} X_i\ell_i(X_{t+1}, \ldots, X_n) + h_1(X_{t+1}, \ldots, X_n).$$
$$q_2 = h_2(X_{t+1}, \ldots, X_n),$$

where g, h_1, h_2 are quadratic forms over k and the ℓ_i are linear forms over k.

If rank$(g) = t$, then there is an invertible linear change of variable over k so that

$$q_1 = g(X_1, \ldots, X_t) + h'_1(X_{t+1}, \ldots, X_n).$$
$$q_2 = h_2(X_{t+1}, \ldots, X_n),$$

where h'_1 is some quadratic form. Thus, q_2 remains the same under the change of variable.

Proof. For $1 \leqslant i \leqslant n$, let e_i denote the i^{th} standard basis vector for k^n. For $j = 1, 2$, let $f_j : k^n \to k$ denote quadratic maps such that for each $(x_1, \ldots, x_n) \in k^n$, we have

$$f_j(x_1e_1 + \cdots + x_ne_n) = q_j(x_1, \ldots, x_n).$$

Thus, q_j is the quadratic form associated to f_j with respect to the standard basis $\{e_1, \ldots, e_n\}$.

Since g has rank t, Lemma $B.1.8$ implies that there exist $e'_{t+1}, \ldots, e'_n \in k^n$ with the following properties.

1. $k^n = \text{span}(e_1, \ldots, e_t)\widehat{\bigoplus}_{f_1}\text{span}(e'_{t+1}, \ldots, e'_n)$.
2. For $t + j \leqslant j \leqslant n$, $e'_j = e_j + \sum_{s=1}^t c_{sj} e_s$ for some $c_{sj} \in k$.
3. The quadratic form q'_1 associated to f_1 with respect to the basis

$$\{e_1, \ldots, e_t, e'_{t+1}, \ldots, e'_n\}$$

has the shape

$$q' = g(X_1, \ldots, X_t) + h'_1(X_{t+1}, \ldots, X_n)$$

where h is some quadratic form.

Lemma $B.1.8$ also implies that $\det(q_1) = \det(q'_1)$, but we will not need that fact for this proof. Let q'_2 denote the quadratic form associated to f_2 with respect to the basis $\{e_1, \ldots, e_t, e'_{t+1}, \ldots, e'_n\}$. We will show that $q'_2 = q_2$. Let $1 \leqslant i \leqslant t$ and $t + 1 \leqslant j \leqslant n$. Since $q_2(X_1, \ldots, X_n) = h_1(X_{t+1}, \ldots, X_n)$, and $e'_j = e_j + \sum_{s=1}^t c_{sj} e_s$, we deduce that

$$\begin{aligned} f_2(e'_j) &= q_2(e'_j) \\ &= q_2(c_{1j}, \ldots, c_{tj}, 0, \ldots, 0, 1, 0, \ldots, 0) \\ &= h_2(e_j) \\ &= q_2(e_j) \\ &= f_2(e_j) \end{aligned}$$

where the one occurs in the j^{th} entry. Likewise,

$$B_{f_2}(e_i, e'_j) = B_{f_2}(e_i, e_j).$$

It follows that $q'_2 = q_2 = h_2(X_{t+1}, \ldots, X_n)$.

□

Lemma B.1.10. *Let K be a p-adic field, $\mathcal{O}_K$ be the ring of integers, and let π be an uniformizing element for K. Let $Q \in K[X_1, \ldots, X_n]$ be a quadratic form with $n \geqslant 2$. Let $e_i \in K^n$ denote the i^{th} standard basis vector of K^n. Let $F : K^n \to K$ denote the quadratic map associated to Q with respect to the standard basis $\{e_1, \ldots, e_n\}$. Suppose $Q(X)$ has the following shape:*

$$\begin{aligned} Q(X) = G(X_1, \ldots, X_t) + \pi \sum_{i=1}^{t} X_i L_i(X_{t+1}, \ldots, X_n) \\ + \pi H(X_{t+1}, \ldots, X_n), \end{aligned} \tag{B.1.3}$$

where G, H are quadratic forms over $\mathcal{O}_K$ and the L_i are linear forms over $\mathcal{O}_K$.

Suppose $det(G)$ is a unit in $\mathcal{O}_K$. Then there exist $e'_{t+1}, \ldots, e'_n \in (\mathcal{O}_K)^n$ with the following properties.

1. *$K^n = span(e_1, \ldots, e_t)\widehat{\bigoplus} span(e'_{t+1}, \ldots, e'_n)$.*

2. *For* $t+1 \leqslant j \leqslant n$, $e_j' = e_j + \sum_{s=1}^{t} c_{sj} e_s$, *where* $c_{sj} \in \mathcal{O}_K$ *and* $\pi \mid c_{sj}$.

3. *The quadratic form* Q' *associated to* F *with respect to the basis*

$$\{e_1, \ldots, e_t, e_{t+1}', \ldots, e_n'\}$$

has the shape

$$Q' = G(X_1, \ldots, X_t) + H'(X_{t+1}, \ldots, X_n),$$

where $H' \in \mathcal{O}_K[X_{t+1}, \ldots, X_n]$ *is a quadratic form with* $H' \equiv H \bmod \pi^2$.

4. $det(Q) = det(Q')$.

Proof. Let $M_Q = (m_{ij})$ denote the matrix of Q with respect to the standard basis of K^n. Let M_G denote the matrix of G with respect to the standard basis of K^t. Note that the upper $t \times t$ block of M_Q is the matrix M_G. For each $1 \leqslant i \leqslant n$, let $R_i = (m_{i1}, \ldots, m_{it})$. Note that for $1 \leqslant i \leqslant t$, R_i is the i^{th} row of M_G. Since $\det(G)$ is a unit, we see that $\text{span}_{\mathcal{O}_K}(R_1, \ldots, R_t) = (\mathcal{O}_K)^t$. Therefore, for each $j \in \{t+1, \ldots, n\}$, there exist $c_{1j}, \ldots, c_{tj} \in \mathcal{O}_K$ such that

$$c_{1j} R_1 + c_{2j} R_2 + \cdots + c_{tj} R_t = -R_j.$$

Equation $B.1.3$ implies that $\pi \mid R_j$. Since $\det(G)$ is a unit, the rows $R_1, \ldots, R_t$ are linearly independent modulo π. Therefore, $\pi \mid c_{1j}, \ldots, c_{tj}$. Let $U = \text{span}(e_1, \ldots, e_t)$, and for each $t+1 \leqslant j \leqslant n$, let $e_j' = e_j + \sum_{s=1}^{t} c_{sj} e_s$. Then Lemma $B.1.7$ implies that $\text{span}(e_{t+1}', \ldots, e_n') \subseteq U^{\perp}$, and

$$K^n = \text{span}(e_1, \ldots, e_t) \hat{\oplus} \text{span}(e_{t+1}', \ldots, e_n').$$

The quadratic form Q with respect to the basis $\{e_1, \ldots, e_t, e_{t+1}', \ldots, e_n'\}$ has the shape

$$Q = G(X_1, \ldots, X_t) + H'(X_{t+1}, \ldots, X_n),$$

where $H' \in \mathcal{O}_K[X_{t+1}, \ldots, X_n]$ is some quadratic form. Note that the change of basis matrix between the two bases is a triangular matrix with ones along the diagonal, hence the determinant of the change of basis matrix is 1. Thus $\det(Q) = \det(Q')$. To determine H', observe that

$$H' = \left(\sum_{j=t+1}^{n} Q(e_j') X_j^2 \right) + \left(\sum_{t+1 \leqslant j < \ell \leqslant n} B_Q(e_j', e_\ell') X_j X_\ell \right).$$

We will show that $Q(e_j') \equiv Q(e_j) \bmod \pi^2$, and $B_Q(e_j', e_\ell') \equiv B_Q(e_j, e_\ell) \bmod \pi^2$. This will imply that $H' \equiv H \bmod \pi^2$, as desired.

Observe that for $t+1 \leqslant j \leqslant n$, we have

$$\begin{aligned} Q(e_j') &= Q\left(e_j + \sum_{s=1}^{t} c_{sj} e_s\right). \\ &= Q(e_j) + Q\left(\sum_{s=1}^{t} c_{sj} e_s\right) + B_Q\left(e_j, \sum_{s=1}^{t} c_{sj} e_s\right). \\ &= Q(e_j) + Q\left(\sum_{s=1}^{t} c_{sj} e_s\right) + \sum_{s=1}^{t} c_{sj} B_Q(e_j, e_s). \end{aligned}$$

Since $\pi \mid c_{sj}$, we get $\pi^2 \mid Q(\sum_{s=1}^{t} c_{sj} e_s)$. Equation $B.1.3$ implies that $\pi \mid B_Q(e_j, e_s)$ for $1 \leqslant s \leqslant t$. Then $\pi^2 \mid \sum_{s=1}^{t} c_{sj} B_Q(e_j, e_i)$. Thus $Q(e_j') \equiv Q(e_j) \bmod \pi^2$.

Similarly, we have

$$\begin{aligned} B_Q(e_j', e_\ell') &= B_Q\left(e_j + \sum_{s=1}^{t} c_{sj} e_s, e_\ell + \sum_{s=1}^{t} c_{s\ell} e_s\right). \\ &= B_Q(e_j, e_\ell) + \left(\sum_{s=1}^{t} c_{s\ell} B_Q(e_j, e_s)\right) + \left(\sum_{s=1}^{t} c_{sj} B_Q(e_s, e_\ell)\right) \\ &+ B_Q\left(\sum_{s=1}^{t} c_{sj} e_s, \sum_{s=1}^{t} c_{s\ell} e_s\right). \end{aligned}$$

We have $\pi \mid c_{sj}$ and $\pi \mid c_{s\ell}$. Equation $B.1.3$ implies that $\pi \mid B_Q(e_j, e_s)$ for $t+1 \leqslant j \leqslant n$, and $\pi \mid B_Q(e_s, e_\ell)$ for $t+1 \leqslant \ell \leqslant n$. It follows that $B_Q(e_j', e_\ell') \equiv B_Q(e_j, e_\ell) \bmod \pi^2$. □

B.2 Forms over Finite Fields

Lemma B.2.1. *Let k be a finite field of characteristic not 2. Let $q \in k[X_1, \ldots, X_n]$ be a quadratic form with $n \geqslant 2$ even. If q has rank n and det(q) $= (-1)^{\frac{n}{2}} d$, where $d \in k^\times$ is a nonsquare, then q splits off exactly $\frac{n-2}{2}$ hyperbolic planes over k.*

Proof. Since k is a finite field and q has rank n, we know q splits off at least $\frac{n-2}{2}$ hyperbolic planes, hence

$$q = X_1 X_2 + \cdots + X_{n-3} X_{n-2} + q_0(X_{n-1}, X_n),$$

where q_0 has rank 2. We have

$$\det(q_0) = (-1)^{\frac{n-2}{2}} \det(q) = (-1)^{\frac{n-2}{2}} (-1)^{\frac{n}{2}} d = -d.$$

Since $\det(q_0) = -d$ with $d \in k^\times$ a nonsquare, we deduce that q_0 is anisotropic. Thus q splits off exactly $\frac{n-2}{2}$ hyperbolic planes. □

Lemma B.2.2. *Let $n(x_1, x_2)$ and $n(x_3, x_4)$ be anisotropic binary quadratic forms over a finite field k. Then $n(x_1, x_2) + n(x_3, x_4)$ vanishes on a 2-dimensional space over k.*

We prove Lemma B.2.2 by proving three general statements (Lemmas B.2.3, B.2.4, and B.2.5 below).

Lemma B.2.3. *Let k be an arbitrary field. Let $q(x_1, \ldots, x_n)$ be a quadratic form over k and assume that $rad(b_q) = 0$. Let $g(x_1, \ldots, x_n, y_1, \ldots, y_n) = q(x_1, \ldots, x_n) - q(y_1, \ldots, y_n)$. Then $rad(b_g) = 0$ and g vanishes on an n-dimensional subspace of k^{2n}.*

Proof. It is straightforward to check that $\mathrm{rad}(b_g) = 0$. Let W be the subspace of k^{2n} consisting of vectors $(a_1, \ldots, a_n, a_1, \ldots, a_n)$ where each $a_i \in k$. Then $\dim(W) = n$ and $(q(x_1, \ldots, x_n) - q(y_1, \ldots, y_n))(W) = 0$. □

Lemma B.2.4. *Let k be an arbitrary field. Suppose for some $n \geqslant 1$ that there exists a unique (up to isometry) quadratic form $q(x_1, \ldots, x_n)$ with q anisotropic over k and $rad(b_q) = 0$. Then $q(x_1, \ldots, x_n) \sim cq(x_1, \ldots, x_n)$ for every nonzero $c \in k$.*

Proof. Since $c \in k$ is nonzero, it follows that $\mathrm{rad}(b_{cq}) = 0$ and cq is anisotropic over k. Thus $q \sim cq$ by the hypothesis. □

Lemma B.2.5. *Let k be a finite field. Then there exists a unique (up to isometry) 2-dimensional quadratic form $n(x_1, x_2)$ that is anisotropic with $rad(b_{n(x_1,x_2)}) = 0$*

Proof. Lemma F.1.4 proves the result for $\mathrm{char}(k) = 2$. Assume $\mathrm{char}(k) \neq 2$. Let $d \in k^\times$ be a nonsquare. Note that $X^2 - dY^2$ is anisotropic of rank 2. Let $q(X, Y) \in k[X, Y]$ be an anisotropic rank 2 quadratic form. We will show that q is equivalent to $X^2 - dY^2$.

Consider $q(X, Y) - Z^2$. By Chevalley-Warning, this form is isotropic over k. Let (x_1, y_1, z_1) be a nontrivial zero. Since q is anisotropic, $z_1 \neq 0$. Thus $q(x_1, y_1) = z_1^2$, with $(x_1, y_1) \neq (0, 0)$. Then $q(\frac{x_1}{z_1}, \frac{y_1}{z_1}) = 1$. Through an invertible linear change of variable, we can assume $q(1, 0) = 1$. Write $q = X^2 + bXY + cY^2$. Let $f(X, Y) = q(X - \frac{b}{2}Y, Y)$. Then f is equivalent to q, and

$$f(X, Y) = (X - \frac{b}{2}Y)^2 + b(X - \frac{b}{2}Y)Y + cY^2.$$

Notice that the coefficient of X^2 in f is 1, and the coefficient of XY is 0. Thus $f(X, Y) = X^2 - c'Y^2$ for some $c' \in k$. Since f is anisotropic, c' is a nonsquare, hence $c' = de^2$ for some $e \in k^\times$. It follows that f is equivalent to $X^2 - dY^2$.

□

Proof of Lemma B.2.2. Lemmas B.2.4 and B.2.5 imply that $n(x_3, x_4) \sim -n(x_3, x_4)$. Then $n(x_1, x_2) + n(x_3, x_4) \sim n(x_1, x_2) - n(x_3, x_4)$ vanishes on a 2-dimensional space by Lemma B.2.3. □

Lemma B.2.6. *Suppose $n(X_1, X_2)$ and $n(X_3, X_4)$ are anisotropic quadratic form over a finite field k. Then $n(X_1, X_2) + n(X_3, X_4)$ splits off 2 hyperbolic planes over k.*

Proof. Lemma $B.2.2$ implies that $n(X_1, X_2) + n(X_3, X_4)$ vanishes on a 2-dimensional space over k. Thus Lemma $B.1.1$ implies that $n(X_1, X_2) + n(X_3, X_4)$ splits off 2 hyperbolic planes. □

Lemma B.2.7. *(Ireland and Rosen, page 150, problem 17.) Let F_q denote a finite field with q elements. For each $m > 0$ there is a homogeneous form of degree m in m variables over F_{q^m} with no nontrivial zero.*

Proof. Let $\omega_1, \ldots, \omega_m$ be a basis for F_{q^m} over F_q. Consider the homogeneous form of degree m:

$$f(x_1, \ldots, x_m) = \prod_{i=0}^{m-1} (\omega_1^{q^i} x_1 + \cdots + \omega_m^{q^i} x_m).$$

Suppose $(a_1, \ldots, a_m) \in A^m(F_q)$ is a zero of f. Then $\omega_1^{q^j} a_1 + \cdots + \omega_m^{q^j} a_m = 0$ for some j. Suppose p is the characteristic of F_q and write $q = p^k$ for some $k \geqslant 1$. Then

$$\omega_1^{p^{jk}} a_1 + \cdots + \omega_m^{p^{jk}} a_m = 0.$$

In F_q, every element is a p^{th} power. It follows that every element is a p^2 power, and a p^3 power, and so on. So for each i we can write $a_i = b_i^{p^{jk}}$ for some $b_i \in F_q$. This gives us

$$0 = \omega_1^{p^{jk}} b_1^{p^{jk}} + \cdots + \omega_m^{p^{jk}} b_m^{p^{jk}} = (\omega_1 b_1 + \cdots \omega_m b_m)^{p^{jk}}.$$

Therefore $\omega_1 b_1 + \cdots + \omega_m b_m = 0$. Since the ω_i's are linearly independent, we get that each $b_i = 0$, hence each $a_i = 0$ so that $(a_1, \ldots, a_m)$ is the trivial solution. □

Lemma B.2.8. *(Ireland and Rosen, page 150, problem 18.) Let F_q denote a finite field with q elements. Let $g_1, g_2, \ldots, g_m \in F_q[x_1, x_2, \ldots, x_n]$ be homogeneous polynomials of degree d and assume that $n > md$. Then there is a nontrivial common zero over F_{q^m}.*

Proof. Let f be the homogeneous polynomial of degree m as in the previous exercise:

$$f(x_1, \ldots, x_m) = \prod_{i=0}^{m-1} (\omega_1^{q^i} x_1 + \cdots + \omega_m^{q^i} x_m).$$

Since each g_i is homogeneous of degree d, it follows that the polynomial f^* defined by

$$f^*(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

is homogeneous of degree md. Note that since each g_i is homogeneous, f^* has the trivial zero. Since $n > md$, Chevalley's Theorem implies that f^* has a nontrivial zero, say $a = (a_1, \ldots, a_n)$. By Exercise 17, f has only the trivial zero, so it must be that a is a common zero of the g_i's. □

Lemma B.2.9. *Let $g_1(x_1, \ldots, x_n)$ and $g_2(x_1, \ldots, x_n)$ be quadratic forms defined over a finite field F. If $n \geqslant 5$, then g_1 and g_2 have a common nontrivial zero over F.*

Proof. Recall that over any finite field, up to equivalence, there is a unique anisotropic quadratic form of rank 2. Let $f(x_1, x_2)$ be an anisotropic quadratic form of rank 2 over F. Define $f^*(x_1, \ldots, x_n)$ by

$$f^*(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), g_2(x_1, \ldots, x_n)).$$

Then f^* is homogeneous of degree 4, and $f^*(0, \ldots, 0) = 0$. Since $n > 4$, Chevalley's Theorem implies that f^* has a nontrivial zero, say $a = (a_1, \ldots, a_n) \in F^n$. Then

$$f^*(g_1(a_1, \ldots, a_n), g_2(a_1, \ldots, a_n)) = 0.$$

Therefore $(g_1(a_1, \ldots, a_n), g_2(a_1, \ldots, a_n))$ is a zero of f. Since f is anisotropic, we must have

$$g_1(a_1, \ldots, a_n) = g_2(a_1, \ldots, a_n) = 0.$$

Therefore, $(a_1, \ldots, a_n)$ is a common nontrivial zero of g_1 and g_2. □

Lemma B.2.10. *Let $s_1(X, Y)$ and $s_2(X, Y)$ be quadratic forms over a finite field F. Suppose that s_1 and s_2 have no common factor and that $r(s_1, s_2) = 2$. Then there are at least $\frac{1}{2}(|F| - 1)^2$ pairs $(a, b) \in F^2$, not both zero, for which $as_1 + bs_2$ is a hyperbolic plane, and at least $\frac{1}{2}(|F| - 1)^2$ such pairs for which $as_1 + bs_2$ is anisotropic of rank 2.*

Proof. See [7, Lemma 8.3, p.62] □

Lemma B.2.11. *Let k be a finite field and $q \in k[X_1, \ldots, X_n]$ be a quadratic form with $n \geqslant 1$. Then q vanishes on a subspace over k of dimension*

$$\begin{cases} \frac{n-2}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Moreover, if q has order $< n$, then q vanishes on a subspace of dimension

$$\begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. We begin by proving the first statement, where we make no assumption on the order of q. We induct on n. For $n = 1, 2$, there is nothing to prove. Let $n \geqslant 3$ and assume by induction that the result holds for quadratic forms in $m < n$ variables over k. Given $q \in k[X_1, \ldots, X_n]$, if order$(q) = n$, then q splits off $\begin{cases} \frac{n-2}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$ hyperbolic planes, and the result follows. Assume order$(q) = m < n$. Through a change of variable, we can assume $q = q'(X_1, \ldots, X_m)$ for some quadratic form q'. By induction, q' vanishes on a subspace over k of dimension

$$\begin{cases} \frac{m-2}{2} & \text{if } m \text{ is even} \\ \frac{m-1}{2} & \text{if } m \text{ is odd.} \end{cases}$$

Therefore, if m is even, then q vanishes on a subspace over k of dimension

$$\frac{m-2}{2} + n - m = \frac{2n-m-2}{2} > \frac{2n-n-2}{2} = \frac{n-2}{2}, \tag{B.2.1}$$

which is sufficient. If m is odd, then q vanishes on a subspace over k of dimension

$$\frac{m-1}{2} + n - m = \frac{2n-m-1}{2} > \frac{2n-n-1}{2} = \frac{n-1}{2}, \tag{B.2.2}$$

which is sufficient. The second statement follows equations $B.2.1$ and $B.2.2$. □

Lemma B.2.12. *Suppose q_1 and q_2 are quadratic forms over a finite field F in $M = 2m+1$ variables, $m \geqslant 1$. Then $\{q_1, q_2\}$ vanish on a subspace of dimension $(M-3)/2 = m-1$ over F.*

Proof. This follows from Amer's Theorem. □

Lemma B.2.13. *Suppose q_1 and q_2 are quadratic forms over a finite field F in $M = 2m$ variables, $m \geqslant 1$. Then $\{q_1, q_2\}$ vanish on a subspace of dimension $(M-4)/2 = m-2$ over F.*

Proof. This follows from Amer's Theorem. □

Recall that given a quadratic form $q \in F[X_1, \ldots, X_n]$ over a field F, we define $D_F(q)$ to be the maximal dimension of a subspace in F^n on which q vanishes.

Lemma B.2.14. *Let k be a finite field. Let $q_1, q_2 \in k[X_1, \ldots, X_n]$ be quadratic forms with $n \geqslant 4$ even and $D_k(q_1, q_2) = \frac{n-4}{2}$. If $\mathcal{P}_k(q_1, q_2)$ contains a form of order 2, then there are at least*

$$\frac{1}{2}(|k|-1)^2 - (|k|-1)$$

nonzero pairs $(a, b) \in k^2$ for which $aq_1 + bq_2$ splits off $\frac{n}{2}$ hyperbolic planes over k. In particular, if $|k| > 3$, then there is at least one form in $\mathcal{P}_k(q_1, q_2)$ that splits off $\frac{n}{2}$ hyperbolic planes over k.

Proof. Without loss of generality, assume q_1 has order 2. Through a change of variable, we can write $q_1 = q_1'(X_1, X_2)$, where q_1' is a quadratic form over k of order 2. We can write q_2 in the following way:

$$q_2 = q_2'(X_1, X_2) + X_1\ell_1(X_3, \ldots, X_n) + X_2\ell_2(X_3, \ldots, X_n) + q(X_3, \ldots, X_n)$$

for quadratic forms q_2', q and linear forms ℓ_1, ℓ_2, all over k. We will show that q_1' is anisotropic.

Assume q_1' is isotropic. Through a change of variable involving X_1 and X_2, we can assume $q_1'(0,1) = 0$. Thus $q_1' = X_1\ell(X_1, X_2)$ for some linear form ℓ over k. By Lemma $B.2.11$, the form $q_2(0, X_2, \ldots, X_n)$ vanishes on a subspace $U' \subset k^{n-1}$ of dimension $\frac{n-2}{2}$. Let

$$U = \{(0, x_2, \ldots, x_n) \mid (x_2, \ldots, x_n) \in U'\}.$$

Then q_1 and q_2 both vanish on U, which has dimension $\frac{n-2}{2}$, a contradiction.

Therefore, q_1' is anisotropic. Next, we will show that $D_k(q) = \frac{n-4}{2}$.

Suppose q vanishes on a subspace $W' \subset k^{n-2}$. Let

$$W = \{(0, 0, x_3, \ldots, x_n) \mid (x_3, \ldots, x_n) \in W'\}.$$

Then $q_1(W) = q_2(W) = 0$. Thus $\dim(W) \leqslant D_k(q_1, q_2) = \frac{n-4}{2}$. On the other hand, since q has $n-2$ variables, Lemma B.2.11 implies that q vanishes on a subspace over k of dimension $\frac{n-4}{2}$. We deduce that $D_k(q) = \frac{n-4}{2}$.

Since $D_k(q) = \frac{n-4}{2}$, Lemma B.2.11 implies that q has order $n-2$. Then Lemma 2.1.14 implies that q has rank $n-2$. We therefore have

$$\begin{aligned} q_1 &= q_1'(X_1, X_2) \\ q_2 &= q_2'(X_1, X_2) + X_1\ell_1(X_3, \ldots, X_n) + X_2\ell_2(X_3, \ldots, X_n) + q(X_3, \ldots, X_n), \end{aligned}$$

where q_1' is anisotropic and q has rank $n-2$. Since q has rank $n-2$, Lemma B.1.9 implies that we can perform an invertible linear change of variable over k so that

$$\begin{aligned} q_1 &= q_1'(X_1, X_2) \\ q_2 &= h(X_1, X_2) + q(X_3, \ldots, X_n) \end{aligned}$$

for some quadratic form h. Since q has order $n-2$ and $D_k(q) = \frac{n-4}{2}$, we deduce that q splits off exactly $\frac{n-4}{2}$ hyperbolic planes. Through a change of variable involving $X_3, \ldots, X_n$, we can assume $q = X_3X_4 + \cdots + X_{n-3}X_{n-2} + g(X_{n-1}, X_n)$, where g is anisotropic. Thus

$$\begin{aligned} q_1 &= q_1'(X_1, X_2) \\ q_2 &= h(X_1, X_2) + X_3X_4 + \cdots + X_{n-3}X_{n-2} + g(X_{n-1}, X_n). \end{aligned}$$

To finish, we consider the following two cases.

Case 1. Suppose q_1' and h are linearly independent. This, together with the fact that q_1' is anisotropic, implies that q_1' and h do not share a common factor over k. Thus Lemma B.2.10 implies that there are at least $\frac{1}{2}(|k|-1)^2$ pairs $(a, b) \in k^2$, not both zero, for which $aq_1' + bh$ is anisotropic. At most $|k|-1$ of these pairs have $b = 0$. Therefore, there are at least

$$\frac{1}{2}(|k|-1)^2 - (|k|-1)$$

nonzero pairs $(a, b) \in k^2$ for which $aq_1' + bh$ is anisotropic and $b \neq 0$.

Case 2. Suppose q_1' and h are linearly dependent. By adding a multiple of q_1 to q_2, we can assume $h = 0$. Let $\lambda, \mu \in k^\times$. Then

$$\lambda q_1 + \mu q_2 = \lambda q_1'(X_1, X_2) + \mu X_3X_4 + \cdots + \mu X_{n-3}X_{n-2} + \mu g(X_{n-1}, X_n).$$

By Lemma $B.2.6$, $\lambda q_1' + \mu g$ splits off 2 hyperbolic planes. Thus, $\lambda q_1 + \mu q_2$ splits off $\frac{n}{2}$ hyperbolic planes. There are $|k|-1$ choices for λ and $|k|-1$ choices for μ, which gives us $(|k|-1)^2$ pairs in $\mathcal{P}_k(q_1, q_2)$ that split off $\frac{n}{2}$ hyperbolic planes, which is sufficient. $\square$

Remark: The first statement of Lemma $B.2.14$ is vacuously true for $|k| \in \{2,3\}$. The following examples show how the second statement of Lemma $B.2.14$ can fail when $|k| \in \{2,3\}$. Let $N(X,Y) \in k[X,Y]$ be anisotropic. Let

$$q_1 = N(X_1, X_2)$$
$$q_2 = X_1X_2 + X_3X_4 + \cdots + X_{n-3}X_{n-2} + N(X_{n-1}, X_n).$$

Note that $D_k(q_1, q_2) = \frac{n-4}{2}$. To show that no forms in $\mathcal{P}_k(q_1, q_2)$ split off $\frac{n}{2}$ hyperbolic planes, since $q_1 = N(X_1, X_2)$, it is sufficient to only consider forms of the shape $\lambda q_1 + q_2$, where $\lambda \in k$

Assume $|k| = 2$, then neither q_2 nor $q_1 + q_2$ split off $\frac{n}{2}$ hyperbolic planes.

Assume $|k| = 3$. Take $N(X_1, X_2) = X_1^2 + X_2^2$. Then neither q_2, $q_1 + q_2$, nor $2q_1 + q_2$ split off $\frac{n}{2}$ hyperbolic planes.

B.2.1 Systems of Quadratic Forms over Finite Fields

The content in this section is due to David Leep.

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_q^\times$ be the multiplicative group of nonzero elements of $\mathbb{F}_q$. The order of a quadratic form is the minimum number of variables needed to write the quadratic form after an invertible linear transformation.

Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a nonzero quadratic form and assume that f has order m, $1 \leqslant m \leqslant n$. There are three cases, which are called Type I, Type II, and Type III. Let $h(x,y)$ denote the unique, up to isometry, anisotropic quadratic forms in $\mathbb{F}_q[x,y]$. If m is even, then

$$f \cong \begin{cases} x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-1}x_m & \text{if } f \text{ is Type I,} \\ x_1x_2 + \cdots + x_{m-3}x_{m-2} + h(x_{m-1}, x_m) & \text{if } f \text{ is Type II.} \end{cases}$$

If m is odd, then f is Type III and

$$f \cong x_1x_2 + \cdots + x_{m-2}x_{m-1} + ax_m^2,$$

for some $a \in \mathbb{F}_q^\times$.

The following theorem can be found in many places including [13] and [18, Chapter IV]. We include a proof here for completeness.

Theorem B.2.15. *Assume the notation and hypotheses above. Then*

$$N(f, \mathbb{F}_q^n) = \begin{cases} q^{n-m}(q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m}{2}-1}) & \textit{if } f \textit{ is Type I,} \\ q^{n-m}(q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m}{2}-1}) & \textit{if } f \textit{ is Type II,} \\ q^{n-m} \cdot q^{m-1} & \textit{if } f \textit{ is Type III.} \end{cases}$$

Proof. We can assume that $f = f(x_1, \ldots, x_m) \in \mathbb{F}_q^m$. The proof is by induction on m. If $m = 1$, then f is Type III and $f = ax_1^2$ for some $a \in \mathbb{F}_q^\times$. Then $f = 0$ implies that $x_1 = 0$, so $N(f, \mathbb{F}_q^n) = q^{n-1} = q^{n-m} \cdot 1 = q^{n-m}$.

Suppose that $m = 2$. If f is Type I, then $f \cong x_1x_2$ and $N(f, \mathbb{F}_q^n) = q^{n-2}(2q-1) = q^{n-2}(q + q - 1)$. If f is Type II, then $N(f, \mathbb{F}_q^n) = q^{n-2} \cdot 1 = q^{n-2}(q - q + 1)$.

Assume that $m \geqslant 3$ and that the result has been proved for smaller values of m. Then $f \cong x_1x_2 + f_1(x_3, \ldots, x_m)$ and f, f_1 are the same Type. We first consider the case $x_2 \neq 0$, then the case $x_2 = 0$. This gives

$$\begin{aligned} N(f,\mathbb{F}_q^m) &= (q-1)q^{m-2} + qN(f_1, \mathbb{F}_q^{m-2}) \\ &= \begin{cases} q^{m-1} - q^{m-2} + q(q^{m-3} + q^{\frac{m-2}{2}} - q^{\frac{m-2}{2}-1}) & \text{if } f \text{ is Type I,} \\ q^{m-1} - q^{m-2} + q(q^{m-3} - q^{\frac{m-2}{2}} + q^{\frac{m-2}{2}-1}) & \text{if } f \text{ is Type II,} \\ q^{m-1} - q^{m-2} + q(q^{m-3}) & \text{if } f \text{ is Type III,} \end{cases} \\ &= \begin{cases} q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m}{2}-1} & \text{if } f \text{ is Type I,} \\ q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m}{2}-1} & \text{if } f \text{ is Type II,} \\ q^{m-1} & \text{if } f \text{ is Type III.} \end{cases} \end{aligned}$$

The result follows from this because $N(f, \mathbb{F}_q^n) = q^{n-m}N(f, \mathbb{F}_q^m)$. □

Let $Q_1, \ldots, Q_r \in \mathbb{F}_q[x_1, \ldots, x_n]$ be a system of quadratic forms defined over $\mathbb{F}_q$. Let $\vec{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ and $\vec{c} = (c_1, \ldots, c_r) \in \mathbb{F}_q^r$. For a quadratic form $Q \in \mathbb{F}_q[x_1, \ldots, x_n]$, let

$$N(Q) = |\{\vec{a} \in \mathbb{F}_q^n \mid Q(\vec{a}) = 0\}|.$$

Thus $N(Q)$ counts the zero vector. Let

$$N_0 = |\{\vec{a} \in \mathbb{F}_q^n \mid Q_i(\vec{a}) = 0,\ 1 \leqslant i \leqslant r\}|.$$

The $\mathbb{F}_q$-pencil of $\{Q_1, \ldots, Q_r\}$, denoted $\mathcal{P}_{\mathbb{F}_q}(Q_1, \ldots, Q_r)$, is the set of all $\mathbb{F}_q$-linear combinations of $\{Q_1, \ldots, Q_r\}$.

Proposition B.2.16.

$$q^n + \sum_{\substack{\vec{c} \in \mathbb{F}_q^r \\ \vec{c} \neq \vec{0}}} N\left(\sum_{i=1}^r c_iQ_i\right) = q^{n+r-1} + q^{r-1}(q-1)N_0$$

Proof. If $(Q_1(\vec{a}), \ldots, Q_r(\vec{a})) \neq (0, \ldots, 0)$, then $Q(\vec{a}) = 0$ for exactly q^{r-1} forms in $\mathcal{P}_{\mathbb{F}_q}(Q_1, \ldots, Q_r)$. If $(Q_1(\vec{a}), \ldots, Q_r(\vec{a})) = (0, \ldots, 0)$, then $Q(\vec{a}) = 0$ for all q^r forms in $\mathcal{P}_{\mathbb{F}_q}(Q_1, \ldots, Q_r)$. Thus

$$\sum_{\vec{c} \in \mathbb{F}_q^r} N\left(\sum_{i=1}^r c_iQ_i\right) = q^{r-1}(q^n - N_0) + q^rN_0.$$

Therefore

$$q^n + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} N\left(\sum_{i=1}^{r} c_i Q_i\right) = q^{n+r-1} + q^{r-1}(q-1)N_0.$$

□

Suppose that $Q \in \mathbb{F}_q[x_1, \ldots, x_n]$ and that the order of Q is m where $0 \leqslant m \leqslant n$. To compute $N(Q)$, there are four cases to consider.

$$N(Q) = q^{n-m}\begin{cases} q^{m-1} + q^{\frac{m-2}{2}}(q-1) & \text{if } Q \text{ is Type I} \\ q^{m-1} - q^{\frac{m-2}{2}}(q-1) & \text{if } Q \text{ is Type II} \\ q^{m-1} & \text{if } Q \text{ is Type III} \\ q^{m} & \text{if } Q = 0. \end{cases}$$

For details of this calculation, see Theorem B.2.15.

Theorem B.2.17. *Assume the notation from above. Then*

$$N_0 = q^{n-r} + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-r-\frac{m}{2}} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type I} \\ -q^{n-r-\frac{m}{2}} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type II} \\ 0 & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type III} \end{cases}$$

Proof.

$$q^n + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} N\left(\sum_{i=1}^{r} c_i Q_i\right) = q^{n+r-1} + q^{r-1}(q-1)N_0.$$

$$q^n + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-1} + q^{n-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type I} \\ q^{n-1} - q^{n-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type II} \\ q^{n-1} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type III.} \end{cases} = q^{n+r-1} + q^{r-1}(q-1)N_0$$

$$q^n + (q^r - 1)q^{n-1} + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type I} \\ -q^{n-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type II} \\ 0 & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type III} \end{cases} = q^{n+r-1} + q^{r-1}(q-1)N_0$$

$$q^{n-1} + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-m+\frac{m-2}{2}} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type I} \\ -q^{n-m+\frac{m-2}{2}} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type II} \\ 0 & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type III.} \end{cases} = q^{r-1}N_0$$

$$q^{n-r} + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-m+\frac{m-2}{2}-(r-1)} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type I} \\ -q^{n-m+\frac{m-2}{2}-(r-1)} & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type II} \\ 0 & \text{if } \sum_{i=1}^{r} c_i Q_i \text{ is Type III.} \end{cases} = N_0$$

$$q^{n-r} + \sum_{\substack{\vec{c}\in\mathbb{F}_q^r \\ \vec{c}\neq\vec{0}}} \begin{cases} q^{n-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is Type I} \\ -q^{n-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is Type II} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is Type III.} \end{cases} = N_0$$

□

Proposition B.2.18. *Assume that $r = 2$ and $n \geqslant 5$. Then $N_0 \geqslant 2$.*

Proof. This result follows immediately from Chevalley's theorem. However, we will give a proof using Theorem B.2.17.

Let $Q_1, Q_2 \in \mathbb{F}_q[x_1, \ldots, x_n]$ be quadratic forms with $n \geqslant 5$. First suppose that a form in the $\mathbb{F}_q$-pencil of Q_1 and Q_2 has order $\leqslant 2$. We can assume that $Q_1 = Q_1(x_1, x_2)$. Then set $x_1 = x_2 = 0$. Then $Q_2(0, 0, x_3, x_4, \ldots, x_n)$ is isotropic over $\mathbb{F}_q$ because $n - 2 \geqslant 3$, and thus Q_1, Q_2 have a nontrivial common zero over $\mathbb{F}_q$.

Now assume that each form in the $\mathbb{F}_q$-pencil of Q_1 and Q_2 has order $\geqslant 3$. Then in Theorem B.2.17, whenever m occurs in the formula we have m is even (because Q has Type I or II) and thus $m \geqslant 4$. Theorem B.2.17 now gives

$$N_0 \geqslant q^{n-2} - (q^2 - 1)q^{n-2-\frac{4}{2}} = q^{n-2} - (q^2 - 1)q^{n-4} = q^{n-4} \geqslant q \geqslant 2.$$

□

Lemma B.2.19. *Assume that $r = 2$, $n \geqslant 3$, and $m \geqslant 3$ for all $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$. Then $N_0 = 1$ if and only if $n = 4$, $m = 4$ for all $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$, and each $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$ is Type II.*

Proof. First assume that $n = 4$, $m = 4$ for all $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$, and each $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$ is Type II. Then Theorem B.2.17 gives $N_0 = 1$.

Now assume that $N_0 = 1$. Proposition B.2.18 implies that $n \leqslant 4$. If $n = 3$, then $m = 3$ for each $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$. Then Theorem B.2.17 would give $N_0 = q \geqslant 2$, a contradiction. Thus $n = 4$. Now we have $1 = N_0 \geqslant q^2 + (q^2 - 1)(-q^0) = 1$. Therefore equality occurs and so we must have $m = 4$ for all $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$ and each $Q \in \mathcal{P}_{\mathbb{F}_q}(Q_1, Q_2)$ is Type II. □

Lemma B.2.20. *Let $q_1, q_2 \in \mathbb{F}_q[X_1, \ldots, X_4]$ be quadratic forms. Suppose every form in $\mathcal{P}_{\mathbb{F}_q}(q_1, q_2)$ has order $\geqslant 3$. Then $D_{\mathbb{F}_q}(q_1, q_2) = 0$ if and only if every form in $\mathcal{P}_{\mathbb{F}_q}(q_1, q_2)$ has order 4 and splits off exactly 1 hyperbolic plane.*

Proof. This is a rephrasing of Lemma B.2.19. □

Lemma B.2.21. *Let $g_1, g_2 \in \mathbb{F}_q[X_1, \ldots, X_5]$ be quadratic forms. Suppose every form in $\mathcal{P} = \mathcal{P}_{\mathbb{F}_q}(g_1, g_2)$ has order $\geqslant 2$. Further, assume that any form in $\mathcal{P}$ of order 2 is anisotropic. Then there is at least one form in $\mathcal{P}$ of order $\geqslant 3$.*

Proof. For sake of contradiction, assume that every form in $\mathcal{P}$ is anisotropic of order 2. Applying Theorem B.2.17 for $n = 5$ and $r = 2$ gives us

$$N_0 = q^3 - (q^2 - 1)q^2 = q^2(q - q^2 + 1).$$

Since $q \geqslant 2$, $q - q^2 + 1 < 0$. This is contradiction because $N_0 \geqslant 1$. □

Lemma B.2.22. *Suppose $g_1, g_2 \in \mathbb{F}_q[X_1, X_3, X_3]$ are quadratic forms with $D_{\mathbb{F}_q}(g_1, g_2) = 0$ (i.e. $N_0 = 1$). Suppose every form in $\mathcal{P}_{\mathbb{F}_q}(g_1, g_2)$ is either anisotropic of order 2 or has order 3. Then there are exactly $q - 1$ pairs $(a, b) \in \mathbb{F}_q^2$, not both zero, for which $ag_1 + bg_2$ is anisotropic of order 2.*

Proof. Let δ be the number of pairs $(a, b) \in \mathbb{F}_q^2$, not both zero, for which $ag_1 + bg_2$ is anisotropic of order 2 (i.e. type II with $m = 2$). Applying Theorem B.2.17 with $N_0 = 1$, $n = 3$ and $r = 2$ gives $1 = q - \delta$, hence $\delta = q - 1$. □

Lemma B.2.23. *Suppose $h_1, h_2 \in \mathbb{F}_q[X_1, X_2]$ are linearly independent quadratic forms with $D_{\mathbb{F}_q}(h_1, h_2) = 0$ (i.e. $N_0 = 1$). Then there are at least q pairs $(a, b) \in \mathbb{F}_q^2$, not both zero, for which $ah_1 + bh_2$ is isotropic.*

Proof. Since h_1 and h_2 are linearly independent, every form in $\mathcal{P} = \mathcal{P}_{\mathbb{F}_q}(h_1, h_2)$ has order $\geqslant 1$. For each $i = 1, 2, 3$, let δ_i denote the the number of pairs $(a, b) \in \mathbb{F}_q^2$, not both zero, for which $ah_1 + bh_2$ is type i. It follows that the number of pairs $(a, b) \in \mathbb{F}_q^2$, not both zero, for which $ah_1 + bh_2$ is isotropic is $\delta_1 + \delta_3$. We will show that $\delta_1 + \delta_3 \geqslant q$.

Applying Theorem B.2.17 with $N_0 = 1$, $n = 2$, and $r = 2$ gives us

$$1 = 1 + \delta_1 q^{-1} - \delta_2 q^{-1}.$$

It follows that $\delta_1 = \delta_2$.

Suppose $q = 2$. Then the number of forms in the pencil $\mathcal{P}_{\mathbb{F}_q}(h_1, h_2)$ is $q^2 - 1 = 3$. Thus, either $\delta_1 = \delta_2 = \delta_3 = 1$ or $\delta_1 = \delta_2 = 0$ and $\delta_3 = 3$. In either case, the inequality $\delta_1 + \delta_3 \geqslant q = 2$ is satisfied, as desired.

Suppose $q \geqslant 3$. Let $\delta = \delta_1 = \delta_2$. We have

$$2\delta + \delta_3 = |\mathcal{P}_{\mathbb{F}_q}(h_1, h_2)| = q^2 - 1.$$

Observe $\delta \leqslant \frac{q^2-1}{2}$ and that

$$\delta + \delta_3 = q^2 - 1 - \delta \geqslant q^2 - 1 - \frac{q^2 - 1}{2} = \frac{q^2 - 1}{2}.$$

Since $q \geqslant 3$, we get $\frac{q^2-1}{2} \geqslant q$. This completes the proof. □

Appendix C: Modules over PID's

Let R be a PID and let K be the fraction field of R. Let p be an irreducible element in R and let (p) be the prime ideal generated by p. Let $n \geqslant 1$ and let $V = K^n$. Let $v_p : K \to \mathbb{Z} \cup \{\infty\}$ denote the p-adic valuation of K.

Theorem C.0.1. *Let $v_1, \ldots, v_m \in R^n$ and assume that $v_1, \ldots, v_m$ are linearly independent over K. Then there exist $w_1, \ldots, w_m \in R^n$ satisfying the following conditions.*

1. *$v_1, \ldots, v_m$ and $w_1, \ldots, w_m$ span the same subspace of K^n.*

2. *$w_1, \ldots, w_m$ are linearly independent over $R/(p)$.*

We shall give two proofs of this theorem.

Proof # 1: We have $m \leqslant n$ because $v_1, \ldots, v_m$ are linearly independent over K. Let $v_i = (a_{i1} \cdots a_{in}) \in R^n$, $1 \leqslant i \leqslant m$, and let $A = (a_{ij})$ be the corresponding $m \times n$ matrix.

Denote the $\binom{n}{m}$ $m \times m$ submatrices of A by A_α where $1 \leqslant \alpha \leqslant \binom{n}{m}$. Since each entry of A lies in R, we have $v_p(\det(A_\alpha)) \geqslant 0$ for every α. Let

$$c(A) = \min \left\{ v_p(\det(A_\alpha)) \mid 1 \leqslant \alpha \leqslant \binom{n}{m} \right\}.$$

Thus $c(A) \geqslant 0$. Since $v_1 \ldots, v_m$ are linearly independent over K, at least one $\det(A_\alpha) \neq 0$, and thus $c(A) \neq \infty$.

Suppose that $v_1, \ldots, v_m$ are linearly dependent over $R/(p)$. Then there exist $b_1, \ldots, b_m \in R$, where at least one $b_i \notin (p)$, such that $b_1 v_1 + \cdots + b_m v_m = pv$ for some $v \in R^n$. We can assume that $b_m \notin (p)$. In particular, $b_m \neq 0$. Let

$$w_i = \begin{cases} v_i, & 1 \leqslant i \leqslant m-1 \\ v, & i = m. \end{cases}$$

Then $v_1, \ldots, v_m$ and $w_1, \ldots, w_m$ span the same subspace of K^n. Note that $w_1, \ldots, w_m \in R^n$.

Let B, C denote the $m \times n$ matrices associated to

$$w_1, \ldots, w_{m-1}, pw_m,$$

and

$$w_1, \ldots, w_{m-1}, w_m,$$

respectively. The first $m-1$ rows of A, B, C are the same. We have $\det(B_\alpha) = b_m \det(A_\alpha)$ and $\det(C_\alpha) = p^{-1} b_m \det(A_\alpha)$ for each α. Since $b_m \notin (p)$, we have $c(B) = c(A)$ and $c(C) = c(A) - 1$. We have $c(A) = c(B) \geqslant 1$ because $pw_m \in pR^n$, and thus $c(C) \geqslant 0$.

If $w_1, \ldots, w_m$ are linearly independent over $R/(p)$, then we are done. If not, then we repeat this construction. The process must end because $c(A) \geqslant 0$ at each step. Thus eventually we come to a matrix A with $c(A) = 0$. For such a matrix, we have $\det(A_\alpha) \notin (p)$ for some α, which means that the vectors are linearly independent over $R/(p)$.

Proof # 2: Let $M = R^n$. Then M is a finitely generated module over the PID R. Let N be the R-submodule of M generated by $v_1, \ldots, v_m$. That is, $N = R \cdot v_1 + \cdots + R \cdot v_m$. [6, Chapter 12, Theorem 4, p.460] implies that there is an R-basis $y_1, \ldots, y_n$ of M and nonzero elements $d_1, \ldots, d_m \in R$ such that $d_1 y_1, \ldots, d_m y_m$ is an R-basis of N. That is, $N = R \cdot d_1 y_1 + \cdots + R \cdot d_m y_m$.

The subspace of K^n spanned by $v_1, \ldots, v_m$ is the same as the subspace spanned by $d_1 y_1, \ldots, d_m y_m$. Since each $d_i \neq 0$, it follows that the subspace of K^n spanned by $v_1, \ldots, v_m$ is the same as the subspace spanned by $y_1, \ldots, y_m$.

We now show that $y_1, \ldots, y_n$ are linearly independent over $R/(p)$. Suppose that there exist $a_1, \ldots, a_n \in R$, where at least one $a_i \notin (p)$, such that $a_1 y_1 + \cdots + a_n y_n = pv$ for some $v \in M$. Since $y_1, \ldots, y_n$ is an R-basis of M, we can write $v = b_1 y_1 + \cdots + b_n y_n$ where each $b_i \in R$. Then $a_1 v_1 + \cdots + a_n y_n = p(b_1 y_1 + \cdots + b_n y_n)$, which implies that $a_i = pb_i$ for $1 \leqslant i \leqslant n$, a contradiction.

Thus $y_1, \ldots, y_n$ are linearly independent over $R/(p)$, and so the same holds for the subset $y_1, \ldots, y_m$.

Appendix D: The Discriminant of a Binary Homogeneous Form

D.1 General Definition

We begin by defining the discriminant of an arbitrary homogeneous form $P = P(X, Y)$ over an infinite field K and show that our definition is well-defined.

Definition D.1.1. *Over the algebraic closure $\overline{K}$, P splits into linear factors:*

$$P(X,Y) = \prod_{i=1}^{n}(\alpha_i X - \beta_i Y) \qquad \alpha_i, \beta_i \in \overline{K}.$$

The discriminant of P, denoted disc(P), is defined as

$$disc(P) = \prod_{i<j}(\alpha_j\beta_i - \alpha_i\beta_j)^2.$$

For this definition to be well-defined, we need to show that it is independent of the factorization of P into linear factors. To this end, suppose

$$P(x,y) = \prod_{i=1}^{n}(\alpha_i' X - \beta_i' Y)$$

is another factorization of P, where $\alpha_i', \beta_i' \in \overline{K}$. We consider two cases.

(i) Suppose $\prod_{i=1}^n \alpha_i \neq 0$. Observe that $P(1,0) = \prod_{i=1}^n \alpha_i = \prod_{i=1}^n \alpha_i'$. Thus $\prod_{i=1}^n \alpha_i' \neq 0$. We have

$$\prod_{i=1}^{n}(\alpha_i X - \beta_i Y) = \prod_{i=1}^{n}(\alpha_i' X - \beta_i' Y).$$

$$\left(\prod_{i=1}^{n}\alpha_i\right)\prod_{i=1}^{n}(X - (\beta_i/\alpha_i)Y) = \left(\prod_{i=1}^{n}\alpha_i'\right)\prod_{i=1}^{n}(X - (\beta_i'/\alpha_i')Y).$$

Since $\prod_{i=1}^n \alpha_i = \prod_{i=1}^n \alpha_i'$, we obtain

$$\prod_{i=1}^{n}(X - (\beta_i/\alpha_i)Y) = \prod_{i=1}^{n}(X - (\beta_i'/\alpha_i')Y).$$

Take $Y = 1$ to get

$$\prod_{i=1}^{n}(X - \beta_i/\alpha_i) = \prod_{i=1}^{n}(X - \beta_i'/\alpha_i').$$

There is some reordering of the indices so that

$$\frac{\beta_i}{\alpha_i} = \frac{\beta'_i}{\alpha'_i}.$$

Let $\gamma_i = \frac{\alpha'_i}{\alpha_i}$. Then $\alpha_i\gamma_i = \alpha'_i$ and

$$\frac{\beta_i}{\alpha_i} = \frac{\beta'_i}{\alpha'_i} = \frac{\beta'_i}{\alpha\gamma_i}.$$

This implies that $\beta'_i = \gamma_i\beta_i$. Also, since $\prod_{i=1}^n \alpha_i = \prod_{i=1}^n \alpha'_i$, we get that $\prod_{i=1}^n \gamma_i = 1$. We have

$$P(x,y) = \prod_{i=1}^n (\alpha'_i X - \beta'_i Y) = \prod_{i=1}^n (\gamma_i\alpha_i X - \gamma_i\beta_i Y)$$

so that the discriminant of P with respect to this factorization is

$$\begin{aligned}
\text{disc}(P) &= \prod_{i<j} (\gamma_j\gamma_i\alpha_j\beta_i - \gamma_j\gamma_i\alpha_i\beta_j)^2 . \\
&= \prod_{i<j} \left((\gamma_j\gamma_i)^2(\alpha_j\beta_i - \alpha_i\beta_j)^2\right) . \\
&= \left(\prod_{i=1}^n \gamma_i^{2(n-1)}\right) \prod_{i<j}(\alpha_j\beta_i - \alpha_i\beta_j)^2. \\
&= \prod_{i<j}(\alpha_j\beta_i - \alpha_i\beta_j)^2.
\end{aligned}$$

This is the discriminant of P with respect to our original factorization. We conclude that our definition of disc(P) is well-defined in this case.

(ii) If $\prod_{i=1}^n \alpha_i = 0$, then factor out the highest power of Y from P:

$$P(X,Y) = Y^k P'(X,Y).$$

Now if $P'(X,Y) = \prod_{i=1}^n(\alpha''_i X - \beta''_i Y)$, then $\prod_{i=1}^n \alpha''_i \neq 0$. Apply case (i) to P' to finish the proof.

Lemma D.1.2. *Let $P(X,Y) \in K[X,Y]$ be a homogeneous form over an infinite field K. Then $P(X,Y)$ has repeated linear factors if and only if disc$(P) = 0$.*

Proof. Notice that

$$\begin{aligned}
\text{disc}(P) = 0 &\iff \det\begin{bmatrix}\alpha_j & \alpha_i \\ \beta_j & \beta_i\end{bmatrix} = 0 \\
&\iff (\alpha_j,\beta_j) \text{ and } (\alpha_i,\beta_i) \text{ are linearly dependent.}
\end{aligned}$$

It follows that disc$(P) = 0$ if and only if two of the factors in $P = \prod_{i=1}^n(\alpha_i x - \beta_i y)$ differ by a scalar multiple. □

Theorem D.1.3. *Let R be an integral domain and F be its fraction field. Assume char(F) $\neq 2$. Let $P(X,Y) \in F[X,Y]$ be a homogeneous form. Then the following statements hold.*

1. *If $P(X,Y) \in R[X,Y]$, then disc($P(X,Y)) \in R$.*
2. *disc($P(X,Y)$) is a polynomial over $\mathbb{Z}$ in the coefficients of P.*

Proof. (1) If $P(X,Y) = 0$, then $\mathrm{disc}(P(X,Y)) = 0 \in R$. Now assume that $P(X,Y) \neq 0$. Then

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

where $P(X,Y)$ is a homogeneous polynomial of degree n with $\lambda_i, \mu_i \in F^{alg}$ and $(\lambda_i, \mu_i) \neq (0,0)$, $1 \leqslant i \leqslant n$.

If λ_i (or μ_i) is zero for more than one i, then (D.1.2) implies that $\mathrm{disc}(P(X,Y)) = 0$. 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, $1 \leqslant i \leqslant n$. Then we can rewrite

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

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

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

Then $p(Z) \in R[Z]$ is polynomial of degree n and $P(X,Y)$ is the homogenization of $p(Z)$. Let $p'(Z) = \sum_{i=0}^{n-1} \beta_i Z^i$ denote the derivative of p with respect Z. By [10, Proposition 8.5, page 204], the resultant of p, p' is

$$\mathrm{Res}(p,p') = (-1)^{n(n-1)/2} \alpha_n D(p(Z)),$$

where

$$D(p(Z)) = \alpha_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (t_i - t_j)^2.$$

By the definition of resultant in [10, page 200], $\mathrm{Res}(p,p')$ is the determinant of the matrix A_{2n-1} below whose entries are determined by the coefficients of p and p'. This implies that $\mathrm{Res}(p,p') \in R$.

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

The matrix A_{2n-1} is a $(n + (n-1)) \times (n + (n-1))$ matrix with entries in R and where 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, $\mathrm{Res}(p, p')$ is also divisible by α_n. This implies that

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

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

$$\begin{aligned} \alpha_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (t_i - t_j)^2 &= \left(\prod_{i=1}^n \lambda_i \right)^{2n-2} \prod_{1 \leqslant i < j \leqslant n} \left(\frac{\mu_i}{\lambda_i} - \frac{\mu_j}{\lambda_j} \right)^2 \\ &= \left(\prod_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j \right)^2 \prod_{1 \leqslant i < j \leqslant n} \left(\frac{\mu_i}{\lambda_i} - \frac{\mu_j}{\lambda_j} \right)^2 \\ &= \prod_{1 \leqslant i < j \leqslant n} (\lambda_i \mu_j - \lambda_j \mu_i)^2 = \mathrm{disc}(P(X, Y)). \end{aligned}$$

Putting these equations together give $\mathrm{disc}(P(X, Y)) \in R$.

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 $\lambda_i \neq 0$, $1 \leqslant i \leqslant n-1$, the proof of Case 1 shows that

$$\prod_{1 \leqslant i < j \leqslant n-1} (\lambda_i \mu_j - \lambda_j \mu_i)^2 \in R.$$

Since $\prod_{i=1}^{n-1} \lambda_i \in R$, and $\lambda_n = 0$, $\mu_n = -1$, we have

$$\begin{aligned} \mathrm{disc}(P(X, Y)) &= \prod_{1 \leqslant i < j \leqslant n} (\lambda_i \mu_j - \lambda_j \mu_i)^2 \\ &= \prod_{i=1}^{n-1} (-\lambda_i)^2 \prod_{1 \leqslant i < j \leqslant n-1} (\lambda_i \mu_j - \lambda_j \mu_i)^2 \in R. \end{aligned}$$

(2) Suppose $P(X,Y)$ has degree n. We can write $P(X,Y) = \sum_{i+j=n} a_{ij} X^i Y^j$, where $a_{ij} \in F$. Let t_{ij} be variables over $\mathbb{Z}$ (algebraically independent over $\mathbb{Q}$). Let $P'(X,Y) = \sum_{i+j=n} t_{ij} X^i Y^j$. Let $R = \mathbb{Z}[\{t_{ij}\}]$. Then $P'(X,Y) \in R[X,Y]$. By (2), we have $\mathrm{disc}(P'(X,Y)) \in R = \mathbb{Z}[\{t_{ij}\}]$. By substituting t_{ij} with a_{ij}, we get that $\mathrm{disc}(P(X,Y))$ is a polynomial over $\mathbb{Z}$ in the coefficients of P. □

D.2 The Discriminant of det$(\lambda Q_1 + \mu Q_2)$

Let $Q_1 = Q_1(X_1, \ldots, X_n)$ and $Q_2 = Q_2(X_1, \ldots, X_n)$ be quadratic forms over an infinite field K. We define

$$F(x, y; Q_1, Q_2) = F(x, y) = \det(xQ_1 + yQ_2)$$

so that F is a homogeneous form in the variables x and y. We assume that $F(x, y)$ does not vanish identically over $\overline{K}$ and $F(x, y)$ splits into distinct linear factors over $\overline{K}$, where $\overline{K}$ denotes the algebraic closure of K. Therefore

$$F(x, y) = \prod_{i=1}^{n} (\alpha_i x - \beta_i y) \qquad \alpha_i, \beta_i \in \overline{K}.$$

Since K is an infinite field, the zero polynomial is the only polynomial that vanishes identically over K. We are assuming that $F(x, y)$ does not vanish identically over $\overline{K}$; therefore, we deduce that there is some form Q in the pencil (Q_1, Q_2) that has rank n. Then $(Q_1, Q_2) = (Q, Q')$ for some form Q' in the pencil. This shows that we can assume $\mathrm{rk}(Q_1) = n$ from the start.

Since $F(1, 0) = \det(Q_1)$, we deduce that $\det(Q_1)$ is the coefficient of x^n in $F(x, y)$, hence $\det(Q_1) = \prod_{i=1}^{n} \alpha_i$. Factoring out $\det(Q_1)$ from $F(x, y)$ yields

$$F(x, y) = \det(Q_1) \prod_{i=1}^{n} (x - (\beta_i/\alpha_i)y).$$

Let $\lambda_i = \beta_i/\alpha_i$ Now, unlike Heath-Brown, we will define $\Delta(Q_1, Q_2)$ in the following way:

Definition D.2.1.

$$\Delta(Q_1, Q_2) := \mathit{det}(Q)^{2(n-1)} \prod_{i<j} (\lambda_i - \lambda_j)^2.$$

It may not be obvious that this definition is independent of the factorization of F. We will show that $\Delta(Q_1, Q_2) = \mathrm{disc}(F)$. This will imply that our definition of $\Delta(Q_1, Q_2)$ is well-defined since we already showed that the discriminant of F is independent of the factorization of F.

Proposition D.2.2. *We have $\Delta(Q_1, Q_2) = \mathit{disc}(F)$.*

Proof. Observe that

$$\begin{aligned}\Delta(Q_1,Q_2) &= \det(Q)^{2(n-1)}\prod_{i<j}(\lambda_i-\lambda_j)^2.\\ &= \det(Q)^{2(n-1)}\prod_{i<j}\left(\frac{\beta_i}{\alpha_i}-\frac{\beta_j}{\alpha_j}\right)^2.\\ &= \det(Q)^{2(n-1)}\prod_{i<j}\left(\frac{\alpha_j\beta_i-\alpha_i\beta_j}{\alpha_i\alpha_j}\right)^2.\end{aligned}$$

For each i, there are $n-1$ j's such that $i<j$. Thus, as the product runs through pairs (i,j) with $i<j$, each α_i will appear $n-1$ times. This implies that

$$\begin{aligned}\Delta(Q_1,Q_2) &= \det(Q)^{2(n-1)}\prod_{i<j}\left(\frac{\alpha_j\beta_i-\alpha_i\beta_j}{\alpha_1^{n-1}\alpha_2^{n-1}\cdots\alpha_n^{n-1}}\right)^2.\\ &= \det(Q)^{2(n-1)}\prod_{i<j}\frac{(\alpha_j\beta_i-\alpha_i\beta_j)^2}{\alpha_1^{2(n-1)}\alpha_2^{2(n-1)}\cdots\alpha_n^{2(n-1)}}.\\ &= \det(Q)^{2(n-1)}\left(\frac{1}{\alpha_1\alpha_2\cdots\alpha_n}\right)^{2(n-1)}\prod_{i<j}(\alpha_j\beta_i-\alpha_i\beta_j)^2.\end{aligned}$$

Since $\prod_{i=1}^n\alpha_i=\det(Q)$, we see that $\det(Q)^{2(n-1)}$ cancels above, and so we conclude that

$$\Delta(Q_1,Q_2)=\prod_{i<j}(\alpha_j\beta_i-\alpha_i\beta_j)^2. \qquad (**)$$

From this formula, we see that $\Delta(Q_1,Q_2)=\mathrm{disc}(F(x,y))$, which is what Heath-Brown uses as the definition of $\Delta(Q_1,Q_2)$.

□

Let $T\in\mathrm{GL}(K^n)$ and $U\in\mathrm{GL}_2(K)$. If

$$U=\begin{bmatrix}a&b\\c&d\end{bmatrix},$$

then

$$(Q_1,Q_2)^U=(aQ_1+bQ_2,cQ_1+dQ_2).$$

We define $(Q_1,Q_2)_T$ by

$$(Q_1,Q_2)_T=(Q_1(TX),Q_2(TX)).$$

Corollary D.2.3. *Given $T\in GL(K^n)$ and $U\in GL_2(K)$, we have*

$$\Delta((Q_1,Q_2)_T^U)=(det(U))^{n(n-1)}(det(T))^{4(n-1)}\Delta(Q_1,Q_2).$$

Proof. It suffices to show that $\Delta(Q_1, Q_2)^U = (\det(U))^{n(n-1)}\Delta(Q_1, Q_2)$ and $\Delta(Q_1, Q_2)_T = (\det(T))^{4(n-1)}\Delta(Q_1, Q_2)$.

(1) $\Delta(Q_1, Q_2)^U$: Let $Q_1' = aQ_1 + bQ_2$ and $Q_2' = cQ_1 + dQ_2$. Observe that

$$\begin{aligned}\det(xQ_1' + yQ_2') &= \det(x(aQ_1 + bQ_2) + y(cQ_1 + dQ_2)).\\ &= \det((ax + cy)Q_1 + (xb + dy)Q_2).\\ &= F(ax + cy, xb + dy).\\ &= \prod_{i=1}^{n} \left(\alpha_i(ax + cy) - \beta_i(xb + dy)\right).\\ &= \prod_{i=1}^{n} \left((a\alpha_i - b\beta_i)x - (d\beta_i - c\alpha_i)y\right).\end{aligned}$$

Let $\alpha_i' = a\alpha_i - b\beta_i$ and $\beta_i' = d\beta_i - c\alpha_i$. Then

$$\Delta(Q_1', Q_2') = \prod_{i<j}(\alpha_j'\beta_i' - \alpha_i'\beta_j')^2.$$

Let $A = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$, $B = \begin{bmatrix} \alpha_j & \alpha_i \\ \beta_j & \beta_i \end{bmatrix}$, and $C = \begin{bmatrix} \alpha_j' & \alpha_i' \\ \beta_j' & \beta_i' \end{bmatrix}$. Then

$$\alpha_j'\beta_i' - \alpha_i'\beta_j' = \det(C) = \det(A)\det(B) = \det(U)\det(B).$$

It follows that

$$\begin{aligned}\Delta(Q_1', Q_2') &= \prod_{i<j} \left(\det(U)^2(\alpha_j\beta_i - \alpha_i\beta_j)^2\right).\\ &= \left(\det(U)^2\right)^{\frac{n(n-1)}{2}} \Delta(Q_1, Q_2).\\ &= \det(U)^{n(n-1)}\Delta(Q_1, Q_2).\end{aligned}$$

(2) $\Delta(Q_1, Q_2)_T$: Let A be the matrix of $T : K^n \to K^n$ with respect to the standard basis for K^n so that $T(X) = AX$ for $X \in K^n$. Let $M(Q_1) = B_1$ and $M(Q_2) = B_2$ so that

$$Q_1(X) = X^T B_1 X \quad \text{and} \quad Q_2(X) = X^T B_2 X.$$

Then

$$Q_1(TX) = X^T A^T B_1 AX \quad \text{and} \quad Q_2(TX) = X^T A^T B_2 AX.$$

Observe

$$\begin{aligned}\det(xQ_1(TX) + yQ_2(TX)) &= \det(xA^T B_1 A + yA^T B_2 A).\\ &= \det(A^T)\det(xB_1 + yB_2)\det(A).\\ &= \det(A)^2 F(x, y).\\ &= \det(A)^2 \prod_{i=1}^{n}(\alpha_i x - \beta_i y).\\ &= \prod_{i=1}^{n}(\det(A)^{2/n}(\alpha_i x - \beta_i y)).\end{aligned}$$

Therefore

$$\begin{aligned}\Delta(Q_1(TX), Q_2(TX)) &= \prod_{i<j} \left(\det(A)^{4/n}(\alpha_j\beta_i - \alpha_i\beta_j)\right)^2. \\ &= \left(\det(A)^{8/n}\right)^{\frac{n(n-1)}{2}} \Delta(Q_1, Q_2). \\ &= \det(A)^{4(n-1)}\Delta(Q_1, Q_2). \\ &= \det(T)^{4(n-1)}\Delta(Q_1, Q_2).\end{aligned}$$

□

Proposition D.2.4. *Let K be the completion of a number field k with respect to a valuation v and $\mathcal{O}_K$ the valuation ring. Suppose $Q_1 = Q_1(X_1, \ldots, X_n)$ and $Q_2 = Q_2(X_1, \ldots, X_n)$ are quadratic forms with coefficients in $\mathcal{O}_K$ and that rk$(Q_1) = n$. If $F(x, y) = det(xQ_1 + yQ_2)$ has coefficients in $\mathcal{O}_K$, then $\Delta(Q_1, Q_2) = disc(F) \in \mathcal{O}_K$.*

Proof. First note that the valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ extends to $v : \overline{K} \to \mathbb{Z} \cup \{\infty\}$. Over $\overline{K}$, we have

$$F(x, y) = \prod_{i=1}^{n}(\alpha_i x - \beta_i y) \quad \alpha_i, \beta_i \in \overline{K}.$$

Since $\text{rk}(Q_1) = n$, we have that $\prod_{i=1}^{n} \alpha_i \neq 0$. Let

$$r_i = \begin{cases} \alpha_i & \text{if } v(\alpha_i) \leqslant v(\beta_i) \\ \beta_i & \text{if } v(\beta_i) \leqslant v(\alpha_i). \end{cases}$$

If $v(\alpha_i) = v(\beta_i)$, then arbitrarily pick r_i to be one of α_i or β_i. If $\beta_i = 0$, then $v(\alpha_i) \leqslant v(\beta_i) = \infty$, in which case $r_i = \alpha_i$. It follows that none of the r_i's are zero. Let $\alpha_i' = \alpha_i/r_i$ and $\beta_i' = \beta_i/r_i$. Then $v(\alpha_i'), v(\beta_i') \geqslant 0$ and

$$\begin{aligned}F(x, y) &= \prod_{i=1}^{n}(r_i\alpha_i' x - r_i\beta_i' y). \\ &= r_1 r_2 \cdots r_n \prod_{i=1}^{n}(\alpha_i' x - \beta_i' y).\end{aligned}$$

Let $G(x, y) = \prod_{i=1}^{n}(\alpha_i' x - \beta_i' y)$ so that $F(x, y) = r_1 r_2 \cdots r_n G(x, y)$. Note that $G(x, y)$ has coefficients in $\mathcal{O}_K$. By how we defined r_i, we see that for each i, either $\alpha_i' = 1$ or $\beta_i' = 1$. It follows that if $\mathcal{F}$ is the residue field, then each monomial $\alpha_i' x - \beta_i' y$ is nonzero in $\mathcal{F}[x, y]$, hence G is nonzero in $\mathcal{F}[x, y]$. Then G has a coefficient that is a unit, say u. Since the coefficients of F are in $\mathcal{O}_K$, we see that $r_1 r_2 \cdots r_n u \in \mathcal{O}_K$. Because u is a unit, we get $r_1 r_2 \cdots r_n \in \mathcal{O}_K$. Since

$$\Delta(Q_1, Q_2) = \text{disc}(F) = (r_1 \cdots r_n)^{2(n-1)} \prod_{i<j}(\alpha_j'\beta_i' - \alpha_i'\beta_j')^2,$$

we conclude that $\Delta(Q_1, Q_2) \in \mathcal{O}_K$.

□

D.2.1 Over an Integral Domain

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

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

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

If $P(X,Y)$ is not identically zero, then

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

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

By unique factorization in $F[X,Y]$, the linear factors $\lambda_i X - \mu_i Y$ are uniquely determined up to multiplication by nonzero elements in F.

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

$$\mathscr{I}(f,g) = \prod_{1 \leqslant i < j \leqslant n} (\lambda_i \mu_j - \lambda_j \mu_i)^2. \tag{D.2.1}$$

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 $c_i \in F$ is nonzero, $1 \leqslant i \leqslant n$, and $\prod_{i=1}^{n} c_i = 1$. Then

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

Remark: Note that by definition $D.1.1$, we have

$$\mathscr{I}(f,g) = \operatorname{disc}(\det(Xf - Yg)).$$

Theorem D.2.5. *Let $f, g \in F[X_1, \ldots, X_n]$ 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* $f, g \in R[X_1, \ldots, X_n]$*, then* $\mathscr{I}(f, g) \in R$.

3. $\mathscr{I}(f, g)$ *is a polynomial over* $\mathbb{Z}$ *in the coefficients of* f *and* g.

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

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

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

Let $a, b, c, d \in F$. We now show that

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

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

This gives

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

(2) Since $f, g \in R[X_1, \ldots, X_n]$, we have $P(X, Y) \in R[X, Y]$. By Theorem $D.1.3$, $\mathscr{I}(f, g) = \mathrm{disc}(\det(P(X, Y)) \in R$.

(3) Suppose that $f = \sum_{1\leqslant i\leqslant j\leqslant n} t_{ij}X_iX_j$ and $g = \sum_{1\leqslant i\leqslant j\leqslant n} t'_{ij}X_iX_j$ where $\{t_{ij}\}$ and $\{t'_{ij}\}$ are variables over $\mathbb{Z}$ (algebraically independent over $\mathbb{Q}$). Let $R = \mathbb{Z}[\{t_{ij}, t'_{ij}\}]$. By (2), $\mathscr{I}(f, g) \in R = \mathbb{Z}[\{t_{ij}, t'_{ij}\}]$, which proves (3). □

Appendix E: Complete Discretely Valued Fields

Lemma E.0.1. *Let R be a commutative ring and let $M = R^n$ be the free R-module of rank n. Let $f : M \to R$ be a quadratic map with associated symmetric R-bilinear form $B_f : M \times M \to R$ given by $B_f(v,w) = f(v+w) - f(v) - f(w)$. Let $\{e_1, \dots, e_n\}$ be a free R-basis of M. Let $A = (a_{ij}) \in \mathcal{M}_{n\times n}(R)$ be the matrix given by*

$$a_{ij} = \begin{cases} f(e_i) & \text{if } i = j \\ B_f(e_i, e_j) & \text{if } i < j \\ 0 & i > j. \end{cases}$$

The following statements hold.

1. *$f(v) = v^t A v$ for all $v \in R^n$.*
2. *$B_f(v,w) = w^t(A + A^t)v$ for all $v, w \in R^n$.*

Proof. Let $v = \sum_{i=1}^n c_i e_i \in M$ where each $c_i \in R$. Then

$$\begin{aligned} v^t A v &= \sum_{i=1}^n \sum_{j=1}^n a_{ij} c_i c_j = \sum_{i=1}^n f(e_i) c_i^2 + \sum_{1 \leqslant i < j \leqslant n} B_f(e_i, e_j) c_i c_j \\ &= f(c_1 e_1 + \cdots + c_n e_n) = f(v). \end{aligned}$$

Let $v, w \in R^n$. Then

$$\begin{aligned} B_f(v,w) &= f(v+w) - f(v) - f(w) \\ &= (v+w)^t A (v+w) - v^t A v - w^t A w \\ &= w^t A v + v^t A w = w^t A v + (v^t A w)^t = w^t A v + w^t A^t v \\ &= w^t (A + A^t) v. \end{aligned}$$

□

The rank of a quadratic map f is defined to be the rank of B_f. Thus the rank of f is the rank of the symmetric $n \times n$ matrix $A + A^t$.

Let $v : K \to \mathbb{Z} \cup \{\infty\}$ be a nontrivial valuation. We shall assume that v is surjective. Let R be the ring of integers of (K, v). Thus $R = \{a \in K \mid v(a) \geqslant 0\}$. Let $\mathfrak{m}$ be the unique maximal ideal of R. Thus $\mathfrak{m} = \{a \in R \mid v(a) > 0\}$. Let k be the residue field of (K, v). Thus $k = R/\mathfrak{m}$. Note that K is the fraction field of R.

We shall assume that K is complete with respect to this discrete valuation. We abbreviate this information by saying that $(K, v, R, \mathfrak{m}, k)$ is a complete discretely valued field.

For $f, g \in R[x_1, \ldots, x_n]$, we write $f \equiv g \bmod \mathfrak{m}^N$ to mean

$$f \equiv g \bmod \mathfrak{m}^N R[x_1, \ldots, x_n].$$

Proposition E.0.2. *Let $(K, v, R, \mathfrak{m}, k)$ be a complete discretely valued field. Let $f \in R[x_1, \ldots, x_n]$ be a quadratic form of rank n over K.*

There exists $N \in \mathbb{Z}_{>0}$ that depends on f so that if $g \in R[x_1, \ldots, x_n]$ is a quadratic form satisfying $f \equiv g \bmod \mathfrak{m}^N$, then g has rank n over K and f is equivalent to g over R; that is, there exists $C \in \mathcal{M}_{n\times n}(R)$ such that C is invertible over R and $f(Cx) = g(x)$.

Proof. Lemma E.0.1 implies that there exists $A \in \mathcal{M}_{n\times n}(R)$ such that $f(x) = x^t Ax$. Since f has rank n, it follows that $A + A^t$ has rank n and thus $A + A^t$ is an invertible matrix over K.

Let $(A + A^t)^{-1} = (b_{ij})$, $b_{ij} \in K$. Let $v(\det(A + A^t)) = M$. Then $M \in \mathbb{Z}_{\geqslant 0}$. Since

$$\mathrm{Adj}(A + A^t)(A + A^t) = \det(A + A^t)I_n,$$

it follows that

$$(A + A^t)^{-1} = \det(A + A^t)^{-1}\mathrm{Adj}(A + A^t).$$

Therefore $v(b_{ij}) \geqslant -M$ for each entry b_{ij}.

Let $N = 2M + 1$. We assume that $g \equiv f \bmod \mathfrak{m}^N$. Let $C_0 = I_n$. Then $f(C_0(x)) = f(x) \equiv g(x) \bmod \mathfrak{m}^N$.

Suppose $i \geqslant 1$ and we have found by induction $C_{i-1} \in \mathcal{M}_{n\times n}(R)$ such that C_{i-1} is invertible over R and $g(x) \equiv f(C_{i-1}x) \bmod \mathfrak{m}^{N+i-1}$.

Lemma E.0.1 implies that $g(x) - f(C_{i-1}x) = x^t Dx$ for some $D \in \mathcal{M}_{n\times n}(\mathfrak{m}^{N+i-1}R)$. Let

$$T_i = (A + A^t)^{-1}(C_{i-1}^t)^{-1}D \in \mathcal{M}_{n\times n}(\mathfrak{m}^{N-M+i-1}R) = \mathcal{M}_{n\times n}(\mathfrak{m}^{M+i}R).$$

Since $f(T_i x) \in \mathfrak{m}^{2M+2i}R[x_1, \ldots, x_n]$ and $2M + 2i \geqslant N + i$, the definition of T_i implies that

$$\begin{aligned} f((C_{i-1} + T_i)x) &= f(C_{i-1}x + T_i x) \\ &= f(C_{i-1}x) + f(T_i x) + x^t C_{i-1}^t (A + A^t)T_i x \\ &\equiv f(C_{i-1}x) + x^t C_{i-1}^t (A + A^t)T_i x \\ &= f(C_{i-1}x) + x^t Dx = g(x) \bmod \mathfrak{m}^{N+i}. \end{aligned}$$

Let $C_i = C_{i-1} + T_i$. Then $g(x) \equiv f(C_i x) \bmod \mathfrak{m}^{N+i}$ and we have $C_i \equiv C_{i-1} \bmod \mathfrak{m}^{M+i}R$.

The matrix C_i is invertible over R because $C_i \equiv C_0 = I_n \bmod \mathfrak{m}$ and thus $\det C_i$ is a unit in R.

Since $C_i \equiv C_{i-1} \bmod \mathfrak{m}^{M+i}R$, each entry in $\{C_i\}_{i=0}^{\infty}$ is a Cauchy sequence. Thus $C = \lim_{i\to\infty} C_i$ exists because R is complete. It follows that $C \in M_n(R)$. Since

$C \equiv C_0 = I_n \bmod \mathfrak{m}$, we have $\det(C) \equiv 1 \bmod \mathfrak{m}$, and so $\det(C)$ is a unit in R. It follows that C is invertible over R.

Since $g(x) \equiv f(C_i x) \bmod \mathfrak{m}^{N+i}$ for every $i \geqslant 0$, it follows that

$$g(x) = \lim_{i\to\infty} f(C_i x) = f(\lim_{i\to\infty} C_i x) = f((\lim_{i\to\infty} C_i)x) = f(Cx).$$

Therefore f and g are equivalent over R.

To show that g has rank n over K, note that since $g(x) = f(Cx)$, we have

$$g(v) = f(Cv) = (Cv)^t A(Cv) = v^t(C^t AC)v$$

for all $v \in K^n$. Therefore, the rank of g is the rank of the matrix

$$(C^t AC) + (C^t AC)^t = C^t AC + C^t A^t C = C^t(A + A^t)C.$$

Since $A + A^t$ has rank n and C is invertible, we conclude that $C^t(A + A^t)C$ has rank n. □

Appendix F: Artin-Schreier Subgroup

F.1 Arf Invariant

We begin with a general concept that holds over fields k with $\mathrm{char}(k) = p > 0$.

Let k be a field with char $k = p > 0$. Let $\wp(k) = \{a^p - a \mid a \in k\}$. Then $\wp(k)$ is an additive subgroup of k because $(a^p - a) + (b^p - b) = (a + b)^p - (a + b)$ and $-(a^p - a) = (-a)^p - (-a)$.$\wp(k)$ is called the Artin-Schreier subgroup of k.

Lemma F.1.1. *If k is a finite field with char$(k) = p$, then $[k : \wp(k)] = p$.*

Proof. Let $\theta : (k, +) \to (k, +)$ be defined by $\theta(a) = a^p - a$. Then θ is an additive homomorphism because the calculation above shows that $\theta(a + b) = \theta(a) + \theta(b)$. It follows that $\mathrm{im}(\theta) = \wp(k)$. We have $\ker(\theta) = \mathbb{F}_p$ because $a^p - a = 0$ if and only if $a^p = a$, which holds if and only if $a \in \mathbb{F}_p \subseteq k$. Thus $|\ker(\theta)| = p$, and so $p = |\ker(\theta)| = \frac{|k|}{|\mathrm{im}(\theta)|}$. This gives $[k : \wp(k)] = p$. □

Lemma F.1.2. *Let k be a field with char $k = 2$.*

1. *If $t \in k$, the quadratic form $x^2 + xy + ty^2$ is isotropic over k if and only if $t \in \wp(k)$.*

2. *If $r + \wp(k) = s + \wp(k)$, where $r, s \in k$, then the quadratic forms $x^2 + xy + ry^2$ and $x^2 + xy + sy^2$ are equivalent over k.*

3. *If k is a finite field with char $k = 2$, then the quadratic forms $x^2 + xy + ry^2$ and $x^2 + xy + sy^2$ are equivalent over k if and only if $r + \wp(k) = s + \wp(k)$, where $r, s \in k$.*

Proof. We first prove (1). Suppose that $x^2 + xy + ty^2$ is isotropic over k. Then there exists $a, b \in k$, not both zero, such that $a^2 + ab + tb^2 = 0$. If $b = 0$, then $a = 0$, which is excluded. Thus $b \neq 0$. Then $\left(\frac{a}{b}\right)^2 + \frac{a}{b} + t = 0$, which implies that $t \in \wp(k)$ because char $k = 2$. Now suppose that $t \in \wp(k)$. Then $t = c^2 - c$ for some $c \in k$. Then $c^2 + c \cdot 1 + t \cdot 1^2 = 0$, which implies that $x^2 + xy + ty^2$ is isotropic over k.

Next, we prove (2). Let $s = r + c^2 - c$ where $c \in k$. Then $(x + cy)^2 + (x + cy)y + ry^2 = x^2 + xy + (r + c^2 + c)\, y^2 = x^2 + xy + sy^2$.

To prove (3), suppose that k is finite and $x^2 + xy + ry^2$ and $x^2 + xy + sy^2$ are equivalent over k. Then either both are isotropic over k or both are anisotropic over

k. By Lemma $F.1.1$, we have $k = \wp(k) \cup (t + \wp(k)$ for some $t \in k, t \notin \wp(k)$. Then by (1), either $r, s \in \wp(k)$ or $r, s \in t + \wp(k)$. In both cases, we have $r + \wp(k) = s + \wp(k)$. □

Proposition F.1.3. *Let k be a field with char$(k) = 2$. Let $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in k, b \neq 0$.*

1. *Then f is equivalent over k to $a'x^2 + xy + c'y^2$ for some $a', c' \in k$.*
2. *If k is perfect, then f is equivalent over k to $x^2 + xy + \frac{ac}{b^2}y^2$.*

Proof. To prove (1), observe that $ax^2 + bxy + cy^2 = ax^2 + x(by) + \frac{c}{b^2}(by)^2$. Thus we may take $a' = a$ and $b' = \frac{c}{b^2}$

As for (2), since $f \neq 0$, an invertible linear change of variables lets us assume that $f(1, 0) \neq 0$. Thus we can assume that $a \neq 0$. If k is perfect, then $k = k^2$, so $\sqrt{a} \in k$. Then

$$ax^2 + bxy + cy^2 = (\sqrt{a}x)^2 + (\sqrt{a}x)\left(\frac{b}{\sqrt{a}}y\right) + \frac{ac}{b^2}\left(\frac{b}{\sqrt{a}}y\right)^2.$$

□

Corollary F.1.4. *Let k be a finite field with char$(k) = 2$. Then there is a unique, up to equivalence, anisotropic binary quadratic form of rank 2 of the shape $ax^2+bxy+cy^2$ with $b \neq 0$.*

Proof. By Proposition $F.1.3$, any anisotropic binary quadratic form over k is equivalent to one of the form $x^2 + xy + ry^2$. By Lemma $F.1.2$, any two such anisotropic binary quadratic forms over k are equivalent. Note that $\det(x^2 + xy + ry^2) = -1 \neq 0$, hence $x^2 + xy + ry^2$ has rank 2. □

Definition F.1.5. *If $b \neq 0$, the Arf invariant of $ax^2+bxy+cy^2$ is defined by* $\mathrm{Arf}(f) = \frac{ac}{b^2} + \wp(k)$. *The Arf invariant is not defined if $b = 0$.*

It is not easy to show that the Arf invariant is an invariant. Lemma $F.1.2$ gives an argument for the case of a finite field.

Proposition F.1.6. *Let k be a field with char$(k) = 2$. Let*

$$f(x, y) = ax^2 + bxy + cy^2$$

where $a, b, c \in k, b \neq 0$, and let

$$g(x, y) = f(mx + ny, px + qy) = Ax^2 + Bxy + Cy^2$$

where $m, n, p, q \in k$ and $mq - np \neq 0$. Then $B \neq 0$ and

$$\frac{AC}{B^2} = \frac{ac}{b^2} + \left(\frac{amn + bmq + cpq}{b(mq + np)}\right)^2 + \frac{amn + bmq + cpq}{b(mq + np)} \in \frac{ac}{b^2} + \wp(k).$$

The proof is by a brute force calculation. We have

Proof.

$$A = am^2 + bmp + cp^2,$$
$$B = b(mq + np),$$
$$C = an^2 + bnq + cq^2.$$

One shows directly that

$$\begin{aligned}\left(am^2 + bmp + cp^2\right)&\left(an^2 + bnq + cq^2\right)\\ =&ac(mq + np)^2 + (amn + bmq + cpq)^2\\ &+ b(mq + np)(amn + bmq + cpq)\end{aligned}$$

□

Corollary F.1.7. *Let k be a field with char $k = 2$. The Arf invariant of a binary quadratic form is an invariant. That is, if $m, n, p, q \in k$ and $mq - np \neq 0$, then*

$$\begin{aligned}\operatorname{Arf}&\left(ax^2 + bxy + cy^2\right)\\ &= \operatorname{Arf}\left(a(mx + ny)^2 + b(mx + ny)(px + qy) + c(px + qy)^2\right).\end{aligned}$$

F.2 Applications

Let K be a field with $\operatorname{char}(K) = 2$ and let L be a finite extension of K. Let $\wp(K)$ and $\wp(L)$ denote the Artin-Schreier subgroups. Thus $\wp(K) = \{a^2 + a \mid a \in K\}$ and similarly for L. Then $\wp(K)$ is an additive subgroup of K and similarly for L. Then the (additive) quotient group $K/\wp(K)$ is defined.

Let $\operatorname{tr} : L \to K$ denote the trace map. From here on, assume that K is a finite field with $|K| = q$. Let $[L : K] = n$. Then $|L| = q^n$. Note that $a^{q^n} = a$ for all $a \in L$.

Lemma F.2.1. *Let $b \in L$. Then $b \in \wp(L)$ if and only if $tr(b) \in \wp(K)$.*

Proof. If $a \in L$, then $\operatorname{tr}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{n-1}}$. Since $(\operatorname{tr}(a))^q = \operatorname{tr}(a)$, it follows that $\operatorname{tr}(a) \in K$.

It is easy to check that $\operatorname{tr} : L \to K$ is an additive homomorphism. We have $|\ker(\operatorname{tr})| \leqslant q^{n-1}$ because a polynomial of degree q^{n-1} has at most q^{n-1} roots. Further, we have $|\operatorname{im}(\operatorname{tr})| \leqslant q$ because $|K| = q$. By the first isomorphism theorem, $L/\ker(\operatorname{tr}) \cong \operatorname{im}(\operatorname{tr})$. It follows that

$$|\ker(\operatorname{tr})| \cdot |\operatorname{im}(\operatorname{tr})| = |L| = q^n.$$

Therefore, $|\ker(\operatorname{tr})| = q^{n-1}$ and $|\operatorname{im}(\operatorname{tr})| = q$. This shows that tr is a surjective additive homomorphism.

Next, we will show that $|\wp(L)| = q^n/2$ and $|\wp(K)| = q/2$. The map $K \to K$ given by $x \mapsto x^2 + x$ is an additive homomorphism because $\operatorname{char}(K) = 2$. Note that the image of this map is $\wp(K)$. The kernel has order 2 because $x^2 + x = 0$ if and only if $x = 0$ or $x = 1$. Thus, the image has order $q/2$. Likewise, the map $L \to L$ given by $x \mapsto x^2 + x$ is an additive homomorphism such that the kernal has order 2 and the image, $\wp(L)$, has order $q^n/2$.

The next step is to prove that $\mathrm{tr}(\wp(L)) \subset \wp(K)$. We begin by showing that $\mathrm{tr}(a^2) = (\mathrm{tr}(a))^2$. Note that since $\mathrm{char}(L) = 2$, it follows that q is a power of 2. Observe that

$$\begin{aligned}(\mathrm{tr}(a))^2 &= (a + a^q + \cdots + a^{q^{n-1}})^2. \\ &= a^2 + a^{2q} + \cdots + a^{2(q^{n-1})}. \\ &= a^2 + (a^2)^q + \cdots + (a^2)^{q^{n-1}}. \\ &= \mathrm{tr}(a^2).\end{aligned}$$

The containment $\mathrm{tr}(\wp(L)) \subset \wp(K)$ follows from the equations

$$\mathrm{tr}(a^2 + a) = \mathrm{tr}(a^2) + \mathrm{tr}(a) = (\mathrm{tr}(a))^2 + \mathrm{tr}(a) \in \wp(K).$$

Because $\mathrm{tr} : L \to K$ is a surjective homomorphism, and the projection $K \to K/\wp(K)$ is a surjective homomorphism, it follows that the composition $L \to K \to K/\wp(K)$ is a surjective homomorphism from L to $K/\wp(K)$. This induces a surjective homomorphism $L/\wp(L) \to K/\wp(K)$. Since this map is surjective, and $|L/\wp(L)| = |K/\wp(K)| = 2$, it must also be injective. In particular, if $b \in L$, then $b \in \wp(L)$ if and only if $\mathrm{tr}(b) \in \wp(K)$.

□

Bibliography

[1] M. Amer. Quadratische formen über funktionenkörpern. unpublished dissertation, Johannes Gutenberg Universität, Mainz, 1976.

[2] J. K. Arason. Cohomologische invarianten quadratischer formen. *Journal of Algebra*, 36(3):448–491, 1975.

[3] R. Baeza. Discriminants of polynomials and of quadratic forms. *J. Algebra*, 72(1):17–28, 1981.

[4] B. Birch, D. J. Lewis, and T. Murphy. Simultaneous quadratic forms. *Amer. J. Math.*, 84:110–115, 1962.

[5] L. Chakri and D. B. Leep. Nonsingular zeros of polynomials defined over p-adic fields. *Communications in Algebra*, 39(1):1–4, 2010.

[6] D. Dummit and R. Foote. *Abstract Algebra.* John Wiley and Sons, New Jersey, 3rd edition, 2004.

[7] D. R. Heath-Brown. Zeros of pairs of quadratic forms. *J.reine angew. Math.*, 739:41–80, 2018.

[8] D. R. Heath-Brown and L. B. Pierce. Simultaneous integer values of pairs of quadratic forms. *J.reine angew. Math.*, 2015. DOI 10.151/crelle-2014-0112.

[9] T. Y. Lam. *Introduction to Quadratic Forms over Fields*, volume 67. The American Mathematical Society, Rhode Island, 2005.

[10] S. Lang. *Algebra.* Springer, New York, 3rd edition, 2002.

[11] D. Leep. The Amer-Brumer theorem over arbitrary fields. preprint.

[12] D. Leep. The u-invariant of p-adic function fields. *J. Reine Angew. Math*, 679:65–73, 2013.

[13] D. Leep and L. Schueller. Zeros of a pair of quadratic forms defined over a finite field. *Finite Fields and their Applications*, 5(2):157–176, 1999.

[14] D. B. Leep and N. Sahajpal. Pairs of quadratic forms over the real numbers. *Bulletin of the Irish Mathematical Society*, 91:49–72, 2023.

[15] D. B. Leep and L. M. Schueller. A characterization of nonsingular pairs of quadratic forms. *J. Algebra Appl.*, 1:391–412, 2002.

[16] R. Parimala and V. Suresh. The u-invariant of the function fields of p-adic curves. *Ann. of Math*, 172(2):1391–1405, 2010.

[17] W. Scharlau. *Quadratic and Hermitian Forms*, volume 270 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1985.

[18] W. M. Schmidt. *Equations over Finite Fields An Elementary Approach*, volume 536 of *Lecture Notes in Mathematics*. Springer-Verlag Berlin, 1976.

[19] A. R. Wadsworth. Discriminants in characteristic two. *Linear and Multilinear Algebra*, 17(3-4):235–263, 1985.

Vita

John R. Hall

Place of Birth:

Norton, VA

Education:

Appalachian State University, Boone, NC
M.A. in Mathematics, May 2016

University of Virginia's College at Wise, Wise, VA
B.S. in Mathematics, May 2012

Professional Positions:

Graduate Teaching Assistant, University of Kentucky, Fall 2018–Spring 2024

Graduate Teaching Assistant, Appalachian State University, Fall 2016 – Spring 2018

Honors

Enoch Scholarship in Algebra, Fall 2023

Webb Summer Research Award, Summer 2023

Publications:

Leibniz algebras with low dimensional maximal Lie quotients
with W. Cook, V. Klima, C. Murray
Involve, a Journal of Mathematics 12-5 (2019), 839-853
DOI 10.2140/involve.2019.12.839