Canonical matrices of forms and pairs of forms over finite and $\mathfrak{p}$-adic fields

Vladimir V. Sergeichuk
Institute of Mathematics,
Tereshchenkivska 3, Kiev, Ukraine,
sergeich@imath.kiev.ua

Abstract

Canonical matrices of

(a) bilinear and sesquilinear forms,

(b) pairs of forms, in which every form is symmetric or skew-symmetric, and

(c) pairs of Hermitian forms

are given over finite fields of characteristic $\neq 2$ and over $\mathfrak{p}$-adic fields (i.e., finite extensions of the field $\mathbb{Q}_p$ of p-adic numbers) with $p \neq 2$.

These canonical matrices are special cases of the canonical matrices of (a)–(c) over a field of characteristic not 2 that were obtained by the author [*Math. USSR–Izv.* 31 (1988) 481–501] up to classification of quadratic or Hermitian forms over its finite extensions; we use the known classification of quadratic and Hermitian forms over finite fields and $\mathfrak{p}$-adic fields.

AMS classification: 15A21.

Keywords: Bilinear forms, Sesquilinear forms, Congruence, Canonical matrices, Finite fields, Local fields, Fields of p-adic numbers.

1 Introduction

We give canonical matrices of

(a) bilinear and sesquilinear forms,

(b) pairs of forms in which every form is symmetric or skew-symmetric, and

(c) pairs of Hermitian forms

over

(i) finite fields of characteristic different from 2, and

(ii) $\mathfrak{p}$-adic fields (i.e., finite extensions of the field $\mathbb{Q}_p$ of p-adic numbers); for simplicity, we take $p \neq 2$.

Our canonical matrices are special cases of the canonical matrices of (a)–(c) over a field $\mathbb{F}$ of characteristic not 2 that were obtained in [15] up to classification of quadratic or Hermitian forms over finite extensions of $\mathbb{F}$. We use the known classification of quadratic and Hermitian forms over finite extensions of (i) and (ii).

Analogous canonical matrices of (a)–(c) could be obtained over any local field (which is either a $\mathfrak{p}$-adic field or the field of formal power series of one variable over a finite field) since the classification of quadratic and Hermitian forms over local fields is known.

In Section 2 we recall canonical forms of (a)–(c) obtained in [15]. In Sections 3 and 4 we give canonical forms of (a)–(c) over (i) and (ii).

2 Canonical matrices over any field of characteristic not 2

In this section $\mathbb{F}$ denotes a field of characteristic different from 2 with a fixed involution $\mathbb{F} \to \mathbb{F}$; that is, a bijection $a \mapsto \bar{a}$ satisfying

$$\overline{a+b} = \bar{a} + \bar{b}, \quad \overline{ab} = \bar{a}\bar{b}, \quad \bar{\bar{a}} = a \qquad \text{for all } a, b \in \mathbb{F}.$$

We recall canonical forms of (a)–(c) obtained in [15] by the method that was developed by Roiter and the author in [11, 14, 15]; it reduces the problem of classifying systems of forms and linear mappings over $\mathbb{F}$ to the problems of classifying

- systems of linear mappings over $\mathbb{F}$, and

- quadratic and Hermitian forms over skew fields that are finite extensions of $\mathbb{F}$.

This method was applied to the problem of classifying bilinear and sesquilinear forms in [6, 7, 8] and to the problem of classifying isometric operators on vector spaces with scalar product given by a nonsingular quadratic or Hermitian form in [16].

For any matrix $A = [a_{ij}]$ over $\mathbb{F}$, we write $A^* := \bar{A}^T = [\bar{a}_{ji}]$. Square matrices A and B are said to be *similar* if $S^{-1}AS = B$, *congruent* if $S^TAS = B$, and **congruent* if $S^*AS = B$ for a nonsingular S. Pairs of matrices (A_1, A_2) and (B_1, B_2) are *congruent* if $S^TA_1S = B_1$ and $S^TA_2S = B_2$; they are **congruent* if $S^*A_1S = B_1$ and $S^*A_2S = B_2$ for a nonsingular S. The transformations of congruence ($A \mapsto S^TAS$) and *congruence ($A \mapsto S^*AS$) are associated with the bilinear form x^TAy and the sesquilinear form x^*Ay, respectively.

The involution on $\mathbb{F}$ can be the identity. Thus, we consider congruence as a special case of *congruence.

Every square matrix A over $\mathbb{F}$ is similar to a direct sum, uniquely determined up to permutation of summands, of *Frobenius blocks*

$$\Phi = \begin{bmatrix} 0 & & 0 & -c_m \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -c_2 \\ 0 & & 1 & -c_1 \end{bmatrix}, \qquad (1)$$

whose characteristic polynomial

$$\chi_\Phi(x) = p_\Phi(x)^l = x^m + c_1x^{m-1} + \cdots + c_m$$

is an integer power of a polynomial $p_\Phi(x)$ that is irreducible over $\mathbb{F}$; this direct sum is called the *Frobenius canonical form* or the *rational canonical form* of A, see [2, Section 6]. If $\chi_\Phi(x) = (x - \lambda)^m$, then Φ is similar to the Jordan block

$$J_m(\lambda) := \begin{bmatrix} \lambda & & & 0 \\ 1 & \lambda & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{bmatrix} \qquad (m\text{-by-}m). \qquad (2)$$

For each polynomial

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}[x],$$

we define the polynomials

$$\bar{f}(x) := \bar{a}_0x^n + \bar{a}_1x^{n-1} + \cdots + \bar{a}_n, \tag{3}$$
$$f^\vee(x) := \bar{a}_n^{-1}(\bar{a}_nx^n + \cdots + \bar{a}_1x + \bar{a}_0) \quad \text{if } a_n \neq 0. \tag{4}$$

In particular,

$$f^\vee(x) = a_n^{-1}(a_nx^n + \cdots + a_1x + a_0) \tag{5}$$

if the involution on $\mathbb{F}$ is the identity.

The following lemma was proved in [15, Lemma 6] (or see [8, 16]).

Lemma 2.1. *Let $\mathbb{F}$ be a field with involution $a \mapsto \bar{a}$, let $p(x) = p^\vee(x)$ be an irreducible polynomial over $\mathbb{F}$, and consider the field*

$$\mathbb{F}(\kappa) = \mathbb{F}[x]/p(x)\mathbb{F}[x], \qquad \kappa := x + p(x)\mathbb{F}[x], \tag{6}$$

with involution

$$f(\kappa)^\circ := \bar{f}(\kappa^{-1}). \tag{7}$$

Then each element of $\mathbb{F}(\kappa)$ on which the involution acts identically is uniquely representable in the form $q(\kappa)$, in which

$$q(x) = a_rx^r + \cdots + a_1x + a_0 + \bar{a}_1x^{-1} + \cdots + \bar{a}_rx^{-r}, \quad a_0 = \bar{a}_0, \tag{8}$$

r is the integer part of $(\deg p(x))/2$, $a_0, \dots, a_r \in \mathbb{F}$, and if $\deg p(x)$ is even then

$$a_r = \begin{cases} 0 & \text{if the involution on } \mathbb{F} \text{ is the identity,} \\ \bar{a}_r & \text{if the involution on } \mathbb{F} \text{ is not the identity and } p(0) \neq 1, \\ -\bar{a}_r & \text{if the involution on } \mathbb{F} \text{ is not the identity and } p(0) = 1. \end{cases}$$

For each square matrix Φ and

$$\varepsilon = \begin{cases} 1 \text{ or } -1, & \text{if the involution on } \mathbb{F} \text{ is the identity,} \\ 1, & \text{if the involution on } \mathbb{F} \text{ is nonidentity,} \end{cases}$$

denote by $\sqrt[*]{\Phi}$ and Φ_ε fixed nonsingular matrices (if they exist) such that

$$\sqrt[*]{\Phi} = (\sqrt[*]{\Phi})^*\Phi, \tag{9}$$

$$\Phi_\varepsilon = \Phi_\varepsilon^*, \qquad \Phi_\varepsilon\Phi = \varepsilon(\Phi_\varepsilon\Phi)^*. \tag{10}$$

We use the notation $\sqrt[*]{\Phi}$ both in the case of nonidentity involution and in the case of the identity involution on $\mathbb{F}$, but if we know that the involution is the identity then we prefer to write $\sqrt[T]{\Phi}$ instead of $\sqrt[*]{\Phi}$.

It suffices to construct $\sqrt[*]{\Phi}$ and Φ_ε for canonical matrices Φ under similarity since if $\Psi = S^{-1}\Phi S$ then we can take

$$\sqrt[*]{\Psi} = S^* \sqrt[*]{\Phi} S, \qquad \Psi_\varepsilon = S^*\Phi_\varepsilon S.$$

Existence conditions and explicit forms of $\sqrt[*]{\Phi}$ and Φ_ε for all Frobenius blocks Φ will be given in Lemmas 2.6 and 2.7.

Define the *skew sum* of two matrices

$$[A \diagdown B] := \begin{bmatrix} 0 & B \\ A & 0 \end{bmatrix}.$$

Theorem 2.2 ([15, Theorem 3]; see also [8, Theorem 2.2])**.** (a) *Let $\mathbb{F}$ be a field of characteristic different from 2 with involution (which can be the identity). Every square matrix A over $\mathbb{F}$ is *congruent to a direct sum of matrices of the following types:*

(i) $J_n(0)$*;*

(ii) $[\Phi \diagdown I_n]$*, where Φ is an $n \times n$ nonsingular Frobenius block such that $\sqrt[*]{\Phi}$ does not exist (see Lemma 2.6); and*

(iii) $\sqrt[*]{\Phi}q(\Phi)$*, where Φ is a nonsingular Frobenius block such that $\sqrt[*]{\Phi}$ exists and $q(x) \neq 0$ has the form (8) from Lemma 2.1 in which $p(x) = p_\Phi(x)$ is the irreducible divisor of the characteristic polynomial of Φ.*

(b) *The summands are determined to the following extent:*

Type (i) *uniquely.*

Type (ii) *up to replacement of Φ by the Frobenius block Ψ that is similar to Φ^{-*} (i.e., whose characteristic polynomial is $\chi_\Phi^\vee(x)$, see (4)).*

Type (iii) *up to replacement of the whole group of summands*

$$\sqrt[*]{\Phi}q_1(\Phi) \oplus \cdots \oplus \sqrt[*]{\Phi}q_s(\Phi)$$

with the same Φ *by*

$$\sqrt[*]{\Phi}q'_1(\Phi) \oplus \cdots \oplus \sqrt[*]{\Phi}q'_s(\Phi)$$

in which each $q'_i(x)$ *is a nonzero function of the form* (8) *and the Hermitian forms*

$$\begin{gathered} q_1(\kappa)x_1^\circ y_1 + \cdots + q_s(\kappa)x_s^\circ y_s, \\ q'_1(\kappa)x_1^\circ y_1 + \cdots + q'_s(\kappa)x_s^\circ y_s \end{gathered}$$

are equivalent over the field (6) *with involution* (7).

(c) *Frobenius blocks in* (a) *and* (b) *can be replaced by arbitrary matrices that are similar to them* (*for example, by Jordan blocks if* $\mathbb{F}$ *is algebraically closed*).

Define the $(n-1)\times n$ matrices

$$F_n := \begin{bmatrix} 1 & 0 & & 0 \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{bmatrix}, \quad G_n := \begin{bmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & 0 & 1 \end{bmatrix} \tag{11}$$

for each $n = 1, 2, \dots$, and define the *direct sum* of two matrix pairs:

$$(A_1, B_1) \oplus (A_2, B_2) := (A_1 \oplus A_2,\ B_1 \oplus B_2).$$

Theorem 2.3 ([15, Theorem 4])**.** (a) *Let* $\mathbb{F}$ *be a field of characteristic different from* 2 *with involution* (*which can be the identity*)*. Let* A *and* B *be* ε*-Hermitian and* δ*-Hermitian matrices over* $\mathbb{F}$ *of the same size:*

$$A^* = \varepsilon A, \qquad B^* = \delta B,$$

in which

$$(\varepsilon, \delta) = \begin{cases} (1,1), & \textit{if the involution on } \mathbb{F} \textit{ is nonidentity,} \\ (1,1) \textit{ or } (1,-1) \textit{ or } (-1,-1), & \textit{otherwise.} \end{cases}$$

Then (A, B) *is *congruent to a direct sum of matrix pairs of the following types:*

(i) $([F_n \diagdown \varepsilon F_n^*],\ [G_n \diagdown \delta G_n^*])$, *in which* F_n *and* G_n *are defined in* (11)*;*

(ii) $([I_n \diagdown \varepsilon I_n],\ [\Phi \diagdown \delta\Phi^*])$, *in which* Φ *is an* $n \times n$ *Frobenius block such that* Φ_δ *(see* (10)*) does not exist if* $\varepsilon = 1$*;*

(iii) $A_\Phi^{f(x)} := (\Phi_\delta, \Phi_\delta\Phi) f(\Phi)$ *only if* $\varepsilon = 1$, *in which* $0 \neq f(x) = \bar{f}(\delta x) \in \mathbb{F}[x]$ *(see* (3)*), and* $\deg(f(x)) < \deg(p_\Phi(x))$*;*

(iv) $([J_n(0) \diagdown \varepsilon J_n(0)^*], [I_n \diagdown (-I_n)])$ *only if* $\delta = -1$, *in which* n *is odd if* $\varepsilon = 1$*;*

(v)

$$B_n^a := \left(a \begin{bmatrix} 0 & & & & & 1 & 0 \\ & & & & \delta & \cdot & \\ & & & 1 & \cdot & & \\ & & \delta & \cdot & & & \\ & \cdot & \cdot & & & & \\ \cdot & \cdot & & & & & \\ 0 & & & & & & 0 \end{bmatrix},\ a \begin{bmatrix} 0 & & & & & & 1 \\ & & & & & \delta & \\ & & & & 1 & & \\ & & & \delta & & & \\ & & \cdot & & & & \\ & \cdot & & & & & \\ \cdot & & & & & & 0 \end{bmatrix} \right), \tag{12}$$

in which the matrices are n-by-n, $\varepsilon = 1$, $0 \neq a = \bar{a} \in \mathbb{F}$, *and* n *is even if* $\delta = -1$.

(b) *The summands are determined to the following extent:*

Type (i) *uniquely.*

Type (ii) *up to replacement of* Φ *by the Frobenius block* Ψ *with* $\chi_\Psi(x) = (\varepsilon\delta)^{\det \chi_\Phi} \bar{\chi}_\Phi(\varepsilon\delta x)$.

Type (iii) *up to replacement of the whole group of summands*

$$A_\Phi^{f_1(x)} \oplus \cdots \oplus A_\Phi^{f_s(x)}$$

with the same Φ *by*

$$A_\Phi^{g_1(x)} \oplus \cdots \oplus A_\Phi^{g_s(x)}$$

such that the Hermitian forms

$$\begin{aligned} &f_1(\omega)x_1^\circ y_1 + \cdots + f_s(\omega)x_s^\circ y_s, \\ &g_1(\omega)x_1^\circ y_1 + \cdots + g_s(\omega)x_s^\circ y_s \end{aligned}$$

are equivalent over the field $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ *with involution* $f(\omega)^\circ = \bar{f}(\delta\omega)$.

Type (iv) *uniquely.*

Type (v) *up to replacement of the whole group of summands*

$$B_n^{a_1} \oplus \cdots \oplus B_n^{a_s} \tag{13}$$

with the same n by

$$B_n^{b_1} \oplus \cdots \oplus B_n^{b_s} \tag{14}$$

such that the Hermitian forms

$$\begin{gathered} a_1\bar{x}_1y_1 + \cdots + a_s\bar{x}_sy_s, \\ b_1\bar{x}_1y_1 + \cdots + b_s\bar{x}_sy_s \end{gathered}$$

are equivalent over $\mathbb{F}$.

(c) *Frobenius blocks in* (a) *and* (b) *can be replaced by arbitrary matrices that are similar to them* (*for example, by Jordan blocks if $\mathbb{F}$ is algebraically closed*).

Taking $\varepsilon = \delta = -1$ in Theorem 2.3, we obtain the following well-known canonical form of pairs skew-symmetric matrices; see, for example, [12, 17].

Corollary 2.4. *Over any field of characteristic not 2, each pair of skew-symmetric matrices of the same size is congruent to a direct sum, uniquely determined up to permutation of summands, of pairs of the form:*

(i) $([F_n \diagdown -F_n^T], [G_n \diagdown -G_n^T])$, *in which F_n and G_n are defined in* (11)*;*

(ii) $([I_n \diagdown -I_n], [\Phi \diagdown -\Phi^T])$, *in which Φ is an $n \times n$ Frobenius block;*

(iii) $([J_n(0) \diagdown -J_n(0)^T], [I_n \diagdown -I_n])$.

Remark 2.5. If $\delta = -1$ then the matrix pair B_n^a defined in (12) consists of $n \times n$ matrices and n is even. In this case, the pair

$$C_n^a := \left(a\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix},\ a\begin{bmatrix} 0 & & & & & 1 \\ & & & & \iddots & \\ & & & 1 & & \\ & & -1 & & & \\ & \iddots & & & & \\ -1 & & & & & 0 \end{bmatrix} \right) \tag{15}$$

of symmetric and skew-symmetric matrices of size $n\times n$ can be used in (12)–(14) instead of B_n^a. This follows from the proof of Theorem 4 in [15] since the pairs B_n^a and C_n^a are equivalent; that is, $RB_n^aS=C_n^a$ for some nonsingular R and S.

Let

$$f(x)=\gamma_0x^m+\gamma_1x^{m-1}+\dots+\gamma_m\in\mathbb{F}[x],\qquad m\geqslant 1,\ \gamma_0\neq 0\neq\gamma_m.$$

A vector $(a_1,a_2,\dots,a_n)$ over $\mathbb{F}$ is called *f-recurrent* if either $n\leqslant m$, or

$$\gamma_0a_l+\gamma_1a_{l+1}+\dots+\gamma_ma_{l+m}=0\qquad\text{for all } l=1,2,\dots,n-m.$$

Thus, this vector is completely determined by any fragment of length m.

Existence conditions and explicit forms of $\sqrt[*]{\Phi}$ and Φ_ε for Frobenius blocks Φ are given in the following two lemmas.

Lemma 2.6 ([15, Theorem 7]; a detailed proof in [8, Lemma 2.3])**.** *Let $\mathbb{F}$ be a field of characteristic not 2 with involution (possibly, the identity). Let Φ be an $n\times n$ nonsingular Frobenius block whose characteristic polynomial is a power of an irreducible polynomial $p_\Phi(x)$.*

(a) $\sqrt[*]{\Phi}$ *exists if and only if*

$$p_\Phi(x)=p_\Phi^\vee(x)\ \text{(see (4)), and}\tag{16}$$

if the involution on $\mathbb{F}$ is the identity, also $p_\Phi(x)\neq x+(-1)^{n+1}$. (17)

(b) *If* (16) *and* (17) *are satisfied and*

$$\chi_\Phi(x)=x^n+c_1x^{n-1}+\dots+c_n\tag{18}$$

is the characteristic polynomial of Φ, then for $\sqrt[*]{\Phi}$ one can take the Toeplitz matrix

$$\sqrt[*]{\Phi}:=[a_{i-j}]=\begin{bmatrix} a_0 & a_{-1} & \ddots & a_{1-n}\\ a_1 & a_0 & \ddots & \ddots\\ \ddots & \ddots & \ddots & a_{-1}\\ a_{n-1} & \ddots & a_1 & a_0\end{bmatrix},\tag{19}$$

whose vector of entries $(a_{1-n}, a_{2-n}, \dots, a_{n-1})$ *is the* χ_Φ*-recurrent extension of the vector*

$$v = (a_{1-m}, \dots, a_m) = (a, 0, \dots, 0, \bar{a}) \tag{20}$$

of length

$$2m = \begin{cases} n & \text{if } n \text{ is even,} \\ n+1 & \text{if } n \text{ is odd,} \end{cases} \tag{21}$$

in which

$$a := \begin{cases} 1 & \text{if } n \text{ is even, except for the case} \\ & \qquad p_\Phi(x) = x + c \text{ with } c^{n-1} = -1, \\ \chi_\Phi(-1) & \text{if } n \text{ is odd and } p_\Phi(x) \neq x+1, \\ e - \bar{e} & \text{otherwise, with any fixed } \bar{e} \neq e \in \mathbb{F}. \end{cases} \tag{22}$$

Lemma 2.7 ([15, Theorem 8])**.** *Let* $\mathbb{F}$ *be a field of characteristic not* 2 *with involution* (*possibly, the identity*)*. Let* Φ *be an* $n \times n$ *Frobenius block* (1) *over* $\mathbb{F}$*. Existence conditions for the matrix* Φ_ε *are:*

$$p_\Phi(x) = \varepsilon^n \bar{p}_\Phi(\varepsilon x) \ (\text{see } (3)), \tag{23}$$

$$\text{if } \varepsilon = -1 \text{ then also } \chi_\Phi(x) \notin \{x^2, x^4, x^6, \dots\}. \tag{24}$$

With these conditions satisfied, one can take

$$\Phi_\varepsilon = [\varepsilon^i a_{i+j}],$$

in which the sequence $(a_2, a_3, \dots, a_{2n})$ *is* χ*-recurrent, and is defined by the fragment*

$$(a_2, \dots, a_{n+1}) = \begin{cases} (1, 0, \dots, 0) & \text{if } \Phi \text{ is nonsingular,} \\ (0, \dots, 0, 1) & \text{if } \Phi \text{ is singular.} \end{cases} \tag{25}$$

3 Canonical forms over finite fields

In this section we give canonical matrices of bilinear and sesquilinear forms, pairs of symmetric or skew-symmetric forms, and pairs of Hermitian forms over a finite field $\mathbb{F}$ of characteristic not 2. We use Theorems 2.2 and 2.3, in which these canonical matrices are given up to classification of quadratic and Hermitian forms over finite extensions of $\mathbb{F}$ (that is, over finite fields of characteristic not 2), and the following lemma.

Lemma 3.1 ([3, Chap. 1, § 8]). (a) *Each quadratic form of rank r over a finite field $\mathbb{F}$ of characteristic not 2 is equivalent to*

$$\text{either } x_1^2 + x_2^2 + \cdots + x_r^2, \qquad \text{or } \zeta x_1^2 + x_2^2 + \cdots + x_r^2,$$

where ζ is a fixed nonsquare in $\mathbb{F}$.

(b) *Each Hermitian form of rank r over a finite field of characteristic not 2 with nonidentity involution is equivalent to $\bar{x}_1 y_1 + \cdots + \bar{x}_r y_r$.*

Utv. (b) eshe iz Scharlau ch 10, 1.6, examples (i).

3.1 Canonical matrices for congruence and *congruence

Define the n-by-n matrix

$$\Gamma_n = \begin{bmatrix} 0 & & & & \cdot^{\cdot^{\cdot}} \\ & & & -1 & \cdot^{\cdot^{\cdot}} \\ & & 1 & 1 & \\ & -1 & -1 & & \\ 1 & 1 & & & 0 \end{bmatrix} \qquad (\Gamma_1 = [\,1\,]). \tag{26}$$

Theorem 3.2. *Every square matrix over a finite field $\mathbb{F}$ of characteristic different from 2 is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $J_n(0)$;

(ii) $[\Phi \diagdown I_n]$, *in which Φ is an $n \times n$ nonsingular Frobenius block such that*

$$p_\Phi(x) \neq p_\Phi^\vee(x) \ (\textit{see } (5)) \qquad \textit{or} \qquad p_\Phi(x) = x + (-1)^{n+1}, \tag{27}$$

and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$;

(iii) $\sqrt[T]{\Phi}$, *in which Φ is a nonsingular Frobenius block such that $p_\Phi(x) = p_\Phi^\vee(x)$ and $\deg p_\Phi(x) \geqslant 2$;*

(iv) *for each $n = 1, 2, \ldots$:*

- Γ_n,
- *at most one summand* $\zeta\Gamma_n$, *in which* ζ *is a fixed nonsquare of* $\mathbb{F}$.

Proof. Let $\mathbb{F}$ be a finite field of characteristic not 2 with the identity involution. By Theorem 2.2(a), every square matrix A over $\mathbb{F}$ is congruent to a direct sum of matrices of the form

$$\text{(a) } J_n(0), \quad \text{(b) } [\Phi \diagdown I_n] \text{ if } \sqrt[T]{\Phi} \text{ does not exist}, \quad \text{(c) } \sqrt[T]{\Phi}q(\Phi).$$

Consider each of these summands.

Summands (a). Theorem 2.2(b) ensures that the summands of the form $J_n(0)$ are uniquely determined by A, which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.6(a), $\sqrt[T]{\Phi}$ does not exist if and only if (27) holds. Theorem 2.2(b) ensures that the summands of the form $[\Phi \diagdown I_n]$ are uniquely determined by A, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$. This gives the summands (ii).

Summands (c). Let Φ be a nonsingular $n \times n$ Frobenius block for which $\sqrt[T]{\Phi}$ exists. Then by Lemma 2.6(a)

$$p_\Phi(x) = p_\Phi^\vee(x), \qquad p_\Phi(x) \neq x + (-1)^{n+1}. \tag{28}$$

Consider the whole group of summands of the form $\sqrt[T]{\Phi}q(\Phi)$ with the same Φ:

$$\sqrt[T]{\Phi}q_1(\Phi) \oplus \cdots \oplus \sqrt[T]{\Phi}q_s(\Phi). \tag{29}$$

Let first $\deg p_\Phi(x) > 1$. Then the involution $f(\kappa)^\circ := f(\kappa^{-1})$ on the field $\mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ (see (6) and (7)) is nonidentity; otherwise $\kappa = \kappa^\circ = \kappa^{-1}$, $\kappa^2 - 1 = 0$, $(x^2-1)|p_\Phi(x)$, and hence $p_\Phi(x) = x \pm 1$ since it is irreducible. By Lemma 3.1(b), the Hermitian form

$$q_1(\kappa)x_1^\circ y_1 + \cdots + q_s(\kappa)x_s^\circ y_s$$

over $F(\kappa)$ is equivalent to $x_1^\circ y_1 + \cdots + x_s^\circ y_s$. By Theorem 2.2(b), the matrix (29) is congruent to $\sqrt[T]{\Phi} \oplus \cdots \oplus \sqrt[T]{\Phi}$ and the summands of the form $\sqrt[T]{\Phi}$ with $\deg p_\Phi(x) > 1$ are uniquely determined by A. This gives the summands (iii).

Let now $p_\Phi(x) = x + c$. Then by (28) and (4) $x + c = c^{-1}(cx+1)$, $c = c^{-1}$, $c = \pm 1$. The inequality in (28) implies

$$p_\Phi(x) = x + (-1)^n. \tag{30}$$

By [8, Eq.(70)],

$$\Gamma_n^{-T}\Gamma_n = \Upsilon_n := (-1)^{n+1}\begin{bmatrix} 1 & 2 & & * \\ & 1 & \ddots & \\ & & \ddots & 2 \\ 0 & & & 1 \end{bmatrix}. \tag{31}$$

Hence $\Gamma_n = \sqrt[T]{\Upsilon_n}$ and Υ_n is similar to $J_n((-1)^{n+1})$, which is similar to Φ due to (30). By Theorem 2.2(c) we can take Υ_n instead of Φ with $p_\Phi(x) = x + (-1)^n$ in Theorem 2.2(a,b). The field $\mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is $\mathbb{F}$ with the identity involution; all polynomials $q_i(x)$ in (29) are some scalars $a_i \in \mathbb{F}$. By Lemma 3.1(a), the quadratic form

$$q_1(\kappa)x_1^2 + \cdots + q_s(\kappa)x_s^2 = a_1x_1^2 + \cdots + a_sx_s^2$$

over $\mathbb{F}$ is equivalent to

$$\text{either} \;\; x_1^2 + \cdots + x_r^2, \qquad \text{or} \;\; \zeta x_1^2 + x_2^2 + \cdots + x_r^2,$$

in which ζ is a fixed nonsquare of $\mathbb{F}$. Theorem 2.2(b) ensures that (29) is congruent to

$$\text{either} \;\; \Gamma_n \oplus \cdots \oplus \Gamma_n, \qquad \text{or} \;\; \zeta\Gamma_n \oplus \Gamma_n \oplus \cdots \oplus \Gamma_n,$$

and this sum is uniquely determined by A. This gives the summands (iv). $\square$

Note that if $\sqrt[T]{\Phi}$ exists, then $\deg p_\Phi(x)$ is even or $p_\Phi(x) = x + (-1)^n$. Indeed, $p_\Phi(x) = p_\Phi^\vee(x)$ by (16). Let $p_\Phi(x) = x^n + c_1x^{n-1} + \cdots + c_n$. Then

$$x^n + c_1x^{n-1} + \cdots + c_n = c_n^{-1}(c_nx^n + \cdots + c_1x + 1),$$

$c_n = c_n^{-1}$, and $\theta := c_n = \pm 1$. If $n = 2m+1$, then

$$p_\Phi(x) = x^n + c_1x^{n-1} + \cdots + c_{m+1}x^{m+1} + \theta c_{m+1}x^m + \cdots + \theta c_1x^{n-1} + \theta,$$

and so $p_\Phi(-\theta) = 0$. Since $p_\Phi(x)$ is irreducible, $p_\Phi(x) = x + \theta$. By the inequality (17), $p_\Phi(x) = x + (-1)^n$.

JaJa Example: $\mathbb{F}_5/(x^2 + x + 1)$.

Theorem 3.3. *Let $\mathbb{F}$ be a finite field of characteristic not 2 with nonidentity involution. Every square matrix over $\mathbb{F}$ is *congruent to a direct sum, uniquely determined up to permutation of summands, of matrices of the following types:*

(i) $J_n(0)$;

(ii) $[\Phi \diagdown I_n]$, *in which* Φ *is an* $n \times n$ *nonsingular Frobenius block such that* $p_\Phi(x) \neq p_\Phi^\vee(x)$ *(see (4)) and* Φ *is determined up to replacement by the Frobenius block* Ψ *with* $\chi_\Psi(x) = \chi_\Phi^\vee(x)$*;*

(iii) $\sqrt[*]{\Phi}$, *in which* Φ *is a nonsingular Frobenius block such that* $p_\Phi(x) = p_\Phi^\vee(x)$.

Proof. Let $\mathbb{F}$ be a finite field of characteristic not 2 with nonidentity involution. By Theorem 2.2(a), every square matrix A over $\mathbb{F}$ is *congruent to a direct sum of matrices of the form

$$\text{(a) } J_n(0), \quad \text{(b) } [\Phi \diagdown I_n] \text{ if } \sqrt[*]{\Phi} \text{ does not exist}, \quad \text{(c) } \sqrt[*]{\Phi}q(\Phi).$$

Consider each of these summands.

Summands (a). Theorem 2.2(b) ensures that the summands of the form $J_n(0)$ are uniquely determined by A, which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.6(a), $\sqrt[*]{\Phi}$ does not exist if and only if $p_\Phi(x) \neq p_\Phi^\vee(x)$. Theorem 2.2(b) ensures that the summands of the form $[\Phi \diagdown I_n]$ are uniquely determined by A, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$. This gives the summands (ii).

Summands (c). Let Φ be a nonsingular $n \times n$ Frobenius block for which $\sqrt[*]{\Phi}$ exists; this means that $p_\Phi(x) = p_\Phi^\vee(x)$. Consider the whole group of summands of the form $\sqrt[*]{\Phi}q(\Phi)$ with the same Φ:

$$\sqrt[*]{\Phi}q_1(\Phi) \oplus \cdots \oplus \sqrt[*]{\Phi}q_s(\Phi). \tag{32}$$

The involution $f(\kappa)^\circ := f(\kappa^{-1})$ on the field $\mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ (see (6) and (7)) is nonidentity since it extends the nonidentity involution on $\mathbb{F}$. By Lemma 3.1(b), the Hermitian form

$$q_1(\kappa)x_1^\circ y_1 + \cdots + q_s(\kappa)x_s^\circ y_s$$

over $F(\kappa)$ is equivalent to $x_1^\circ y_1 + \cdots + x_s^\circ y_s$, and so by Theorem 2.2(b) the matrix (32) is *congruent to $\sqrt[*]{\Phi} \oplus \cdots \oplus \sqrt[*]{\Phi}$ and this direct sum is uniquely determined by A. This gives the summands (iii). $\square$

3.2 Canonical pairs of symmetric or skew-symmetric matrices

In this section, we give canonical matrices of pairs consisting of symmetric or skew-symmetric forms. Canonical matrices of pairs of skew-symmetric forms are given in Corollary 2.4; it remains to consider pairs, in which the first form is symmetric and the second is symmetric or skew-symmetric.

For square matrices A, B, C, D of the same size, we write

$$(A, B) \oplus (C, D) = (A \oplus C, B \oplus D), \qquad (A, B)C = (AC, BC).$$

Theorem 3.4. *Each pair of symmetric matrices of the same size over a finite field $\mathbb{F}$ of characteristic not 2 is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $([F_n \diagdown F_n^T], [G_n \diagdown G_n^T])$, *where F_n and G_n are defined in* (11)*;*

(ii) *for each nonsingular Frobenius block Φ:*

- $(\Phi_1, \Phi_1\Phi)$, *in which Φ_1 is defined in* (10)*,*
- *at most one summand $(\Phi_1, \Phi_1\Phi)f_\Phi(\Phi)$, in which $f_\Phi(x) \in \mathbb{F}[x]$ is a fixed (for each Φ) polynomial of degree $< \deg(p_\Phi(x))$ such that*

$$f_\Phi(\omega) \in \mathbb{F}(\omega) := \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$$

is not a square;

(iii) *for each $n = 1, 2, \dots$:*

- *the pair of $n \times n$ matrices*

$$B_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & 0 \end{bmatrix} \right), \tag{33}$$

- *at most one summand ζB_n, in which ζ is a fixed nonsquare of $\mathbb{F}$.*

Proof. Let $\mathbb{F}$ be a finite field of characteristic not 2 with the identity involution. By Lemma 2.7, the matrix Φ_1 exists for each nonsingular Frobenius block Φ over $\mathbb{F}$. By Theorem 2.3(a), each pair (A, B) of symmetric matrices of the same size is congruent to a direct sum of pairs of the form

$$\text{(a) } ([F_n \diagdown F_n^T], [G_n \diagdown G_n^T]), \quad \text{(b) } A_\Phi^{f(x)} := (\Phi_1, \Phi_1\Phi)f(\Phi), \quad \text{(c) } B_n^a,$$

in which $f(x) \in \mathbb{F}[x]$ is a nonzero polynomial of degree $< \deg(p_\Phi(x))$ and $0 \neq a \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands of the form (a) are uniquely determined by (A, B), which gives the summands (i) of the theorem.

Summands (b). Consider the whole group of summands of the form $A_\Phi^{g(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{g_1(x)} \oplus \cdots \oplus A_\Phi^{g_s(x)}. \tag{34}$$

By Lemma 3.1(a), the quadratic form

$$q_1(\omega)x_1^2 + \cdots + q_s(\omega)x_s^2$$

over $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is equivalent to

$$\text{either} \ \ x_1^2 + \cdots + x_r^2, \qquad \text{or} \ \ f_\Phi(\omega)x_1^2 + x_2^2 + \cdots + x_r^2,$$

in which $f_\Phi(x) \in \mathbb{F}[x]$ is a fixed nonzero polynomial of degree $< \deg(p_\Phi(x))$ such that $f_\Phi(\omega) \in \mathbb{F}(\omega)$ is not a square. Theorem 2.2(b) ensures that (34) is congruent to

$$\text{either} \ \ A_\Phi^1 \oplus \cdots \oplus A_\Phi^1, \qquad \text{or} \ \ A_\Phi^{f_\Phi(x)} \oplus A_\Phi^1 \oplus \cdots \oplus A_\Phi^1,$$

and this sum is uniquely determined by (A, B). This gives the summands (ii).

Summands (c). Consider the whole group of summands of the form B_n^a with the same n:

$$B_n^{a_1} \oplus \cdots \oplus B_n^{a_s}. \tag{35}$$

By Lemma 3.1(a), the quadratic form $a_1x_1^2 + \cdots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to either $x_1^2 + \cdots + x_r^2$, or $\zeta x_1^2 + x_2^2 + \cdots + x_r^2$, in which ζ is a fixed nonsquare of $\mathbb{F}$. Theorem 2.2(b) ensures that (35) is congruent to

$$\text{either} \ \ B_n^1 \oplus \cdots \oplus B_n^1, \qquad \text{or} \ \ B_n^\zeta \oplus B_n^1 \oplus \cdots \oplus B_n^1,$$

and this sum is uniquely determined by (A, B). This gives the summands (iii). $\square$

Theorem 3.5. *Each pair consisting of a symmetric matrix and a skew-symmetric matrix of the same size over a finite field $\mathbb{F}$ of characteristic not 2 is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $([F_n \diagdown F_n^T],\ [G_n \diagdown -G_n^T])$, *in which F_n and G_n are defined in (11);*

(ii) $([I_n \diagdown I_n],\ [\Phi \diagdown -\Phi^T])$, *in which Φ is an $n \times n$ Frobenius block such that*

$$p_\Phi(x) \notin \mathbb{F}[x^2], \qquad \Phi \neq J_1(0), J_3(0), J_5(0), \dots \tag{36}$$

(see (2)), and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = (-1)^{\det \chi_\Phi} \chi_\Phi(-x)$;

(iii) $(\Phi_{-1}, \Phi_{-1}\Phi)$, *in which Φ is a Frobenius block such that $p_\Phi(x) \in \mathbb{F}[x^2]$;*

(iv) $([J_n(0) \diagdown J_n(0)^T], [I_n \diagdown -I_n])$, *in which n is odd;*

(v) *for each $n = 1, 2, 3, \dots$:*

- *the pair of n-by-n symmetric and skew-symmetric matrices defined as follows:*

$$C_n := \left(\begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & & & 1 & 0 \\ & & & & \iddots & \iddots & \\ & & & 1 & 0 & & \\ & & -1 & 0 & & & \\ & \iddots & 0 & & & & \\ -1 & \iddots & & & & & \\ 0 & & & & & & 0 \end{bmatrix} \right) \tag{37}$$

if n is odd, and

$$C_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & & 1 \\ & & & \iddots & \\ & & & 1 & \\ & & -1 & & \\ & \iddots & & & \\ -1 & & & & 0 \end{bmatrix} \right) \tag{38}$$

if n is even,

- *at most one summand of the form ζC_n, in which ζ is a fixed non-square of $\mathbb{F}$.*

Proof. Let $\mathbb{F}$ be a finite field of characteristic not 2 with the identity involution. By Theorem 2.3(a) and Remark 2.5, each pair (A, B) consisting of a symmetric matrix A and a skew-symmetric matrix B of the same size is congruent to a direct sum of pairs of the form

(a) $([F_n \diagdown F_n^T],\ [G_n \diagdown -G_n^T])$,

(b) $([I_n \diagdown I_n],\ [\Phi \diagdown -\Phi^T])$ if Φ_{-1} does not exist,

(c) $A_\Phi^{f(x)} := (\Phi_{-1}, \Phi_{-1}\Phi) f(\Phi)$, in which $0 \neq f(x) = f(-x) \in \mathbb{F}[x]$ and $\deg(f(x)) < \deg(p_\Phi(x))$,

(d) $([J_n(0) \diagdown J_n(0)^T], [I_n \diagdown -I_n])$, in which n is odd,

(e) C_n^a (defined in (15)), in which n is even and $0 \neq a \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands (a) are uniquely determined by (A, B), which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.7, Φ_{-1} does not exist if and only if (36) is satisfied. Theorem 2.3(b) ensures that the summands (b) are uniquely determined by (A, B), up to replacement of Φ by Ψ with $\chi_\Psi(x) = (-1)^{\det \chi_\Phi} \chi_\Phi(-x)$, which gives the summands (ii).

Summands (c). By Lemma 2.7, Φ_{-1} exists if and only if (36) is not satisfied; that is,

$$p_\Phi(x) \in \mathbb{F}[x^2] \quad \text{or} \quad \Phi = J_1(0), J_3(0), J_5(0), \dots \tag{39}$$

Consider the whole group of summands of the form $A_\Phi^{f(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{f_1(x)} \oplus \dots \oplus A_\Phi^{f_s(x)}. \tag{40}$$

Let first $p_\Phi(x) \in \mathbb{F}[x^2]$. Then the involution $f(\omega)^\circ = f(-\omega)$ on $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is nonidentity (since $\omega^\circ = -\omega \neq \omega$). By Lemma 3.1(b), the Hermitian form

$$f_1(\omega) x_1^\circ y_1 + \dots + f_s(\omega) x_s^\circ y_s$$

over $\mathbb{F}(\omega)$ is equivalent to $x_1^\circ y_1 + \dots + x_r^\circ y_r$. Theorem 2.2(b) ensures that (40) is congruent to $A_\Phi^1 \oplus \dots \oplus A_\Phi^1$, which gives the summands (iii).

Let now $\Phi = J_n(0)$ with $n = 2m+1$ and $m = 1, 2, \dots$. The equalities (10) hold for the $n \times n$ matrices

$$\Phi' := \begin{bmatrix} 0 & & & & & & 0 \\ -1 & \ddots & & & & \iddots & \\ & \ddots & 0 & 0 & 0 & & \\ & & -1 & 0 & 0 & & \\ & & 0 & 1 & 0 & & \\ & \iddots & & & \ddots & \ddots & \\ 0 & & & & & 1 & 0 \end{bmatrix}, \qquad \Phi'_{-1} := \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} \tag{41}$$

instead of Φ and Φ_{-1}. Since Φ and Φ' are similar, by Theorem 2.3(c) we can take $C_n^{f(x)} := (\Phi'_{-1}, \Phi'_{-1}\Phi')f(\Phi')$ instead of $A_\Phi^{f(x)}$ and

$$C_n^{f_1(x)} \oplus \dots \oplus C_n^{f_s(x)} \tag{42}$$

instead of (40).

Since $p_\Phi(x) = x$, the field $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is $\mathbb{F}$ with the identity involution and all polynomials $f_i(x)$ in (42) are some scalars $a_i \in \mathbb{F}$. By Lemma 3.1(a), the quadratic form $a_1x_1^2 + \dots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to either $x_1^2 + \dots + x_r^2$, or $\zeta x_1^2 + x_2^2 + \dots + x_r^2$, in which ζ is a fixed nonsquare of $\mathbb{F}$. Theorem 2.2(b) ensures that (40) is congruent to

$$\text{either} \quad C_n^1 \oplus \dots \oplus C_n^1, \qquad \text{or} \quad C_n^\zeta \oplus C_n^1 \oplus \dots \oplus C_n^1, \tag{43}$$

and this sum is uniquely determined by (A, B). This gives the summands (v) with odd n.

Summands (d). Theorem 2.3(b) ensures that the summands of the form (d) are uniquely determined by (A, B), which gives the summands (iv).

Summands (e). Consider the whole group of summands of the form C_n^a with the same n:

$$C_n^{a_1} \oplus \dots \oplus C_n^{a_s}. \tag{44}$$

By Lemma 3.1(a), the quadratic form $a_1x_1^2 + \dots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to either $x_1^2 + \dots + x_r^2$, or $\zeta x_1^2 + x_2^2 + \dots + x_r^2$, in which ζ is a fixed nonsquare of $\mathbb{F}$. Theorem 2.2(b) and Remark 2.5 ensure that (44) is congruent to

$$\text{either} \quad C_n^1 \oplus \dots \oplus C_n^1, \qquad \text{or} \quad C_n^\zeta \oplus C_n^1 \oplus \dots \oplus C_n^1,$$

and this sum is uniquely determined by (A,B), which gives the summands (v) with even n. $\square$

3.3 Canonical pairs of Hermitian matrices

Theorem 3.6. *Let $\mathbb{F}$ be a finite field of characteristic not 2 with nonidentity involution. Let $\mathbb{F}_\circ$ be the fixed field of $\mathbb{F}$. Each pair of Hermitian matrices of the same size over $\mathbb{F}$ is *congruent to a direct sum, uniquely determined up to permutation of summands, of pairs of the following types:*

(i) $([F_n \diagdown F_n^*], [G_n \diagdown G_n^*])$, *in which F_n and G_n are defined in* (11)*;*

(ii) $([I_n \diagdown I_n], [\Phi \diagdown \Phi^*])$, *in which Φ is an $n \times n$ Frobenius block over $\mathbb{F}$ such that $p_\Phi(x) \notin \mathbb{F}_\circ[x]$, and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = \bar{\chi}_\Phi(x)$ (see* (3)*);*

(iii) $(\Phi_1, \Phi_1\Phi)$, *in which Φ is a Frobenius block over $\mathbb{F}_\circ$;*

(iv) *the pair of $n \times n$ matrices*

$$B_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & 0 \end{bmatrix} \right), \quad n = 1, 2, \dots \tag{45}$$

Proof. Let $\mathbb{F}$ be a finite field of characteristic not 2 with nonidentity involution. By Theorem 2.3(a), each pair (A,B) of Hermitian matrices over $\mathbb{F}$ of the same size is *congruent to a direct sum of pairs of the form

(a) $([F_n \diagdown F_n^*], [G_n \diagdown G_n^*])$,

(b) $([I_n \diagdown I_n], [\Phi \diagdown \Phi^*])$ if Φ_1 does not exist,

(c) $A_\Phi^{f(x)} := (\Phi_\delta, \Phi_1\Phi)f(\Phi)$, in which $0 \neq f(x) = \bar{f}(x) \in \mathbb{F}[x]$ and $\deg(f(x)) < \deg(p_\Phi(x))$,

(d) B_n^a (defined in (12)), in which $0 \neq a = \bar{a} \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands of the form (a) are uniquely determined by (A,B), which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.7(a), Φ_1 does not exist if and only if $p_\Phi(x) \neq \bar{p}_\Phi(x)$; that is, $p_\Phi(x) \notin \mathbb{F}_\circ[x]$. Theorem 2.3(b) ensures that the summands of the form (b) are uniquely determined, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \bar{\chi}_\Phi(x)$. This gives the summands (ii).

Summands (c). Consider the whole group of summands of the form $A_\Phi^{f(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{f_1(x)} \oplus \cdots \oplus A_\Phi^{f_s(x)}. \tag{46}$$

By Lemma 3.1(b), the Hermitian form

$$f_1(\omega)x_1^\circ y_1 + \cdots + f_s(\omega)x_s^\circ y_s$$

over $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ with involution $f(\omega)^\circ = \bar{f}(\omega)$ is equivalent to $x_1^\circ x_1 + \cdots + x_s^\circ x_s$. Theorem 2.3(b) ensures that (46) is *congruent to $A_\Phi^1 \oplus \cdots \oplus A_\Phi^1$ and this sum is uniquely determined by (A, B). This gives the summands (iii).

Summands (d). Consider the whole group of summands of the form B_n^a with the same n:

$$B_n^{a_1} \oplus \cdots \oplus B_n^{a_s}. \tag{47}$$

By Lemma 3.1(b), the Hermitian form $a_1\bar{x}_1 y_1 + \cdots + a_s\bar{x}_s y_s$ over $\mathbb{F}$ is equivalent to $\bar{x}_1 y_1 + \cdots + \bar{x}_s y_s$. Theorem 2.2(b) ensures that (47) is *congruent to $B_n^1 \oplus \cdots \oplus B_n^1$ and this sum is uniquely determined by (A, B). This gives the summands (iv).

$\square$

4 Canonical forms over $\mathfrak{p}$-adic fields

In this section $\mathbb{K}$ is a finite extension of $\mathbb{Q}_p$ with $p \neq 2$.

Let us recall the classification of quadratic and Hermitian forms over $\mathbb{K}$. Each nonzero element of $\mathbb{Q}_p$ can be represented in the form

$$a = \alpha_z p^z + \alpha_{z+1}p^{z+1} + \cdots, \qquad z \in \mathbb{Z}, \quad \alpha_z \neq 0, \tag{48}$$

in which all $\alpha_i \in \{0, 1, \ldots, p-1\}$. The *exponential variation* on $\mathbb{K}$ is the following mapping $\nu : \mathbb{K} \to \mathbb{R} \cup \{+\infty\}$:

$$\nu(a) := \begin{cases} +\infty, & \text{if } a = 0,\\ z, & \text{if } 0 \neq a \in \mathbb{Q}_p \text{ is represented in the form (48)},\\ \nu(\alpha_m)/m, & \text{if } a \notin \mathbb{Q}_p \text{ and its minimum polynomial of over } \mathbb{Q}_p \text{ is}\\ & \qquad x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m. \end{cases}$$

The ring
$$\mathcal{O}(\mathbb{K}) := \{a \in \mathbb{K} \,|\, \nu(a) \geqslant 0\} \tag{49}$$
is called the *ring of integers* of $\mathbb{K}$; it is a principal ideal ring, whose unique maximal ideal is
$$\mathfrak{m} := \{a \in \mathbb{K} \,|\, \nu(a) > 0\} = \pi\mathcal{O}(\mathbb{K}). \tag{50}$$
Each generator π of $\mathfrak{m}$ is called a *prime element*. The set
$$\mathcal{O}(\mathbb{K})^{\times} := \{a \in \mathbb{K} \,|\, \nu(a) = 0\} \tag{51}$$
is the group of all invertible elements of $\mathcal{O}(\mathbb{K})$; they are called the *units* of $\mathbb{K}$.

The factor ring
$$\mathcal{O}(\mathbb{K})/\mathfrak{m} \tag{52}$$
is a field, which is called the *residue field* of $\mathbb{K}$; it is a finite extension of the residue field $\mathbb{F}_p = \mathbb{Q}_p/p\mathbb{Q}_p$ of $\mathbb{Q}_p$.

Lemma 4.1. *Let $\mathbb{K}$ be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. Let its residue field $\mathcal{O}(\mathbb{K})/\mathfrak{m}$ consist of p^m elements. Let $u \in \mathcal{O}(\mathbb{K})^{\times} \setminus \mathbb{K}^{\times 2}$ be a unit that is not a square, and π be a prime element. Then each quadratic form of rank $r \geqslant 1$ over $\mathbb{K}$ is equivalent to exactly one form*
$$c_1x_1^2 + c_2x_2^2 + \cdots + c_tx_t^2 + x_{t+1}^2 + \cdots + x_r^2, \tag{53}$$
in which $(c_1, \dots, c_t)$ is one of the sequences:
$$(1),\ (u),\ (\pi),\ (u\pi),\ (u,\pi),\ (u,u\pi),\ (\pi,r\pi),\ (u,\pi,r\pi), \tag{54}$$
where
$$r := \begin{cases} u & \text{if } p^m \equiv 1 \mod 4, \\ 1 & \text{if } p^m \equiv 3 \mod 4. \end{cases} \tag{55}$$

Lemma 4.2. *Let a field $\mathbb{K}$ with nonidentity involution be a finite extension of $\mathbb{Q}_p$, $p \neq 2$. Let $\mathbb{K}_\circ$ be the fixed field with respect to this involution. Let $u \in \mathcal{O}(\mathbb{K}_\circ)^{\times} \setminus \mathbb{K}_\circ^{\times 2}$ be a unit that is not a square, and π be a prime element of $\mathbb{K}_\circ$. Then each Hermitian form with nonzero determinant over $\mathbb{K}$ is classified by dimension and determinant; moreover, it is equivalent to*
$$\text{either } \ \bar{x}_1y_1 + \cdots + \bar{x}_ny_n, \qquad \text{or } \ t\bar{x}_1y_1 + \bar{x}_2y_2 + \cdots + \bar{x}_ny_n,$$

in which

$$t := \begin{cases} \pi & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u}), \\ u & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{\pi}) \text{ or } \mathbb{K}_\circ(\sqrt{u\pi}). \end{cases} \tag{56}$$

Proof. By [13, Ch. 10, Example 1.6(ii)], regular Hermitian forms over $\mathbb{K}$ are classified by dimension and determinant. □

4.1 Canonical matrices for congruence and *congruence

Theorem 4.3. *Let a field $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. Every square matrix over $\mathbb{F}$ is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $J_n(0)$;

(ii) $[\Phi \diagdown I_n]$, *in which Φ is an $n \times n$ nonsingular Frobenius block over $\mathbb{F}$ such that*

$$p_\Phi(x) \neq p_\Phi^\vee(x) \text{ (see (5))} \qquad \text{or} \qquad p_\Phi(x) = x + (-1)^{n+1} \tag{57}$$

and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$;

(iii) *for each nonsingular Frobenius block Φ over $\mathbb{F}$ such that $p_\Phi(x) = p_\Phi^\vee(x)$ and $\deg p_\Phi(x) \geqslant 2$:*

- $\sqrt[T]{\Phi}$,
- *at most one summand of the form*

$$\begin{cases} \sqrt[T]{\Phi}\tilde{\pi}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u}), \\ \sqrt[T]{\Phi}\tilde{u}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{\pi}) \text{ or } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u\pi}), \end{cases}$$

in which $\mathbb{K}$ is the following field with involution:

$$\mathbb{K} := \mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x], \qquad f(\kappa)^\circ := f(\kappa^{-1})$$

(see (6) and (7)), $\mathbb{K}_\circ$ is its fixed field, π is a prime element of $\mathbb{K}_\circ$, $u \in \mathcal{O}(\mathbb{K}_\circ)^\times \setminus \mathbb{K}_\circ^{\times 2}$ is a unit that is not a square, $\tilde{\pi}(x), \tilde{u}(x) \in \mathbb{F}[x, x^{-1}]$ are the functions of the form (8) such that $\tilde{\pi}(\kappa) = \pi$ and $\tilde{u}(\kappa) = u$;

(iv) *for each* $n = 1, 2, \dots$*:*

- Γ_n *(defined in* (26)*),*
- *at most one summand from the list*

$$u\Gamma_n,\ \pi\Gamma_n,\ u\pi\Gamma_n,\ u\Gamma_n \oplus \pi\Gamma_n,\ u\Gamma_n \oplus u\pi\Gamma_n,$$
$$\pi\Gamma_n \oplus r\pi\Gamma_n,\ u\Gamma_n \oplus \pi\Gamma_n \oplus r\pi\Gamma_n,$$

in which

$$r := \begin{cases} u & \text{if } p^m \equiv 1 \mod 4, \\ 1 & \text{if } p^m \equiv 3 \mod 4, \end{cases} \tag{58}$$

p^m *is the number of elements of the residue field* $\mathcal{O}(\mathbb{F})/\mathfrak{m}$ *of* $\mathbb{F}$*,* $u \in \mathcal{O}(\mathbb{F})^\times \setminus \mathbb{F}^{\times 2}$ *is a unit that is not a square, and* π *is a prime element of* $\mathbb{F}$*.*

Proof. Let a field $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. By Theorem 2.2(a), every square matrix A over $\mathbb{F}$ is congruent to a direct sum of matrices of the form

$$\text{(a) } J_n(0), \quad \text{(b) } [\Phi \diagdown I_n] \text{ if } \sqrt[T]{\Phi} \text{ does not exist}, \quad \text{(c) } \sqrt[T]{\Phi} q(\Phi).$$

Consider each of these summands.

Summands (a). Theorem 2.2(b) ensures that the summands of the form $J_n(0)$ are uniquely determined by A, which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.6(a), $\sqrt[T]{\Phi}$ does not exist if and only if (57) holds. Theorem 2.2(b) ensures that the summands of the form $[\Phi \diagdown I_n]$ are uniquely determined by A, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$. This gives the summands (ii).

Summands (c). Let Φ be a nonsingular $n \times n$ Frobenius block for which $\sqrt[T]{\Phi}$ exists. Then by Lemma 2.6(a)

$$p_\Phi(x) = p_\Phi^\vee(x), \qquad p_\Phi(x) \neq x + (-1)^{n+1}. \tag{59}$$

Consider the whole group of summands of the form $\sqrt[T]{\Phi} q(\Phi)$ with the same Φ:

$$\sqrt[T]{\Phi} q_1(\Phi) \oplus \cdots \oplus \sqrt[T]{\Phi} q_s(\Phi). \tag{60}$$

Let first $\deg p_\Phi(x) > 1$. Then the involution $f(\kappa)^\circ := f(\kappa^{-1})$ on the field $\mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ (see (6) and (7)) is nonidentity; otherwise $\kappa = \kappa^\circ =$

κ^{-1}, $\kappa^2-1=0$, x^2-1 divides $p_\Phi(x)$, and hence $p_\Phi(x)=x\pm 1$ since it is irreducible. By Lemma 4.2, the Hermitian form

$$q_1(\kappa)x_1^\circ y_1+\dots+q_s(\kappa)x_s^\circ y_s$$

over $\mathbb{F}(\kappa)$ is equivalent to either $x_1^\circ y_1+\dots+x_s^\circ y_s$ or $tx_1^\circ y_1+x_2^\circ y_2+\dots+x_s^\circ y_s$, in which t is defined in (56). Theorem 2.2(b) ensures that the matrix (60) is congruent to

$$\text{either}\quad \sqrt[T]{\Phi}\oplus\dots\oplus\sqrt[T]{\Phi},\qquad \text{or}\quad \sqrt[T]{\Phi}\tilde{t}(\Phi)\oplus\sqrt[T]{\Phi}\oplus\dots\oplus\sqrt[T]{\Phi},$$

in which $\tilde{t}(x)\in\mathbb{F}[x,x^{-1}]$ is the function of the form (8) such that $\tilde{t}(\kappa)=t$. This sum is uniquely determined by A, which gives the summands (iii).

Let now $p_\Phi(x)=x+c$. Then by (59) and (4), $x+c=c^{-1}(cx+1)$, $c=c^{-1}$, $c=\pm1$. The inequality in (59) implies

$$p_\Phi(x)=x+(-1)^n. \tag{61}$$

By (31), $\Gamma_n=\sqrt[T]{\Upsilon_n}$ and Υ_n is similar to $J_n((-1)^{n+1})$, which is similar to Φ due to (30). By Theorem 2.2(c) we can take Υ_n instead of Φ with $p_\Phi(x)=x+(-1)^n$ in Theorem 2.2(a,b). The field $\mathbb{F}(\kappa)=\mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is $\mathbb{F}$ with the identity involution; all polynomials $q_i(x)$ in (60) are some scalars $a_i\in\mathbb{F}$, by Lemma 4.1 with $\mathbb{K}=\mathbb{F}$, the quadratic form

$$q_1(\kappa)x_1^2+\dots+q_s(\kappa)x_s^2=a_1x_1^2+\dots+a_sx_s^2$$

over $\mathbb{F}$ is equivalent to exactly one form (53), in which $(c_1,\dots,c_t)$ is one of the sequences (54). Theorem 2.2(b) ensures that (60) is congruent to a direct sum of matrices of the form (iv), and this sum is uniquely determined by A. This gives the summands (iv). $\square$

Theorem 4.4. *Let a field $\mathbb{F}$ with nonidentity involution be a finite extension of $\mathbb{Q}_p$ with $p\neq 2$. Every square matrix A over $\mathbb{F}$ is *congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $J_n(0)$;

(ii) $[\Phi\diagdown I_n]$, *in which Φ is an $n\times n$ nonsingular Frobenius block over $\mathbb{F}$ such that $p_\Phi(x)\neq p_\Phi^\vee(x)$ (see (4)) and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x)=\chi_\Phi^\vee(x)$;*

(iii) *for each nonsingular Frobenius block* Φ *over* $\mathbb{F}$ *such that* $p_\Phi(x) = p_\Phi^\vee(x)$*:*

- $\sqrt[*]{\Phi}$,
- *at most one summand of the form*

$$\begin{cases} \sqrt[*]{\Phi}\tilde{\pi}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u}), \\ \sqrt[*]{\Phi}\tilde{u}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{\pi}) \text{ or } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u\pi}), \end{cases}$$

in which $\mathbb{K}$ *is the following field with involution:*

$$\mathbb{K} := \mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x], \qquad f(\kappa)^\circ := \bar{f}(\kappa^{-1})$$

(see (3), (6) *and* (7)*),* $\mathbb{K}_\circ$ *is its fixed field,* π *is a prime element of* $\mathbb{K}_\circ$*,* $u \in \mathcal{O}(\mathbb{K}_\circ)^\times \setminus \mathbb{K}_\circ^{\times 2}$ *is a unit that is not a square,* $\tilde{\pi}(x), \tilde{u}(x) \in \mathbb{F}[x, x^{-1}]$ *are the functions of the form* (8) *such that* $\tilde{\pi}(\kappa) = \pi$ *and* $\tilde{u}(\kappa) = u$.

Proof. Let a field $\mathbb{F}$ with nonidentity involution be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. By Theorem 2.2(a), every square matrix A over $\mathbb{F}$ is *congruent to a direct sum of matrices of the form

$$\text{(a) } J_n(0), \quad \text{(b) } [\Phi \diagdown I_n] \text{ if } \sqrt[*]{\Phi} \text{ does not exist}, \quad \text{(c) } \sqrt[*]{\Phi}q(\Phi).$$

Consider each of these summands.

Summands (a). Theorem 2.2(b) ensures that the summands of the form $J_n(0)$ are uniquely determined by A, which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.6(a), $\sqrt[*]{\Phi}$ does not exist if and only if $p_\Phi(x) \neq p_\Phi^\vee(x)$. Theorem 2.2(b) ensures that the summands of the form $[\Phi \diagdown I_n]$ are uniquely determined by A, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \chi_\Phi^\vee(x)$. This gives the summands (ii).

Summands (c). Let Φ be a nonsingular $n \times n$ Frobenius block for which $\sqrt[*]{\Phi}$ exists; this means that $p_\Phi(x) = p_\Phi^\vee(x)$. Consider the whole group of summands of the form $\sqrt[*]{\Phi}q(\Phi)$ with the same Φ:

$$\sqrt[*]{\Phi}q_1(\Phi) \oplus \cdots \oplus \sqrt[*]{\Phi}q_s(\Phi). \tag{62}$$

The involution $f(\kappa)^\circ := f(\kappa^{-1})$ on the field $\mathbb{F}(\kappa) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ (see (6) and (7)) is nonidentity since it extends the nonidentity involution on $\mathbb{F}$. By Lemma 4.2 with $\mathbb{K} := \mathbb{F}(\kappa)$, the Hermitian form

$$q_1(\kappa)x_1^\circ y_1 + \cdots + q_s(\kappa)x_s^\circ y_s$$

over $\mathbb{F}(\kappa)$ is equivalent to either $x_1^\circ y_1+\dots+x_s^\circ y_s$, or $tx_1^\circ y_1+x_2^\circ y_2+\dots+x_s^\circ y_s$, in which t is defined in (56). By Theorem 2.2(b), the matrix (62) is *congruent to

$$\text{either}\quad \sqrt[*]{\Phi}\oplus\dots\oplus\sqrt[*]{\Phi},\qquad \text{or}\quad \sqrt[*]{\Phi}\tilde{t}(\Phi)\oplus\sqrt[*]{\Phi}\oplus\dots\oplus\sqrt[*]{\Phi},$$

where $\tilde{t}(x)\in\mathbb{F}[x,x^{-1}]$ is the function of the form (8) such that $\tilde{t}(\kappa)=t$. This sum is uniquely determined by A, which gives the summands (iii). □

4.2 Canonical pairs of symmetric or skew-symmetric matrices

For each Frobenius block Φ, denote by $\sqrt[T]{\Phi}$ and Φ_ε ($\varepsilon=\pm1$) fixed nonsingular matrices satisfying, respectively, the conditions

$$\sqrt[T]{\Phi}=(\sqrt[T]{\Phi})^TA, \tag{63}$$

$$\Phi_\varepsilon=\Phi_\varepsilon^T,\quad \Phi_\varepsilon A=\varepsilon(\Phi_\varepsilon A)^T, \tag{64}$$

in which A is similar to Φ. Each of these matrices may not exist for some Φ; existence conditions and explicit forms of these matrices were established in [15].

Theorem 4.5. *Let a field $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ with $p\neq 2$. Each pair of symmetric matrices of the same size over $\mathbb{F}$ is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $([F_n\diagdown F_n^T],\,[G_n\diagdown G_n^T])$*, in which F_n and G_n are defined in* (11)*;*

(ii) *for each nonsingular Frobenius block Φ over $\mathbb{F}$:*

- $(\Phi_1,\Phi_1\Phi)$*, in which Φ_1 is defined in* (10)*,*
- *at most one summand of the form*

$$(\Phi_1,\Phi_1\Phi)f_1(\Phi)\oplus\dots\oplus(\Phi_1,\Phi_1\Phi)f_t(\Phi),$$

in which $(f_1(x),\dots,f_t(x))$ is a sequence of polynomials over $\mathbb{F}$ of degree $<\deg(p_\Phi(x))$ such that the sequence $(f_1(\omega),\dots,f_t(\omega))$ of elements of the field

$$\mathbb{K}:=\mathbb{F}(\omega)=\mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$$

is one of the sequences

$$(1),\ (u),\ (\pi),\ (u\pi),\ (u,\pi),\ (u,u\pi),\ (\pi,r\pi),\ (u,\pi,r\pi), \tag{65}$$

where

$$r := \begin{cases} u & \text{if } p^m \equiv 1 \mod 4, \\ 1 & \text{if } p^m \equiv 3 \mod 4, \end{cases} \tag{66}$$

p^m *is the number of elements of the residue field* $\mathcal{O}(\mathbb{K})/\mathfrak{m}$ *of* $\mathbb{K}$, $u \in \mathcal{O}(\mathbb{K})^\times \setminus \mathbb{K}^{\times 2}$ *is a unit that is not a square, and* π *is a prime element of* $\mathbb{K}$*;*

(iii) *for each* $n = 1, 2, \dots$*:*

- *the pair of* n*-by-*n *matrices*

$$B_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix} \right), \tag{67}$$

- *at most one summand of the form*

$$B_n c_1 \oplus \cdots \oplus B_n c_t, \tag{68}$$

in which $(c_1, \dots, c_t)$ *is one of the sequences*

$$(1),\ (u),\ (\pi),\ (u\pi),\ (u,\pi),\ (u,u\pi),\ (\pi,r\pi),\ (u,\pi,r\pi), \tag{69}$$

where

$$r := \begin{cases} u & \text{if } p^m \equiv 1 \mod 4, \\ 1 & \text{if } p^m \equiv 3 \mod 4, \end{cases} \tag{70}$$

p^m *is the number of elements of the residue field* $\mathcal{O}(\mathbb{F})/\mathfrak{m}$ *of* $\mathbb{F}$, $u \in \mathcal{O}(\mathbb{F})^\times \setminus \mathbb{F}^{\times 2}$ *is a unit that is not a square, and* π *is a prime element of* $\mathbb{F}$*.*

Proof. Let a field $\mathbb{F}$ with the identity involution be a finite extension of $\mathbb{Q}_p$, $p \neq 2$. By Lemma 2.7, the matrix Φ_1 exists for each nonsingular Frobenius block Φ over $\mathbb{F}$. By Theorem 2.3(a), each pair (A, B) of symmetric matrices of the same size is congruent to a direct sum of pairs of the form

(a) $([F_n \diagdown F_n^T], [G_n \diagdown G_n^T])$, (b) $A_\Phi^{f(x)} := (\Phi_1, \Phi_1\Phi)f(\Phi)$, (c) B_n^a, in which $f(x) \in \mathbb{F}[x]$ is a nonzero polynomial of degree $< \deg(p_\Phi(x))$ and $0 \neq a \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands of the form (a) are uniquely determined by (A, B), which gives the summands (i) of the theorem.

Summands (b). Consider the whole group of summands of the form $A_\Phi^{g(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{g_1(x)} \oplus \cdots \oplus A_\Phi^{g_s(x)}. \tag{71}$$

By Lemma 4.1, the quadratic form

$$q_1(\omega)x_1^2 + \cdots + q_s(\omega)x_s^2$$

over $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is equivalent to exactly one form (53), in which $(a_1, \dots, a_t)$ is one of the sequences (54). Theorem 2.3(b) ensures that (71) is congruent to a direct sum of pairs of the form (ii) and this sum is uniquely determined by (A, B), which gives the summands (ii).

Summands (c). For each n, consider the whole group of summands of the form B_n^a with the same n:

$$B_n^{a_1} \oplus \cdots \oplus B_n^{a_s}. \tag{72}$$

By Lemma 4.1, the quadratic form $a_1x_1^2 + \cdots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to to exactly one form (53), in which $(c_1, \dots, c_t)$ is one of the sequences (54). Theorem 2.3(b) ensures that (72) is congruent to a direct sum of pairs of the form (iii) and this sum is uniquely determined by (A, B), which gives the summands (iii). $\square$

Theorem 4.6. *Let a field $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. Each pair consisting of a symmetric matrix and a skew-symmetric matrix of the same size over $\mathbb{F}$ is congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $([F_n \diagdown F_n^T], [G_n \diagdown -G_n^T])$, *in which F_n and G_n are defined in* (11)*;*

(ii) $([I_n \diagdown I_n], [\Phi \diagdown -\Phi^T])$, *in which Φ is an $n \times n$ Frobenius block over $\mathbb{F}$ such that*

$$p_\Phi(x) \notin \mathbb{F}[x^2], \qquad \Phi \neq J_1(0), J_3(0), J_5(0), \dots \tag{73}$$

(see (2)), and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = (-1)^{\det \chi_\Phi} \chi_\Phi(-x)$;

(iii) *for each Frobenius block Φ over $\mathbb{F}$ such that $p_\Phi(x) \in \mathbb{F}[x^2]$:*

- $(\Phi_{-1}, \Phi_{-1}\Phi)$,
- *at most one summand of the form*

$$\begin{cases} (\Phi_{-1}, \Phi_{-1}\Phi)\tilde{\pi}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u}), \\ (\Phi_{-1}, \Phi_{-1}\Phi)\tilde{u}(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{\pi}) \text{ or } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u\pi}), \end{cases}$$

in which $\mathbb{K}$ is the following field with involution:

$$\mathbb{K} := \mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x], \qquad f(\omega)^\circ = f(-\omega),$$

$\mathbb{K}_\circ$ is its fixed field, π is any prime element of $\mathbb{K}_\circ$, and $u \in \mathcal{O}(\mathbb{K}_\circ)^\times \setminus \mathbb{K}_\circ^{\times 2}$ is any unit that is not a square; $\tilde{\pi}(x)$ and $\tilde{u}(x)$ are polynomials over $\mathbb{F}$ of degree $< \deg(p_\Phi(x))$ such that

$$\tilde{\pi}(x) = \tilde{\pi}(-x),\ \tilde{\pi}(\omega) = \pi, \qquad \tilde{u}(x) = \tilde{u}(-x),\ \tilde{u}(\omega) = u;$$

(iv) $([J_n(0) \diagdown J_n(0)^T], [I_n \diagdown -I_n])$, *in which n is odd;*

(v) *for each $n = 1, 2, 3, \dots$:*

- *the pair of n-by-n symmetric and skew-symmetric matrices defined as follows:*

$$C_n := \left(\begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & & & 1 & 0 \\ & & & & \iddots & \iddots & \\ & & & 1 & 0 & & \\ & & -1 & 0 & & & \\ & \iddots & 0 & & & & \\ -1 & \iddots & & & & & \\ 0 & & & & & & 0 \end{bmatrix} \right) \tag{74}$$

if n is odd, and

$$C_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & & 1 \\ & & & & \iddots \\ & & & 1 & \\ & & -1 & & \\ & \iddots & & & \\ -1 & & & & 0 \end{bmatrix} \right) \tag{75}$$

if n is even, and

- *at most one summand of the form*
$$C_n c_1 \oplus \dots \oplus C_n c_t, \tag{76}$$
in which $(c_1, \dots, c_t)$ is one of the sequences
$$(1),\ (u),\ (\pi),\ (u\pi),\ (u,\pi),\ (u,u\pi),\ (\pi,r\pi),\ (u,\pi,r\pi), \tag{77}$$
where
$$r := \begin{cases} u & \text{if } p^m \equiv 1 \mod 4, \\ 1 & \text{if } p^m \equiv 3 \mod 4, \end{cases} \tag{78}$$
p^m is the number of elements of the residue field $\mathcal{O}(\mathbb{F})/\mathfrak{m}$ of $\mathbb{F}$, $u \in \mathcal{O}(\mathbb{F})^\times \setminus \mathbb{F}^{\times 2}$ is a unit that is not a square, and π is a prime element of $\mathbb{F}$.

Proof. Let a field $\mathbb{F}$ with the identity involution be a finite extension of $\mathbb{Q}_p$, $p \neq 2$. By Theorem 2.3(a) and Remark 2.5, each pair (A, B) consisting of a symmetric matrix A and a skew-symmetric matrix B of the same size is congruent to a direct sum of pairs of the form

(a) $([F_n \diagdown F_n^T], [G_n \diagdown -G_n^T])$,

(b) $([I_n \diagdown I_n], [\Phi \diagdown -\Phi^T])$ if Φ_{-1} does not exist,

(c) $A_\Phi^{f(x)} := (\Phi_{-1}, \Phi_{-1}\Phi) f(\Phi)$, in which $0 \neq f(x) = f(-x) \in \mathbb{F}[x]$ and $\deg(f(x)) < \deg(p_\Phi(x))$,

(d) $([J_n(0) \diagdown J_n(0)^T], [I_n \diagdown -I_n])$, in which n is odd,

(e) C_n^a (defined in (15)), in which n is even and $0 \neq a \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands of the form (a) are uniquely determined by (A, B), which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.7, Φ_{-1} does not exist if and only if (73) is satisfied. Theorem 2.3(b) ensures that the summands of the form (b) are uniquely determined by (A, B), up to replacement of Φ by Ψ with $\chi_\Psi(x) = (-1)^{\det \chi_\Phi} \chi_\Phi(-x)$, which gives the summands (ii).

Summands (c). By Lemma 2.7, Φ_{-1} exists if and only if (73) is not satisfied; that is,

$$p_\Phi(x) \in \mathbb{F}[x^2] \quad \text{or} \quad \Phi = J_1(0), J_3(0), J_5(0), \dots \tag{79}$$

Consider the whole group of summands of the form $A_\Phi^{f(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{f_1(x)} \oplus \cdots \oplus A_\Phi^{f_s(x)}. \tag{80}$$

Let first $p_\Phi(x) \in \mathbb{F}[x^2]$. Then the involution $f(\omega)^\circ = f(-\omega)$ on $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is nonidentity (since $\omega^\circ = -\omega \neq \omega$). By Lemma 4.2, the Hermitian form

$$f_1(\omega)x_1^\circ y_1 + \cdots + f_s(\omega)x_s^\circ y_s$$

over $\mathbb{F}(\omega)$ is equivalent to either $x_1^\circ y_1 + \cdots + x_s^\circ y_s$, or $tx_1^\circ y_1 + x_2^\circ y_2 + \cdots + x_s^\circ y_s$, in which t is defined in (56). Theorem 2.2(b) ensures that (80) is congruent to

$$\text{either} \quad A_\Phi^1 \oplus \cdots \oplus A_\Phi^1, \qquad \text{or} \quad A_\Phi^1 \tilde{t}(\Phi) \oplus A_\Phi^1 \oplus \cdots \oplus A_\Phi^1,$$

where $\tilde{t}(x) \in \mathbb{F}[x, x^{-1}]$ is the function of the form (8) such that $\tilde{t}(\kappa) = t$. This sum is uniquely determined by (A, B), which gives the summands (iii).

Let now $\Phi = J_n(0)$ with $n = 2m + 1$ and $m = 1, 2, \dots$ The equalities (10) hold for the $n \times n$ matrices Φ' and Φ'_{-1} defined in (41) instead of Φ and Φ_{-1}. Since Φ and Φ' are similar, by Theorem 2.3(c) we can take $C_n^{f(x)} := (\Phi'_{-1}, \Phi'_{-1}\Phi')f(\Phi')$ instead of $A_\Phi^{f(x)}$ and

$$C_n^{f_1(x)} \oplus \cdots \oplus C_n^{f_s(x)} \tag{81}$$

instead of (40).

Since $p_\Phi(x) = x$, the field $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ is $\mathbb{F}$ with the identity involution and all polynomials $f_i(x)$ in (42) are some scalars $a_i \in \mathbb{F}$. By Lemma 4.1, the quadratic form $a_1x_1^2 + \cdots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to exactly one form (53), in which $(c_1, \dots, c_t)$ is one of the sequences (54). Theorem 2.3(b) ensures that (81) is congruent to a direct sum of pairs of the form (iii), and this sum is uniquely determined by (A, B). This gives the summands (v) with odd n.

Summands (d). Theorem 2.3(b) ensures that the summands of the form (d) are uniquely determined by (A, B), which gives the summands (iv).

Summands (e). Consider the whole group of summands of the form C_n^a with the same n:

$$C_n^{a_1} \oplus \cdots \oplus C_n^{a_s}. \tag{82}$$

By Lemma 4.1, the quadratic form $a_1x_1^2 + \cdots + a_sx_s^2$ over $\mathbb{F}$ is equivalent to exactly one form (53), in which $(c_1, \dots, c_t)$ is one of the sequences (54). Theorem 2.3(b) ensures that (82) is congruent to a direct sum of pairs of the form (iii), and this sum is uniquely determined by (A, B). This gives the summands (v) with even n. $\square$

4.3 Canonical pairs of Hermitian matrices

Theorem 4.7. *Let a field $\mathbb{F}$ with nonidentity involution be a finite extension of $\mathbb{Q}_p$, $p \neq 2$. Let $\mathbb{F}_\circ$ be the fixed field of $\mathbb{F}$. Each pair of Hermitian matrices of the same size over $\mathbb{F}$ is *congruent to a direct sum that is uniquely determined up to permutation of summands and consists of any number of summands of the following types:*

(i) $([F_n \diagdown F_n^*], [G_n \diagdown G_n^*])$, *in which F_n and G_n are defined in* (11)*;*

(ii) $([I_n \diagdown I_n], [\Phi \diagdown \Phi^*])$, *in which Φ is an $n \times n$ Frobenius block such that $p_\Phi(x) \notin \mathbb{F}_\circ[x]$, and Φ is determined up to replacement by the Frobenius block Ψ with $\chi_\Psi(x) = \bar{\chi}_\Phi(x)$ (see* (3)*);*

(iii) *for each Frobenius block Φ over $\mathbb{F}$ such that $p_\Phi(x) \in \mathbb{F}_\circ[x]$:*

- $(\Phi_1, \Phi_1\Phi)$, *in which Φ_1 is defined in Lemma 2.7,*
- *at most one summand of the form*

$$\begin{cases} (\Phi_1, \Phi_1\Phi)f_\pi(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u}), \\ (\Phi_1, \Phi_1\Phi)f_u(\Phi) & \text{if } \mathbb{K} = \mathbb{K}_\circ(\sqrt{\pi}) \text{ or } \mathbb{K} = \mathbb{K}_\circ(\sqrt{u\pi}), \end{cases}$$

in which $\mathbb{K}$ is the following field with involution:

$$\mathbb{K} := \mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x], \qquad f(\omega)^\circ = \bar{f}(\omega),$$

$\mathbb{K}_\circ$ is its fixed field, π is any prime element of $\mathbb{K}_\circ$, and $u \in \mathcal{O}(\mathbb{K}_\circ)^\times \setminus \mathbb{K}_\circ^{\times 2}$ is any unit that is not a square, $\tilde{\pi}(x)$ and $\tilde{u}(x)$ are polynomials over $\mathbb{F}_\circ$ of degree $< \deg(p_\Phi(x))$ such that

$$\tilde{\pi}(\omega) = \pi, \qquad \tilde{u}(\omega) = u;$$

(iv) *for each* $n = 1, 2, \dots$*:*

- *the pair of* n*-by-*n *matrices*

$$B_n := \left(\begin{bmatrix} 0 & & 1 & 0 \\ & \iddots & \iddots & \\ 1 & 0 & & \\ 0 & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & & 1 \\ & & \iddots & \\ & 1 & & \\ 1 & & & 0 \end{bmatrix} \right),$$

- *at most one summand of the form*

$$\begin{cases} B_n\pi & \text{if } \mathbb{F} = \mathbb{F}_\circ(\sqrt{u}), \\ B_n u & \text{if } \mathbb{F} = \mathbb{F}_\circ(\sqrt{\pi}) \text{ or } \mathbb{F} = \mathbb{F}_\circ(\sqrt{u\pi}), \end{cases}$$

  in which π *is a prime element of* $\mathbb{F}_\circ$ *and* $u \in \mathcal{O}(\mathbb{F}_\circ)^\times \setminus \mathbb{F}_\circ^{\times 2}$ *is a unit that is not a square.*

Proof. Let a field $\mathbb{F}$ with nonidentity involution be a finite extension of $\mathbb{Q}_p$, $p \neq 2$. By Theorem 2.3(a), each pair (A, B) of Hermitian matrices of the same size over $\mathbb{F}$ is *congruent to a direct sum of pairs of the form

(a) $([F_n \diagdown F_n^*], [G_n \diagdown G_n^*])$,

(b) $([I_n \diagdown I_n], [\Phi \diagdown \Phi^*])$ if Φ_1 does not exist,

(c) $A_\Phi^{f(x)} := (\Phi_\delta, \Phi_1\Phi)f(\Phi)$, in which $0 \neq f(x) = \bar{f}(x) \in \mathbb{F}[x]$ and $\deg(f(x)) < \deg(p_\Phi(x))$.

(d) B_n^a (defined in (12)), in which $0 \neq a = \bar{a} \in \mathbb{F}$.

Consider each of these summands.

Summands (a). Theorem 2.3(b) ensures that the summands of the form (a) are uniquely determined by (A, B), which gives the summands (i) of the theorem.

Summands (b). By Lemma 2.7(a), Φ_1 does not exist if and only if $p_\Phi(x) \neq \bar{p}_\Phi(x)$; that is, $p_\Phi(x) \notin \mathbb{F}_\circ[x]$. Theorem 2.3(b) ensures that the summands of the form (b) are uniquely determined, up to replacement of Φ by Ψ with $\chi_\Psi(x) = \bar{\chi}_\Phi(x)$. This gives the summands (ii).

Summands (c). Consider the whole group of summands of the form $A_\Phi^{f(x)}$ with the same nonsingular Frobenius block Φ:

$$A_\Phi^{f_1(x)} \oplus \dots \oplus A_\Phi^{f_s(x)}. \tag{83}$$

By Lemma 4.2, the Hermitian form

$$f_1(\omega)x_1^\circ y_1 + \cdots + f_s(\omega)x_s^\circ y_s$$

over $\mathbb{F}(\omega) = \mathbb{F}[x]/p_\Phi(x)\mathbb{F}[x]$ with involution $f(\omega)^\circ = \bar{f}(\omega)$ is equivalent to either $x_1^\circ y_1 + \cdots + x_s^\circ y_s$, or $tx_1^\circ y_1 + x_2^\circ y_2 + \cdots + x_s^\circ y_s$, in which t is defined in (56). Theorem 2.2(b) ensures that (80) is *congruent to

$$\text{either} \quad A_\Phi^1 \oplus \cdots \oplus A_\Phi^1, \qquad \text{or} \quad A_\Phi^1 \tilde{t}(\Phi) \oplus A_\Phi^1 \oplus \cdots \oplus A_\Phi^1,$$

in which $\tilde{t}(x) \in \mathbb{F}[x, x^{-1}]$ is the function of the form (8) such that $\tilde{t}(\kappa) = t$. This sum is uniquely determined by (A, B), which gives the summands (iii).

Summands (d). Consider the whole group of summands of the form B_n^a with the same n:

$$B_n^{a_1} \oplus \cdots \oplus B_n^{a_s}. \tag{84}$$

By Lemma 4.2, the Hermitian form

$$a_1 x_1^\circ y_1 + \cdots + a_s x_s^\circ y_s$$

over $\mathbb{F}$ is equivalent either $x_1^\circ y_1 + \cdots + x_s^\circ y_s$, or $tx_1^\circ y_1 + x_2^\circ y_2 + \cdots + x_s^\circ y_s$, in which t is defined in (56). Theorem 2.2(b) ensures that (84) is *congruent to

$$\text{either} \quad B_n \oplus \cdots \oplus B_n, \qquad \text{or} \quad B_n \tilde{t}(\Phi) \oplus B_n \oplus \cdots \oplus B_n,$$

in which $\tilde{t}(x) \in \mathbb{F}[x, x^{-1}]$ is the function of the form (8) such that $\tilde{t}(\kappa) = t$. This sum is uniquely determined by (A, B), which gives the summands (iv). ☐

5 Appendix: Quadratic forms over finite extensions of p-adic fields

In this section, we recall some known results on quadratic forms over finite extensions of p-adic fields that are used in the paper.

Let $\mathbb{F}$ be a field and let ν be an *exponential variation* on $\mathbb{F}$; that is, a map $\nu : \mathbb{F} \to \mathbb{R} \cup \{+\infty\}$ with the properties

$$\nu(x) = +\infty \quad \Longleftrightarrow \quad x = 0, \tag{85}$$

$$\min\{\nu(x), \nu(y)\} \leqslant \nu(x + y), \tag{86}$$

$$\nu(x) + \nu(y) = \nu(xy) \tag{87}$$

for all $x, y \in \mathbb{F}$.

For example, the field $\mathbb{Q}_p$ of p-adic numbers possesses an exponential variation that is defined on each nonzero p-adic number as follows:

$$v(a_z p^z + a_{z+1} p^{z+1} + \dots) = z, \tag{88}$$

where $a_i \in \{0, 1, \dots, p-1\}$, $a_z \neq 0$, and $z \in \mathbb{Z}$.

In this section $\mathbb{F}$ denotes a finite extension of $\mathbb{Q}_p$, $p \neq 2$. In this case the exponential variation (20) can be extended to an exponential variation of $\mathbb{F}$. This variation is unique and is given by the formula:

$$\nu(a) = \frac{1}{n} v(N(a)) \qquad \text{for all } a \in \mathbb{F}, \tag{89}$$

in which $n := (\mathbb{F} : \mathbb{Q}_p) = \dim_{\mathbb{Q}_p} \mathbb{F}$ is the degree of $\mathbb{F}$ over $\mathbb{Q}_p$ and $N(a)$ is the *norm* of a in $\mathbb{F}$ over $\mathbb{Q}_p$; that is, the determinant of the linear mapping $x \mapsto xa$ on $\mathbb{F}$ as a vector space over $\mathbb{Q}_p$. If $x^m + \alpha_1 x^{m-1} + \dots + \alpha_m$ is the minimum polynomial of $a \in \mathbb{F}$ over $\mathbb{Q}_p$ then the variation (89) can be also given by the formula:

$$\nu(a) = \frac{1}{m} v(\alpha_m) \qquad \text{for all } a \in \mathbb{F}. \tag{90}$$

Note that there exists a natural number e such that $e\nu(\mathbb{F}^\times) = \mathbb{Z}$. The ring

$$\mathcal{O} := \{x \in \mathbb{F} \,|\, \nu(x) \geqslant 0\} \tag{91}$$

is called the *ring of integers* (with respect to ν);

$$\mathfrak{m} := \{x \in \mathbb{F} \,|\, \nu(x) > 0\} = \pi R \tag{92}$$

is the unique maximal ideal of R and its generator π is called a *prime element* (it is any element of $\mathbb{F}$ with the smallest positive $\nu(\pi)$; that is, $\nu(\pi) = 1/e$); the factor ring

$$\mathcal{O}/\mathfrak{m} \tag{93}$$

is a field, which is called the *residue field*; and the set

$$\mathcal{O}^\times := \{x \in \mathbb{F} \,|\, \nu(x) = 0\} \tag{94}$$

is the group of all invertible elements of $\mathcal{O}$ (which are called *units*).

The residue field $\mathcal{O}/\mathfrak{m}$ is an extension of the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$ and

$$e(\mathcal{O}/\mathfrak{m} : \mathbb{F}_p) = n = (\mathbb{F} : \mathbb{Q}_p) \tag{95}$$

By [9, Section VI, Theorem 2.2] or [13, Ch. 6, Facts 4.1] $\mathbb{F}^\times/\mathbb{F}^{\times 2}$ consists of 4 cosets, represented by $1,\ u,\ \pi,\ u\pi$, where $u \in \mathcal{O}^\times$ is a unit with $u \notin \mathbb{F}^{\times 2}$ (or, which is equivalent, with $u + \mathfrak{m} \notin (\mathcal{O}/\mathfrak{m})^{\times 2}$; see [4, Example 3.11], recall that $p \neq 2$).

The *Hilbert symbol* is defined for $a, b \in \mathbb{F}^\times$ by

$$(a,b)_{\mathbb{F}} := \begin{cases} 1 & \text{if } ax^2 + by^2 \text{ represents } 1, \\ -1 & \text{otherwise.} \end{cases} \tag{96}$$

The *Hasse invariant* of a form $q \sim a_1x_1^2 + a_2x_2^2 + \cdots + a_rx_r^2$ with $a_1, \ldots, a_r \in \mathbb{F}^\times$ is

$$c(q) := \prod_{i<j} (a_i, a_j)_{\mathbb{F}} \tag{97}$$

(see [10, Ch. VIII, p. 210]).

By [10, Ch. VIII, Theorem 4.10], two quadratic forms over $\mathbb{F}$ are equivalent if and only if they have the same rank n, the same discriminant d (in $\mathbb{F}^\times/\mathbb{F}^{\times 2}$), and the same Hasse invariant. By [10, Ch. VIII, Proposition 4.11], if q is a quadratic form of rank r, then

- If $r = 1$ then $c(q) = 1$.
- If $r = 2$ and $c(q) = -1$ then $d(q) \neq -1$ (mod squares).

Apart from these constraints, every triple $r \geqslant 1$, $d \in \{1,\ u,\ \pi,\ u\pi\}$ (mod squares), $c = \pm 1$ occurs as the set of invariants of a quadratic form over $\mathbb{F}$.

Theorem 5.1. *Let $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$. Let its residue field $\mathcal{O}/\mathfrak{m}$ consist of p^m elements. Let $u \in \mathcal{O}^\times \setminus \mathbb{F}^{\times 2}$ be a unit that is not a square, and π be a prime element. Then each quadratic form of rank $r \geqslant 1$ over $\mathbb{F}$ is equivalent to exactly one form*

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_tx_t^2 + x_{t+1}^2 + \cdots + x_r^2, \tag{98}$$

in which $(a_1, \ldots, a_t)$ is one of the sequences:

$$(1),\ (u),\ (\pi),\ (u\pi),\ (u,\pi),\ (u,u\pi), \tag{99}$$

$$\begin{cases} (\pi, u\pi),\ (u,\pi,u\pi) & \textit{if } p^m \equiv 1 \mod 4, \\ (\pi,\pi),\ (u,\pi,\pi) & \textit{if } p^m \equiv 3 \mod 4. \end{cases} \tag{100}$$

Proof. Let us show that the forms (98) give all possible invariant triples (r, d, c).

The forms (98) with $t = 1$ and $a_1 \in \{1,\ u,\ \pi,\ u\pi\}$ give all possible triples (r, d, c) with $c = 1$; in particular, all possible triples with $r = 1$.

The remaining forms (98) have the Hasse invariant $c = -1$ since:

• $(u, \pi)_{\mathbb{F}} = -1$ by [4, p. 53, Case 2].

• $(u, u\pi)_{\mathbb{F}} = (u, u)_{\mathbb{F}}(u, \pi)_{\mathbb{F}} = -1$ since $(u, u)_{\mathbb{F}} = 1$ by [4, p. 53, Case 1].

• $(\pi, \pi)_{\mathbb{F}} = (-1)^{(q-1)/2}$ by [4, p. 53, Case 3]. Thus, $(\pi, \pi)_{\mathbb{F}} = -1$ if $p^m \equiv 3 \mod 4$ and $(\pi, u\pi)_{\mathbb{F}} = (\pi, u)_{\mathbb{F}}(\pi, \pi)_{\mathbb{F}} = -1$ if $p^m \equiv 1 \mod 4$.

• If $p^m \equiv 3 \mod 4$ then the Hasse invariant of the form with triple (u, π, π) is $(u, \pi)_{\mathbb{F}}(u, \pi)_{\mathbb{F}}(\pi, \pi)_{\mathbb{F}} = (\pi, \pi)_{\mathbb{F}} = -1$. If $p^m \equiv 1 \mod 4$ then the Hasse invariant of the form with triple $(u, \pi, u\pi)$ is $(u, \pi)_{\mathbb{F}}(u, u\pi)_{\mathbb{F}}(\pi, u\pi)_{\mathbb{F}} = (u, u)_{\mathbb{F}}(u, \pi)^3_{\mathbb{F}}(\pi, \pi)_{\mathbb{F}} = (u, \pi)_{\mathbb{F}}(\pi, \pi)_{\mathbb{F}} = -1$.

In particular, we have 3 invariant triples with $r = 2$, $c = -1$, and

$$d \in \begin{cases} \{u\pi,\ \pi,\ u\} \text{ (mod squares)} & \text{if } p^m \equiv 1 \mod 4, \\ \{u\pi,\ \pi,\ 1\} \text{ (mod squares)} & \text{if } p^m \equiv 3 \mod 4. \end{cases}$$

But if $r = 2$ and $c = -1$ then d can have only 3 values (mod squares) since $d \neq -1$ (mod squares); thus, we have all possible invariant triples with $r = 2$.

We have all possible invariant triples with $r \geqslant 3$ and $c = -1$, since then $d \in \{1,\ u,\ \pi,\ u\pi\}$ (mod squares). $\square$

5.1 Irreducible polynomials over $\mathbb{Q}_p$

Let $f(x) \in \mathbb{Z}_p[x]$ be a monic polynomial whose reduction modulo p is irreducible in $\mathbb{F}_p[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$. [5, Corollary 5.3.8]

The Eisenstein criterion. Suppose that the polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{Z}_p[x]$ satisfies the conditions $p|a_i$ for all i and $p^2 \nmid a_n$. Then $f(x)$ is irreducible over $\mathbb{Q}_p$. [1, Theorem 5.5].

Let n and m be coprime natural numbers. Then the polynomial $x^n - p^m$ is irreducible over $\mathbb{Q}_p$. [1, Theorem 5.3].

5.2 Hermitian forms over local rings

Theorem 5.2. *Let $\mathbb{F}$ be a finite extension of $\mathbb{Q}_p$, $p \neq 2$, with a fixed non-identity involution. Let $\mathbb{F}_\circ$ be the fixed field with respect to this involution. Let $u \in \mathcal{O}(\mathbb{F}_\circ)^\times \setminus \mathbb{F}_\circ^{\times 2}$ be a unit that is not a square, and π be a prime element* *of* $\mathbb{F}_\circ$. *Then each regular (=with nonzero determinant) Hermitian form over* $\mathbb{F}$ *is equivalent to either*

$$\bar{x}_1 y_1 + \cdots + \bar{x}_n y_n,$$

or

$$\begin{cases} \pi\bar{x}_1 y_1 + \bar{x}_2 y_2 + \cdots + \bar{x}_n y_n & \text{if } \mathbb{F} = \mathbb{F}_\circ(\sqrt{u}), \\ u\bar{x}_1 y_1 + \bar{x}_2 y_2 + \cdots + \bar{x}_n y_n & \text{if } \mathbb{F} = \mathbb{F}_\circ(\sqrt{\pi}) \text{ or } \mathbb{F}_\circ(\sqrt{u\pi}). \end{cases}$$

Proof. Since $(\mathbb{F} : \mathbb{F}_\circ) = 2$, we have $\mathbb{F} = \mathbb{F}_\circ(\alpha)$, where α is a root of $f(x) = x^2 + 2ax + b \in \mathbb{F}_\circ[x]$. Write $\lambda := \alpha + a$, then $(\lambda - a)^2 + 2a(\lambda - a) + b = \lambda^2 - a^2 + b = 0$.

Therefore, we can take α such that $\alpha^2 = \beta \in \mathbb{F}_\circ$. Moreover, $(\alpha a)^2 = \beta a^2$ for each $a \in \mathbb{F}_\circ$. But $\mathbb{F}_\circ^\times/\mathbb{F}_\circ^{\times 2}$ consists of 4 cosets, represented by $1,\ u,\ \pi,\ u\pi$. Hence, we can take α such that

$$\alpha^2 = \beta \in \{1,\ u,\ \pi,\ u\pi\},$$

then $\mathbb{F}$ is $\mathbb{F}_\circ(\sqrt{u})$, or $\mathbb{F}_\circ(\sqrt{\pi})$, or $\mathbb{F}_\circ(\sqrt{u\pi})$. Since $\bar{\alpha}^2 = \beta$, the involution on $\mathbb{F}$ is $c + d\alpha \mapsto a - d\alpha$, $c, d \in \mathbb{F}_\circ$. The element

$$N(c + d\alpha) = (c + d\alpha)(c - d\alpha) = c^2 - d^2\beta \in \mathbb{F}_\circ$$

is the *norm* of $c + d\alpha$. The set $N(\mathbb{F}^\times)$ of norms of all nonzero elements is a group. By [13, Ch. 6, Fact 4.3], *the norm residue group* $\mathbb{F}_\circ^\times/N(\mathbb{F}^\times)$ *consists of* 2 *elements.*

- Let $\mathbb{F} = \mathbb{F}_\circ(\sqrt{u})$. Then $\alpha^2 = u$, $N(c+d\alpha) = c^2 - d^2 u$. If $\pi \in N(\mathbb{F}^\times)$ then there is $c + d\alpha$ such that $N(c + d\alpha) = c^2 - d^2 u = \pi$. Then $c^2 - d^2 u = 0 \mod \pi$; i.e. $u = (c/d)^2 \mod \pi$. A contradiction. Therefore, the cosets of $\mathbb{F}_\circ^\times/N(\mathbb{F}^\times)$ are represented by $1,\ \pi$.
- Let $\mathbb{F} = \mathbb{F}_\circ(\sqrt{\pi})$. Then $\alpha^2 = \pi$, $N(\alpha) = -\pi$. But $-\pi$ is a prime element too, so $1,\ u,\ -\pi,\ -u\pi$ represent 4 cosets of $\mathbb{F}_\circ^\times/\mathbb{F}_\circ^{\times 2}$. Thus, the cosets of $\mathbb{F}_\circ^\times/N(\mathbb{F}^\times)$ are represented by $1,\ u$.
- Let $\mathbb{F} = \mathbb{F}_\circ(\sqrt{u\pi})$. Then $\alpha^2 = u\pi$, $N(\alpha) = -u\pi$. But $-u\pi$ is a prime element too. Thus, the cosets of $\mathbb{F}_\circ^\times/N(\mathbb{F}^\times)$ are represented by $1,\ u$.

Let $\phi(x, y) = \alpha_1\bar{x}_1 y_1 + \cdots + \alpha_n\bar{x}_n y_n$ be a regular (all α_i are nonzero) Hermitian form over $\mathbb{F}$. Then the determinant $\det(\phi) := a_1 \dots a_n N(\mathbb{F}^\times) \in \mathbb{F}_\circ^\times/N(\mathbb{F}^\times)$ is an invariant of $\phi(x)$. By [13, Ch. 10, Example 1.6(ii)], regular Hermitian forms over $\mathbb{F}$ are classified by dimension and determinant. $\square$

References

[1] A.J. Baker, An Introduction to p-adic Numbers and p-adic Analysis, http://www.maths.gla.ac.uk/∼ajb

[2] T.S. Blyth, E.F. Robertson, *Further Linear Algebra*, Springer-Verlag, London, 2006.

[3] J.A. Diedonné, *La géométrie des groupes classiques*, 3me éd., Springer, 1971.

[4] Adam Gamzon, The Hasse-Minkowski Theorem, Honors Scholar Theses, University of Connecticut, 2006. (http://digitalcommons.uconn.edu/srhonors_theses/17)

[5] Fernando Quadros Gouvêa, P-Adic Numbers: An Introduction. Springer, 1993.

[6] R.A. Horn, V.V. Sergeichuk, Congruence of a square matrix and its transpose, *Linear Algebra Appl.* 389 (2004) 347–353.

[7] R.A. Horn, V.V. Sergeichuk, Canonical forms for complex matrix congruence and *congruence, *Linear Algebra Appl.* 416 (2006) 1010–1032.

[8] R.A. Horn, V.V. Sergeichuk, Canonical matrices of bilinear and sesquilinear forms, *Linear Algebra Appl.* 428 (2008) 193–223.

[9] T.Y. Lam, Introduction to quadratic forms over fields, American Mathematical Society, Providence, Rhode Island, 2005.

[10] J.S. Milne, Class field theory, 1997, Chapter VIII (http://www.jmilne.org/math/CourseNotes/math776.html)

[11] A.V. Roiter, Bocses with involution, in: *Representations and quadratic forms*, Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev, 1979, 124–128 (in Russian).

[12] R. Scharlau, Paare alternierder Formen, Math. Z. 147 (1976) 13–19.

[13] W. Scharlau, Quadratic and Hermitian Forms, Grundlehren der Math. Wiss. 270, Springer-Verlag, 1985.

[14] V.V. Sergeichuk, Representations of simple involutive quivers, in: *Representations and quadratic forms*, Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev, 1979, 127–148 (in Russian).

[15] V.V. Sergeichuk, Classification problems for systems of forms and linear mappings, *Math. USSR–Izv.* 31 (1988) 481–501. (arXiv ???)

[16] V.V. Sergeichuk, Canonical matrices of isometric operators on indefinite inner product spaces, *Linear Algebra Appl.* 428 (2008) 154–192.

[17] R.C. Thompson, Pencils of complex and real symmetric and skew matrices, Linear Algebra Appl. 147 (1991) 323–371.