When does a linear map belong to at least one orthogonal or symplectic group?

Clément de Seguins Pazzis

Lycée Privé Sainte-Geneviève, 2 rue de l'École des Postes, 78029 Versailles Cedex, France

ARTICLE INFO

ABSTRACT

Given an endomorphism u of a finite-dimensional vector space over an arbitrary field $\mathbb{K}$, we give necessary and sufficient conditions for the existence of a regular quadratic form (respectively, a symplectic form) for which u is orthogonal (respectively, symplectic). Since a solution to this problem is already known in the case $\mathrm{char}(\mathbb{K}) \neq 2$, our main contribution lies in the case $\mathrm{char}(\mathbb{K}) = 2$. When $\mathrm{char}(\mathbb{K}) = 2$, we also give necessary and sufficient conditions for the existence of a regular symmetric bilinear form for which u is orthogonal. When $\mathbb{K}$ is finite with characteristic 2, we give necessary and sufficient conditions for the existence of an hyperbolic quadratic form (respectively, a regular non-hyperbolic quadratic form, respectively, a regular nonalternate symmetric bilinear form) for which u is orthogonal.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

1.1. The problem

In this paper, $\mathbb{K}$ denotes an arbitrary field and $\mathrm{char}(\mathbb{K})$ is its characteristic. We choose an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. We use the French convention for integers: $\mathbb{N}$ denotes the set of non-negative integers, and $\mathbb{N}^* := \mathbb{N} \smallsetminus \{0\}$ the set of positive ones. Given integers a and b, we denote by $[\![a, b]\!]$ the set of all *integers n* such that $a \leqslant n \leqslant b$.

We denote by $\mathrm{M}_n(\mathbb{K})$ the algebra of square matrices with n rows and entries in $\mathbb{K}$. A matrix A of $\mathrm{M}_n(\mathbb{K})$ is called **alternate** when it is skew-symmetric with zero diagonal entries, i.e., $\forall X \in$

E-mail address: dsp.prof@gmail.com

$\mathbb{K}^n$, $X^T A X = 0$ (of course, when char$(\mathbb{K}) \neq 2$, the alternate matrices of $M_n(\mathbb{K})$ are its skew-symmetric matrices).

Similarity of two matrices A and B is written $A \sim B$. For $k \in \mathbb{N}^*$ and $\lambda \in \mathbb{K}$, we denote by $J_k(\lambda) \in M_k(\mathbb{K})$ the Jordan matrix of order k with eigenvalue λ.

Given a monic polynomial $P = x^n - \sum_{k=0}^{n-1} a_k x^k \in \mathbb{K}[x]$, we denote by

$$C(P) := \begin{bmatrix} 0 & & & 0 & a_0 \\ 1 & 0 & & & a_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & & 0 & a_{n-2} \\ 0 & & & 1 & a_{n-1} \end{bmatrix}$$

its **companion matrix**.

Given a vector space V over $\mathbb{K}$, we denote by GL(V) the group of linear automorphisms of V.

A **symplectic form** is a non-degenerate alternate form. For such a form b on a vector space V, a **symplectic morphism** of (V, b) is an automorphism u of V such that $\forall (x, y) \in V^2,\ b(u(x), u(y)) = b(x, y)$.

The reduction of special endomorphisms (e.g. selfadjoint endomorphisms, orthogonal – or unitary – endomorphisms, normal endomorphisms) plays an important part in the study of real and complex vector spaces. The generalization to an arbitrary quadratic or symplectic form, however, is much more difficult (see the early treatments in [1,2,8,14,15]). A complete classification of selfadjoint, skew-selfadjoint and orthogonal automorphisms is however known up to the classification of hermitian forms when char$(\mathbb{K}) \neq 2$ (see [10,11])

Instead of trying to find canonical forms for special morphisms in this setting, an easier problem is to find necessary and sufficient conditions for an endomorphism to be selfadjoint, skew-selfadjoint or orthogonal for at least one regular quadratic form (or for a symplectic form). The first important result on the topic was obtained by Frobenius [3], who proved that every endomorphism of a finite-dimensional vector space V is selfadjoint for at least one regular symmetric bilinear form on V (to put things differently, every square matrix is the product of two symmetric matrices, one of which is nonsingular). Later, Stenzel [12] determined when an endomorphism could be skew-selfadjoint for a regular quadratic form, or selfadjoint or skew-selfadjoint for a symplectic form: he only tackled the case of complex vector spaces but his results were later generalized to an arbitrary field [6].

In this paper, we tackle the case of the automorphisms of a finite-dimensional vector space that are orthogonal (respectively, symplectic) for at least one regular quadratic form (respectively, symplectic form). In Chapter XI of [4] and more recently in [7], this problem is solved for orthogonal morphisms when the underlying field is $\mathbb{C}$, but the proof generalizes to an arbitrary algebraically closed field of characteristic not 2 (this yields the possible Jordan canonical forms of the matrices in the orthogonal group $O_n(\mathbb{C})$). The solution for symplectic morphisms is also known [5] for algebraically closed fields of characteristic not 2. The deep results from [10] yield the solution to both problems for an arbitrary field of characteristic not 2.

Here, we completely solve the problem for an arbitrary field, possibly of characteristic 2. Although the results are already known in the case char$(\mathbb{K}) \neq 2$, we reprove them along the way since doing so has a low additional cost.

Definition 1. Let $u \in$ GL(V) for some finite-dimensional vector space V over $\mathbb{K}$. We say that u is:

- **essentially orthogonal** when u is q-orthogonal for some regular quadratic form q on V, i.e., $\forall x \in V,\ q(u(x)) = q(x)$;
- **essentially bilin-orthogonal** when u is an isometry for some regular symmetric bilinear form b on V, i.e., $\forall (x, y) \in V^2,\ b(u(x), u(y)) = b(x, y)$;
- **essentially symplectic** when u is a symplectic morphism for some symplectic form b on V, i.e., $\forall (x, y) \in V^2,\ b(u(x), u(y)) = b(x, y)$.

When char$(\mathbb{K}) \neq 2$, the essentially orthogonal morphisms are the essentially bilin-orthogonal ones. When char$(\mathbb{K}) = 2$, the following implications hold:

u essentially orthogonal $\Rightarrow$ u essentially symplectic $\Rightarrow$ u essentially bilin-orthogonal.

Indeed, the polar form of a regular quadratic form is symplectic.

Our main problem may now be stated: determine canonical forms for essentially orthogonal, essentially bilin-orthogonal, and essentially symplectic morphisms.

We adapt the same definitions to square matrices: notice then that the set of essentially orthogonal (respectively, essentially bilin-orthogonal, respectively, essentially symplectic) matrices of $M_n(\mathbb{K})$ is invariant under similarity, and we have the following characterizations:

- a matrix $M \in GL_n(\mathbb{K})$ is essentially symplectic if and only if $M^T A M = A$ for some nonsingular alternate matrix A;
- a matrix $M \in GL_n(\mathbb{K})$ is essentially bilin-orthogonal if and only if $M^T S M = S$ for some nonsingular symmetric matrix S;
- if char$(\mathbb{K}) = 2$, then $M \in GL_n(\mathbb{K})$ is essentially orthogonal if and only if there exists $A \in M_n(\mathbb{K})$ such that $M^T A M + A$ is alternate and the alternate matrix $A + A^T$ is nonsingular.

Let $M \in GL_n(\mathbb{K})$ have one of the above properties. Then there exists a nonsingular matrix $A \in GL_n(\mathbb{K})$ such that $M = A^{-1}(M^{-1})^T A$, hence M must be similar to $(M^{-1})^T$. However, $(M^{-1})^T$ is itself similar to M^{-1} (see [13]).

Proposition 1. *Let $M \in GL_n(\mathbb{K})$ which is either essentially orthogonal, essentially symplectic or essentially bilin-orthogonal. Then $M \sim M^{-1}$.*

As we shall see, the converse is not true (this is obvious for essentially symplectic morphisms since symplectic forms exist only in even dimensions).

1.2. Main results

Before stating our main theorems, we need a few extra definitions:

Definition 2. A polynomial $P(x) \in \mathbb{K}[x]$ has **valuation** 0 if $P(0) \neq 0$. Given a monic polynomial $P = \sum_{k=0}^{n} a_k x^k \in \mathbb{K}[x]$ of degree n and valuation 0, we define $P^{\#} := \frac{1}{a_0} \sum_{k=0}^{n} a_{n-k} x^k$ and call it the **reciprocal polynomial** of P. We say that P is a **palindromial** when $P = P^{\#}$.

Remark that when $P = \prod_{k=1}^{n}(x - \lambda_k)$, one has $P^{\#} = \prod_{k=1}^{n}(x - \frac{1}{\lambda_k})$. Moreover, the map $P \mapsto P^{\#}$ defines an involution on the set of monic polynomials of $\mathbb{K}[x]$ with valuation 0 and satisfies $(PQ)^{\#} = P^{\#} Q^{\#}$ for all such polynomials: in particular, it preserves divisibility and irreducibility.

We now state our main results.

Theorem 2. *Let $A \in GL_n(\mathbb{K})$. The following conditions are equivalent:*

- *(i) A is essentially symplectic.*
- *(ii) A is similar to A^{-1} and, for every $k \in \mathbb{N}$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k + 1$ associated to A is even.*
- *(iii) $\forall \lambda \in \overline{\mathbb{K}} \setminus \{0, 1, -1\}$, $\forall k \in \mathbb{N}^*$, $rk(A - \lambda I_n)^k = rk(A - \frac{1}{\lambda} I_n)^k$ and, for every $k \in \mathbb{N}$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k + 1$ associated to A is even.*
- *(iv) All the elementary factors of A are palindromials and, for every $k \in \mathbb{N}$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k + 1$ associated to A is even.*

(v) *There are nonsingular matrices B and C such that $A \sim B \oplus B^{-1} \oplus C$, all the elementary factors of C are palindromials and C contains only even-sized Jordan blocks for the eigenvalues 1 and -1.*

Theorem 3. *Let $A \in \mathrm{GL}_n(\mathbb{K})$ and assume that $\mathrm{char}(\mathbb{K}) = 2$. The following conditions are equivalent:*

(i) *A is essentially bilin-orthogonal.*
(ii) *A is similar to A^{-1} and, for every $k \in \mathbb{N}^*$, the number of Jordan blocks of size $2k + 1$ associated to A for the eigenvalue 1 is even.*
(iii) *$\forall \lambda \in \overline{\mathbb{K}} \smallsetminus \{0, 1\}$, $\forall k \in \mathbb{N}^*$, $\mathrm{rk}(A - \lambda I_n)^k = \mathrm{rk}(A - \frac{1}{\lambda} I_n)^k$ and, for every $k \in \mathbb{N}^*$, the number of Jordan blocks of size $2k + 1$ associated to A for the eigenvalue 1 is even.*
(iv) *All the elementary factors of A are palindromials and, for every $k \in \mathbb{N}^*$, the number of Jordan blocks of size $2k + 1$ associated to A for the eigenvalue 1 is even.*
(v) *There are nonsingular matrices B and C such that $A \sim B \oplus B^{-1} \oplus C$, all the elementary factors of C are palindromials and each Jordan block of C for the eigenvalue 1 is either even-sized or has size 1.*

Theorem 4. *Let $A \in \mathrm{GL}_n(\mathbb{K})$ and assume that $\mathrm{char}(\mathbb{K}) \neq 2$. The following conditions are equivalent:*

(i) *A is essentially orthogonal.*
(ii) *A is similar to A^{-1} and, for every $k \in \mathbb{N}^*$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k$ associated to A is even.*
(iii) *$\forall \lambda \in \overline{\mathbb{K}} \smallsetminus \{0, 1, -1\}$, $\forall k \in \mathbb{N}^*$, $\mathrm{rk}(A - \lambda I_n)^k = \mathrm{rk}(A - \frac{1}{\lambda} I_n)^k$ and, for every $k \in \mathbb{N}^*$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k$ associated to A is even.*
(iv) *All the elementary factors of A are palindromials and, for every $k \in \mathbb{N}^*$ and each one of the eigenvalues 1 and -1, the number of Jordan blocks of size $2k$ associated to A is even.*
(v) *There are nonsingular matrices B and C such that $A \sim B \oplus B^{-1} \oplus C$, all the elementary factors of C are palindromials and C contains only odd-sized Jordan blocks for the eigenvalues 1 and -1.*

Theorem 5. *If $\mathrm{char}(\mathbb{K}) = 2$, then the essentially orthogonal matrices of $\mathrm{M}_n(\mathbb{K})$ are its essentially symplectic ones.*

When n is even, condition (iii) in Theorem 3 implies that the number of Jordan blocks of size 1 for A is even: this shows that being essentially bilin-orthogonal is the same as being essentially symplectic (whereas not every non-degenerate symmetric bilinear form is symplectic).

Structure of the paper: In Section 2, we reduce the proofs of Theorems 2–5 to the following elementary cases:

- A is similar to $B \oplus B^{-1}$ for some nonsingular matrix B (this is easily dealt with in Section 2.3).
- A is **unipotent** i.e., triangularizable with 1 as its sole eigenvalue: see Section 3.2 for the necessary condition for A to be essentially orthogonal (respectively, symplectic, respectively, bilin-orthogonal), and Section 3.3 for the sufficient condition.
- A is the companion matrix of P^a for some integer $a \geqslant 1$ and some irreducible palindromial P of degree greater than 1 (see Section 4 for the fact that such a matrix is always essentially orthogonal and essentially symplectic, hence also essentially bilin-orthogonal). When $\mathbb{K}$ is finite, this involves field extensions and hermitian forms.

The last two sections deal with refinements of the above theorems for specific fields of characteristic 2. In Section 5, we determine, when $\mathbb{K}$ is perfect and $\mathrm{char}(\mathbb{K}) = 2$, the bilin-orthogonal automorphisms u that are orthogonal for at least one nonalternate regular symmetric bilinear form, i.e., we determine the matrices that are similar to a matrix of the orthogonal group $\mathrm{O}_n(\mathbb{K})$. In Section 6, we investigate the essentially orthogonal morphisms when $\mathbb{K}$ is finite and has characteristic 2. In that case, there are

exactly two equivalence classes of regular quadratic forms on a given even-dimensional vector space V over $\mathbb{K}$ (namely, the hyperbolic and the non-hyperbolic ones), and we give necessary and sufficient conditions for an automorphism of V to be orthogonal for at least one regular quadratic form belonging to a given equivalence class.

2. Reducing the problem to more elementary ones

2.1. Two basic principles

Let A and B be two essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilin-orthogonal) matrices. Since the orthogonal direct sum of two regular quadratic forms (respectively, symplectic forms, respectively, symmetric bilinear forms) is regular, the matrix $A \oplus B :=$ $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ is essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilin-orthogonal).

Notice also that if A is an essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilin-orthogonal) matrix, then its opposite matrix $-A$ is also essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilin-orthogonal).

2.2. When is a nonsingular matrix similar to its inverse?

The following characterizations are known but we prove them as they are crucial to our study:

Proposition 6. Let $A \in \mathrm{GL}_n(\mathbb{K})$. The following conditions are then equivalent:

- (i) A is similar to A^{-1}.
- (ii) $\forall \lambda \in \overline{\mathbb{K}} \smallsetminus \{0\}$, $\forall k \in \mathbb{N}^*$, $\mathrm{rk}(A - \lambda I_n)^k = \mathrm{rk}(A - \frac{1}{\lambda} I_n)^k$.
- (iii) The elementary factors of A are all palindromials.
- (iv) There are nonsingular matrices B and C such that $A \sim B \oplus B^{-1} \oplus C$ and all the irreducible monic factors in the minimal polynomial of C are palindromials.

Proof.
- The equivalence between (i) and (ii) is straightforward since $\mathrm{rk}(A^{-1} - \lambda I_n)^k = \mathrm{rk}\, A^{-k}(A - \frac{1}{\lambda} I_n)^k = \mathrm{rk}(A - \frac{1}{\lambda} I_n)^k$ for every $\lambda \in \overline{\mathbb{K}} \smallsetminus \{0\}$ and $k \in \mathbb{N}^*$.
- Given a monic polynomial $P \in \mathbb{K}[x]$ with valuation 0, notice that the companion matrix $C(P)$ has a cyclic inverse with minimal polynomial $P^{\#}$, and hence is similar to $C(P^{\#})$. As $P \mapsto P^{\#}$ preserves divisibility, if the elementary factors of A are $P_1, \ldots, P_N$, then the elementary factors of A^{-1} are $P_1^{\#}, \ldots, P_N^{\#}$: this proves (i) $\Leftrightarrow$ (iii).
- Let B be a nonsingular matrix, let C be a square matrix all whose elementary factors are palindromials, and assume that $A \sim B \oplus B^{-1} \oplus C$. Then

$$A^{-1} \sim B^{-1} \oplus B \oplus C^{-1} \sim B^{-1} \oplus B \oplus C \sim A$$

by applying (iii) $\Rightarrow$ (i) to C. Therefore (iv) $\Rightarrow$ (i).
- Implication (iii) $\Rightarrow$ (iv) needs to be proved only when A is a companion matrix. Assume then that $A = C(P)$ for some palindromial $P \in \mathbb{K}[x]$. Then the involution $Q \mapsto Q^{\#}$ must permute the irreducible factors of P, therefore we may write

$$P = \prod_{i=1}^{p} Q_i^{\alpha_i} (Q_i^{\#})^{\alpha_i} \prod_{j=1}^{q} R_j^{\beta_j},$$

where $Q_1, \ldots, Q_p, R_1, \ldots, R_q$ are irreducible and monic, $Q_1, \ldots, Q_p, Q_1^{\#}, \ldots, Q_p^{\#}, R_1, \ldots, R_q$ are all different, $R_1, \ldots, R_q$ are palindromials, and $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$ are positive integers.

It follows that

$$A \sim \bigoplus_{i=1}^{p} C(Q_i^{\alpha_i}) \ \oplus \ \bigoplus_{i=1}^{p} C((Q_i^{\#})^{\alpha_i}) \ \oplus \ \bigoplus_{j=1}^{q} C(R_j^{\beta_j}).$$

Setting $B := \bigoplus_{i=1}^{p} C(Q_i^{\alpha_i})$ and $C := \bigoplus_{j=1}^{q} C(R_j^{\beta_j})$, we then have

$$A \sim B \oplus B^{-1} \oplus C$$

and all the irreducible monic factors in the minimal polynomial of C are palindromials. $\square$

Using the same techniques as in the preceding proof, the equivalence between statements (ii) to (v) in each one of Theorems 2, 3 and 4 is obvious and we shall give no further details about it. In each of these theorems, it remains to prove only implications (i) $\Rightarrow$ (ii) and (v) $\Rightarrow$ (i).

2.3. Matrices of the form $B \oplus B^{-1}$

The case of matrices of the form $B \oplus B^{-1}$ is the easiest one:

Proposition 7. *Let $B \in GL_n(\mathbb{K})$. Then the matrix $B \oplus B^{-1}$ is both essentially orthogonal and essentially symplectic.*

Proof. A previous remark shows that $B \oplus B^{-1}$ is similar to $A := B \oplus (B^T)^{-1}$, so it suffices to show that A is essentially orthogonal and essentially symplectic. Setting $S := \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$ and $K := \begin{bmatrix} 0 & -I_n \\ I_n & 0 \end{bmatrix}$, we see that S and K are both nonsingular, with S symmetric and K alternate. A straightforward computation shows that $A^T S A = S$ and $A^T K A = K$, hence A is essentially symplectic, and it is essentially orthogonal if $\mathrm{char}(\mathbb{K}) \neq 2$.

If nevertheless $\mathrm{char}(\mathbb{K}) = 2$, set $C := \begin{bmatrix} 0 & I_n \\ 0 & 0 \end{bmatrix}$ and notice that $C + C^T = K$ is nonsingular and $A^T C A + C = 0$, hence A is essentially orthogonal. $\square$

Notice also that the matrix $(1) \in M_1(\mathbb{K})$ is essentially bilin-orthogonal (any regular symmetric bilinear form on $\mathbb{K}$ is adapted to it).

Let us now see what remains to be proved of the implication (v) $\Rightarrow$ (i) in each theorem:

(a) We need to prove that for every irreducible palindromial $P \in \mathbb{K}[x]$ which has no root in $\{1, -1\}$, and every integer $a \geqslant 1$, the companion matrix of P^a is both essentially orthogonal and essentially symplectic.

(b) We need to prove that, when $\mathrm{char}(\mathbb{K}) \neq 2$, the Jordan matrix $J_{2k+1}(1)$ is essentially orthogonal for each $k \in \mathbb{N}$ (in which case this is also true of $J_{2k+1}(-1)$ since it is similar to $-J_{2k+1}(1)$).

(c) We need to prove that the Jordan matrix $J_{2k}(1)$ is essentially symplectic for each $k \in \mathbb{N}^*$ (in which case this is also true of $J_{2k}(-1)$), and essentially orthogonal for each $k \in \mathbb{N}^*$ when $\mathrm{char}(\mathbb{K}) = 2$.

Knowing this also yields Theorem 5 provided Theorem 2 holds: indeed, it shows that if $\mathrm{char}(\mathbb{K}) = 2$, then A is essentially orthogonal whenever it satisfies property (v) in Theorem 2.

2.4. Reducing (i) $\Rightarrow$ (ii) to the unipotent case

Here, we show that the implication (i) $\Rightarrow$ (ii) in Theorems 2–4 needs to be proved only in the case of a unipotent matrix. We already know that a matrix that is essentially orthogonal, essentially symplectic or essentially bilin-orthogonal is similar to its inverse, so we will not care anymore about this part of condition (ii).

Our starting point is the following basic lemma:

Proposition 8. *Let b be a regular bilinear form on a finite-dimensional vector space V, and assume that b is symmetric or alternate. Let $u \in \mathrm{GL}(V)$ be a b-isometry, i.e., $\forall (x, y) \in V^2$, $b(u(x), u(y)) = b(x, y)$. Let $P \in \mathbb{K}[x]$ be a monic polynomial with valuation 0. Then $\mathrm{Ker}\, P(u) = (\mathrm{Im}\, P^{\#}(u))^{\perp_b}$.*

Proof. The adjoint $u^{\star}$ of u with respect to b is u^{-1}. Writing $P = \sum_{k=0}^{n} a_k x^k$, with $a_n \neq 0$, and setting $Q := \sum_{k=0}^{n} a_{n-k} x^k$, we find that

$$P(u)^{\star} = P(u^{\star}) = P(u^{-1}) = Q(u) \circ u^{-n} = a_0\, P^{\#}(u) \circ u^{-n},$$

therefore $\mathrm{Im}\, P(u)^{\star} = \mathrm{Im}\, P^{\#}(u)$ and the claimed result follows from the classical identity $\mathrm{Ker}\, v = (\mathrm{Im}\, v^{\star})^{\perp_b}$, which holds for every endomorphism v of V. $\square$

Corollary 9. *Let b and u be as in the Proposition 8, and let P and Q be monic polynomials with valuation 0 such that $P^{\#}$ is prime with Q. Then $\mathrm{Ker}\, P(u) \perp_b \mathrm{Ker}\, Q(u)$.*

Proof. Indeed, $\mathrm{Ker}\, Q(u) \subset \mathrm{Im}\, P^{\#}(u)$ since $P^{\#}$ is prime with Q. $\square$

With the same assumptions, assume further that $\mathrm{char}(\mathbb{K}) \neq 2$ and split the minimal polynomial μ of u as $\mu = R(x)\, (x-1)^p (x+1)^q$ where R has no root in $\{1, -1\}$, hence neither does $R^{\#}$. The previous corollary and the kernel decomposition theorem show that $V = \mathrm{Ker}\, R(u) \overset{\perp_b}{\oplus} \mathrm{Ker}(u - \mathrm{id})^p \overset{\perp_b}{\oplus} \mathrm{Ker}\, (u+\mathrm{id})^q$, hence $\mathrm{Ker}(u-\mathrm{id})^p$ and $\mathrm{Ker}(u+\mathrm{id})^q$ are both regular b-spaces: we deduce that the restrictions of u to $\mathrm{Ker}(u-\mathrm{id})^p$ and $\mathrm{Ker}(u+\mathrm{id})^q$ are both isometries for regular bilinear forms which are symplectic (respectively, symmetric) if b is symplectic (respectively, symmetric): moreover, if u is essentially orthogonal, then its restrictions to $\mathrm{Ker}(u - \mathrm{id})^p$ and $\mathrm{Ker}(u + \mathrm{id})^q$ are essentially orthogonal. This leaves us with only two cases: $u - \mathrm{id}$ is nilpotent or $u + \mathrm{id}$ is nilpotent. However, in the second case, $(-u) - \mathrm{id}$ is nilpotent hence only the first case needs to be addressed (see Section 2.1).

The case $\mathrm{char}(\mathbb{K}) = 2$ is handled similarly and even more easily since only the eigenvalue 1 needs to be taken into account.

In order to prove implication (i) $\Rightarrow$ (ii) in Theorems 2–4, it suffices to prove the following result:

Proposition 10. *Let b be a regular bilinear form on a finite-dimensional vector space V, and $u \in \mathrm{GL}(V)$ be a b-isometry, i.e., $\forall (x, y) \in V^2$, $b(u(x), u(y)) = b(x, y)$. Assume that $u - \mathrm{id}_V$ is nilpotent.*

- *(a) If b is symplectic, then, for every $k \in \mathbb{N}$, the number of Jordan blocks of u with size $2k + 1$ is even.*
- *(b) If $\mathrm{char}(\mathbb{K}) = 2$ and b is symmetric, then, for every $k \in \mathbb{N}^*$, the number of Jordan blocks of u with size $2k + 1$ is even.*
- *(c) If $\mathrm{char}(\mathbb{K}) \neq 2$ and b is symmetric, then, for every $k \in \mathbb{N}^*$, the number of Jordan blocks of u with size $2k$ is even.*

3. The case of unipotent matrices

We start by giving two proofs of Proposition 10; the first one is short. The second one is substantially longer and may thus be skipped at first reading; it is, however, unavoidable in order to grasp fully the discussion featured in Section 6. Let b be a regular bilinear form, symmetric or alternate, on a finite-dimensional vector space V, and $u \in \mathrm{GL}(V)$ be a b-isometry such that $u - \mathrm{id}$ is nilpotent.

3.1. Short proof of Proposition 10

(i) Assume that b is symplectic. It then suffices to prove that $\mathrm{rk}(u - \mathrm{id})^{2k}$ is even for every $k \in \mathbb{N}$.

For every $k \in \mathbb{N}$ and every $x \in V$, one has

$$b(u^k(x), (u - \mathrm{id})^{2k}(x)) = b((u^{-1} - \mathrm{id})^k(u^k(x)), (u - \mathrm{id})^k(x))$$
$$= (-1)^k b((u - \mathrm{id})^k(x), (u - \mathrm{id})^k(x)) = 0.$$

This shows that the bilinear form $(x, y) \mapsto b(u^k(x), (u - \mathrm{id})^{2k}(y))$ is alternate, hence its rank is even. However its rank is that of $(u - \mathrm{id})^{2k}$ since $(x, y) \mapsto b(u^k(x), y)$ is non-degenerate (because $u \in \mathrm{GL}(V)$).

(ii) Assume now that b is symmetric and $\mathrm{char}(\mathbb{K}) = 2$. It suffices to prove that $\mathrm{rk}(u - \mathrm{id})^{2k}$ is even for every $k \in \mathbb{N}^*$.

Let $k \in \mathbb{N}^*$ and $x \in V$, and set $y := (u - \mathrm{id})^{k-1}(x)$. With the same computation as in (i),

$$b(u^k(x), (u - \mathrm{id})^{2k}(x)) = b((u - \mathrm{id})(y), (u - \mathrm{id})(y)) = b(u(y), u(y)) + b(y, y) = 0.$$

As in (i), this shows that $\mathrm{rk}(u - \mathrm{id})^{2k}$ is even.

(iii) Assume that b is symmetric and $\mathrm{char}(\mathbb{K}) \neq 2$. It then suffices to prove that $\mathrm{rk}(u - \mathrm{id})^{2k+1}$ is even for every $k \in \mathbb{N}$.

For every $k \in \mathbb{N}$ and every $x \in V$, setting $y := (u - \mathrm{id})^k(x)$, one finds:

$$b(u^k(u + \mathrm{id})(x), (u - \mathrm{id})^{2k+1}(x)) = b((\mathrm{id} - u)^k(u + \mathrm{id})(x), (u - \mathrm{id})^{k+1}(x))$$
$$= (-1)^k b((u + \mathrm{id})(y), (u - \mathrm{id})(y))$$
$$= (-1)^k (b(u(y), u(y)) - b(y, y)) = 0.$$

Setting $c : (x, y) \mapsto b(u^k(u + \mathrm{id})(x), y)$, we deduce that $(x, y) \mapsto c(x, (u - \mathrm{id})^{2k+1}(y))$ is alternate, hence its rank is even. However this rank is that of $(u - \mathrm{id})^{2k+1}$ since c is non-degenerate (indeed b is non-degenerate and $u^k \circ (u + \mathrm{id})$ is an automorphism of V since $\mathrm{char}(\mathbb{K}) \neq 2$ and u is unipotent).

3.2. Long proof of Proposition 10

Set $n := \dim V$. In this proof, orthogonality is always considered with respect to b unless specified otherwise.

Using the Jordan reduction theorem "block-wise" yields a decomposition [1]:

$$V = \bigoplus_{k=1}^{2n} \bigoplus_{i=1}^{k} V_{k,i},$$

where for every $k \in [\![1, n]\!]$, some $V_{k,i}$ might be $\{0\}$ and:

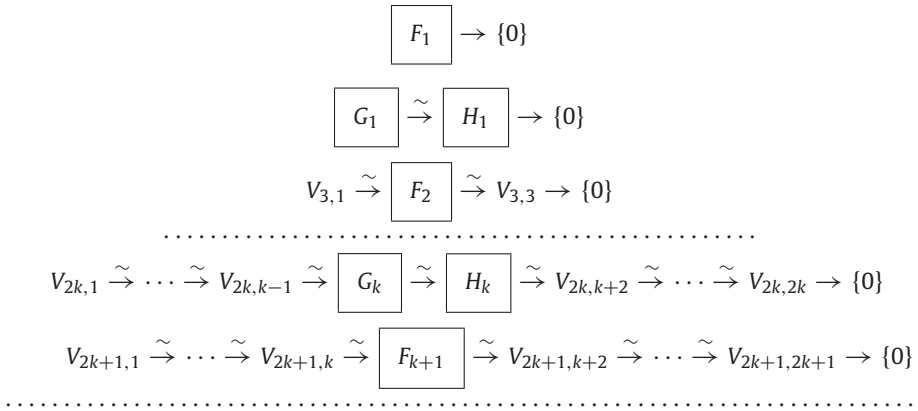- for every $i \in [\![1, k-1]\!]$, the linear map $u - \mathrm{id}$ induces an isomorphism from $V_{k,i}$ to $V_{k,i+1}$;
- $(u - \mathrm{id})(x) = 0$ for every $x \in V_{k,k}$.

Then $\mathrm{Ker}(u - \mathrm{id})^{k-1} \oplus \bigoplus_{i=k}^{2n} V_{i,i-k+1} = \mathrm{Ker}(u - \mathrm{id})^k$ for every $k \in \mathbb{N}^*$. For each $k \in [\![1, n]\!]$, set

$$F_k := V_{2k-1,k} \qquad G_k := V_{2k,k} \quad \text{and} \quad H_k = V_{2k,k+1}.$$

---

[1]   For convenience purpose, we use $2n$ instead of n as an upper bound for the first direct sum.

The following diagram accounts for the action of $u - $ id on the various spaces we have just defined.

$$\boxed{F_1} \to \{0\}$$

$$\boxed{G_1} \xrightarrow{\sim} \boxed{H_1} \to \{0\}$$

$$V_{3,1} \xrightarrow{\sim} \boxed{F_2} \xrightarrow{\sim} V_{3,3} \to \{0\}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$V_{2k,1} \xrightarrow{\sim} \cdots \xrightarrow{\sim} V_{2k,k-1} \xrightarrow{\sim} \boxed{G_k} \xrightarrow{\sim} \boxed{H_k} \xrightarrow{\sim} V_{2k,k+2} \xrightarrow{\sim} \cdots \xrightarrow{\sim} V_{2k,2k} \to \{0\}$$

$$V_{2k+1,1} \xrightarrow{\sim} \cdots \xrightarrow{\sim} V_{2k+1,k} \xrightarrow{\sim} \boxed{F_{k+1}} \xrightarrow{\sim} V_{2k+1,k+2} \xrightarrow{\sim} \cdots \xrightarrow{\sim} V_{2k+1,2k+1} \to \{0\}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Set

$$F := \bigoplus_{k=1}^{n} F_k, \quad G := \bigoplus_{k=1}^{n} G_k \quad \text{and} \quad H := \bigoplus_{k=1}^{n} H_k$$

and

$$E := \bigoplus_{k=1}^{2n} \bigoplus_{i=[(k+1)/2]+1}^{k} V_{k,i}.$$

Notice that $\dim F_k$ (respectively, $\dim G_k = \dim H_k$) is the number of Jordan blocks of size $2k - 1$ (respectively, $2k$) for u.

Proposition 8 yields:

$$\forall k \in \mathbb{N}^*, \quad \mathrm{Ker}(u - \mathrm{id})^k = \left[\mathrm{Im}(u - \mathrm{id})^k \right]^{\perp}.$$

For every $k \in [\![1, n]\!]$ and $i \in [\![1, k]\!]$, we see that $V_{k,i} \subset \mathrm{Ker}(u - \mathrm{id})^{k+1-i}$ and $V_{k,i} \subset \mathrm{Im}(u - \mathrm{id})^{i-1}$, and it follows that

$$E \perp (E \oplus F \oplus G \oplus H).$$

On the other hand, we notice that $\mathrm{codim}_V E = \dim(E \oplus F \oplus G \oplus H)$, therefore

$$E^{\perp} = E \oplus F \oplus G \oplus H$$

and we deduce that $F \oplus G \oplus H$ is b-regular.

Using again the relation $\mathrm{Ker}(u - \mathrm{id})^k \perp \mathrm{Im}(u - \mathrm{id})^k$ for each $k \in \mathbb{N}^*$, we find that for every $(k, l) \in [\![1, n]\!]^2$, $k \leqslant l$ implies $H_k \perp H_l$, and $k < l$ implies $F_k \perp F_l$ and $H_k \perp G_l$.

Finally, we work with $W := F \oplus G \oplus H$ equipped with the (symmetric or alternate) regular bilinear form b_W induced by b, and we consider the endomorphism v of W that coincides with u on G and is the identity on $F \oplus H$: since $(u - \mathrm{id})(F \oplus H)$ is included in E, and is therefore orthogonal to W, we find that v is a b_W-isometry with $\mathrm{Ker}(v - \mathrm{id}) = F \oplus H$ and $\mathrm{Im}(v - \mathrm{id}) = H$.

Claim 1. *For each $k \in [\![1, n]\!]$, the subspaces F_k and $G_k \oplus H_k$ are b-regular.*

Proof. Notice that $H^{\perp} = \mathrm{Im}(v - \mathrm{id})^{\perp} = \mathrm{Ker}(v - \mathrm{id}) = F \oplus H$ (orthogonality is now considered with respect to b_W).

We deduce that both F and $G \oplus H$ are b-regular. Since $F = F_1 \overset{\perp}{\oplus} F_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} F_n$, it follows that $F_1, \ldots, F_n$ are all b-regular.

Notice then that H_1 is orthogonal to $H_1 \oplus \overset{n}{\underset{k=2}{\oplus}} (G_k \oplus H_k)$. Since $\dim G_1 = \dim H_1$, we deduce that the orthogonal subspace of H_1 in $H \oplus G$ is $\overset{n}{\underset{k=2}{\oplus}} (G_k \oplus H_k)$, which shows that both $G_1 \oplus H_1$ and $\overset{n}{\underset{k=2}{\oplus}} (G_k \oplus H_k)$ are b-regular. Continuing by induction, we find that $G_k \oplus H_k$ is b-regular for each $k \in [\![1, n]\!]$. □

At this point, we may prove Proposition 10 by distinguishing between three cases:

(a) Assume that b is symplectic. Then, for each $k \in [\![1, n]\!]$, the restriction of b to $F_k \times F_k$ is symplectic, which shows that $\dim F_k$ is even.

(b) Assume that $\operatorname{char}(\mathbb{K}) = 2$ and b is symmetric. Let $k \in [\![2, n]\!]$. The key point is that the quadratic form $x \mapsto b(x, x)$ vanishes on F_k. Indeed, given $x \in F_k$, we may find some $y \in V_{2k-1,k-1}$ such that $x = u(y) - y$, hence $b(x, x) = b(u(y), u(y)) + b(y, y) = 0$ since b is skew-symmetric. It follows that b induces a symplectic form on F_k, hence $\dim F_k$ is even.

(c) Assume finally that $\operatorname{char}(\mathbb{K}) \neq 2$ and b is symmetric. Let $k \in [\![1, n]\!]$ and denote by v_k the endomorphism of $G_k \oplus H_k$ induced by v. Set $p := \dim H_k$. Then H_k is a totally isotropic subspace for b, hence we may find an hyperbolic basis $\mathbf{B}$ of $G_k \oplus H_k$ whose first p vectors belong to H_k. Since $H_k = \operatorname{Ker}(v_k - \mathrm{id}) = \operatorname{Im}(v_k - \mathrm{id})$, we find that $M_{\mathbf{B}}(v_k) = \begin{bmatrix} I_p & A \\ 0 & I_p \end{bmatrix}$ for some $A \in \operatorname{GL}_p(\mathbb{K})$.

Since $\mathbf{B}$ is hyperbolic and v_k is $b_{G_k \oplus H_k}$-orthogonal, a straightforward computation shows that A is skew-symmetric. Since $\operatorname{char}(\mathbb{K}) \neq 2$, this shows that $\dim H_k = p$ is even.

The proof of Proposition 10 is now complete, and it follows that implication (i) $\Rightarrow$ (ii) in Theorems 2, 3 and 4 is proved.

3.3. Jordan blocks with eigenvalue 1

Our aim here is to prove the following two results, which are already known in the case $\operatorname{char}(\mathbb{K}) \neq 2$. We reproduce the proof for the sake of completeness and because the strategy is to be reused later on.

Proposition 11. *Let $n \in \mathbb{N}^*$. Then the Jordan matrix $J_{2n}(1)$ is essentially symplectic. If $\operatorname{char}(\mathbb{K}) = 2$, then $J_{2n}(1)$ is also essentially orthogonal.*

Proposition 12. *Assume that $\operatorname{char}(\mathbb{K}) \neq 2$. Let $n \in \mathbb{N}$. Then the Jordan matrix $J_{2n+1}(1)$ is essentially orthogonal.*

Proof of Proposition 11. Let $A = (a_{i,j}) \in M_{2n}(\mathbb{K})$. A straightforward computation shows that $J_{2n}(1)^T A J_{2n}(1) = A$ if and only if both of the following conditions are satisfied:

(i) $a_{i,j-1} + a_{i-1,j} + a_{i-1,j-1} = 0$ for every $(i, j) \in [\![2, 2n]\!]^2$;
(ii) $a_{k,1} = a_{1,k} = 0$ for every $k \in [\![1, 2n - 1]\!]$.

We construct such a matrix $A \in M_{2n}(\mathbb{K})$ as follows:

• we set $a_{i,j} := 0$ whenever $i + j < 2n + 1$;
• we set $a_{i,2n+1-i} := (-1)^i$ for every $i \in [\![1, 2n]\!]$;
• we set $a_{i,j} := 0$ whenever $i > n$ and $j > n$;
• we then define (doubly-)inductively $a_{i,j}$ for i from n down to 2 and for j from $2n - i + 2$ up to $2n$ by $a_{i,j} := -a_{i,j-1} - a_{i+1,j-1}$;
• symmetrically, we define $a_{i,j}$ for j from n down to 2 and for i from $2n - j + 2$ up to $2n$ by $a_{i,j} := -a_{i-1,j} - a_{i-1,j+1}$.

One checks that A satisfies conditions (i) and (ii). Moreover, A has the form

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 0 & & & -1 & * \\ \vdots & & \cdot\cdot\cdot & & \\ 0 & 1 & & * & * \\ -1 & * & & * & * \end{bmatrix}$$

and hence A is nonsingular. Had we replaced the second point by $a_{2n+1-i,i} := (-1)^{i+1}$, the matrix would have been A^T since the other conditions are symmetrical. Since $a_{2n+1-i,i} = (-1)^{2n-i} = -(-1)^{i+1}$ and all the other conditions are linear, this shows that $A^T = -A$. As all the diagonal entries of A have been set to zero, this shows that A is alternate. Therefore $J_{2n}(1)$ is essentially symplectic.

Assume finally that $\text{char}(\mathbb{K}) = 2$ and choose an arbitrary symplectic form b for which $u : X \mapsto J_{2n}(1)X$ is a symplectic morphism. Then a (regular) quadratic form q with polar form b is determined by choosing $(q(e_1), \ldots, q(e_{2n}))$ arbitrarily in $\mathbb{K}^{2n}$ (where $(e_1, \ldots, e_{2n})$ is the canonical basis of $\mathbb{K}^{2n}$). Given such a form q, the map u is q-orthogonal if and only if $q(u(e_i)) = q(e_i)$ for every $i \in [\![1, 2n]\!]$, which is equivalent to having $q(e_{i-1}) = -b(e_i, e_{i-1})$ whenever $i \geqslant 2$. Obviously one may find a quadratic form q which fits these conditions (and we may even choose $q(e_{2n})$ as we please). $\square$

Proof of Proposition 12. Using the same arguments as in the previous proof, we see that it suffices to find a nonsingular symmetric matrix $A = (a_{i,j}) \in M_{2n+1}(\mathbb{K})$ which satisfies:

(i) $a_{i,j-1} + a_{i-1,j} + a_{i-1,j-1} = 0$ for every $(i, j) \in [\![2, 2n+1]\!]^2$;
(ii) $a_{k,1} = a_{1,k} = 0$ for every $k \in [\![1, 2n]\!]$.

We construct such a matrix $A \in M_{2n+1}(\mathbb{K})$ as follows:

- we set $a_{i,j} := 0$ whenever $i + j < 2n + 2$;
- we set $a_{i,2n+2-i} := (-1)^i$ for every $i \in [\![1, 2n+1]\!]$;
- we set $a_{i,j} := 0$ whenever $i > n + 1$ and $j > n + 1$;
- we set $a_{i,n+1} := \dfrac{(-1)^i}{2}$ whenever $i > n + 1$ and $a_{n+1,j} := \dfrac{(-1)^j}{2}$ whenever $j > n + 1$;
- we then define (doubly)-inductively $a_{i,j}$ for i from n down to 2 and for j from $2n - i + 3$ up to $2n + 1$ by $a_{i,j} := -a_{i,j-1} - a_{i+1,j-1}$;
- symmetrically, we define $a_{i,j}$ for j from n down to 2 and for i from $2n - j + 3$ up to $2n + 1$ by $a_{i,j} := -a_{i-1,j} - a_{i-1,j+1}$.

One checks that A satisfies conditions (i) and (ii) and is both symmetric and nonsingular, the key points being that $a_{n+1,n+1} + a_{n+1,n+2} + a_{n+2,n+1} = 0$ and $a_{n+1,n+2} = a_{n+2,n+1}$ (this is precisely where we need the assumption on the characteristic of $\mathbb{K}$). $\square$

4. The case of elementary companion matrices

In order to conclude our proof of Theorems 2–4, we must prove implication (v) $\Rightarrow$ (i) in each of them. By the considerations of Sections 2.2, 2.3, and 3.3, we must prove the following proposition:

Proposition 13. Let $P \in \mathbb{K}[x]$ be an irreducible palindromial with no root in $\{1, -1\}$, and let $a \in \mathbb{N}^*$. Then the companion matrix $C(P^a)$ is both essentially orthogonal and essentially symplectic.

We distinguish between two cases, whether $\mathbb{K}$ is finite or not.

4.1. The case of an infinite field

Assume that $\mathbb{K}$ is infinite, and notice that Proposition 13 holds trivially in $\overline{\mathbb{K}}$: indeed, any palindromial Q of $\overline{\mathbb{K}}[x]$ with degree 1 is $x - \lambda$ for some $\lambda \in \overline{\mathbb{K}} \smallsetminus \{0\}$ such that $\frac{1}{\lambda} = \lambda$, hence $\lambda = \pm 1$. It follows that Theorems 2, 3 and 4 all hold for the field $\overline{\mathbb{K}}$. It thus suffices to prove the following result:

Proposition 14. *Assume that $\mathbb{K}$ is infinite and let $\mathbb{L}$ be a field extension of $\mathbb{K}$. Let $A \in M_n(\mathbb{K})$, and assume that A is essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilinorthogonal) in $M_n(\mathbb{L})$. Then A is essentially orthogonal (respectively, essentially symplectic, respectively, essentially bilin-orthogonal) in $M_n(\mathbb{K})$.*

Proof. The line of reasoning here is classical.

- Assume that $A^T S A = S$ for some nonsingular symmetric matrix $S \in M_n(\mathbb{L})$. Choose a basis $(b_1, \ldots, b_p)$ of the $\mathbb{K}$-linear subspace of $\mathbb{L}$ spanned by the entries of S, and split up $S = b_1 S_1 + \cdots + b_p S_p$ where $S_1, \ldots, S_p$ are symmetric matrices of $M_n(\mathbb{K})$. Since $A \in M_n(\mathbb{K})$, we find that $A^T S_k A = S_k$ for every $k \in [\![1, p]\!]$, hence $A^T(x_1 S_1 + \cdots + x_p S_p)A = x_1 S_1 + \cdots + x_p S_p$ for every $(x_1, \ldots, x_p) \in \mathbb{K}^p$.

  The polynomial $\det(x_1 S_1 + \cdots + x_p S_p) \in \mathbb{K}[x_1, \ldots, x_p]$ is nonzero since $\det(b_1 S_1 + \cdots + b_p S_p) \neq 0$. As $\mathbb{K}$ is infinite, we deduce that we may find some $(x_1, \ldots, x_p) \in \mathbb{K}^p$ such that $\det(x_1 S_1 + \cdots + x_p S_p) \neq 0$. It follows that $S' := x_1 S_1 + \cdots + x_p S_p$ is a nonsingular symmetric matrix of $M_n(\mathbb{K})$ which satisfies $A^T S' A = S'$.

  This shows that A is essentially bilin-orthogonal over $\mathbb{K}$ if it is essentially bilin-orthogonal over $\mathbb{L}$.

- A similar argument shows that A is essentially symplectic over $\mathbb{K}$ if it is essentially symplectic over $\mathbb{L}$.

- Assume finally that $\mathrm{char}(\mathbb{K}) \neq 2$ and A is essentially orthogonal over $\mathbb{L}$. Choose $M \in M_n(\mathbb{L})$ such that $A^T M A + M$ is alternate and $M + M^T$ is nonsingular. As before, split up $M = b_1 M_1 + \cdots + b_p M_p$ where $M_1, \ldots, M_p$ are all matrices of $M_n(\mathbb{K})$ with $A^T M_k A + M_k$ alternate for each $k \in [\![1, p]\!]$, and $(b_1, \ldots, b_p) \in \mathbb{L}^p$ is linearly independent over $\mathbb{K}$. With the same argument as before, we see that we may find $(x_1, \ldots, x_p) \in \mathbb{K}^p$ such that $x_1(M_1 + M_1^T) + \cdots + x_p(M_p + M_p^T)$ is nonsingular, in which case $M' := x_1 M_1 + \cdots + x_p M_p$ is such that $A^T M' A + M'$ is alternate and $M' + (M')^T$ is nonsingular. This shows that if A is essentially orthogonal over $\mathbb{L}$, then it is essentially orthogonal over $\mathbb{K}$. $\square$

As a consequence of Theorems 2–5, Proposition 14 still holds when $\mathbb{K}$ is finite, although we do not know any direct proof of it.

4.2. The case of a finite field

When $\mathbb{K}$ is finite, we know that P, being irreducible, must be separable (i.e., it has distinct roots $x_1, \ldots, x_n$ in $\overline{\mathbb{K}}$). As we have seen earlier, we must have $n \geqslant 2$ (in fact, n is even since no root of P in $\overline{\mathbb{K}}$ is fixed by the involution $a \mapsto a^{-1}$). We introduce the quotient field $\mathbb{L} := \mathbb{K}[x]/(P(x))$ and denote by y the class of x in it. Since P is a palindromial, y^{-1} is another root of P in $\mathbb{L}$ hence we may find an automorphism σ of $\mathbb{L}$ over $\mathbb{K}$ such that $\sigma(y) = y^{-1}$. It follows that $\sigma^2(y) = \sigma(y^{-1}) = \sigma(y)^{-1} = y$, hence $\sigma^2 = \mathrm{id}$ because $\mathbb{L} = \mathbb{K}[y]$.

We then define the subfield $\mathbb{K}' = \{z \in \mathbb{L} : \sigma(z) = z\}$ of $\mathbb{L}$ and notice that $\mathbb{L}$ is a quadratic extension of $\mathbb{K}'$: indeed, $\mathbb{L} = \mathbb{K}'[y]$, and $(X - y)(X - \sigma(y))$ is the minimal polynomial of y on $\mathbb{K}'$ since $y \notin \mathbb{K}'$, $y\sigma(y) = 1$ and $y + \sigma(y) \in \mathbb{K}'$ (because $\sigma^2 = \mathrm{id}$).

By an hermitian matrix of $M_k(\mathbb{L})$, we mean an hermitian matrix with respect to the quadratic extension $\mathbb{K}' - \mathbb{L}$, i.e., a matrix $H \in M_k(\mathbb{L})$ which satisfies $\sigma(H)^T = H$.

Let us come back to the matrix $C(P^a)$ and remark that

$$C(P^a) \sim J_a(1) \otimes C(P).$$

There are numerous ways to prove this: we note that, over $\overline{\mathbb{K}}$,

$$
\begin{aligned}
C(P^a) &\sim C((x - x_1)^a) \oplus C((x - x_2)^a) \oplus \cdots \oplus C((x - x_n)^a) \\
&\sim J_a(x_1) \oplus J_a(x_2) \oplus \cdots \oplus J_a(x_n) \\
&\sim x_1 J_a(1) \oplus \cdots \oplus x_n J_a(1) \\
&\sim J_a(1) \otimes \mathrm{Diag}(x_1, \ldots, x_n) \\
&\sim J_a(1) \otimes C(P),
\end{aligned}
$$

and invoke the invariance of similarity when the ground field is extended. It then suffices to prove that $A := J_a(1) \otimes C(P)$ is both essentially orthogonal and essentially symplectic. Now set $D := I_a \otimes C(P)$ the block-diagonal matrix with a diagonal blocks all equal to $C(P)$. Then D has P as minimal polynomial hence D induces a structure of $\mathbb{L}$-vector space on $V := \mathbb{K}^{na}$. Moreover $u : X \mapsto AX$ is $\mathbb{L}$-linear since A commutes with D, and u is represented by the matrix $y.J_a(1)$ in some basis of the $\mathbb{L}$-vector space V.

We need the following result, which we will prove later:

Lemma 15. *There is a nonsingular hermitian matrix $H \in \mathrm{M}_a(\mathbb{L})$ such that $J_a(1)$ is H-unitary, i.e., $\sigma(J_a(1))^T H J_a(1) = H$, i.e., $J_a(1)^T H J_a(1) = H$.*

Fix such a matrix H and denote by $b : (X, Y) \mapsto \sigma(X)^T H Y$ the hermitian product on V (identified with $\mathbb{L}^a$) associated to it. Since $y\sigma(y) = 1$, we find that $y . \mathrm{id}_V$ is b-unitary, and we then deduce from the assumptions that u is b-unitary. Set finally

$$q : X \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(b(X, X))$$

and notice that q is a quadratic form on the $\mathbb{K}$-vector space V for which u is orthogonal.

Notice that for every $(X, Y) \in V^2$,

$$
\begin{aligned}
q(X + Y) - q(X) - q(Y) &= \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(b(X, Y) + b(Y, X)) = \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}\big(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}'}(b(X, Y))\big) \\
&= \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\, b(X, Y),
\end{aligned}
$$

and since b is non-degenerate, it follows that the polar form of q is also non-degenerate (whatever the value of char$(\mathbb{K})$).

Assume finally that char$(\mathbb{K}) \neq 2$. We may then choose $\varepsilon \in \mathbb{L} \setminus \mathbb{K}'$ such that $\sigma(\varepsilon) = -\varepsilon$, and classically

$$(X, Y) \mapsto \varepsilon\,(b(X, Y) - b(Y, X))$$

is a symplectic form on the $\mathbb{K}'$-vector space V for which u is a symplectic morphism. It follows that

$$(X, Y) \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}\big(\varepsilon(b(X, Y) - b(Y, X))\big)$$

is a symplectic form on the $\mathbb{K}$-vector space V for which u is a symplectic morphism. We may then finish the proof of Proposition 13 by establishing Lemma 15.

Proof of Lemma 15. Assume first that char$(\mathbb{K}) \neq 2$, and choose $\varepsilon \in \mathbb{L} \setminus \{0\}$ such that $\sigma(\varepsilon) = -\varepsilon$.

- If a is odd, we use Proposition 12 to find a nonsingular symmetric matrix $S \in \mathrm{M}_a(\mathbb{K})$ such that $J_a(1)^T S J_a(1) = S$ and we set $H := S$.
- If a is even, we use Proposition 11 to find a nonsingular alternate matrix $N \in \mathrm{M}_a(\mathbb{K})$ such that $J_a(1)^T N J_a(1) = N$, and we set $H := \varepsilon N$.

In any case, H has the claimed properties.

Assume now that $\mathrm{char}(\mathbb{K}) = 2$. If a is even, we find a nonsingular alternate matrix $N \in \mathrm{M}_n(\mathbb{K})$ such that $J_a(1)^T N J_a(1) = N$, and we notice that $H := N$ is hermitian. Assume finally that a is odd. Then $\mathbb{K}' = \mathrm{Ker}(\sigma + \mathrm{id})$. Choose $\alpha \in \mathbb{L} \setminus \mathbb{K}'$ and notice that $\beta := \alpha + \sigma(\alpha)$ belongs to $\mathbb{K}' \setminus \{0\}$. We write $a = 2b + 1$ for some integer b, and define $H \in \mathrm{M}_a(\mathbb{K})$ as follows:

- we set $h_{i,j} := 0$ whenever $i + j < 2b + 2$;
- we set $h_{i,2b+2-i} := \beta$ for every $i \in [\![1, 2b + 1]\!]$;
- we set $h_{i,j} := 0$ whenever $i > b + 1$ and $j > b + 1$;
- we set $h_{i,b+1} := \alpha$ whenever $i > b + 1$ and $h_{b+1,j} := \sigma(\alpha)$ whenever $j > b + 1$;
- we then define (doubly)-inductively $h_{i,j}$ for i from b down to 2 and for j from $2b - i + 3$ up to $2b + 1$ by $h_{i,j} := -h_{i,j-1} - h_{i+1,j-1}$;
- symmetrically, we define $h_{i,j}$ for j from b down to 2 and for i from $2b - j + 3$ up to $2b + 1$ by $h_{i,j} := -h_{i-1,j} - h_{i-1,j+1}$.

As in the proof of Proposition 11, one shows that H is nonsingular, hermitian, and $J_a(1)^T H J_a(1) = H$. □

This finishes our proof of implication (v) $\Rightarrow$ (i) in Theorems 2, 3 and 4. Therefore, all those theorems are proved, and Theorem 5 follows from them and from Proposition 13, as explained earlier.

5. Refinements for symmetric bilinear forms in characteristic 2

In this section, we assume that $\mathbb{K}$ has characteristic 2 and is *perfect* (e.g. $\mathbb{K}$ is finite or algebraically closed). Let $n \in \mathbb{N}^*$. Then the following results hold (see Chapter XXXV of [9]):

- if n is odd, the matrix I_n is, up to congruence, the sole nonsingular symmetric matrix of $\mathrm{M}_n(\mathbb{K})$;
- for every $n \in \mathbb{N}$, the matrix I_n is, up to congruence, the sole nonsingular nonalternate symmetric matrix of $\mathrm{M}_n(\mathbb{K})$.

When n is odd, we have successfully determined the Jordan canonical forms of the elements in the group $\mathrm{O}_n(\mathbb{K})$. Assume, for the rest of the section, that n is even. Then we have two congruence classes of symmetric matrices in $\mathrm{M}_n(\mathbb{K})$: the one of I_n and the one of $\begin{bmatrix} 0 & I_{n/2} \\ I_{n/2} & 0 \end{bmatrix}$. We have already classified the essentially symplectic morphisms, so we are now interested in the automorphisms that are orthogonal for some regular nonalternate symmetric bilinear form. A necessary condition for having this property is the following:

Proposition 16. *Let $u \in \mathrm{GL}(V)$ and assume that there is a regular nonalternate symmetric bilinear form b for which u is orthogonal.*

Then 1 is an eigenvalue of u.

Proof. We lose no generality in assuming that $V = \mathbb{K}^n$ and $b : (X, Y) \mapsto X^T Y$. Set $q : X \mapsto b(X, X)$, and notice that $q(x_1, \ldots, x_n) = (x_1 + \cdots + x_n)^2$ for every $(x_1, \ldots, x_n) \in \mathbb{K}^n$. Since $q \circ u = q$ and $\mathrm{char}(\mathbb{K}) = 2$, we deduce that the linear form $f : (x_1, \ldots, x_n) \mapsto x_1 + \cdots + x_n$ satisfies $f \circ u = f$. This proves that 1 is an eigenvalue of the transposed endomorphism $u^T : (\mathbb{K}^n)^\star \to (\mathbb{K}^n)^\star$, hence 1 is an eigenvalue of u. □

Remark 1. The result actually holds for an arbitrary field of characteristic 2, with a subtler proof (see exercise 17 in Chapter XXXV of [9]).

We shall see that the converse is true, which leads to the following theorem:

Theorem 17. *Assume that $\mathbb{K}$ is perfect of characteristic* 2, *and let $n \in \mathbb{N}^*$. Let $A \in \mathrm{GL}_{2n}(\mathbb{K})$. The following conditions are equivalent:*

> (i) *A is similar to a matrix of $\mathrm{O}_{2n}(\mathbb{K})$.*
> (ii) *A is essentially symplectic and* 1 *is an eigenvalue of A.*

For an arbitrary field of characteristic 2, condition (ii) characterizes the even-sized matrices that are orthogonal for at least one regular nonalternate symmetric bilinear form (use Remark 1).

In order to prove the theorem, we consider an essentially bilin-orthogonal morphism $u \in \mathrm{GL}(V)$, with $\dim V$ even, and assume that 1 is an eigenvalue of u. We need to find a nonalternate regular symmetric bilinear form b on V for which $u \in O(b)$. Notice that since $\dim V$ is even, three situations may arise:

> (a) There is a Jordan block of size 1 for the eigenvalue 1 of u, in which case the proof of implication $(v) \Rightarrow (i)$ in Theorem 3 gives an explicit construction of a nonalternate b (the key point being that $\mathrm{id}_{\mathbb{K}}$ is orthogonal for the nonalternate form $(x, y) \mapsto xy$).
> (b) At least one Jordan block of u for the eigenvalue 1 is even-sized: in this case, we define A almost as in the proof of Proposition 11 but set $a_{2n,2n} = 1$ instead of $a_{2n,2n} = 0$. One checks that this yields a regular nonalternate symmetric bilinear form for which $X \mapsto J_{2n}X$ is orthogonal. Using the method of the proof of implication $(v) \Rightarrow (i)$ in Theorem 3, we find a well-suited b for u.
> (c) There is an integer $k \geqslant 1$ such that u has a Jordan block of size $2k + 1$ for the eigenvalue 1; since u is essentially bilin-orthogonal, it has an even number of such blocks (with k fixed); rather than use all these blocks to form a matrix of type $B \oplus B^{-1}$, we may keep a pair of them separated from the rest and try to prove directly that their direct sum is orthogonal for some nonalternate regular symmetric bilinear form. If this is true, then the same arguments as before show that we may find a well-suited b for u.

In order to conclude our proof of Theorem 17, it suffices to establish the following lemma:

Lemma 18. *Let $n \in \mathbb{N}^*$. Then there is a nonalternate nonsingular symmetric matrix $S \in \mathrm{M}_{4n+2}(\mathbb{K})$ such that $J_{2n+1}(1) \oplus J_{2n+1}(1)$ is S-orthogonal.*

Proof. We work with

$$J_{2n+1}(1) \otimes I_2 = \begin{bmatrix} I_2 & I_2 & & (0) \\ 0 & I_2 & \ddots & \\ & & \ddots & I_2 \\ (0) & & 0 & I_2 \end{bmatrix},$$

which is similar to $J_{2n+1}(1) \oplus J_{2n+1}(1)$. We search for a suitable S of the form

$$\begin{bmatrix} S_{1,1} & S_{1,2} & \cdots & S_{1,2n+1} \\ S_{2,1} & S_{2,2} & \cdots & S_{2,2n+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{2n+1,1} & S_{2n+1,2} & \cdots & S_{2n+1,2n+1} \end{bmatrix},$$

where the $S_{i,j}$'s are 2×2 matrices. The condition that $J_{2n+1}(1) \otimes I_2$ is S-orthogonal is equivalent to having:

(i) $S_{i,j-1} + S_{i-1,j} + S_{i-1,j-1} = 0$ for every $(i,j) \in [\![2, 2n+1]\!]^2$;

(ii) $S_{k,1} = S_{1,k} = 0$ for every $k \in [\![1, 2n]\!]$.

Set $K := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $L := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, and notice that $L + L^T = K$. We define the $S_{i,j}$'s as follows:

- we set $S_{i,j} := 0$ whenever $i + j < 2n + 2$;
- we set $S_{i,2n+2-i} := K$ for every $i \in [\![1, 2n+1]\!]$;
- we set $S_{i,j} := 0$ whenever $i > n + 1, j > n + 1$ and $(i,j) \neq (2n+1, 2n+1)$;
- we set $S_{2n+1,2n+1} := I_2$;
- we set $S_{i,n+1} := L$ whenever $i > n + 1$;
- we set $S_{n+1,j} := L^T$ whenever $j > n + 1$;
- we then define (doubly)-inductively $S_{i,j}$ for i from n down to 2 and for j from $2n - i + 3$ up to $2n + 1$ by $S_{i,j} := -S_{i,j-1} - S_{i+1,j-1}$;
- symmetrically, we define $S_{i,j}$ for j from n down to 2 and for i from $2n - j + 3$ up to $2n + 1$ by $S_{i,j} := -S_{i-1,j} - S_{i-1,j+1}$.

One checks that S is symmetric, nonsingular, nonalternate (consider the last two diagonal entries) and that $J_{2n+1}(1) \otimes I_2$ is S-orthogonal. $\square$

6. Refinements for quadratic forms over a finite field of characteristic 2

In this section, $\mathbb{K}$ is a field of characteristic 2. If $\mathbb{K}$ is finite, there are two equivalence classes of regular quadratic forms of dimension $2n$ over $\mathbb{K}$. We wish to determine, for a given essentially orthogonal automorphism $u \in \mathrm{GL}(\mathbb{K}^{2n})$, the equivalence classes of the regular quadratic forms for which u is orthogonal.

Since the theory of quadratic forms in characteristic 2 is rather exotic, we start with a quick reminder of some notations and basic facts.

- The map $\mathcal{P} : x \mapsto x^2 + x$ from $\mathbb{K}$ to $\mathbb{K}$ is a group homomorphism for $+$ with kernel $\{0, 1\}$. If $\mathbb{K}$ is finite, then its range is a subgroup of index 2 of $\mathbb{K}$.
- Given a regular quadratic form q over a finite-dimensional $\mathbb{K}$-vector space, we choose a symplectic basis of the polar form b_q: in this basis, q is represented by a matrix of the form $\begin{bmatrix} A & I_n \\ 0 & B \end{bmatrix}$, and the class of $\mathrm{tr}(AB)$ in the quotient group $\mathbb{K}/\mathcal{P}(\mathbb{K}) \simeq \mathbb{Z}/2$ is independent on the choices of the basis and of the matrices A and B: this class, denoted by $\Delta(q)$, is the **Arf invariant** of q. When q is hyperbolic, its Arf invariant is 0.
- The Arf invariant is additive from $\perp$ to $+$, and when $\mathbb{K}$ is finite, it classifies the regular quadratic forms of a given dimension up to equivalence.
- In particular, for every $a \in \mathbb{K}$, the Arf invariant of the quadratic form $[1, a]_{\mathbb{K}} : (x, y) \mapsto x^2 + xy + ay^2$ on $\mathbb{K}^2$ is the class of a in $\mathbb{K}/\mathcal{P}(\mathbb{K})$.

6.1. A sufficient condition for being orthogonal for both types of regular quadratic forms

Let $u \in \mathrm{GL}(V)$ be an essentially orthogonal automorphism. We claim that if 1 is an eigenvalue of u, then, for any $\delta \in \mathbb{K}/\mathcal{P}(\mathbb{K})$, there is a regular quadratic form q on V with Arf invariant δ and for which u is q-orthogonal. Since Theorem 2 shows that the odd-sized Jordan blocks of u for the eigenvalue 1 are paired, it suffices to prove the following lemmas (the case of Jordan blocks of size one being trivial):

Lemma 19. *Let $n \in \mathbb{N}^*$ and $\delta \in \mathbb{K}/\mathcal{P}(\mathbb{K})$. Then there is a regular quadratic form on $\mathbb{K}^{2n}$ with Arf invariant δ for which $J_{2n}(1)$ is orthogonal.*

Lemma 20. *Let $n \in \mathbb{N}^*$ and $\delta \in \mathbb{K}/\mathcal{P}(\mathbb{K})$. Then there is a regular quadratic form on $\mathbb{K}^{4n+2}$ with Arf invariant δ for which $J_{2n+1}(1) \oplus J_{2n+1}(1)$ is orthogonal.*

Proof of Lemma 19. Denote by $(e_1, \ldots, e_{2n})$ the canonical basis of $\mathbb{K}^{2n}$.

If $n = 1$, we remark that any orthogonal group contains a reflection and that every reflection of a 2-dimensional vector space over $\mathbb{K}$ is represented by the matrix $J_2(1)$.

Assume now that $n \geqslant 2$, and let $a \in \mathbb{K}$.

We define $A = (a_{i,j}) \in M_{2n}(\mathbb{K})$ as follows:

- we set $a_{i,j} := 0$ whenever $i + j < 2n + 1$;
- we set $a_{i,2n+1-i} := 1$ for every $i \in [\![1, 2n]\!]$;
- we set $a_{i,j} := 0$ whenever $i > n + 1$ and $j > n + 1$;
- we set $a_{n+1,n+1} := 0$;
- we set $a_{i,n+1} := a$ whenever $i > n + 1$, and $a_{n+1,j} := a$ whenever $j > n + 1$;
- we then define (doubly)-inductively $a_{i,j}$ for i from n down to 2 and for j from $2n - i + 2$ up to $2n$ by $a_{i,j} := -a_{i,j-1} - a_{i+1,j-1}$;
- symmetrically, we define $a_{i,j}$ for j from n down to 2 and for i from $2n - j + 2$ up to $2n$ by $a_{i,j} := -a_{i-1,j} - a_{i-1,j+1}$.

The matrix A is nonsingular and alternate, and $J_{2n}(1)^T A J_{2n}(1) = A$. Define then q as the unique quadratic form on $\mathbb{K}^{2n}$ with polar form $b : (X, Y) \mapsto X^T A Y$ and such that $q(e_{2n}) = 0$ and $q(e_i) = a_{i,i+1}$ for every $i \in [\![1, 2n - 1]\!]$. Then $X \mapsto J_{2n}(1)X$ is q-orthogonal and $q(e_i) = 0$ for every $i \in [\![1, n - 1]\!]$. It follows that $\mathrm{span}(e_1, \ldots, e_{n-1})$ is totally q-isotropic. Using the hyperbolic inflation principle (see [9, Chapter VII, Proposition 3.2.5]), we find that q is Witt-equivalent (see [9, Chapter IX, Definition 1.0.26]) to its restriction q' to $\mathrm{span}(e_n, e_{n+1})$ (notice that $\mathrm{span}(e_1, \ldots, e_{n+1})$ is the orthogonal of $\mathrm{span}(e_1, \ldots, e_{n-1})$ for b). However $q(e_n) = b(e_n, e_{n+1}) = 1$ and $q(e_{n+1}) = b(e_{n+1}, e_{n+2}) = a$, and (e_n, e_{n+1}) is a symplectic basis of $\mathrm{span}(e_n, e_{n+1})$, hence $q' \simeq [1, a]_{\mathbb{K}}$. We deduce that $\Delta(q) = [a]$, which completes the proof. $\square$

Proof of Lemma 20. The strategy is quite similar to that of our proof of Lemma 18. We work with $M := J_{2n+1}(1) \otimes I_2$. We let $a \in \mathbb{K}$ and we find a nonsingular alternate matrix S of the form

$$
\begin{bmatrix}
S_{1,1} & S_{1,2} & \cdots & S_{1,2n+1} \\
S_{2,1} & S_{2,2} & \cdots & S_{2,2n+1} \\
\vdots & \vdots & \ddots & \vdots \\
S_{2n+1,1} & S_{2n+1,2} & \cdots & S_{2n+1,2n+1}
\end{bmatrix}
$$

such that $M^T S M = S$, where the $S_{i,j}$'s are 2×2 matrices. Set $K := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $L := \begin{bmatrix} a & 0 \\ 1 & 1 \end{bmatrix}$, and notice that $L + L^T = K$. We then define the $S_{i,j}$'s as follows:

- we set $S_{i,j} := 0$ whenever $i + j < 2n + 2$;
- we set $S_{i,2n+2-i} := K$ for every $i \in [\![1, 2n+1]\!]$;
- we set $S_{i,j} := 0$ whenever $i > n + 1$ and $j > n + 1$;
- we set $S_{i,n+1} := L$ whenever $i > n + 1$;
- we set $S_{n+1,j} := L^T$ whenever $j > n + 1$;
- we then define (doubly)-inductively $S_{i,j}$ for i from n down to 2 and for j from $2n - i + 3$ up to $2n + 1$ by $S_{i,j} := -S_{i,j-1} - S_{i+1,j-1}$;
- symmetrically, we define $S_{i,j}$ for j from n down to 2 and for i from $2n - j + 3$ up to $2n + 1$ by $S_{i,j} := -S_{i-1,j} - S_{i-1,j+1}$.

One checks that S is alternate and nonsingular, and that $M^T S M = S$. Denote by $(e_1, \ldots, e_{4n+2})$ the canonical basis of $\mathbb{K}^{4n+2}$, and let q be an arbitrary quadratic form on $\mathbb{K}^{4n+2}$ with polar form b : $(X, Y) \mapsto X^T S Y$. Then M is q-orthogonal if and only if $q(e_k) = q(e_k + e_{k-2})$ for every $k \in [\![3, 4n+2]\!]$, i.e., $q(e_k) = b(e_k, e_{k+2})$ for every $k \in [\![1, 4n]\!]$.

In this case, $q(e_1) = q(e_2) = \cdots = q(e_{2n}) = 0$, and since $\mathrm{span}(e_1, \ldots, e_{2n})$ is totally b-singular, it follows that it is also totally q-isotropic. As in the previous proof, the hyperbolic inflation principle ensures that q is Witt-equivalent to its restriction q' to $\mathrm{span}(e_{2n+1}, e_{2n+2})$. However $q(e_{2n+1}) = b(e_{2n+1}, e_{2n+3}) = a$ and $q(e_{2n+2}) = b(e_{2n+2}, e_{2n+4}) = 1$, and (e_{2n+1}, e_{2n+2}) is a b-symplectic basis of $\mathrm{span}(e_{2n+1}, e_{2n+2})$, hence $\Delta(q') = [a]$. We deduce that $\Delta(q) = [a]$, which completes the proof. $\square$

Corollary 21. *Assume that $\mathbb{K}$ is finite and let $u \in \mathrm{GL}(V)$ be an essentially symplectic morphism. If 1 is an eigenvalue of u, then there exists an hyperbolic form on V for which u is orthogonal and a regular non-hyperbolic quadratic form on V for which u is orthogonal.*

6.2. On essentially symplectic morphisms for which 1 is not an eigenvalue

In this section, we assume that $\mathbb{K}$ is finite and we consider an essentially symplectic morphism u of which 1 is not an eigenvalue. We intend to prove that all the quadratic forms for which u is orthogonal are equivalent: we do so by calculating their Arf invariant. Let q be a regular quadratic form for which u is orthogonal (we say that q is u-**adapted**), and denote by b_q its polar form.

Lemma 22. *Let W be a linear subspace of V which is both totally b_q-singular and stabilized by u. Then q vanishes on W.*

Proof. Indeed, for every $x \in W$, one has $q((u - \mathrm{id})(x)) = q(u(x)) + q(x) + b_q(x, u(x)) = 0$, and the result follows since $u - \mathrm{id}$ is an automorphism of the finite-dimensional vector space W. $\square$

We now split up the minimal polynomial of u as

$$\mu_u = Q \, Q^{\#} \, P_1^{a_1} \cdots P_p^{a_p},$$

where Q is prime with $Q^{\#}$, and $P_1, \ldots, P_p$ are pairwise distinct irreducible palindromials with a degree greater than 1 (and the a_i's are positive integers). Both Q and $Q^{\#}$ are prime with each P_k. The subspaces $W := \mathrm{Ker}(Q \, Q^{\#})(u)$, $V_1 := \mathrm{Ker} \, P_1^{a_1}(u), \ldots, V_p := \mathrm{Ker} \, P_p^{a_p}(u)$ must then be pairwise q-orthogonal, hence

$$q \simeq q_W \perp q_{V_1} \perp \ldots \perp q_{V_p}.$$

Notice that q_W is hyperbolic: indeed $\mathrm{Ker} \, Q(u)$ and $\mathrm{Ker} \, Q^{\#}(u)$ are both totally b_q-singular and stabilized by u, so the previous lemma shows that q vanishes on both of them. It follows that

$$\Delta(q) = \sum_{k=1}^{p} \Delta(q_{V_k}).$$

It now suffices to investigate the case μ_u is a power of an irreducible palindromial P with $\deg P > 1$:

Proposition 23. *Let $P \in \mathbb{K}[x]$ be an irreducible palindromial of degree greater than 1. Let $u \in \mathrm{GL}(V)$ be an automorphism whose minimal polynomial is a power of P, and let q be a regular u-adapted quadratic form on V. Denote by N the number of blocks of type $C(P^{2a+1})$ (with $a \in \mathbb{N}$) in the primary canonical form of u. Then $\Delta(q) = N \cdot [\varepsilon]$, where $\varepsilon \in \mathbb{K} \backslash \mathcal{P}(\mathbb{K})$.*

Before proving this result, we immediately deduce our final theorem:

Theorem 24. *Assume that $\mathbb{K}$ is a finite field of characteristic 2. Let $u \in \mathrm{GL}(V)$ be an essentially symplectic automorphism, and denote by N the number of blocks of type $C(P^{2a+1})$, with $a \in \mathbb{N}$ and P an irreducible palindromial of degree greater than 1, in the primary canonical form of u.*

(a) *If 1 is an eigenvalue of u, then there is an hyperbolic form q_1 on V and a regular non-hyperbolic form q_2 on V such that $u \in \mathrm{O}(q_1) \cap \mathrm{O}(q_2)$.*

(b) *If 1 is not an eigenvalue of u and N is even, then every u-adapted regular quadratic form on V is hyperbolic.*

(c) *If 1 is not an eigenvalue of u and N is odd, then every u-adapted regular quadratic form on V is non-hyperbolic.*

We now turn to the proof of Proposition 23. To start with, we use essentially the same method as in the proof of Proposition 10 (see Section 3.2). With the same notations, we replace the endomorphism $u - \mathrm{id}$ with $P(u)$ and add the condition that the subspace $\bigoplus_{i=p}^{k} V_{k,i}$ be stabilized by u for every $k \in [\![1, 2n]\!]$ and every $p \in [\![1, k]\!]$. Finally, for every $x \in F \oplus G \oplus H$, $v(x)$ is defined as the unique vector of $F \oplus G \oplus H$ such that $v(x) - u(x) \in E$ (that we may decompose V into the sum of the $V_{k,i}$'s is a classical consequence of the generalized Jordan reduction theorem).

Notice that $\mathrm{Ker}\, P(v) = F \oplus H$ and $\mathrm{Im}\, P(v) = H$. The rest of the arguments of Section 3.2 hold in this new context, which shows that E is totally b_q-singular, hence totally q-isotropic by Lemma 22. Applying again Lemma 22 to v on H, we find that H is totally q-isotropic. The hyperbolic inflation theorem then ensures that q is Witt-equivalent to q_F, which leads to $\Delta(q) = \Delta(q_F)$.

We have thus reduced the situation to the one where P is the minimal polynomial of u, which we now consider. As in Section 4.2, we set $\mathbb{L} := \mathbb{K}[x]/(P(x))$, denote by y the class of the indeterminate x in $\mathbb{L}$, by σ the $\mathbb{K}$-automorphism of $\mathbb{L}$ such that $\sigma(y) = y^{-1}$, and we set $\mathbb{K}' := \{z \in \mathbb{L} : \sigma(z) = z\}$. Notice that u induces a structure of $\mathbb{L}$-vector space on V. This reduces the situation to the one where $V = \mathbb{L}^n$ for some $n \geqslant 1$, and u is the multiplication by y in the vector space $\mathbb{L}^n$.

Lemma 25. *Let B be a symmetric bilinear form on the $\mathbb{K}$-vector space $\mathbb{L}$ such that $B(ya, yb) = B(a, b)$ for every $(a, b) \in \mathbb{L}^2$. Then there is a (unique) $c \in \mathbb{L}$ such that $B(a, b) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(c\, \sigma(a)b)$ for every $(a, b) \in \mathbb{L}^2$.*

Proof. Since $(a, b) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(ab)$ is a regular bilinear form on the $\mathbb{K}$-vector space $\mathbb{L}$, there is a unique endomorphism φ of the $\mathbb{K}$-vector space $\mathbb{L}$ such that $\forall(a, b) \in \mathbb{L}^2$, $B(a, b) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\varphi(a)b)$. Since $\mathbb{K}$ is a finite field, $\mathbb{L}$ is a Galois extension of $\mathbb{K}$. Therefore, we may decompose $\varphi = \sum_{\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \lambda_\tau . \tau$ for a unique family (λ_τ) of elements of $\mathbb{L}$. However, $B(ya, yb) = B(a, b)$ for every $(a, b) \in \mathbb{L}^2$ and hence the uniqueness of φ shows that $\varphi(yz)y = \varphi(z)$ for every $z \in \mathbb{L}$. Since $y\varphi(yz) = \sum_{\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} y\tau(y)\lambda_\tau . \tau(z)$ for every $z \in \mathbb{L}$, we deduce that $y\tau(y)\lambda_\tau = \lambda_\tau$ for every $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Let $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. If $\tau(y) = y^{-1}$, then $\tau = \sigma$ since y generates $\mathbb{L}$ as a $\mathbb{K}$-algebra. We deduce that $\lambda_\tau = 0$ whenever $\tau \neq \sigma$. Therefore $\varphi = \lambda_\sigma\, \sigma$, hence $c := \lambda_\sigma$ has the required properties. $\square$

Claim 2. *The polar form b_q of q has the form $(X, Y) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(X)^T AY)$ for some nonsingular hermitian matrix $A \in \mathrm{M}_n(\mathbb{L})$ (hermitian in the sense that $\sigma(A)^T = A$).*

Proof. Denote by $(e_1, \ldots, e_n)$ the canonical basis of the $\mathbb{L}$-vector space $\mathbb{L}^n$. For every $(i, j) \in [\![1, n]\!]^2$, the map $b_{i,j} : (a, b) \mapsto b_q(ae_i, be_j)$ satisfies the conditions of Lemma 25, so we may find $z_{i,j} \in \mathbb{L}$ such that $b_{i,j}(a, b) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(z_{i,j}\sigma(a)b)$ for every $(a, b) \in \mathbb{L}^2$. Set then $A := (z_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathrm{M}_n(\mathbb{L})$ and notice that

$$\forall(X, Y) \in (\mathbb{L}^n)^2, \quad b_q(X, Y) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(X)^T AY).$$

Since b_q is symmetric, it follows that

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(X)^T AY) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(Y)^T AX) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(\sigma(Y)^T AX)^T) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\sigma(X)^T \sigma(A)^T Y)$$

for every $(X, Y) \in (\mathbb{L}^n)^2$. Let $(X, Y) \in (\mathbb{L}^n)^2$ and $\lambda \in \mathbb{L}$. Applying the previous identity to $(X, \lambda Y)$ yields $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\big(\lambda(\sigma(X)^T AY - \sigma(X)^T \sigma(A)^T Y)\big) = 0$. It follows that $\sigma(X)^T AY - \sigma(X)^T \sigma(A)^T Y = 0$. Therefore $\sigma(A)^T = A$. Finally, since b_q is regular, we find that A is nonsingular. $\square$

The relations $\forall x \in V, \ q(u(x) - x) = b_q(x, u(x))$ and the fact that $u - \mathrm{id}$ is an automorphism of V show that q is the unique quadratic form on V with polar form b_q such that $u \in O(q)$. Since the map $X \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(\sigma(X)^T AX)$ qualifies, it equals q.

Notice that the Gaussian reduction of hermitian forms still holds in characteristic 2. Since $\mathbb{K}$ is perfect, we deduce that q is equivalent to the form $(x_1, \ldots, x_n) \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(x_1\sigma(x_1) + \cdots + x_n\sigma(x_n))$, which is itself equivalent to the orthogonal sum of n copies of the form $x \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(x\sigma(x))$ on the $\mathbb{K}$-vector space $\mathbb{L}$. In order to conclude, we prove the following:

Claim 3. *The quadratic form $\varphi : x \mapsto \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(x\sigma(x))$ on the $\mathbb{K}$-vector space $\mathbb{L}$ is non-hyperbolic.*

Choose $a \in \mathbb{K}' \setminus \mathcal{P}(\mathbb{K}')$. Notice that $\varphi : x \mapsto x\sigma(x)$ is a regular non-isotropic quadratic form on the 2-dimensional $\mathbb{K}'$-vector space $\mathbb{L}$, hence its Arf invariant is a. This shows that this form is equivalent to $[a, 1]_{\mathbb{K}'}$ (both have the same Arf invariant). Let $\mathbf{B} := (e_1, \ldots, e_m)$ be a basis of the $\mathbb{K}$-vector space $\mathbb{K}'$ and set $P := (\mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(e_ie_j))_{1\leqslant i,j\leqslant m}$ and $P_a := (\mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(ae_ie_j))_{1\leqslant i,j\leqslant m}$. Obviously, the matrix $\begin{bmatrix} P_a & P \\ 0 & P \end{bmatrix}$

represents φ in some basis of the $\mathbb{K}$-vector space $\mathbb{L}$. Multiplying it by $C := \begin{bmatrix} I_m & 0 \\ 0 & P^{-1} \end{bmatrix}$ on the left

and by C^T on the right, we find that $\begin{bmatrix} P_a & I_m \\ 0 & P^{-1} \end{bmatrix}$ represents φ, hence $\Delta(\varphi) = [\mathrm{tr}(P_aP^{-1})]$. However

$\mathrm{tr}(P_aP^{-1}) = \mathrm{tr}(P^{-1}P_a) = \mathrm{Tr}_{\mathbb{K}'/\mathbb{K}}(a)$ since $P_a = P \times M_{\mathbf{B}}(x \mapsto ax)$. In order to conclude the proof of Claim 3, it suffices to establish the following final lemma:

Lemma 26. *Let $\mathbb{K} - \mathbb{L}$ be an extension of finite fields of characteristic 2. Then $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ induces a group isomorphism from $\mathbb{L}/\mathcal{P}(\mathbb{L})$ to $\mathbb{K}/\mathcal{P}(\mathbb{K})$.*

Proof. For every $x \in \mathbb{L}$, notice that

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x^2 + x) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \sigma(x^2 + x) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \sigma(x)^2 + \sum_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} \sigma(x) = \mathcal{P}(\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)),$$

therefore $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ maps $\mathcal{P}(\mathbb{L})$ into $\mathcal{P}(\mathbb{K})$. It follows that $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ induces a group homomorphism from $\mathbb{L}/\mathcal{P}(\mathbb{L})$ to $\mathbb{K}/\mathcal{P}(\mathbb{K})$. This homomorphism is onto since $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$ maps $\mathbb{L}$ onto $\mathbb{K}$, being a nonzero $\mathbb{K}$-linear form on $\mathbb{L}$. Since both groups $\mathbb{L}/\mathcal{P}(\mathbb{L})$ and $\mathbb{K}/\mathcal{P}(\mathbb{K})$ have order 2, the claimed result follows. $\square$

This finishes the proof of Proposition 23 and Theorem 24.

References

[1] N. Burgoyne, R. Cushman, Conjugacy classes in linear groups, J. Algebra 44 (1977) 339–362.
[2] I.K. Cikunov, Structure of isometric transformations of a symplectic or orthogonal vector space Russian, Ukrainian Math. Z. 18 (4) (1966) 79–93.
[3] G. Frobenius, Über die mit einer Matrix vertauschbaren Matrizen, Sitzungsber. Preuss. Akad. Wiss. (1910) 3–15.
[4] F.R. Gantmacher, Matrix Theory, vol. 2, Chelsea, New York, 1977.
[5] K. Gongopadhyay, R.S. Kulkarni, On the existence of an invariant non-degenerate bilinear form under a linear map, Linear Algebra Appl. 414 (2011) 89–103.
[6] R. Gow, T.J. Laffey, Pairs of alternating forms and products of two skew-symmetric matrices, Linear Algebra Appl. 63 (1984) 119–132.
[7] R.A. Horn, D.I. Merino, The Jordan canonical forms of complex orthogonal and skew-symmetric matrices, Linear Algebra Appl. 302–303 (1999) 411–421.

 [8] J. Milnor, On isometries of inner product spaces, Invent. Math. 8 (1969) 83–97.
 [9] C. de Seguins Pazzis, Invitation aux formes quadratiques, Calvage & Mounet, Paris, 2011.
[10] V.V. Sergeichuk, Classification problems for systems of forms and linear mappings, Math. USSR Izv. 31 (3) (1988) 481–501.
[11] V.V. Sergeichuk, Canonical matrices of isometric operators on indefinite inner product space, Linear Algebra Appl. 428 (2008) 154–192.
[12] H. Stenzel, Über die Darstellbarkeit einer Matrix als Produkt von zwei symmetrischer Matrizen, als Produkt von zwei alternierenden Matrizen und als Produkt von einer symmetrischen und einer alternierenden Matrix, Math. Z. 15 (1922) 1–25.
[13] O. Taussky, The role of symmetric matrices in the study of general matrices, Linear Algebra Appl. 5 (1972) 147–154.
[14] J. Williamson, Matrices normal with respect to an hermitian matrix, Amer. J. Math. 60 (1938) 355–373.
[15] J. Williamson, Normal matrices over a field of characteristic zero, Amer. J. Math. 61 (1939) 335–356.