Journal of Algebra 400 (2014) 161–184

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On the bilinear structure associated to Bezoutians

F. Jouve [a], F. Rodriguez Villegas [b,c,1]

[a] Département de Mathématiques, Bâtiment 425, Faculté des Sciences d'Orsay, Université Paris-Sud, F-91405 Orsay Cedex, France
[b] The Abdus Salam International Centre for Theoretical Physics, Strada Costiera 11, 34151 Trieste, Italy
[c] Department of Mathematics, University of Texas at Austin, 1 University Station, C1200 Austin, TX, USA

ARTICLE INFO

Article history:
Received 3 May 2010
Available online 21 December 2013
Communicated by Eva Bayer-Fluckiger

Keywords:
Bilinear forms
Bezoutian of polynomials
Characteristic polynomials
Jordan form of isometries

ABSTRACT

This paper is partly a survey of known results on quadratic forms that are hard to find in the literature. Our main focus is a twisted form of a construction due to Bezout. This *skew Bezoutian* is a symplectic (resp. quadratic) space associated to a pair of reciprocal (or skew reciprocal) coprime polynomials of same degree. The isometry group of this space turns out to contain a certain associated hypergeometric group. Using the skew Bezoutian we construct explicit isometries of bilinear spaces with given invariants (such as the characteristic polynomial or Jordan form and, in the quadratic case, the spinor norm).

1. Introduction

Given a finite dimensional commutative algebra A over a field k it is useful to have a non-trivial *transfer map* that takes bilinear modules over A to bilinear modules over k preserving non-degeneracy. A typical case is that of $A = K$ a separable finite field extension where one can use the usual trace $\mathrm{Tr}_{K/k}$ for this purpose; for an inseparable field extension K/k however, the trace $\mathrm{Tr}_{K/k}$ is identically zero. Nevertheless, one may still find suitable linear maps (see [20, Remark 1.4] and [2, Discussion preceding Proposition (2.2)]).

As an example, consider the *unit form* $\Psi(x, y) = xy$ on a finite dimensional k-algebra (with unit) A. It is clearly non-degenerate. Transferring this form to k consists of finding a k-linear map $t : A \to k$ such that the k-bilinear form $t \circ \Psi(x, y) = t(xy)$ is non-degenerate as well. The resulting pair (A, t) is called a *Frobenius algebra*.

E-mail addresses: florent.jouve@math.u-psud.fr (F. Jouve), villegas@ictp.it (F. Rodriguez Villegas).

[1] FRV was supported by NSF grant DMS-0800099. He would also like to thank the Centre de Recerca Matemàtica in Barcelona for its hospitality.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.10.030

In Section 2 we study in some detail the situation where the Frobenius algebra A is *monogenic*, i.e., $A = k[\alpha]$ for some $\alpha \in A$. We show that the isomorphism classes of these algebras over k are parametrized by rational functions $w \in k[T]$ with $w(\infty) = 0$. In turn, the associated bilinear form is essentially given by the classical Bezoutian of the polynomials p and q, where $w = p/q$ in lowest terms.

In Section 3 we further assume the characteristic of the base field k to be different from 2 and we study a skew version of the classical Bezoutian, which turns out to be quite interesting. For example, we show how it gives a natural description of the Hermitian form fixed by an associated hypergeometric group.

The rest of the paper is devoted to applications (in characteristic different from 2) of the skew Bezoutian to the problem of the existence of isometries with prescribed characteristic polynomial (and/or spinor norm in the quadratic case) or with prescribed Jordan form.

Using the trace map and other linear maps to transfer quadratic A-modules to quadratic k-modules, where A is a separable k-algebra, appears prominently in the literature. A general account of applications of trace forms to the construction of lattices via number fields can be found in [5]. See also [20, Section 1], [16, pp. 109–110] or [2, Beginning of Section 2] for a general construction.

Transfer constructions are used in knot theory at least since the 1960's; a survey of some of the results can be found in [16]. The trace plays a prominent role, but other transfers are also used, in particular by Trotter (see for instance [27, pp. 292–294] and [26, pp. 181–182]). Moreover a general study of transfers and their applications was started in the late 1960's by Scharlau ([23,24]; see also [18, Chapter 7] for a detailed exposition of Scharlau's results), and still plays a very important role in the study of quadratic and Hermitian forms.

2. Monogenic Frobenius algebras and the Bezoutian

Let k be a field. A *monogenic Frobenius algebra over* k, MFA for short, is a triple (A, α, t), where A is a finite dimensional k-algebra, $A = k[\alpha]$, and $t : A \to k$ is a linear map such that the bilinear form

$$\langle x, y\rangle := t(xy), \quad x, y \in A,$$

is non-degenerate. With some notation abuse we will say in this case that the linear map t is non-degenerate. Two such algebras (A, α, t), (A', α', t') are isomorphic if there is an isomorphism of algebras $\phi : A \to A'$ such that $\alpha' = \phi(\alpha)$ and $t' = t \circ \phi^{-1}$.

Let A be a k-algebra and $t : A \to k$ be a non-degenerate linear map. For $a \in A$ the map $t_a(x) := t(ax)$ is also non-degenerate if and only if a is not a zero-divisor. In particular, there is natural action of the group of units $A^\times$ of A on the set of non-degenerate linear maps $t : A \to k$ defined by setting $(a \cdot t)(x) := t_a(x) = t(ax)$, where $a \in A^\times$.

The following theorem gives a parametrization of MFA's.

Theorem 2.1. *For any $d \geqslant 1$ the map $(A, \alpha, t) \mapsto w(T)$, where*

$$w(T) := \sum_{\ell \geqslant 0} t\bigl(\alpha^\ell\bigr) T^{-\ell-1} \in k\llbracket T^{-1}\rrbracket,$$

induces a bijection between isomorphism classes of d-dimensional MFA's (A, α, t) over k and rational functions $w \in k(T) \cap k\llbracket T^{-1}\rrbracket$ of degree d with $w(\infty) = 0$.

Proof. Let (A, α, t) be a d-dimensional MFA over k. Consider the power series

$$w(T) := \sum_{\ell \geqslant 0} t\bigl(\alpha^\ell\bigr) T^{-\ell-1} \in k\llbracket T^{-1}\rrbracket.$$

Let $q = T^d + \sum_{i=0}^{d-1} q_i T^i \in k[T]$ be the minimal polynomial of α over k. Set $q_d = 1$ and $q_i = 0$ for $i > d$. We have:

$$q(T)w(T) = \sum_{\ell\in\mathbb{Z}} \sum_{i\geqslant \ell+1} q_i t\bigl(\alpha^{i-\ell-1}\bigr)T^{\ell}. \tag{2.1}$$

On the right hand side the coefficient of T^ℓ vanishes as soon as $\ell \geqslant d$ since $q_i = 0$ for $i > d$. Moreover, since q vanishes at α, we have for any integer ℓ

$$0 = \alpha^{-\ell-1} \sum_{i\geqslant 0} q_i\alpha^i = \sum_{i\geqslant 0} q_i\alpha^{i-\ell-1}.$$

Thus the coefficient of T^ℓ on the right hand side of (2.1) also vanishes for $\ell + 1 \leqslant 0$. We deduce that $q(T)w(T)$ is a polynomial $p \in k[T]$ of degree $\leqslant d-1$ with

$$p(T) := \sum_{\ell=0}^{d-1} \sum_{i=\ell+1}^{d} q_i t\bigl(\alpha^{i-\ell-1}\bigr)T^{\ell}.$$

The rational function $w = p/q \in k(T)$ satisfies $w(\infty) = 0$ since $\deg(p) < \deg(q)$. This calculation is valid for any linear map t without assuming it is non-degenerate.

The Gram matrix of $\langle\cdot,\cdot\rangle$ in the k-basis $(1, \alpha, \dots, \alpha^{d-1})$ of A is the Hankel matrix

$$H(p/q) := \bigl(t\bigl(\alpha^{i+j}\bigr)\bigr)_{0\leqslant i,j\leqslant d-1}. \tag{2.2}$$

By assumption the bilinear form $\langle\cdot,\cdot\rangle$ is non-degenerate hence the determinant of $H(p/q)$ is non-zero. By Kronecker's theorem (in [17], see e.g. [11, Theorem 8.20 and Proposition 8.22]) p and q are coprime and $\deg w = d$. Obviously w depends only on the isomorphism class of (A, α, t). Indeed if (A, α, t) and (A', α', t') are two isomorphic MFA's and if ϕ is a fixed isomorphism then for all $\ell \geqslant 0$,

$$t'\bigl({\alpha'}^{\ell}\bigr) = t \circ \phi^{-1}\bigl(\phi(\alpha)^{\ell}\bigr) = t\bigl(\alpha^{\ell}\bigr).$$

Conversely, suppose we are given a rational function $w = p(T)/q(T) \in k(T)$ satisfying $w(\infty) = 0$ and $\deg(w) = d \geqslant 1$. Without loss of generality we may assume q monic, $\deg q = d$, $(p, q) = 1$, p non-zero and $\deg p < d$. Set

$$A := k[T]/(q).$$

Let α be the image of T in A; then $\{1, \alpha, \dots, \alpha^{d-1}\}$ is a k-basis of A. Let $\sum_{\ell\geqslant 0} t_\ell T^{-\ell-1} \in k[\![T^{-1}]\!]$ be the power series expansion of w at ∞. Define the k-linear map

$$t : A \to k, \qquad \alpha^{\ell} \mapsto t_\ell, \quad \ell = 0, 1, \dots, d-1. \tag{2.3}$$

By construction the power series in T^{-1}:

$$\tilde{w}(T) := \sum_{\ell\geqslant 0} t\bigl(\alpha^{\ell}\bigr)T^{-\ell-1},$$

has the same first d coefficients as w. On the other hand, as observed above, $\tilde{p}(T) := q(T)\tilde{w}(T)$ is a polynomial of degree $\leqslant d-1$. Hence the first d coefficients of $\tilde{p}(T)$ and $q(T)w(T) = p(T)$ agree and it follows that $w = \tilde{w}$.

Again, since $(p, q) = 1$, by Kronecker's theorem the matrix $H(p/q)$ has non-zero determinant and hence the bilinear form on A defined by $(x, y) \mapsto t(xy)$ is non-degenerate. This completes the proof of the theorem. $\square$

Corollary 2.2. 1) *Given a monic polynomial $q \in k[T]$ of degree $\deg(q) > 0$ there exists a MFA of the form $(k[T]/(q), T \bmod q, t)$.*

2) *For any MFA (A, α, t) the unit group $A^\times$ acts transitively on the non-degenerate linear maps on A.*

Proof. To prove 1), it is enough to take $w = 1/q$. Let $(k[T]/(q), T \bmod q, t)$ be the corresponding MFA. Say t' is another non-degenerate linear map on it and let p/q be the associated rational function. To show 2), it is enough to prove that

$$\sum_{l \geqslant 0} t\big(p(\alpha)\alpha^l\big)T^{-l-1} = \frac{p(T)}{q(T)},$$

where $\alpha := T \bmod q$, since then $t' = p(\alpha) \cdot t$. To see this note that if $p(T) = \sum_{j=0}^{d-1} p_j T^j$ then the left hand side equals

$$\sum_{l \geqslant 0} \sum_{j=0}^{d-1} p_j t_{l+j} T^{-l-1} = \sum_{l \geqslant 0} \sum_{j=0}^{d-1} p_j t_l T^{j-l-1} = p(T) \cdot \frac{1}{q(T)},$$

finishing the proof. $\square$

Remark 2.3. Over the complex numbers the space of rational functions w of degree d with $w(\infty) = 0$ is naturally isomorphic to a circle bundle over the moduli space of $SU(2)$ monopoles of charge d [9].

2.1. Examples

1) If q is irreducible and separable (i.e., q is irreducible and k has characteristic 0 or q is irreducible, k has characteristic $l > 0$, and q is not a polynomial in T^l) then $A := k[T]/(q)$ is a field, K say, and it is well-known that $t = \mathrm{Tr}_{K/k}$ is non-degenerate (in fact the algebra A is separable over k if and only if $\mathrm{Tr}_{A/k}$ is non-degenerate). It is not hard to see that the underlying MFA corresponds to the rational function p/q, where $p \equiv dq/dT \bmod q$. Indeed let L be the Galois closure of K/k. Since the extension K/k is separable there are $d := [K : k]$ distinct k-embeddings $\sigma_1, \ldots, \sigma_d : K \hookrightarrow L$. The Galois action of $G := \mathrm{Gal}(L/K)$ on L extends to an action on $L(T)$ via $\sigma(\sum \lambda_i T^i) := \sum \sigma(\lambda_i) T^i$. Therefore

$$w = \sum_{i \geqslant 0} \mathrm{Tr}_{K/k}\big(\alpha^i\big)T^{-i-1} = \sum_{i \geqslant 0} \left(\sum_{j=1}^{d} \sigma_j\big(\alpha^i\big)\right) T^{-i-1} = \frac{1}{T} \sum_{j=1}^{d} \sigma_j\left(\sum_{i \geqslant 0} (\alpha/T)^i\right).$$

The inner sum equals $T/(T - \alpha)$ hence:

$$w = \sum_{j=1}^{d} \sigma_j\left(\frac{1}{T - \alpha}\right) = \sum_{j=1}^{d} \frac{1}{T - \sigma_j(\alpha)} = \frac{dq/dT}{q}.$$

2) Another extreme case is $A = k[T]/(T^d)$. If say $p = 1$ then the rational function w given by Theorem 2.1 is simply $1/T^d$. The k-linear map $t : k[T]/(T^d) \to k$ corresponding to w is defined by $t(\alpha^i) = 0$ for $0 \leqslant i \leqslant d - 2$ and $t(\alpha^{d-1}) = 1$. Thus t can be identified with the projection $A \to A$ with image $k\alpha^{d-1}$. The non-degeneracy of t can be shown by elementary arguments. Namely, if $z = \sum z_i \alpha^i \in A$ is orthogonal to any $y \in A$ with respect to the inner product $(x, y) \mapsto t(xy)$ then in particular, for any fixed index i we have $t(z \cdot \alpha^{d-1-i}) = z_i = 0$. Thus $z = 0$.

2.2. Reproducing kernel

Given a Frobenius algebra (A, t) of dimension d consider the *Casimir element* (or *reproducing kernel*) defined by

$$C := \sum_{i=1}^{d} e_i \otimes e_i^{\#} \in A \otimes A,$$

where $e_1, \ldots, e_d$ is any basis of A over k and $e_i^{\#}$ is its dual basis (with respect to the bilinear form $\langle\cdot,\cdot\rangle$ determined by t), i.e.,

$$\langle e_i, e_j^{\#}\rangle = t\bigl(e_i e_j^{\#}\bigr) = \delta_{i,j}, \quad i, j = 1, \ldots, d.$$

This element is well defined; it does not depend on the choice of basis used in its definition.

We have

$$C = \sum_{i,j=1}^{d} \langle e_i^{\#}, e_j^{\#}\rangle e_i \otimes e_j.$$

For a MFA (A, α, t) with $A \simeq k[T]/(q)$ for some $q \in k[T]$ monic of degree d (namely, the minimal polynomial of α) we can represent elements of $A \otimes A$ as polynomials in $k[x, y]$ of degree at most $d-1$ in each variable.

Taking $e_i := \alpha^{i-1}$ for $i = 1, \ldots, d$ as our basis of A we obtain

$$C = \sum_{i,j=1}^{d} b_{i,j}^{\#} x^{i-1} y^{j-1},$$

where $b_{i,j}^{\#} := \langle e_i^{\#}, e_j^{\#}\rangle$.

The matrix $B^{\#} := (b_{i,j}^{\#})$ is the inverse of the Hankel matrix $H(p/q)$ in (2.2) since the matrices

$$\bigl(\langle e_i, e_j\rangle\bigr), \qquad \bigl(\langle e_i^{\#}, e_j^{\#}\rangle\bigr)$$

are inverses of each other. Combining this observation with the proof of Corollary 2.2 we obtain the following.

Proposition 2.4. *With the above notation and assumptions*

$$H(1/q) M_p = {}^t M_p H(1/q) = H(p/q) = \bigl(B^{\#}\bigr)^{-1},$$

where M_p is the matrix of multiplication by p in $k[T]/(q)$ in the basis $1, T, \ldots, T^{d-1}$.

2.3. Classical Bezoutian

Given two polynomials $p, q \in k[T]$, the *classical Bezoutian* is the symmetric matrix $B(p, q) := (b_{i,j})$, where

$$\frac{p(x)q(y) - p(y)q(x)}{x - y} = \sum_{i,j=1}^{d} b_{i,j} x^{i-1} y^{j-1}, \tag{2.4}$$

with $d := \max\{\deg(p), \deg(q)\}$. We have the following matrix expression for $B(p, q)$.

Lemma 2.5. *Let Q be the matrix with entries (q_{i+j-1}), where $1 \leqslant i, j \leqslant d$ and $q = \sum_{i\geqslant 0} q_i T^i \in k[T]$ is a polynomial of degree d. Assume $\deg p \leqslant d$, then*

$$B(p, q) = -M_p Q,$$

where M_p is the matrix of multiplication by p in $k[T]/(q)$.

Proof. Expand the left hand side of (2.4) in Laurent series in $k[x, y][[y^{-1}]]$. Modulo $q(x)$ the coefficient of y^{j-1} is that of

$$-p(x)q(y)y^{-1} \sum_{i\geqslant 0} \left(\frac{x}{y}\right)^i$$

and this is easily seen to equal $-p(x) \sum_{i\geqslant 0} q_{i+j} x^i$. □

We leave the easy proof of the following lemma to the reader

Lemma 2.6. *We have*

$$Q = H(1/q)^{-1}.$$

Putting together Propositions 2.4 and Lemmas 2.5 and 2.6 we finally obtain a connection between the Casimir element C and the classical Bezoutian.

Theorem 2.7. *With the above notation and assumptions*

$$B^{\#} = B(q, r),$$

where $r \in k[T]$ is a polynomial of degree less than d such that $rp \equiv 1 \bmod q$. Or, equivalently,

$$C = \frac{q(x)r(y) - q(y)r(x)}{x - y}.$$

Remark 2.8. We have discussed two symmetric matrices associated to a pair of coprime polynomials $p, q \in k[T]$: the Hankel matrix $H(p/q)$ and the Bezoutian $B(p, q)$. Combining Propositions 2.4, 2.5 and Lemma 2.6 we find that they are actually congruent up to a minus sign

$${}^{t}Q\, H(p/q) Q = -B(p, q)$$

(note that Q is symmetric).

The Bezoutian plays an important role in mathematical control theory, see for example [11].

3. The skew Bezoutian

We now turn to a construction that is a skew version of the classical Bezoutian.

3.1. Preliminaries

Let k be a field and d a positive integer; consider the algebra $A := k[T]/(T^d)$. Given a power series $a = a_0 + a_1T + a_2T^2 + \cdots \in k[\![T]\!]$ let $M(a) \in k^{d\times d}$ be the matrix of the k-linear map $A \to A$ defined by multiplication by a in the basis $1, T, \ldots, T^{d-1}$ of A. Concretely,

$$M(a) = \begin{pmatrix} a_0 & 0 & & 0 \\ a_1 & a_0 & & \\ \vdots & & \ddots & 0 \\ a_{d-1} & \cdots & \cdots & a_0 \end{pmatrix}.$$

The map $a \mapsto M(a)$ is clearly a homomorphism of k-algebras $k[\![T]\!] \to M^{d\times d}(k)$.

We will assume from now on that k has characteristic different from 2. For a polynomial $q \in k[T]$ we let q^* be the polynomial q with its coefficients reversed, i.e.,

$$q^*(T) := T^{\deg(q)} q(1/T), \quad q \in k[T],$$

where $\deg(q)$ is the degree of q.

For further reference let us note a few simple observations about the operation $*$. In general, $*$ is not additive but we have

$$(p+q)^* = p^* + q^*, \quad \text{if } \deg(p) = \deg(q)$$

and $(pq)^* = p^*q^*$ always. We extend $*$ to $k(T)$ by multiplicativity. Then for $w = p/q$ we have

$$w^*(T) := \frac{p^*}{q^*} = T^{\deg(p)-\deg(q)} w\bigl(T^{-1}\bigr).$$

We will say that $w \in k(T)$ is *reciprocal* if $w^* = w$, *skew-reciprocal* if $w^* = -w$ and in general ε*-reciprocal* if $w^* = \varepsilon w$ with $\varepsilon = \pm 1$.

To shorten the notation we let ν_ε, for $\varepsilon = \pm 1$, denote the valuation on $k[T]$ at $T - \varepsilon$. If $p \in k[T]$ is skew-reciprocal then $p(1) = 0$. It follows that in fact $\nu_+(p)$ must be odd since otherwise $p(T)/(T-1)^{\nu_+(p)}$ would be a skew-reciprocal polynomial not vanishing at $T = 1$. Similarly, if $p \in k[T]$ is ε-reciprocal with $\varepsilon = -(-1)^{\deg(p)}$ then $p(-1) = 0$ and again, $\nu_-(p)$ must be odd. In particular, if $p(-1) \neq 0$ then $\deg(p)$ must be even.

3.2. Definition

Let $w \in k(T)$ be a rational function with coefficients in k. Assume that w is regular at 0 and ∞. Then we have the two power series expansions

$$w(T) = w_0 + w_1T + \cdots, \qquad w(T) = w_0^* + w_1^*T^{-1} + \cdots.$$

Let d be the degree of $w = p/q$ where the fraction is written in lowest terms. With the above notation define the *skew Bezoutian* of w as

$$B^*(w) = {}^tM\big(T^{d-\deg p}w^*\big) - M(w) = \begin{pmatrix} w_0^* - w_0 & w_1^* & \cdots & w_{d-1}^* \\ -w_1 & w_0^* - w_0 & w_1^* & w_{d-2}^* \\ \vdots & \ddots & \ddots & w_1^* \\ -w_{d-1} & \cdots & -w_1 & w_0^* - w_0 \end{pmatrix}.$$

(We learned of this construction in [13].) Note that $B^*(w)$ is a *Toeplitz* matrix (constant entries along diagonals). Also, in the case where $d = \deg p = \deg q$ (for instance if $w(\infty) = 1$, as will be assumed later) one has the simpler definition $B^*(w) = {}^tM(w^*) - M(w)$.

There is a more conceptual way to give B^*, closer to the approach of the previous section on Frobenius algebras, as follows. Let $R := k[T, T^{-1}]$ and let $t : R \to k$ be the linear map corresponding to taking constant terms; i.e., $t(1) := 1$ and $t(T^n) := 0$ for all non-zero integers n.

We may represent elements in the dual space $\omega \in \mathrm{Hom}(R, k)$ as formal infinite series of the form

$$\omega := \sum_{n\in\mathbb{Z}} \omega\big(T^n\big)T^{-n}.$$

Following the usual rules of multiplication of series gives $\mathrm{Hom}(R, k)$ the structure of an R-module. Then

$$\omega(u) = t(u \cdot \omega), \quad u \in R.$$

With this notation define $\omega \in \mathrm{Hom}(R, k)$ by

$$\omega := \sum_{n\geqslant 0} w_n^* T^n - \sum_{n\geqslant 0} w_n T^{-n}.$$

Explicitly,

$$\omega\big(T^n\big) = \begin{cases} -w_n & n > 0, \\ w_0^* - w_0 & n = 0, \\ w_{-n}^* & n < 0. \end{cases} \tag{3.1}$$

Then the skew Bezoutian B^* is the matrix with entries $\omega(T^{i-j})$ for $i, j = 0, 1, \ldots, d-1$.

The first thing to point out is the value of the determinant of $B^*(w)$. Write $w = p/q$ for $p, q \in k[T]$ relatively prime. By assumption $d = \deg(w) = \max\{\deg(p), \deg(q)\}$. But since we also assume w is regular at infinity we must have $\deg(p) \leqslant \deg(q) = d$.

Proposition 3.1. *Let q_0 and q_d be the constant and leading coefficients of q respectively. Then we have*

$$q_0^d q_d^{\deg(p)} \det B^*(w) = (-1)^{d-\deg(p)} \operatorname{Res}(p, q)$$

Proof. Assume first that $\deg(p) = d$. The following block-matrix identity is easy to check using the fact that M is a homomorphism.

$$\begin{pmatrix} {}^tM(w^*) & M(w) \\ I_d & I_d \end{pmatrix} \cdot \begin{pmatrix} {}^tM(q^*) & 0 \\ 0 & M(q) \end{pmatrix} = \begin{pmatrix} {}^tM(p^*) & M(p) \\ {}^tM(q^*) & M(q) \end{pmatrix},$$

where I_d is the $d \times d$ identity matrix. The right hand side is then precisely the Sylvester matrix of p and q whose determinant is $\operatorname{Res}(p, q)$. On the other hand, the determinant of the left hand side equals $(q_0 q_d)^d \det B^*(w)$.

We may consider the case $\deg(p) < d$ as a specialization of the generic case of $\deg(p) = d$. Then the determinant on the right hand side is easily seen to equal $(-q_d)^{d-\deg(p)}\operatorname{Res}(p,q)$ completing the proof. □

Remark 3.2. The proof we gave follows that of a generalization of Proposition 3.1 to subresultants in [8, Proposition 11]. The fact that the classical Bezoutian has determinant related to the resultant goes back to Bezout. From a computational point of view the Bezoutian has the advantage that it is a matrix of size $\max\{\deg(p), \deg(q)\}$ versus the Sylvester matrix that has size $\deg(p) + \deg(q)$.

Consider the case that $\deg(p) = d$. It follows from the proof of the proposition that

$$B^*(p,q) := {}^tM(q^*)B^*(w)M(q) = {}^tM(p^*)M(q) - {}^tM(q^*)M(p) \tag{3.2}$$

has determinant $\operatorname{Res}(p,q)$. This matrix can be described in a very similar way to that of the classical Bezoutian (2.4). Indeed, it is not hard to see that its entries are the coefficients of the two variable polynomial

$$\frac{p(x)q^*(y) - q(x)p^*(y)}{xy-1}. \tag{3.3}$$

As in the proof of the proposition we may think of the case $\deg(p) < d$ as a specialization of the generic case $\deg(p) = d$ and define $B^*(p,q)$ accordingly (namely, p^* should be replaced by $T^d p(T^{-1})$). In general we have

$$\det\bigl(B^*(p,q)\bigr) = (-q_d)^{d-\deg(p)}\operatorname{Res}(p,q).$$

3.3. *Bilinear form*

We now consider the bilinear form determined by the skew Bezoutian. Let $V := R/(q^*)$ with basis $1, T, \ldots, T^{d-1}$. We claim that the linear form ω (3.1) vanishes on the ideal $(q^*) \subseteq R$ and therefore induces a corresponding linear form on V. To see this we compute

$$q^* \cdot \omega = q^* \sum_{n\geqslant 0} w_n^* T^n - q^* \sum_{n\geqslant 0} w_n T^{-n}.$$

The first term equals $q^*(T)w(T^{-1}) = T^{d-\deg(p)}q^*(T)w^*(T) = T^{d-\deg(p)}p^*(T)$ and similarly, the second term also equals $q^*(T)w(T^{-1})$ canceling out. It follows that $\omega(T^n q^*(T)) = t(T^n q^*(T)\cdot\omega) = 0$ for all n.

From now on we assume

$$w\bigl(T^{-1}\bigr) = -\varepsilon w(T), \qquad w(\infty) = 1, \tag{3.4}$$

for some $\varepsilon = \pm 1$. Then

$${}^tB^*(w) = \varepsilon B^*(w),$$

and, in the notation of the previous section,

$$w_n = -\varepsilon w_n^*, \quad n = 0, 1, \ldots.$$

Therefore,

$$B^*(w) = \begin{pmatrix} \varepsilon+1 & w_1^* & \cdots & w_{d-1}^* \\ \varepsilon w_1^* & \varepsilon+1 & \cdots & w_{d-2}^* \\ \vdots & \vdots & \vdots & \vdots \\ \varepsilon w_{d-1}^* & \varepsilon w_{d-2}^* & \cdots & \varepsilon+1 \end{pmatrix}. \tag{3.5}$$

Recall that $w = p/q$ is in lowest terms. The assumptions (3.4) imply that both p and q must be reciprocal or skew-reciprocal polynomials of degree d. Let ε_p and ε_q be the corresponding signs: $p^* = \varepsilon_p p$ and $q^* = \varepsilon_q q$ with $\varepsilon = \varepsilon_p \varepsilon_q$. Note that we cannot have $\varepsilon_p = \varepsilon_q = -1$ since p and q are relatively prime by assumption.

We may give the *skew Bezoutian* bilinear form in a way analogous to the classical one. The new ingredient is the involution $\iota : T \mapsto T^{-1}$ of R that descends to V since it fixes the ideal (q^*). Indeed we have that $B^*(w)$ is the Gram matrix in the basis $1, T, \ldots, T^{d-1}$ of the bilinear form Ψ on V defined by

$$\Psi(u, v) := t\big(uv^\iota \cdot w\big) = \omega\big(uv^\iota\big),$$

where, with some notation abuse, $u, v \in V$. Concretely,

$$\Psi\big(T^i, T^j\big) = \omega\big(T^{i-j}\big), \quad i, j \in \mathbb{Z}. \tag{3.6}$$

This bilinear form satisfies

$$\Psi(v, u) = \varepsilon \Psi(u, v). \tag{3.7}$$

We will say that (V, Ψ) is an *ε-symmetric* bilinear space over k. By Proposition 3.1 this space is non-degenerate since p and q are relatively prime.

3.4. Properties

In addition to the bilinear form Ψ the skew Bezoutian carries some extra structures not shared by the classical Bezoutian. It has a distinguished vector v_0, the class of the polynomial $1 \in R$, with $\Psi(v_0, v_0) = 1 + \varepsilon$ and an isometry γ, given by multiplication by T (the fact that it is an isometry is clearly seen in (3.6), for example). Note that by construction γ has characteristic polynomial $\pm q$ (the monic generator of the ideal $(q^*) = (q)$). Moreover, the translates $v_0, \gamma(v_0), \gamma^2(v_0), \ldots$ generate the whole space V. In fact, these properties characterize the skew Bezoutian as we now show.

Given $v_0 \in V$ with $\Psi(v_0, v_0) = 1 + \varepsilon$ we define its associated *ε-reflection* to be the isometry given by

$$\sigma(v) := v - \Psi(v_0, v)v_0. \tag{3.8}$$

(In the skew-symmetric case σ is usually called a *transvection*.) Note that σ is of order two if $\varepsilon = +1$ but of infinite order if $\varepsilon = -1$. In fact,

$$\sigma^{-1}(v) := v - \varepsilon \Psi(v_0, v)v_0.$$

We have

$$\sigma(v_0) = -\varepsilon v_0, \qquad \sigma(v) = v, \quad \text{if } \Psi(v_0, v) = 0.$$

Hence σ fixes a codimension 1 subspace of V and $\det(\sigma) = -\varepsilon$.

Recall that an isometry of a non-degenerate bilinear space has a characteristic polynomial which is reciprocal or skew-reciprocal.

Theorem 3.3. *Let (V, Ψ) be a non-degenerate, finite dimensional, ε-symmetric bilinear space over k. Suppose there exists an isometry γ of this space and a vector $v_0 \in V$ such that*

(i) $\Psi(v_0, v_0) = 1 + \varepsilon$,
(ii) *V is generated by $v_0, \gamma v_0, \gamma^2 v_0, \dots$.*

Then (V, Ψ) is the skew Bezoutian $B^*(w)$ with $w = p/q$, where q is the characteristic polynomial of γ and p is the characteristic polynomial of $\gamma\sigma$ with σ the ε-reflection associated to v_0.

Proof. Let d be the dimension of V. Note that $\mathcal{V} := \{v_0, \gamma v_0, \dots, \gamma^{d-1} v_0\}$ is a basis of V. Indeed, by the Cayley–Hamilton theorem $\gamma^n v_0$ is in the span of $\mathcal{V}$ and hence so is every v in V by hypothesis (ii). Again by hypothesis (ii), $\mathcal{V}$ is linearly independent.

Define for every $n \in \mathbb{Z}$

$$c_n := \Psi\big(\gamma^n v_0, v_0\big). \tag{3.9}$$

Note that $c_{-n} = \varepsilon c_n$. We claim that

$$1 + \sum_{n \geqslant 1} c_n T^n$$

is the power series expansion of a rational function of denominator q. Write $q = \sum_{k \geqslant 0} q_k T^k$. By assumption $q_{d-k} = q_k$ for $k = 0, \dots, d$ and $q_0 = q_d = 1$. Then

$$q(T)\left(1 + \sum_{n \geqslant 1} c_n T^n\right) = \sum_{n \geqslant 0} r_n T^n = 1 + \sum_{n \geqslant 1} r_n T^n,$$

where $r_n = q_n + \sum_{k=1}^{n} c_k q_{n-k}$ for $n \geqslant 1$. Since $q_n = 0$ for $n > d$ we have

$$r_n = \sum_{k=0}^{d} c_{n-k} q_k = \sum_{k=0}^{d} c_{n-d+k} q_{d-k} = \sum_{k=0}^{d} c_{n-d+k} q_k, \quad n > d.$$

Hence

$$r_n = \Psi\big(\gamma^{n-d} q(\gamma) v_0, v_0\big) = 0, \quad n > d.$$

We now show that $r_{d-n} = -\varepsilon r_n$ for $n = 0, \dots, d$. Since $q(\gamma) = 0$ we have for $n < d$

$$r_{d-n} = q_n + \sum_{k=1}^{d-n} q_{n+k} c_k = q_n - \Psi\big(s_n(\gamma)\gamma^{-n} v_0, v_0\big),$$

where $s_n := \sum_{k=0}^{n} q_k T^k$. Hence

$$r_{d-n} = q_n - \sum_{k=0}^{n} q_k c_{k-n} = q_n - (1+\varepsilon) q_n - \varepsilon \sum_{k=0}^{n-1} q_k c_{n-k} = -\varepsilon r_n.$$

We have shown then that $p(T) := -\varepsilon \sum_{n=0}^{d} r_n T^n$ is $(-\varepsilon)$-reciprocal; since $r_0 = 1$ it is also monic. In other words, we have that (V, Ψ) is isometric to the skew Bezoutian $B^*(p, q)$.

It remains to show that p is the characteristic polynomial of $\delta := \gamma\sigma$. For every $n \in \mathbb{Z}$ let σ_n be the ε-reflection associated to $v_n := \gamma^n v_0$. Note that $\Psi(v_n, v_n) = 1 + \varepsilon$. We have

$$\sigma_n = \gamma^n \sigma \gamma^{-n}$$

and hence by induction

$$\delta^n = \sigma_1 \cdots \sigma_n \gamma^n.$$

Let $u_0 := v_0$ and $u_n := \sigma_n^{-1} \cdots \sigma_1^{-1} v_0$ for $n > 0$. Let also $e_n := \varepsilon\Psi(\delta^n v_0, v_0)$ for $n \in \mathbb{Z}$. Then

$$e_{n+1} = \Psi(v_0, \sigma_1 \cdots \sigma_{n+1} v_{n+1}) = \Psi(u_{n+1}, v_{n+1}).$$

Since

$$u_{n+1} = \sigma_{n+1}^{-1} u_n = u_n - \varepsilon\Psi(u_n, v_{n+1}) v_{n+1}, \quad n \geqslant 0$$

we get

$$e_{n+1} = \Psi(u_n, v_{n+1}) - \varepsilon\Psi(u_n, v_{n+1})\Psi(v_{n+1}, v_{n+1}) = -\varepsilon\Psi(u_n, v_{n+1}).$$

Therefore $u_{n+1} = u_n + e_{n+1} v_{n+1}$ and by induction

$$u_n = v_0 + \sum_{k=1}^{n} e_k v_k.$$

Finally,

$$-e_{n+1} = \Psi(v_{n+1}, u_n) = c_{n+1} + \sum_{k=1}^{n} e_k c_{n+1-k}$$

and

$$\left(1 + \sum_{n\geqslant 1} c_n T^n\right)\left(1 + \sum_{n\geqslant 1} e_n T^n\right) = 1. \tag{3.10}$$

Combined with our previous calculation we see that

$$p(T)\left(1 + \sum_{n\geqslant 1} e_n T^n\right) = -\varepsilon q(T).$$

So if $p(T) = \sum_{n=0}^{d} p_n T^n$ then

$$0 = \sum_{k=0}^{d} e_{n-d+k} p_{d-k} = -\varepsilon \sum_{k=0}^{d} e_{n-d+k} p_k, \quad n > d$$

and

$$\Psi\big(p(\delta)v_0, \delta^{d-n}v_0\big) = 0, \quad n > d. \tag{3.11}$$

It is not hard to see that $\delta^n v_0 = -\varepsilon v_n + \sum_{j=1}^{n-1} \alpha_{n,j} v_j$ for $n = 1, \dots, d-1$, for some $\alpha_{n,j} \in k$ (note that for $n = 1$ the equality is $\delta v_0 = -\varepsilon v_1$). It follows that the $\delta^n v_0$ with $n \in \mathbb{Z}$ span V and by (3.11) $p(\delta) = 0$. $\square$

Remark 3.4. The equivalence established by Theorem 3.3 is a skew analogue of that in Theorem 2.1, where the new ingredient is the involution $T \mapsto T^{-1}$ of the algebra $k[T, T^{-1}]/(q)$. A similar result appears in [9, Proposition 3.2].

3.5. *Hypergeometric groups*

We choose now $k = \mathbb{C}$. The subgroup $\Gamma \subseteq \mathrm{GL}(V)$ generated by γ, δ, σ (see Theorem 3.3) is a hypergeometric group in the sense of [7, Definition 3.1], with parameters the multisets of roots of p and q. In other words, we have a triple of elements in $\mathrm{GL}(V)$ which multiply to the identity, two of which have a prescribed characteristic polynomial and the third fixes a codimension one subspace of V. By a theorem of Levelt such triples are unique up to conjugation by $\mathrm{GL}(V)$ (see [7, Theorem 3.5]).

Since our polynomials are coprime it is proved in [7, Proposition 3.3 and Theorem 4.3] that Γ acts irreducibly. Furthermore, if we assume p and q have real coefficients, since they are (± 1)-reciprocal, Γ fixes a non-degenerate bilinear form Ψ on V which is unique up to scaling. Our discussion here shows that this form is none other than the skew Bezoutian $B^*(p, q)$ of p and q. This was mentioned in [22]. For general p and q with complex coefficients it is not hard to extend the construction of the skew-Bezoutian and this now yields a Hermitian form fixed by Γ.

Over $\mathbb{R}$ the signature σ of Ψ can be computed by a skew version of the classical theorem of Hermite [14, p. 409] for the usual Bezoutian. (Here $\varsigma := r - s$ if Ψ is isometric to $x_1^2 + \cdots + x_r^2 - y_1^2 - \cdots - y_s^2$ over $\mathbb{R}$.) For the classical Bezoutian the signature depends on the interlacing pattern of the roots of p and q in $\mathbb{R}$. For the skew Bezoutian it depends on the interlacing pattern of the roots on the unit circle S^1. In both cases this can be phrased in terms of the Cauchy index for the rational function p/q (on $\mathbb{R}$ for the classical case, on S^1 for the skew case; for the latter see [13, Theorem 2.1]).

A conceptual formulation of Hermite's result is as follows. The rational function $w = p/q \in \mathbb{R}[T]$ gives a continuous map $w : \mathbb{P}^1(\mathbb{R}) \to \mathbb{P}^1(\mathbb{R})$. In turn this yields a homomorphism $H_1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z}) \to H_1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z})$. After fixing an isomorphism $H_1(\mathbb{P}^1(\mathbb{R}), \mathbb{Z}) \simeq \mathbb{Z}$ this map is multiplication by some integer which is none other than the signature ς. The same applies for the skew Bezoutian. Since $w(T^{-1}) = -\varepsilon w(T)$ the values of w on S^1 are either real or purely imaginary. Hence w gives a continuous map $S^1 \to \mathbb{P}^1(\mathbb{R})$ in either case. This yields a map $\mathbb{Z} \to \mathbb{Z}$ via H_1 well defined up to sign. Choosing orientations appropriately this map is again multiplication by the signature ς (defined as zero in the skew symmetric case).

In practice one can compute ς using Sylverster's simple characterization (that applies equally well to both the classical and the skew cases). We associate to w a word ϕ in two letters say A and B as follows. Start with the empty word. Traverse $\mathbb{P}^1(R)$ or S^1 in the standard orientation starting at the base point ∞ or 1 respectively. Append A (resp. B) to ϕ on the right if you encounter a root of p (resp. q), including multiplicities, finishing when you reach back the base point. Now recursively remove from ϕ any instance of repeated symbols AA or BB. We end with a word consisting of r pairs $\cdots ABAB \cdots$ or $\cdots BABA \cdots$. Then ς equals r or $-r$ respectively.

In particular, Ψ is definite if and only if the roots of p and q interlace in the unit circle. This is one of the crucial calculations of [7] (see e.g. Theorem 4.8 in [7]), which was done directly without any reference to Hermite's result or its variants.

It is not hard to see [1, Proposition 2.3.3] that the number of words corresponding to signature ς is

$$\binom{d}{\frac{1}{2}(d-\varsigma)}^2.$$

(Necessarily $\varsigma \equiv d \bmod 2$; in fact in the symmetric case, if d is even then $\varsigma \equiv d \bmod 4$.) It follows that we should expect the signature to be typically small if p and q are picked in some random fashion. This appears to be indeed the case. For example, considering all pair of coprime polynomials with only cyclotomic factors and of degree 15 with $\epsilon = -1$ we find the following distribution of signatures

ς	15	13	11	9	7	5	3	1
#	25	118	179	5935	41 242	75 458	184 173	268 640

with symmetrical values for $\varsigma = -1, -3, \ldots, -15$.

3.6. Examples

We end this section with some examples. The skew Bezoutian construction can be done over a commutative ring (details will appear in a later publication). Here we work over $\mathbb{Z}$.

Alternate constructions for the first two examples below can be found in [5, Section 3]. In [5] the constructions use the trace form (as mentioned in the introduction) with respect to an extension $K/\mathbf{Q}$, where K is a suitable cyclotomic field. Examples in [5] and [4, §4] also include the Leech lattice, the Coxeter–Todd lattice, etc. See also [3, §1] for related work where the question of the existence of a definite unimodular lattice with an isometry having a prescribed cyclotomic characteristic polynomial is addressed.

1) Let

$$p = \Phi_1\Phi_2\Phi_3\Phi_5 = x^8 + 2x^7 + 2x^6 + x^5 - x^3 - 2x^2 - 2x - 1,$$
$$q = \Phi_{30} = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1,$$

where Φ_n is the n-th cyclotomic polynomial. Then

$$w = -p/q = 1 + x + x^2 + x^3 + x^4 + x^5 - x^{10} + O\left(x^{11}\right)$$

and

$$B^*(p/q) = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 \end{pmatrix}$$

The lattice $\mathbb{Z}[x]/(q)$ with this quadratic form is the well-known E_8 lattice and γ is a Coxeter element of the corresponding Weyl group.

2) Similarly the A_n lattice with Cartan matrix

$$C_n := \begin{pmatrix} 2 & -1 & 0 & \cdots & & 0 & 0 \\ -1 & 2 & -1 & \cdots & & & 0 \\ & & & \vdots & & & \\ 0 & & & \cdots & -1 & 2 & -1 \\ 0 & 0 & & \cdots & & -1 & 2 \end{pmatrix}$$

arises as the skew Bezoutian $B^*(p/q)$, where

$$p = x^n - 1, \qquad q = x^n + x^{n-1} + \cdots + x + 1$$

and γ represents an n-cycle in S_n.

3) Let $q = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ be the Lehmer polynomial (the integer polynomial of smallest known Mahler measure bigger than 1). For p, we search among the polynomials of degree 10 which are products of cyclotomics. We find eight such that $B^*(p,q)$ is isometric to the unimodular lattice $I_{9,1}$ of signature $(9,1)$. These are tabulated below.

$\Phi_1^3\Phi_2\Phi_3\Phi_5$	$x^{10} - x^8 - x^7 + x^3 + x^2 - 1$
$\Phi_1\Phi_2^3\Phi_3\Phi_5$	$x^{10} + 4x^9 + 7x^8 + 7x^7 + 4x^6 - 4x^4 - 7x^3 - 7x^2 - 4x - 1$
$\Phi_1\Phi_2\Phi_3\Phi_5\Phi_6$	$x^{10} + x^9 + x^8 + x^7 + x^6 - x^4 - x^3 - x^2 - x - 1$
$\Phi_1\Phi_2\Phi_3\Phi_7$	$x^{10} + 2x^9 + 2x^8 + x^7 - x^3 - 2x^2 - 2x - 1$
$\Phi_1\Phi_2\Phi_3\Phi_9$	$x^{10} + x^9 - x - 1$
$\Phi_1\Phi_2\Phi_3\Phi_{18}$	$x^{10} + x^9 - 2x^7 - 2x^6 + 2x^4 + 2x^3 - x - 1$
$\Phi_1\Phi_2\Phi_5\Phi_8$	$x^{10} + x^9 + x^6 - x^4 - x - 1$
$\Phi_1\Phi_2\Phi_5\Phi_{10}$	$x^{10} - 1$

We do not know if these isometries are in the same conjugacy class.

4) In the paper [21] the authors consider the modification $q(x) := p(x) \pm x^m$ of a monic reciprocal polynomial p of even degree $2m$ consisting of adding a single monomial $\pm x^m$. The skew Bezoutian $B^*(p,q)$ then yields a skew-symmetric form of determinant $\operatorname{Res}(p,q) = 1$ and a symplectic transformation of characteristic polynomial q. For example, if we again take q to be the Lehmer polynomial we see that it is also the characteristic polynomial of a symplectic transformation. As pointed out in [21, §4] it is remarkable that $q(x) + x^5$ is actually a product of cyclotomic polynomials.

In light of Theorem 3.3, the modification used in [21] can be seen as an example of modifying a symplectic transformation by multiplying it by a single transvection. It would be interesting to extend their results and study how this modification affects the Mahler measure of the characteristic polynomial.

4. Isometries with given characteristic polynomial

The goal of this section is to give a new and effective proof of the following well-known result (see, e.g. [20, Lemma 1.2 and Remarks 1.3, 1.4, 1.5]), using the skew Bezoutian.

We keep the notation of Section 3.

Theorem 4.1. *Let $q \in k[T]$ be a monic reciprocal polynomial of degree $d \geqslant 1$. Then*

1) *There exists a non-degenerate symmetric bilinear space over k of dimension d with an isometry of characteristic polynomial q.*
2) *If, in addition, d is even there exists a non-degenerate skew-symmetric bilinear space over k of dimension d with an isometry of characteristic polynomial q.*

For related work where a quadratic structure is prescribed as well see [6].

Proof. The main idea is to use the skew Bezoutian. If we can find a polynomial $p \in k[T]$, which is $(-\varepsilon)$-reciprocal and coprime to q then the skew Bezoutian $B^*(p,q)$ provides an explicit answer to what we are looking for. As discussed above, the skew Bezoutian comes equipped with an isometry of characteristic polynomial q and is non-degenerate if p and q are coprime. Knowledge of $\operatorname{Res}(p,q)$ will help us show that the bilinear form we construct is non-degenerate by Proposition 3.1.

In the skew-symmetric case, where $\varepsilon = -1$ and d is assumed even, we may always find such a p. Indeed, the polynomial

$$p(T) := q(T) + T^m,$$

where $m := d/2$ satisfies all the requirements we need: p is clearly reciprocal and coprime to q. Moreover we may easily compute $\operatorname{Res}(p,q)$. It is $(\prod_b b)^m$, where b runs over the roots of q counted with multiplicity, and this equals $q(0)^m$. Since q is monic and reciprocal $q(0) = 1$. See the remark following the proof for a discussion on the relevance of this computation.

Now we turn to the case where $\varepsilon = 1$. Let $\mathcal{Q}_0$ be the polynomial of $k[T]$ such that one has the factorization

$$q(T) = (T-1)^{\nu_+}(T+1)^{\nu_-}\mathcal{Q}_0(T), \qquad \mathcal{Q}_0(\pm 1) \neq 0. \tag{4.1}$$

As q is reciprocal, by the observations of Section 3.1, its order of vanishing ν_+ at 1 is even. Hence, $\mathcal{Q}_0$ is also reciprocal; let d_0 be its degree. Assume for the moment that $d_0 > 0$ and set

$$\mathcal{P}_0(T) := (T-1)^e(T+1)^{d_0-e},$$

for some odd integer $0 \leqslant e \leqslant d_0$. Note that $d_0 - e$ is odd also since d_0 is even as $\mathcal{Q}_0$ is a reciprocal polynomial not vanishing at -1 (see Section 3.1).

By construction $\mathcal{P}_0$ is monic, skew-reciprocal, of degree d_0 and coprime to $\mathcal{Q}_0$. The skew Bezoutian (V_0, Ψ_0) of $\mathcal{P}_0, \mathcal{Q}_0$ is then a non-degenerate symmetric bilinear space over k of dimension d_0. The corresponding isometry γ_0 has characteristic polynomial $\mathcal{Q}_0$. To obtain the space V we are after we consider

$$V := V_0 \perp V_+ \perp V_-$$

where $V_\pm$ is a vector space over k of dimension $\nu_\pm$. We put on $V_\pm$ an arbitrary non-degenerate symmetric bilinear form $\Psi_\pm$ and consider $\Psi := \Psi_0 \perp \Psi_+ \perp \Psi_-$ and $\gamma := \gamma_0 \perp \mathrm{id}_{V_+} \perp (-\mathrm{id}_{V_-})$. It is now clear that (V, Ψ) and γ fulfill the requirements.

The same construction works if $d_0 = 0$; just ignore V_0 altogether. This completes the proof of 1). $\square$

Remark 4.2. Note that the proof actually gives a (skew-)symmetric space and an isometry of characteristic polynomial q defined over the ring of coefficients of the polynomials p and q. In case 2) of Theorem 4.1 the determinant of this space is 1 as can be seen from the computation performed in the proof. For case 1), see Remark 6.3.

It seems natural to try and compute other invariants attached to the bilinear space constructed in terms of the polynomials p and q. In the following section we focus on the case $\varepsilon = 1$ and we investigate how the spinor norm of the isometry constructed in the proof of Theorem 4.1 can be expressed in terms of the polynomial q.

5. Spinor norm of an isometry with prescribed characteristic polynomial

Recall that if (V, Ψ) is a non-degenerate finite dimensional quadratic space, the spinor norm of an isometry of (V, Ψ) can be defined as follows: first let v be a non-isotropic vector of V and let r_v be the reflection with respect to the hyperplane $v^\perp$. We define the spinor norm $\mathrm{N}_{\mathrm{spin}}(r_v)$ to be the class in $k^\star/(k^\star)^2$ of $\Psi(v,v)$. Now any isometry σ of V is a product $\prod_v r_v$, where v runs over a finite set of non-isotropic vectors of V. It is known that $\sigma \mapsto \prod_v \Psi(v,v)$ gives a well-defined *spinor norm* homorphism

$$\mathrm{N}_{\mathrm{spin}} : O(V,\Psi) \to k^\star/\left(k^\star\right)^2,$$

which is onto as soon as $d := \dim V \geqslant 2$. Note in particular that $\mathrm{N}_{\mathrm{spin}}(-\mathrm{id}_V) = \det(V, \Psi)$, where $\det(V, \Psi) := \det(\Psi(v_i, v_j))$ for any basis $v_1, \ldots, v_d$ of V. (If $v_1, \ldots, v_d$ is an orthogonal basis of V then $-\mathrm{id}_V = \prod_{i=1}^{d} r_{v_i}$ and $\det V = \prod_{i=1}^{d} \Psi(v_i, v_i)$.)

We recall the following formula due to Zassenhaus (see [29, p. 444]) which gives a useful way to compute the spinor norm of an isometry. To state and prove the results of this section it will be convenient to use the following notation introduced by Zassenhaus in his original paper. If σ is an endomorphism of V and if $\lambda \in k$ then we let $M(\lambda, \sigma)$ be the maximal subspace of V on which $\sigma - \lambda \mathrm{id}_V$ acts as a nilpotent endomorphism of V. In particular the dimension of $M(\lambda, \sigma)$ is the multiplicity of λ as a root of the characteristic polynomial of σ.

Theorem 5.1 *(Zassenhaus). Let γ be an isometry of a non-degenerate quadratic space (V, Ψ) over k and let $\nu_\pm$ be the dimension of $M(\pm 1, \gamma)$. Let q be the characteristic polynomial of γ. Then $M(-1, \gamma)$ is non-degenerate and, if we denote by q_- the polynomial such that*

$$q(T) = (T+1)^{\nu_-} q_-(T), \qquad q_-(-1) \neq 0,$$

then

$$\mathrm{N}_{\mathrm{spin}}(\gamma) = \det\bigl(M(-1, \gamma), \Psi\bigr)(-2)^{-(\dim V - \nu_-)} q_-(-1),$$

in $k^\star/(k^\star)^2$.

Proof. Let us describe the main ideas of the proof based on Zassenhaus original paper [29, pp. 444–446]. Let us consider the subspace of V:

$$\widehat{M}(-1, \gamma) := \bigcap_{n \geqslant 1} (\sigma + \mathrm{id}_V)^n V.$$

Then Zassenhaus shows [29, Proposition 2, p. 437 and its corollary p. 438] that one has the orthogonal splitting

$$V = M(-1, \gamma) \perp \widehat{M}(-1, \gamma),$$

thus both these spaces are non-degenerate with respect to the restriction of Ψ. In particular the formula

$$\mathrm{sn}(\gamma) := \det\bigl(M(-1, \gamma), \Psi\bigr) \cdot \det\biggl(\frac{\gamma + \mathrm{id}_V}{2} \Bigm| \widehat{M}(-1, \gamma)\biggr), \tag{5.1}$$

defines a function on the orthogonal group $O(V, \Psi)$ with values in the classes modulo non-zero squares of $k^\star$. Zassenhaus then shows [29, Theorem, p. 446] that the map sn is a group homomorphism and that it coincides with $\mathrm{N}_{\mathrm{spin}}$ (see [29, (2.10b), p. 446]).

One has $M(-1, \gamma)^\perp = \widehat{M}(-1, \gamma)$ and the restriction of γ to $M(-1, \gamma)^\perp$ has characteristic polynomial q_-. Therefore (5.1) yields

$$\mathrm{N}_{\mathrm{spin}}(\gamma) = \det\bigl(M(-1, \gamma), \Psi\bigr) \cdot (-2)^{-(\dim V - \nu_-)} q_-(-1),$$

in $k^\star/(k^\star)^2$, which completes the proof. □

Corollary 5.2. *With notation as above fix an isometry γ of (V,Ψ). Let $q \in k[T]$ be the characteristic polynomial of γ and let $\mathcal{Q}_0 \in k[T]$ be as in (4.1). Then the spinor norm of γ is given by*

$$\mathrm{N}_{\mathrm{spin}}(\gamma) = \mathcal{Q}_0(-1)\det\bigl(M(-1,\gamma),\Psi\bigr),$$

in $k^\star/(k^\star)^2$.

Proof. With notation of Theorem 5.1 one has

$$q_-(T) = (T-1)^{\nu_+}\mathcal{Q}_0(T).$$

We deduce

$$\mathrm{N}_{\mathrm{spin}}(\gamma) = \det\bigl(M(-1,\gamma),\Psi\bigr)(-2)^{-(\dim V-\nu_-)}(-2)^{\nu_+}\mathcal{Q}_0(-1),$$

in $k^\star/(k^\star)^2$.
Therefore:

$$\begin{aligned}\mathrm{N}_{\mathrm{spin}}(\gamma) &= \det\bigl(M(-1,\gamma),\Psi\bigr)(-2)^{-(\dim V-(\nu_-+\nu_+))}\mathcal{Q}_0(-1)\\ &= \det\bigl(M(-1,\gamma),\Psi\bigr)(-2)^{d_0}\mathcal{Q}_0(-1),\end{aligned}$$

modulo non-zero squares. That is the desired formula since $d_0 := \deg \mathcal{Q}_0$ is even. □

From the above corollary we further deduce how to decide when we can prescribe the spinor norm and the characteristic polynomial of an isometry.

Corollary 5.3. *Let $q \in k[T]$ be a monic reciprocal polynomial of degree $d \geqslant 1$ and let $\mathcal{Q}_0 \in k[T]$ be as in (4.1).*

(i) *If $\nu_-(q) > 0$ then there exists a non-degenerate symmetric bilinear space over k of dimension d with an isometry γ of characteristic polynomial q and arbitrary spinor norm $\mathrm{N}_{\mathrm{spin}}(\gamma)$. In particular, this is true if d is odd.*
(ii) *If $\nu_-(q) = 0$ and γ is an isometry with characteristic polynomial q then its spinor norm equals $\mathcal{Q}_0(-1)$ (modulo non-zero squares). In particular, this is the case if q is separable and d is even.*

Proof. (i) Fix a representative s for a class in $k^\star/(k^\star)^2$. If $\nu_- > 0$ we can always choose V_- to have $\det(V_-) \equiv s\mathcal{Q}_0(-1) \bmod (k^\star)^2$. The result now follows from Corollary 5.2. If d is odd by the observations of Section 3.1 ν_- is odd and hence positive.

(ii) The first statement follows from Corollary 5.2. Assume q to be separable; if $\nu_-(q) > 0$ then the quotient $q(T)/(T+1)$ is a reciprocal polynomial of odd degree. So -1 is also a root of the quotient which contradicts the separability of q. □

6. Discriminant of a quadratic space having an isometry with prescribed characteristic polynomial

This section is devoted to the study of the relation between the discriminant of a quadratic space (V,Ψ) and the characteristic polynomial of an isometry of $O(V,\Psi)$. If (V,Ψ) is a quadratic space over k we let its *discriminant* be $\mathrm{disc}(V,\Psi) := (-1)^{n(n-1)/2}\det(V,\Psi)$ where $d := \dim V$.

The results we present here are well-known. The idea emphasized in the following statement (that can be found, e.g., in [20, Theorem 3.4]) is that to an ε-symmetric non-degenerate bilinear space (V,Ψ) equipped with an isometry γ, we can naturally associate a $(-\varepsilon)$-symmetric non-degenerate bilinear space (V,Ψ_γ).

Lemma 6.1. *Let (V, Ψ) be an ε-symmetric non-degenerate bilinear space and let γ be an isometry of (V, Ψ). We define the bilinear form Ψ_γ on V by:*

$$\Psi_\gamma(u, v) = \Psi\big(\big(\gamma - \gamma^{-1}\big)(u), v\big), \quad u, v \in V.$$

Denoting as before by q the characteristic polynomial of γ, we have:

(i) (V, Ψ_γ) *is* $(-\varepsilon)$*-symmetric,*
(ii) $\det(V, \Psi_\gamma) = q(1)q(-1) \det\gamma \det(V, \Psi)$,
(iii) γ *is an isometry of the bilinear space* (V, Ψ_γ).

Proof. First note that for any isometry γ of a bilinear space $(V, \langle\cdot,\cdot\rangle)$ and any element $h \in k[x, x^{-1}]$ we have

$$\big\langle h(\gamma)u, v\big\rangle = \big\langle u, h\big(\gamma^{-1}\big)v\big\rangle, \quad u, v \in V. \tag{6.1}$$

For (i) we fix $u, v \in V$ and we compute, using (6.1),

$$\Psi_\gamma(v, u) = \Psi\big(\big(\gamma - \gamma^{-1}\big)v, u\big) = \Psi\big(v, \big(\gamma^{-1} - \gamma\big)u\big) = -\Psi\big(v, \big(\gamma - \gamma^{-1}\big)u\big).$$

The right hand side equals $-\varepsilon\Psi_\gamma(u, v)$ since Ψ is ε-symmetric.

For (ii), we denote by d the dimension of V and we fix a basis $\mathcal{B} = (e_1, \ldots, e_d)$ of V. Let $\mathcal{Q}$ be the Gram matrix of Ψ with respect to $\mathcal{B}$ and M be the matrix representation of γ in the basis $\mathcal{B}$. The Gram matrix of Ψ_γ with respect to $\mathcal{B}$ is $(\Psi((\gamma - \gamma^{-1})e_i, e_j))_{i,j}$. That matrix equals ${}^t((M - M^{-1}))\mathcal{Q}$. Taking determinants we get

$$\det(V, \Psi_\gamma) = \det\big(M - M^{-1}\big) \det(V, \Psi) = \det\big(\gamma - \gamma^{-1}\big) \det(V, \Psi),$$

which is the formula we wanted since $\det(\gamma - \gamma^{-1}) = \det(\gamma)\det(\gamma^2 - \mathrm{id}_V) = \det(\gamma)q(-1)q(1)$.

Finally, (iii) is a straightforward consequence of the fact that γ and $\gamma - \gamma^{-1}$ commute. $\square$

The construction of the bilinear form Ψ_γ from the data (Ψ, γ) can be iterated to produce a sequence of bilinear forms $\Psi_0 = \Psi$, $\Psi_1 = \Psi_\gamma$, and more generally for any $j \geqslant 0$:

$$\Psi_j : (u, v) \in V \times V \mapsto \Psi\big(\big(\gamma - \gamma^{-1}\big)^j u, v\big).$$

The generalization of Lemma 6.1 to Ψ_j is straightforward and can be found in [20, Theorem 3.4]. Using Lemma 6.1 we deduce the following statement.

Proposition 6.2. *Let $q \in k[x]$ be a monic reciprocal polynomial with $q(\pm 1) \neq 0$. Then the discriminant* $\mathrm{disc}(V, \Psi)$ *of a non-degenerate quadratic space (V, Ψ) over k with an isometry of characteristic polynomial q is uniquely determined. More precisely, for any such space we have*

$$\det(V, \Psi) \equiv q(-1)q(1) \bmod \big(k^\star\big)^2.$$

This statement is well-known and can be found e.g. in [19, §7, Lemma c)].

Proof. We invoke Lemma 6.1(ii) in the case $\varepsilon = 1$. Indeed $\det\gamma = 1$ since q is reciprocal. Moreover the formula for $\det(V, \Psi_\gamma)$ implies that Ψ_γ is non-degenerate by our assumption on q and Ψ. Thus $\det(V, \Psi_\gamma)$ is a square since (V, Ψ_γ) is a non-degenerate skew-symmetric bilinear space. $\square$

Remark 6.3. In fact, from the proof of Theorem 4.1 we see that for every odd integer e in the range $0 \leqslant e \leqslant \deg q = d$ we can find (V, Ψ) defined over the ring of coefficients of q that satisfies:

$$\det(V, \Psi) = q(1)q(-1)^{d-e}.$$

From the above proposition we deduce the following corollary that answers the question investigated in this section.

Corollary 6.4. *Let (V, Ψ) be a non-degenerate quadratic space over k.*

(i) *Let q be a reciprocal polynomial which is the characteristic polynomial of an isometry γ of (V, Ψ). Then with notation as in Section 5 (in particular we use the factorization (4.1)),*

$$\det(V, \Psi) \equiv \det\bigl(M(-1, \gamma)\bigr) \det\bigl(M(1, \gamma)\bigr) \mathcal{Q}_0(-1)\mathcal{Q}_0(1) \bmod \bigl(k^\star\bigr)^2. \tag{6.2}$$

(ii) *Let q be a separable reciprocal polynomial in $k[T]$ of even degree. If there exists an isometry γ of a non-degenerate quadratic k-space (V, Ψ) of characteristic polynomial q then* $\operatorname{disc}(V, \Psi) \equiv \operatorname{disc}(q) \bmod (k^\star)^2$.

Proof. From [29, Proposition 2 and its corollary] and since we assume $\operatorname{char} k \neq 2$, one easily deduces the orthogonal decomposition:

$$V = M(1, \gamma) \perp M(-1, \gamma) \perp \bigl(\widehat{M}(1, \gamma) \cap \widehat{M}(-1, \gamma)\bigr). \tag{6.3}$$

Thus

$$\det V = \det M(1, \gamma) \det M(-1, \gamma) \det\bigl(\widehat{M}(1, \gamma) \cap \widehat{M}(-1, \gamma)\bigr),$$

where the quadratic structure on each vector space is given by the suitable restriction of Ψ.

Each subspace on the right hand side of (6.3) is stable under γ and by definition of the subspaces $M(\pm 1, \gamma)$, the restriction of γ to $\widehat{M}(1, \gamma) \cap \widehat{M}(-1, \gamma)$ has characteristic polynomial $\mathcal{Q}_0$. Thus (i) follows by applying Proposition 6.2.

The statement (ii) is an easy consequence of (i) and the following well-known lemma. □

Lemma 6.5. *Let $q \in k[x]$ be a monic separable reciprocal polynomial of even degree $2m$. Then*

$$\operatorname{disc} q \equiv (-1)^m q(-1)q(1) \bmod \bigl(k^\star\bigr)^2.$$

Proof. The hypothesis on q guarantees that $q(\pm 1) \neq 0$, i.e., $q = \mathcal{Q}_0$. Indeed, if q is reciprocal then ν_+ must be even. If in addition q is separable then $\nu_+(q) = 0$. As we argued in the proof of Corollary 5.3(ii) we also have $\nu_-(q) = 0$.

We may assume without loss of generality that q is irreducible. Let $K := k[x]/(q)$. The extension K/k is separable and $\operatorname{disc} q$ is the discriminant of the quadratic space (K, Ψ), where $\Psi(a, b) := \operatorname{Tr}_{K/k}(ab)$. A calculation like that in [12, Proposition A.3] (see also the discussion at the beginning of Section 2 in [2]) finishes the proof. (Let $L \subseteq K$ be the subfield fixed by the involution $x \mapsto x^{-1}$, and let $\mathbb{N}_{L/k}$ denote the norm map relative to L/k. Then $K = L(x - x^{-1})$. The subspaces L and $(x - x^{-1})L$ are orthogonal hence $\det K = \mathbb{N}_{L/k}(x - x^{-1}) \det L^2$ and $\mathbb{N}_{L/k}(x - x^{-1}) = q(-1)q(1)$.) □

For an alternate proof of the lemma see [10, Proof of Theorem 2]. The statement (ii) of Corollary 6.4 can be found e.g. in [2, Theorem (1.2)].

7. Isometries with given Jordan form

We end with a characterization of the Jordan form of isometries of non-degenerate bilinear spaces. The main result goes back to (at least) Wall [28] (see also [15], [20, Section 3] and [25, IV, 2.15 (iii)]). We include a proof for the reader's convenience using the skew Bezoutian to construct the isometries.

We assume our field k is now algebraically closed (and of characteristic different from 2 as before). Fix a vector space V of dimension r over k. For $\gamma \in \mathrm{End}(V), \lambda \in k^\star$ and $m \in \mathbb{N}$, let $\mu(\gamma; \lambda, m)$ be the number of Jordan blocks of γ of size m and eigenvalue λ.

We start with a few preparatory results. The following crucial statement (very close to the first part of [20, Theorem 3.2]), will help us perform a reduction step needed in the proof of Theorem 7.5.

Lemma 7.1. *Let (V, Ψ) be a non-degenerate ε-symmetric space equipped with a unipotent isometry γ. We have an orthogonal splitting*:

$$V = \perp_{m \geqslant 1} V^{(m)},$$

where γ acts on each $V^{(m)}$ as a sum of Jordan blocks $J_1(m)$. In particular, each $(V^{(m)}, \Psi)$ is a non-degenerate ε-symmetric space.

Proof. Let n be the largest index m with $V^{(m)} \neq 0$. We claim that $V^{(n)}$ is non-degenerate.

Since γ is unipotent and preserves $\mathrm{rad}(V^{(n)}, \Psi)$ we have $\mathrm{rad}(V^{(n)}, \Psi) \subseteq \ker(\gamma - \mathrm{id}_V) = \mathrm{Im}((\gamma - \mathrm{id}_V)^{n-1})$.

Taking $h(x) = (x-1)^{n-1}$ in (6.1) it follows that $\mathrm{rad}(V^{(n)}, \Psi) \subseteq \mathrm{rad}(V, \Psi)$ proving our claim. We deduce that $V^{(n)}$ splits off from V as an orthogonal direct summand.

We conclude by finite descending induction on $m \geqslant 1$. □

The following lemma can be seen as a complement to Lemma 6.1. In the notation of Lemma 6.1 it gives an additional property of Ψ_γ in the case where -1 is not an eigenvalue of γ. For any bilinear space $(W, \langle\cdot,\cdot\rangle)$, its *radical* $\mathrm{rad}(W)$ is the subspace $\{v \in W\colon \langle v, w\rangle = 0 \text{ for all } w \in W\}$.

Lemma 7.2. *With notation as in Lemma 6.1, we assume further that $\gamma + \mathrm{id}_V$ is invertible. Then we have*

$$\mathrm{rad}(V, \Psi_\gamma) = \ker(\gamma - \mathrm{id}_V).$$

Proof. Fix a vector $u \in V$. We have $u \in \mathrm{rad}(V, \Psi_\gamma)$ if and only if $\Psi((\gamma - \gamma^{-1})u, v) = 0$ for all $v \in V$. Since Ψ is non-degenerate, this is equivalent to $(\gamma - \gamma^{-1})u = 0$, i.e. $(\gamma^2 - \mathrm{id}_V)u = 0$. Rewriting the last equation

$$(\gamma + \mathrm{id}_V) \circ (\gamma - \mathrm{id}_V)u = 0,$$

the lemma follows since we have assumed $\gamma + \mathrm{id}_V$ to be invertible. □

Remark 7.3. As for the case of Lemma 6.1 the generalization of Lemma 7.2 to Ψ_j is straightforward. Let us mention for example that if Ψ is ε-symmetric then Ψ_j is $(-1)^j\varepsilon$-symmetric with radical $\ker((\gamma - \mathrm{id}_V)^j)$ (see [20, Theorem 3.4] where the general version of the construction is used).

Corollary 7.4. *With hypotheses as in Lemma 6.1, assume $\varepsilon = 1$ and γ unipotent. Consider the Jordan block decomposition of γ*:

$$\bigoplus_{i=1}^{r} J_{m_i}(1), \quad m_1 \leqslant m_2 \leqslant \cdots \leqslant m_r, \ \sum_i m_i = \dim V,$$

where $J_{m_i}(1)$ stands for the Jordan block of size m_i attached to the eigenvalue 1. *We have*

$$\sum_{i=1}^{r}(m_i-1)\equiv 0 \pmod 2.$$

In particular there are evenly many indices i for which m_i is even.

Proof. Since $(V/\mathrm{rad}(V,\Psi_\gamma),\Psi_\gamma)$ is a non-degenerate skew-symmetric space, its dimension is even. It follows then from Lemma 7.2 that $\dim V\equiv\dim\ker(\gamma-\mathrm{id}_V)\pmod 2$. Since γ is unipotent its number of Jordan blocks equals $\dim\ker(\gamma-\mathrm{id}_V)$ therefore

$$\sum_{i=1}^{r}m_i\equiv r \pmod 2.$$

Equivalently $\sum_{i=1}^{r}(m_i-1)$ is even. $\square$

We can now state and prove the main result of this section.

Theorem 7.5. *Let $\gamma\in\mathrm{End}(V)$. Then γ preserves a non-degenerate ε-symmetric bilinear form on V if and only if*

(i)

$$\mu(\gamma,\lambda,m)=\mu\big(\gamma,\lambda^{-1},m\big),\quad \lambda\neq\pm1,\ m\in\mathbb{N},$$

and

(ii)

$$(m-\delta)\mu(\gamma,\pm1,m)\equiv 0 \bmod 2,\quad m\in\mathbb{N},$$

where $\delta:=\frac{1}{2}(1+\varepsilon)$.

Proof. We give details for the orthogonal case $\varepsilon=1$ the symplectic case $\varepsilon=-1$ is completely analogous. For $m\geqslant 1$ let $J_m(\lambda)$ denote the Jordan block with size m and eigenvalue λ.

First we exhibit an isometry with a prescribed Jordan form satisfying the hypothesis (i) and (ii). Identify V with k^d. If $\gamma\in\mathrm{End}(V)$ is an endomorphism having Jordan form $M=J_m(\lambda)\oplus J_m(\lambda^{-1})$ with $\lambda\neq\lambda^{-1}$ consider $q=(T-\lambda)^m(T-\lambda^{-1})^m$. By Theorem 4.1 there exists a skew-reciprocal polynomial $p\in k[T]$ such that q is the characteristic polynomial of an isometry of the non-degenerate quadratic space determined by $B^*(p,q)$, which by Theorem 3.3 has Jordan form M. A similar argument applies to $J_m(\pm1)$ for m odd taking $q=(T-1)^m$ and $p=(T+1)^m$.

Finally, let m be even and set again $p:=(T+1)^m$ and $q:=(T-1)^m$. Now $U:=B^*(p,q)$, however, is skew-symmetric. Consider instead the symmetric matrix

$$A=\begin{pmatrix}0 & U\\ -U & 0\end{pmatrix}.$$

Since p and q are relatively prime U and hence also A yield non-degenerate bilinear pairings. By Theorems 3.3 and 4.1 there exists $\gamma^{\pm}$ with Jordan form $J_m(\pm1)$ preserving U. The map $\gamma:=\gamma^{\pm}\oplus\gamma^{\pm}$ then preserves A giving our desired isometry.

We now show that the conditions on the multiplicities of the Jordan blocks are necessary. Suppose then that $\gamma \in \mathrm{End}(V)$ preserves a non-degenerate, symmetric bilinear pairing $\langle\cdot,\cdot\rangle$ on V. It follows that as $k[x, x^{-1}]$-modules $V^* \simeq V$. This implies (i).

For $\lambda \in k^\star$ let $V_\lambda \subseteq V$ be the subspace annihilated by some power of $\gamma - \lambda$ and let $W_\lambda := V_\lambda \oplus V_{\lambda^{-1}}$ if $\lambda \neq \lambda^{-1}$ and $W_{\pm 1} := V_{\pm 1}$. Taking $h(x) = (x - \lambda)(x - \lambda^{-1})$ or $x - (\pm 1)$ in (6.1) we see that the distinct non-zero W_λ's are mutually orthogonal with orthogonal sum V and, in particular, they are non-degenerate. To prove (ii) we may hence assume without loss of generality that γ is unipotent so $V = V_1$.

Applying Lemma 7.1, we can restrict further to the case where $V = V^{(m)}$ is a non-degenerate quadratic space on which γ acts as a sum of $\mu(\gamma, 1, m)$ Jordan blocks $J_1(m)$.

Applying Corollary 7.4 to γ, we deduce that $\mu(\gamma, 1, m)(m - 1)$ is even, which is what we wanted to prove.

Note that in the skew-symmetric case (ii) follows directly from Lemma 7.1. Indeed γ restricts to a unipotent isometry of the non-degenerate skew-symmetric space $(V^{(m)}, \Psi)$. Thus the dimension $m\mu(\gamma, 1, m)$ of this space is even. $\square$

Acknowledgment

We would like to thank Eva Bayer for comments and suggestions on an earlier version of the paper as well as for pointing us to the relevant literature especially regarding references from knot theory.

References

[1] S. Adduci, On real and p-adic Bezoutians, Dissertation, The University of Texas at Austin, 2010, available at, http://repositories.lib.utexas.edu/bitstream/handle/2152/ETD-UT-2010-05-998/ADDUCI-DISSERTATION.pdf.
[2] R. Baeza, Discriminants of polynomials and of quadratic forms, J. Algebra 72 (1981) 17–28.
[3] E. Bayer-Fluckiger, Definite unimodular lattices having an automorphism of given characteristic polynomial, Comment. Math. Helv. 59 (1) (1984) 509–538.
[4] E. Bayer-Fluckiger, J. Martinet, Formes quadratiques liées aux algèbres semi-simples, J. Reine Angew. Math. 451 (1994) 51–69.
[5] E. Bayer-Fluckiger, Lattices and number fields, in: Algebraic Geometry: Hirzebruch 70, Warsaw, 1998, in: Contemp. Math., vol. 241, Amer. Math. Soc., Providence, RI, 1999, pp. 69–84.
[6] E. Bayer-Fluckiger, Isometries of quadratic spaces, J. Eur. Math. Soc. (2013), in press.
[7] F. Beukers, G. Heckman, Monodromy for the hypergeometric function ${}^nF_{n-1}$, Invent. Math. 95 (2) (1989) 325–354.
[8] C. Brunie, P. Saux Picart, Symmetric subresultants and applications, J. Symbolic Comput. 42 (9) (2007) 884–919.
[9] S. Donaldson, Nahm's equations and the classification of monopoles, Comm. Math. Phys. 96 (3) (1984) 387–407.
[10] B.H. Edwards, Rotations and discriminants of quadratic spaces, Linear Multilinear Algebra 8 (1980) 241–246.
[11] P.A. Fuhrmann, A Polynomial Approach to Linear Algebra, Second edition, Universitext, Springer, New York, 2012.
[12] B. Gross, C. McMullen, Automorphisms of even unimodular lattices and unramified Salem numbers, J. Algebra 257 (2) (2002) 265–290.
[13] N. Hamada, B. Anderson, The unit circle Cauchy index: definition, characterization and polynomial zero distribution, SIAM J. Appl. Math. 44 (4) (1984) 803–818.
[14] C. Hermite, Oeuvres de Charles Hermite. Volume 1, Cambridge Lib. Collect., Cambridge University Press, Cambridge, 2009.
[15] 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.
[16] M. Kervaire, C. Weber, A survey of multidimensional knots, Knot theory, in: Proc. Sem., Plans-sur-Bex, 1977, in: Lecture Notes in Math., vol. 685, Springer, Berlin, 1978, pp. 61–134.
[17] L. Kronecker, Zur Theorie der Elimination einer Variablen aus zwei algebraischen Gleichungen, in: Monatsber. Königl. Preussischen Akad. Wies., Berlin, 1881, pp. 535–600, Reprinted as in: Math. Werke, vol. 2, B.G. Teubner, Leipzig, 1897, pp. 113–192, or Chelsea, New York, 1968.
[18] T.Y. Lam, Introduction to Quadratic Forms Over Fields, Grad. Stud. Math., vol. 67, Amer. Math. Soc., Providence, RI, 2005.
[19] J. Levine, Invariants of knot cobrodism, Invent. Math. 8 (1969) 98–110.
[20] J. Milnor, On isometries of inner product spaces, Invent. Math. 8 (1969) 83–97.
[21] M. Mossinghoff, C. Pinner, J. Vaaler, Perturbing polynomials with all their roots on the unit circle, Math. Comp. 67 (224) (1998) 1707–1726.
[22] F. Rodriguez Villegas, Integral ratios of factorials and algebraic hypergeometric functions, arXiv:math/0701362.
[23] W. Scharlau, Zur Pfisterschen Theorie der quadratischen Formen, Invent. Math. 6 (1969) 327–328.
[24] W. Scharlau, Induction theorems and the structure of the Witt group, Invent. Math. 11 (1970) 37–44.
[25] T.A. Springer, R. Steinberg, Conjugacy classes, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Math., vol. 131, Springer-Verlag, Berlin, New York, 1970, pp. 167–266.
[26] H.F. Trotter, On S-equivalence of Seifert matrices, Invent. Math. 20 (1973) 173–207.

[27] H.F. Trotter, Knot module and Seifert matrices. Knot theory, in: Proc. Sem., Plans-sur-Bex, 1977, in: Lecture Notes in Math., vol. 685, Springer, Berlin, 1978, pp. 291–299.
[28] G. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Aust. Math. Soc. 3 (1963) 1–62.
[29] H. Zassenhaus, On the spinor norm, Arch. Math. 13 (1962) 434–451.