Operators
and
Matrices
Volume 17, Number 3 (2023), 639–651 doi:10.7153/oam-2023-17-42

MINIMAL GENERATING AND SEPARATING SETS FOR $O(3)$–INVARIANTS OF SEVERAL MATRICES

RONALDO JOSÉ SOUSA FERREIRA AND ARTEM LOPATIN*

(*Communicated by I. Klep*)

Abstract. Given an algebra $\mathbb{F}[H]^G$ of polynomial invariants of an action of the group G over the vector space H, a subset S of $\mathbb{F}[H]^G$ is called separating if S separates all orbits that can be separated by $\mathbb{F}[H]^G$. A minimal separating set is found for some algebras of matrix invariants of several matrices over an infinite field of arbitrary characteristic different from two in case of the orthogonal group. Namely, we consider the following cases:

- $GL(3)$-invariants of two matrices;
- $O(3)$-invariants of $d>0$ skew-symmetric matrices;
- $O(4)$-invariants of two skew-symmetric matrices;
- $O(3)$-invariants of two symmetric matrices.

A minimal generating set is also given for the algebra of orthogonal invariants of three 3×3 symmetric matrices.

1. Introduction

1.1. Definitions

All vector spaces, algebras, and modules are over an infinite field $\mathbb{F}$ of an arbitrary characteristic $p=\mathrm{char}\,\mathbb{F}\geqslant 0$, unless otherwise stated. By an algebra we always mean an associative algebra.

Given $n>1$ and $d\geqslant 1$, we consider the polynomial algebras

$$\begin{aligned}
R\ &= \mathbb{F}[x_{ij}(k)\mid 1\leqslant i,j\leqslant n,\quad 1\leqslant k\leqslant d];\\
R_+ &= \mathbb{F}[x_{ij}(k)\mid 1\leqslant j\leqslant i\leqslant n,\ 1\leqslant k\leqslant d];\\
R_- &= \mathbb{F}[x_{ij}(k)\mid 1\leqslant j< i\leqslant n,\ 1\leqslant k\leqslant d].
\end{aligned}$$

together with $n\times n$ *generic* matrices X_k, *symmetric generic* matrices Y_k and *skew-symmetric generic* matrices Z_k:

$$(X_k)_{ij}=x_{ij}(k),\qquad (Y_k)_{ij}=\begin{cases} x_{ij}(k), & \text{if } i\geqslant j\\ x_{ji}(k), & \text{if } i<j\end{cases},\qquad (Z_k)_{ij}=\begin{cases} x_{ij}(k), & \text{if } i>j\\ 0, & \text{if } i=j\\ -x_{ji}(k), & \text{if } i<j\end{cases}.$$

Mathematics subject classification (2020): 16R30, 15B10, 13A50.

Keywords and phrases: Invariant theory, matrix invariants, classical linear groups, separating invariants, generators, positive characteristic.

This research was supported by FAPESP 2016/00541-0 and FAEPEX 2449/18.

* Corresponding author.

Here $(A)_{ij}$ stands for the $(i,j)^{\text{th}}$ entry of a matrix A. The t^{th} coefficient of the characteristic polynomial of an $n\times n$ matrix A is denoted by $\sigma_t(A)$. As an example, $\mathrm{tr}(A)=\sigma_1(A)$ and $\det(A)=\sigma_n(A)$. Denote by $M(n)$ the space of all $n\times n$ matrices over $\mathbb{F}$, $S_+(n)=\{A\in M(n)\,|\,A^T=A\}$, $S_-(n)=\{A\in M(n)\,|\,A^T=-A\}$ and $O(n)=\{A\in M(n)\,|\,AA^T=I_n\}$. Consider the algebras of *matrix invariants* $R^{GL(n)}$, $R^{O(n)}$, $R_+^{O(n)}$, $R_-^{O(n)}$, respectively, that are generated by $\sigma_t(b)$, where $1\leqslant t\leqslant n$ and b ranges over all monomials in

- $X_1,\ldots,X_d$ (see [22], [20], [7]),
- $X_1,\ldots,X_d,X_1^T,\ldots,X_d^T$ (see [20], [29]), where $p\neq 2$,
- $Y_1,\ldots,Y_d$ (see [30] or [14]), where $p\neq 2$,
- $Z_1,\ldots,Z_d$ (see [30] or [14]), where $p\neq 2$,

respectively. Note that in case $p=0$ or $p>n$ the algebras of invariants considered above are generated by $\mathrm{tr}(b)$, where b is the same as above. In what follows, whenever we consider the orthogonal group $O(n)$ or algebras $R^{O(n)}$, $R_+^{O(n)}$, $R_-^{O(n)}$, we assume that $p\neq 2$. The ideal of relations between the generators of $R^{GL(n)}$ was described in [21, 20, 28]. In case $p=0$ relations between generators of $R^{O(n)}$ were computed in [20] and in case $p\neq 2$ relations between generators of matrix $O(n)$-invariants were obtained in [16] and [17].

The elements of R, R_+, R_-, respectively, can be interpreted as polynomial functions from

- $H=M(n)\oplus\cdots\oplus M(n)$,
- $H_+=S_+(n)\oplus\cdots\oplus S_+(n)$,
- $H_-=S_-(n)\oplus\cdots\oplus S_-(n)$,

respectively, to $\mathbb{F}$ as follows: $x_{ij}(k)$ sends $u=(A_1,\ldots,A_d)\in H$ to $(A_k)_{i,j}$. We can consider H as $GL(n)$-module by the formula: $g\cdot v=(gA_1g^{-1},\ldots,gA_dg^{-1})$ for $g\in GL(n)$ and $v=(A_1,\ldots,A_d)\in H$. Then H_+ and H_- are $O(n)$-modules.

Assume that (G,A,V) is one of the following triples: $(GL(n),R,H)$, $(O(n),R,H)$, $(O(n),R_+,H_+)$, $(O(n),R_-,H_-)$. Then

$$A^G=\{f\in A\,|\,f(g\cdot v)=f(v)\text{ for all }g\in G,\ v\in V\}$$

(see the papers above mentioned, where the generators for the algebras of invariants were found).

The notion of separating invariants was introduced in 2002 by Derksen and Kemper [2] as a weaker concept than generating invariants. Given a subset S of A^G, we say that elements u,v of V *are separated by* S if exists an invariant $f\in S$ with $f(u)\neq f(v)$. If $u,v\in V$ are separated by A^G, then we simply say that they *are separated.* A subset $S\subset A^G$ of the invariant ring is called *separating* if for any u,v from V that are separated we have that they are separated by S. Separating sets over finite fields were studied in a recent paper [10].

It follows from more general result of Domokos [3] and Draisma, Kemper, Wehlau [8] that for any $n>1$ there exists $C(n)$, which does not depend on d, such that the set of all elements of A^G of degree less than $C(n)$ is separating for all d. On the other hand, in case $0<p\leqslant n$ a similar statement is not valid for generating systems for $R^{GL(n)}$ (see [4]) and $R^{O(n)}$ (see [19]).

In [9] it was established that the set

$$\begin{array}{ll} \mathrm{tr}(X_i),\ \det(X_i), & 1\leqslant i\leqslant d,\\ \mathrm{tr}(X_iX_j), & 1\leqslant i<j\leqslant d,\\ \mathrm{tr}(X_iX_jX_k), & 1\leqslant i<j<k\leqslant d. \end{array}$$

is a minimal (by inclusion) separating set for the algebra of matrix invariants $R^{GL(2)}$ for any $d\geqslant 1$. The case of three nilpotent 3×3 matrices over an algebraically closed field of zero characteristic was considered in [1]. A minimal separating set for the algebra $R^{SL(2)\times SL(2)}$ of semi-invariants of 2×2 matrices over an arbitrary algebraically closed field was explicitly described in [5, 6].

In this paper we will establish minimal (by inclusion) separating sets for the following algebras of invariants:

- $R^{GL(3)}$ for $d=2$ (see Theorem 3.1), namely,

$$\sigma_t(X_i),\ i=1,2,\ t=1,2,3;$$
$$\mathrm{tr}(X_1X_2),\ \mathrm{tr}(X_1^2X_2),$$
$$tr(X_1X_2^2),\ \mathrm{tr}(X_1^2X_2^2),\ \mathrm{tr}(X_1^2X_2^2X_1X_2);$$

- $R_-^{O(3)}$ for all $d>0$, where $p\neq 2$ (see Theorem 4.2), namely,

$$\sigma_2(Z_i);$$
$$tr(Z_iZ_j),\ i<j;\ \mathrm{tr}(Z_iZ_jZ_k),\ i<j<k,$$

  where $1\leqslant i,j,k\leqslant d$;

- $R_-^{O(4)}$ for $d=2$, where $p\neq 2$ (see Theorem 5.1), namely,

$$\sigma_2(Z_i),\ \det(Z_i),\ i=1,2;$$
$$\mathrm{tr}(Z_1Z_2),\ \sigma_2(Z_1Z_2),\ \mathrm{tr}(Z_1^2Z_2^2),\ \mathrm{tr}(Z_1^3Z_2),\ \mathrm{tr}(Z_1Z_2^3);$$

- $R_+^{O(3)}$ for $d=2$, where $p\neq 2$ (see Theorem 6.1), namely,

$$\sigma_t(Y_i),\ i=1,2,\ t=1,2,3;\ \ \mathrm{tr}(Y_1Y_2),\ \mathrm{tr}(Y_1^2Y_2),\ \mathrm{tr}(Y_1Y_2^2),\ \mathrm{tr}(Y_1^2Y_2^2).$$

  We will establish that the last set is a minimal generating set for $R_+^{O(3)}$ for $d=2$.

We will also construct a minimal generating set for $R_{+}^{O(3)}$ for $d=3$ (see Theorem 7.1), namely,

$$\sigma_t(Y_i),\ i,t\in\{1,2,3\};\ \operatorname{tr}(Y_iY_j),\ \operatorname{tr}(Y_i^2Y_j),\ \operatorname{tr}(Y_iY_j^2),\ \operatorname{tr}(Y_i^2Y_j^2),\ 1\leqslant i<j\leqslant 3;$$
$$\operatorname{tr}(Y_1Y_2Y_3),$$
$$\operatorname{tr}(Y_1^2Y_2Y_3),\ \operatorname{tr}(Y_2^2Y_1Y_3),\ \operatorname{tr}(Y_3^2Y_1Y_2),\ \ \operatorname{tr}(Y_1^2Y_2^2Y_3),\ \operatorname{tr}(Y_1^2Y_3^2Y_2),\ \operatorname{tr}(Y_2^2Y_3^2Y_1).$$

Note that over a field of real numbers a minimal generating set for $R_{+}^{O(3)}$ for each $d>0$ was constructed by Spencer and Rivlin in series of papers [23, 24, 25, 26] (see also [27]).

1.2. Notations

For a monomial $c\in R$ denote by $\deg c$ its *degree* and by $\operatorname{mdeg} c$ its *multidegree*, i.e., $\operatorname{mdeg} c=(t_1,\ldots,t_d)$, where t_k is the total degree of the monomial c in $x_{ij}(k)$, $1\leqslant i,j\leqslant n$, and $\deg c=t_1+\cdots+t_d$. Obviously, the algebras $R^{GL(n)}$, $R^{O(n)}$, $R_{+}^{O(n)}$, $R_{-}^{O(n)}$ have $\mathbb{N}$-grading by degrees and $\mathbb{N}^d$-grading by multidegrees.

Denote by E_{ij} the matrix such that the $(i,j)^{\text{th}}$ entry is equal to one and the rest of entries are zeros. For short, we write J_3 for $E_{12}+E_{23}$.

2. Decomposable invariants

In this section we assume $n=3$ and $d>0$. We consider some fact about decomposable invariants that we are going to apply later.

Assume that a triple (G,A,V) is the same as in Section 1. We say that an $\mathbb{N}$-homogeneous invariant $f\in A^G$ is *decomposable* and write $f\equiv 0$ if f is a polynomial in $\mathbb{N}$-homogeneous invariants of A^G of strictly lower degree. If f is not decomposable, then we say that f is *indecomposable* and write $f\not\equiv 0$. In case $f-h\equiv 0$ we write $f\equiv h$. Denote by $P_{\mathbb{F}}$ the ring of polynomials in $Y_1,\ldots,Y_d$ without free terms and by P the set of (non-empty) products of $Y_1,\ldots,Y_d$ and set $P_1=P\sqcup\{I_3\}$.

Consider the surjective homomorphism $\Psi: R^{GL(n)}\to R_{+}^{O(n)}$ defined by $x_{ij}(k)\to x_{ij}(k)$ in case $i\geqslant j$ and by $x_{ij}(k)\to x_{ji}(k)$ otherwise. Note that the image of $\operatorname{tr}(X_{i_1}\cdots X_{i_k})$ with respect to Ψ is $\operatorname{tr}(Y_{i_1}\cdots Y_{i_k})$.

LEMMA 2.1. *Assume $p\neq 2$, $x,y\in P$ and $q\in P_{\mathbb{F}}$. Then the next formulas hold in $R_{+}^{O(3)}$:*

(a) $\operatorname{tr}(xyx^2q)\equiv-\operatorname{tr}(x^2yxq)$*;*

(b) $\operatorname{tr}(Y_1^2Y_2^iY_1Y_3^j)\equiv 0$ *for* $i,j=1,2$*;*

(c) $\operatorname{tr}(Y_1^2Y_2^2Y_1Y_2)\equiv 0$*;*

(d) $\operatorname{tr}(Y_1^2Y_2^2Y_3^2)\equiv 0$ *if* $p\neq 3$*;*

(e) $\mathrm{tr}(y^2x^2yxq) \equiv -\mathrm{tr}(x^2y^2xyq)$*;*

(f) $\mathrm{tr}(Y_1^2Y_2^2Y_1Y_2Y_3^i) \equiv 0$ *for* $i=1,2$*;*

Proof. **(a)** Applying the homomorphism Ψ to formula (20) of [12] we obtain the required.

For the sake of completeness, we show that part (a) can also be proven by straightforward calculations. Namely, part (a) follows from the next equality, which holds for every 3×3 matrices A,B,C over any commutative ring:

$$\begin{gathered}\mathrm{tr}(A^2BAC)+\mathrm{tr}(ABA^2C)\\ =\mathrm{tr}(A)\Big(-\mathrm{tr}(A^2CB)+\mathrm{tr}(ABAC)+\mathrm{tr}(BA^2C)-\mathrm{tr}(AB)\,\mathrm{tr}(AC)-\mathrm{tr}(B)\,\mathrm{tr}(A^2C)\Big)\\ +\sigma_2(A)\Big(\mathrm{tr}(ACB)-\mathrm{tr}(BAC)+\mathrm{tr}(B)\,\mathrm{tr}(AC)\Big)\\ -\det(A)\,\mathrm{tr}(BC)+\mathrm{tr}(A^3C)\,\mathrm{tr}(B)+\mathrm{tr}(A^2C)\,\mathrm{tr}(AB)+\mathrm{tr}(AC)\,\mathrm{tr}(A^2B).\end{gathered}$$

(b) Applying the equality $\mathrm{tr}(A^T)=\mathrm{tr}(A)$ that holds for any matrix A and part (a) of the lemma we obtain

$$\mathrm{tr}(Y_1^2Y_2^iY_1Y_3^j)=\mathrm{tr}(Y_3^jY_1Y_2^iY_1^2)=\mathrm{tr}(Y_1Y_2^iY_1^2Y_3^j)\equiv-\mathrm{tr}(Y_1^2Y_2^iY_1Y_3^j)$$

in $R_+^{O(3)}$. Since $p\neq 2$, the proof of part (b) is completed.

(c) Making the substitution $Y_3\to Y_2$ in part (b) of this lemma, where $i=2$ and $j=1$, we obtain the required.

(d) Since $p\neq 3$, applying the homomorphism Ψ to part 7 of Lemma 18 from [13] we obtain

$$\mathrm{tr}(Y_1^2Y_2^2Y_3^2)\equiv-\mathrm{tr}(Y_1^2Y_3^2Y_2^2)=-\mathrm{tr}(Y_1^2Y_2^2Y_3^2).$$

Since we also have that $p\neq 2$, the proof of part (d) is completed.

(e) Formula (14) of [12], which is valid for any p, together with Lemma 3 of [12] imply that the analogue of part (e) of this lemma is valid for $R^{GL(3)}$. The application of homomorphism Ψ concludes the proof of part (e).

(f) Applying two times part (a) of the lemma to $f=\mathrm{tr}(Y_3^iY_2Y_1Y_2^2Y_1^2)$ we obtain that

$$f\equiv\mathrm{tr}(Y_3^iY_2^2Y_1^2Y_2Y_1)\equiv-\mathrm{tr}(Y_3^iY_1^2Y_2^2Y_1Y_2),$$

where the second equivalence follows from part (e) of the lemma. On the other hand, $f=\mathrm{tr}(Y_3^iY_1^2Y_2^2Y_1Y_2)$ and the proof of part (f) is completed. □

3. Invariants of two 3×3 matrices

THEOREM 3.1. *For $d=2$ the following set is a minimal separating set for the algebra $R^{GL(3)}$ of $GL(3)$-invariants of two matrices:*

$$\begin{gathered}\operatorname{tr}(X_i),\ \sigma_2(X_i),\ \det(X_i),\ i=1,2,\\ \operatorname{tr}(X_1X_2),\ \operatorname{tr}(X_1^2X_2),\ \operatorname{tr}(X_1X_2^2),\ \operatorname{tr}(X_1^2X_2^2),\\ \operatorname{tr}(X_1^2X_2^2X_1X_2).\end{gathered}$$

Proof. Denote the set from the formulation of the theorem by S. It is well-known that S generates $R^{GL(3)}$ (for example, see [11]). Thus S is a separating set. To prove that S is a minimal separating set we will show that for any element $f\in S$ the set $S_0=S\backslash\{f\}$ is not separating.

The case of f from the list $\operatorname{tr}(X_i)$, $\sigma_2(X_i)$, $\det(X_i)$ $(i=1,2)$ is obvious.

Assume $f=\operatorname{tr}(X_1X_2)$. Then for $A_1=B_1=J_3$ (see Section 1.2), $A_2=E_{32}$, $B_2=E_{12}$ we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set.

Assume $f=\operatorname{tr}(X_1^2X_2)$. Then for

$$A_1=B_1=J_3,\qquad A_2=\begin{pmatrix}0&1&1\\0&1&-1\\0&1&-1\end{pmatrix},\quad B_2=\begin{pmatrix}0&0&0\\1&0&0\\-1&0&0\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set. Similarly, we consider the case of $f=\operatorname{tr}(X_1X_2^2)$.

Assume $f=\operatorname{tr}(X_1^2X_2^2)$. Then for

$$A_1=B_1=J_3,\qquad A_2=\begin{pmatrix}0&1&0\\0&-1&0\\1&1&1\end{pmatrix},\quad B_2=\begin{pmatrix}0&1&0\\1&0&0\\1&0&0\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set.

Assume $f=\operatorname{tr}(X_1^2X_2^2X_1X_2)$. Then for

$$A_1=B_1=J_3,\qquad A_2=\begin{pmatrix}1&0&0\\1&-1&0\\1&-1&0\end{pmatrix},\quad B_2=\begin{pmatrix}-1&0&0\\0&0&1\\1&0&1\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set. The theorem is proven. □

4. Orthogonal invariants of several 3×3 skew-symmetric matrices

LEMMA 4.1. *The set*

$$\sigma_2(Z_1),\ \sigma_2(Z_2),\ \mathrm{tr}(Z_1Z_2)$$

is a minimal separating set for the algebra $I=R_-^{O(3)}$ for $d=2$ in case $p\neq 2$.

Proof. Denote the set from the formulation of the lemma by S. The set S generates the algebra of invariants I (for example, see Theorem 1.4 of [15]). Thus S is a separating set. To prove that S is a minimal separating set we will show that for any element $f\in S$ the set $S_0=S\backslash\{f\}$ is not separating.

The case of $f=\sigma_2(Z_i)$ $(i=1,2)$ is obvious.

Assume $f=\mathrm{tr}(Z_1Z_2)$. Then for $A_1=A_2=B_1=-B_2=E_{12}-E_{21}$ we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set. The lemma is proven. □

THEOREM 4.2. *Assume $d>0$ and $p\neq 2$. Then the set*

$$\sigma_2(Z_i),\ 1\leqslant i\leqslant d,$$
$$\mathrm{tr}(Z_iZ_j),\ 1\leqslant i<j\leqslant d,$$
$$\mathrm{tr}(Z_iZ_jZ_k),\ 1\leqslant i<j<k\leqslant d,$$

is a minimal separating set for the algebra $R_-^{O(3)}$ of $O(3)$-invariants of d skew-symmetric matrices.

Proof. Denote the set from the formulation of the theorem by S. By Theorem 1.4 of [15] the set S generates the algebra of invariants $R_-^{O(3)}$. Hence S is a separating set for $R_-^{O(3)}$. Applying Lemma 4.1 we obtain that to prove that S is a minimal separating set it is enough to show that in case $d=3$ the set $S_0=S\backslash\{\mathrm{tr}(Z_1Z_2Z_3)\}$ is not separating.

For $A_1=B_1=E_{12}-E_{21}$, $A_3=B_3=E_{13}-E_{31}$, and

$$A_2=\begin{pmatrix}0&0&1\\0&0&1\\-1&-1&0\end{pmatrix},\quad B_2=\begin{pmatrix}0&0&1\\0&0&-1\\-1&1&0\end{pmatrix}$$

we have that $u=(A_1,A_2,A_3)$ and $v=(B_1,B_2,B_3)$ are not separated by S_0, but $\mathrm{tr}(Z_1Z_2Z_3)$ separates u and v in case $p\neq 2$. Thus S_0 is not a separating set. The theorem is proven. □

5. Orthogonal invariants of two 4×4 skew-symmetric matrices

THEOREM 5.1. *Assume $d=2$ and $p\neq 2$. Then the set*

$$\sigma_2(Z_i),\ \det(Z_i),\ i=1,2,$$
$$\mathrm{tr}(Z_1Z_2),\ \sigma_2(Z_1Z_2),\ \mathrm{tr}(Z_1^2Z_2^2),\ \mathrm{tr}(Z_1^3Z_2),\ \mathrm{tr}(Z_1Z_2^3),$$

is a minimal separating set for the algebra $R_{-}^{O(4)}$ of $O(4)$-invariants of two skew-symmetric matrices.

Proof. Assume $d=2$. Denote the set from the formulation of the theorem by S. By Theorem 1.1 of [18], the set S generates the algebra of invariants $R_{-}^{O(4)}$. Hence S is a separating set for $R_{-}^{O(4)}$. To prove that S is a minimal separating set we will show that for any element $f\in S$ the set $S_0=S\backslash\{f\}$ is not separating.

If f is $\sigma_2(Z_1)$ or $\mathrm{tr}(Z_1Z_2)$, then S_0 is not separating by Lemma 4.1.

Assume $f=\det(Z_1)$. For

$$A_1=\begin{pmatrix} 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & -1 & 0 & 0\\ -1 & 0 & 0 & 0 \end{pmatrix},\qquad B_1=\begin{pmatrix} 0 & 1 & 0 & 1\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$A_2=B_2=0$ we have that $u=(A_1,A_2)$ and $v=(B_1,B_2)$ are not separated by S_0, but $\det(Z_1)$ separates u and v. Thus S_0 is not a separating set.

Assume $f=\sigma_2(Z_1Z_2)$. For

$$A_1=\begin{pmatrix} 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0 \end{pmatrix},\quad A_2=B_2=\begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ -1 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 \end{pmatrix},\quad B_1=\begin{pmatrix} 0 & -1 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0 \end{pmatrix}$$

we have that $u=(A_1,A_2)$ and $v=(B_1,B_2)$ are not separated by S_0, but $\sigma_2(Z_1Z_2)$ separates u and v. Thus S_0 is not a separating set.

Assume $f=\mathrm{tr}(Z_1^2Z_2^2)$. For

$$A_1=\begin{pmatrix} 0 & 1 & 1 & 1\\ -1 & 0 & -1 & -2\\ -1 & 1 & 0 & -1\\ -1 & 2 & 1 & 0 \end{pmatrix},\qquad A_2=\begin{pmatrix} 0 & -1 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$B_1=\begin{pmatrix} 0 & -2 & 0 & -1\\ 2 & 0 & 0 & 2\\ 0 & 0 & 0 & 0\\ 1 & -2 & 0 & 0 \end{pmatrix},\qquad B_2=\begin{pmatrix} 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\\ -1 & 0 & 0 & 1\\ 0 & 0 & -1 & 0 \end{pmatrix}$$

we have that $u=(A_1,A_2)$ and $v=(B_1,B_2)$ are not separated by S_0, but $\mathrm{tr}(Z_1^2Z_2^2)$ separates u and v. Thus S_0 is not a separating set.

Assume $f=\mathrm{tr}(Z_1Z_2^3)$. For

$$A_1=B_1=\begin{pmatrix} 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 1\\ -1 & -1 & 0 & 0\\ -1 & -1 & 0 & 0 \end{pmatrix},\ A_2=\begin{pmatrix} 0 & 1 & 0 & 1\\ -1 & 0 & 0 & -1\\ 0 & 0 & 0 & 1\\ -1 & 1 & -1 & 0 \end{pmatrix},\ B_2=\begin{pmatrix} 0 & 1 & 0 & -1\\ -1 & 0 & 0 & 1\\ 0 & 0 & 0 & 1\\ 1 & -1 & -1 & 0 \end{pmatrix}$$

we have that $u=(A_1,A_2)$ and $v=(B_1,B_2)$ are not separated by S_0, but $\mathrm{tr}(Z_1Z_2^3)$ separates u and v. Thus S_0 is not a separating set. The case of $f=\mathrm{tr}(Z_1^3Z_2)$ is similar. The theorem is proven. □

6. Orthogonal invariants of two 3×3 symmetric matrices

THEOREM 6.1. *Assume that $p\neq 2$ and $d=2$. Then the set*

$$\mathrm{tr}(Y_i),\ \sigma_2(Y_i),\ \det(Y_i),\ i=1,2,$$
$$\mathrm{tr}(Y_1Y_2),\ \mathrm{tr}(Y_1^2Y_2),\ \mathrm{tr}(Y_1Y_2^2),\ \mathrm{tr}(Y_1^2Y_2^2)$$

is a minimal generating set and a minimal separating set for the algebra of $O(3)$-invariants $R_+^{O(3)}$ of two symmetric matrices.

Proof. Denote by S the set from the formulation of the theorem and by S_X the result of substitutions $Y_i\to X_i$ $(i=1,2)$ in S. It is well-known that $S_X\cup\{\mathrm{tr}(X_1^2X_2^2X_1X_2)\}$ generates $R^{GL(3)}$ in case $d=2$ (for example, see [11]). Considering the surjective homomorphism Ψ from Section 2 we obtain that $S\cup f$ generates $R_+^{O(3)}$, where $f=\mathrm{tr}(Y_1^2Y_2^2Y_1Y_2)$. Since f is decomposable in $R_+^{O(3)}$ by part (b) of Lemma 2.1, then S generates $R_+^{O(3)}$. Thus S is a separating set. To prove that S is a minimal separating set we will show that for any element $f\in S$ the set $S_0=S\backslash\{f\}$ is not separating.

Assume $f=\mathrm{tr}(Y_1Y_2)$. Then for

$$A_1=B_1=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},\quad A_2=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix},\quad B_2=\begin{pmatrix}1&0&0\\0&-1&0\\0&0&0\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set.

Assume $f=\mathrm{tr}(Y_1^2Y_2)$. Then for

$$A_1=B_1=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix},\quad A_2=\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix},\quad B_2=\begin{pmatrix}1&0&0\\0&-1&0\\0&0&0\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set. The case of $f=\mathrm{tr}(Y_1Y_2^2)$ is similar.

Assume $f=\mathrm{tr}(Y_1^2Y_2^2)$. Then for

$$A_1=\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix},\quad A_2=B_1=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix},\quad B_2=\begin{pmatrix}0&0&0\\0&1&0\\0&0&-1\end{pmatrix}$$

we have that (A_1,A_2) and (B_1,B_2) are not separated by S_0, but f separates (A_1,A_2) and (B_1,B_2). Thus S_0 is not a separating set.

The cases of $f=\sigma_k(Y_i)$ $(i=1,2,\ k=1,2,3)$ are trivial. For the sake of completeness, we point out that in case $f=\det(Y_1)$ we consider

$$A_1=-B_1=\begin{pmatrix}1&0&0\\0&1&0\\0&0&-2\end{pmatrix},\quad A_2=B_2=0.$$

Therefore, S is a minimal separating set. This result together with the fact that S is a generating set imply that S is a minimal generating set for $R_+^{O(3)}$. □

7. Orthogonal invariants of three 3×3 symmetric matrices

THEOREM 7.1. *For $d=3$ consider the following set S:*

$$\begin{gathered}\operatorname{tr}(Y_i),\ \sigma_2(Y_i),\ \det(Y_i),\ i=1,2,3,\\ \operatorname{tr}(Y_iY_j),\ \operatorname{tr}(Y_i^2Y_j),\ \operatorname{tr}(Y_iY_j^2),\ \operatorname{tr}(Y_i^2Y_j^2),\ 1\leqslant i<j\leqslant 3,\\ \operatorname{tr}(Y_1Y_2Y_3),\\ \operatorname{tr}(Y_1^2Y_2Y_3),\ \operatorname{tr}(Y_2^2Y_1Y_3),\ \operatorname{tr}(Y_3^2Y_1Y_2),\\ \operatorname{tr}(Y_1^2Y_2^2Y_3),\ \operatorname{tr}(Y_1^2Y_3^2Y_2),\ \operatorname{tr}(Y_2^2Y_3^2Y_1).\end{gathered}$$

Then the set

- *S, if $p\neq 2,3$,*
- *$S\cup\{\operatorname{tr}(Y_1^2Y_2^2Y_3^2)\}$, if $p=3$,*

is a minimal generating set for the algebra of $O(3)$-invariants $R_+^{O(3)}$ of three symmetric matrices.

Proof. Denote by S_1 the set from the formulation of the theorem. We split the proof into two parts, namely, at first we show that S_1 generates $R_+^{O(3)}$ and then we prove that S_1 is minimal.

(a) We apply Ψ to the (minimal) generating set for $R^{GL(3)}$ from Theorem 1 of [11] and obtain that $R_+^{O(3)}$ is generated by $S\cup G_1$ in case $p\neq 2,3$ and by $S\cup G_1\cup G_2$ in case $p=3$. Here G_1 is the set

$$\begin{gathered}f_{ij}=\operatorname{tr}(Y_i^2Y_j^2Y_iY_j),\ i<j;\quad \operatorname{tr}(Y_1Y_3Y_2);\quad h_1=\operatorname{tr}(Y_1^2Y_2^2Y_3^2);\\ \operatorname{tr}(Y_i^2Y_jY_k),\ j>k;\quad \operatorname{tr}(Y_i^2Y_j^2Y_k),\ i>j;\\ r_{ijk}=\operatorname{tr}(Y_i^2Y_jY_iY_k),\ j<k;\quad s_{ijk}=\operatorname{tr}(Y_i^2Y_j^2Y_iY_k),\end{gathered}$$

where $1\leqslant i,j,k\leqslant 3$ are pairwise different, and G_2 is the set

$$\begin{gathered}h_2=\operatorname{tr}(Y_1^2Y_3^2Y_2^2),\\ a_{ijk}=\operatorname{tr}(Y_iY_j^2Y_k^2Y_jY_k),\quad b_{ijk}=\operatorname{tr}(Y_i^2Y_j^2Y_iY_k^2),\quad c_{ijk}=\operatorname{tr}(Y_i^2Y_j^2Y_k^2Y_jY_k),\end{gathered}$$

where $j<k$, $1\leqslant i,j,k\leqslant 3$ are pairwise different. Parts (b), (c), (f) of Lemma 2.1 imply that f_{ij}, r_{ijk}, s_{ijk}, a_{ijk}, b_{ijk}, c_{ijk} are decomposable in $R_{+}^{O(3)}$. It follows from part (d) of Lemma 2.1 that h_1 and h_2 are decomposable in $R_{+}^{O(3)}$ in case $p\neq 3$. Finally, the equalities $\mathrm{tr}(Y_1Y_3Y_2)=\mathrm{tr}(Y_1Y_2Y_3)\in S$, $\mathrm{tr}(Y_i^2Y_jY_k)=\mathrm{tr}(Y_i^2Y_kY_j)$, $\mathrm{tr}(Y_i^2Y_j^2Y_k)=\mathrm{tr}(Y_j^2Y_i^2Y_k)$, and $h_1=h_2$ imply that S_1 generates the algebra $R_{+}^{O(3)}$.

(b) Since all elements of S have pairwise different multidegrees, to show that S is a minimal generating set it is enough to establish that all elements of S_1 are indecomposable in $R_{+}^{O(3)}$. Then by Theorem 6.1 we can only verify the following claims:

(1) $f_1=\mathrm{tr}(Y_1Y_2Y_3)$ is indecomposable,

(2) $f_2=\mathrm{tr}(Y_1^2Y_2Y_3)$ is indecomposable,

(3) $f_3=\mathrm{tr}(Y_1^2Y_2^2Y_3)$ is indecomposable,

(4) $f_4=\mathrm{tr}(Y_1^2Y_2^2Y_3^3)$ is indecomposable in case $p=3$.

Assume that f_1 is decomposable, i.e., f_1 is a polynomial in invariants of lower degree. Then it is easy to see that

$$\mathrm{tr}(A_1A_2A_3)=0 \tag{1}$$

for all nilpotent matrices $A_1,A_2,A_3\in S_{+}(3)$ with entries in $\mathbb{F}$. Moreover, equality (1) is valid for any extension of $\mathbb{F}$. In particular, we can assume that $\mathbb{F}$ is algebraically closed.

We will use the following symmetric nilpotent matrices as tests:

$$R_1=\begin{pmatrix}0&1&0\\1&0&\mathbb{I}\\0&\mathbb{I}&0\end{pmatrix},\ R_2=\begin{pmatrix}1&1&0\\1&-3&2\mathbb{I}\sqrt{2}\\0&2\mathbb{I}\sqrt{2}&2\end{pmatrix},\ R_3=\begin{pmatrix}0&-1&0\\-1&0&\mathbb{I}\\0&\mathbb{I}&0\end{pmatrix}$$

$$T_1=\begin{pmatrix}1&\mathbb{I}&0\\\mathbb{I}&-1&0\\0&0&0\end{pmatrix},\ T_2=\begin{pmatrix}1&-\mathbb{I}&0\\-\mathbb{I}&-1&0\\0&0&0\end{pmatrix},\ T_3=\begin{pmatrix}1&0&\mathbb{I}\\0&0&0\\\mathbb{I}&0&-1\end{pmatrix},$$

where $\mathbb{I}^2=-1$. Note that $T_i^2=0$ for $i=1,2,3$.

We have $\mathrm{tr}(T_1T_2T_3)=2\neq 0$; a contradiction to equality (1).

Assume that f_2 is decomposable. Then it is easy to verify that there exists $\alpha\in\mathbb{F}$ such that

$$\mathrm{tr}(A_1^2A_2A_3)=\alpha\,\mathrm{tr}(A_1A_2)\,\mathrm{tr}(A_1A_3) \tag{2}$$

for all nilpotent matrices $A_1,A_2,A_3\in S_{+}(3)$ with entries in $\mathbb{F}$, which we assume to be algebraically closed. For $\underline{A}=(A_1,A_2,A_3)=(T_1,T_2,T_3)$ equality (2) implies $\alpha=0$. Hence for $\underline{A}=(R_1,R_2,T_1)$ equality (2) imply $1+(1-2\sqrt{2})\mathbb{I}=0$. It is easy to see that the obtained equality does not hold in case $p\neq 2$.

Assume that f_3 is decomposable. Then it is easy to verify that there exist $\alpha,\beta,\gamma\in\mathbb{F}$ such that

$$\mathrm{tr}(A_1^2A_2^2A_3)=\alpha\,\mathrm{tr}(A_1A_2)\,\mathrm{tr}(A_1A_2A_3)+\beta\,\mathrm{tr}(A_1A_3)\,\mathrm{tr}(A_1A_2^2)+\gamma\mathrm{tr}(A_2A_3)\,\mathrm{tr}(A_1^2A_2) \quad (3)$$

for all nilpotent matrices $A_1,A_2,A_3\in S_+(3)$ with entries in $\mathbb{F}$, which we assume to be algebraically closed. Considering $\underline{A}=(T_1,T_2,T_3)$ in equality (3) we obtain $\alpha=0$. For $\underline{A}=(T_1,R_1,T_2)$ equality (3) implies $\beta=0$. If $\underline{A}=(R_1,T_1,T_2)$ in equality (3), then we have $\gamma=0$. Finally, for $\underline{A}=(R_1,R_2,T_1)$ equality (3) imply $2(\mathbb{I}-1)(\sqrt{2}-1)=0$; a contradiction.

Assume that f_4 is decomposable. It is easy to verify that there exist $\alpha_i,\beta_i,\gamma,\delta\in\mathbb{F}$ $(i=1,2,3)$ such that $\mathrm{tr}(A_1^2A_2^2A_3^3)=$

$$\begin{gathered}\alpha_1\,\mathrm{tr}(A_1^2A_2A_3)\,\mathrm{tr}(A_2A_3)+\alpha_2\,\mathrm{tr}(A_2^2A_1A_3)\,\mathrm{tr}(A_1A_3)+\alpha_3\,\mathrm{tr}(A_3^2A_1A_2)\,\mathrm{tr}(A_1A_2)\\ +\beta_1\,\mathrm{tr}(A_1^2A_3)\,\mathrm{tr}(A_2^2A_3)+\beta_2\,\mathrm{tr}(A_1^2A_2)\,\mathrm{tr}(A_3^2A_2)+\beta_3\,\mathrm{tr}(A_2^2A_1)\,\mathrm{tr}(A_3^2A_1)\\ +\gamma\mathrm{tr}(A_1A_2A_3)^2+\delta\,\mathrm{tr}(A_1A_2)\,\mathrm{tr}(A_1A_3)\,\mathrm{tr}(A_2A_3)\end{gathered}$$

for all nilpotent matrices $A_1,A_2,A_3\in S_+(3)$ with entries in $\mathbb{F}$, which we assume to be algebraically closed. Making the substitution $\underline{A}=(T_1,T_2,T_3)$ in the above equality we obtain $\delta=-\gamma$. Then, consequently considering substitutions $\underline{A}=(R_1,T_1,T_2)$, $\underline{A}=(T_1,R_1,T_2)$ and $\underline{A}=(T_1,T_2,R_1)$ we obtain that $\alpha_1=\alpha_2=\alpha_3=2\gamma$. Similarly, substitutions $\underline{A}=(R_1,R_2,T_1)$, $\underline{A}=(R_1,T_1,R_2)$ and $\underline{A}=(T_1,R_1,R_2)$ imply that $\beta_1=\beta_2=\beta_3=-\gamma$. Finally, applying the substitution $\underline{A}=(R_1,R_2,R_3)$ we get $6\gamma=-1$, which is a contradiction in case $p=3$. Therefore, S_1 is a minimal generating set for $R_+^{O(3)}$. □

REFERENCES

[1] F. B. CAVALCANTE, A. LOPATIN, *Separating invariants of three nilpotent* 3×3 *matrices*, Linear Algebra and its Applications **607** (2020), 9–28.

[2] H. DERKSEN AND G. KEMPER, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I. Encyclopaedia of Mathematical Sciences, 130, Springer-Verlag, Berlin, 2002. x+268 pp.

[3] M. DOMOKOS, *Typical separating invariants*, Transform. Groups **12** (2007), 49–63.

[4] M. DOMOKOS, S. G. KUZMIN, A. N. ZUBKOV, *Rings of matrix invariants in positive characteristic*, J. Pure Appl. Algebra **176** (2002), 61–80.

[5] M. DOMOKOS, *Characteristic free description of semi-invariants of* 2×2 *matrices*, J. Pure Appl. Algebra **224** (2020), no. 5, 106220.

[6] M. DOMOKOS, *Addendum to "Characteristic free description of semi-invariants of* 2×2 *matrices" [J. Pure Appl. Algebra 224 (2020), no. 5, 106220]*, J. Pure Appl. Algebra **224** (2020), no. 6, 106270.

[7] S. DONKIN, *Invariants of several matrices*, Invent. Math. **110** (1992), 389–401.

[8] J. DRAISMA, G. KEMPER, D. WEHLAU, *Polarization of separating invariants*, Canad. J. Math. **60**, (2008) no. 3, 556–571.

[9] I. KAYGORODOV, A. LOPATIN, YU. POPOV, *Separating invariants for* 2×2 *matrices*, Linear Algebra and its Applications **559** (2018), 114–124.

[10] G. KEMPER, A. LOPATIN, F. REIMERS, *Separating invariants over finite fields*, Journal of Pure and Applied Algebra **226** (2022), 106904.

[11] A. A. LOPATIN, *The invariant ring of triples of* 3×3 *matrices over a field of arbitrary characteristic*, Sibirsk. Mat. Zh. **45** (2004), no. 3, 624–633 (Russian), English translation: Siberian Mathematical Journal **45** (2004), no. 3, 513–521.

[12] A. A. LOPATIN, *The algebra of invariants of 3×3 matrices over a field of arbitrary characteristic*, Commun. Algebra **32** (2004), no. 7, 2863–2883.

[13] A. A. LOPATIN, *Relatively free algebras with the identity $x^3 = 0$*, Commun. Algebra **33** (2005), no. 10, 3583–3605.

[14] A. A. LOPATIN, *Invariants of quivers under the action of classical groups*, J. Algebra **321** (2009), 1079–1106.

[15] A. A. LOPATIN, *Orthogonal invariants of skew-symmetric matrices*, Linear and Multilinear Algebra **59** (2011), 851–862.

[16] A. A. LOPATIN, *Relations between $O(n)$-invariants of several matrices*, Algebras and Representation Theory **15** (2012), 855–882.

[17] A. A. LOPATIN, *Free relations for matrix invariants in the modular case*, Journal of Pure and Applied Algebra **216** (2012), 427–437.

[18] A. A. LOPATIN, *Minimal system of generators for $O(4)$-invariants of two skew-symmetric matrices*, Linear and Multilinear Algebra, **66** (2018), no. 2, 347–356.

[19] A. A. LOPATIN, *Indecomposable orthogonal invariants of several matrices over a field of positive characteristic*, International Journal of Algebra and Computation **21** (2021), no. 1, 161–171.

[20] C. PROCESI, *The invariant theory of $n\times n$ matrices*, Adv. Math. **19** (1976), 306–381.

[21] YU. P. RAZMYSLOV, *Trace identities of full matrix algebras over a field of characteristic 0*, Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), no. 4, 723–756 (Russian), English translation: Math. USSR Izv. **8** (1974), no. 4, 727–760.

[22] K. S. SIBIRSKII, *Algebraic invariants of a system of matrices*, Sibirsk. Mat. Zh. **9** (1968), no. 1, 152–164 (Russian), English translation: Soviet Math. Dokl. **8** (1967), 36–40.

[23] A. J. M. SPENCER, R. S. RIVLIN, *The theory of matrix polynomials and its application to the mechanics of isotropic continua*, Arch. Rational Mech. Anal. **2** (1958/1959), 309–336.

[24] A. J. M. SPENCER, R. S. RIVLIN, *Finite integrity bases for five or fewer symmetric 3×3 matrices*, Arch. Rational Mech. Anal. **2** (1958/1959), 435–446.

[25] A. J. M. SPENCER, *Further results in the theory of matrix polynomials*, Arch. Rational Mech. Anal. **4** (1960), 214–230.

[26] A. J. M. SPENCER, *The invariants of six symmetric 3×3 matrices*, Arch. Rational Mech. Anal. **7** (1961), 64–77.

[27] A. J. M. SPENCER, *Theory of invariants*, Continuum Physics, vol. I, part III, Academic Press, New York, 1971.

[28] A. N. ZUBKOV, *On a generalization of the Razmyslov–Procesi theorem*, Algebra and Logic **35** (1996), no. 4, 241–254.

[29] A. N. ZUBKOV, *Invariants of an adjoint action of classical groups*, Algebra and Logic **38** (1999), no. 5, 299–318.

[30] A. N. ZUBKOV, *Invariants of mixed representations of quivers I*, J. Algebra Appl. **4** (2005), no. 3, 245–285.

(Received June 14, 2022)

Ronaldo José Sousa Ferreira
Federal University of Maranhão
Rua Santa Clara, 2010, Grajaú 65940-000, MA, Brazil
e-mail: ronaldoj.sf@hotmail.com

Artem Lopatin
State University of Campinas
Sergio Buarque de Holanda, 651, Campinas 13083-859, SP, Brazil
e-mail: dr.artem.lopatin@gmail.com