Article

The Square-Zero Basis of Matrix Lie Algebras

Raúl Durán Díaz [1,*], **Víctor Gayoso Martínez** [2,*], **Luis Hernández Encinas** [2] and **Jaime Muñoz Masqué** [2]

1   Departamento de Automática, Universidad de Alcalá, E-28871 Alcalá de Henares, Spain
2   Instituto de Tecnologías Físicas y de la Información (ITEFI) Consejo Superior de Investigaciones Científicas (CSIC), E-28006 Madrid, Spain; luis@iec.csic.es (L.H.E.); jaime@iec.csic.es (J.M.M.)
*   Correspondence: raul.duran@uah.es (R.D.D.); victor.gayoso@iec.csic.es (V.G.M.)

check for updates

Abstract: A method is presented that allows one to compute the maximum number of functionally-independent invariant functions under the action of a linear algebraic group as long as its Lie algebra admits a basis of square-zero matrices even on a field of positive characteristic. The class of such Lie algebras is studied in the framework of the classical Lie algebras of arbitrary characteristic. Some examples and applications are also given.

Keywords: invariant function; Lie algebra of matrices; linear algebraic groups; linear representation; square-zero matrix

MSC: primary 14L24; secondary 11E57; 12J15; 13A50; 14L35; 15B33; 17B10; 17B15; 20G05; 20G15; 20G40

1. Introduction

The modern theory of invariants of linear representations was formulated in the fundamental book [1], which currently represents an essential chapter in the theory of group representations (cf. MSC2020: 20Cxx). Several interesting expositions and applications of this theory to algebraic and differential geometry can be seen, for example, in [2–4].

For finite groups, the main results are well known. The ring of invariants of a finite group is known to be generated by a finite number of algebraically independent homogeneous polynomials (Hilbert's finiteness theorem) if and only if such a group is a group of reflections (Shephard–Todd–Chevalley theorem), and in general, there is also a bound (Noether's degree bound) for the number of generators of their invariant algebra. Furthermore, there are algorithms for computing fundamental invariants (see, e.g., ([4] §2.5), [5]).

In the case of matrix groups with positive dimension, the situation is much more complex. Actually, there are only three procedures to calculate a basis for the vector space of invariants of fixed degree (cf. ([4] §4.5)): (1) the Ω-process, (2) solving equations arising from the Lie algebra action, and (3) generating invariants in symbolic representation. The second procedure reduces the problem to linear algebra and is especially well suited to computational methods (e.g., see ([4] §2.5) [5,6]), since it linearizes the calculation of invariants to that of the "infinitesimal" invariants associated with the induced representation of the Lie algebra of the group. In fact, if $\rho\colon G \to GL(V)$ is a linear representation of a connected affine group defined over a ground field $\mathbb{F}$, then ρ induces a Lie-algebra homomorphism $\rho_*\colon \mathfrak{g} \to \mathfrak{gl}(V)$, and in the case $\mathbb{F} = \mathbb{C}$, the invariant functions are the first integrals of the vector space defined by the image of ρ_*.

Unfortunately, classical invariant theory is developed in the setting of complex vector spaces, which allows the passage from the group to its Lie algebra, and more importantly, from the Lie algebra to the group, via the exponential map. But in positive characteristic the exponential map does not

exist, and therefore, the procedure (2) is invalidated. While the most outstanding difference between affine algebraic groups on $\mathbb{C}$ and those defined on a field of positive characteristic is undoubtedly the inexistence of exponential map for the latter ones, other important differences exist as well (see, for example, ([7] III-5)).

A summary of contents of the article is as follows: First of all, in Section 3, the class of Lie subalgebras $\mathfrak{g} \subseteq \mathfrak{gl}(n,\mathbb{F})$ admitting a (vector-space) basis of square-zero matrices, is considered. For the sake of simplicity we call this class in the sequel, SQZ-LA class. Square-zero matrices have been dealt with in several settings and with different purposes; for example, see [8–13], among other papers and authors.

We will consider such matrices in connection with the aforementioned problem of linearizing the calculation of invariants of a representation of an affine algebraic group defined on a field of positive characteristic.

Next, the main result of the paper (Theorem 1) is presented, which states that if $\rho\colon G \to GL(n,\mathbb{F})$ is a linear representation of a linear algebraic group G and its Lie algebra $\mathfrak{g}$ is in the SQZ-LA class, then every G-invariant function $\mathcal{I} \in \mathbb{F}[V^*]$ is a common first-integral of the system of derivations $\rho_*(X)$, $\forall X \in \mathfrak{g}$, and the number of algebraically independent G-invariant functions in $\mathbb{F}[V^*]$ is upper-bounded by the difference $n^2 - r$, where r is the generic rank of the $\mathbb{F}[V^*]$-module $\mathcal{M}$ spanned by all the derivations $\rho_*(X)$. Several consequences of Theorem 1 are deduced and specific examples are explained in detail.

Having established the importance of the SQZ-LA class of Lie algebras, Section 4 is devoted to study which ones of the usual Lie algebras belong to this class. Among them, the Lie algebras of the special linear group and of the symplectic group over an arbitrary field are proven to belong to the SQZ-LA class; see Propositions 1 and 3, respectively.

Special types of matrices have also connections with several applications. For example, it is noticeable that skew-symmetric matrices, a class dealt with in the present work can appear in modeling mechanical systems, a field with active research (e.g., see [14,15]). Nilpotent matrices (we deal in particular with square-zero matrices) appear customarily when modeling differential-algebraic control systems, usually known as descriptor linear systems (e.g., see [16]).

Among other standing-out instances, we can also count the cases of special and symplectic groups—having many applications in mechanics, symplectic geometry and topology—for which the structure of their algebra of G-invariant functions under a linear representation is proven to be an $\mathbb{F}$-algebra of polynomials (see Corollary 1 below).

Some counterexamples are also included, and certain Lie algebras in characteristic 2 with geometric interest are proved to be in the SQZ-LA class as well.

The article closes with an exposition of the conclusions.

2. Terminology and Notation

If $\mathbb{F}$ is a field, then a subset $\mathcal{X} \subseteq \mathbb{F}^m$ is said to be "algebraic" if there exist a finite set of polynomials $P_1, \ldots, P_k \in \mathbb{F}[X_1, \ldots, X_m]$ such that

$$\mathcal{X} = \{x = (x_1, \ldots, x_m) \in \mathbb{F}^m : P_1(x) = \ldots P_k(x) = 0\}.$$

If $\mathcal{X}$ is an algebraic subset in $X \subseteq \mathbb{F}^m$, then the ring of algebraic functions on $\mathcal{X}$ is denoted by $\mathbb{F}[\mathcal{X}] = \mathbb{F}[X_1, \ldots, X_m]/I_{\mathcal{X}}$, where $I_{\mathcal{X}}$ denotes the ideal in $\mathbb{F}[X_1, \ldots, X_m]$ of polynomials vanishing over $\mathcal{X}$.

If $I_{\mathcal{X}}$ is a prime ideal, the field of fractions of $\mathbb{F}[\mathcal{X}]$ is denoted by $\mathbb{F}(\mathcal{X})$. In general, notation for algebraic sets has been taken from [17].

The algebra of $n \times n$ matrices with entries in $\mathbb{F}$ is denoted by $\mathfrak{gl}(n,\mathbb{F})$, which is considered as a Lie algebra by means of the Lie bracket given by $[A, B] = AB - BA$, $\forall A, B \in \mathfrak{gl}(n,\mathbb{F})$, where on the right-hand side, the product denotes a matricial product.

Furthermore, $G \subseteq GL(n, \mathbb{F})$ denotes the group of invertible $n \times n$ matrices with entries in $\mathbb{F}$ endowed with the group structure defined by matrix multiplication, and $\mathfrak{gl}(n, \mathbb{F})$ is identified with its Lie algebra.

The algebraic ring of the group $G \subseteq GL(n, \mathbb{F})$ is the set of quotients $\frac{P}{\delta^n}$, where $P \in \mathbb{F}[\mathfrak{gl}(n, \mathbb{F})]$ is a polynomial, $n \in \mathbb{N}$, and $\delta \colon \mathfrak{gl}(n, \mathbb{F}) \to \mathbb{F}$ is the function $\delta(A) = \det(A)$, $\forall A \in \mathfrak{gl}(n, \mathbb{F})$.

A set-theoretic subgroup $G \subseteq GL(n, \mathbb{F})$ is said to be a linear algebraic group if it is an algebraic subset in $\mathfrak{gl}(n, \mathbb{F})$.

Notation and elementary properties of algebraic groups have been taken from Fogarty's book [7].

The Lie algebra $\mathfrak{g}$ of a linear algebraic group G is identified with the Lie algebra of left-invariant derivations (cf. [7], 3.17); namely, $\mathfrak{g} = \mathrm{Der}_{\mathbb{F}}(\mathbb{F}[G])^G$.

If $A = (a_{ij})_{i,j=1}^n \in \mathfrak{gl}(n, \mathbb{F})$, then the corresponding invariant derivation is given by $D_A = \sum_{i,j,k=1}^n a_{ik} x_{ji} \frac{\partial}{\partial x_{jk}}$.

3. A Class of Lie Algebras

Let us consider the following definition:

Definition 1. *Let $\mathbb{F}$ be a field. We define as square-zero Lie algebra class (in short, SQZ-LA class) the class of Lie subalgebras $\mathfrak{g}$ in $\mathfrak{gl}(n, \mathbb{F})$ admitting a basis $\mathcal{B}$ (as a vector space over $\mathbb{F}$) such that the square of any matrix in $\mathcal{B}$ is zero.*

Lemma 1. *Let $G \subseteq GL(n, \mathbb{F})$ be a linear algebraic group with associated Lie algebra $\mathfrak{g}$. If U is a square-zero matrix in the Lie subalgebra $\mathfrak{g} \subset \mathfrak{gl}(n, \mathbb{F})$, then $I + tU$ belongs to G, $\forall t \in \mathbb{F}$, where $I \in GL(V)$ denotes the identity map.*

Proof. If $U \in \mathfrak{g}$ is a square-zero matrix, then $H = \{I + tU : t \in \mathbb{F}\}$ is a linear algebraic group of dimension 1 with Lie algebra $\mathfrak{h} = \{tU : t \in \mathbb{F}\}$, and by virtue of the assumption, we have $\mathfrak{g} \cap \mathfrak{h} = \mathfrak{h}$. Hence $\dim(G \cap H) = \dim H = 1$, so that $H = G \cap H$, or equivalently $H \subseteq G$. $\square$

Definition 2. *Let $G \subseteq GL(n, \mathbb{F})$ be a linear algebraic group and let $V = \mathbb{F}^n$. A function $\mathcal{I} \in \mathbb{F}[V^*] = S^\bullet(V^*)$ is said to be G-invariant if $\mathcal{I}(g \cdot v) = \mathcal{I}(v)$ for all $g \in G$ and all $v \in V$.*

The importance of the SQZ-LA class lies in the following result:

Theorem 1. *Let G be a linear algebraic group, let $\rho \colon G \to GL(n, \mathbb{F})$ be a linear representation of G, and let $\rho_* \colon \mathfrak{g} \to \mathfrak{gl}(n, \mathbb{F})$ be the homomorphism of Lie algebras induced by ρ. If $V = \mathbb{F}^n$ and $\mathfrak{g}$ is in the SQZ-LA class, then every G-invariant function $\mathcal{I} \in \mathbb{F}[V^*]$ is a common first-integral of the system of derivations $\rho_*(X)$, $\forall X \in \mathfrak{g}$. Hence, the number of algebraically-independent, G-invariant functions in $\mathbb{F}[V^*]$ is upper-bounded by the difference $n^2 - r$, where r is the generic rank of the $\mathbb{F}[V^*]$-module $\mathcal{M}$ spanned by all the derivations $\rho_*(X)$, $\forall X \in \mathfrak{g}$; i.e., r is the dimension of the $\mathbb{F}(V^*)$-vector space $\mathbb{F}(V^*) \otimes_{\mathbb{F}[V^*]} \mathcal{M}$.*

Proof. Let $\mathcal{B}$ be a basis for a $\mathfrak{g}$ in the SQZ-LA class. By virtue of Lemma 1, the matrix $I + tB$ belongs to G and we have $\mathcal{I}((I + tB) \cdot v) = \mathcal{I}(v)$, for all $t \in \mathbb{F}$ and $B \in \mathcal{B}$, and by taking derivatives at $t = 0$, we deduce that $\rho_*(X)(\mathcal{I}) = 0$, $\forall X \in \mathfrak{g}$, because the map $\mathfrak{g} \ni X \mapsto \rho_*(X) \in \mathrm{Der}\,\mathbb{F}[V^*]$ is $\mathbb{F}$-linear. Consequently, if $\mathcal{B} = \{B_1, \ldots, B_m\}$, then the $\mathbb{F}[V^*]$-module $\mathcal{M}$ is spanned by the invariant vector fields $\rho_*(B_i)$, $1 \le i \le m$, and the differential $d\mathcal{I} \in \Omega_{\mathbb{F}}(\mathbb{F}[V^*])$ of every invariant function $\mathcal{I}$ verifies $d\mathcal{I}(X) = 0$, $\forall X \in \mathcal{M}$, thereby finishing the proof. $\square$

In classical invariant theory over complex numbers, a method for computing the maximum number of algebraically-independent invariants consists of solving the linear equations arising from the system of first integrals of vector fields $\rho_*(X)$, $X \in \mathfrak{g}$; e.g., see ([4] Theorem 4.5.2). Theorem 1 extends this procedure to a class of linear representations of positive characteristic.

It would also be interesting to adapt the algorithms given in [6] to the linear representations of a linear algebraic group whose Lie algebra is in the SQZ-LA class of positive characteristic.

Remark 1. *As $\rho_*\colon \mathfrak{g} \to \mathfrak{gl}(n,\mathbb{F})$ is a homomorphism of Lie algebras, $\mathcal{M}$ is an involutive submodule in $\operatorname{Der}\mathbb{F}[V^*]$. In the real or complex cases, Frobenius's theorem implies that the maximum number of algebraically-independent, first-integral functions of $\mathcal{M}$ is $n^2 - r$ exactly, but in general the upper bound $n^2 - r$ is not necessarily reached as several of these first-integral functions may be fractional or even transcendental functions. Nevertheless, we have*

Corollary 1. *If $\rho\colon G \to GL(n,\mathbb{F})$ is as in Theorem 1, $\mathbb{F}$ is algebraically closed of characteristic zero, and $G = SL(n,\mathbb{F})$ or $G = Sp(2n,\mathbb{F})$, then the algebra $\mathbb{F}[V^*]^G$ of G-invariant functions is an $\mathbb{F}$-algebra of polynomials in $n^2 - r$ variables.*

Proof. According to ([18] Théorème 1), in the two cases of the statement above we have $\mathbb{F}[V^*]^G = \mathbb{F}[p_1,\ldots,p_m]$, where the polynomials $p_1,\ldots,p_m$ are algebraically independent. Hence, their differentials $dp_1,\ldots,dp_m$ form a basis of the dual module to $\operatorname{Der}_{\mathbb{F}}(\mathbb{F}[V^*])^G$ by virtue of ([19] VIII. Proposition 5.5), and we thus obtain $m = n^2 - r$. □

Example 1. *Let $GL(2,\mathbb{F})$ act on $V = \mathbb{F}^2 \oplus S^2(\mathbb{F}^2)$ naturally and let (v_1, v_2) be the standard basis for V; by setting*

$$
\begin{aligned}
v &= \quad xv_1 + yv_2 \in \mathbb{F}^2, \\
s &= \quad z(v_1 \otimes v_1) + t(v_1 \otimes v_2 + v_2 \otimes v_1) + u(v_2 \otimes v_2) \in S^2(\mathbb{F}^2),
\end{aligned}
$$

we deduce that the basic invariant is the function $\mathcal{I}_1\colon O \to \mathbb{F}$ defined on the Zariski open subset O of non-degenerate metrics as follows: $\mathcal{I}_1(v,s) = s^\flat(v,v)$, where $s^\flat \in S^2(\mathbb{F}^2)^*$ is the covariant symmetric tensor induced by s, assuming s is non-singular. In coordinates, $\mathcal{I}_1(v,s) = \frac{2xyt - x^2 u - y^2 z}{t^2 - zu}$. Hence $\mathbb{F}[V^*]^{GL(2,\mathbb{F})} = \mathbb{F}$ and $\mathbb{F}(V^*)^{GL(2,\mathbb{F})} = \mathbb{F}(\mathcal{I}_1)$. Nevertheless, the result depends strongly on the linear representation being considered. For example, if we consider the natural representation of $GL(2,\mathbb{F})$ on $V = \mathbb{F}^2 \oplus S^2(\mathbb{F}^2)^*$, then the basic invariant is the function $\mathcal{I}_1'(v,s^*) = s^*(v,v)$, which is globally defined, and, in this case, we have $\mathbb{F}[V^*]^{GL(2,\mathbb{F})} = \mathbb{F}[\mathcal{I}_1']$.

Example 2. *If the natural representation of $SL(2,\mathbb{F})$ on $V = \mathbb{F}^2 \oplus S^2(\mathbb{F}^2)$ is considered, then, besides $\mathcal{I}_1$, there exists another globally defined invariant—namely, the discriminant function, i.e., $\mathcal{I}_2(v,s) = zu - t^2$. Hence, $\mathcal{I}_1\mathcal{I}_2$ is also globally defined and we have $\mathbb{F}[V^*]^{SL(2,\mathbb{F})} = \mathbb{F}[\mathcal{I}_1\mathcal{I}_2, \mathcal{I}_2]$.*

Example 3. *A more complex example is the following: If V is a six-dimensional $\mathbb{F}$-vector space and*

$$\Omega\colon V \times V \to \mathbb{F}$$

is a non-degenerate alternate bilinear form, then, as a computation shows, the generic rank of $\mathcal{M}$ for the linear representation of $Sp(\Omega)$ on $\wedge^3 V^*$ is 18; see [20] for the details. As $\dim \wedge^3 V^* = 20$, it follows that there exist two invariant functions, both of them polynomial functions.

Example 4. *Given $A \in \mathfrak{gl}(2,\mathbb{C})\backslash\{0\}$, let X be the infinitesimal generator of the one-parameter group $\exp(tA)$, $t \in \mathbb{C}$. Let α, β be the eigenvalues of A. We distinguish several cases. If $\alpha \neq \beta$, $\alpha\beta \neq 0$, then the vector field X admits a first integral in $\mathbb{C}(x,y)$ if and only if $\alpha^{-1}\beta \in \mathbb{Q}$; otherwise, every non-constant first integral of X is a transcendental function. If $\alpha\beta = 0$, then X admits a first integral in $\mathbb{C}[x,y]$. If $\alpha = \beta \neq 0$ and the annihilator polynomial of A is $(\lambda - \alpha)^2$, then $X = \alpha x \frac{\partial}{\partial x} + (1 + \alpha y)\frac{\partial}{\partial y}$ and its basic first integral is the function $\mathcal{I} = x \exp(-\alpha y / x)$. If the annihilator is $\lambda - \alpha$, then X admits a first integral in $\mathbb{C}(x,y)$. Finally, if $\alpha = \beta = 0$ then the annihilator A is λ^2 and X admits the function x as a first integral.*

4. The SQZ-LA Class Studied

Notation 1. *Let $(v_i)_{i=1}^n$ be the standard basis for $\mathbb{F}^n$ with dual basis $(v^i)_{i=1}^n$. Every matrix $A \in \mathfrak{gl}(n, \mathbb{F})$ is identified with the endomorphism on $\mathbb{F}^n$ to which such matrix corresponds in the basis $(v_1, \dots, v_n)$. If $x = x^h v_h$, then $E_{ij}(x) = x^j v_i$, or equivalently $E_{ij}(v_k) = \delta_{jk} v_i$, which means that E_{ij} is the matrix with 1 in the entry (i, j) and 0 in the rest of entries. Therefore, $(E_{hi} \circ E_{jk})(v_l) = \delta_{kl} \delta_{ij} v_h$. Hence,*

$$
\begin{aligned}
E_{hi} \circ E_{jk} &= \delta_{ij} E_{hk}, \\
(E_{hi})^2 = \delta_{hi} E_{hi} &=
\begin{cases}
0, & i \neq h \\
E_{hh}, & i = h
\end{cases}
\end{aligned}
\tag{1}
$$

The Lie algebra of $n \times n$ traceless matrices with entries in $\mathbb{F}$ is denoted by $\mathfrak{sl}(n, \mathbb{F})$. The Lie algebra of $n \times n$ skew-symmetric matrices with entries in $\mathbb{F}$ is denoted by $\mathfrak{so}(n, \mathbb{F})$. The Lie algebra of $2n \times 2n$ matrices X with entries in $\mathbb{F}$ such that $X^T J_n + J_n X = 0$, where

$$
J_n = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},
$$

and $I_n \in \mathfrak{gl}(n, \mathbb{F})$ is the identity matrix, is denoted by $\mathfrak{sp}(2n, \mathbb{F})$.

By using the formulas (1) and the standard basis for the Lie algebra $\mathfrak{sl}(n, \mathbb{F})$, i.e., the $n^2 - 1$ matrices $E_{hi}, h \neq i, h, i = 1, \dots, n$; $E_{hh} - E_{11}, 2 \leq h \leq n$, we obtain

Proposition 1. *The matrices*

$$
\begin{aligned}
E_{hi}, \quad h \neq i, \quad & h, i = 1, \dots, n, \\
E_{hh} - E_{11} - E_{1h} + E_{h1}, \quad & 2 \leq h \leq n,
\end{aligned}
$$

are a basis for $\mathfrak{sl}(n, \mathbb{F})$ fulfilling the property in Definition 1.

Proposition 2. *If the characteristic of $\mathbb{F}$ is either zero or is positive p and p does not divide n, then the identity matrix $I \in \mathfrak{gl}(n, \mathbb{F})$ cannot be written as a sum of square-zero matrices.*

Proof. If $I = N_1 + \dots + N_k$, $(N_i)^2 = 0$, $1 \leq i \leq k$, as the trace of a nilpotent matrix vanishes, then by taking traces on both sides in the previous equation, we have $n = 0$ if the characteristic of $\mathbb{F}$ is zero, and $n \equiv 0 \bmod p$ if the characteristic is p. $\square$

Corollary 2. *If the characteristic of $\mathbb{F}$ is 2, then the identity matrix $I \in \mathfrak{gl}(n, \mathbb{F})$ can be written as a sum of square-zero matrices if and only if n is even.*

Proof. If n is odd, the result follows from Proposition 2. If $n = 2m$, then let $(v_i)_{i=1}^n$ be a basis for $V = \mathbb{F}^n$ with dual basis $(v_i^*)_{i=1}^n$. The space $\mathrm{End}(V)$ is identified with $V^* \otimes V$ as usual, so that we have

$$
I = \sum_{i=1}^m \left(v_{2i-1}^* \otimes v_{2i-1} + v_{2i}^* \otimes v_{2i} \right).
$$

Thus

$$
\sum_{i=1}^m \left(v_{2i-1}^* + v_{2i}^* \right) \otimes \left(v_{2i-1} + v_{2i} \right) = \quad I + \sum_{i=1}^m \left(v_{2i-1}^* \otimes v_{2i} + v_{2i}^* \otimes v_{2i-1} \right),
$$

$A_i = \left(v_{2i-1}^* + v_{2i}^*\right) \otimes (v_{2i-1} + v_{2i})$, $v_{2i-1}^* \otimes v_{2i}$, and $v_{2i}^* \otimes v_{2i-1}$, $1 \le i \le m$, are square-zero matrices, and for every $1 \le h \le n$, we have

$$
\begin{aligned}
A_i(v_h) &= (\delta_{h,2i-1} + \delta_{h,2i})(v_{2i-1} + v_{2i}), \\
(A_i)^2(v_h) &= (\delta_{h,2i-1} + \delta_{h,2i}) A_i (v_{2i-1} + v_{2i}) \\
&= 2(\delta_{h,2i-1} + \delta_{h,2i})(v_{2i-1} + v_{2i}) \\
&= 0 \bmod 2, \\
\left(v_{2i-1}^* \otimes v_{2i}\right)^2 v_h &= \delta_{h,2i-1}\left(v_{2i-1}^* \otimes v_{2i}\right)(v_{2i}) \\
&= 0, \\
\left(v_{2i}^* \otimes v_{2i-1}\right)^2 v_h &= \delta_{h,2i}\left(v_{2i}^* \otimes v_{2i-1}\right)(v_{2i-1}), \\
&= 0.
\end{aligned}
$$

□

Similarly, by starting with the standard basis for the symplectic Lie algebra $\mathfrak{sp}(2n, \mathbb{F})$, i.e.,

$$
\begin{array}{llll}
E_{i,n+i}, & E_{n+i,i}, & E_{ii} - E_{n+i,n+i}, & 1 \le i \le n, \\
E_{ij} - E_{n+i,n+j}, & E_{ji} - E_{n+j,n+i}, & E_{i,n+j} - E_{j,n+i}, & 1 \le i < j \le n, \\
& & E_{n+i,j} - E_{j+n,i}, & 1 \le i < j \le n,
\end{array}
$$

we obtain

Proposition 3. *The matrices*

$$
\begin{array}{llll}
E_{i,n+i}, E_{n+i,i}, & & 1 \le i \le n, \\
E_{ii} - E_{n+i,n+i} + E_{i,n+i} - E_{n+i,i}, & & 1 \le i \le n, \\
E_{ij} - E_{n+i,n+j}, & & E_{ji} - E_{n+j,n+i}, & 1 \le i < j \le n, \\
E_{i,n+j} - E_{j,n+i}, & & E_{n+i,j} - E_{j+n,i}, & 1 \le i < j \le n,
\end{array}
$$

are a basis for $\mathfrak{sp}(2n, \mathbb{F})$, fulfilling the property in Definition 1.

Similarly, we have

Proposition 4. *The standard basis E_{hi}, $1 \le h < i \le n$, of the Lie subalgebra of strictly upper triangular matrices in $\mathfrak{gl}(n, \mathbb{F})$ satisfies the property in Definition 1.*

As for the Lie algebra $\mathfrak{so}(n, \mathbb{F})$, with basis $E_{hi} - E_{ih}$, $1 \le h < i \le n$, we have

Proposition 5. *Let $x_1, \ldots, x_n$ be the column vectors of a matrix $X \in \mathfrak{so}(n, \mathbb{F})$ of rank r, and let $x_{i_1}, \ldots, x_{i_r}$, $1 \le i_1 < \ldots < i_r \le n$, be r linearly independent column vectors of X. The necessary and sufficient condition for the square of X to be zero is that the subspace $\langle x_{i_1}, \ldots, x_{i_r} \rangle$ is totally isotropic with respect to the scalar product $\langle \cdot, \cdot \rangle$ given by $\langle v_i, v_j \rangle = \delta_{ij}$, $i, j = 1, \ldots, n$.*

Proof. As X is skew-symmetric, for all $i, j = 1, \ldots, n$, we have

$$
\left(X^2\right)_{ij} = \sum_{h=1}^{n} x_{ih} x_{hj} = -\sum_{h=1}^{n} x_{hi} x_{hj} = -\langle x_i, x_j \rangle.
$$

Hence, $X^2 = 0$ if and only if $\langle x_i, x_j \rangle = 0$ for $1 \le i \le j \le n$.

Further, if $k, l \notin \{i_1, \ldots, i_r\}$, then $x_k = \sum_{a=1}^{r} \lambda_{ka} x_{i_a}$, $x_l = \sum_{b=1}^{r} \lambda_{lb} x_{i_b}$; consequently, $\langle x_k, x_l \rangle = \sum_{a=1}^{r} \sum_{b=1}^{r} \lambda_{ka} \lambda_{lb} \langle x_{i_a}, x_{i_b} \rangle$. It follows that $X^2 = 0$ if and only if $\langle x_{i_a}, x_{i_b} \rangle = 0$ for $1 \le a \le b \le r$. □

Corollary 3. *If the ground field $\mathbb{F}$ is formally real, then the only matrix X in $\mathfrak{so}(n, \mathbb{F})$ with $X^2 = 0$ is the zero matrix.*

Proof. In fact, if $x = \sum_{i=1}^{n} x^i v_i$, then: $\langle x, x \rangle = \sum_{i=1}^{n} (x^i)^2$, and by virtue of the hypothesis, it follows that the only totally isotropic subspace for $\langle \cdot, \cdot \rangle$ is $\{0\}$. □

Remark 2. *If the characteristic of $\mathbb{F}$ is $\neq 2$, then the only matrix X in $\mathfrak{so}(2, \mathbb{F})$ such that $X^2 = 0$ is the zero matrix, as $[\alpha(E_{12} - E_{21})]^2 = -\alpha^2 I$. The same holds for $\mathfrak{so}(3, \mathbb{F})$. In fact, if*

$$X = a(E_{12} - E_{21}) + b(E_{13} - E_{31}) + c(E_{23} - E_{32}),$$

then, as the matrix X^2 is symmetric, the condition $X^2 = 0$ leads one to the following system of six equations: $a^2 + b^2 = 0$, $ab = 0$; $a^2 + c^2 = 0$, $ac = 0$; $b^2 + c^2 = 0$, $bc = 0$. Hence $a + b = 0$, $a + c = 0$, $b + c = 0$, and consequently, $a = b = c = 0$.

Remark 3. *If an m-dimensional subalgebra $\mathfrak{g} \subseteq \mathfrak{gl}(n, \mathbb{F})$ belongs to the SQZ-LA class, then for every basis $A_1, \ldots, A_m$ of $\mathfrak{g}$, symmetric $m \times m$ matrices S_h, $1 \leq h \leq m$, must exist such that $\mathrm{trace}(S_h C^k) = 0$, for every $h, k = 1, \ldots, m$, where C^k is the $m \times m$ matrix defined by $[A_i, A_j] = C_{ij}^k A_k$. In fact, if $B_h = \lambda_h^i A_i$ is a square-zero basis for $\mathfrak{g}$, then $s_h^{ij} A_i A_j = 0$, for every $i, j = 1, \ldots, m$, where $s_h^{ij} = \lambda_h^i \lambda_h^j$. Hence, $s_h^{ij} c_{ij}^k A_k = 0$, thereby proving the remark. Therefore, it can be known whether a matrix algebra does not belong to the SQZ-LA class in polynomial time by simply solving a system of linear equations.*

Next, following the notation and results of [21], we study whether certain Lie algebras in characteristic 2 are in the SQZ-LA class. Assume the characteristic of $\mathbb{F}$ is 2, let $f \colon V \times V \to \mathbb{F}$ be a bilinear form, and let $L(f) \subseteq \mathfrak{gl}(V)$ be its associated Lie subalgebra; i.e.,

$$L(f) = \{X \in \mathfrak{gl}(V) : f(X(u), v) = f(u, X(v)), \forall u, v \in V\}.$$

(Recall that we are in characteristic 2.) If, in addition, $\mathbb{F}$ is algebraically closed, then according to ([21] Theorem 1.1) the Lie algebra $L(f)$ is reductive if and only if either (i) $f = 0$ and $n \neq 2$, in which case $L(f) = \mathfrak{gl}(V)$, (ii) or $n = 2m + 1$ and f admits a Gram matrix J_{2m+1}, in which case $L(f)$ is Abelian of dimension $m + 1$, (iii) or else f admits as Gram matrix a direct sum of matrices of the types indicated below, in which case $L(f)$ is isomorphic to the direct sum of the Lie algebras associated to these matrix summands:

TYPE 0:
$A = \begin{pmatrix} 0 & J_m \\ I_m & 0 \end{pmatrix}$, $L(A)$ Abelian of dimension m;

$B = \begin{pmatrix} 0 & 0 \\ I_m & 0 \end{pmatrix}$, $L(B) \cong \mathfrak{gl}(m)$, $m > 2$.

TYPE λ, $\lambda \in \mathbb{F}$, $\lambda \neq 1$:
$A = \begin{pmatrix} 0 & J_m(\lambda) \\ I_m & 0 \end{pmatrix}$, $L(A)$ Abelian of dimension m;

$B = \begin{pmatrix} 0 & \lambda I_m \\ I_m & 0 \end{pmatrix}$, $L(B) \cong \mathfrak{gl}(m)$, $m > 2$.

TYPE 1:
$A = \Gamma_m$, m odd, $L(A)$ Abelian of dimension $\frac{1}{2}(m + 1)$;

$B = \begin{pmatrix} 0 & J_2(1) \\ I_2 & 0 \end{pmatrix}$, $L(B)$ Abelian of dimension 4;

$C = I_m$, $m > 2$, $L(C) \cong \mathfrak{so}(m)$;

$$D = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}, m > 2, L(D) \cong \mathfrak{sp}(2m).$$

In the case (i) the condition in Definition 1 does not hold for $L(f)$ as this condition never holds for $\mathfrak{gl}(m, \mathbb{F})$. In the case (ii) the condition in Definition 1 does not hold for $L(f)$ whatever the odd integer $n > 1$. Finally, in the case of the matrix A in Type 0, $L(A)$ is the Abelian Lie algebra generated by the powers

$$\begin{pmatrix} (J_m)^T & 0 \\ 0 & J_m \end{pmatrix}^i, \quad 0 \le i \le m - 1.$$

From Proposition 4 it follows that the algebra $L(A)$ is in the SQZ-LA class, whereas $L(B)$ in Type 0 is not. The Lie algebras $L(A)$ and $L(B)$ in Type 1 are not in the SQZ-LA class either. As for $L(C) \cong \mathfrak{so}(m)$ in Type 1, they do or do not belong to the SQZ-LA class depending on the nature of the ground field, as we have seen above. Finally, the Lie algebra $L(D)$ is not in the SQZ-LA class, as follows directly from Proposition 3.

5. Conclusions

In this work, we have focused our attention on the class of Lie algebras of matrices, with coefficients in a field $\mathbb{F}$ of arbitrary characteristic, admitting a basis, as vector space on $\mathbb{F}$, of square-zero matrices. We termed such a class of Lie algebras as the SQZ-LA class.

This article has evidenced the interest of the SQZ-LA class in computing the number of invariants of a linear representation of its associated affine group.

In view of this interest, a study has also been carried out of such Lie algebras and examples and other applications thereof have been shown.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SQZ-LA   Square-zero Lie algebra

References

1. Weyl, H. *The Classical Groups, Their Invariants and Representations*; Princeton University Press: Princeton, NJ, USA, 1946.
2. Goodman, R.; Wallach, N.R. *Representations and Invariants of the Classical Groups*; Cambridge University Press: Cambridge, UK, 1998.
3. Procesi, C. *Lie Groups, An Approach through Invariants and Representations*; Springer Science+Business Media, LLC: Berlin/Heidelberg, Germany, 2007.
4. Sturmfels, B. Algorithms in Invariant Theory. In *Texts and Monographs in Symbolic Computation*; Springer: Vienna, Austria, 1993.

5. Michler, G.O. Some problems in computational representation theory. *J. Symb. Comput.* **1990**, *9*, 571–582. [CrossRef]

6. Derksen, H.; Kemper, G. Computational Invariant Theory. In *Invariant Theory and Algebraic Transformation Groups*; With Two Appendices by Vladimir L. Popov, and an Addendum by Norbert A'Campo and Popov; Springer: Heidelberg, Germany, 2015; Volume III.

7. Fogarty, J. *Invariant Theory*; W. A. Benjamin, Inc.: New York, NY, USA; Amsterdam, The Netherlands, 1969.

8. Botha, J.D. Sums of two square-zero matrices over an arbitrary field. *Linear Algebra Appl.* **2012**, *436*, 516–524. [CrossRef]

9. Botha, J.D. Square-zero factorization of matrices. *Linear Algebra Appl.* **2016**, *488*, 71–85. [CrossRef]

10. Botha, J.D. Products of idempotent and square-zero matrices. *Linear Algebra Appl.* **2016**, *497*, 116–133. [CrossRef]

11. Karagueuzian, D.; Oliver, B.; Ventura, J. The components of a variety of matrices with square zero and submaximal rank. In *Commutative Algebra*; Lecture Notes in Pure and Applied Mathematics; Chapman & Hall/CRC: Boca Raton, FL, USA, 2006; Volume 244, pp. 151–164.

12. Mohammadian, A. Sums and products of square-zero matrices. *Comm. Algebra* **2012**, *40*, 4568–4574. [CrossRef]

13. Takahashi, K. On sums of three square-zero matrices. *Linear Algebra Appl.* **2000**, *306*, 45–57. [CrossRef]

14. Mackey, D.S.; Mackey, N.; Mehl, C.; Mehrmann, V. Skew-symmetric matrix polynomials and their Smith forms. *Linear Algebra Appl.* **2013**, *438*, 4625–4653. [CrossRef]

15. Mehrmann, V.; Watkins, D. Structure-Preserving Methods for Computing Eigenpairs of Large Sparse Skew-Hamiltonian/Hamiltonian Pencils. *SIAM J. Sci. Comput.* **2000**, *22*, 1905–1925. [CrossRef]

16. Duan, G.R. *Analysis and Design of Descriptor Linear Systems*, 1st ed.; Advances in Mechanics and Mathematics; Springer: New York, NY, USA, 2010; Volume 23. [CrossRef]

17. Abhyankar, S.S. Algebraic Geometry for Scientists and Engineers. In *Mathematical Surveys and Monographs*; American Mathematical Society: Providence, RI, USA, 1990; Volume 35.

18. Kac, V.G.; Popov, V.L.; Vinberg, E.B. Sur les groupes linéaires algébriques dont l'algèbre des invariants est libre. *C. R. Acad. Sci. Paris* **1976**, *283*, A875–A878.

19. Lang, S. *Algebra*; Addison-Wesley Publishing Company, Inc.: Reading, MA, USA, 1993.

20. Muñoz Masqué, J.; Pozo Coronado, L.M. A new look at the classification of the tri-covectors of a 6-dimensional symplectic space. *Linear Multilinear Algebra* **2019**, *67*, 939–952. [CrossRef]

21. Ruhallah Ahmadi, S.; Izadi, M.A.; Szechtman, F. Lie algebras and bilinear forms in characteristic 2. *Linear Algebra Appl.* **2014**, *448*, 299–314. [CrossRef]