Journal of Symbolic Computation 125 (2024) 102312

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

A computational approach to almost-inner derivations ☆

Heiko Dietrich [a], Willem A. de Graaf [b]

[a] School of Mathematics, Monash University, Clayton VIC 3800, Australia
[b] Department of Mathematics, University of Trento, Povo (Trento), Italy

ARTICLE INFO

Article history:
Received 22 November 2023
Accepted 27 February 2024
Available online 4 March 2024

Keywords:
Lie algebras
Almost-inner derivations
Tate-Shafarevich algebra

ABSTRACT

We present a computational approach to determine the space of almost-inner derivations of a finite dimensional Lie algebra given by a structure constant table. We also present an example of a Lie algebra for which the quotient algebra of the almost-inner derivations modulo the inner derivations is non-abelian. This answers a question of Kunyavskii and Ostapenko.

1. Introduction

Let $\mathfrak{g}$ be a finite dimensional Lie algebra over a field F. A linear map $\delta\colon \mathfrak{g} \to \mathfrak{g}$ is a derivation if for all $a, b \in \mathfrak{g}$ it satisfies

$$\delta([a,b]) = [\delta(a), b] + [a, \delta(b)].$$

The set of all derivations of $\mathfrak{g}$ forms an F-vector space, denoted $\mathrm{Der}(\mathfrak{g})$, and a short calculation shows that $\mathrm{Der}(\mathfrak{g})$ is a Lie-subalgebra of $\mathfrak{gl}(\mathfrak{g})$. For every $a \in \mathfrak{g}$ the adjoint homomorphism $\mathrm{ad}(a)\colon \mathfrak{g} \to \mathfrak{g}$, $b \mapsto [a, b]$, is a derivation; these are the inner derivations of $\mathfrak{g}$ and they form a subalgebra $\mathrm{Inn}(\mathfrak{g})$ of $\mathrm{Der}(\mathfrak{g})$; note that $[\mathrm{ad}(a), \mathrm{ad}(b)](x) = \mathrm{ad}([a,b])(x)$. In particular, the map $\mathrm{ad}\colon \mathfrak{g} \to \mathrm{Inn}(\mathfrak{g})$ is a surjective homomorphism whose kernel is the centre $\mathfrak{z}(\mathfrak{g})$ of $\mathfrak{g}$, and $\mathrm{Inn}(\mathfrak{g})$ is spanned by $\mathrm{ad}(b)$ where b runs over an F-basis of $\mathfrak{g}$. If δ is a derivation of $\mathfrak{g}$, then $[\delta, \mathrm{ad}(a)] = \mathrm{ad}(\delta(a))$ for all $a \in \mathfrak{g}$, which shows that

☆ The authors thank Boris Kunyavskii for proposing this question to us (at the Monash Prato Workshop 'Lie Theory: frontiers, algorithms, and applications'), and suggesting to look at the example of Sah (1968).

E-mail addresses: heiko.dietrich@monash.edu (H. Dietrich), willem.degraaf@unitn.it (W.A. de Graaf).

https://doi.org/10.1016/j.jsc.2024.102312

$\mathrm{Inn}(\mathfrak{g})$ is an ideal of $\mathrm{Der}(\mathfrak{g})$. A derivation δ of $\mathfrak{g}$ is almost-inner if there exists a map $A_\delta\colon \mathfrak{g}\to\mathfrak{g}$ such that for every $a\in\mathfrak{g}$ it satisfies

$$\delta(a)=[A_\delta(a),a],$$

that is, $\delta(a)\in[\mathfrak{g},a]$ for all $a\in\mathfrak{g}$. The map A_δ is neither unique nor linear in general; for example, one can modify each image of A_δ by adding a different central element of $\mathfrak{g}$. The F-space of all almost-inner derivations on $\mathfrak{g}$ is denoted $\mathrm{AID}(\mathfrak{g})$. An almost-inner derivation δ is central almost-inner if there is some $a\in\mathfrak{g}$ such that $\delta-\mathrm{ad}(a)$ maps $\mathfrak{g}$ into the centre of $\mathfrak{g}$. We follow the convention in Burde et al. (2018) and denote the space of central almost inner derivation of $\mathfrak{g}$ by $\mathrm{CAID}(\mathfrak{g})$. Since $\mathrm{ad}(a)(b)=[a,b]$ for every $a,b\in\mathfrak{g}$, the inner derivation $\mathrm{ad}(a)$ is an almost-inner derivation with constant map $A_{\mathrm{ad}(a)}=a$. More generally, in (Burde et al., 2018, Proposition 2.3) the following inclusion of Lie subalgebras of $\mathrm{Der}(\mathfrak{g})$ is shown

$$\mathrm{Inn}(\mathfrak{g})\leqslant\mathrm{CAID}(\mathfrak{g})\leqslant\mathrm{AID}(\mathfrak{g})\leqslant\mathrm{Der}(\mathfrak{g}).$$

Recall that $\mathrm{Inn}(\mathfrak{g})=\mathrm{Der}(\mathfrak{g})$ for every semisimple Lie algebra over a field of characteristic 0, see for example (Humphreys, 1978, Theorem 5.3).

Clearly, $\mathrm{Inn}(\mathfrak{g})$ is an ideal in each of these subalgebras. It is shown in (Burde et al., 2018, Proposition 2.4) that $\mathrm{CAID}(\mathfrak{g})$ is an ideal in $\mathrm{AID}(\mathfrak{g})$, but it remains open whether or not $\mathrm{AID}(\mathfrak{g})$ is an ideal in $\mathrm{Der}(\mathfrak{g})$: this is conjectured to be true in (Burde et al., 2018, Remark 2.5). For more details on known results, we refer to Burde et al. (2018, 2021); for example, it is known that $\mathrm{AID}(\mathfrak{g})=\mathrm{CAID}(\mathfrak{g})=\mathrm{Inn}(\mathfrak{g})$ for every complex Lie algebra $\mathfrak{g}$ of dimension at most 4, see (Burde et al., 2018, Proposition 2.8).

Almost-inner derivations have first been considered by Gordon and Wilson Gordon and Wilson (1984) in a differential-geometric context. They have recently been studied by Saeedi and collaborators (see, e.g. Amiri and Saeedi (2018); Sheikh-Mohseni et al. (2015)) and Burde, Dekimpe, and Verbeke (see, e.g. Burde et al. (2018, 2021); Verbeke (2020)). Most recently, Kunyavskii and Ostapenko Kunyavskii and Ostapenko (2023) used $\mathrm{AID}(\mathfrak{g})$ to define an algebra-theoretic analog of the Tate-Shafarevich group, the Tate-Shafarevich algebra of a Lie algebra $\mathfrak{g}$,

$$Ш(\mathfrak{g})=\mathrm{AID}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g}),$$

see (Kunyavskii and Ostapenko, 2023, Section 2). They point out that algebras with nonzero $Ш(\mathfrak{g})$ reveal important geometric phenomena. One of their main results is the proof that $\mathrm{AID}(\mathfrak{g})$ is an ideal of $\mathrm{Der}(\mathfrak{g})$ for nilpotent $\mathfrak{g}$, partially answering the aforementioned conjecture affirmatively. This also implies that $Ш(\mathfrak{g})$ is an ideal of $\mathrm{Out}(\mathfrak{g})=\mathrm{Der}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$ for nilpotent $\mathfrak{g}$, see (Kunyavskii and Ostapenko, 2023, Theorem 2.5).

The first author of Kunyavskii and Ostapenko (2023) asked us for computational methods to determine the subalgebra $\mathrm{AID}(\mathfrak{g})$, and whether there is a Lie algebra $\mathfrak{g}$ for which $\mathrm{AID}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$ is non-abelian, see (Kunyavskii and Ostapenko, 2023, Question 4.1(i)). We develop such an approach in Section 2, and then discuss some computational examples (including an affirmative answer to the question) in Sections 3 and 4.

2. Computational approach

Let $\mathfrak{g}$ be a Lie algebra over a field F, with basis $\mathcal{B}=\{b_1,\dots,b_n\}$ and corresponding structure constants $\sigma_{i,j}^k$, that is, for each $i,j\in\{1,\dots,n\}$ we have $[b_i,b_j]=\sum_{k=1}^n\sigma_{i,j}^k b_k$. Let δ be an endomorphism of $\mathfrak{g}$, represented by an $n\times n$ matrix with entries $d_{j,k}$, such that $\delta(b_j)=\sum_{k=1}^n d_{j,k}b_k$ for each i. Since δ is a derivation if and only if $\delta([b_i,b_j])=[\delta(b_i),b_j]+[b_i,\delta(b_j)]$ for all i,j, this translates to the following equations for each $i,j,\ell\in\{1,\dots,n\}$:

$$\sum\nolimits_{k=1}^n(\sigma_{i,j}^k d_{k,\ell}-\sigma_{k,j}^\ell d_{i,k}-\sigma_{i,k}^\ell d_{j,k})=0.$$

Since $[b_i,b_j]=-[b_j,b_i]$, it suffices to consider $i>j$. This shows that a basis for the derivation algebra $\mathrm{Der}(\mathfrak{g})$ can be computed by solving a system of $n^2(n+1)/2$ linear equations with n^2 unknowns, see also (de Graaf, 2000, Section 1.9). A basis of $\mathrm{Inn}(\mathfrak{g})$ as a subalgebra can readily be computed by determining the matrices (with respect to $\mathcal{B}$) of the adjoints $\mathrm{ad}(b_i)$ for every $i \in \{1, \ldots, n\}$.

In conclusion, linear algebra methods can be used to compute $\mathrm{Der}(\mathfrak{g})$ and $\mathrm{Inn}(\mathfrak{g})$, and therefore also a complement subspace $U \leqslant \mathrm{Der}(\mathfrak{g})$ such that

$$\mathrm{Der}(\mathfrak{g}) = \mathrm{Inn}(\mathfrak{g}) \oplus U.$$

In the sequel we fix one such space U. Since $\mathrm{Inn}(\mathfrak{g}) \leqslant \mathrm{AID}(\mathfrak{g})$, to determine $\mathrm{AID}(\mathfrak{g})$, it suffices to compute the space $U \cap \mathrm{AID}(\mathfrak{g})$.

Definition 2.1. For $z_0 \in \mathfrak{g}$ let D_{z_0} be the subspace of U that consists of all derivations δ that act as an inner derivation on the 1-dimensional subspace spanned by z_0; note that δ is not inner since $U \cap \mathrm{Inn}(\mathfrak{g}) = \{0\}$. In other words, $\delta \in D_{z_0}$ if and only if $\delta \in U$ and $\delta(z_0) = [z_0, x]$ for some $x \in \mathfrak{g}$.

If $z_0 \in \mathfrak{g}$ and ψ_{z_0} denotes the linear map

$$\psi_{z_0} \colon U \oplus \mathfrak{g} \to \mathfrak{g}, \quad (\delta, x) \mapsto \delta(z_0) - [z_0, x],$$

then D_{z_0} is the image of the kernel $\ker \psi_{z_0}$ under the projection $U \oplus \mathfrak{g} \to U$. This shows that we can compute D_{z_0} by solving a linear equation system. In particular,

$$U \cap \mathrm{AID}(\mathfrak{g}) = \bigcap\nolimits_{z_0 \in \mathfrak{g}} D_{z_0}.$$

Clearly, a finite intersection suffices to construct $U \cap \mathrm{AID}(\mathfrak{g})$ in this way. However, it is not clear how to chose suitable elements z_0, and how to establish that the intersection is as small as possible.

We fix the previous notation and, throughout, let V be a subspace of U, for example, the intersection of multiple spaces D_{z_0} for arbitrarily chosen elements $z_0 \in \mathfrak{g}$, so that

$$\mathrm{AID}(\mathfrak{g}) \leqslant \mathrm{Inn}(\mathfrak{g}) \oplus V.$$

Let $\{\delta_1, \ldots, \delta_s\}$ be a basis of V. How to decide whether $\delta = \sum_{i=1}^{s} d_i \delta_i \in V$ lies in $\mathrm{AID}(\mathfrak{g})$? The following proposition provides an answer, but we need some notation before we can state it.

For a vector $z = (z_1, \ldots, z_n) \in F^n$ define the $n \times n$ matrix $M(z)$ as

$$M(z) = (m_{k,j}(z))_{k,j} \quad \text{where each} \quad m_{k,j}(z) = \sum\nolimits_{i=1}^{n} z_i \sigma_{i,j}^{k};$$

recall that the $\sigma_{i,j}^{k}$ are the structure constants with respect to the basis $\{b_1, \ldots, b_n\}$ of $\mathfrak{g}$. Also define $b_z \in \mathfrak{g}$ by

$$b_z = z_1 b_1 + \cdots + z_n b_n.$$

For $\delta \in V$ write $\delta(b_z) = c_1(z) b_1 + \cdots + c_n(z) b_n$ with each $c_i(z) \in F$, and define the column vector $v_\delta(z)$ as

$$v_\delta(z) = (c_1(z), \ldots, c_n(z))^{\mathsf{T}}.$$

Lastly, denote by

$$M_\delta(z) = [M(z) | v_\delta(z)]$$

the augmented matrix $M(z)$ with additional column $v_\delta(z)$.

Proposition 2.2. *The derivation $\delta \in V$ lies in $\mathrm{AID}(\mathfrak{g})$ if and only if for all $z \in F^n$*

$$\mathrm{rank}(M(z)) = \mathrm{rank}(M_\delta(z)).$$

Proof. The derivation δ is almost-inner if and only if for every $z \in F^n$ there exists some $x \in \mathfrak{g}$ such that $\delta(b_z) = [b_z, x]$. Writing $x = x_1 b_1 + \ldots + x_n b_n$ we have

$$[b_z, x] = \sum_{i,j=1}^{n} z_i x_j [b_i, b_j] = \sum_{k=1}^{n} (\sum_{i,j=1}^{n} z_i x_j \sigma_{i,j}^k) b_k.$$

Using the definition of $v_\delta(z)$ and its components $c_k(z)$, the derivation δ lies in $\mathrm{AID}(\mathfrak{g})$ if and only if for all $z_1, \ldots, z_n \in F$, there exist $x_1, \ldots, x_n \in F$ such that for each $k \in \{1, \ldots, n\}$

$$c_k(z) = (\sum_{i,j=1}^{n} z_i x_j \sigma_{i,j}^k) = \sum_{j=1}^{n} (\sum_{i=1}^{n} z_i \sigma_{i,j}^k) x_j.$$

The latter holds if and only if

$$M(z) \cdot (x_1, \ldots, x_n)^\intercal = v_\delta(z) \tag{2.1}$$

where $M(z)$ and $v_\delta(z)$ are as defined prior to the proposition. We have that (2.1) has a solution if and only if $v_\delta(z)$ lies in the column space of $M(z)$. The claim follows. □

Note that $m_{k,j}(z)$ and $c_i(z)$ are (linear) polynomials in $z_1, \ldots, z_n$. Now let $z = (z_1, \ldots, z_n)$ be the vector of indeterminates of $F[z_1, \ldots, z_n]$ and consider the corresponding matrices $M(z)$ and $M_\delta(z)$. The rank of a matrix can be defined as the largest integer r such that there exists a nonzero $r \times r$ minor, that is, a nonzero determinant of an $r \times r$ submatrix. For a fixed r, denote by $K_r(z)$ and $K_{\delta,r}(z)$ the set of all $r \times r$ minors of $M(z)$ and of $M_\delta(z)$, respectively; so the elements in $K_r(z)$ and $K_{\delta,r}(z)$ are polynomials in $F[z_1, \ldots, z_n]$. Let $\mathcal{I}_r(z)$ and $\mathcal{I}_{\delta,r}(z)$ be the ideals generated by $K_r(z)$ and $K_{\delta,r}(z)$, respectively. Recall that the radical of an ideal I in a ring R is the ideal $\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$.

Proposition 2.3. *Let $\delta \in V$ be a derivation. If δ is not an almost-inner derivation, then there exists some r and $w \in \mathcal{I}_{\delta,r}(z)$ with $w \notin \sqrt{\mathcal{I}_r(z)}$. Conversely, if the field is algebraically closed and there exist some r and $w \in \mathcal{I}_{\delta,r}(z)$ such that $w \notin \sqrt{\mathcal{I}_r(z)}$, then δ is not an almost-inner derivation.*

Proof. If δ is not an almost-inner derivation, then there exists $\tilde{z} \in F^n$ such that $r = \mathrm{rank}(M_\delta(\tilde{z}))$ is larger than $\mathrm{rank}(M(\tilde{z}))$, that is, there is some $r \times r$ minor $w(\tilde{z})$ of $M_\delta(\tilde{z})$ that does not vanish, but all $r \times r$ minors of $M(\tilde{z})$ are 0. Thus, $\tilde{z}$ is a common root of all elements in $\mathcal{I}_r(z)$, but not of all elements in $\mathcal{I}_{\delta,r}(z)$. In particular, $w(z)$ lies in $\mathcal{I}_{\delta,r}(z)$, but not in $\sqrt{\mathcal{I}_r(z)}$.

Conversely, suppose that there exists some r and $w \in \mathcal{I}_{\delta,r}(z)$ such that $w \notin \sqrt{\mathcal{I}_r(z)}$. Over an algebraically closed field, Hilbert's Nullstellensatz (Cox et al., 2015, Theorem 4.1.2) says that $\sqrt{\mathcal{I}_r(z)}$ is exactly the set of all polynomials that vanish on all the common roots of the elements in $\mathcal{I}_r(z)$. This means that there is a common root $\tilde{z}$ for all the elements in $\mathcal{I}_r(z)$, but $\tilde{z}$ is not a root of $w(z)$. This implies that $\mathrm{rank}(M_{\delta,r}(\tilde{z}))$ is greater than $\mathrm{rank}(M_r(\tilde{z}))$, and therefore δ is not an almost-inner derivation by Proposition 2.2. □

We note that deciding membership in the radical can be achieved without computing the radical, see (Cox et al., 2015, Proposition 4.2.8).

Corollary 2.4. *Let $\delta \in V$ be a derivation.*

a) *Over an algebraically closed field, $\delta \in \mathrm{AID}(\mathfrak{g})$ if and only if $\mathcal{I}_{\delta,r}(z) \subseteq \sqrt{\mathcal{I}_r(z)}$ for every $r > 1$.*
b) *If $\mathcal{I}_{\delta,r}(z) \subseteq \sqrt{\mathcal{I}_r(z)}$ for each $r > 1$, then $\delta \in \mathrm{AID}(\mathfrak{g})$ (even for non-algebraically closed fields).*

Remark 2.5. If the latter condition in part a) of the corollary does not hold, then there exists some $r \times r$ minor $w(z) \in \mathcal{I}_{\delta,r}(z)$ that does not lie in $\sqrt{\mathcal{I}_r(z)}$; in particular, there exists a point $\tilde{z}$ such that $w(\tilde{z})$ is not zero, but $\tilde{z}$ is a common root of all the elements in $\mathcal{I}_r(z)$. One can attempt to find $\tilde{z}$ by working in the polynomial ring $F[z_1, \ldots, z_n, y]$ and finding a common zero of the polynomials in the ideal generated by $K_r(z)$ and $w(z)y - 1$: such a common zero annihilates every generator in $K_r(z)$, but due to $w(\tilde{z})y = 1$, it cannot be a zero of $w(z)$. Once such an element $\tilde{z} \in F^n$ is found, one can reduce V to $V \cap D_{b_{\tilde{z}}}$. Note that the latter intersection is smaller than V since $\delta \in V$, but $\delta \notin D_{b_{\tilde{z}}}$. Eventually, one can iterate this method to reduce V to a smaller subspace such that one can verify that each generator is an almost-inner derivation. However, it is still a computational challenge to find these suitable points $\tilde{z}$. In particular, for fields that are not algebraically closed, it is not even known whether the problem of finding such points is decidable, cf. Hilbert's 10th Problem over $\mathbb{Q}$, see (Poonen, 2017, Section 2.6.4).

3. Computational examples

Our methods can quickly deal with small-dimensional Lie algebras. For example, we went through the classification of 8-dimensional filiform Lie algebras given in Ancochéa-Bermúdez and Goze (1988). For the cases where the Lie algebra depends on a parameter we set it equal to 1. Our methods readily compute the quotient $\mathrm{AID}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$, and it has dimension 0, 1, or 2 in all cases. When the dimension of the Lie algebra increases we can still quickly get a good idea of $\mathrm{AID}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$ by computing the intersection of many spaces D_{z_0} for arbitrarily chosen z_0. However, proving that a given derivation is almost-inner by the minors-method described above quickly becomes cumbersome due to the large number of minors that has to be considered.

We now illustrate our method with some computations in the algebra system Magma Bosma et al. (1997).

Example 3.1. We consider the complex Lie algebra $\mathfrak{g} = \mathfrak{g}_{6,23}$ of (Verbeke, 2020, p. 112). It is a 6-dimensional Lie algebra with basis $\{b_1, \dots, b_6\}$ whose non-zero commutators are $[b_1, b_2] = b_3$, $[b_1, b_3] = b_5$, $[b_1, b_4] = b_6$, and $[b_2, b_4] = b_5$. The complement space to $\mathrm{Inn}(\mathfrak{g})$ in $\mathrm{Der}(\mathfrak{g})$ has dimension 10, and the intersection of a few spaces D_z quickly finds a 2-dimensional subspace $U \leqslant \mathrm{Der}(\mathfrak{g})$ such that $\mathrm{AID}(\mathfrak{g}) \leqslant \mathrm{Inn}(\mathfrak{g}) \oplus U$. We choose a basis $\{\delta_1, \delta_2\}$ of U and let $\delta = d_1\delta_1 + d_2\delta_2$, such that Equation (2.1) reads

$$\begin{pmatrix} -z_2 & z_1 & 0 & 0 \\ -z_3 & -z_4 & z_1 & z_2 \\ -z_4 & 0 & 0 & z_1 \end{pmatrix} \cdot (x_1, x_2, x_3, x_4)^\intercal = (-d_1 z_1, -d_2 z_2, 0)^\intercal.$$

To show that $\delta_1 \in \mathrm{AID}(\mathfrak{g})$, we consider $d_1 = 1$ and $d_2 = 0$, and the matrices

$$M(z) = \begin{pmatrix} -z_2 & z_1 & 0 & 0 \\ -z_3 & -z_4 & z_1 & z_2 \\ -z_4 & 0 & 0 & z_1 \end{pmatrix} \quad \text{and} \quad M_\delta(z) \begin{pmatrix} -z_2 & z_1 & 0 & 0 & -z_1 \\ -z_3 & -z_4 & z_1 & z_2 & 0 \\ -z_4 & 0 & 0 & z_1 & 0 \end{pmatrix}.$$

The following Magma code establishes that $\mathcal{I}_{\delta,3}(z) \subseteq \sqrt{\mathcal{I}_3(z)}$ and $\mathcal{I}_{\delta,2}(z) \subseteq \sqrt{\mathcal{I}_2(z)}$, and now Corollary 2.4 proves that δ_1 is in $\mathrm{AID}(\mathfrak{g})$. The same computation with $M_\delta(z)$ adjusted to $\delta = \delta_2$ proves that $\delta_2 \in \mathrm{AID}(\mathfrak{g})$. Thus, in this case, $\mathrm{AID}(\mathfrak{g}) = \mathrm{Inn}(\mathfrak{g}) \oplus U$ for some 2-dimensional U.

```
Mv  := Matrix([[-z2,z1,0,0,0],[-z3,-z4,z1,z2,-z2],[-z4,0,0,z1,0]]);
M   := Matrix([[-z2,z1,0,0],[-z3,-z4,z1,z2],[-z4,0,0,z1]]);
I3  := Radical(ideal<P|Minors(M,3)>);
I3v := ideal<P|Minors(Mv,3)>;
I2  := Radical(ideal<P|Minors(M,2)>);
I2v := ideal<P|Minors(Mv,2)>;
forall(i){ i : i in GroebnerBasis(I2v) | i in I2};
//true
forall(i){ i : i in GroebnerBasis(I3v) | i in I3};
//true
```

Example 3.2. Now let $\mathfrak{g}$ be the complex 5-dimensional Lie algebra of (Verbeke, 2020, Lemma 8.2.11), whose non-vanishing brackets are $[b_1, b_4] = b_1$, $[b_1, b_5] = -b_2$, $[b_2, b_4] = b_2$, $[b_2, b_5] = b_1$, $[b_4, b_5] =$

b_3. A complement U to $\mathrm{Inn}(\mathfrak{g})$ in $\mathrm{Der}(\mathfrak{g})$ has dimension 2, and we choose a basis $\{\delta_1, \delta_2\}$. For $\delta = \delta_1$, we obtain the following calculations:

```
C<i> := CyclotomicField(4);
P<z1,z2,z3,z4,z5,x1,x2,x3,x4,x5,y,d1,d2>:= PolynomialRing(C,13);
m   := Matrix([[-z4,-z5,0,z1,z2],[z5,-z4,0,z2,-z1],[0,0,0,-z5,z4]]);
mv  := Matrix([[-z4,-z5,0,z1,z2,-z1],[z5,-z4,0,z2,-z1,-z2],
               [0,0,0,-z5,z4,0]]);
I3  := Radical(ideal<P|Minors(m,3)>);
I3v := ideal<P|Minors(mv,3)>;
forall(i){ i : i in GroebnerBasis(I3v) | i in I3};
//false; next, we try to find a suitable \tilde z
gb  := GroebnerBasis(I3);
exists(min){min : min in Minors(mv,3) | not min in I3};
// true
Append(~gb, min*y - 1);
gb  := GroebnerBasis(tmp);
// [ z1^2*z5*y + z2^2*z5*y - 1,   z4^2 + z5^2 ]
> [Evaluate(f,[1,1,0,-i,1,0,0,0,0,0,1/2,0,0]) : f in gb];
// [ 0, 0 ]
```

At the end of this computation we have found $\tilde{z} = (1, 1, 0, -i, 1)$ and $y = 1/2$, where $i = \imath$ is a primitive 4-th root of unity, such that D_z with $z = b_1 + b_2 - \imath b_4 + b_5$ satisfies $\dim(U \cap D_z) = 1$. One can now iterate this process and eventually establish that $\mathrm{AID}(\mathfrak{g}) = \mathrm{Inn}(\mathfrak{g})$. The quoted code also shows that over the subfield $\mathbb{R}$ it is not possible to find such an element $\tilde{z}$: the equation $z_4^2 + z_5^2 = 0$ forces $z_4 = z_5 = 0$, but then $z_1^2 z_5 y + z_2^2 z_5 y - 1 = -1$ is never 0.

Example 3.3. In (Burde and Moens, 2020, Propositions 3.5 and 3.8) two examples of Lie algebras $\mathfrak{g}$ over fields of positive characteristic were given such that the quotient $\mathrm{Der}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$ is simple and non-solvable. The first example is $\mathfrak{psl}(3, F)$, where F is a field of characteristic 3. The second example is the ideal J generated by the short root vectors of the simple Lie algebra of type F_4 over a field of characteristic 2. In both cases, by computing the intersection of a small number of spaces D_{z_0}, our methods quickly show that $\mathrm{AID}(\mathfrak{g}) = \mathrm{Inn}(\mathfrak{g})$.

4. A non-abelian $Ш(\mathfrak{g})$

We now provide an affirmative answer to (Kunyavskii and Ostapenko, 2023, Question 4.1(i)) in the positive characteristic case (Kunyavskii and Ostapenko, 2023, Section 4.1.2), namely, we construct a Lie algebra $\mathfrak{g}$ such that $Ш(\mathfrak{g}) = \mathrm{AID}(\mathfrak{g})/\mathrm{Inn}(\mathfrak{g})$ is non-abelian. The Lie algebra $\mathfrak{g}$ is defined by a finite p-group constructed in (Sah, 1968, Theorem p. 67). We briefly describe the construction of that group, and then comment on the construction of $\mathfrak{g}$ and computation of $\mathrm{AID}(\mathfrak{g})$.

Let p be a prime, let $F = \mathbb{F}_q$ be the field with $q = p^3$ elements, and let $R = F^3$ be the 3-dimensional F-vector space. Denote by $\{1, \pi, \pi^2\}$ an F-basis of R and define a left multiplication on R by $\pi f = f^q \pi$ for $f \in F$, and $\pi^i \pi^j = \pi^{i+j}$ if $i + j \leqslant 2$ and $\pi^i \pi^j = 0$ otherwise. The multiplicative group $U_1(R) = 1 + R\pi$ acts via left multiplication on the additive group R, giving rise to the split extension

$$G_p = (R, +) \rtimes U_1(R).$$

If $\{1, \alpha, \alpha^2\}$ is a $\mathbb{Z}_p$-basis of F, then $U_1(R)$ is generated by $\{1 + \alpha^i \pi^j \mid i = 0, 1, 2;\ j = 1, 2\}$, the centre Z of $U_1(R)$ is generated by $\{1 + \alpha^i \pi^2 \mid i = 0, 1, 2\}$, and $Z \cong U_1(R)/Z \cong (\mathbb{Z}/p\mathbb{Z})^3$. Thus, G_p can be described as an extension $C_p^9 \rtimes (C_p^3.C_p^3)$ of order p^{15}; here C_n denotes a cyclic group of order n.

For $p = 2, 3$ we have constructed G_p in GAP GAP Group as a group given by a polycyclic presentation. For $p = 2$, the group $U_1(R)$ can be reconstructed in GAP as SmallGroup(64,82); the group G_2 has order $2^{15} = 32768$ and can be reconstructed in GAP as PcGroupCode(c,32768), where

$$\begin{aligned} c = &\,7967110418574553081670398114259915186817035422811746306474238743720883\\ &1725611328458148063967477625450818367910830831150163051940361653140207\\ &3356972696434071737990061156240486161235975. \end{aligned}$$

For $p = 3$, the groups $U_1(R)$ and G_3 are isomorphic to the groups constructed in GAP asSmall-Group(729, 122) and PcGroupCode(c,14348907), where

$$\begin{aligned} c = &\,2394257517593284993878744790303485055907699526905097239261910228496569\\ &7037971664120902046779276348374342035162654519026274575815342804754951\\ &7041150514460591292399372711230903481919137251508110943248577780211134\\ &77919143155502672960892416353913323520. \end{aligned}$$

There are several standard ways to attach a Lie algebra to a finite p-group. Here we use the p-central series $G_p = G_p^1 \geqslant G_p^2 \geqslant G_p^3 \geqslant G_p^4 = 1$. The quotients G_i/G_{i+1} are elementary abelian p-groups, and hence can be viewed as vector spaces over the field $\mathbb{F}_p$ with p elements. The Lie algebra $\mathfrak{g}_p$ is the direct sum of these spaces and the Lie bracket on $\mathfrak{g}_p$ is induced by the commutator in G_p. We refer to (de Graaf, 2000, §1.4) for a precise account (in this reference the Jennings series is used, but for the p-central series it works in the same way).

For $\mathfrak{g}_2$ and $\mathfrak{g}_3$ we computed the intersection of a large number of spaces D_{z_0} for arbitrarily chosen $z_0 \in \mathfrak{g}_p$. In both cases, this quickly yields a space of dimension 21 of possible almost-inner derivations that are not inner. By running over *all* elements $z_0 \in \mathfrak{g}_p$, we then proved that this space indeed consists of almost-inner derivations. We note that when extending the field and considering the Lie algebras $\mathbb{F}_8 \otimes_{\mathbb{F}_2} \mathfrak{g}_2$ and $\mathbb{F}_{27} \otimes_{\mathbb{F}_3} \mathfrak{g}_3$, it is quickly shown by computing the intersection of a number of spaces D_{z_0} that the algebra of almost-inner derivations is equal to the algebra of inner derivations. This is reflected by the fact that for the ideals generated by minors we have many k such that $\mathcal{I}_{\delta,k}(z)$ is not contained in $\sqrt{\mathcal{I}_k(z)}$. However, these ideals turn out to be too complicated to be analysed further in detail.

We provide some more details for $\mathfrak{g}_3$: this algebra has basis $\{v_1, \ldots, v_{15}\}$ with multiplication table given in Fig. 1. The algebra of derivations of $\mathfrak{g}_3$ has dimension 45, and the ideal of inner derivations $\mathrm{Inn}(\mathfrak{g}_3)$ has dimension 12. In the subalgebra $\mathrm{AID}(\mathfrak{g}_3)$ of almost-inner derivations satisfies $\mathrm{AID}(\mathfrak{g}_3) = \mathrm{Inn}(\mathfrak{g}_3) \oplus U$ where U is a subalgebra of dimension 21. In Fig. 2 we explicitly define two non-commuting elements d_1 and d_2 of U.

CRediT authorship contribution statement

Heiko Dietrich: Investigation, Methodology, Writing – original draft, Writing – review & editing. **Willem A. de Graaf:** Investigation, Methodology, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

$$
\begin{aligned}
&[v_1, v_2] = 2v_7, && [v_3, v_4] = 2v_{11},\\
&[v_1, v_3] = v_7 + 2v_8, && [v_3, v_5] = v_{11} + 2v_{12},\\
&[v_1, v_4] = 2v_{10}, && [v_3, v_6] = 2v_{10} + v_{12},\\
&[v_1, v_5] = v_{11}, && [v_3, v_{10}] = 2v_{13} + v_{14},\\
&[v_1, v_6] = v_{12}, && [v_3, v_{11}] = v_{13} + 2v_{14} + 2v_{15},\\
&[v_1, v_{10}] = 2v_{13}, && [v_3, v_{12}] = v_{13} + v_{14} + 2v_{15},\\
&[v_1, v_{11}] = v_{14} + v_{15}, && [v_4, v_7] = v_{13},\\
&[v_1, v_{12}] = 2v_{15}, && [v_4, v_8] = 2v_{15},\\
&[v_2, v_3] = 2v_8 + v_9, && [v_4, v_9] = v_{14} + v_{15},\\
&[v_2, v_4] = 2v_{12}, && [v_5, v_7] = v_{14} + v_{15},\\
&[v_2, v_5] = 2v_{10} + v_{12}, && [v_5, v_8] = 2v_{13} + v_{15},\\
&[v_2, v_6] = v_{11}, && [v_5, v_9] = 2v_{14} + v_{15},\\
&[v_2, v_{10}] = v_{13} + 2v_{15}, && [v_6, v_7] = 2v_{15},\\
&[v_2, v_{11}] = v_{13} + 2v_{14} + v_{15}, && [v_6, v_8] = 2v_{14} + 2v_{15},\\
&[v_2, v_{12}] = v_{14} + 2v_{15}, && [v_6, v_9] = 2v_{13} + v_{15}.
\end{aligned}
$$

Fig. 1. Structure constants for $\mathfrak{g}_3$; if $[v_i, v_j]$ is not listed, then $[v_i, v_j] = 0$.

$$
\begin{aligned}
&d_1(v_2) = v_7, && d_2(v_2) = v_{10},\\
&d_1(v_3) = 2v_7 + v_8, && d_2(v_7) = v_{13},\\
&d_1(v_4) = 2v_{11} + 2v_{12}, && d_2(v_8) = v_{13},\\
&d_1(v_5) = 2v_{10}, && d_2(v_9) = 2v_{13} + 2v_{14},\\
&d_1(v_6) = v_{10}, && \\
&d_1(v_{10}) = v_{14}, && \\
&d_1(v_{11}) = v_{13}, && \\
&d_1(v_{12}) = 2v_{13}. &&
\end{aligned}
$$

Fig. 2. Definitions of two non-commuting elements of U; if $d_i(v_k)$ is not listed, then $d_i(v_k) = 0$.

References

Amiri, A., Saeedi, F., 2018. On pointwise inner derivations of Lie algebras. Asian-Eur. J. Math. 11 (5), 1850070.

Ancochéa-Bermúdez, J.M., Goze, M., 1988. Classification des algèbres de Lie filiformes de dimension 8. Arch. Math. (Basel) 50 (6), 511–525.

Bosma, W., Cannon, J., Playoust, C., 1997. The magma algebra system I: the user language. J. Symb. Comput. 24, 235–265.

Burde, D., Dekimpe, K., Verbeke, B., 2018. Almost inner derivations of Lie algebras. J. Algebra Appl. 17 (11), 1850214.

Burde, D., Dekimpe, K., Verbeke, B., 2021. Almost inner derivations of Lie algebras II. J. Algebra Comput. 31, 341–364.

Burde, D., Moens, W.A., 2020. A Zassenhaus conjecture and CPA-structures on simple modular Lie algebras. J. Algebra 559 (529–546).

Cox, D.A., Little, J., O'Shea, D., 2015. Ideals, Varieties, and Algorithms. Undergrad. Texts Math. Springer, Cham.

Gordon, C.S., Wilson, E.N., 1984. Isospectral deformations of compact solvmanifolds. J. Differ. Geom. 19, 241–256.

de Graaf, W.A., 2000. Lie Algebras: Theory and Algorithms. North-Holland Mathematical Library.

GAP Group. GAP – groups, algorithms and programming. https://gap-system.org.

Humphreys, J.E., 1978. Introduction to Lie Algebras and Representation Theory. Grad. Texts Math., vol. 9. Springer.
Kunyavskii, B., Ostapenko, V.Z., 2023. Tate-Shafarevich groups and algebras. Int. J. Algebra Comput. 33 (4), 819–836.
Poonen, B., 2017. Rational Points on Varieties. Grad. Stud. Math., vol. 186. Americ. Math. Soc., Providence, RI.
Sah, C.-H., 1968. Automorphisms of finite groups. J. Algebra 10 (47–68).
Sheikh-Mohseni, S., Saeedi, F., Badrkhani Asl, M., 2015. On special subalgebras of derivations of Lie algebras. Asian-Eur. J. Math. 8 (2), 1550032.
Verbeke, B., 2020. Almost inner derivations of Lie algebras. PhD thesis. Arenberg Doctoral School, KU Leuven. https://lirias.kuleuven.be/retrieve/587183.