# On derivations of subalgebras of real semisimple Lie algebras 

Paolo Ciatti ${ }^{1}$ • Michael G. Cowling ${ }^{2}$

Received: 24 August 2016 / Accepted: 21 June 2017 / Published online: 28 June 2017
© Fondazione Annali di Matematica Pura ed Applicata and Springer-Verlag GmbH Germany 2017


#### Abstract

Let $\mathfrak{g}$ be a real semisimple Lie algebra with Iwasawa decomposition $\mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$. We show that, except for some explicit exceptional cases, every derivation of the nilpotent subalgebra $\mathfrak{n}$ that preserves its restricted root space decomposition is of the form $\operatorname{ad}(W)$, where $W \in \mathfrak{m} \oplus \mathfrak{a}$.


Keywords Lie theory • Semisimple Lie algebras and their representations • Nilpotent Lie algebras

Mathematics Subject Classification 17B40 • 22E60 • 30L10

## 1 Introduction

Let $\mathfrak{g}$ be a semisimple Lie algebra, with Iwasawa decomposition $g=\mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$, where $\mathfrak{k}$ is compact, $\mathfrak{a}$ is abelian, and $\mathfrak{n}$ is nilpotent, and let $\mathfrak{m}$ be the centraliser of $\mathfrak{a}$ in $\mathfrak{k}$. Then $\mathfrak{n}=\sum_{\gamma \in \Sigma^{+}} \mathfrak{g}_{\gamma}$, where $\Sigma^{+}$is the set of positive restricted roots and $\mathfrak{g}_{\gamma}$ is the restricted root space corresponding to the restricted root $\gamma$.

[^0]We study the derivations of $\mathfrak{n}$ which preserve its root space decomposition, that is, the derivations $D$ such that $D\left(\mathfrak{g}_{\gamma}\right) \subseteq \mathfrak{g}_{\gamma}$ for each positive restricted root $\gamma$. By definition and the Jacobi identity, if $W \in \mathfrak{m} \oplus \mathfrak{a}$, then $[H, W]=0$ for all $H \in \mathfrak{a}$, and so $[H,[W, X]]=[W,[H, X]]=\gamma(H)[W, X]$ for all $X \in \mathfrak{g}_{\gamma}$; thus ad $(W)$ preserves the root space decomposition. The main point of this paper is that, unless $\mathfrak{g}$ contains a simple summand of the form $\mathfrak{s o}(n, 1)$ or $\mathfrak{s u}(n, 1)$, every root-space-preserving derivation $D$ of $\mathfrak{n}$ is of the form $\operatorname{ad}(W)$, where $W \in \mathfrak{m} \oplus \mathfrak{a}$, and more precisely the symmetric part of $D$ is in $\operatorname{ad}(\mathfrak{a})$ while the skew-symmetric part of $D$ is in $\operatorname{ad}(\mathfrak{m})$.

The root-space-preserving derivations are known for real rank-one simple Lie algebras. Indeed, Korányi [16] showed that in the rank-one case, $\mathfrak{n}$ is an $H$-type Lie algebra, and the Lie algebra of derivations and the automorphism group of an $H$-type algebra were found by Riehm [20] and Saal [21]. Our work may be viewed as a development of the ideas of these authors.

Here is our strategy. First, the algebra $\mathfrak{g}$ splits into a sum of simple ideals, and we show that it suffices to consider the case where $\mathfrak{g}$ is simple. As noted, the real rank-one case is understood; we treat the algebras of real rank two by considering the possible restricted root systems separately, and using a detailed analysis of several $H$-type algebras contained in $\mathfrak{n}$ in each case. A key argument at this stage is showing that each derivation is the sum of a symmetric and an antisymmetric derivation. To treat the general case, we again show that it suffices to treat symmetric and an antisymmetric derivations separately. The symmetric derivations act by scalars on each restricted root space, and belong to ad $(\mathfrak{a})$, but the skew-symmetric derivations are trickier. We handle these by introducing identities ( $D_{\gamma, \delta}$ ) and ( $E_{\gamma, \delta}$ ), where $\gamma, \delta \in \Sigma^{+}$, which involve the interplay of a derivation with the Cartan involution $\theta$, and show that these identities characterise derivations in $\operatorname{ad}(\mathfrak{m})$ in simple Lie algebras of arbitrary real rank. We prove these identities for the simple algebras of higher rank by reducing to subalgebras of real rank one and two, and then using our analysis of these algebras.

This paper is a step towards the classification of the derivations and automorphisms of $\mathfrak{n}$, which is interesting for a variety of reasons. One reason is to find the derivations of (minimal) parabolic subalgebras of semisimple Lie algebras, which has been a lively field in recent years; see, for example, Chen [2] and Wang and Yu [22]. Every derivation of a parabolic subalgebra induces a derivation of its nilradical; if we can show that these are Lie multiplication by elements of the subalgebra, then we are well on the way to finding the derivations of the whole subalgebra. Another reason is the question of classification of nilpotent Lie algebras: In general, this is an impossibly tedious matter, but one might hope to do better with algebras with lots of symmetry; to see whether this is viable, we need to understand some examples.

Next, to carry out harmonic analysis on the simply connected nilpotent Lie group associated with $\mathfrak{n}$, which has applications in diverse areas including theoretical physics and linear partial differential equations, it is important to understand its symmetries; see, for example, the study of Folland [12].

A fourth reason for studying the automorphisms of $\mathfrak{n}$ is the theory of quasiconformal mappings of "Carnot groups". Indeed, as defined by Pansu [19], the derivative of a quasiconformal mapping of an Iwasawa $N$ group is an automorphism, and restrictions on the automorphisms give rise to restrictions on the quasiconformal mappings. Further, it was shown by Yamaguchi [24], using the theory of Tanaka prolungations and the Borel-Bott-Weil theorem, and Cowling et al. [8], using more elementary arguments, that the space of "multicontact mappings", that is, mappings whose differentials preserve the simple root spaces, is finite-dimensional when all the derivations that preserve the root spaces are of the form $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$. The result presented here leads to the same conclusion in an even simpler way. Indeed, unless $\mathfrak{n}$ has
dimension 1 or 2, the Tanaka prolongation of $\mathfrak{n}$ through $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$ is finite-dimensional; see Ottazzi and Warhurst [18], and this implies that multicontact mappings form a finitedimensional Lie group. While a more abstract approach, for instance via cohomology, might well also establish our main result for Iwasawa algebras, our more concrete analysis also provides tools that should apply to more general algebras that do not arise as subalgebras of semisimple algebras.

It is also of interest to consider derivations that preserve the grading of $\mathfrak{n}$, that is, the subspaces $\sum_{\alpha} \mathfrak{g}_{\alpha}$ where we sum over all $\alpha$ of the same height, and to consider derivations of nilradicals of more general parabolic algebras; we will return to these questions in future work.

This paper is organised as follows. In Sect. 2 we analyse the derivations of an $H$-type algebra. We start by showing that every derivation is the sum of a symmetric derivation and a skew-symmetric derivation; we then describe symmetric and skew-symmetric derivations separately.

In Sect. 3, we consider real semisimple Lie algebras. First, we reduce matters to the case of simple Lie algebras, and then we show that these contain various $H$-type algebras. We also see how the geometry of root systems is reflected in the structure of various subalgebras of $\mathfrak{g}$. Most of the ideas behind this section may be found in Ciatti [3-7].

In Sect. 4, we consider the grading of a semisimple Lie algebra associated with a choice of positive roots, and grading-preserving derivations of $\mathfrak{g}$, of $\mathfrak{m} \oplus \mathfrak{a} \oplus \mathfrak{n}$ and of $\mathfrak{n}$. We find a simple Lie algebraic criterion for a skew-symmetric grading-preserving derivation of $\mathfrak{n}$ to extend to a derivation of $\mathfrak{g}$; this extended derivation is not only grading preserving but also root space preserving.

Finally, in Sect. 5 we apply the results of Sects. 2 and 3 to the study of the derivations of $\mathfrak{n}$ that preserve the root space decomposition. These are sums of symmetric derivations and skew-symmetric derivations. The main idea is to show that our assertion is true when the real rank of $\mathfrak{g}$ is 1 or 2 , and then apply this result to the rank-two subalgebras of a general simple Lie algebra, deducing from these the full result.

Main Theorem If no simple summand of $\mathfrak{g}$ is isomorphic to $\mathfrak{s o}(n, 1)$ or $\mathfrak{s u}(n, 1)$ for any $n$, then all the derivations of $\mathfrak{n}$ that preserve the root spaces are of the form $\operatorname{ad}(W)$, where $W \in \mathfrak{m} \oplus \mathfrak{a}$. Otherwise, there are derivations of $\mathfrak{n}$ that preserve the root spaces that do not arise in this way.

## 2 Derivations of an $\boldsymbol{H}$-type Lie algebra

In this section, we first define $H$-type Lie algebras, which arose in the work of Kaplan [14], and then describe their derivations. These are always the sum of a symmetric derivation and a skew-symmetric derivation. In Corollary 2.6, skew-symmetric derivations are decomposed as the sum of two components, one of which is trivial on the centre. The symmetric derivations are classified in Corollary 2.8 by a diagonalisation process.

Let $\mathfrak{h}$ be a two-step nilpotent Lie algebra, endowed with an inner product $\langle\cdot, \cdot\rangle$. We denote by $\mathfrak{z}$ the centre of $\mathfrak{h}$ and by $\mathfrak{v}$ the orthogonal complement of $\mathfrak{z}$; given a subspace $\mathfrak{s}$ of $\mathfrak{h}$, we write $I_{\mathfrak{s}}$ for the identity map on $\mathfrak{s}$. Then

$$
\mathfrak{g}=\mathfrak{v} \oplus \mathfrak{z}
$$

(throughout this paper, $\oplus$ denotes a vector space direct sum; in general, the summands need not be Lie algebras). For each $Z$ in $\mathfrak{z}$, we define $J_{Z}$ in $\operatorname{End}(\mathfrak{v})$ by

$$
\begin{equation*}
\left\langle J_{Z} X, Y\right\rangle=\langle Z,[X, Y]\rangle \quad \forall X, Y \in \mathfrak{v} . \tag{2.1}
\end{equation*}
$$

Then $J_{Z}$ is trivially skew-symmetric, that is, $J_{Z}^{\top}=-J_{Z}$, where ${ }^{\top}$ denotes the transpose relative to the inner product. We say that $\mathfrak{h}$ is of Heisenberg type, or just $H$-type, when

$$
\begin{equation*}
J_{Z}^{2}=-\|Z\|^{2} I_{\mathfrak{v}} \tag{2.2}
\end{equation*}
$$

for all $Z \in \mathfrak{z}$. Equivalently, for each $X \in \mathfrak{v}$ of length 1 , the map $\operatorname{ad}(X)$ is an isometry from $\operatorname{ker}(\operatorname{ad}(X))^{\perp}$ onto $\mathfrak{z}$. For the rest of this section, we assume that $\mathfrak{h}$ is an $H$-type algebra.

By polarisation, (2.2) implies that

$$
\begin{equation*}
J_{Z} J_{Z^{\prime}}+J_{Z^{\prime}} J_{Z}=-2\left\langle Z, Z^{\prime}\right\rangle I_{\mathfrak{v}} \quad \forall Z, Z^{\prime} \in \mathfrak{z} \tag{2.3}
\end{equation*}
$$

Thus the $J_{Z}$ generate a Clifford algebra.
Recall that a derivation of a Lie algebra $\mathfrak{h}$ is a linear endomorphism $D: \mathfrak{h} \rightarrow \mathfrak{h}$ such that

$$
D([X, Y])=[D X, Y]+[X, D Y] \quad \forall X, Y \in \mathfrak{h} ;
$$

every derivation of a Lie algebra automatically preserves the centre. We say that a linear endomorphism $D$ of $\mathfrak{h}$ preserves the grading if $D(\mathfrak{v}) \subseteq \mathfrak{v}$ and $D(\mathfrak{z}) \subseteq \mathfrak{z}$, and write $\mathcal{D}(\mathfrak{h})$ for the Lie algebra of all grading-preserving derivations of $\mathfrak{h}$. We denote by $\mathcal{D}^{\text {sym }}(\mathfrak{h})$ the subspace of $\mathcal{D}(\mathfrak{h})$ of all symmetric derivations and by $\mathcal{D}^{\text {skew }}(\mathfrak{h})$ the Lie subalgebra of all skew-symmetric derivations. We also write $\mathcal{D}_{0}^{\text {sym }}(\mathfrak{h})$ and $\mathcal{D}_{0}^{\text {skew }}(\mathfrak{h})$ for the subspaces of these spaces of derivations that vanish on $\mathfrak{z}$.

Proposition 2.1 Let $D$ be a grading-preserving linear endomorphism of $\mathfrak{h}$. Then $D$ is a derivation if and only if

$$
\begin{equation*}
J_{D^{\top} Z}=D^{\top} J_{Z}+J_{Z} D \quad \forall Z \in \mathfrak{z} . \tag{2.4}
\end{equation*}
$$

Suppose moreover that $\left.D\right|_{\mathfrak{z}}=0$. If $D$ is skew-symmetric, then $D$ is a derivation if and only if $D$ commutes with all the $J_{Z}$ and if $D$ is symmetric, then $D$ is a derivation if and only if $D$ anticommutes with all the $J_{Z}$.

Proof From (2.1), it follows that $D$ is a derivation if and only if, for all $Z$ in $\mathfrak{z}$ and $X, Y$ in $\mathfrak{v , ~}$

$$
\begin{aligned}
\left\langle J_{D^{\top} Z} X, Y\right\rangle & =\left\langle D^{\top} Z,[X, Y]\right\rangle=\langle Z, D[X, Y]\rangle \\
& =\langle Z,[D X, Y]\rangle+\langle Z,[X, D Y]\rangle \\
& =\left\langle J_{Z} D X, Y\right\rangle+\left\langle D^{\top} J_{Z} X, Y\right\rangle,
\end{aligned}
$$

proving the result.
The next result is known, but we give a proof for completeness.
Lemma 2.2 (Riehm [20]) For every pair of orthogonal vectors $Z^{\prime}$ and $Z^{\prime \prime}$ in $\mathfrak{z}$, the gradingpreserving linear map $\Phi_{Z^{\prime} Z^{\prime \prime}}$, defined by

$$
\Phi_{Z^{\prime} Z^{\prime \prime}}(X+Z)=J_{Z^{\prime}} J_{Z^{\prime \prime}} X+2\left\langle Z^{\prime}, Z\right\rangle Z^{\prime \prime}-2\left\langle Z^{\prime \prime}, Z\right\rangle Z^{\prime}
$$

for all $Z \in \mathfrak{z}$ and all $X \in \mathfrak{v}$, is a skew-symmetric derivation of $\mathfrak{h}$.

Proof It is evident that $\Phi_{Z^{\prime} Z^{\prime \prime}}$ is skew-symmetric. By Proposition 2.1, it suffices to show that

$$
J_{\Phi_{Z^{\prime} Z^{\prime \prime}}(Z)} X=\Phi_{Z^{\prime} Z^{\prime \prime}} J_{Z} X-J_{Z} \Phi_{Z^{\prime} Z^{\prime \prime}} X \quad \forall X \in \mathfrak{v} .
$$

We consider the right-hand side of the equation, and use (2.3):

$$
\begin{aligned}
J_{Z^{\prime}} J_{Z^{\prime \prime}} J_{Z} X-J_{Z} J_{Z^{\prime}} J_{Z^{\prime \prime}} X= & -2\left\langle Z, Z^{\prime \prime}\right\rangle J_{Z^{\prime}} X-J_{Z^{\prime}} J_{Z} J_{Z^{\prime \prime}} X \\
& +2\left\langle Z, Z^{\prime}\right\rangle J_{Z^{\prime \prime}} X+J_{Z^{\prime}} J_{Z} J_{Z^{\prime \prime}} X \\
= & 2\left\langle Z^{\prime}, Z\right\rangle J_{Z^{\prime \prime}} X-2\left\langle Z^{\prime \prime}, Z\right\rangle J_{Z^{\prime}} X \\
= & J_{2\left\langle Z^{\prime}, Z\right\rangle Z^{\prime \prime}-2\left\langle Z^{\prime \prime}, Z\right\rangle Z^{\prime} X}= \\
= & J_{\Phi_{Z^{\prime} Z^{\prime \prime}}(Z)} X,
\end{aligned}
$$

as required.
We define $\mathcal{R}(\mathfrak{h})$ to be the vector subspace of $\mathcal{D}(\mathfrak{h})$ of all grading-preserving derivations of $\mathfrak{h}$ spanned by the $\Phi_{Z^{\prime} Z^{\prime \prime}}$. As observed by Riehm [20], the subspace $\mathcal{R}(\mathfrak{h})$ is a subalgebra of $\mathcal{D}(\mathfrak{h})$. To see this, we take an orthonormal basis $\left\{Z_{1}, \ldots, Z_{m}\right\}$ for $\mathfrak{z}$, and write $\Phi_{i j}$ in place of $\Phi_{Z_{i} Z_{j}}$. Since $\Phi_{Z^{\prime} Z^{\prime \prime}}$ depends linearly on $Z^{\prime}$ and on $Z^{\prime \prime}$, every element of $\mathcal{R}(\mathfrak{h})$ is a linear combination of the $\Phi_{i j}$. Moreover,

$$
\Phi_{i j} \Phi_{k l}-\Phi_{k l} \Phi_{i j}= \begin{cases}0 & \text { if }\{i, j\} \cap\{k, l\}=\varnothing \\ 2 \Phi_{j l} & \text { if } i=k\end{cases}
$$

which shows that $\mathcal{R}(\mathfrak{h})$ is closed under taking commutators. We omit the proof of these commutation relations, as we do not need this result.

Corollary 2.3 Suppose that $D$ is a grading-preserving derivation of $\mathfrak{h}$. Then we may write $D$ as $D_{0}+D_{1}$, where $D_{0} \in \mathcal{D}(\mathfrak{h})$ and $\left.D_{0}\right|_{\mathfrak{z}}$ is symmetric, and $D_{1} \in \mathcal{R}(\mathfrak{h})$.

Proof The skew-symmetric part of the restriction $\left.D\right|_{\mathfrak{z}}$ of $D$ to $\mathfrak{z}$ decomposes as a linear combination of the $\left.\Phi_{i j}\right|_{\mathfrak{z}}$ defined above; we take $D_{1}$ to be the same linear combination of the $\Phi_{i j}$, and $D_{0}$ to be $D-D_{1}$. The result follows immediately.

Corollary 2.4 Suppose that $D \in \mathcal{D}(\mathfrak{h})$ and $\left.D\right|_{\mathfrak{z}}$ is symmetric. Then $D^{\top} \in \mathcal{D}(\mathfrak{h})$.
Proof Since $\left.D\right|_{\mathfrak{z}}$ is symmetric, it is diagonalisable. Take an eigenvector $Z$ in $\mathfrak{z}$ with eigenvalue $2 \mu$. By Proposition 2.1,

$$
2 \mu J_{Z}=J_{D Z}=J_{D^{\top} Z}=D^{\top} J_{Z}+J_{Z} D
$$

whence multiplication on both sides by $J_{Z}$ gives

$$
-2 \mu|Z|^{2} J_{Z}=-|Z|^{2} J_{Z} D^{\top}-|Z|^{2} D J_{Z},
$$

and

$$
J_{D Z}=D J_{Z}+J_{Z} D^{\top}
$$

This holds for all eigenvectors $Z$ of $D$, and so for all $Z \in \mathfrak{z}$ by linearity, so $D^{\top}$ is a derivation, again by Proposition 2.1.

Corollary 2.5 Suppose that $D$ is a grading-preserving endomorphism of $\mathfrak{h}$. Then $D \in \mathcal{D}(\mathfrak{h})$ if and only if $D^{\top} \in \mathcal{D}(\mathfrak{h})$. Hence if $D \in \mathcal{D}(\mathfrak{h})$, then we may write $D$ as $D^{a}+D^{s}$, where $D^{s} \in \mathcal{D}^{\text {sym }}(\mathfrak{h})$ and $D^{a} \in \mathcal{D}^{\text {skew }}(\mathfrak{h})$.

Proof For the first part, it suffices to suppose that $D \in \mathcal{D}(\mathfrak{h})$ and show that $D^{\top} \in \mathcal{D}(\mathfrak{h})$. In light of Corollary 2.3, by subtracting off an element of $\mathcal{R}(\mathfrak{h})$ if necessary, we may assume that $\left.D\right|_{\mathfrak{z}}$ is symmetric. It follows that $D^{\top} \in \mathcal{D}(\mathfrak{h})$, as required.

For the second part of the corollary, take

$$
D^{s}=\frac{1}{2}\left(D+D^{\top}\right) \quad \text { and } \quad D^{a}=\frac{1}{2}\left(D-D^{\top}\right)
$$

the conclusion is obvious.
Hence, to describe the elements of $\mathcal{D}(\mathfrak{h})$, we can study symmetric and skew-symmetric derivations separately. First we consider the skew-symmetric derivations.
Corollary 2.6 Each $D$ in $\mathcal{D}^{\text {skew }}(\mathfrak{h})$ decomposes as a sum $D_{0}+R$, where $D_{0} \in \mathcal{D}_{0}^{\text {skew }}(\mathfrak{h})$ and $R \in \mathcal{R}(\mathfrak{h})$. In particular, $\left.D_{0}\right|_{\mathfrak{v}}$ commutes with all the maps $J_{Z}$.

Proof This is a consequence of Corollary 2.3 and Proposition 2.1.
Now we consider a symmetric derivation $D$, which is diagonalisable with real eigenvalues. Since $D$ preserves $\mathfrak{v}$ and $\mathfrak{z}$, these spaces decompose into eigenspaces for $D$. We take $\mathfrak{v}_{\lambda}$ to be the eigenspace of $\left.D\right|_{\mathfrak{v}}$ for the eigenvalue $\lambda$, and, given a subspace $\mathfrak{s}$ of $\mathfrak{h}$, we write $P_{\mathfrak{s}}$ for the orthogonal projection of $\mathfrak{h}$ onto $\mathfrak{s}$.

Proposition 2.7 Suppose that $D \in \mathcal{D}^{\text {sym }}(\mathfrak{h})$. Then $\left.D\right|_{\mathfrak{z}}=2 \mu I_{\mathfrak{z}}$ for some $\mu$ in $\mathbb{R}$. Moreover, if $X \in \mathfrak{v}_{\lambda}$, then

$$
\begin{equation*}
D J_{Z} X=(2 \mu-\lambda) J_{Z} X \quad \text { and } \quad D J_{Z} J_{Z^{\prime}} X=\lambda J_{Z} J_{Z^{\prime}} X \tag{2.5}
\end{equation*}
$$

for all $Z$ and $Z^{\prime}$ in $\mathfrak{j}$.
Proof Fix an orthonormal basis $\left\{Z_{1}, \ldots, Z_{m}\right\}$ of $\mathfrak{z}$ such that $D Z_{i}=2 \mu_{i} Z_{i}$ when $i=$ $1, \ldots, m$, with $\mu_{i} \in \mathbb{R}$. From (2.4), it follows that

$$
D J_{Z_{i}} X=J_{D Z_{i}} X-J_{Z_{i}} D X=\left(2 \mu_{i}-\lambda\right) J_{Z_{i}} X
$$

when $i=1, \ldots, m$, and the first formula of (2.5) is established, and similarly,

$$
\begin{equation*}
D J_{Z_{i}} J_{Z_{k}} X=\left(2 \mu_{i}-2 \mu_{k}+\lambda\right) J_{Z_{i}} J_{Z_{k}} X \tag{2.6}
\end{equation*}
$$

when $i, k=1, \ldots, m$.
If $\operatorname{dim}(\mathfrak{z})=1$, then $\left.D\right|_{\mathfrak{z}}=2 \mu I_{\mathfrak{z}}$ for some $\mu$ in $\mathbb{R}$ and the second formula of (2.5) is trivial, so we suppose henceforth that $\operatorname{dim}(\mathfrak{z})>1$. By interchanging $i$ and $k$ in (2.6), we see that

$$
D J_{Z_{k}} J_{Z_{i}} X=\left(2 \mu_{k}-2 \mu_{i}+\lambda\right) J_{Z_{k}} J_{Z_{i}} X,
$$

which yields

$$
D J_{Z_{i}} J_{Z_{k}} X=\left(2 \mu_{k}-2 \mu_{i}+\lambda\right) J_{Z_{i}} J_{Z_{k}} X,
$$

when $i \neq k$, since $J_{Z_{i}} J_{Z_{k}}=-J_{Z_{k}} J_{Z_{i}}$ by (2.3). This equality, compared with (2.6), shows that $\mu_{i}=\mu_{k}$, and the lemma follows.

Corollary 2.8 Let $D$ be a derivation in $\mathcal{D}^{\text {sym }}(\mathfrak{h})$. Denote by $2 \mu$ the eigenvalue of $D$ on $\mathfrak{z}$, and by $\left\{\lambda_{1}, \ldots, \lambda_{r}\right\}$ the distinct eigenvalues of $D$ on $\mathfrak{v}$, listed in decreasing order, and by $\mathfrak{v}_{i}$ the corresponding eigenspaces. Then $\lambda_{i}+\lambda_{r+1-i}=2 \mu$, and we may write

$$
D=\mu\left(2 P_{\mathfrak{z}}+P_{\mathfrak{v}}\right)+\sum_{i=1}^{\lfloor r / 2\rfloor}\left(\lambda_{i}-\mu\right)\left(P_{\mathfrak{v}_{i}}-P_{\mathfrak{v}_{r+1-i}}\right) ;
$$

all the maps $\left(P_{\mathfrak{v}_{i}}-P_{\mathfrak{v}_{r+1-i}}\right)$ and $2 P_{\mathfrak{z}}+P_{\mathfrak{v}}$ are derivations.
Proof This follows from Propositions 2.7 and 2.1.

## 3 Structure of semisimple Lie algebras

In this section, we describe the restricted root structure and the standard Iwasawa and Bruhat decompositions of a semisimple Lie algebra. Then we exhibit a number of $H$-type subalgebras of the Iwasawa $\mathfrak{n}$ subalgebra. Next, we analyse the structure of $\mathfrak{g}$ and $\mathfrak{n}$ in more detail.

### 3.1 Semisimple Lie algebras of the noncompact type

Take a real semisimple Lie algebra $\mathfrak{g}$ with Killing form $B$ and Cartan involution $\theta$, and let $\mathfrak{k} \oplus \mathfrak{p}$ be the corresponding Cartan decomposition of $\mathfrak{g}$. Fix a maximal subalgebra $\mathfrak{a}$ of $\mathfrak{p}$; its dimension is known as the real rank of $\mathfrak{g}$. Given an element $\alpha$ of $\operatorname{Hom}(\mathfrak{a}, \mathbb{R})$, we define the (possibly trivial) subspace $\mathfrak{g}_{\alpha}$ of $\mathfrak{g}$ by

$$
\mathfrak{g}_{\alpha}=\{X \in \mathfrak{g}:[H, X]=\alpha(H) X, \forall H \in \mathfrak{a}\} .
$$

Then $\alpha$ is said to be a restricted root if $\alpha \neq 0$ and $\mathfrak{g}_{\alpha} \neq\{0\}$. We denote by $\Sigma$ the restricted root system, that is, the set of all restricted roots. Note that $\left[\mathfrak{g}_{\alpha}, \mathfrak{g}_{\beta}\right] \subseteq \mathfrak{g}_{\alpha+\beta}$ for all $\alpha, \beta \in$ $\operatorname{Hom}(\mathfrak{a}, \mathbb{R})$, because $\operatorname{ad}(H)$ is a derivation for each $H \in \mathfrak{a}$. Hence if $\alpha$ and $\beta$ are roots, then $\alpha+\beta$ is also a root, unless $\alpha+\beta=0$ or $\left[\mathfrak{g}_{\alpha}, \mathfrak{g}_{\beta}\right]=\{0\}$. Since $\mathfrak{a}$ is $\theta$-invariant, so is $\mathfrak{g}_{0}$, and it follows easily that $\mathfrak{g}_{0}=\mathfrak{m} \oplus \mathfrak{a}$, where $\mathfrak{m}=\mathfrak{g}_{0} \cap \mathfrak{k}$. Then

$$
\mathfrak{g}=\mathfrak{m} \oplus \mathfrak{a} \oplus \sum_{\alpha \in \Sigma} \mathfrak{g}_{\alpha} .
$$

Henceforth, in this paper, unless stated explicitly otherwise, we write rank and root rather than real rank and restricted root for brevity; this should not create any confusion.

We recall that $\Sigma$ is said to be decomposable if $\Sigma=\Sigma_{1} \cup \Sigma_{2}$, where $\Sigma_{1}$ and $\Sigma_{2}$ are disjoint nontrivial subsets of $\Sigma$ and $\langle\gamma, \delta\rangle=0$ for all $\gamma \in \Sigma_{1}$ and all $\delta \in \Sigma_{2}$, and indecomposable otherwise. It is standard (see, for instance, Helgason [13] or Knapp [15]) that $\Sigma$ is indecomposable if and only if $\mathfrak{g}$ is simple, that is, cannot be written as a direct sum of nontrivial pairwise commuting ideals. We recall also that $\Sigma$ is said to be reduced if the only multiples of a root $\gamma$ that also lie in $\Sigma$ are $\pm \gamma$.

A Weyl chamber is a maximal open subset of $\mathfrak{a}$ in which no root vanishes. We choose one of these, $C$ say, and say that a root $\gamma$ is positive, and write $\gamma \in \Sigma^{+}$, when $\gamma(H)>0$ for all $H \in C$. Then $\Sigma^{+}$is closed under addition and $\Sigma=\Sigma^{+} \cup\left(-\Sigma^{+}\right)$. We write $\Delta$ for the smallest subset of $\Sigma^{+}$such that the boundary of $C$ is a subset of the set $\bigcup_{\alpha \in \Delta}\{H \in \mathfrak{a}: \alpha(H)=0\}$; the roots in $\Delta$ are called simple. Set

$$
\mathfrak{n}=\sum_{\alpha \in \Sigma^{+}} \mathfrak{g}_{\alpha} .
$$

Then we obtain the Bruhat decomposition of $\mathfrak{g}$, namely,

$$
\mathfrak{g}=\theta \mathfrak{n} \oplus \mathfrak{m} \oplus \mathfrak{a} \oplus \mathfrak{n}
$$

Each root $\gamma$ in $\Sigma^{+}$may be written uniquely as a sum $\sum_{\alpha \in \Delta} n_{\alpha} \alpha$, where each $n_{\alpha}$ is a nonnegative integer. The positive integer $\sum_{\alpha \in \Delta} n_{\alpha}$ is called the height of $\gamma$, and written
height $(\gamma)$. Clearly the height of a simple root is 1 , and moreover

$$
\operatorname{height}(\gamma+\delta)=\operatorname{height}(\gamma)+\operatorname{height}(\delta)
$$

for all $\gamma, \delta \in \Sigma^{+}$such that $\gamma+\delta \in \Sigma^{+}$. Then $\mathfrak{n}$ is graded by height; more precisely, we may write $\mathfrak{n}=\sum_{h \in \mathbb{Z}^{+}} \mathfrak{g}_{h}$, where $\left[\mathfrak{g}_{h}, \mathfrak{g}_{k}\right] \subseteq \mathfrak{g}_{h+k}$.

### 3.2 Reduction to the simple case

Our first simplification is a reduction of the problem to the case of the Iwasawa $\mathfrak{n}$ subalgebra of a simple Lie algebra $\mathfrak{g}$.

Proposition 3.1 Suppose that $\mathfrak{g}=\mathfrak{g}^{1} \oplus \mathfrak{g}^{2} \oplus \cdots \oplus \mathfrak{g}^{J}$, where $J>1$ and each $\mathfrak{g}^{j}$ is a nontrivial simple ideal, and that $\mathfrak{n}=\mathfrak{n}^{1} \oplus \mathfrak{n}^{2} \oplus \cdots \oplus \mathfrak{n}^{J}$ is the corresponding decomposition of $\mathfrak{n}$ into subalgebras. Then

$$
\mathcal{D}(\mathfrak{n})=\sum_{j=1}^{J} \mathcal{D}\left(\mathfrak{n}^{\mathfrak{j}}\right) .
$$

Remark 3.2 This is to be interpreted in the sense that each root-space-preserving derivation of $\mathfrak{n}$ preserves each of the subalgebras $\mathfrak{n}^{j}$, and the restriction to each subalgebra is a root-space-preserving derivation thereof, and vice versa.

Some of the simple summands $\mathfrak{g}^{j}$ may be compact. In this case, the corresponding space $\mathfrak{n}^{j}$ is $\{0\}$; we define $\mathcal{D}(\{0\})=\{0\}$.

Proof Since $D$ in $\mathcal{D}(\mathfrak{n})$ preserves the root spaces, it preserves each $\mathfrak{g}_{\alpha}$ and hence each $\mathfrak{n}^{j}$. So one direction of the assertion is proved. The other is obvious.

Remark 3.3 If we replace the root-space-preserving assumption by a grading-preserving assumption, and add the hypothesis that no summand is isomorphic to $\mathfrak{s o}(n, 1)$ for any $n$, then the result still holds. Indeed, when there is no abelian summand, $\mathfrak{n}$ is "totally nonabelian" in the language of Cowling and Ottazzi [11], and the conclusion follows from [11, Corollary 2.4].

### 3.3 The simple case

In light of Proposition 3.1, we may and shall assume that $\mathfrak{g}$ is simple in the rest of this paper.
Two observations underpin our approach to the study of derivations. First, derivations are local, in the sense that if $D$ is a root-space-preserving linear endomorphism of $\mathfrak{n}$, then linearity implies that $D$ is a derivation if and only if

$$
D[X, Y]=[D X, Y]+[X, D Y] \quad \forall X \in \mathfrak{g}_{\gamma} \quad \forall Y \in \mathfrak{g}_{\delta},
$$

as $\gamma$ and $\delta$ range over $\Sigma^{+}$. This identity holds trivially if $\gamma+\delta$ is not a root, for then both sides are 0 . If $\gamma+\delta$ is a root, then the subalgebra $\mathfrak{n}^{\{\gamma, \delta\}}$, defined by

$$
\mathfrak{n}^{\{\gamma, \delta\}}=\sum_{\epsilon \in \Sigma^{+} \cap(\mathbb{R} \gamma+\mathbb{R} \delta)} \mathfrak{g}_{\epsilon},
$$

is the Iwasawa $\mathfrak{n}$ subalgebra of a simple subalgebra of $\mathfrak{g}$, whose rank is 1 if $\gamma=\delta$ and 2 otherwise. Then we can understand $D$ provided we understand its restriction to Iwasawa $\mathfrak{n}$ algebras of simple Lie algebras of rank one and rank two.

The second observation is that $\mathfrak{n}$ may be equipped with a natural inner product so that, in the rank-one case, $\mathfrak{n}$ itself is an $H$-type algebra, while in the rank-two cases, $\mathfrak{n}$ has many $H$-type subalgebras. We will use what we know about the derivations of $H$-type algebras, but first we need to find $H$-type subalgebras of $\mathfrak{n}$.

### 3.4 Subalgebras of $\mathfrak{n}$ of $\boldsymbol{H}$-type

If $c>0$, then the symmetric bilinear form $\langle\cdot, \cdot\rangle$ on $\mathfrak{g}$, given by

$$
\begin{equation*}
\langle X, Y\rangle=-c B(X, \theta Y), \tag{3.1}
\end{equation*}
$$

is an inner product, which induces an inner product on the dual of $\mathfrak{a}$, also written $\langle\cdot, \cdot\rangle$; we denote the corresponding norms by $\|\cdot\|$. We fix $c$ so that the length of the longest roots is $\sqrt{2}$. In the vector space decomposition $\mathfrak{m} \oplus \mathfrak{a} \oplus \sum_{\alpha \in \Sigma} \mathfrak{g}_{\alpha}$ of $\mathfrak{g}$, the distinct summands are orthogonal.

Now the Killing form satisfies the well-known identity

$$
B([Z, X], Y)+B(X,[Z, Y])=0 \quad \forall X, Y, Z \in \mathfrak{g},
$$

and so $\operatorname{ad}(Y)^{\top}=-\operatorname{ad}(\theta Y)$, that is,

$$
\begin{equation*}
\langle X,[Y, Z]\rangle=-\langle[\theta Y, X], Z\rangle \quad \forall X, Y, Z \in \mathfrak{g} . \tag{3.2}
\end{equation*}
$$

If $\gamma \in \Sigma$ and $X, Y \in \mathfrak{g}_{\gamma}$, then $[\theta X, Y] \in \mathfrak{g}_{0}$. Further, for all $H \in \mathfrak{a}$,

$$
\begin{equation*}
\langle H,[\theta X, Y]\rangle=-\langle[X, H], Y\rangle=\langle[H, X], Y\rangle=\gamma(H)\langle X, Y\rangle . \tag{3.3}
\end{equation*}
$$

On the one hand, if $X \perp Y$, then $\langle H,[\theta X, Y]\rangle=0$, and so $[\theta X, Y] \in \mathfrak{a}^{\perp}$, whence $[\theta X, Y] \in$ $\mathfrak{m}$. On the other hand, $\theta[\theta X, X]=-[\theta X, X]$, so $[\theta X, X] \in \mathfrak{a}$. We write $H_{\gamma}$ for the unique element of $\mathfrak{a}$ such that $\delta\left(H_{\gamma}\right)=\langle\delta, \gamma\rangle$ for all $\delta \in \operatorname{Hom}(\mathfrak{a}, \mathbb{R})$, or equivalently for all $\delta \in \Sigma$. Now (3.3) implies that

$$
\begin{equation*}
\delta([\theta X, X])=\langle\delta, \gamma\rangle\|X\|^{2} \quad \text { and } \quad[\theta X, X]=\|X\|^{2} H_{\gamma} \tag{3.4}
\end{equation*}
$$

for all $X \in \mathfrak{g}_{\gamma}$. For future purposes, note that

$$
\begin{equation*}
\mathfrak{a}=\sum_{\alpha \in \Sigma^{+}} \mathbb{R} H_{\alpha} \tag{3.5}
\end{equation*}
$$

in general, this sum is not direct.
Our next results allow us to find various subalgebras of $\mathfrak{n}$ that are $H$-type algebras, or nearly so.

Lemma 3.4 Suppose that $\gamma, \delta$, and $\gamma+\delta$ are positive roots. For all $Z$ in $\mathfrak{g}_{\gamma+\delta}$, we define the linear operator $J_{Z}$ on $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta}$ by

$$
\begin{equation*}
J_{Z}=\operatorname{ad}(Z) \circ \theta \tag{3.6}
\end{equation*}
$$

Then $J_{Z}$ maps $\mathfrak{g}_{\gamma}$ into $\mathfrak{g}_{\delta}$ and $\mathfrak{g}_{\delta}$ into $\mathfrak{g}_{\gamma}$; further

$$
\begin{equation*}
\left\langle J_{Z} X, Y\right\rangle=\langle Z,[X, Y]\rangle \quad \forall X, Y \in \mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} . \tag{3.7}
\end{equation*}
$$

Proof The mapping properties of $J_{Z}$ are consequences of the orthogonality of distinct root spaces, while (3.7) follows from the definition of $J_{Z}$ and (3.2).

Lemma 3.5 Suppose that $\gamma, \delta$, and $\gamma+\delta$ are positive roots, and that $J_{Z}$ is defined as in Lemma 3.4. Suppose also that neither $2 \gamma+\delta$ nor $\gamma+2 \delta$ is a root. Then

$$
\begin{equation*}
\left[X, J_{Z} X\right]=\langle\gamma+\delta, \gamma\rangle\|X\|^{2} Z \quad \forall X \in \mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} \tag{3.8}
\end{equation*}
$$

and

$$
\begin{equation*}
J_{Z}^{2} X=-\langle\gamma+\delta, \gamma\rangle\|Z\|^{2} X \quad \forall X \in \mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta}, \tag{3.9}
\end{equation*}
$$

Thus if $Z \neq 0$, then $J_{Z}$ is a linear isomorphism of $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta}$ that exchanges $\mathfrak{g}_{\delta}$ and $\mathfrak{g}_{\gamma}$. Moreover, if $\gamma=\delta$, then $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{2 \gamma}$ is an H-type algebra, while if neither $2 \gamma$ nor $2 \delta$ is a root, then $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} \oplus \mathfrak{g}_{\gamma+\delta}$ is an H-type algebra.

Proof When $2 \gamma+\delta$ is not a root, $[X, Z]=0$ for all $Z$ in $\mathfrak{g}_{\gamma+\delta}$ and all $X$ in $\mathfrak{g}_{\gamma}$. Hence, from the Jacobi identity and (3.4),

$$
\begin{aligned}
{\left[X, J_{Z} X\right] } & =[X,[Z, \theta X]] \\
& =[[X, Z], \theta X]+[Z,[X, \theta X]] \\
& =(\gamma+\delta)([\theta X, X]) Z \\
& =\langle\gamma+\delta, \gamma\rangle\|X\|^{2} Z,
\end{aligned}
$$

and similarly,

$$
\begin{aligned}
J_{Z}\left(J_{Z} X\right) & =[Z, \theta[Z, \theta X]] \\
& =[Z,[\theta Z, X]] \\
& =[X,[\theta Z, Z]]+[\theta Z,[Z, X]] \\
& =-\langle\gamma+\delta, \gamma\rangle\|Z\|^{2} X .
\end{aligned}
$$

By exchanging the role of $\gamma$ and $\delta$ in the last two formulae, we see that

$$
\left[Y, J_{Z} Y\right]=\langle\gamma+\delta, \delta\rangle\|Y\|^{2} Z
$$

and

$$
J_{Z}\left(J_{Z} Y\right)=-\langle\gamma+\delta, \delta\rangle\|Z\|^{2} Y
$$

for all $Z \in \mathfrak{g}_{\gamma+\delta}$ and all $Y \in \mathfrak{g}_{\delta}$ when $\gamma+2 \delta$ is not a root. Hence (3.8) and (3.9) are proved, and $J_{Z}$ is a linear isomorphism from $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta}$ onto $\mathfrak{g}_{\delta} \oplus \mathfrak{g}_{\gamma}$ when $Z \neq 0$.

Either $\gamma=\delta$ or the roots $\gamma$ and $\delta$ span a root system of rank 2. By inspection of the possibilities, we see that the hypotheses that $\gamma, \delta$, and $\gamma+\delta$ are roots and $2 \gamma+\delta$ and $\gamma+2 \delta$ are not roots imply that $\|\gamma\|=\|\delta\|$ and $\langle\gamma+\delta, \delta\rangle=\langle\gamma+\delta, \gamma\rangle>0$. Now (3.8) and (3.9) follow immediately. Further, if $\gamma=\delta$ or neither $2 \gamma$ nor $2 \delta$ is a root, then $\langle\gamma+\delta, \gamma\rangle=1$, and so

$$
J_{Z}^{2} X=-\|Z\|^{2} X \quad \forall X \in \mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} \quad \forall Z \in \mathfrak{g}_{\gamma+\delta}
$$

as required.
Remark 3.6 We have just shown that the Iwasawa $\mathfrak{n}$ algebras of real rank one simple Lie algebras are $H$-type. Further, inspection of the root systems of rank one and two shows that if $\gamma, \delta$, and $\gamma+\delta$ are roots and $2 \gamma+\delta$ and $\gamma+2 \delta$ are not roots, then either $2 \gamma$ and $2(\gamma+\delta)$ are both roots, or neither is a root.

Corollary 3.7 Suppose that $\gamma, \delta$, and $\gamma+\delta$ are positive roots, and that neither $2 \gamma+\delta$ nor $\gamma+2 \delta$ is a root. If $D$ is a root-space-preserving derivation of $\mathfrak{g}$ whose restriction to $\mathfrak{g}_{\gamma+\delta}$ is symmetric, then

$$
\begin{equation*}
D^{\top}[X, Y]=\left[D^{\top} X, Y\right]+\left[X, D^{\top} Y\right] \quad \forall X \in \mathfrak{g}_{\gamma} \quad \forall Y \in \mathfrak{g}_{\delta} . \tag{3.10}
\end{equation*}
$$

Proof The proof is a mild generalisation of the proof of Corollary 2.4. Observe first that if $E$ is a root-space-preserving linear endomorphism of $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} \oplus \mathfrak{g}_{\gamma+\delta}$, then $E[X, Y]=$ $[E X, Y]+[X, E Y]$ if and only if

$$
\begin{align*}
\left\langle J_{E^{\top} Z} X, Y\right\rangle & =\left\langle E^{\top} Z,[X, Y]\right\rangle \\
& =\langle Z, E[X, Y]\rangle  \tag{3.11}\\
& =\langle Z,[E X, Y]\rangle+\langle Z,[X, E Y]\rangle \\
& =\left\langle J_{Z} E X, Y\right\rangle+\left\langle E^{\top} J_{Z} X, Y\right\rangle,
\end{align*}
$$

for all $X \in \mathfrak{g}_{\gamma}$, all $Y \in \mathfrak{g}_{\delta}$, and all $Z \in \mathfrak{g}_{\gamma+\delta}$.
Since $\left.D\right|_{\mathfrak{g}_{\alpha+\beta}}$ is symmetric, it is diagonalisable. Take an eigenvector $Z$ in $\mathfrak{g}_{\alpha+\beta}$ with eigenvalue $2 \mu$. By (3.11),

$$
2 \mu J_{Z}=J_{D Z}=J_{D^{\top} Z}=D^{\top} J_{Z}+J_{Z} D
$$

whence composition on both sides by $J_{Z}$ gives

$$
-2 \mu|Z|^{2} J_{Z}=-|Z|^{2} J_{Z} D^{\top}-|Z|^{2} D J_{Z}
$$

and

$$
J_{D Z}=D J_{Z}+J_{Z} D^{\top}
$$

This holds for all eigenvectors $Z$ of $D$, and so for all $Z \in \mathfrak{z}$ by linearity, so (3.10) holds by (3.11).

We are supposing that $\mathfrak{g}$ is simple, so $\Sigma$ is indecomposable. In particular, $\Sigma$ contains just one highest root (see Bourbaki [1, p. 165, Proposition 25]), which we denote by $\omega$. We fix the constant $c$ in (3.1) by requiring that $\|\omega\|^{2}=2$. Then for each $\gamma \in \Sigma$, the number $\langle\gamma, \omega\rangle$ is one of $\pm 2, \pm 1$ and 0 ; further, it is $\pm 2$ if and only if $\gamma= \pm \omega$.

Define

$$
\Sigma_{1}=\{\gamma \in \Sigma:\langle\gamma, \omega\rangle=1\} \text { and } \Sigma_{0}=\{\gamma \in \Sigma:\langle\gamma, \omega\rangle=0\},
$$

and write $\Sigma_{0}^{+}$for $\Sigma^{+} \cap \Sigma_{0}$. Then, by Ciatti [6, Lemma 2.1],

$$
\Sigma^{+}=\Sigma_{0}^{+} \cup \Sigma_{1} \cup\{\omega\} .
$$

Further, define

$$
\mathfrak{v}=\sum_{\gamma \in \Sigma_{1}} \mathfrak{g}_{\gamma}, \quad \mathfrak{h}=\mathfrak{v} \oplus \mathfrak{g}_{\omega} \quad \text { and } \quad \mathfrak{n}_{0}=\sum_{\gamma \in \Sigma_{0}^{+}} \mathfrak{g}_{\gamma}
$$

then

$$
\mathfrak{n}=\mathfrak{n}_{0} \oplus \mathfrak{v} \oplus \mathfrak{g}_{\omega}=\mathfrak{n}_{0} \oplus \mathfrak{h} .
$$

Following Ciatti [6], for $Z$ in $\mathfrak{g}_{\omega}$, we define the operator $J_{Z}: \mathfrak{v} \rightarrow \mathfrak{v}$ by

$$
\begin{equation*}
J_{Z} X=[Z, \theta X] . \tag{3.12}
\end{equation*}
$$

Then by definition and (3.2),

$$
\left\langle J_{Z} X, Y\right\rangle=\langle[Z, \theta X], Y\rangle=\langle Z,[X, Y]\rangle \quad \forall X, Y \in \mathfrak{v} .
$$

Lemma 3.8 (Ciatti [3]) The pair $(\mathfrak{v} \oplus \mathfrak{z},\langle\cdot, \cdot\rangle)$ is an H-type algebra with centre $\mathfrak{g}_{\omega}$, that is, $[\mathfrak{v}, \mathfrak{v}]=\mathfrak{g}_{\omega}$ and

$$
\begin{equation*}
J_{Z}^{2} X=-\|Z\|^{2} X \tag{3.13}
\end{equation*}
$$

for all $Z$ in $\mathfrak{g}_{\omega}$ and $X$ in $\mathfrak{v}$.
Proof This follows from Lemma 3.5.
Now we list some $H$-type subalgebras of the Iwasawa $\mathfrak{n}$ algebras of rank-two simple Lie algebras. When the root system is of type $A_{2}$, then $\mathfrak{n}$ is itself an $H$-type algebra. When the root system is of type $B_{2}$, say $\Sigma=\{\alpha, \beta, \alpha+\beta, 2 \alpha+\beta\}$, then $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta}$ is an $H$-type subalgebra (and moreover $\mathfrak{g}_{\beta} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta}$ is abelian and hence a degenerate $H$-type algebra too). When the root system is of type $B C_{2}$, say $\Sigma=\{\alpha, 2 \alpha, \beta, \alpha+\beta, 2 \alpha+\beta, 2 \alpha+2 \beta\}$, then $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{2 \alpha}$ and $\mathfrak{g}_{\beta} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+2 \beta}$ are $H$-type subalgebras, and $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta}$ is close to an $H$-type subalgebra (see Lemma 3.5). Finally, when the root system is of type $G_{2}$, say $\Sigma=\{\alpha, \beta, \alpha+\beta, 2 \alpha+\beta, 3 \alpha+\beta, 3 \alpha+\beta\}$, then $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{3 \alpha+\beta}$ and $\mathfrak{g}_{\beta} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{3 \alpha+\beta} \oplus \mathfrak{g}_{3 \alpha+2 \beta}$ are $H$-type subalgebras.

### 3.5 The fine structure of $\mathfrak{g}$

We now study $\mathfrak{g}$ in more detail.
Lemma 3.9 Suppose that $\gamma, \delta$, and $\gamma+\delta$ are positive roots, and that $\gamma-\delta$ and $\gamma+2 \delta$ are not roots. If $U \in \mathfrak{g}_{\delta} \backslash\{0\}$, then

$$
\begin{equation*}
\left\{[U, X]: X \in \mathfrak{g}_{\gamma}\right\}=\mathfrak{g}_{\gamma+\delta} \quad \text { and } \quad\left\{[\theta U, Y]: Y \in \mathfrak{g}_{\gamma+\delta}\right\}=\mathfrak{g}_{\gamma} \tag{3.14}
\end{equation*}
$$

Consequently, $\operatorname{dim}\left(\mathfrak{g}_{\gamma}\right)=\operatorname{dim}\left(\mathfrak{g}_{\gamma+\delta}\right)$ and $\operatorname{ad}(U)$ is bijective from $\mathfrak{g}_{\gamma}$ to $\mathfrak{g}_{\gamma+\delta}$.
Proof The hypotheses imply that $\langle\gamma+\delta, \delta\rangle=\frac{1}{2}\langle\delta, \delta\rangle \neq 0$. Evidently, if $Y \in \mathfrak{g}_{\gamma+\delta}$, then $[\theta U, Y] \in \mathfrak{g}_{\gamma}$ and
$[U,[\theta U, Y]]=[[U, \theta U], Y]+[\theta U,[U, Y]]=(\gamma+\delta)([U, \theta U]) Y=-\langle\gamma+\delta, \delta\rangle\|U\|^{2} Y$
by (3.4), and it follows that $Y$ is in the range of $\operatorname{ad}(U)$. This proves the left hand formula of (3.14) and hence $\operatorname{dim}\left(\mathfrak{g}_{\gamma}\right) \geq \operatorname{dim}\left(\mathfrak{g}_{\gamma+\delta}\right)$. The right-hand formula and the opposite inequality $\operatorname{dim}\left(\mathfrak{g}_{\gamma}\right) \leq \operatorname{dim}\left(\mathfrak{g}_{\gamma+\delta}\right)$ may be shown similarly.

The bijectivity of $\operatorname{ad}(U)$, and of $\operatorname{ad}(\theta U)$, follow.
Lemma 3.10 Suppose that $\gamma, \delta, \gamma+\delta$ and $\gamma+2 \delta$ are positive roots, and that $\gamma-\delta$ and $\gamma+3 \delta$ are not roots. If $U \in \mathfrak{g}_{\gamma} \backslash\{0\}$ and $X \in \mathfrak{g}_{\delta} \backslash\{0\}$, then

$$
[U, X] \neq 0 \text { and }[[U, X], X] \neq 0
$$

Proof First, $[U, \theta X]=0$ since $\gamma-\delta$ is not a root.
The hypotheses imply that $\gamma$ and $\delta$ span a root subsystem of type $B_{2}$ or $B C_{2}$, whence $2 \gamma+\delta$ is not a root, and that $\langle\gamma+\delta, \delta\rangle=0$ while $\langle\gamma, \delta\rangle \neq 0$ (see Bourbaki [1, p. 148, Théorème 1]). Now $[U, X] \neq 0$, by Lemma 3.9 with the roles of $\gamma$ and $\delta$ exchanged.

Next, by the Jacobi identity and the facts that $\langle\gamma+\delta, \delta\rangle=0$ and $[U, \theta X]=0$,

$$
\begin{aligned}
{[[[U, X], X], \theta X] } & =[[\theta X, X],[U, X]]+[[[U, X], \theta X], X] \\
& =(\gamma+\delta)([\theta X, X])[U, X]+[[[U, X], \theta X], X] \\
& =\langle\gamma+\delta, \delta\rangle\|X\|^{2}[U, X]+[[U,[X, \theta X]], X]+[[[U, \theta X], X], X] \\
& =\langle\gamma, \delta\rangle\|X\|^{2}[U, X] \neq 0,
\end{aligned}
$$

which ensures that $[[U, X], X] \neq 0$ if neither $U$ nor $X$ is 0 .
We are going to analyse general simple Lie algebras by looking carefully at subalgebras of rank 1 or 2 . Given a subset $E$ of $\Sigma^{+}$, we write $\mathfrak{g}^{\mathrm{E}}$ for the subalgebra of $\mathfrak{g}$ generated by the root spaces $\mathfrak{g}_{\epsilon}$ where $\epsilon$ ranges over span E .

We define, for any root $\gamma, \mathfrak{m}^{\{\gamma\}}=\mathfrak{m} \cap \mathfrak{g}^{\{\gamma\}}$ and

$$
\mathfrak{m}^{\gamma}=\operatorname{span}\left\{[X, \theta Y]: X, Y \in \mathfrak{g}_{\gamma},\langle X, Y\rangle=0\right\} .
$$

Lemma 3.11 Suppose that $\gamma, \delta$ and $\gamma+\delta$ are positive roots. Then

$$
\begin{aligned}
& \left\{[X, Y]: X \in \mathfrak{g}_{\gamma}, Y \in \mathfrak{g}_{\delta}\right\}=\mathfrak{g}_{\gamma+\delta} ; \\
& \quad\left\{U \in \mathfrak{g}_{\gamma}:\left.\operatorname{ad}(U)\right|_{\mathfrak{g}_{\delta}}=0\right\}=\{0\} .
\end{aligned}
$$

Proof We observe that $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$ is irreducible on $\mathfrak{g}_{\epsilon}$ for any positive root $\epsilon$. Indeed, we know that $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$ maps $\mathfrak{g}_{\epsilon}$ into itself, while from Kostant's double transitivity theorem [17], $\operatorname{ad}\left(\mathfrak{m}^{\{\epsilon\}}\right)$ is transitive on the unit sphere in $\mathfrak{g}_{\epsilon}$, whence $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$ takes any nonzero vector in $\mathfrak{g}_{\epsilon}$ to any other nonzero vector. (For an alternative approach to this, see Cowling et al. [9]).

It follows that the subspace $\left[\mathfrak{m} \oplus \mathfrak{a},\left[\mathfrak{g}_{\gamma}, \mathfrak{g}_{\delta}\right]\right]$ is either $\mathfrak{g}_{\gamma+\delta}$ or $\{0\}$. Hence, to prove the first equality, it suffices to show that

$$
\begin{equation*}
\left[\mathfrak{g}_{\gamma}, \mathfrak{g}_{\delta}\right] \neq\{0\} . \tag{3.15}
\end{equation*}
$$

To do this, we consider the subset $(\mathbb{Z} \gamma+\mathbb{Z} \delta) \cap \Sigma$ of $\Sigma$, which is a root system in its own right.

If this root subsystem is of rank one, then necessarily $\delta=\gamma$, and $\gamma+\delta=2 \gamma$. In this case, $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{2 \gamma}$ is an $H$-type algebra, and (3.15) follows.

If the root system is of type $A_{2}$, then we are done, since $\mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{\delta} \oplus \mathfrak{g}_{\gamma+\delta}$ is an $H$-type algebra.

If the root system is of type $B_{2}$ or $B C_{2}$, then (3.15) follows from Lemma 3.10.
If the root system is of type $G_{2}$, then the algebra is split or complex, and in this case the result is well known.

Finally, suppose that $U \in \mathfrak{g}_{\gamma} \backslash\{0\}$ and $[U, X]=0$ for all $X \in \mathfrak{g}_{\delta}$. Then

$$
[\operatorname{ad}(W) U, X]=\operatorname{ad}(W)[U, X]-[U, \operatorname{ad}(W) X]=0
$$

for all $X \in \mathfrak{g}_{\delta}$ and all $W \in \mathfrak{m} \oplus \mathfrak{a}$, and hence $[V, X]=0$ for all $V \in \mathfrak{g}_{\gamma}$ and all $X \in \mathfrak{g}_{\delta}$, which is impossible.

Lemma 3.12 The following hold:
(i) if $\gamma$ is a root, then $\mathfrak{m}^{-\gamma}=\mathfrak{m}^{\gamma}$,
(ii) if $\gamma$ is a root, then $\left[\mathfrak{m}, \mathfrak{m}^{\gamma}\right] \subseteq \mathfrak{m}^{\gamma}$,
(iii) if $\gamma, \delta$ and $\epsilon$ are roots and $\epsilon \in \mathbb{Z} \gamma+\mathbb{Z} \delta$, then $\mathfrak{m}^{\epsilon} \subseteq \mathfrak{m}^{\gamma}+\mathfrak{m}^{\delta}$,
(iv) if $\gamma$ is a root, then $\mathfrak{m}^{\gamma} \subseteq \mathfrak{m}^{\{\gamma\}}$, with equality if $\gamma / 2$ is not a root,
(v) $\mathfrak{m}=\sum_{\gamma \in \Delta} \mathfrak{m}^{\gamma}=\sum_{\gamma \in \Sigma^{+}} \mathfrak{m}^{\gamma}$.

Proof Observe that if $X, Y \in \mathfrak{g}_{-\gamma}$, then $[X, \theta Y]=-[\theta Y, \theta(\theta X)]$, and $\theta Y, \theta X \in \mathfrak{g}_{\gamma}$, so (i) holds.

Now we prove (ii). If $Z \in \mathfrak{m}$ and $X, Y \in \mathfrak{g}_{\gamma}$, then

$$
[Z,[X, \theta Y]]=[[Z, X], \theta Y]+[X,[Z, \theta Y]]
$$

Both summands lie in $\mathfrak{m}^{\gamma}$. Thus $\mathfrak{m}^{\gamma}$ is an ideal in $\mathfrak{m}$, and in particular, is a subalgebra.
Next, we prove (iii). First, if $\gamma, \delta$ and $\gamma+\delta$ are roots and $W, Z \in \mathfrak{g}_{\gamma+\delta}$, then there exist $X \in \mathfrak{g}_{\gamma}$ and $Y \in \mathfrak{g}_{\delta}$ such that $[X, Y]=Z$, by Lemma 3.11. Then

$$
\begin{aligned}
{[W, \theta Z]=[W,[\theta X, \theta Y]] } & =[[W, \theta X], \theta Y]+[\theta X,[W, \theta Y]] \\
& =[W, \theta X], \theta Y]-[[W, \theta Y], \theta X] \in \mathfrak{m}^{\gamma}+\mathfrak{m}^{\delta} .
\end{aligned}
$$

To prove (iii), we use (i) and the observation above repeatedly.
To prove (iv), observe that if $2 \gamma$ and $\frac{1}{2} \gamma$ are not roots, then $\mathfrak{g}_{-\gamma} \oplus \mathfrak{m}^{\gamma} \oplus \mathbb{R} H_{\gamma} \oplus \mathfrak{g}_{\gamma}$ coincides with the subalgebra $\mathfrak{g}^{\{\gamma\}}$, whence $\mathfrak{m}^{\gamma}=\mathfrak{m}^{\{\gamma\}}$. Similarly, if $\gamma$ and $2 \gamma$ are both roots, then $\mathfrak{m}^{2 \gamma} \subseteq \mathfrak{m}^{\gamma}$, by (ii), so $\mathfrak{g}_{-2 \gamma} \oplus \mathfrak{g}_{-\gamma} \oplus \mathfrak{m}^{\gamma} \oplus \mathbb{R} H_{\gamma} \oplus \mathfrak{g}_{\gamma} \oplus \mathfrak{g}_{2 \gamma}$ coincides with the subalgebra $\mathfrak{g}^{\{\gamma\}}$, and again $\mathfrak{m}^{\gamma}=\mathfrak{m}^{\{\gamma\}}$. Finally, if $\gamma$ and $\frac{1}{2} \gamma$ are both roots, $\mathfrak{m}^{\gamma} \subseteq \mathfrak{m}^{\gamma / 2}$, and $\mathfrak{m}^{\gamma} \subseteq \mathfrak{m}^{\{\gamma\}}$. This inclusion is strict when $\mathfrak{g}^{\{\gamma\}}$ is $\mathfrak{s u}(n, 1)$ (where $n>1$ ) or $\mathfrak{s p}(n, 1)$ (where $n>1$ ).

To prove (v), we use (i) and (iii) repeatedly.

## 4 Derivations of semisimple Lie algebras

In this section, we discuss the height of roots and the associated grading of the Lie algebra $\mathfrak{g}$, and prove a number of results on height-preserving derivations. Then we prove a localisation result for derivations of $\mathfrak{g}$. Our final result is a necessary and sufficient condition for a skewsymmetric root-space-preserving derivation of $\mathfrak{n}$ to be of the form $\operatorname{ad}(Z)$ for some $Z \in \mathfrak{m}$.

Lemma 4.1 Suppose that $W \in \mathfrak{g}_{0}$. Then $W=0$ if and only if $\left.\operatorname{ad}(W)\right|_{\mathfrak{g}_{\beta}}=0$ for all $\beta \in \Delta$.
Proof One implication is obvious. To prove the other, suppose that ad $\left.(W)\right|_{\mathfrak{g}_{\beta}}=0$ for all $\beta \in \Delta$. Then $\operatorname{ad}(W)$ vanishes on $\mathfrak{n}$, whence $\operatorname{ad}(\theta W)$ also vanishes on $\mathfrak{n}$ since $\operatorname{ad}(\theta W)=$ $-\operatorname{ad}(W)^{\top}$.

Now if $X \in \mathfrak{n}$, then

$$
[W, \theta X]=\theta[\theta W, X]=0 .
$$

Since $\mathfrak{g}$ is simple, and $\operatorname{ad}(W)$ is a derivation that vanishes on $\mathfrak{n} \oplus \theta \mathfrak{n}$ and hence on the algebra that this generates, that is, $\mathfrak{g}$, we conclude that $W=0$.

We are interested in the derivations $D$ of $\mathfrak{n}$ that preserve the root space structure, that is, are such that $D\left(\mathfrak{g}_{\alpha}\right) \subseteq \mathfrak{g}_{\alpha}$ for all $\alpha \in \Sigma^{+}$. We write $\mathcal{D}(\mathfrak{n})$ for the space of these mappings.

Recall that the height of the positive root $\alpha$, written height $(\alpha)$, is defined to be $\sum_{j=1}^{r} n_{j}$, where $\alpha=\sum_{j=1}^{r} n_{j} \alpha_{j}$ and $\alpha_{j} \in \Delta$. Note that there is an element $H_{0}$ of $\mathfrak{a}$ such that [ $\left.H_{0}, X\right]=$ height $(\alpha) X$ for all $X \in \mathfrak{g}_{\alpha}$ and all $\alpha \in \Delta$. We may extend the height function to all roots: we set height $(\gamma)=h$ when $\left[H_{0}, X\right]=h X$ for all $X \in \mathfrak{g}_{\gamma}$. When $h$ is a nonzero integer, we write $\mathfrak{g}_{h}$ for $\sum_{\gamma} \mathfrak{g}_{\gamma}$, where we sum over the $\gamma$ in $\Sigma$ such that height $(\gamma)=h$. We defined $\mathfrak{g}_{0}$ to be the "null root space" $\mathfrak{m} \oplus \mathfrak{a}$, which fortunately coincides with the subspace of $\mathfrak{g}$ of elements of height 0 , and so $\mathfrak{g}_{0}$ may also be used to describe the latter space, consistently with our $\mathfrak{g}_{h}$ notation.

Proposition 4.2 The Lie algebra $\mathfrak{g}$ is graded: more precisely, $\mathfrak{g}=\sum_{h \in \mathbb{Z}} \mathfrak{g}_{h}$, and $\left[\mathfrak{g}_{h}, \mathfrak{g}_{h^{\prime}}\right] \subseteq$ $\mathfrak{g}_{h+h^{\prime}}$. Next, $\mathfrak{n}$ is stratified, that is, $\left[\mathfrak{g}_{h}, \mathfrak{g}_{1}\right]=\mathfrak{g}_{h+1}$ for all $h \in \mathbb{Z}^{+}$, so $\mathfrak{g}_{1}$ generates $\mathfrak{n}$. Finally, if $0<h<\operatorname{height}(\omega)$, then $\left\{X \in \mathfrak{g}_{h}:\left.\operatorname{ad}(X)\right|_{\mathfrak{g}_{1}}=0\right\}=\{0\}$.

Proof The linear operator ad $\left(H_{0}\right)$ on $\mathfrak{g}$ is diagonalisable, whence $\mathfrak{g}$ decomposes as a sum of eigenspaces; given that the simple roots correspond to eigenvalue 1 and all positive roots are sums of simple roots (with multiplicities), all eigenvalues are integers. Further, $\operatorname{ad}\left(H_{0}\right)$ is a derivation and so $\left[\mathfrak{g}_{h}, \mathfrak{g}_{h^{\prime}}\right] \subseteq \mathfrak{g}_{h+h^{\prime}}$.

If height $(\gamma)=h+1$ where $h>0$, then there exists $\alpha \in \Delta$ such that $\gamma-\alpha$ is a root, by [8, Lemma 3.1]. Lemma 3.11 shows that $\left[\mathfrak{g}_{\alpha}, \mathfrak{g}_{\gamma-\alpha}\right]=\mathfrak{g}_{\gamma}$, and it follows that $\mathfrak{g}_{\gamma} \subseteq\left[\mathfrak{g}_{1}, \mathfrak{g}_{h}\right]$. This applies to all $\gamma$ of height $h+1$ and so $\mathfrak{g}_{h+1} \subseteq\left[\mathfrak{g}_{1}, \mathfrak{g}_{h}\right]$. The converse inclusion has already been established.

Finally, suppose that $X \in \mathfrak{g}_{h}$ and $\left.\operatorname{ad}(X)\right|_{\mathfrak{g}_{1}}=0$. Write $X$ as $\sum_{\gamma} X_{\gamma}$, where $X_{\gamma} \in \mathfrak{g}_{\gamma}$ and height $(\gamma)=h$. Now

$$
0=[[H, X], Y]=[[H, Y], X]+[H,[X, Y]] \quad \forall Y \in \mathfrak{g}_{1}
$$

whence $\left.\operatorname{ad}([H, X])\right|_{\mathfrak{g}_{1}}=0$ for all $H \in \mathfrak{a}$. The algebra of operators generated by the operators $\operatorname{ad}(H)$ for all $H \in \mathfrak{a}$ is closed under transpose and hence spanned by its minimal projections, which are precisely the projections onto the root spaces $\mathfrak{g}_{\gamma}$ as $\gamma$ varies over $\Sigma$. We deduce that ad $\left.\left(X_{\gamma}\right)\right|_{\mathfrak{g}_{1}}=0$ for all $\gamma$ of height $h$. By Lemma 3.11, each $X_{\gamma}$ is zero.

We are now going to work with derivation identities.
Definition 4.3 Suppose that $D$ is a derivation of $\mathfrak{n}$. For $\gamma, \delta \in \Sigma^{+}$, let $\left(D_{\gamma, \delta}\right)$ be the formula

$$
D[X, \theta Z]=[D X, \theta Z]+[X, \theta D Z]
$$

for all $X \in \mathfrak{g}_{\gamma}$ and all $Z \in \mathfrak{g}_{\delta}$, and ( $E_{\gamma, \delta}$ ) be the formula

$$
D[[X, \theta Y], Z]=[[D X, \theta Y], Z]+[[X, \theta D Y], Z]+[[X, \theta Y], D Z]
$$

for all $X, Y \in \mathfrak{g}_{\gamma}$ and all $Z \in \mathfrak{g}_{\delta}$.
Note that if $D$ were a derivation of $\mathfrak{g}$ such that $\theta D=D \theta$, then these formulae would follow from the Jacobi identity. At this point, we are not asserting their truth!

Theorem 4.4 Suppose that $D$ is a skew-symmetric height-preserving derivation of $\mathfrak{n}$, and that ( $E_{\gamma, \delta}$ ), as in Definition 4.3, holds for all $\gamma, \delta \in \Delta$. Then the following statements hold.
(i) There is a unique well-defined linear map $\tilde{D}: \mathfrak{g}_{0} \rightarrow \mathfrak{g}_{0}$ such that

$$
\tilde{D}[X, \theta Y]=[D X, \theta Y]+[X, \theta D Y] \quad \forall X, Y \in \mathfrak{g}_{1} .
$$

(ii) The range of the linear map $\tilde{D}$ is contained in $\mathfrak{m}$.
(iii) The linear map $E: \mathfrak{g}_{0} \oplus \mathfrak{n} \rightarrow \mathfrak{g}_{0} \oplus \mathfrak{n}$, defined by

$$
E(W+X)=\tilde{D} W+D X \quad \forall W \in \mathfrak{g}_{0} \quad \forall X \in \mathfrak{n},
$$

is a derivation.
(iv) If $h \geq k \geq 0$, then

$$
E[U, \theta V]=[E U, \theta V]+[U, \theta E V] \quad \forall U \in \mathfrak{g}_{h} \quad \forall V \in \mathfrak{g}_{k}
$$

Proof To prove (i), we first claim that if $\alpha, \beta \in \Delta$ and $\alpha \neq \beta$, then

$$
\begin{equation*}
[D X, \theta Y]+[X, \theta D Y]=0 \quad \forall X \in \mathfrak{g}_{\alpha} \quad \forall Y \in \mathfrak{g}_{\beta} . \tag{4.1}
\end{equation*}
$$

To see this, take $W$ in $\mathfrak{g}_{0}$ of the form $[U, \theta V]$, where $U, V \in \mathfrak{g}_{\gamma}$, for some $\gamma \in \Delta$. Since $D$ is a skew-symmetric derivation,

$$
\begin{aligned}
\langle[D X, \theta Y]+[X, \theta D Y], W\rangle & =-\langle D X,[W, Y]\rangle-\langle X,[W, D Y]\rangle \\
& =\langle X, D[W, Y]\rangle-\langle X,[W, D Y]\rangle \\
& =\langle X,[[D U, \theta V]+[U, \theta D V], Y]\rangle \\
& =-\langle[X, \theta Y],[D U, \theta V]+[U, \theta D V]\rangle \\
& =0,
\end{aligned}
$$

since $[X, \theta Y]=0$ because $\alpha-\beta$ is not a root; the third step uses $\left(E_{\gamma, \beta}\right)$. Since $\mathfrak{g}_{0}$ is spanned by elements of the form $[U, \theta V]$, our claim is established.

Now we define $L: \bigcup_{\alpha \in \Delta} \mathfrak{g}_{\alpha} \times \bigcup_{\alpha \in \Delta} \mathfrak{g}_{\alpha} \rightarrow \mathfrak{g}_{0}$ by $L(X, Y)=[X, \theta Y]$. Then $L$ extends automatically to a linear map, also denoted $L$, from $\mathfrak{g}_{1} \otimes \mathfrak{g}_{1}$ to $\mathfrak{g}_{0}$. Take $X_{j}, Y_{j} \in \mathfrak{g}_{1}$, and suppose that $\sum_{j}\left[X_{j}, \theta Y_{j}\right]=0$ in $\mathfrak{g}_{0}$. Write each $X_{j}$ as $\sum_{\alpha} X_{j, \alpha}$ and each $Y_{j}$ as $\sum_{\beta} Y_{j, \beta}$, where $X_{j, \alpha} \in \mathfrak{g}_{\alpha}$ and $Y_{j, \beta} \in \mathfrak{g}_{\beta}$; here $\alpha$ and $\beta$ range over $\Delta$. Then

$$
\sum_{j}\left[X_{j}, \theta Y_{j}\right]=\sum_{j, \alpha}\left[X_{j, \alpha}, \theta Y_{j, \alpha}\right]
$$

since $\left[X_{j, \alpha}, \theta Y_{j, \beta}\right]=0$ because $\alpha-\beta$ is not a root if $\alpha \neq \beta$. If $\gamma \in \Delta$ and $W \in \mathfrak{g}_{\gamma}$, then

$$
\sum_{j}\left[\left[X_{j}, \theta Y_{j}\right], W\right]=0 \quad \text { and } \quad \sum_{j}\left[\left[X_{j}, \theta Y_{j}\right], D W\right]=0
$$

by hypothesis. Thus by ( $E_{\alpha, \gamma}$ ),

$$
\begin{aligned}
0 & =D \sum_{j}\left[\left[X_{j}, \theta Y_{j}\right], W\right]=D \sum_{j, \alpha}\left[\left[X_{j, \alpha}, \theta Y_{j, \alpha}\right], W\right] \\
& =\sum_{j, \alpha}\left[\left[D X_{j, \alpha}, \theta Y_{j, \alpha}\right], W\right]+\left[\left[X_{j, \alpha}, \theta D Y_{j, \alpha}\right], W\right]+\left[\left[X_{j, \alpha}, \theta Y_{j, \alpha}\right], D W\right] \\
& =\sum_{j, \alpha}\left[\left[D X_{j, \alpha}, \theta Y_{j, \alpha}\right]+\left[X_{j, \alpha}, \theta D Y_{j, \alpha}\right], W\right]+\sum_{j}\left[\left[X_{j}, \theta Y_{j}\right], D W\right] \\
& =\sum_{j, \alpha, \beta}\left[\left[D X_{j, \alpha}, \theta Y_{j, \beta}\right]+\left[X_{j, \alpha}, \theta D Y_{j, \beta}\right], W\right],
\end{aligned}
$$

and this shows that

$$
\sum_{j}\left[\left[D X_{j, \alpha}, \theta Y_{j, \beta}\right]+\left[X_{j, \alpha}, \theta D Y_{j, \beta}\right], W\right]=0
$$

From Lemma 4.1, we see that

$$
\sum_{j}\left[D X_{j, \alpha}, \theta Y_{j, \beta}\right]+\left[X_{j, \alpha}, \theta D Y_{j, \beta}\right]=0
$$

It follows immediately that $\tilde{D}$, given by

$$
\tilde{D} \sum_{j}\left[X_{j}, \theta Y_{j}\right]=\sum_{j}\left(\left[D X_{j}, \theta Y_{j}\right]+\left[X_{j}, \theta D Y_{j}\right]\right)
$$

is well defined; clearly $\tilde{D}$ is also unique.
To prove (ii), note that if $X, Y \in \mathfrak{g}_{\alpha}$ where $\alpha \in \Delta$, and $H \in \mathfrak{a}$, then

$$
\begin{aligned}
\langle[D X, \theta Y]+[X, \theta D Y], H\rangle & =\langle D X,[H, Y]\rangle+\langle X,[H, D Y]\rangle \\
& =\langle D X,[H, Y]\rangle+\langle[H, X], D Y\rangle \\
& =\alpha(H)\langle D X, Y\rangle+\langle X, D Y\rangle \\
& =0,
\end{aligned}
$$

since $D$ is skew-symmetric. This equality now holds for all $X, Y \in \mathfrak{g}_{1}$ by linearity and (4.1), and so the range of $\tilde{D}$ is contained in $\mathfrak{m}$.

We now extend $D$ and $\tilde{D}$ to a linear map $E$ on $\mathfrak{g}_{0}+\mathfrak{n}$ by setting $E(W+X)=\tilde{D} W+D X$ for all $W \in \mathfrak{g}_{0}$ and all $X \in \mathfrak{n}$. Since $D$ is a derivation on $\mathfrak{n}$, to show that $E$ is a derivation it suffices to show that

$$
\begin{equation*}
D[W, X]=[\tilde{D} W, X]+[W, D X] \quad \forall W \in \mathfrak{g}_{0} \quad \forall X \in \mathfrak{n} . \tag{4.2}
\end{equation*}
$$

and

$$
\begin{equation*}
\tilde{D}[W, U]=[\tilde{D} W, U]+[W, \tilde{D} U] \quad \forall W, U \in \mathfrak{g}_{0} \tag{4.3}
\end{equation*}
$$

To prove (4.2), observe that

$$
D[W, X]-[\tilde{D} W, X]-[W, D X]=([D, \operatorname{ad}(W)]-\operatorname{ad}(\tilde{D} W)) X,
$$

and $[D, \operatorname{ad}(W)]-\operatorname{ad}(\tilde{D} W)$ is a derivation. To show that it is 0 on $\mathfrak{n}$, it suffices to show that it vanishes on $\mathfrak{g}_{\beta}$ for all simple roots $\beta$. By linearity, it suffices to take $W$ of the form $[X, \theta Y$ ] where $X, Y \in \mathfrak{g}_{\alpha}$ and $\alpha \in \Delta$; this case follows from $\left(E_{\alpha, \beta}\right)$.

To prove (4.3), we may suppose by linearity that $U=[X, \theta Y]$ where $X, Y \in \mathfrak{g}_{\alpha}$ for some $\alpha \in \Delta$. Now $\theta \tilde{D} \theta=\tilde{D}$, so

$$
\begin{aligned}
\tilde{D}[W,[X, \theta Y]]= & \tilde{D}[[W, X], \theta Y]+\tilde{D}[X,[W, \theta Y]] \\
= & \tilde{D}[[W, X], \theta Y]+\tilde{D}[X, \theta[\theta W, Y]] \\
= & {[D[W, X], \theta Y]+[[W, X], \theta D Y] } \\
& +[D X,[W, \theta Y]]+[X, \theta D[\theta W, Y]] \\
= & {[[\tilde{D} W, X], \theta Y]+[[W, D X], \theta Y]+[[W, X], \theta D Y] } \\
& +[D X,[W, \theta Y]]+[X, \theta[\tilde{D} \theta W, Y]]+[X, \theta[\theta W, D Y]] \\
= & {[[\tilde{D} W, X], \theta Y]+[[W, D X], \theta Y]+[[W, X], \theta D Y] } \\
& +[D X,[W, \theta Y]]+[X,[\tilde{D} W, \theta Y]]+[X,[W, \theta D Y]] \\
= & {[\tilde{D} W,[X, \theta Y]]+[W,[D X, \theta Y]]+[W,[X, \theta D Y]] } \\
= & {[\tilde{D} W,[X, \theta Y]]+[W, \tilde{D}[X, \theta Y]] }
\end{aligned}
$$

and (4.3) holds.
Finally, we prove (iv), using induction on $h$ and $k$. We need to prove the identity ( $D_{h, k}$ ), given by

$$
E[X, \theta Y]=[E X, \theta Y]+[X, \theta E Y] \quad \forall X \in \mathfrak{g}_{h} \quad \forall Y \in \mathfrak{g}_{k} .
$$

First we suppose that $k=1$. The identity $\left(D_{h, 1}\right)$ is equivalent to

$$
[E[X, \theta Y], Z]=[[E X, \theta Y], Z]+[[X, \theta E Y], Z]
$$

for all $X \in \mathfrak{g}_{h}$, all $Y \in \mathfrak{g}_{1}$ and all $Z \in \mathfrak{g}_{1}$, by Proposition 4.2. Write $W$ for $[X, Z]$ in $\mathfrak{g}_{h+1}$. Since $E$ is a derivation, from the Jacobi identity and the definition of $E$

$$
\begin{aligned}
{[ } & E \\
\quad= & E[[[X, \theta Y], Z]-[[E X, \theta Y], Z]-[[X, \theta E Y], Z] \\
= & E[[X, Z], \theta Y]+E[X,[\theta Y, Z]]-[[X, \theta Y], E Z]-[[E X, \theta Y], Z]-[[X, \theta E Y], Z] \\
= & E[[X, Z], \theta Y]+[E X,[\theta Y, Z]]+[X,[\theta E Y, Z]]+[X,[\theta Y, E Z]] \\
& \quad-[[X, \theta Y], E Z]-[[E X, \theta Y], Z]-[[X, \theta E Y], Z] \\
= & E[[X, Z], \theta Y]+[\theta Y,[E X, Z]]+[\theta E Y,[X, Z]]+[\theta Y,[X, E Z]] \\
= & E[W, \theta Y]-[E W, \theta Y]-[W, \theta E Y] .
\end{aligned}
$$

We deduce that if ( $D_{h+1,1}$ ) holds, the last line vanishes; hence the first line vanishes, and ( $D_{h, 1}$ ) holds. Since ( $D_{h, 1}$ ) holds for large positive $h$ (because there is nothing to prove as $\left.\mathfrak{g}_{h}=\{0\}\right),\left(D_{h, 1}\right)$ holds for all positive $h$.

Now suppose that ( $D_{h, 1}$ ) and ( $D_{h, k}$ ) hold where $1 \leq k<h$. Take $X \in \mathfrak{g}_{h}, Y_{1} \in \mathfrak{g}_{1}$ and $Y_{2} \in \mathfrak{g}_{k}$. Then

$$
\begin{aligned}
E & {\left[X, \theta\left[Y_{1}, Y_{2}\right]\right]-\left[E X, \theta\left[Y_{1}, Y_{2}\right]\right]-\left[X, \theta E\left[Y_{1}, Y_{2}\right]\right] } \\
= & E\left[\left[X, \theta Y_{1}\right], \theta Y_{2}\right]+E\left[\theta Y_{1},\left[X, \theta Y_{2}\right]\right]-\left[\left[E X, \theta Y_{1}\right], \theta Y_{2}\right]-\left[\theta Y_{1},\left[E X, \theta Y_{2}\right]\right] \\
& -\left[X,\left[\theta E Y_{1}, \theta Y_{2}\right]\right]-\left[X,\left[\theta Y_{1}, \theta E Y_{2}\right]\right] \\
= & {\left[E\left[X, \theta Y_{1}\right], \theta Y_{2}\right]+\left[\left[X, \theta Y_{1}\right], \theta E Y_{2}\right]+\left[\theta E Y_{1},\left[X, \theta Y_{2}\right]\right]+\left[\theta Y_{1}, E\left[X, \theta E Y_{2}\right]\right] } \\
& -\left[\left[E X, \theta Y_{1}\right], \theta Y_{2}\right]-\left[\theta Y_{1},\left[E X, \theta Y_{2}\right]\right]-\left[X,\left[\theta E Y_{1}, \theta Y_{2}\right]\right]-\left[X,\left[\theta Y_{1}, \theta E Y_{2}\right]\right] \\
= & {\left[\left[E X, \theta Y_{1}\right], \theta Y_{2}\right]+\left[\left[X, E \theta Y_{1}\right], \theta Y_{2}\right]+\left[\left[X, \theta Y_{1}\right], \theta E Y_{2}\right]+\left[\theta E Y_{1},\left[X, \theta Y_{2}\right]\right] } \\
& +\left[\theta Y_{1},\left[E X, \theta Y_{2}\right]\right]+\left[\theta Y_{1},\left[X, \theta E Y_{2}\right]\right]-\left[\left[E X, \theta Y_{1}\right], \theta Y_{2}\right]-\left[\theta Y_{1},\left[E X, \theta Y_{2}\right]\right] \\
& -\left[X,\left[\theta E Y_{1}, \theta Y_{2}\right]\right]-\left[X,\left[\theta Y_{1}, E \theta Y_{2}\right]\right] \\
= & {\left[\left[X, E \theta Y_{1}\right], \theta Y_{2}\right]+\left[\left[X, \theta Y_{1}\right], \theta E Y_{2}\right]+\left[\theta E Y_{1},\left[X, \theta Y_{2}\right]\right]+\left[\theta Y_{1},\left[X, \theta E Y_{2}\right]\right] } \\
& -\left[X,\left[\theta E Y_{1}, \theta Y_{2}\right]\right]-\left[X,\left[\theta Y_{1}, E Y_{2}\right]\right] \\
= & 0 .
\end{aligned}
$$

By Proposition 4.2, ( $D_{h, k+1}$ ) also holds. By induction, ( $D_{h, k}$ ) holds whenever $h \geq k \geq 0$.
Theorem 4.5 Suppose that $D$ is a skew-symmetric height-preserving derivation of $\mathfrak{n}$. Then the following are equivalent:
(i) there exists a height-preserving derivation $\tilde{D}$ of $\mathfrak{g}$ whose restriction to $\mathfrak{n}$ coincides with $D$;
(ii) $D=\operatorname{ad}(W)$ for some $W \in \mathfrak{m}$;
(iii) $\left(E_{\gamma, \delta}\right)$ holds for all $\gamma, \delta \in \Sigma^{+}$.
(iv) $\left(E_{\gamma, \delta}\right)$ holds for all $\gamma, \delta \in \Delta$.

Further, if any of these conditions hold, then $\tilde{D}$ is root space preserving.
Proof Suppose that (i) holds. Since all derivations of $\mathfrak{g}$ are inner, $\tilde{D}=\operatorname{ad}(W)$ for some $W \in \mathfrak{g}$. Evidently ad $(W)$ preserves height if and only if $W \in \mathfrak{g}_{0}$. Thus $W \in \mathfrak{m} \oplus \mathfrak{a}$. Since $D$ is skew-symmetric, $W \in \mathfrak{m}$, and (ii) is proved.

If (ii) holds, then the Jacobi identity and the fact that $\theta W=W$ imply that

$$
\begin{aligned}
D & {[[X, \theta Y], Z] } \\
& =\operatorname{ad}(W)[[X, \theta Y], Z] \\
& =[[\operatorname{ad}(W) X, \theta Y], Z]+[[X \operatorname{ad}(W) \theta Y], Z]+[[X, \theta Y], \operatorname{ad}(W) Z] \\
& =[[\operatorname{ad}(W) X, \theta Y], Z]+[[X, \theta \operatorname{ad}(W) Y], Z]+[[X, \theta Y], \operatorname{ad}(W) Z] \\
& =[[D X, \theta Y], Z]+[[X, \theta D Y], Z]+[[X, \theta Y], D Z],
\end{aligned}
$$

and (iii) holds.
It is trivial that (iii) implies (iv).
Suppose that (iv) holds. We are going to construct a derivation $\tilde{E}$ that extends the derivation $E$ of Theorem 4.4 to the simple Lie algebra $\mathfrak{g}$ and preserves heights.

When $X \in \mathfrak{g}_{0} \oplus \mathfrak{n}$, we set $\tilde{E} X=E X$. When $X \in \mathfrak{g}_{0} \oplus \theta \mathfrak{n}$, we define

$$
\begin{equation*}
\tilde{E} X=\theta E(\theta X) \tag{4.4}
\end{equation*}
$$

These definitions agree when $X \in \mathfrak{g}_{0}$ by part (ii) of Theorem 4.4. It follows from the definition that

$$
\begin{equation*}
\theta \tilde{E} \theta=\tilde{E} \tag{4.5}
\end{equation*}
$$

Finally, to show that $\tilde{D}$ is a derivation, we have to verify that

$$
\tilde{D}[U, V]=[\tilde{D} U, V]+[U, \tilde{D} V] \quad \forall U, V \in \mathfrak{g} .
$$

By linearity, it suffices to demonstrate this for $U \in \mathfrak{g}_{h}$ and $V \in \mathfrak{g}_{k}$, for all possible heights $h$ and $k$. There are various cases to consider. We label the relevant identity $\left(D_{h, k}\right)$ :

$$
\tilde{D}[U, V]=[\tilde{D} U, V]+[U, \tilde{D} V] \quad \forall U \in \mathfrak{g}_{h} \quad \forall V \in \mathfrak{g}_{k} .
$$

Case 1: $h \geq 0$ and $k \geq 0$. This case is trivial as $\tilde{E}$ coincides with $E$ on $\mathfrak{g}_{0} \oplus \mathfrak{n}$.
Case 2: $h \leq 0$ and $k \leq 0$. In this case, we take $X, Y \in \mathfrak{g}_{0} \oplus \theta \mathfrak{n}$, so $\theta X, \theta Y \in \mathfrak{g}_{0} \oplus \mathfrak{n}$, and then

$$
\begin{aligned}
\tilde{E}[X, Y] & =\theta E[\theta X, \theta Y]=\theta[E \theta X, \theta Y]+\theta[\theta X, E \theta Y] \\
& =[\tilde{E} X, Y]+[X, \tilde{E} Y],
\end{aligned}
$$

and ( $D_{h, k}$ ) holds.
Case 3: $h k<0$. We need to show that

$$
\tilde{E}[X, Y]=[\tilde{E} X, Y]+[X, \tilde{E} Y] \quad \forall X \in \mathfrak{g}_{h} \quad \forall Y \in \mathfrak{g}_{k} . \quad\left(D_{h, k}\right)
$$

If $h+k \geq 0$, this follows from part (iv) of Theorem 4.4 and (4.5); otherwise, we conjugate by $\theta$, as in Case 2 .

We conclude with the observation that if $\tilde{E}=\operatorname{ad}(Z)$ for some $Z \in \mathfrak{m}$, then $\tilde{E}$ is root space preserving.

## 5 Derivations of $\mathfrak{n}$

We are now able to consider a nilpotent Lie algebra $\mathfrak{n}$ that arises in the Iwasawa decomposition of a real simple Lie algebra $\mathfrak{g}$. We write $\mathcal{D}(\mathfrak{n})$ for the space of root-space-preserving derivations of $\mathfrak{n}$.

Theorem 5.1 If $\mathfrak{g}$ is simple and not isomorphic to $\mathfrak{s o}(n, 1)$ or $\mathfrak{s u}(n, 1)$, then every $D$ in $\mathcal{D}(\mathfrak{n})$ is given by

$$
D=\operatorname{ad}(W),
$$

where $W \in \mathfrak{m} \oplus \mathfrak{a}$.
The main theorem follows from this and Proposition 3.1.
We prove Theorem 5.1 by showing that every derivation is the sum of a symmetric and a skew-symmetric derivation, and treating these separately. The symmetric derivations are handled using the following lemma, which reduces matters to showing that symmetric derivations act by scalars on the root spaces.

Lemma 5.2 If a derivation $D$ of $\mathfrak{n}$ acts by a real scalar $\lambda_{\alpha}$ on each root space $\mathfrak{g}_{\alpha}$ where $\alpha \in \Delta$, then $D=\operatorname{ad}(H)$ for some $H \in \mathfrak{a}$.

Proof Since $D$ is a derivation, it is determined by the $\lambda_{\alpha}$ where $\alpha$ is simple; further, the simple roots form a basis of $\operatorname{Hom}(\mathfrak{a}, \mathbb{R})$ and so there exists $H \in \mathfrak{a}$ such that $\alpha(H)=\lambda_{\alpha}$ for each simple root. Hence $D=\operatorname{ad}(H)$.

Remark 5.3 A similar observation is valid when $\mathfrak{g}$ is complex and $D$ acts by a complex scalar on each root space, since every derivation of a complex Lie algebra is complex linear. Hence Theorem 5.1 is trivial when $\mathfrak{g}$ is a split or complex Lie algebra. In fact, in the split case (that is, when all the roots have multiplicity 1 ) it follows that $\mathcal{D}(\mathfrak{n})=\operatorname{ad}(\mathfrak{a})$. In particular, Theorem 5.1 holds for the algebras with root system $D_{n}$ (where $n \geq 4$ ), $E_{6}, E_{7}, E_{8}$ or $G_{2}$, since these are either split or complex, by the classification.

The skew-symmetric derivations are treated using Theorem 4.5, which shows that a skewsymmetric derivation $D$ lies in $\operatorname{ad}(\mathfrak{m})$ when the identity ( $E_{\alpha, \beta}$ ) holds for all simple roots $\alpha$ and $\beta$. For convenience, we recall this identity:

$$
D[[X, \theta Y], V]=[[D X, \theta Y], V]+[[X, \theta D Y], V]+[[X, \theta Y], D V]
$$

for all $X, Y \in \mathfrak{g}_{\alpha}$ and all $V \in \mathfrak{g}_{\beta}$.
Another key ingredient of our proof, which we use in parallel with the previous observation, is a reduction to Lie algebras of rank at most two. Recall that if E is a subset of $\Sigma$, then $\mathfrak{g}^{\mathrm{E}}$ denotes the subalgebra of $\mathfrak{g}$ generated by all the spaces $\mathfrak{g}_{\epsilon}$, where $\epsilon \in \mathrm{E}$. We also denote by $\mathfrak{m}^{\mathrm{E}}$ and $\mathfrak{n}^{\mathrm{E}}$ the algebras $\mathfrak{m} \cap \mathfrak{g}^{\mathrm{E}}$ and $\mathfrak{n} \cap \mathfrak{g}^{\mathrm{E}}$, and by $\Sigma^{\mathrm{E}}$ the root subsystem $\Sigma \cap \operatorname{span}(\mathrm{E})$.

Now we come to the proof proper. We first consider the rank-one case; this is known, and we just state what we need. Next, we consider the real rank-two case, and the third step is to consider the case where the real rank is higher than two.

### 5.1 The rank-one algebras

The algebras are well known (see, for instance, Weyl [23]) and the root-space-preserving derivations are well known. We summarise the results in the following proposition for the
convenience of the reader. As the simple algebras for which $\mathcal{D}(\mathfrak{n}) \neq \operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$ are rank one, a case-by-case analysis is appropriate.

Proposition 5.4 (Riehm [20], Saal [21]) Let $\mathfrak{g}$ be a simple Lie algebra of real rank one. Then $\mathcal{D}(\mathfrak{n})=\mathcal{D}^{\text {sym }}(\mathfrak{n}) \oplus \mathcal{D}^{\text {skew }}(\mathfrak{n})$. Moreover,
(i) if $\mathfrak{g}=\mathfrak{s o}(1, n+1)$, then $\mathcal{D}(\mathfrak{n})=\mathfrak{s l}(n, \mathbb{R}) \oplus \mathbb{R}$;
(ii) if $\mathfrak{g}=\mathfrak{s u}(1, n+1)$, then $\mathcal{D}(\mathfrak{n})=\mathfrak{s p}(n, \mathbb{R}) \oplus \mathbb{R}$;
(iii) if $\mathfrak{g}=\mathfrak{s p}(1, n+1)$, then $\mathcal{D}(\mathfrak{n})=\mathfrak{s p}(n-1) \oplus \mathfrak{s p}(1) \oplus \mathbb{R}$;
(iv) if $\mathfrak{g}=\mathfrak{f}(4,-20)$, then $\mathcal{D}(\mathfrak{n})=\mathfrak{s o}(7) \oplus \mathbb{R}$.

In all cases, the summand $\mathbb{R}$ corresponds to $\operatorname{ad}(\mathfrak{a})$. In the first two cases, $\mathcal{D}^{\text {sym }}(\mathfrak{n})$ strictly contains $\operatorname{ad}(\mathfrak{a})$; in the last two cases, $\mathcal{D}^{\text {sym }}(\mathfrak{n})$ coincides with $\operatorname{ad}(\mathfrak{a})$. In all cases, $\mathcal{D}^{\text {skew }}(\mathfrak{n})$ coincides with $\operatorname{ad}(\mathfrak{m})$.

Remark 5.5 In the first two cases, $\mathfrak{n}$ is not rigid enough to prevent the occurrence of derivations that are not in $\operatorname{ad}(\mathfrak{m} \oplus \mathfrak{a})$.

Proof This follows from the work of Riehm [20] and Saal [21]; see also Folland [12] and Pansu [19]. Alternatively, the reader may combine the results about $H$-type algebras with the description of the rank-one simple Lie algebras in terms of $H$-type algebras by Cowling et al. [10].

Corollary 5.6 Suppose that $\mathfrak{g}$ is a simple Lie algebra of arbitrary rank, and D is a skewsymmetric root-space-preserving derivation of $\mathfrak{n}$. Then the identity ( $E_{\alpha, \alpha}$ ) holds for all positive roots $\alpha$.

Proof For all roots $\alpha$, the restriction $\left.D\right|_{\mathfrak{n}^{(\alpha)}}$ is a skew-symmetric root-space-preserving derivation, and from Theorem 5.1 we deduce that $\left.D\right|_{\mathfrak{n}^{\{\alpha\}}} \in \operatorname{ad}\left(\mathfrak{m}^{\{\alpha\}}\right)$. Then $\left(E_{\alpha, \alpha}\right)$ holds by Theorem 4.5.

### 5.2 The rank-two algebras

Let $\mathfrak{g}$ be a simple Lie algebra of rank two and denote by $\mathfrak{n}$ an Iwasawa subalgebra of $\mathfrak{g}$. We shall prove that each root-space-preserving derivation of $\mathfrak{n}$ is the sum of a symmetric and a skew-symmetric derivation, that the symmetric derivation lies in $\operatorname{ad}(\mathfrak{a})$, and that the skew-symmetric part satisfies ( $E_{\alpha, \beta}$ ) for all $\alpha$ and $\beta$ in $\Sigma^{+}$.

Before we analyse the various cases, we need a general result about derivations which we will use when the root system is of type $B_{2}$ or $B C_{2}$.

Lemma 5.7 Suppose that $\alpha, \beta$ and $\alpha+\beta$ are positive roots while $\alpha-\beta$ and $\alpha+2 \beta$ are not roots, and that $D \in \mathcal{D}(\mathfrak{n})$. Then

$$
\begin{equation*}
D^{\top}[U, X]=\left[D^{\top} U, X\right]+\left[U, D^{\top} X\right] \quad \forall U \in \mathfrak{g}_{\beta} \quad \forall X \in \mathfrak{g}_{\alpha} . \tag{5.1}
\end{equation*}
$$

Proof By Proposition 5.4, the skew-symmetric part of the restriction of $D$ to $\mathfrak{g}_{\beta}$ coincides with $\operatorname{ad}(Z)$ for some $Z$ in $\mathfrak{m}^{\beta}$. Write $D_{0}$ for $D-\operatorname{ad}(Z)$. Since $\operatorname{ad}(Z)$ is a skew-symmetric derivation, $D$ satisfies (5.1) if and only if $D_{0}$ does. Thus, by replacing $D$ by $D_{0}$ if necessary, there is no loss of generality in assuming that the restriction of $D$ to $\mathfrak{g}_{\beta}$ is symmetric.

We need to show (5.1). The eigenvectors of $\left.D\right|_{\mathfrak{g}_{\beta}}$ span $\mathfrak{g}_{\beta}$, and so by linearity it will suffice to show (5.1) when $U$ is an eigenvector of $D$ and $X$ is arbitrary. Take $U$ in $\mathfrak{g}_{\beta} \backslash\{0\}$ and $\lambda \in \mathbb{R}$
such that $D U=\lambda U$. By Lemma 3.9, $\operatorname{ad}(U): \mathfrak{g}_{\alpha} \rightarrow \mathfrak{g}_{\alpha+\beta}$ is surjective, and so it will suffice to show that

$$
\left\langle D^{\top}[U, X],[U, Y]\right\rangle=\left\langle\left[D^{\top} U, X\right],[U, Y]\right\rangle+\left\langle\left[U, D^{\top} X\right],[U, Y]\right\rangle
$$

for the eigenvector $U$ in $\mathfrak{g}_{\beta}$ and arbitrary $X$ and $Y$ in $\mathfrak{g}_{\alpha}$. Now, by the hypothesis that $D$ is a root-space-preserving derivation, the choice of $U$, (3.2), the Jacobi identy, and the fact that $\alpha-\beta$ is not a root, the left hand side is equal to

$$
\begin{aligned}
\langle[U, X], D[U, Y]\rangle & =\langle[U, X],[D U, Y]\rangle+\langle[U, X],[U, D Y]\rangle \\
& =\langle[U, X],[\lambda U, Y]\rangle-\langle X,[\theta U,[U, D Y]]\rangle \\
& =\langle[\lambda U, X],[U, Y]\rangle-\langle X,[[\theta U, U], D Y]\rangle-\langle X,[U,[\theta U, D Y]]\rangle \\
& =\langle[\lambda U, X],[U, Y]\rangle-\langle X, \alpha([\theta U, U]) D Y\rangle \\
& =\left\langle\left[D^{\top} U, X\right],[U, Y]\right\rangle-\alpha([\theta U, U])\left\langle D^{\top} X, Y\right\rangle
\end{aligned}
$$

and similarly $\left\langle\left[U, D^{\top} X\right],[U, Y]\right\rangle$ is equal to

$$
\begin{aligned}
-\left\langle D^{\top} X,[\theta U,[U, Y]]\right\rangle & =-\left\langle D^{\top} X,[[\theta U, U], Y]\right\rangle-\left\langle D^{\top} X,[U,[\theta U, Y]]\right\rangle \\
& =-\left\langle D^{\top} X, \alpha([\theta U, U]) Y\right\rangle \\
& =-\alpha([\theta U, U])\left\langle D^{\top} X, Y\right\rangle
\end{aligned}
$$

The result now follows.

### 5.2.1 The case $A_{2}$

Until further notice, we assume that $\mathfrak{g}$ has root system $A_{2}$, the simplest indecomposible root system of rank 2 . We label the simple roots $\alpha$ and $\beta$, so that the highest root is $\alpha+\beta$ and $\Sigma^{+}=\{\alpha, \beta, \alpha+\beta\}$. With the notation of Lemma 3.8, $\Sigma_{1}=\{\alpha, \beta\}$ and $\Sigma_{0}=\varnothing$. We shall use the result of Ciatti [6, Proposition 4.1] about the structure of $\mathfrak{n}$, giving a proof for the convenience of the reader. We first recall that $\mathfrak{n}$ is an $H$-type algebra, and for $Z \in \mathfrak{g}_{\alpha+\beta}$, the map $J_{Z}$ on $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\beta}$ is determined by the condition that

$$
\left\langle J_{Z} X, Y\right\rangle=\langle Z,[X, Y]\rangle \quad \forall X, Y \in \mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\beta} .
$$

Lemma 5.8 For every nontrivial $X$ in $\mathfrak{g}_{\alpha}$,

$$
\begin{equation*}
\mathfrak{g}_{\beta}=\left\{J_{Z} X: Z \in \mathfrak{g}_{\alpha+\beta}\right\} \tag{5.2}
\end{equation*}
$$

and

$$
\begin{equation*}
\mathfrak{g}_{\alpha}=\left\{J_{Z^{\prime}} J_{Z} X: Z, Z^{\prime} \in \mathfrak{g}_{\alpha+\beta}\right\} . \tag{5.3}
\end{equation*}
$$

Proof We may and shall assume that $X$ is a unit vector, and take $Y \in \mathfrak{g}_{\beta}$. By (3.12) and the Jacobi identity,

$$
J_{[Y, X]} X=[[Y, X], \theta X]=[[\theta X, X], Y]=\beta([\theta X, X]) Y=Y,
$$

which proves that $Y \in\left\{J_{Z} X: Z \in \mathfrak{g}_{\alpha+\beta}\right\}$.
Now, by (3.13), $J_{Z}$ is a linear isomorphism that exchanges $\mathfrak{g}_{\beta}$ and $\mathfrak{g}_{\alpha}$ for all nonzero $Z$ in $\mathfrak{g}_{\alpha+\beta}$, so (5.3) follows from (5.2).

Proposition 5.9 Every root-space-preserving derivation of $\mathfrak{n}$ is the sum of a symmetric and a skew-symmetric derivation.

Proof By Lemma 3.8, $\mathfrak{n}$ is $H$-type. The result follows from Corollary 2.5.
Proposition 5.10 Every symmetric root-space-preserving derivation D of $\mathfrak{n}$ lies in $\operatorname{ad}(\mathfrak{a})$.
Proof From Corollary 2.8, $D$ is the sum of a symmetric derivation $D_{0}$ that vanishes on $\mathfrak{g}_{\alpha+\beta}$ and $\operatorname{ad}(H)$ for some $H$ in $\mathfrak{a}$. Since $D_{0}$ is symmetric and preserves root spaces, we may take an eigenvector $X$ of $D_{0}$ in $\mathfrak{g}_{\alpha}$ with corresponding eigenvalue $\lambda$. By Proposition 2.1 and Lemma 5.8, $D_{0}$ anticommutes with the maps $J_{Z}$ and so acts as $-\lambda$ on $\mathfrak{g}_{\beta}$, and hence as $\lambda$ on $\mathfrak{g}_{\alpha}$. This implies that $D_{0}$ lies in $\operatorname{ad}(\mathfrak{a})$ by Lemma 5.2.

Proposition 5.11 The basic derivation identity ( $E_{\gamma, \delta}$ ) holds as $\gamma$ and $\delta$ range over the set $\{\alpha, \beta\}$ of simple roots. Consequently, every derivation $D$ in $\mathcal{D}^{\text {skew }}(\mathfrak{n})$ is equal to $\operatorname{ad}(Z)$ for some $Z$ in m .

Proof Recall the basic derivation identity ( $E_{\gamma, \delta}$ ), that is, the identity

$$
D[[X, \theta Y], Z]=[[D X, \theta Y, Z]+[[X, \theta D Y], Z]+[[X, \theta Y], D Z]
$$

for all $X, Y \in \mathfrak{g}_{\gamma}$ and all $Z \in \mathfrak{g}_{\delta}$. By Theorem 4.5, it suffices to prove ( $E_{\gamma, \delta}$ ) as $\gamma$ and $\delta$ range over $\{\alpha, \beta\}$. The identities ( $E_{\alpha, \alpha}$ ) and ( $E_{\beta, \beta}$ ) hold by Corollary 5.6.

Now we prove $\left(E_{\alpha, \beta}\right)$. Suppose that $X, Y \in \mathfrak{g}_{\alpha}$ and $Z \in \mathfrak{g}_{\beta}$. Since $\beta-\alpha$ is not a root,

$$
\begin{aligned}
D & {[[X, \theta Y], Z]-[[D X, \theta Y], Z]-[[X, \theta D Y], Z]-[[X, \theta Y], D Z] } \\
& =D[[X, Z], \theta Y]-[[D X, Z], \theta Y]-[[X, Z], \theta D Y]-[[X, D Z], \theta Y] \\
& =D[[X, Z], \theta Y]-[D[X, Z], \theta Y]-[[X, Z], \theta D Y] \\
& =D[W, \theta Y]-[D W, \theta Y]-[W, \theta D Y]
\end{aligned}
$$

where $W=[X, Z] \in \mathfrak{g}_{\alpha+\beta}$; it will suffice to prove that this is 0 for all $W \in \mathfrak{g}_{\alpha+\beta}$ and all $Y \in \mathfrak{g}_{\alpha}$. By the definition of $J_{W}$, for $W \in \mathfrak{g}_{\alpha+\beta}$, we may rewrite the last expression as

$$
D J_{W} Y-J_{D W} Y-J_{W} D Y
$$

and since $D$ is a skew-symmetric derivation, this is 0 by (2.4).
We exchange the roles of $\alpha$ and $\beta$ to prove the remaining identity.

### 5.2.2 The case $B_{2}$

Until further notice, we assume that $\mathfrak{g}$ has root system $B_{2}$. We denote by $\alpha$ and $\beta$ the simple roots, with $\beta$ longer than $\alpha$. Hence $\omega=2 \alpha+\beta$ and $\Sigma^{+}=\{\alpha, \beta, \alpha+\beta, 2 \alpha+\beta\}$.

The first proposition is the basic result: it establishes that every element of $\mathcal{D}(\mathfrak{n})$ is a sum of a symmetric and a skew-symmetric derivation.

Proposition 5.12 If $D$ is in $\mathcal{D}(\mathfrak{n})$, then its transpose $D^{\top}$ is also in $\mathcal{D}(\mathfrak{n})$.
Proof By Lemma 3.8, the algebra $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta}$ is $H$-type. By Corollary 2.5, the restriction of $D^{\top}$ to this $H$-type algebra is a derivation. Hence it suffices to show that

$$
D^{\top}[U, X]=\left[D^{\top} U, X\right]+\left[U, D^{\top} X\right]
$$

for all $X$ in $\mathfrak{g}_{\alpha}$ and all $U$ in $\mathfrak{g}_{\beta}$. The proposition now follows from Lemma 5.7.

Now we describe the symmetric derivations.
Proposition 5.13 Every derivation $D$ in $\mathcal{D}^{\text {sym }}(\mathfrak{n})$ is equal to $\operatorname{ad}(H)$ for some $H$ in $\mathfrak{a}$.
Proof By Lemma 3.5, $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta}$ is an $H$-type algebra. In light of Corollary 2.8, we may assume that $D$ vanishes on $\mathfrak{g}_{2 \alpha+\beta}$, by subtracting $\operatorname{ad}(H)$ for a suitable $H$ in $\mathfrak{a}$.

The derivation $D$, being symmetric, may be diagonalised with real eigenvalues. We fix eigenvectors $U$ in $\mathfrak{g}_{\beta}$ with eigenvalue $\lambda$ and $X$ in $\mathfrak{g}_{\alpha}$ with eigenvalue $\mu$. Since $D$ is a derivation,

$$
D[[U, X], X]=(\lambda+2 \mu)[[U, X], X] .
$$

Now $\alpha$ and $\beta$ satisfy the hypotheses of Lemma 3.10, and so $[[U, X], X]$ is nonzero. Since $D$ vanishes on $\mathfrak{g}_{2 \alpha+\beta}$,

$$
\lambda+2 \mu=0 .
$$

We vary the eigenvector $U$, holding $X$ fixed: This shows that $\lambda$ is independent of $X$. Similarly, $\mu$ is independent of $U$. By Lemma 5.2, this implies the proposition.

Proposition 5.14 The basic derivation identity ( $E_{\gamma, \delta}$ ) holds as $\gamma$ and $\delta$ range over the set $\{\alpha, \beta\}$ of simple roots. Consequently, every derivation $D$ in $\mathcal{D}^{\text {skew }}(\mathfrak{n})$ is equal to $\operatorname{ad}(Z)$ for some $Z$ in m .

Proof Recall the basic derivation identity ( $E_{\gamma, \delta}$ ), that is, the identity

$$
D[[X, \theta Y], Z]=[[D X, \theta Y, Z]+[[X, \theta D Y], Z]+[[X, \theta Y], D Z]
$$

for all $X, Y \in \mathfrak{g}_{\gamma}$ and all $Z \in \mathfrak{g}_{\delta}$. Again by Theorem 4.5, we need to prove $\left(E_{\gamma, \delta}\right)$ as $\gamma$ and $\delta$ range over $\{\alpha, \beta\}$. The identities $\left(E_{\alpha, \alpha}\right)$ and ( $E_{\beta, \beta}$ ) hold by Corollary 5.6.

Now we prove $\left(E_{\beta, \alpha}\right)$. Suppose that $X, Y \in \mathfrak{g}_{\beta}$ and $Z \in \mathfrak{g}_{\alpha}$. Since $\beta-\alpha$ is not a root,

$$
\begin{aligned}
D & {[[X, \theta Y], Z]-[[D X, \theta Y], Z]-[[X, \theta D Y], Z]-[[X, \theta Y], D Z] } \\
& =D[[X, Z], \theta Y]-[[D X, Z], \theta Y]-[[X, Z], \theta D Y]-[[X, D Z], \theta Y] \\
& =D[[X, Z], \theta Y]-[D[X, Z], \theta Y]-[[X, Z], \theta D Y] \\
& =D[W, \theta Y]-[D W, \theta Y]-[W, \theta D Y],
\end{aligned}
$$

where $W=[X, Z] \in \mathfrak{g}_{\alpha+\beta}$; it will suffice to prove that this is 0 for all $W \in \mathfrak{g}_{\alpha+\beta}$ and all $Y \in \mathfrak{g}_{\beta}$. By Lemma 3.9, $\operatorname{ad}(Y)$ maps $\mathfrak{g}_{\alpha}$ onto $\mathfrak{g}_{\alpha+\beta}$, so it will suffice to prove that

$$
D[[U, Y], \theta Y]-[D[U, Y], \theta Y]-[[U, Y], \theta D Y]=0
$$

for all $U \in \mathfrak{g}_{\alpha}$ and all $Y \in \mathfrak{g}_{\beta}$. Since $\alpha-\beta$ is not a root, $[[R, S], \theta T]=[R,[S, \theta T]]$ for all $R \in \mathfrak{g}_{\alpha}$ and all $S, T \in \mathfrak{g}_{\beta}$, whence

$$
\begin{aligned}
D & {[[U, Y], \theta Y]-[D[U, Y], \theta Y]-[[U, Y], \theta D Y] } \\
& =D[[U, Y], \theta Y]-[[D U, Y], \theta Y]-[[U, D Y], \theta Y]-[[U, Y], \theta D Y] \\
& =D[U,[Y, \theta Y]]-[D U,[Y, \theta Y]]-[U,[D Y, \theta Y]]-[U,[Y, \theta D Y]] \\
& =\langle\alpha, \beta\rangle\|Y\|^{2} D U-\langle\alpha, \beta\rangle\|Y\|^{2} D U-[U,[D Y, \theta Y]]-[U,[Y, \theta D Y]] \\
& =[[D Y, \theta Y]+[Y, \theta D Y], U] .
\end{aligned}
$$

Now if $X \perp Y$, then $[X, \theta Y] \in \mathfrak{m}$ and hence

$$
[X, \theta Y]+[Y, \theta X]=\theta[X, \theta Y]+[Y, \theta X]=[\theta X, Y]+[Y, \theta X]=0 .
$$

Applying this with $X$ equal to $D Y$ finishes the proof of $\left(E_{\beta, \alpha}\right)$.

It remains to prove $\left(E_{\alpha, \beta}\right)$. Take $X, Y \in \mathfrak{g}_{\alpha}$ and $U, Z \in \mathfrak{g}_{\beta}$. Then

$$
\begin{aligned}
\langle D & {[[X, \theta Y], Z]-[[D X, \theta Y], Z]-[[X, \theta D Y], Z]-[[X, \theta Y], D Z], U\rangle } \\
= & -\langle[[X, \theta Y], Z], D U\rangle+\langle[D X, \theta Y],[U, \theta Z]\rangle \\
& +\langle[X, \theta D Y],[U, \theta Z]\rangle+\langle[X, \theta Y],[U, \theta D Z]\rangle \\
= & \langle[X, \theta Y],[D U, \theta Z]\rangle-\langle D X,[[U, \theta Z], Y]\rangle \\
& -\langle X,[[U, \theta Z], D Y]\rangle-\langle X,[[U, \theta D Z], Y]\rangle \\
= & -\langle X,[[D U, \theta Z], Y]\rangle+\langle X, D[[U, \theta Z], Y]\rangle \\
& -\langle X,[[U, \theta Z], D Y]\rangle-\langle X,[[U, \theta D Z], Y]\rangle \\
= & \langle X, D[[U, \theta Z], Y]-[[D U, \theta Z], Y]-[[U, \theta Z], D Y]-[[U, \theta D Z], Y]\rangle .
\end{aligned}
$$

This shows that ( $E_{\alpha, \beta}$ ) and ( $E_{\beta, \alpha}$ ) are equivalent, so we are done.
Note that we have not used the fact that $2 \alpha$ and $2(\alpha+\beta)$ are not roots, so this argument holds in the $B C_{2}$ case too.

This completes our discussion of the algebras with root system $B_{2}$. We remind the reader that $C_{2}$ is the same as $B_{2}$. The algebras with root system $G_{2}$ are covered by Remark 5.3. It remains to consider the algebras with root system $B C_{2}$.

### 5.2.3 The case $B C_{2}$

Until further notice, we assume that $\mathfrak{g}$ has root system $B C_{2}$. Denote by $\alpha$ and $\beta$ the simple roots, with $\alpha$ orthogonal to the highest root $\omega$. Then $\Sigma^{+}=\{\alpha, 2 \alpha, \beta, \alpha+\beta, 2 \alpha+\beta, 2 \alpha+2 \beta\}$ and $\omega=2 \alpha+2 \beta$.

Note that $\{ \pm 2 \alpha, \pm \beta, \pm(2 \alpha+\beta), \pm(2 \alpha+2 \beta)\}$ is a root subsystem of type $B_{2}$, write $\mathfrak{n}_{\text {sub }}$ for $\mathfrak{g}_{2 \alpha} \oplus \mathfrak{g}_{\beta} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+2 \beta}$. The results of the previous subsection apply to the root-space-preserving derivations of the subalgebra $\mathfrak{n}_{\text {sub }}$ to give us information about derivations of $\mathfrak{n}$.

The first step is to establish the analogue of Proposition 5.12.
Proposition 5.15 If $D$ is in $\mathcal{D}(\mathfrak{n})$, then its transpose $D^{\top}$ is also in $\mathcal{D}(\mathfrak{n})$.
Proof By linearity, it suffices to show that

$$
\begin{equation*}
D^{\top}[X, Y]=\left[D^{\top} X, Y\right]+\left[X, D^{\top} Y\right] \quad \forall X \in \mathfrak{g}_{\gamma} \quad \forall Y \in \mathfrak{g}_{\delta}, \tag{5.4}
\end{equation*}
$$

as $\gamma$ and $\delta$ range over $\Sigma^{+}$. As $D$ and hence also $D^{\top}$ preserve root spaces, this is trivial unless $\gamma+\delta$ is a root. Moreover, by Corollary 2.5, the restrictions of $D^{\top}$ to the $H$-type algebras $\mathfrak{g}_{\beta} \oplus \mathfrak{g}_{\alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+2 \beta}$ and $\mathfrak{g}_{\alpha} \oplus \mathfrak{g}_{2 \alpha}$ are derivations, and by Proposition 5.12, the restriction of $D^{\top}$ to $\mathfrak{g}_{\beta} \oplus \mathfrak{g}_{2 \alpha} \oplus \mathfrak{g}_{2 \alpha+\beta} \oplus \mathfrak{g}_{2 \alpha+2 \beta}$ is a derivation.

Thus it suffices to prove (5.4) when $(\gamma, \delta)$ is either $(\alpha, \beta)$ or $(\alpha, \alpha+\beta)$. Lemma 5.7 takes care of the case when $\gamma=\alpha$ and $\delta=\beta$.

Since $2(2 \alpha+\beta)$ is not a root, Proposition 5.4 implies that there exists $Z$ in $\mathfrak{m}^{2 \alpha+\beta}$ that agrees with the skew-symmetric part of $D$ on $\mathfrak{g}_{2 \alpha+\beta}$. By subtracting $\operatorname{ad}(Z)$ from $D$ if necessary, we may suppose that $D$ is symmetric on $\mathfrak{g}_{2 \alpha+\beta}$. Now Corollary 3.7 gives (5.4).

Once again, we consider the symmetric derivations.
Proposition 5.16 If the root system of $\mathfrak{g}$ is $B C_{2}$, then every derivation in $\mathcal{D}^{\text {sym }}(\mathfrak{n})$ is given by $\operatorname{ad}(H)$ for some $H$ in $\mathfrak{a}$.

Proof By Proposition 5.13, the restriction of $D$ to $\mathfrak{n}_{\text {sub }}$ is given by $\operatorname{ad}(H)$ for some $H$ in $\mathfrak{a}$. By subtracting $\operatorname{ad}(H)$ if necessary we may suppose that $D$ vanishes on $\mathfrak{n}_{\text {sub }}$; it will then suffice to show that $D$ is trivial.

To do this, we pick an eigenvector $X$ of $D$ in $\mathfrak{g}_{\alpha}$ with eigenvalue $\lambda$ and $U \in \mathfrak{g}_{\beta} \backslash\{0\}$. Since $D$ is a derivation and $D U=0$

$$
D[[U, X], X]=2 \lambda[[U, X], X] .
$$

However, $D[[U, X], X]=0$, since $[[U, X], X]$ lies in $\mathfrak{g}_{2 \alpha+\beta} \subset \mathfrak{n}_{\text {sub }}$. Since $[[U, X], X] \neq 0$ by Lemma 3.10, $\lambda=0$, and $D$ is trivial on $\mathfrak{g}_{\alpha}$. Since $D$ is also trivial on $\mathfrak{g}_{\beta}$, it is trivial on $\mathfrak{g}_{\alpha+\beta}$, and hence trivial on all the root spaces.

We conclude our discussion of the rank-two case with a description of the skew-symmetric derivations.

Proposition 5.17 The basic derivation identity ( $E_{\gamma, \delta}$ ) holds as $\gamma$ and $\delta$ range over the set $\{\alpha, \beta\}$ of simple roots. Consequently, every derivation $D$ in $\mathcal{D}^{\text {skew }}(\mathfrak{n})$ is equal to $\operatorname{ad}(Z)$ for some $Z$ in $\mathfrak{m}$.

Proof This follows from Proposition 5.14, which also holds in the root system $B C_{2}$, and Theorem 4.5.

### 5.3 The general case

Now we prove Theorem 5.1. Henceforth, $\mathfrak{g}$ denotes a real simple Lie algebra of rank at least 3 , and $\mathfrak{n}$ is an Iwasawa nilpotent subalgebra of $\mathfrak{g}$.

Proposition 5.18 Suppose that $D$ is a derivation of $\mathfrak{n}$. Then $D^{\top}$ is also a derivation of $\mathfrak{n}$.
Proof By linearity, this follows provided that

$$
D^{\top}[X, Y]=\left[D^{\top} X, Y\right]+\left[X, D^{\top} Y\right]
$$

for all $X \in \mathfrak{g}_{\gamma}$ and all $Y \in \mathfrak{g}_{\delta}$ where $\gamma$ and $\delta$ range over $\Sigma^{+}$. This is obvious if $\gamma+\delta$ is not a root, while if $\gamma+\delta$ is a root, then it follows by restricting $D$ to $\mathfrak{n}^{\{\gamma, \delta\}}$.

Proposition 5.19 Suppose that $D$ is a symmetric derivation of $\mathfrak{n}$. Then $D$ lies in $\operatorname{ad}(\mathfrak{a})$.
Proof Again, by restricting to rank-two subalgebras, we may show that $D$ acts as a scalar on each root space. By Lemma 5.2, $D \in \operatorname{ad}(\mathfrak{a})$.

Proposition 5.20 Suppose that D is a skew-symmetric derivation of $\mathfrak{n}$. Then $D$ lies in $\operatorname{ad}(\mathfrak{m})$.
Proof Let $D$ be a skew-symmetric root-space-preserving derivation of $\mathfrak{n}$. Again, by restricting to rank-two subalgebras, we may show that $D$ satisfies the basic derivation identity ( $E_{\gamma, \delta}$ ) whenever $\gamma$ and $\delta$ are positive roots. Hence $D \in \operatorname{ad}(\mathfrak{m})$ by Theorem 4.5.

## References

1. Bourbaki, N.: Groupes et algèbres de Lie. Chapitres 4, 5 , et 6 . Éléments de mathématiques XXXIV. Actualités scientifiques et industrielles 1337. Hermann, Paris (1968)
2. Chen, Z.: Generalized derivations on parabolic subalgebras of general linear Lie algebras. Acta Math. Sci. 36, 635-970 (2016)
3. Ciatti, P.: A Clifford algebra approach to simple Lie algebras of real rank two, I: the $A_{2}$ case. J. Lie Theory 10, 53-80 (2000)
4. Ciatti, P.: A Clifford algebra approach to simple Lie algebras of real rank two, II: the $G_{2}$ case. Ann. Mat. Pura Appl. 181, 1-23 (2002)
5. Ciatti, P.: A new proof of the $J^{2}$-condition for real rank one simple Lie algebras and their classification. Proc. Am. Math. Soc. 133, 1611-1616 (2004)
6. Ciatti, P.: A Clifford algebra approach to real simple Lie algebras: the algebras with reduced root system. Math. Z. 242, 781-797 (2002)
7. Ciatti, P.: A Clifford algebra approach to real simple Lie algebras, II: the algebras with root system $B C_{n}$. Math. Z. 244, 35-46 (2003)
8. Cowling, M., De Mari, F., Korányi, A., Riemann, H.M.: Contact and conformal maps in parabolic geometry. I. Geom. Dedic. 111, 65-86 (2005)
9. Cowling, M., Dooley, A., Korányi, A., Ricci, F.: H-type groups and Iwasawa decompositions. Adv. Math. 87, 1-4 (1997)
10. Cowling, M., Dooley, A., Korányi, A., Ricci, F.: An approach to symmetric spaces of rank one via groups of Heisenberg type. J. Geom. Anal. 8, 199-237 (1998)
11. Cowling, M.G., Ottazzi, A.: Structure of stratified groups I. Product decompositions. J. Lie Theory 27, 177-183 (2017)
12. Folland, G.B.: Harmonic Analysis in Phase Space. Annals of Mathematics Studies, vol. 122. Princeton University Press, Princeton (1989)
13. Helgason, S.: Differential Geometry, Lie Groups, and Symmetric Spaces. Academic Press, New York (1978)
14. Kaplan, A.: Fundamental solutions for a class of hypoelliptic PDE generated by compositions of quadratic forms. Trans. Am. Math. Soc. 258, 147-153 (1980)
15. Knapp, A.: Lie Groups. Beyond an Introduction. Birkhäuser, Boston (1996)
16. Korányi, A.: Geometric properties of Heisenberg type groups. Adv. Math. 56, 28-38 (1986)
17. Kostant, B.: On the existence and irreducibility of certain series of representations. Bull. Am. Math. Soc. 75, 627-642 (1969)
18. Ottazzi, A., Warhurst, B.: Contact and 1-quasiconformal maps on Carnot groups. J. Lie Theory 21, 787-811 (2011)
19. Pansu, P.: Métriques de Carnot-Carathéodory et quasiisométries des espaces symétriques de rang un. Ann. Math. 129, 1-60 (1989)
20. Riehm, C.: The automorphism group of a composition of quadratic forms. Trans. Am. Math. Soc. 269, 403-414 (1982)
21. Saal, L.: The automorphism group of a Lie algebra of Heisenberg type. Rend. Sem. Mat. Univ. Pol. Torino 54, 101-113 (1996)
22. Wang, D., Yu, Q.: Derivations of the parabolic subalgebras of the general linear Lie algebra over a commutative ring. Linear Algebra Appl. 418, 763-774 (2006)
23. Weyl, H.: The Theory of Groups and Quantum Mechanics. Methuen, London (1931)
24. Yamaguchi, K.: Differential systems associated with simple graded Lie algebras. In: Progress in Differential Geometry, pp. 413-494. Adv. Stud. Pure Math. 22. Math. Soc. Japan, Tokyo (1993)

[^0]:    Research supported by the Italian Ministero dell'Istruzione, dell'Università e della Ricerca through PRIN 2011-12 "Varietà reali e complesse: geometria, topologia e analisi armonica" and the GNAMPA project "Calcolo funzionale per operatori subellitici su varietà", and by the Australian Research Council through DP-140100531 "Generalised conformal mappings". The first-named author thanks the University of New South Wales and the second-named author thanks the Università di Padova for their hospitality. Both authors thank the referee for helpful and incisive comments.

    Paolo Ciatti
    paolo.ciatti@unipd.it
    Michael G. Cowling
    m.cowling@unsw.edu.au

    1 Università di Padova, Via Marzolo 9, 35121 Padova, Italy
    2 University of New South Wales, UNSW Sydney, Sydney 2052, Australia

