On the Centralizer of $K$ in $U(\mathfrak{g})$

BERTRAM KOSTANT*

Dedicated with respect to Ernest Vinberg

on the occasion of his seventieth birthday

Abstract. Let $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ be a complexified Cartan decomposition of a complex semisimple Lie algebra $\mathfrak{g}$ and let $K$ be the subgroup of the adjoint group of $\mathfrak{g}$ corresponding to $\mathfrak{k}$. If $H$ is an irreducible Harish-Chandra module of $U(\mathfrak{g})$, then $H$ is completely determined by the finite-dimensional action of the centralizer $U(\mathfrak{g})^K$ on any one fixed primary $\mathfrak{k}$ component in $H$. This original approach of Harish-Chandra to a determination of all $H$ has largely been abandoned because one knows very little about generators of $U(\mathfrak{g})^K$. Generators of $U(\mathfrak{g})^K$ may be given by generators of the symmetric algebra analogue $S(\mathfrak{g})^K$. Let $S_m(\mathfrak{g})^K$, $m \in \mathbb{Z}_+$, be the subalgebra of $S(\mathfrak{g})^K$ defined by $K$-invariant polynomials of degree at most $m$. For convenience write $A = S(\mathfrak{g})^K$ and $A_m$ for the subalgebra of $A$ generated by $S_m(\mathfrak{g})^K$. Let $Q$ and $Q_m$ be the respective quotient fields of $A$ and $A_m$. We prove that if $n = \dim \mathfrak{g}$ one has $Q = Q_{2n}$.

We also determine the variety, $\text{Nil}_K$, of unstable points with respect to the action $K$ on $\mathfrak{g}$ and show that $\text{Nil}_K$ is already defined by $A_{2n}$. As pointed out to us by Hanspeter Kraft this fact together with a result of Harm Derksen (See [D]) implies, indeed, that $A = A_r$ where $r = \binom{2n}{2} \dim \mathfrak{p}$.

1. Introduction

1.1. Let $\mathfrak{g}$ be a complex semisimple Lie algebra. The value taken by the Killing form, $B$, on $w, z \in \mathfrak{g}$ will be denoted by $(w, z)$. Let

$$\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$$ (1.1)

be a complexified Cartan decomposition and let $\theta$ be the corresponding complexified Cartan involution. One has that $[\mathfrak{p}, \mathfrak{p}]$ is an ideal of $\mathfrak{k}$ (and $\mathfrak{p} + [\mathfrak{p}, \mathfrak{p}]$ is an ideal of $\mathfrak{g}$). We will assume that (1.1) is proper in the sense that

$$\mathfrak{k} = [\mathfrak{p}, \mathfrak{p}]$$ (1.2)

* Research supported in part by the KG&G Foundation.
(i.e., (1.1) arises from the Cartan decomposition of a real form of $\mathfrak{g}$ without “compact components”). Let $G$ be the adjoint group of $\mathfrak{g} = \text{Lie}\, \mathfrak{g}$ and let $K \subset G$ be the subgroup corresponding to $\mathfrak{k}$. Of course $G$ has trivial center.

We recall that the centralizer $U(\mathfrak{g})^K$ of $K$ in the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$ played a key role in Harish-Chandra’s original approach to the study of certain infinite dimensional representations of $\mathfrak{g}$. A critical end product of the theory is the existence of irreducible Harish-Chandra modules. Such a module $M$ is an irreducible $U(\mathfrak{g})$-module which not only is completely reducible as a $\mathfrak{k}$-module but also the primary components are finite dimensional. Any such primary component then defines a finite-dimensional $U(\mathfrak{g})^K$-module and, remarkably, the entire $U(\mathfrak{g})$-module $M$ is completely determined by the action of $U(\mathfrak{g})^K$ on any one fixed primary component. An early consequence of all of this is Harish-Chandra’s subquotient theorem. (For a considerable simplification and clarification of Harish-Chandra’s proof see Lepowsky [L] and Lepowsky-McCollum [L-M]. See also Wallach [W] and Vogan [V-1]). With the the determination of Harish-Chandra modules reduced to a determination of the finite-dimensional representation theory of $U(\mathfrak{g})^K$ one might have expected a subsequent development of representation theory along these lines. However this has not been the case although a considerable effort in this direction is seen in [V-1]. The main result of [V-1] is a classification theorem. One major obstacle to making progress with this approach is that the algebra $U(\mathfrak{g})^K$ is poorly understood. This is more or less attested to by Vogan in [V-2] where he remarks that $U(\mathfrak{g})^K$ is “hideously complicated”. See p. 17 in [V-2]. Also see [K-T] for a glimpse into this complication.

It is not difficult to construct a linear basis of $U(\mathfrak{g})^K$. The difficulty lies with its ring structure. Progress would be made if we could pin down a set of (algebra) generators of $U(\mathfrak{g})^K$. Indeed focusing on the primary component, given by Vogan’s minimal $\mathfrak{k}$-type, the corresponding representation of $U(\mathfrak{g})^K$ is given by a one-dimensional character. Consequently the whole $U(\mathfrak{g})$-module $M$ is known as soon as one knows the scalar values assigned to these generators by the character.

The algebra $U(\mathfrak{g})^K$ has a natural filtration and PBW implies an algebra isomorphism

$$Gr\, U(\mathfrak{g})^K \cong S(\mathfrak{g})^K$$

where $S(\mathfrak{g})^K$ is the finitely generated integral domain of $\text{Ad}\, K$ invariants in the symmetric algebra $S(\mathfrak{g})$. A set of homogeneous generators of $S(\mathfrak{g})^K$ then yields a set of generators of $U(\mathfrak{g})^K$. The main results of this paper together with a result of Derksen in [D] yields generators of $S(\mathfrak{g})^K$. 

2
1.2. The adjoint action of \( k \in K \) on \( z \in g \) will be denoted by \( k \cdot z \). If \( z \in g \), then \( K \cdot z \) is Zariski closed if and only if it is closed in the usual Hausdorff topology. Let

\[
Cl g = \{ z \in g \mid K \cdot z \text{ is closed} \}
\]

For notational convenience we will put \( A = S(g)^K \). Also for notational convenience we identify \( S(g) \) with the algebra of polynomial functions on \( g \) where for any \( x, y \in g \) and \( m \in \mathbb{Z}_+ \), one has \( x^m(y) = (x, y)^m \). Then \( A \) is the affine algebra of the affine variety \( V \) of all homomorphisms \( A \to \mathbb{C} \), i.e., all closed points in \( \text{Spec} \, A \). Then, from invariant theory, one knows that

\[
V \cong Cl g / K
\]

i.e.,

\[
V \text{ identifies with the set of all closed } K \text{-orbits in } g. \tag{1.4}
\]

For any \( z \in Cl g \) we will let

\[
v_z \in V \text{ be the point corresponding to } K \cdot z. \tag{1.5}
\]

The symmetric algebra \( S(g) \) is filtered by the subspaces \( S_m(g) \), \( m \in \mathbb{Z}_+ \), where \( S_m(g) = \sum_{j=0}^{m} S^j(g) \). Obviously

\[
S_m(g)^K = \sum_{j=0}^{m} S^j(g)^K \tag{1.6}
\]

But then \( A \) is filtered by the subalgebras \( A_m \), \( m \in \mathbb{Z}_+ \), where we let

\[
A_m \text{ be the subalgebra of } A \text{ generated by } S_m(g)^K \tag{1.7}
\]

Let \( V_m \) be the affine variety corresponding to \( A_m \). The injection

\[
0 \to A_m \to A \tag{1.8}
\]

defines a dominant morphism

\[
\gamma_m : V \to V_m \tag{1.9}
\]

Let \( Q \) (resp.\( Q_m \)) be the quotient field of \( A \) (resp.\( A_m \)) and let

\[
n = \text{dim} \, g \tag{1.10}
\]
The first main result is

**Theorem 1.1.** The dominant morphism $\gamma_{2n}$ is birational so that

$$Q = Q_{2n}$$  \hfill (1.11)

In particular any $h \in A$ is of the form

$$h = \frac{f}{g}$$  \hfill (1.12)

where $f, g \in A_{2n}$ and of course $g \neq 0$.

**1.3.** Let $z \in g$ be arbitrary. Then $z$ can be uniquely written

$$z = x + y, \text{ where } x \in \mathfrak{k} \text{ and } y \in \mathfrak{p}$$  \hfill (1.13)

Let $g(z)$ be the Lie subalgebra of $g$ generated by $x$ and $y$. We will use this notation throughout the paper.

In constrast to the closed $K$-orbits in $g$, consider the cone of $K$-unstable points in $g$. Let

$$Nil_K = \{ z \in g \mid f(z) = 0, \forall \text{ homogeneous } f \in S(g)^K \text{ of positive degree} \}$$

Since $S(g)^G \subset S(g)^K$ obviously $Nil_K$ is a subvariety of the nilcone of $g$.

**Theorem 1.2.** Let $z \in g$. Then $z \in Nil_K$ if and only if $g(z)$ is a (nilpotent) Lie algebra of nilpotent elements.

For a number of results about the nilcones of the actions of $K$, or rather $K_{\theta}$, (defined in (2.32) below) on multiple copies of $\mathfrak{p}$ see [K-W]. Also see [P-3]. For the case we are considering here, Wallach raised the question for a determination of some value of $m \in \mathbb{Z}_+$ with the property that $Nil_K$ is given already by the homogeneous elements in $A_m$ of positive degree. The following result answers this question with the same value of $m$ appearing in Theorem 1.1, namely $m = 2n$.

**Theorem 1.3.** Let $z \in g$. Then $z \in Nil_K$ if and only if

$$f(z) = 0, \forall f \in A_{2n} \text{ of positive degree}.$$
The idea of using a degree which defines $\text{Nil}_K$ (in this case $2n$) to determine $r$ such that $A = A_r$, goes back to Popov. See [P-1] and [P-2]. Harm Derksen in [D] has sharply reduced Popov’s estimate of $r$. Thus combining Theorem 1.3 with the result in [D] one has

**Theorem 1.4** One has

$$A = A_r$$

where

$$r = \binom{2n}{2} \dim p$$

where, we recall $n = \dim g$.

I thank Hanspeter Kraft for informing me about Derksen’s result. Kraft formulated Theorem 1.4, seeing it as an immediate consequence of my Theorem 1.3 and Derksen’s result. I also thank Nolan Wallach for motivating me to think about finding an integer $m$ such that $A_m$ defines $\text{Nil}_K$ (see Theorem 1.3). I also thank him for many conversations about invariant theory.

2. The proof of Theorems 1.1, 1.2, 1.3 and 1.4

2.1. Let $\Phi = \Phi(X, Y)$ be the free Lie algebra, over $\mathbb{C}$ on two generators $X, Y$. The Lie algebra $\Phi$ is naturally graded over $\mathbb{Z}_+$ with homogeneous spaces $\Phi^j$. It is then clearly filtered by the subspaces $\Phi_m$, $m \in \mathbb{Z}_+$, where

$$\Phi_m = \sum_{j=0}^{m} \Phi^j$$

Clearly

$$\Phi_{m+1} = \Phi_m + [X, \Phi_m] + [Y, \Phi_m]$$

Using notation introduced in §1.3 one then has a Lie algebra epimorphism,

$$\xi_z : \Phi \to \mathfrak{g}(z), \text{ where } \xi_z(X) = x \text{ and } \xi_z(Y) = y$$
The Lie subalgebra $g(z)$ of $g$ is filtered by the subspaces $g_m(z)$ where we put $g_m(z) = \xi_z(\Phi_m)$. By (2.2) one has

$$g_{m+1}(z) = g_m(z) + [x, g_m(z)] + [y, g_m(z)]$$  \hspace{1cm} (2.4)

**Proposition 2.1.** For any $z \in g$ one has

$$g_{n-1}(z) = g(z)$$  \hspace{1cm} (2.5)

**Proof.** It follows immediately from (2.4) that $g(z) = g_m(z)$ in case

$$g_m(z) = g_{m+1}(z)$$  \hspace{1cm} (2.6)

Indeed (2.6) implies that $g_k(z) = g_m(z)$ for all $k \in \mathbb{Z}_+$ where $k \geq m$.

The statement of the proposition is obviously true if $dim g_1(z) \leq 1$. We can therefore assume $dim g_1(z) = 2$. We refer to the equality (2.6) as “stability at $m$”. If one does not have stability at $m$ then clearly

$$dim g_{m+1}(z) > m + 1$$  \hspace{1cm} (2.7)

But then nonstability at $n - 1$ yields the contradictory statement $dim g_n(z) > n = dim g$. Hence one necessarily has stability at $n - 1$. QED

**2.2.** If $z = x + y$ is the decomposition (1.13) for $z \in g$, then obviously $k \cdot z = k \cdot x + k \cdot y$ is the decomposition (1.13) for $k \cdot z$ for any $k \in K$. The following simple statement is important for us.

**Proposition 2.2.** Let $T, T' \in \Phi_n$. Then $f_{T,T'} \in S_{2n}(g)^K$ where, for $z \in g$,

$$f_{T,T'}(z) = (\xi_z(T), \xi_z(T'))$$  \hspace{1cm} (2.8)

**Proof.** We only have to observe that $f_{T,T'} \in S_{2n}(g)$. The remainder follows from invariance of the Killing form and the fact that for $W \in \Phi, z \in g$ and $k \in K$,

$$k \cdot \xi_z(W) = \xi_{k \cdot z}(W)$$  \hspace{1cm} (2.9)
Let
\[ g^{\text{reg}} = \{ z \in g \mid g(z) = g \} \]

Thus, by Proposition 2.1, \( z \in g^{\text{reg}} \) if and only if
\[
\begin{align*}
g_{n-1}(z) &= g_n(z) \\
&= g
\end{align*}
\] (2.10)

One readily constructs some \( z \in g \) to show that \( g^{\text{reg}} \) is not empty. See Appendix for a proof that \( g^{\text{reg}} \) is not empty.

Let \( d(n) = \dim \Phi_n \). Let \( T_j, j = 1, \ldots, d(n), \) be a basis of \( \Phi_n \). The following is a restatement of Proposition 2.1 and (2.10).

**Proposition 2.3.** Let \( z \in g \). Then \( \xi_z(T_j), j = 1, \ldots, d(n) \), spans \( g(z) \). In particular \( z \in g^{\text{reg}} \) if and only if \( \xi_z(T_j), j = 1, \ldots, d(n) \), spans \( g \).

As functions on \( g \) the entries of the \( d(n) \times d(n) \) matrix \( M(z) \) given by
\[
M_{ij}(z) = (\xi_z(T_i), \xi_z(T_j))
\]
are in \( S_{2n}(g)^K \).

For any \( z \in g \) let \( K_z \) be the stabilizer of \( z \) with respect to the adjoint action \( K \) on \( g \).

Let \( \mathfrak{k}_z = \text{Lie } K_z \). Clearly
\[
\mathfrak{k}_z \text{ is the centralizer of } g(z) \text{ in } \mathfrak{k}
\] (2.11)

From the semisimplicity of \( g \) one then has
\[
\mathfrak{k}_z = 0 \text{ for any } z \in g^{\text{reg}}
\] (2.12)

**Theorem 2.4.** \( g^{\text{reg}} \) is a nonempty Zariski open subset of \( g \). Furthermore if \( z \in g^{\text{reg}} \) then the \( K \)-orbit \( K \cdot z \) is closed. That is,
\[
g^{\text{reg}} \subset Cl(g)
\] (2.13)

Put
\[
V^{\text{reg}} = \{ v \in V \mid v = v_z \text{ for some } z \in g^{\text{reg}} \}
\] (2.14)
Then $V^{K_{reg}}$ is a nonempty Zariski open (and hence dense) subset of $V$.

**Proof.** Let $z \in \mathfrak{g}$. Then clearly

$$\text{rank } M(z) \leq \dim g(z) \quad (2.15)$$

But since the Killing form is nonsingular on $g$ it follows that

$$\text{rank } M(z) = \dim g \iff z \in g^{K_{reg}}$$

Let $z \in g^{K_{reg}}$ and let $z' \in K \cdot z$. But then clearly $M(z) = M(z')$ so that $z' \in g^{K_{reg}}$. But then $k_{z'} = 0$ by (2.12). Thus $\dim K \cdot z = \dim K \cdot z'$. This implies that $K \cdot z$ is closed since the $K$-orbits on the boundary of $K \cdot z$ must have dimension smaller than $\dim K \cdot z$. But now the determinants of all the $\dim g \times \dim g$ minors of $M(z)$ are in $A$. It is an easy exercise to show that $g^{K_{reg}}$ is not empty. (As mentioned above a proof that $g^{K_{reg}}$ is not empty is given in the Appendix.) This proves that $g^{K_{reg}}$ is a nonempty Zariski open subset of $g$ and $V^{K_{reg}}$ is a nonempty Zariski open subset of $V$. QED

**Remark 2.5.** Note that since the entries of $M(z)$ are in $S_{2n}(g)^K$ the determinants of all the $\dim g \times \dim g$ minors of $M(z)$ are, in fact, in $A_{2n}$.

**2.3. Proof of Theorem 1.1.** To show that $\gamma_{2n}$ is birational it suffices, by Theorem 2.4, to prove that there exists a nonempty Zariski open subset $V_* \subset V$ such that the restriction

$$\gamma_{2n} : V_* \to V_{2n} \quad (2.16)$$

is injective. Theorem 2.4 asserts that $V^{K_{reg}}$ is a nonempty open subvariety of $V$. The variety $V_*$, to be constructed, will in fact be a nonempty open subvariety of $V^{K_{reg}}$. Before constructing $V_*$ we will first establish certain properties of the restriction

$$\gamma_{2n} : V^{K_{reg}} \to V_{2n} \quad (2.17)$$

Let $z, z' \in g^{K_{reg}}$ be such that

$$f(z) = f(z'), \ \forall f \in A_{2n} \quad (2.18)$$

We will prove that there exists an automorphism $\pi$ of $g$, which commutes with $\theta$ such that $z' = \pi(z)$.
Assume (2.18) is satisfied. For \( T \in \Phi_m \) and \( j = 1, \ldots, d(n) \), let \( f_{T,j} \in A_{2n} \) be defined by putting, for any \( w \in g \),
\[
f_{T,j}(w) = (\xi_w(T), \xi_w(T_j))
\]
But since \( f_{T,j} \in A_{2n} \), one has
\[
f_{T,j}(z) = f_{T,j}(z')
\]
We construct a linear isomorphism
\[
\pi : g \to g
\]
as follows: Let \( w \in g \). Then, by (2.10), there exists \( T \in \Phi_m \) (obviously not necessarily unique) such that \( \xi_z(T) = w \). Define (to be shown to be well-defined)
\[
\pi(w) = w', \quad \text{where } w' = \xi_{z'}(T)
\]
To see that \( \pi \) is well-defined we have only to establish that if \( T \in \Phi_m \), then
\[
\xi_z(T) = 0, \iff \xi_{z'}(T) = 0
\]
But one has
\[
\xi_z(T) = 0, \iff f_{T,j}(z) = 0, \quad \forall \ j = 1, \ldots, d(n)
\]
The same statement holds when \( z' \) replaces \( z \). But then one has (2.23) so that the linear isomorphism \( \pi \) is well-defined, noting also that
\[
\pi(z) = z'
\]
Lemma 2.6. \( \pi \) is a Lie algebra automorphism which also commutes with \( \theta \). That is, \( \pi \) stabilizes both \( \mathfrak{t} \) and \( \mathfrak{p} \).

Proof. Let
\[
u = \{ t \in g \mid \pi([t, w]) = [\pi(t), \pi(w)], \forall w \in g \}
\]
Then the Jacobi identity immediately implies that \( \nu \) is a Lie subalgebra of \( g \). Let \( w \in g \) be arbitrary. By (2.10) there exists \( T \in \Phi_{n-1} \) such that \( \xi_z(T) = w \). Let \( T_X = [X, T] \) so that \( T_X \in \Phi_n \). Define \( T_Y \in \Phi_n \) similarly where \( Y \) replaces \( X \). Then
\[
\xi_z(T_X) = [x, w]
\]
\[
\xi_z(T_Y) = [y, w]
\]
Let \( \xi_z'(T) = w' \) so that \( \pi(w) = w' \). Also let \( z' = x' + y' \) be the decomposition (1.13) when \( z' \) replaces \( z \). Then

\[
\xi_z'(T_X) = [x', w'] \\
\xi_z'(T_Y) = [y', w']
\]

Thus the Lie subalgebra \( u \) of \( g \) contains \( x \) and \( y \). But then \( u = g \) since \( x \) and \( y \) generate \( g \). Hence \( \pi \) is an automorphism. Now let \( m \leq n \) where \( m \in \mathbb{Z}_+ \). Let \( t_i \in g, i = 1, \ldots, m \), where \( t_i \in \{x, y\} \). Let

\[
w = [t_1, [t_2, [\cdots [t_{m-1}, t_m]\cdots]]]
\]

Then note that \( w \in \mathfrak{k} \) or \( \mathfrak{p} \) according as the number indices \( j \) such that \( t_j = y \) is even or odd. It follows immediately that \( \pi \) stabilizes both \( \mathfrak{k} \) and \( \mathfrak{p} \). QED

We will next restrict \( \gamma_{2n} \) to a nonempty Zariski open subset \( V_1 \) of \( V^{K reg} \) to guarantee that \( \pi \) is an inner automorphism.

One knows the degrees of the generators of \( S(g)^G \). The maximum degree is the Coxeter number of some simple component of \( g \). This number is certainly less than \( n \) and hence

\[
S(g)^G \subset A_{2n}
\]  

(2.26)

Let \( \Gamma \) be the quotient of the group \( Out g \) of outer automorphisms of \( g \) by the normal subgroup \( Inn g = G \) of inner automorphisms. The group \( \Gamma \) is finite. The image, in \( \Gamma \), of any \( \alpha \in Out g \) will be denoted by \( \sigma_\alpha \). Clearly \( S(g)^G \) is stable under the action of \( Out G \) on \( S(g) \). But this clearly defines a representation of

\[
\Gamma \rightarrow Aut S(g)^G
\]  

(2.27)

The following is well known but we will give a proof for completeness.

**Lemma 2.7.** The representation (2.27) is faithful.

**Proof.** Let \( \alpha \in Out g \) and assume that \( \alpha \notin Inn g \). Let \( g \in G \) and put \( \alpha' = Ad g \circ \alpha \). Then \( \sigma_\alpha = \sigma_{\alpha'} \neq 1 \). However \( g \) can be chosen so that \( \alpha' \) stabilizes the Weyl chamber \( C \) of a split Cartan subalgebra of a split real form of \( g \) and \( \alpha'|C \) does not reduce to the identity. However from Weyl group theory one knows that \( S(g)^G \) separates the points of \( C \). This proves that the image of \( \sigma_\alpha \) in (2.27) is not the identity. QED
For any $1 \neq \sigma \in \Gamma$ choose $f_{\sigma} \in S(\mathfrak{g})^G$ such that $f \neq f_{\sigma}$ and let

$$F = \prod_{\sigma \in \Gamma/\{1\}} (f_{\sigma} - \sigma(f_{\sigma}))$$

(2.28)

putting $F = 1$ if $\Gamma$ reduces to the identity. Obviously $F \in S(\mathfrak{g})^G \subset A_{2n}$. Let

$$\mathfrak{g}_{1}^{K,reg} = \{z \in \mathfrak{g}^{K,reg} \mid F(z) \neq 0\}$$

(2.29)

so that $\mathfrak{g}_{1}^{K,reg}$, by Theorem 2.4, is a nonempty Zariski open subset of $\mathfrak{g}^{K,reg}$ and

$$V_{1}^{K,reg} = \{v \mid v = v_z \text{ for some } z \in \mathfrak{g}_{1}^{K,reg}\}$$

(2.30)

is a nonempty Zariski open subset of $V^{K,reg}$. Here we are implicitly using the fact that the intersection of two nonempty Zariski open subsets of an irreducible variety is again a nonempty Zariski open set.

**Lemma 2.8.** Let $z, z' \in \mathfrak{g}_{1}^{K,reg}$ and assume that (2.18) is satisfied. Let $\pi$ be the $\mathfrak{g}$-automorphism of Lemma 2.6. Then $\pi$ is inner. That is, $\pi = \text{Ad } g$ for some $g \in G$ such that $\text{Ad } g$ stabilizes both $\mathfrak{k}$ and $\mathfrak{g}$.

**Proof.** If $\pi$ is inner there is nothing to prove. Assume $\pi$ is not inner and let $1 \neq \sigma \in \Gamma$ be defined by putting $\sigma = \sigma_{\pi^{-1}}$. But by (2.25) one has

$$f_{\sigma}(\pi(z)) = f_{\sigma}(z)$$

(3.31)

But

$$f_{\sigma}(\pi(z)) = (\pi^{-1} f_{\sigma})(z) = (\sigma f_{\sigma})(z)$$

But $(\sigma f_{\sigma})(z) \neq f_{\sigma}(z)$ since $F(z) \neq 0$. This contradicts (2.31). Thus $\pi$ is inner. QED

Let the notation be as in Lemma 2.8. We will now restrict $\gamma_{2n}$ even further to finally guarantee that $g \in K$.

Taking notation from [K-R] let

$$K_\theta = \{g \in G \mid \text{Ad } g \text{ stabilizes both } \mathfrak{k} \text{ and } \mathfrak{p}\}$$

(2.32)

so that, in the notation of Lemma 2.8, $g \in K_\theta$. Obviously $K \subset K_\theta$. Let $\text{Out}_G \mathfrak{k}$ be the group of all automorphisms of $\mathfrak{k}$ of the form $\text{Ad } g|\mathfrak{k}$ for $g \in K_\theta$ and let $\text{Inn } \mathfrak{k}$ be the group of
all inner automorphisms of $\mathfrak{t}$. Obviously $Inn \mathfrak{t}$ is a normal subgroup of $Out_G \mathfrak{t}$. One knows that the quotient group $\Gamma_K = Out_G \mathfrak{t}/Inn \mathfrak{t}$ is finite. See Proposition 1, p. 761 in [K-R]. The argument yielding (2.26) readily also implies

$$S(\mathfrak{t})^K \subset A_{2n}$$

(2.33)

Also the natural action of $Out_G \mathfrak{t}$ on $S(\mathfrak{t})^K$ descends to a representation

$$\Gamma_K \to Aut S(\mathfrak{t})^K$$

(2.34)

The argument establishing Lemma 2.7 is readily modified (to deal with the case where $\mathfrak{t}$ is only reductive but not semisimple) so that one has

**Lemma 2.9.** The representation (2.34) is faithful.

For each $1 \neq \tau \in \Gamma_K$ let $f_\tau \in S(\mathfrak{t})^K$ be such that $f_\tau \neq \tau f_\tau$. If $\Gamma_K$ reduces to the identity put $F_K = 1$, otherwise let

$$F_K = \prod_{\tau \in \Gamma_K/\{1\}} (f_\tau - \tau f_\tau)$$

(2.35)

Let

$$g_* = \{ z \in g_1^{K \ reg} \mid F_K(z) \neq 0 \}$$

(2.36)

and let

$$V_* = \{ v \in V \mid v = v_z \text{ for some } z \in g_* \}$$

(2.37)

Again, since the intersection of two nonempty Zariski open subsets of an irreducible variety is again a nonempty Zariski open set, it follows that $g_*$ is a nonempty Zariski open subset of $g$ and $V_*$ is a nonempty Zariski open subset of $V$. The following lemma establishes Theorem 1.1.

**Lemma 2.10.** Let $z, z' \in g^*$ be such that

$$f(z) = f(z')$$

for all $f \in A_{2n}$. Let $g \in G$ be given by Lemma 2.8 so that

$$Ad g(z) = z'$$

(2.39)
and $g \in K_\theta$ using the notation of (2.32). Then $g \in K$ so that

$$z' \in K \cdot z$$

(2.40)

proving the injectivity of (2.16) and as, noted in the beginning of §2.3, proving Theorem 1.1.

**Proof.** We first prove that $Ad g|\mathfrak{t} \in \text{Inn } \mathfrak{t}$. Assume this is not the case and let $1 \neq \tau$ be the image of $Ad g^{-1}|\mathfrak{t}$ in $\Gamma_K$. Then, by (2.38),

$$f_\tau(Ad g(z)) = f_\tau(z)$$

(2.41)

But, recalling (2.2),

$$f_\tau(Ad g(z)) = f_\tau(Ad g(x))$$

$$= (Ad g^{-1} f_\tau)(x)$$

$$= (\tau f_\tau)(x)$$

$$= (\tau f_\tau)(z)$$

But this contradicts (2.41) since $F_K(z) \neq 0$. Hence there exists $k \in K$ such that if $b = k^{-1} g$, then $b$ centralizes $\mathfrak{t}$. But then both the semisimple element $b_s$ and the unipotent element $b_u$ centralize $\mathfrak{t}$ where $b = b_s b_u$ is the Jordan decomposition of $b$. But, as one knows, the centralizer of $\mathfrak{t}$ in $\mathfrak{g}$ is commutative, reductive and contained in $\mathfrak{t}$. This readily implies that $b_u = 1$ since the nilpotent element $\log b_u$ must commute with $\mathfrak{t}$. Thus $b$ is semisimple. Hence $b$ centralizes a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$. Let $\mathfrak{g}^b$ be the centralizer of $b$ in $\mathfrak{g}$ so that $\mathfrak{h} + \mathfrak{t} \subset \mathfrak{g}^b$. For any simple component $\mathfrak{g}_i$ of $\mathfrak{g}$ let $\mathfrak{t}_i = \mathfrak{g}_i \cap \mathfrak{g}^b$ and let $\mathfrak{p}_i$ be the Killing form orthocomplement of $\mathfrak{t}_i$ in $\mathfrak{g}_i$. Since $\mathfrak{g}^b$ contains $\mathfrak{h}$ it is clear that $\mathfrak{g}^b$ is the sum of its intersections with all the simple components of $\mathfrak{g}$. It follows then that $\mathfrak{p}_i$ is Killing form orthogonal to $\mathfrak{t}$ so that $\mathfrak{p}_i \subset \mathfrak{p}$. Hence $\mathfrak{p}_i + [\mathfrak{p}_i, \mathfrak{p}_i]$ is an ideal in $\mathfrak{g}_i$. By simplicity either $\mathfrak{p}_i = 0$ in which case $\mathfrak{g}_i = \mathfrak{t}_i$ so that $\mathfrak{g}_i$ makes no nontrivial contribution to $b$ or $[\mathfrak{p}_i, \mathfrak{p}_i] = \mathfrak{t}_i \subset \mathfrak{t}$. Since $b$ is in the subgroup of $G$ corresponding to $\mathfrak{h}$ it is then clear that $b \in K$ and hence $g \in K$. QED

**2.4. Proof of Theorem 1.2.** Let $z \in \mathfrak{g}$. Then one knows from invariant theory that $K \cdot z$ has a unique closed $K$-orbit in its closure (this is immediate from (1.4)). Consequently $z \in \text{Nil}_K$ if and only if

$$0 \in \overline{K \cdot z}$$

(2.42)
Assume that $z \in \text{Nil}_K$ and let $k_m \in K$, $m \in \mathbb{Z}_+$, be a sequence such that $k_m \cdot z$ converges to 0. But then recalling the decomposition (1.13) one must have that both $k_m \cdot x$ and $k_m \cdot y$ also converge to 0. But then obviously $k_m \cdot w$ converges to 0 for any $w \in \mathfrak{g}(z)$. But then (recalling that $S(\mathfrak{g})^G \subset S(\mathfrak{g})^K$) $w$ is nilpotent for any $w \in \mathfrak{g}(z)$.

Conversely, assume that every element in $\mathfrak{g}(z)$ is nilpotent. Then there exists a Borel subalgebra $\mathfrak{b}$ of $\mathfrak{g}$ such that $\mathfrak{g}(z) \subset \mathfrak{n}$ where $\mathfrak{n}$ is the nilradical of $\mathfrak{b}$. Put $\mathfrak{b}' = \theta(\mathfrak{b})$ so that $\theta(\mathfrak{n}) = \mathfrak{n}'$ where $\mathfrak{n}'$ is the nilradical of $\mathfrak{b}'$. Let $\mathfrak{s} = \mathfrak{b} \cap \mathfrak{b}'$ so that $\mathfrak{s}$ is a solvable subalgebra of $\mathfrak{g}$ which is stable under $\theta$, since $\theta$ is involutory. Moreover there exists a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ which is contained in $\mathfrak{s}$ since the intersection of any two Borel subalgebras contains a Cartan subalgebra. Furthermore from Weyl group theory

$$\mathfrak{s} = \mathfrak{h} + \mathfrak{n} \cap \mathfrak{n}'$$

(2.43)

is a Levi decomposition of $\mathfrak{s}$. But since $\mathfrak{g}(z)$ is stable under $\theta$ one also has

$$\mathfrak{g}(z) \subset \mathfrak{n} \cap \mathfrak{n}'$$

(2.44)

But now there exists a regular semisimple element $u \in \mathfrak{h}$ such that the spectrum of $ad u|\mathfrak{n}$ is a set of positive numbers. In particular the spectrum of $ad u|\mathfrak{n} \cap \mathfrak{n}'$ is again strictly positive. Now let $u' = \theta(u)$ so that $u' \in \mathfrak{h}'$ where $\mathfrak{h}' = \theta(\mathfrak{h})$. But since $\mathfrak{s}$ is stable under $\theta$ one has $\mathfrak{h}' \subset \mathfrak{s}$. Interchanging the roles of $\mathfrak{h}$ and $\mathfrak{h}'$ it follows that the spectrum of $ad u'|\mathfrak{n} \cap \mathfrak{n}'$ is again strictly positive. But, by Lie’s theorem, the adjoint action of $\mathfrak{s}$ on $\mathfrak{n} \cap \mathfrak{n}$ may be triangularized. The diagonal entries of both $ad u$ and $ad u'$ on $\mathfrak{n} \cap \mathfrak{n}$ are positive. Hence the same is true of $ad v$ where $v = u + u'$. This however implies that for any $w \in \mathfrak{n} \cap \mathfrak{n}'$,

$$exp(-t) v \cdot w$$

converges to 0 as $t$ goes to $+\infty$

(2.45)

(noting that even though $v$ may not be semisimple the nilpotent component of $v$ relative to its Jordan decomposition contributes only polynomial terms in $t$). But this implies that

$$\mathfrak{n} \cap \mathfrak{n}' \subset \text{Nil}_K$$

(2.46)

since $v \in \mathfrak{t}$. Hence $z \in \text{Nil}_K$ proving Theorem 1.2.

2.5. Proof of Theorem 1.3. That is, we prove that if $z \in \mathfrak{g}$ then $z \in \text{Nil}_K$ if and only if $f(z) = 0$ for all homogeneous $f \in A_{2n}$ of positive degree. Of course the “only if”
is obvious since $A_{2n} \subset A$. Assume then that $z \in g$ and $f(z) = 0$ for all homogeneous $f \in A_{2n}$ of positive degree. But then recalling the $d(n) \times d(n)$ matrix $M(z)$ of §2.2 one has

$$(\xi_z(T_i), \xi_z(T_j)) = 0$$

for all $i, j \in \{1, \ldots, d(n)\}$. But then, by Proposition 2.3, one has

$$tr \text{ad} u \text{ad} v = 0$$

for all $u, v \in g(z)$. Thus, since $ad$ is faithful, $g(z)$ is solvable and hence its adjoint action on $g$ can be triangularized. The nilcone of $g$ intersected with $p$ is just the set of zeros of the polynomials in $S(p)^K$ of positive degree (see Proposition 11 in [K-R]). But as one knows the homogeneous generators of $S(p)^K$ have the same degrees as the homogeneous generators of the polynomial invariants of the restricted Weyl group operating on a Cartan subspace of $p$ (the symmetric space analogue of Chevalley’s theorem). But then one easily has $S(p)^K \subset A_{2n}$. (This follows, for example, from Proposition 23 in [K-R].) But since $S(t)^K \subset A_{2n}$ and $S(p)^K \subset A_{2n}$ one has that $x$ and $y$ are nilpotent where $z = x + y$ is the decomposition (1.13). Thus the diagonal entries of $ad x$ and $ad y$ are zero. But since $x$ and $y$ generate $g(z)$ the diagonal entries of any element in $g(z)$ are zero. Thus any element in $g(z)$ is nilpotent. Theorem 1.3 then follows from Theorem 1.2. QED

### 2.6. Proof of Theorem 1.4.

Theorem 1.3 above and Theorem 1.1 in [D] assert that there exists $r$ such that $A = A_r$ where $r \leq \max \{2, \frac{3}{8} \dim p(2n)^2\}$. But then Theorem 1.4 follows since $\frac{1}{2} (x(x - 1)) \geq \frac{3}{8} x^2$ for $x \geq 4$, and (assuming $g \neq 0$), one surely has $n > 2$. QED

### Appendix

The purpose of this appendix is to show that $g^{K \text{reg}}$ is not empty.

1.1A. Let $g = \mathfrak{k} + \mathfrak{a} + \mathfrak{n}$ be a complexified Iwasawa decomposition of $g$, consistent with the complexified Cartan decomposition

$$g = \mathfrak{k} + \mathfrak{p}$$

(e.g. $\mathfrak{a}$ is a complexified Cartan subspace of $\mathfrak{p}$). Let $R \subset \mathfrak{a}^*$ be the set of restricted roots, and for any $\nu \in R$ let $g_\nu \subset g$ be the corresponding restricted root space. Let $R_+ \subset R$
be the set of positive restricted roots defined so that
\[ n = \bigoplus_{\nu \in R_+} g_\nu \]

Let \( \zeta \) be the nonvanishing polynomial function on \( \mathfrak{a} \) defined by putting
\[ \zeta = \prod_{\nu, \nu' \in R, \nu \neq \nu'} (\nu - \nu') \quad (1.2A) \]

Let \( y \in \mathfrak{a} \) be defined so that \( \zeta(y) \neq 0 \)

Let \( \mathfrak{m} \) be the centralizer of \( \mathfrak{a} \) in \( \mathfrak{k} \). We recall that \( \theta \) is the complexified Cartan involution corresponding to (1.1A). For \( \nu \in R_+ \) let \( x_\nu \in \mathfrak{g}_\nu \). Let \( x_{-\nu} \in \mathfrak{g}_{-\nu} \) be defined by putting \( x_{-\nu} = \theta x_\nu \). Let \( \tilde{R} = R \cup \{0\} \) where, here, we regard 0 as the zero linear functional on \( \mathfrak{a} \). Then \( \tilde{R} \) is the set of weights for the adjoint action of \( \mathfrak{a} \) on \( \mathfrak{g} \). Let \( \mathfrak{r} \) be the \( \mathbb{C} \)-span of the set \( \{x_\nu\} \nu \in \tilde{R} \). Also let \( x = \sum_{\nu \in \tilde{R}} x_\nu \) so that \( x \in \mathfrak{f} \) and also \( x \in \mathfrak{r} \).

**Remark 1.1A.** Note that, for any \( \nu \in R \), \( 2\nu \) is a factor of \( \zeta \), so that \( \nu(y) \neq 0 \).

Let \( z = x + y \) and let \( \mathfrak{g}(z) \) be the Lie subalgebra of \( \mathfrak{g} \) generated by \( x \) and \( y \). One notes that \( \mathfrak{r} \) is stable under \( ad \ y \) and that \( ad \ y|\mathfrak{r} \) is diagonalizable with distinct eigenvalues. In fact clearly \( \mathfrak{r} \) is a cyclic \( ad \ y \) module with \( x \) as cyclic generator and hence

**Proposition 1.2A.** One has \( x_\nu \in \mathfrak{g}(z) \) for any \( \nu \in \tilde{R} \).

1.2A. The element \( y \in \mathfrak{p} \) will be fixed as in §1.1A. It will be our objective in this section to show that \( x_0 \) and \( x_\nu, \nu \in R_+ \) can be chosen, consequently \( x \) can chosen, so that \( \mathfrak{g}(z) = \mathfrak{g} \), i.e. \( z \in \mathfrak{g}^{K \text{ reg}} \). This will establish that \( \mathfrak{g}^{K \text{ reg}} \) is not empty.

Let \( \mathfrak{h}_m \) be a Cartan subalgebra of \( \mathfrak{m} \) so that \( \mathfrak{h} = \mathfrak{m} + \mathfrak{a} \) is a Cartan subalgebra of \( \mathfrak{g} \). Let \( \Delta \subset \mathfrak{h}^* \) be the set of roots for \( (\mathfrak{h}, \mathfrak{g}) \), and for each \( \varphi \in \Delta \), let \( e_\varphi \in \mathfrak{g} \) be a corresponding root vector. Obviously \( \mathfrak{g}_\nu \) is stable under \( ad \ \mathfrak{h} \) for any \( \nu \in R \). Hence there exists a subset \( \Delta_\nu \subset \Delta \) such that
\[ \mathfrak{g}_\nu = \sum_{\varphi \in \Delta_\nu} \mathbb{C} e_\varphi \quad (1.3A) \]

It is immediate that
\[ \Delta_{-\nu} = -\Delta_\nu \quad (1.4A) \]
For any $\nu \in R$ let $h_\nu \in a$ be such that, with respect to the Killing form, $(h, h_\nu) = \nu(h)$ for any $h \in a$. It is clear of course that $a$ is spanned by $\{h_\nu \mid \nu \in R_+\}$.

Let $P = \frac{1}{2} (1 - \theta)$ so that $P : g \to p$ is the projection of $g$ on $p$ with respect to (1.1A). Since $g(z)$ is clearly stable under $\theta$ for any $x \in \mathfrak{k}$ it is also stable under $P$. One easily has

**Lemma 1.3A.** Let $\nu \in R$ and let $\varphi \in \Delta_\nu$ so that $-\varphi \in \Delta_{-\nu}$. Then

$$P[e_\varphi, e_{-\varphi}] = c h_\nu$$

for some $c \in \mathbb{C}^\times$.

A useful criterion for $K$ – regularity is given in

**Proposition 1.4A.** For $z$ to be in $g^{K \text{reg}}$ it is necessary and sufficient that $n \subset g(z)$.

**Proof.** The necessity is by definition. Assume $n \subset g(z)$. Then $g_\nu \subset g(z)$ for any $\nu \in R_+$. But clearly $\theta(g_\nu) = g_{-\nu}$ so that $g_{-\nu} \subset g(z)$. But then $h_\nu \in g(z)$ for any $\nu \in R_+$ by Lemma 1.3. Hence $a + n \subset g(z)$. But from the Iwasawa decomposition $P(a + n) = p$. Thus $p \subset g(z)$. However $g = p + [p, p]$. Thus $g(z) = g$. QED

Let $R^1_+$ be the set of all $\nu \in R_+$ such that $\dim g_\nu = 1$ and let $R^2_+$ be the complement of $R^1_+$ in $R_+$. Assume $\nu \in R^2_+$. Then the weights of $ad \mathfrak{h}_m$ on $g_\nu$ are of the form $\varphi|\mathfrak{h}_m$ where $\varphi \in \Delta_\nu$. Since roots, as weights of $ad \mathfrak{h}$ acting on $g$, have multiplicity 1 it follows immediately that the weights of $ad \mathfrak{h}_m$ on $g_\nu$ have multipicitivity one. Thus if $\eta_\nu$ is the polynomial function on $\mathfrak{h}_m$ defined by putting

$$\eta_\nu = \prod_{\varphi, \varphi' \in \Delta_\nu, \varphi \neq \varphi'} (\varphi - \varphi')|\mathfrak{h}_m$$

(1.6A)

then $\eta_\nu$ is nonvanishing. One immediately has

**Proposition 1.5A.** Assume $\nu \in R^2_+$. Let $x' \in \mathfrak{h}_m$ be such that $\eta_\nu(x') \neq 0$. (Such an element $x'$ exists since $\eta_\nu$ is nonvanishing.) Then $g_\nu$ is a cyclic module for $ad x'$.

We can now exhibit an element $z \in g^{K \text{reg}}$. Recall the notation of §1.1A.

**Theorem 1.6A.** For any $\nu \in R^1_+$ let $0 \neq x_\nu \in g_\nu$. If $R^2_+$ is empty let $x_0 = 0$. If $R^2_+$
is not empty let \( \eta \) be the nonvanishing function on \( \mathfrak{h}_m \) defined by putting

\[
\eta = \prod_{\nu \in R^2_+} \eta_{\nu}\tag{1.7A}
\]

Let \( x_0 \in \mathfrak{h}_m \) be such that \( \eta(x_0) \neq 0 \) so that (by Proposition 1.5A) \( \mathfrak{g}_\nu \) is a cyclic module for \( \text{ad } x_0 \) for any \( \nu \in R^2_+ \). For \( \nu \in R^2_+ \) let \( x_\nu \in \mathfrak{g}_\nu \) be a cyclic generator of \( \mathfrak{g}_\nu \) with respect to the action of \( \text{ad } x_0 \). Now let \( y \in \mathfrak{a} \) be as in \( \S 1.1 \), and as in \( \S 1.1 \), let \( x = \sum_{\nu \in \tilde{R}} x_\nu \) where we recall \( x_{-\nu} = \theta(x_\nu) \) for \( \nu \in R_+ \) so that \( x \in \mathfrak{k} \). Then \( \mathfrak{g}(z) = \mathfrak{g} \) where \( z = x + y \).

Proof. One has \( x_\nu \in \mathfrak{g}(z) \) for any \( \nu \in \tilde{R} \) by Proposition 1.2A. Thus \( \mathfrak{g}_\nu \subset \mathfrak{g}(z) \) for any \( \nu \in R^2_+ \). On the other hand if \( R^2_+ \) is not empty then \( \mathfrak{g}_\nu \subset \mathfrak{g}(z) \) for \( \nu \in R^2_+ \) since the Lie algebra generated by \( x_0 \) and \( x_\nu \) contains \( \mathfrak{g}_\nu \). Thus \( \mathfrak{n} \subset \mathfrak{g}(z) \) and hence \( z \in \mathfrak{g}^{K \text{ reg}} \) by Proposition 1.4A. QED

References

[D] H. Derksen, Polynomial bounds for rings of invariants, Proc. Amer. Math. Soc., 129, no.4, 955–963

[K-T] B. Kostant and Juan Tirao, On the structure of certain subalgebras of a universal enveloping algebra, Trans. Amer. Math. Soc., 218(1976), 133–154

[K-R] B. Kostant and S. Rallis, Orbits and Representations associated with Symmetric Spaces, Amer. J. Math., 93(1971), No. 3, 753–809

[K-W] H. Kraft and N. Wallach, On the nullcone of representations of Reductive Groups, Pacific J. Math., 224(2006), 119–140

[L] J. Lepowsky, Algebraic results on representations of semisimple Lie groups, Trans. Amer. Math. Soc., 176(1973), 1–43

[L-M] J. Lepowsky and G. McCollum, On the determination of irreducible modules by restriction to a subalgebra, Trans. Amer. Math. Soc., 176(1973), 44–57

[P-1] V. Popov, Constructive invariant theory, Astérisque, 87-88(1981), 303–334

[P-2] V. Popov, The constructive theory of invariants, Math. USSR Izvest., 10(1982), 359-376

[P-3] V. Popov, The cone of Hilbert nullforms, Steklov Inst. Math. 241(2003), 177–194

[V-1] D. Vogan, The algebraic structure of representations of semi-simple Lie groups, I, Ann. of Math., 109(1979), 1–60
[V-2] D. Vogan, *Representations of Real Reductive Lie Groups*, Birkhäuser, PM 15(1981)

[W] N. Wallach, *Real Reductive Groups, I*, Academic Press Inc, 132, 1988

Bertram Kostant
Dept. of Math.
MIT
Cambridge, MA 02139

E-mail kostant@math.mit.edu