TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 208, 1975

ON THE HARISH-CHANDRA HOMOMORPHISM

BY

J. LEPOWSKY[1]

ABSTRACT. Using the Iwasawa decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$ of a real semisimple Lie algebra $\mathfrak{g}$, Harish-Chandra has defined a now-classical homomorphism from the centralizer of $\mathfrak{k}$ in the universal enveloping algebra of $\mathfrak{g}$ into the enveloping algebra $\mathfrak{A}$ of $\mathfrak{a}$. He proved, using analysis, that its image is the space of Weyl group invariants in $\mathfrak{A}$. Here the weaker fact that the image is contained in this space of invariants is proved "purely algebraically". In fact, this proof is carried out in the general setting of semisimple symmetric Lie algebras over arbitrary fields of characteristic zero, so that Harish-Chandra's result is generalized. Related results are also obtained.

1. **Introduction.** Several years ago, Harish-Chandra introduced a certain mapping which now lies at the foundation of many extensive approaches to the representation theory of semisimple Lie groups. Let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$ be an Iwasawa decomposition of a real semisimple Lie algebra, $\mathfrak{G}$ the universal enveloping algebra of $\mathfrak{g}$, $\mathfrak{G}^{\mathfrak{k}}$ the centralizer of $\mathfrak{k}$ in $\mathfrak{G}$, and $\mathfrak{A}$ the universal enveloping algebra of $\mathfrak{a}$. The Harish-Chandra mapping to which we refer is the homomorphism $p: \mathfrak{G}^{\mathfrak{k}} \to \mathfrak{A}$ defined by the projection to $\mathfrak{A}$ with respect to the decomposition $\mathfrak{G} = \mathfrak{A} \oplus (\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})$ (see [2(b), §4]). Probably the most significant single property of p is that its image is contained in the algebra $\mathfrak{A}_W$ of suitably translated (by half the sum of the positive restricted roots) Weyl group invariants in $\mathfrak{A}$. (Its image actually equals $\mathfrak{A}_W$.) See [2(b), §4] for the original proof. Although this property is "purely algebraic," we know of no existing proofs which do not rely on analysis on the corresponding real semisimple Lie group. The main purpose of this paper is to present a "purely algebraic" proof of the fact that $p(\mathfrak{G}^{\mathfrak{k}}) \subset \mathfrak{A}_W$. The problem of finding such a proof was posed by B. Kostant and also by J. Dixmier.

Received by the editors January 9, 1974.

AMS (MOS) subject classifications (1970). Primary 17B20, 17B35; Secondary 17B05, 17B10, 22E45.

Key words and phrases. Harish-Chandra homomorphism, real semisimple Lie algebra, Iwasawa decomposition, universal enveloping algebra, restricted Weyl group, semisimple symmetric Lie algebra, symmetric decomposition, splitting Cartan subspace, restricted root system.

[1] Partially supported by NSF GP 33893.

Copyright © 1975, American Mathematical Society

In his recent book [1], Dixmier sets up an algebraic formalism which recovers the "algebraic" properties of real semisimple Lie algebras. Beginning with a "semisimple symmetric Lie algebra"—a pair $(\mathfrak{g}, \theta)$ where $\mathfrak{g}$ is a semisimple Lie algebra over an arbitrary field of characteristic zero and θ is an arbitrary automorphism of $\mathfrak{g}$ such that $\theta^2 = 1$—he obtains Cartan subspaces and Iwasawa decompositions [1, §1.13]. He then shows that certain theorems on representations of real semisimple Lie algebras, including some results of [2(a)], [5] and [6], carry over to the general context [1, Chapter 9]. Our proof of the theorem $p(\mathcal{G}^{\mathfrak{k}}) \subset \mathcal{A}_W$ holds in this setting, and therefore generalizes Harish-Chandra's original result. Our argument, which is very different from the existing analytic proofs, is not long; much of this paper consists of material on semisimple symmetric Lie algebras which is well known in the familiar special case of real semisimple Lie algebras.

The contents of this paper are as follows: In §2, we give an exposition of the relevant properties of semisimple symmetric Lie algebras, including a discussion of the restricted root system and the restricted Weyl group.

The subject of §3 is the restriction homomorphism from the algebra of $\mathfrak{k}$-invariant polynomial functions on $\mathfrak{p}$ into the algebra of polynomial functions on $\mathfrak{a}$, where $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ is the "symmetric decomposition" (i.e., eigenspace decomposition) of $\mathfrak{g}$ corresponding to θ, and $\mathfrak{a}$ is a "splitting" Cartan subspace of $\mathfrak{p}$. We show that this map injects into the algebra of Weyl group invariant polynomial functions on $\mathfrak{a}$. We do not know how to prove algebraically that it maps onto these invariants, except when $\dim \mathfrak{a} = 1$. This would be an algebraic generalization of Chevalley's polynomial restriction theorem, and could be used to prove that $p(\mathcal{G}^{\mathfrak{k}})$ is all of $\mathcal{A}_W$. Our proof of the fact that the restriction homomorphism maps into the Weyl group invariant polynomials reduces the problem to the three-dimensional simple case and solves it there. The injectivity follows from [1, Proposition 1.13.13], but our proof avoids the use of algebraic groups. We include an alternate proof, due to G. McCollum, of the key lemma for the injectivity.

The main theorem is stated and proved in §4. We include mention of the kernel of p, which is already known in the general setting (see [5, Remark 4.6], and the presentation in [1, Proposition 9.2.15]), although because of our injectivity result in §3 we can again avoid using Lie or algebraic groups. The proof that $p(\mathcal{G}^{\mathfrak{k}}) \subset \mathcal{A}_W$ is done in two stages: First we prove it when $\dim \mathfrak{a} = 1$ (and in this case we also prove that $p(\mathcal{G}^{\mathfrak{k}}) = \mathcal{A}_W$), using §3. Then we reduce the general case to this case by examining suitable semisimple subalgebras of $\mathfrak{g}$ associated with the simple restricted roots. The intermediate result, Theorem 4.17, is also interesting.

Finally, in the Appendix, we give a vector-valued generalization of the injectivity result of §3. This result also generalizes an argument in [5, proof of Lemma 4.1] (see also [6] and [1, Lemma 9.2.7, part (b) of the proof]) which depends on Lie or algebraic groups. Our original proof was simplified by G. McCollum.

We would like to thank McCollum for many valuable conversations and J. Dixmier for generously giving us access to the manuscript of his book. Certain of our methods were inspired by arguments found in [4] and [7, P. Cartier's Exposé no. 18].

Notations. The dual of a vector space V is denoted V^*. $\mathbf{Z}_+$, $\mathbf{Q}$ and $\mathbf{R}$ denote respectively the set of nonnegative integers and the fields of rational and real numbers. The restriction of a function f to a subset X of its domain is written $f|X$.

2. Preliminaries on semisimple symmetric Lie algebras.

Fix a field k of characteristic zero. Let $(\mathfrak{g}, \theta)$ be a semisimple symmetric Lie algebra over k, in the sense of [1, §1.13]. That is, $\mathfrak{g}$ is a semisimple Lie algebra over k and θ is an automorphism of $\mathfrak{g}$ such that $\theta^2 = 1$. Let $\mathfrak{k}$ be the subalgebra of fixed points for θ, and let $\mathfrak{p} = \{x \in \mathfrak{g} | \theta x = -x\}$, so that $\mathfrak{g} = \mathfrak{k} + \mathfrak{p}$ is a direct sum decomposition, orthogonal with respect to the Killing form of $\mathfrak{g}$. This is called the *symmetric decomposition* of $\mathfrak{g}$ defined by θ. We have $[\mathfrak{k}, \mathfrak{p}] \subset \mathfrak{p}$ and $[\mathfrak{p}, \mathfrak{p}] \subset \mathfrak{k}$.

Let $\mathfrak{a}$ be a Cartan subspace of $\mathfrak{p}$, that is, a maximal abelian subspace of $\mathfrak{p}$ which is reductive in $\mathfrak{g}$; Cartan subspaces exist by [1, Théorème 1.13.6]. Let $\mathfrak{m}$ be the centralizer of $\mathfrak{a}$ in $\mathfrak{k}$, $\mathfrak{l}$ an arbitrary Cartan subalgebra of $\mathfrak{m}$ and $\mathfrak{h} = \mathfrak{l} \oplus \mathfrak{a}$. Then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ [1, Proposition 1.13.7].

Let $\overline{k}$ be a field extension of k, $\overline{\mathfrak{g}} = \mathfrak{g} \otimes \overline{k}$, $\overline{\mathfrak{k}} = \mathfrak{k} \otimes \overline{k}$, etc., and let $\overline{\theta}$ be the $\overline{k}$-linear extension of θ to $\overline{\mathfrak{g}}$. Then $(\overline{\mathfrak{g}}, \overline{\theta})$ is a semisimple symmetric Lie algebra over $\overline{k}$ with symmetric decomposition $\overline{\mathfrak{g}} = \overline{\mathfrak{k}} \oplus \overline{\mathfrak{p}}$, $\overline{\mathfrak{a}}$ is a Cartan subspace of $\overline{\mathfrak{p}}$, $\overline{\mathfrak{m}}$ is the centralizer of $\overline{\mathfrak{a}}$ in $\overline{\mathfrak{k}}$, $\overline{\mathfrak{l}}$ (resp., $\overline{\mathfrak{h}}$) is a Cartan subalgebra of $\overline{\mathfrak{m}}$ (resp., $\overline{\mathfrak{g}}$), and $\overline{\mathfrak{h}} = \overline{\mathfrak{l}} \oplus \overline{\mathfrak{a}}$.

Suppose that $\overline{\mathfrak{h}}$ is a splitting Cartan subalgebra of $\overline{\mathfrak{g}}$. (This can be insured by choosing $\overline{k}$ to be algebraically closed.) Denote by $R \subset \overline{\mathfrak{h}}^*$ the set of roots of $\overline{\mathfrak{g}}$ with respect to $\overline{\mathfrak{h}}$.

Assume now that $\mathfrak{a}$ is a splitting Cartan subspace of $\mathfrak{p}$ in the sense of [1, §1.13], i.e., for all $a \in \mathfrak{a}$, the operator ad a on $\mathfrak{g}$ can be upper triangularized and hence diagonalized. Consider the root space decomposition of $\overline{\mathfrak{g}}$ with respect to $\overline{\mathfrak{h}}$:

$$\overline{\mathfrak{g}} = \overline{\mathfrak{h}} \oplus \coprod_{\lambda \in R} \overline{\mathfrak{g}}^\lambda,$$

where $\overline{\mathfrak{g}}^{\lambda}$ denotes the root space for λ. Let $P: \overline{\mathfrak{h}}^* \to \overline{\mathfrak{a}}^*$ denote the restriction map, and let Σ denote the set of nonzero members of $P(R)$. For all $\bar{k}$-linear functionals $\phi: \overline{\mathfrak{a}} \to \bar{k}$, let

$$\overline{\mathfrak{g}}^{\phi} = \{x \in \overline{\mathfrak{g}} \,|\, [a, x] = \phi(a)x \text{ for all } a \in \overline{\mathfrak{a}}\}.$$

Then clearly

$$\overline{\mathfrak{g}}^0 = \overline{\mathfrak{m}} \oplus \overline{\mathfrak{a}}, \quad \text{and} \quad \overline{\mathfrak{g}} = \overline{\mathfrak{g}}^0 \oplus \coprod_{\phi \in \Sigma} \overline{\mathfrak{g}}^{\phi}.$$

Now for all k-linear functionals $\phi: \mathfrak{a} \to k$, define

$$\mathfrak{g}^{\phi} = \{x \in \mathfrak{g} \,|\, [a, x] = \phi(a)x \text{ for all } a \in \mathfrak{a}\}.$$

Then

$$\mathfrak{g}^0 = \mathfrak{m} \oplus \mathfrak{a},$$

and since $\mathfrak{a}$ is a splitting Cartan subspace, Σ is identified with (i.e., is the set of $\bar{k}$-linear extensions of the members of) $\{\phi \in \mathfrak{a}^* \,|\, \phi \neq 0$ and $\mathfrak{g}^{\phi} \neq 0\}$, and

$$\mathfrak{g} = \mathfrak{g}^0 \oplus \coprod_{\phi \in \Sigma} \mathfrak{g}^{\phi} = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{\phi \in \Sigma} \mathfrak{g}^{\phi}.$$

The members of Σ, regarded as elements of either $\mathfrak{a}^*$ or $\overline{\mathfrak{a}}^*$, are called the *restricted roots* of $\mathfrak{g}$ with respect to $\mathfrak{a}$. Σ spans $\mathfrak{a}^*$ over k and $\overline{\mathfrak{a}}^*$ over $\bar{k}$. Note that $[\mathfrak{g}^{\phi}, \mathfrak{g}^{\psi}] \subset \mathfrak{g}^{\phi+\psi}$ and that $\theta\mathfrak{g}^{\phi} = \mathfrak{g}^{-\phi}$ for all $\phi, \psi \in \mathfrak{a}^*$.

For all $\phi \in \Sigma$, $\overline{\mathfrak{g}}^{\phi} = \coprod \overline{\mathfrak{g}}^{\lambda}$, where λ ranges through $\{\lambda \in R \,|\, P(\lambda) = \phi\}$, and setting $R' = \{\lambda \in R \,|\, P(\lambda) = 0\}$, we have

$$\overline{\mathfrak{g}}^0 = \overline{\mathfrak{h}} \oplus \coprod_{\lambda \in R'} \overline{\mathfrak{g}}^{\lambda}.$$

Moreover, $R'|\overline{\mathfrak{t}}$ is the set of roots of the reductive Lie algebra $\overline{\mathfrak{m}}$ with respect to its splitting Cartan subalgebra $\overline{\mathfrak{t}}$; for all $\lambda \in R'$, the root space $\overline{\mathfrak{m}}^{\lambda|\overline{\mathfrak{t}}} = \overline{\mathfrak{g}}^{\lambda}$; and

$$\overline{\mathfrak{m}} = \overline{\mathfrak{t}} \oplus \coprod_{\lambda \in R'} \overline{\mathfrak{g}}^{\lambda}$$

(see [1, Propositions 1.13.7(iii) and 1.13.9]). Also, setting $R'' = \{\lambda \in R \,|\, P(\lambda) \neq 0\}$, we have $P(R'') = \Sigma$ by definition.

Let B be the Killing form of $\mathfrak{g}$ and $\overline{B}$ its $\bar{k}$-bilinear extension to $\overline{\mathfrak{g}}$, so that $\overline{B}$ is the Killing form of $\overline{\mathfrak{g}}$. Then $\overline{B}$ is nonsingular on $\overline{\mathfrak{h}}$, and so defines naturally a nonsingular symmetric bilinear form, denoted $\overline{B}^*$, on $\overline{\mathfrak{h}}^*$. Moreover, since $\overline{B}(\overline{\mathfrak{t}}, \overline{\mathfrak{a}}) = 0$, $\overline{B}$ is nonsingular on $\overline{\mathfrak{a}}$, thus defining a nonsingular symmetric bilinear form on $\overline{\mathfrak{a}}^*$. Let us identify $\overline{\mathfrak{a}}^*$ with the subspace $\{\lambda \in \overline{\mathfrak{h}}^* \,|\, \lambda|\overline{\mathfrak{t}} = 0\}$ of $\overline{\mathfrak{h}}^*$ by extending the definition of each element of $\overline{\mathfrak{a}}^*$ by requiring it to be zero on $\overline{\mathfrak{t}}$. Then the natural bilinear form on $\overline{\mathfrak{a}}^*$ is exactly the restriction of $\overline{B}^*$ to $\overline{\mathfrak{a}}^*$. Moreover, if we also identify $\overline{\mathfrak{t}}^*$ with the subspace of elements of $\overline{\mathfrak{h}}^*$ vanishing on $\overline{\mathfrak{l}}$, then $\overline{\mathfrak{h}}^* = \overline{\mathfrak{l}}^* \oplus \overline{\mathfrak{a}}^*$, and $\overline{B}^*(\overline{\mathfrak{l}}^*, \overline{\mathfrak{a}}^*) = 0$. In particular, the restriction map $P: \overline{\mathfrak{h}}^* \to \overline{\mathfrak{a}}^*$ coincides both with the projection to $\overline{\mathfrak{a}}^*$ with respect to the above decomposition and with the orthogonal projection to $\overline{\mathfrak{a}}^*$ with respect to $\overline{B}^*$.

The automorphism $\overline{\theta}$ of $\overline{\mathfrak{g}}$ is 1 on $\overline{\mathfrak{l}}$ and -1 on $\overline{\mathfrak{a}}$, and so preserves $\overline{\mathfrak{h}}$. The transpose of $\overline{\theta}|\overline{\mathfrak{h}}$, which we denote by $\overline{\theta}^*$, is the isometry of $\overline{\mathfrak{h}}^*$ which is 1 on $\overline{\mathfrak{l}}^*$ and -1 on $\overline{\mathfrak{a}}^*$. Thus $P: \overline{\mathfrak{h}}^* \to \overline{\mathfrak{a}}^*$ can be realized by the formula $\frac{1}{2}(1 - \overline{\theta}^*)$.

Now let $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ denote the rational span of R in $\overline{\mathfrak{h}}^*$. Then $\overline{\mathfrak{h}}^* = \overline{\mathfrak{h}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} \overline{k}$ in a natural way. Moreover, $\overline{B}^*$ is $\mathbf{Q}$-valued and positive definite on the rational space $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$. Now $\overline{\theta}^*$ preserves R and hence preserves $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$, and so $P = \frac{1}{2}(1 - \overline{\theta}^*)$ also preserves $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$. Thus since Σ consists of the nonzero members of $P(R)$, $\Sigma \subset \overline{\mathfrak{h}}^*_{\mathbf{Q}}$, so that for all $\phi \in \Sigma$, $\overline{B}^*(\phi, \phi)$ is a positive rational number. But B is nonsingular on $\mathfrak{a}$ because $\overline{B}$ is nonsingular on $\overline{\mathfrak{a}}$. Hence B induces naturally a nonsingular symmetric k-bilinear form $(\cdot, \cdot)$ on $\mathfrak{a}^*$. If we identify $\overline{\mathfrak{a}}^*$ with $\mathfrak{a}^* \otimes_k \overline{k}$, then $\overline{B}^*|\mathfrak{a}^*$ is just $(\cdot, \cdot)$ since $\overline{B}^*|\overline{\mathfrak{a}}^*$ is the canonical form on $\overline{\mathfrak{a}}^*$ defined by $\overline{B}|\overline{\mathfrak{a}}$. Hence $\overline{B}^*(\phi, \phi) = (\phi, \phi)$ for all $\phi \in \Sigma$, and we have the following two lemmas:

Lemma 2.1. *Let* $\overline{\mathfrak{a}}^*_{\mathbf{Q}} = \overline{\mathfrak{a}}^* \cap \overline{\mathfrak{h}}^*_{\mathbf{Q}}$ *and* $\overline{\mathfrak{l}}^*_{\mathbf{Q}} = \overline{\mathfrak{l}}^* \cap \overline{\mathfrak{h}}^*_{\mathbf{Q}}$. *Then* $\overline{\mathfrak{h}}^*_{\mathbf{Q}} = \overline{\mathfrak{a}}^*_{\mathbf{Q}} \oplus \overline{\mathfrak{l}}^*_{\mathbf{Q}}$, $\overline{\mathfrak{h}}^* = \overline{\mathfrak{h}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} \overline{k}$, $\overline{\mathfrak{a}}^* = \overline{\mathfrak{a}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} \overline{k}$ *and* $\overline{\mathfrak{l}}^* = \overline{\mathfrak{l}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} \overline{k}$. *Moreover,* $\overline{\mathfrak{a}}^*_{\mathbf{Q}}$ *is the rational span of* Σ, $\overline{\mathfrak{a}}^*_{\mathbf{Q}} \subset \mathfrak{a}^*$ *and* $\mathfrak{a}^* = \overline{\mathfrak{a}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} k$.

Lemma 2.2. $\overline{B}^*|\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ *is rational-valued and positive definite. B is nonsingular on* $\mathfrak{a}$. *Denoting by* $(\cdot, \cdot)$ *the corresponding canonical nonsingular symmetric k-bilinear form on* $\mathfrak{a}^*$, *we have that* $\overline{B}^*|\mathfrak{a}^* = (\cdot, \cdot)$. *In particular,* $(\cdot, \cdot)$ *is rational-valued and positive definite on* $\overline{\mathfrak{a}}^*_{\mathbf{Q}}$, *and for all* $\phi \in \Sigma, (\phi, \phi)$ *is a positive rational number.*

For each $\lambda \in R$, let $w_\lambda : \overline{\mathfrak{h}}^* \to \overline{\mathfrak{h}}^*$ denote the orthogonal reflection through the hyperplane of $\overline{\mathfrak{h}}^*$ orthogonal to λ (with respect to $\overline{B}^*$). Then w_λ is an isometry of $\overline{\mathfrak{h}}^*$ which preserves $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ and R. The *Weyl group* W_R of $\overline{\mathfrak{g}}$ with respect to $\overline{\mathfrak{h}}$ is defined to be the group of isometries of $\overline{\mathfrak{h}}^*$ or of $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ generated by the w_λ $(\lambda \in R)$.

Now let E be the real vector space $\overline{\mathfrak{h}}^*_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{R}$. Then the restriction of $\overline{B}^*$ to $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ extends naturally to an $\mathbf{R}$-bilinear form B_E on E. Since $\overline{B}^*$ is positive definite on $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$, B_E is positive definite on E and hence is a Euclidean scalar product on E. W_R extends naturally to a group of isometries, also denoted W_R, of E, and R becomes a reduced system of roots in E with Weyl group W_R, in the sense of [1, Appendice] and [8, §1.1.2].

Recall that the isometry $\overline{\theta}^*$ of $\overline{\mathfrak{h}}^*$ preserves R and $\overline{\mathfrak{h}}^*_{\mathbf{Q}}$. The $\mathbf{R}$-linear extension of $\overline{\theta}^*|\overline{\mathfrak{h}}^*_{\mathbf{Q}}$ to E is an isometry of E with square 1 which we call

θ_E. Let $\sigma = -\theta_E$, so that σ is an isometry of E which preserves R and has square 1. Then (R, σ) is a σ-system of roots in E, in the sense of [8, §1.1.3], except that we allow the ċases $\sigma = \pm 1$.

Let E_+ (resp., E_-) denote the $+1$ (resp., -1) eigenspace of σ in E, so that $E = E_+ \oplus E_-$, and this is an orthogonal deceomposition. Then

$$\overline{\mathfrak{a}}^*_Q = E_+ \cap \overline{\mathfrak{h}}^*_Q, \quad \overline{\mathfrak{t}}^*_Q = E_- \cap \overline{\mathfrak{h}}^*_Q, \quad E_+ = \overline{\mathfrak{a}}^*_Q \otimes_Q \mathbf{R}, \quad E_- = \overline{\mathfrak{t}}^*_Q \otimes_Q \mathbf{R},$$

and E_+ is the real span of Σ. Recall that we have defined $R' = \{\lambda \in R | P(R) = 0\}$ and $R'' = \{\lambda \in R | P(R) \neq 0\}$. Then clearly $R' = R \cap E_-$,

$$R' = \{\lambda \in R | \sigma\lambda = -\lambda\} = \{\lambda \in R | \lambda|\overline{\mathfrak{a}} = 0\}$$

and

$$R'' = \{\lambda \in R | \sigma\lambda \neq -\lambda\} = \{\lambda \in R | \lambda|\overline{\mathfrak{a}} \neq 0\}.$$

Recall that if $\lambda \in R'$, then the root space $\overline{\mathfrak{g}}^\lambda \subset \overline{\mathfrak{m}}$.

Lemma 2.3. *For all* $\lambda \in R$, $\sigma\lambda - \lambda \notin R$.

Proof. Assume that $\sigma\lambda - \lambda \in R$. Then $\sigma\lambda - \lambda \in R'$, and so $\lambda - \sigma\lambda \in R'$. Thus $\overline{\mathfrak{g}}^{\lambda - \sigma\lambda} \subset \overline{\mathfrak{m}}$. Let e_λ be a nonzero vector in $\overline{\mathfrak{g}}^\lambda$. Then $\overline{\theta} e_\lambda \in \overline{\mathfrak{g}}^{\overline{\theta}^*\lambda} = \overline{\mathfrak{g}}^{-\sigma\lambda}$, and so $[e_\lambda, \overline{\theta} e_\lambda]$ is a nonzero element of $\overline{\mathfrak{g}}^{\lambda - \sigma\lambda} \subset \overline{\mathfrak{m}}$. But $\overline{\theta}[e_\lambda, \overline{\theta} e_\lambda] = [\overline{\theta} e_\lambda, e_\lambda] = -[e_\lambda, \overline{\theta} e_\lambda]$, so that $[e_\lambda, \overline{\theta} e_\lambda] \in \overline{\mathfrak{p}}$. This contradiction proves the lemma. Q.E.D.

This result asserts that (R, σ) is a normal σ-system, in the sense of [8, §1.1.3]. (The proof here, which also appears in [3, p. 76, proof of Lemma 3.6], is more direct than the proof given in [8, Lemma 1.1.3.6] for the special case of real semisimple Lie algebras.) The results of [8, §1.1.3] on normal σ-systems are now applicable in our context. (The cases $\sigma = \pm 1$ do not cause any difficulty.) In particular, since Σ is the set of orthogonal projections to E_+ of the members of R'', we have by [8, Proposition 1.1.3.1]:

Lemma 2.4 (S. Araki). *Σ is a (not necessarily reduced) system of roots in E_+, in the sense of* [8, §1.1.2]. *The Weyl group W of Σ is the group of isometries of E_+ (with respect to B_E) generated by $\{s_\phi | \phi \in \Sigma\}$ where s_ϕ is the reflection through the hyperplane of E_+ orthogonal to ϕ.*

W preserves $E_+ \cap \overline{\mathfrak{h}}^*_Q = \overline{\mathfrak{a}}^*_Q$, and its restriction to this space extends naturally to a group of isometries, still denoted W, of $\mathfrak{a}^*$, with respect to the bilinear form $(\cdot, \cdot)$ in Lemma 2.2. In this context, W is called the *restricted Weyl group* of $\mathfrak{g}$ with respect to $\mathfrak{a}$. It is the group of isometries of $\mathfrak{a}^*$ (with respect to $(\cdot, \cdot)$) generated by $\{s_\phi | \phi \in \Sigma\}$, where in this case s_ϕ is identified with the orthogonal reflection through the hyperplane of $\mathfrak{a}^*$ orthogonal to

ϕ. Similarly, W extends to a group of isometries of $\bar{\mathfrak{a}}^*$.

We shall need the following result:

Lemma 2.5. *Let* $\phi \in \Sigma$ *and* $s \in W$. *Then* $\dim \mathfrak{g}^{\phi} = \dim \mathfrak{g}^{s\phi}$.

Proof. It is sufficient to show that the $\bar{k}$-dimensions of $\bar{\mathfrak{g}}^{\phi}$ and $\bar{\mathfrak{g}}^{s\phi}$ are equal. By [8, Lemma 1.1.3.5 or Proposition 1.1.3.3], there exists $w \in W_R$ (the Weyl group for $\bar{\mathfrak{g}}$ with respect to $\bar{\mathfrak{h}}$) such that w, regarded as an isometry of $\bar{\mathfrak{h}}^*$, preserves $\bar{\mathfrak{a}}^*$ and $\bar{\mathfrak{l}}^*$, and restricts to s on $\bar{\mathfrak{a}}^*$. Hence $P \circ w = w \circ s : \bar{\mathfrak{h}}^* \to \bar{\mathfrak{a}}^*$. But w preserves R, and hence takes $R_{\phi} = \{\lambda \in R \mid P(\lambda) = \phi\}$ onto $R_{s\phi} = \{\lambda \in R \mid P(\lambda) = s\phi\}$. Since

$$\bar{\mathfrak{g}}^{\phi} = \coprod_{\lambda \in R_{\phi}} \bar{\mathfrak{g}}^{\lambda}, \quad \bar{\mathfrak{g}}^{s\phi} = \coprod_{\lambda \in R_{s\phi}} \bar{\mathfrak{g}}^{\lambda},$$

and each $\bar{\mathfrak{g}}^{\lambda}$ is one-dimensional, the lemma is proved. Q.E.D.

Let Σ_+ be an arbitrary positive system in the root system Σ. Then we have the decomposition

$$(*) \qquad \mathfrak{g} = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{\phi \in \Sigma_+} \mathfrak{g}^{\phi} \oplus \coprod_{\phi \in \Sigma_+} \mathfrak{g}^{-\phi}.$$

Let $\mathfrak{n}$ be the subalgebra $\coprod \mathfrak{g}^{\phi}$ $(\phi \in \Sigma_+)$ of $\mathfrak{g}$.

Lemma 2.6. *We have* $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$.

Proof. To show that $\mathfrak{g} = \mathfrak{k} + \mathfrak{a} + \mathfrak{n}$, it is sufficient, in view of $(*)$, to show that $\mathfrak{g}^{-\phi} \subset \mathfrak{k} + \mathfrak{n}$ for all $\phi \in \Sigma_+$. But if $x \in \mathfrak{g}^{-\phi}$, $\theta x \in \theta \mathfrak{g}^{-\phi} = \mathfrak{g}^{\phi}$, so that $x = (x + \theta x) - \theta x \in \mathfrak{k} + \mathfrak{n}$. Now suppose $x \in \mathfrak{k}$, $y \in \mathfrak{a}$ and $z \in \mathfrak{n}$, and suppose $x + y + z = 0$. Then $0 = \theta(x + y + z) = x - y + \theta z$, so that $2y + z - \theta z = 0$. But $\theta z \in \coprod_{\phi \in \Sigma_+} \mathfrak{g}^{-\phi}$, and so by the directness of the sum $(*)$, $y = z = 0$. Hence $x = 0$ also. Q.E.D.

This decomposition is called the *Iwasawa decomposition* of $\mathfrak{g}$ associated with θ, $\mathfrak{a}$ and Σ_+. We may choose a positive system R_+ for R such that $\{\lambda \in R \mid P(\lambda) \in \Sigma_+\} = R_+''$, where $R_+'' = R'' \cap R_+$, and the Iwasawa decomposition implies that $\bar{\mathfrak{g}} = \bar{\mathfrak{k}} \oplus \bar{\mathfrak{a}} \oplus \coprod_{\phi \in R_+''} \bar{\mathfrak{g}}^{\phi}$. We shall not need this last fact.

3. **The polynomial restriction map** F_*. Let k be a field of characteristic zero. For every finite-dimensional vector space V over k, let $S(V)$ denote the symmetric algebra over V. Since k is infinite, $S(V^*)$ is naturally isomorphic to the algebra of polynomial functions on V, i.e., the algebra of sums of products of linear functionals on V. (The isomorphism takes the symmetric algebra product $f_1 f_2 \cdots f_r$ of linear functionals f_i to the corresponding product $f_1 f_2 \cdots f_r$ of functions on V.) Hence we may, and often shall, identify

$S(V^*)$ with the algebra of polynomial functions on V.

Let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ be the symmetric decomposition of a semisimple symmetric Lie algebra $(\mathfrak{g}, \theta)$ over k, $\mathfrak{a} \subset \mathfrak{p}$ a splitting Cartan subspace, and W the corresponding restricted Weyl group. Then $\mathfrak{k}$ acts on $\mathfrak{p}$, hence on $\mathfrak{p}^*$ by contragredience, and thus on $S(\mathfrak{p}^*)$ by unique extension by derivations. Denote by $S(\mathfrak{p}^*)^{\mathfrak{k}}$ the corresponding algebra of $\mathfrak{k}$-annihilated vectors. Also, W acts on $\mathfrak{a}^*$, and hence acts on $S(\mathfrak{a}^*)$ by automorphisms. Let $S(\mathfrak{a}^*)^W$ be the algebra of W-invariants.

Denote by $F : S(\mathfrak{p}^*) \to S(\mathfrak{a}^*)$ the restriction homomorphism, and let $F_* = F|S(\mathfrak{p}^*)^{\mathfrak{k}}$, so that $F_* : S(\mathfrak{p}^*)^{\mathfrak{k}} \to S(\mathfrak{a}^*)$.

Theorem 3.1. *We have* $F_*(S(\mathfrak{p}^*)^{\mathfrak{k}}) \subset S(\mathfrak{a}^*)^W$, *and* $F_* : S(\mathfrak{p}^*)^{\mathfrak{k}} \to S(\mathfrak{a}^*)^W$ *is an algebra injection.* ,

Proof. By passing to an algebraic closure of k if necessary, we observe that to prove the theorem it is sufficient to prove it in case k is algebraically closed. We now make this assumption. However, we shall need it only in the proof that $F_*(S(\mathfrak{p}^*)^{\mathfrak{k}}) \subset S(\mathfrak{a}^*)^W$, and only after Lemma 3.3.

First we shall show that $F_*(S(\mathfrak{p}^*)^{\mathfrak{k}}) \subset S(\mathfrak{a}^*)^W$ and then that F_* is injective. The first assertion will be proved essentially by reducing to the case in which $\mathfrak{g}$ is three-dimensional simple.

Let B be the Killing form of $\mathfrak{g}$. Define a bilinear form B_θ on $\mathfrak{g}$ by

$$B_\theta(x, y) = -B(x, \theta y)$$

for all $x, y \in \mathfrak{g}$, so that B_θ is a nonsingular symmetric form.

Let $\Sigma \subset \mathfrak{a}^*$ be the set of restricted roots of $\mathfrak{g}$ with respect to $\mathfrak{a}$, and let $\mathfrak{m}$ be the centralizer of $\mathfrak{a}$ in $\mathfrak{k}$.

Lemma 3.2. *The decomposition* $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{\phi \in \Sigma} \mathfrak{g}^\phi$ *is a* B_θ*-orthogonal decomposition. In particular,* B_θ *is nonsingular on each* $\mathfrak{g}^\phi$ $(\phi \in \Sigma)$, *on* $\mathfrak{m}$ *and on* $\mathfrak{a}$. *Also,* B *is nonsingular on* $\mathfrak{m}$ *and on* $\mathfrak{a}$.

Proof. It is easy to see that for all $\phi, \psi \in \Sigma$, $B(\mathfrak{g}^\phi, \mathfrak{g}^\psi) = 0$ unless $\phi + \psi = 0$, and that $B(\mathfrak{g}^\phi, \mathfrak{m} + \mathfrak{a}) = 0$. Since $\theta \mathfrak{g}^\phi = \mathfrak{g}^{-\phi}$ for all $\phi \in \Sigma$ and since $B_\theta(\mathfrak{m}, \mathfrak{a}) = B(\mathfrak{m}, \mathfrak{a}) = 0$, the decomposition $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{\phi \in \Sigma} \mathfrak{g}^\phi$ is B_θ-orthogonal. Since B_θ is nonsingular, the restriction of B_θ to each component in this sum is nonsingular. Q.E.D.

(The nonsingularity of B on $\mathfrak{a}$ was proved another way in §2; see Lemma 2.2.)

Since B is nonsingular on $\mathfrak{a}$, B induces a nonsingular symmetric bilinear form $(\cdot, \cdot)$ on $\mathfrak{a}^*$ and an isometry from $\mathfrak{a}^*$ onto $\mathfrak{a}$. For all $\phi \in \Sigma$, let

$x_\phi \in \mathfrak{a}$ be the image of ϕ under this isometry. Then $B(x_\phi, a) = \phi(a)$ for all $a \in \mathfrak{a}$, and $B(x_\phi, x_\psi) = \phi(x_\psi) = (\phi, \psi)$ for all $\phi, \psi \in \Sigma$.

Lemma 3.3. *Let* $\phi \in \Sigma$. *For all* $e \in \mathfrak{g}^\phi$,

$$[e, \theta e] = B(e, \theta e)x_\phi = -B_\theta(e, e)x_\phi.$$

Proof. Since $\theta e \in \theta\mathfrak{g}^\phi = \mathfrak{g}^{-\phi}$, $[e, \theta e] \in \mathfrak{m} + \mathfrak{a}$. But $\theta[e, \theta e] = -[e, \theta e]$, so that $[e, \theta e] \in \mathfrak{p}$. Hence $[e, \theta e] \in \mathfrak{a}$. Since B is nonsingular on $\mathfrak{a}$, it is sufficient to show that $B(a, [e, \theta e]) = B(a, B(e, \theta e)x_\phi)$ for all $a \in \mathfrak{a}$. But

$$B(a, [e, \theta e]) = B([a, e], \theta e) = B(\phi(a)e, \theta e) = \phi(a)B(e, \theta e) = B(a, x_\phi)B(e, \theta e)$$

$$= B(a, B(e, \theta e)x_\phi),$$

proving the lemma. Q.E.D.

Let $\phi \in \Sigma$. Since $(\phi, \phi) \neq 0$ (see Lemma 2.2), we can define

$$h_\phi = 2x_\phi/(\phi, \phi) \in \mathfrak{a},$$

and we have $\phi(h_\phi) = 2$.

Also, since B_θ is a symmetric nonsingular form on $\mathfrak{g}^\phi$ (Lemma 3.2), there exists $e \in \mathfrak{g}^\phi$ such that $B_\theta(e, e) \neq 0$. Setting

$$e_\phi = (2/(\phi, \phi)B_\theta(e, e))^{1/2}e,$$

which we may do since k is algebraically closed, we get

$$B_\theta(e_\phi, e_\phi) = 2/(\phi, \phi).$$

Thus from Lemma 3.3, we have:

Lemma 3.4. $[h_\phi, e_\phi] = 2e_\phi$, $[h_\phi, -\theta e_\phi] = 2\theta e_\phi$ *and* $[e_\phi, -\theta e_\phi] = h_\phi$. *In particular,* $\{h_\phi, e_\phi, \theta e_\phi\}$ *spans a three-dimensional simple subalgebra* $\mathfrak{g}_\phi$ *of* $\mathfrak{g}$.

It is clear that $\mathfrak{g}_\phi$ is stable under θ, so that $\mathfrak{g}_\phi = \mathfrak{k}_\phi \oplus \mathfrak{p}_\phi$, where $\mathfrak{k}_\phi = \mathfrak{g}_\phi \cap \mathfrak{k}$ and $\mathfrak{p}_\phi = \mathfrak{g}_\phi \cap \mathfrak{p}$. Moreover, $(\mathfrak{g}_\phi, \theta|\mathfrak{g}_\phi)$ is a semisimple symmetric Lie algebra. We have

$$\mathfrak{k}_\phi = k(e_\phi + \theta e_\phi) \quad \text{and} \quad \mathfrak{p}_\phi = kh_\phi \oplus k(e_\phi - \theta e_\phi).$$

We shall use $\mathfrak{g}_\phi$ to show that the restriction to $\mathfrak{a}$ of every element of $S(\mathfrak{p}^*)^\mathfrak{k}$ is invariant under the Weyl reflection with respect to ϕ.

From Lemma 3.4, we have

$$[½(e_\phi + \theta e_\phi), h_\phi] = -(e_\phi - \theta e_\phi), \quad [½(e_\phi + \theta e_\phi), e_\phi - \theta e_\phi] = h_\phi$$

and $[\frac{1}{2}(e_\phi + \theta e_\phi), \mathfrak{t}] = 0$, where $\mathfrak{t} = \operatorname{Ker} \phi \subset \mathfrak{a}$.

For all $f \in S(\mathfrak{p}^*)$, $(\frac{1}{2}(e_\phi + \theta e_\phi) \cdot f)|(\mathfrak{p}_\phi \oplus \mathfrak{t}) = \frac{1}{2}(e_\phi + \theta e_\phi) \cdot (f|\mathfrak{p}_\phi \oplus \mathfrak{t})$. In particular, if $f \in S(\mathfrak{p}^*)^\mathfrak{k}$, then $f' = f|(\mathfrak{p}_\phi \oplus \mathfrak{t})$ is a $\mathfrak{k}_\phi$-annihilated polynomial function on $\mathfrak{p}_\phi \oplus \mathfrak{t}$, where $\mathfrak{k}_\phi = k(e_\phi \oplus \theta e_\phi)$ acts on $\mathfrak{p}_\phi \oplus \mathfrak{t}$ as indicated above. The determination of f' is a simple, standard problem in "classical invariant theory," which we proceed to solve.

Let $x = h_\phi + (-1)^{1/2}(e_\phi - \theta e_\phi)$, $y = h_\phi - (-1)^{1/2}(e_\phi - \theta e_\phi)$ and let $\{z_1, \ldots, z_n\}$ be a basis of $\mathfrak{t}$. Then the basis $x, y, z_1, \ldots, z_n$ of $\mathfrak{p}_\phi \oplus \mathfrak{t} = \mathfrak{p}_\phi + \mathfrak{a}$ diagonalizes the action of $\frac{1}{2}(-1)^{1/2}(e_\phi + \theta e_\phi)$, with eigenvalues -1, $1, 0, \ldots, 0$, respectively.

Let $X, Y, Z_1, \ldots, Z_n$ be the basis of $(\mathfrak{p}_\phi \oplus \mathfrak{t})^*$ dual to $x, y, z_1, \ldots, z_n$, so that f' is a polynomial in these variables. Moreover, $\frac{1}{2}(-1)^{1/2}(e_\phi + \theta e_\phi)$ acts on such a polynomial by the derivation law and the negative transpose of the action on $\mathfrak{p}_\phi \oplus \mathfrak{t}$. Hence $X, Y, Z_1, \ldots, Z_n$ is a basis of eigenvectors of $(\mathfrak{p}_\phi \oplus \mathfrak{t})^*$ with eigenvalues $1, -1, 0, \ldots, 0$, respectively.

Write

$$f' = \sum_{j,k \in \mathbf{Z}_+} X^j Y^k f_{jk}(Z_1, \ldots, Z_n),$$

where the f_{jk}'s are uniquely determined polynomials in the Z_i's. The invariance of f' under $\frac{1}{2}(-1)^{1/2}(e_\phi + \theta e_\phi)$ asserts that

$$\sum_{j,k \in \mathbf{Z}_+} (j-k) X^j Y^k f_{jk}(Z_1, \ldots, Z_n) = 0,$$

i.e., that $f_{jk} = 0$ for all pairs j, k such that $j \neq k$. Hence f' is $\frac{1}{2}(-1)^{1/2}(e_\phi + \theta e_\phi)$-invariant if and only if f' is of the form

$$f' = \sum_{j \in \mathbf{Z}_+} (XY)^j f_j(Z_1, \ldots, Z_n),$$

which the f_j's are polynomials in the Z_i's.

Now let $H = X + Y$ and $E = (-1)^{1/2}(X - Y)$, so that the basis $H, E, Z_1, \ldots, Z_n$ of $(\mathfrak{p}_\phi \oplus \mathfrak{t})^*$ is dual to the basis $h_\phi, e_\phi - \theta e_\phi, z_1, \ldots, z_n$ of $\mathfrak{p}_\phi \oplus \mathfrak{t}$. Then f' is of the form

$$f' = \sum_{j \in \mathbf{Z}_+} (H^2 + E^2)^j g_j(Z_1, \ldots, Z_n),$$

where the g_j's are polynomials in the Z_i's.

Since $H|\mathfrak{a}$ is a nonzero multiple of ϕ, $E|\mathfrak{a} = 0$ and each $Z_i|\mathfrak{a}$ annihilates h_ϕ, we have

$$f'|\mathfrak{a} = \sum_{j \in \mathbf{Z}_+} \phi^{2j} h_j,$$

where each h_j is a polynomial in linear functionals on $\mathfrak{a}$ which are orthogonal to ϕ with respect to $(\cdot,\cdot)$. We have shown that for all $f \in S(\mathfrak{p}^*)^{\mathfrak{k}}$, $f|\mathfrak{a} = f'|\mathfrak{a}$ is an element of $S(\mathfrak{a}^*)$ left fixed by the Weyl reflection with respect to ϕ. Since these reflections generate W as ϕ ranges through Σ, $f|\mathfrak{a} \in S(\mathfrak{a}^*)^W$. This proves the first part of the theorem.

We turn now to the injectivity of F_*. In the following proof, we need not assume that k is algebraically closed. We begin with some general comments on symmetric algebras.

Let V be a finite-dimensional vector space (over k), and for all $r \in \mathbf{Z}_+$, let $S^r(V)$ denote the rth homogeneous component of $S(V)$. There is a natural pairing $\{\cdot,\cdot\}$ between $S^r(V^*)$ and $S^r(V)$ given as follows:

$$\{f_1 \cdots f_r, v_1 \cdots v_r\} = \sum_{\sigma} \prod_{i=1}^{r} \langle f_i, v_{\sigma(i)}\rangle,$$

where $v_1, \ldots, v_r \in V$, $f_1, \ldots, f_r \in V^*$, $\langle\cdot,\cdot\rangle$ is the natural pairing between V^* and V and σ ranges through the group of permutations of $\{1, \ldots, r\}$. Then for all $v \in V$ and $f \in S^r(V^*)$, $\{f, v^r\} = r!f(v)$ (regarding f as a polynomial function on V on the right-hand side). We have two immediate consequences:

Lemma 3.5. (i) *$\{\cdot,\cdot\}$ is a nonsingular pairing.*

(ii) *Let Z be a Zariski dense subset of V (i.e., for all $f \in S(V^*)$, $f(Z) = 0$ implies $f = 0$). Then $\{z^r | z \in Z\}$ spans $S^r(V)$.*

Now $\mathfrak{k}$ acts naturally as derivations on $S(\mathfrak{p})$ and $S(\mathfrak{p}^*)$.

Lemma 3.6. *For each $r \in \mathbf{Z}_+$, the natural actions of $\mathfrak{k}$ on $S^r(\mathfrak{p}^*)$ and $S^r(\mathfrak{p})$ are contragredient under $\{\cdot,\cdot\}$.*

Proof. Let $x \in \mathfrak{k}$, $y \in \mathfrak{p}$ and $z \in \mathfrak{p}^*$. By Lemma 3.5(ii), it is sufficient to show that $\{x \cdot z^r, y^r\} = -\{z^r, x \cdot y^r\}$. But

$$\{x \cdot z^r, y^r\} = r\{(x \cdot z)z^{r-1}, y^r\} = rr!\langle x \cdot z, y\rangle\langle z, y\rangle^{r-1}$$

$$= -rr!\langle z, [x, y]\rangle\langle z, y\rangle^{r-1} = -r\{z^r, [x, y]y^{r-1}\} = -\{z^r, x \cdot y^r\},$$

and this proves the lemma. Q.E.D.

The next lemma is the crucial one. We give two proofs, the first inspired by P. Cartier's argument in [7, p. 18–20, Proposition 1], and the second due to G. McCollum.

Lemma 3.7. *Under the natural action of $\mathfrak{k}$ on $S^r(\mathfrak{p})$, $S^r(\mathfrak{a})$ generates $S^r(\mathfrak{p})$. In particular,*

$$S^r(\mathfrak{p}) = S^r(\mathfrak{a}) + \mathfrak{k} \cdot S^r(\mathfrak{p}).$$

Proof #1. It is clearly sufficient to prove the first statement. Since $\mathfrak{g} = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{\phi \in \Sigma} \mathfrak{g}^{\phi}$, $\mathfrak{p} = \mathfrak{a} \oplus \mathfrak{q}$, where $\mathfrak{q}$ is the span of $\{e - \theta e | e \in \mathfrak{g}^{\phi}, \phi \in \Sigma\}$. Now

$$S^r(\mathfrak{p}) = \coprod_{j=0}^{r} S^j(\mathfrak{q}) S^{r-j}(\mathfrak{a}).$$

It will be sufficient to prove by induction on j that the smallest $\mathfrak{k}$-invariant subspace T of $S^r(\mathfrak{p})$ containing $S^r(\mathfrak{a})$ also contains $S^j(\mathfrak{q})S^{r-j}(\mathfrak{a})$. This is clearly true for $j = 0$, so suppose it is true for $0, 1, \ldots, j$. We shall now prove it for $j + 1$. We assume that $j < r$.

Let $\phi \in \Sigma$, $e \in \mathfrak{g}^{\phi}$, $s \in S^j(\mathfrak{q})$ and $a \in \mathfrak{a}$. Then $e + \theta e \in \mathfrak{k}$, and

$$(e + \theta e) \cdot s a^{r-j} = ((e + \theta e) \cdot s) a^{r-j} - (r - j)\phi(a) s (e - \theta e) a^{r-(j+1)}$$

The left-hand side and the first term on the right are in T by the induction hypothesis, and so $\phi(a)s(e - \theta e)a^{r-(j+1)} \in T$. Let $Z = \{a \in \mathfrak{a} | \phi(a) \neq 0$ for all $\phi \in \Sigma\}$. Then Z is Zariski dense in $\mathfrak{a}$ since it is the subset of $\mathfrak{a}$ on which finitely many nonzero polynomial functions do not vanish; the fact that $S(\mathfrak{a}^*)$ is an integral domain implies easily that any such set is Zariski dense. Then for all $\phi \in \Sigma$, $e \in \mathfrak{g}^{\phi}$, $s \in S^j(\mathfrak{q})$ and $a \in Z$, $s(e - \theta e)a^{r-(j+1)} \in T$. But by Lemma 3.5(ii), $\{a^{r-(j+1)} | a \in Z\}$ spans $S^{r-(j+1)}(\mathfrak{a})$. Also, as ϕ, e and s vary, the terms $s(e - \theta e)$ span $S^{j+1}(\mathfrak{q})$. Thus we have shown that

$$S^{j+1}(\mathfrak{q})S^{r-(j+1)}(\mathfrak{a}) \subset T,$$

completing the induction. Q.E.D.

Proof #2 (McCollum). Use the first paragraph of Proof #1 and continue as follows:

Let $\phi \in \Sigma$ and choose $w \in \mathfrak{a}$ such that $\phi(w) = 1$. Let $\mathfrak{t} = \operatorname{Ker} \phi$, so that $\mathfrak{a} = kw \oplus \mathfrak{t}$. Now let $e \in g^{\phi}$, $s \in S^j(\mathfrak{q})$ and $t \in S^{r-j-i}(\mathfrak{t})$, where $1 \leq i \leq r - j$. Then $e + \theta e \in \mathfrak{k}$, and

$$(e + \theta e) \cdot s w^i t = ((e + \theta e) \cdot s) w^i t - i s (e - \theta e) w^{i-1} t + s w^i ((e + \theta e) \cdot t).$$

The left-hand side and the first term on the right are in T by the induction hypothesis, and the last term is zero because $t \in S(\mathfrak{t})$. Hence $s(e - \theta e)w^{i-1}t \in T$. But as i and t vary, the products $w^{i-1}t$ span $S^{r-(j+1)}(\mathfrak{a})$, so that $s(e - \theta e)S^{r-(j+1)}(\mathfrak{a}) \subset T$. Also, as ϕ, e and s vary, the products $s(e - \theta e)$ span $S^{j+1}(\mathfrak{q})$. Hence $S^{j+1}(\mathfrak{q})S^{r-(j+1)}(\mathfrak{a}) \subset T$, and this completes the induction. Q.E.D.

To complete the proof of the injectivity of F_*, let $f \in S(\mathfrak{p}^*)^{\mathfrak{k}}$ and assume $f | \mathfrak{a} = 0$. The homogeneous components of f are annihilated by $\mathfrak{k}$ since the decomposition

$$S(\mathfrak{p}^*) = \coprod_{j=0}^{\infty} S^r(\mathfrak{p}^*)$$

is a $\mathfrak{k}$-module decomposition. Also, the components of f vanish on $\mathfrak{a}$ because $\mathfrak{a}$ is closed under scalar multiplication. Hence we may assume $f \in S^r(\mathfrak{p}^*)^{\mathfrak{k}}$ for some $r \in \mathbf{Z}_+$. Consider the pairing $\{\cdot, \cdot\}$ between $S^r(\mathfrak{p}^*)$ and $S^r(\mathfrak{p})$. Now $\{f, a^r\} = 0$ for all $a \in \mathfrak{a}$, so that $\{f, S^r(\mathfrak{a})\} = 0$ by Lemma 3.5(ii). Also, for all $x \in \mathfrak{k}$ and $s \in S^r(\mathfrak{p})$, $\{f, x \cdot s\} = -\{x \cdot f, s\} = 0$, using Lemma 3.6. Thus $\{f, S^r(\mathfrak{p})\} = 0$ by Lemma 3.7, and $f = 0$ in view of the nonsingularity of $\{\cdot, \cdot\}$ (Lemma 3.5(i)). This proves the injectivity of F_*, and hence the theorem. Q.E.D.

Remark. In the Appendix, we shall give a vector-valued generalization of the injectivity of F_*.

In case dim $\mathfrak{a} = 1$, we get more information. We now assume that dim $\mathfrak{a} = 1$. The following result is clear:

Lemma 3.8. $S(\mathfrak{a}^*)^W$ *consists of the even polynomial functions on* $\mathfrak{a}$, *i.e., those polynomial functions* f *on* $\mathfrak{a}$ *such that* $f(a) = f(-a)$ *for all* $a \in \mathfrak{a}$. *If* f *is an arbitrary nonzero homogeneous quadratic polynomial function on* $\mathfrak{a}$, *then* f *generates* $S(\mathfrak{a}^*)^W$, *and* $S(\mathfrak{a}^*)^W = k[f]$ *is the polynomial algebra generated by* f.

The Killing form B of $\mathfrak{g}$ is nonsingular on $\mathfrak{a}$ (Lemma 2.2 or Lemma 3.2), and its restriction to $\mathfrak{p}$ is $\mathfrak{k}$-invariant. Thus the function b on $\mathfrak{p}$ defined by $p \mapsto B(p, p)$ is a homogeneous quadratic $\mathfrak{k}$-invariant polynomial function on $\mathfrak{p}$ whose restriction to $\mathfrak{a}$ is nonzero. Hence the last lemma implies:

Lemma 3.9. *The subalgebra* $k[b]$ *of* $S(\mathfrak{p}^*)^{\mathfrak{k}}$ *generated by* b *is the polynomial algebra generated by* b, *and* $F_* : k[b] \to S(\mathfrak{a}^*)^W$ *is an algebra isomorphism.*

In view of Theorem 3.1, we therefore have:

Theorem 3.10. *Suppose* dim $\mathfrak{a} = 1$. *Then* $F_* : S(\mathfrak{p}^*)^{\mathfrak{k}} \to S(\mathfrak{a}^*)^W$ *is an algebra isomorphism, and* $S(\mathfrak{p}^*)^{\mathfrak{k}} = k[b]$; *here* $k[b]$ *is the polynomial algebra generated by* b.

Since the restriction of B to $\mathfrak{p}$ is nonsingular and $\mathfrak{k}$-invariant, B induces a $\mathfrak{k}$-module isomorphism from the contragredient $\mathfrak{k}$-module $\mathfrak{p}^*$ to $\mathfrak{p}$, and hence a $\mathfrak{k}$-module and algebra isomorphism from $S(\mathfrak{p}^*)$ to $S(\mathfrak{p})$. Let $b_0 \in S(\mathfrak{p})$ be the image of b under this isomorphism, so that b_0 is the canonical quadratic element of $S(\mathfrak{p})$ associated with the restriction of B to $\mathfrak{p}$, and b_0 is annihilated by $\mathfrak{k}$. Let $S(\mathfrak{p})^{\mathfrak{k}}$ denote the subalgebra of $\mathfrak{k}$-annihilated vectors of $S(\mathfrak{p})$. From Theorem 3.10, we have:

Corollary 3.11. *Suppose* $\dim \mathfrak{a} = 1$. *Then* $S(\mathfrak{p})^{\mathfrak{k}}$ *is generated by* b_0, *so that* $S(\mathfrak{p})^{\mathfrak{k}} = k[b_0]$, *and* $k[b_0]$ *is the polynomial algebra generated by* b_0.

4. The Harish-Chandra map p_*. Let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ be the symmetric decomposition of a semisimple symmetric Lie algebra $(\mathfrak{g}, \theta)$ over a field k of characteristic zero, and let $\mathfrak{a}$ be a splitting Cartan subspace of $\mathfrak{p}$. Denote by $\Sigma \subset \mathfrak{a}^*$ the corresponding restricted root system and W the restricted Weyl group. Fix a positive system $\Sigma_+ \subset \Sigma$, and let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$ be the corresponding Iwasawa decomposition. Define $\rho \in \mathfrak{a}^*$ by the condition

$$\rho(a) = ½ \operatorname{tr}(\operatorname{ad} a|\mathfrak{n})$$

for all $a \in \mathfrak{a}$, or equivalently,

$$\rho = \frac{1}{2} \sum_{\phi \in \Sigma_+} (\dim \mathfrak{g}^{\phi})\phi.$$

Let $\mathfrak{G}$ be the universal enveloping algebra of $\mathfrak{g}$, and let $\mathfrak{K}$, $\mathfrak{A}$ and $\mathfrak{N}$ be the universal enveloping algebras of $\mathfrak{k}$, $\mathfrak{a}$ and $\mathfrak{n}$, respectively, regarded as canonically embedded in $\mathfrak{G}$, by the Poincaré-Birkhoff-Witt theorem. The multiplication map in $\mathfrak{G}$ induces a linear isomorphism $\mathfrak{G} \simeq \mathfrak{K} \otimes \mathfrak{A} \otimes \mathfrak{N}$, by the same theorem. (In this section, $\otimes$ denotes tensor product over k.) Identifying $\mathfrak{G}$ with $\mathfrak{K} \otimes \mathfrak{A} \otimes \mathfrak{N}$, we have

$$\begin{aligned} \mathfrak{G} &= \mathfrak{K} \otimes \mathfrak{A} \otimes (k \cdot 1 \oplus \mathfrak{N}\mathfrak{n}) = \mathfrak{K} \otimes \mathfrak{A} \oplus \mathfrak{G}\mathfrak{n} \\ &= (k \cdot 1 \oplus \mathfrak{k}\mathfrak{K}) \otimes \mathfrak{A} \oplus \mathfrak{G}\mathfrak{n} = \mathfrak{A} \oplus \mathfrak{k}\mathfrak{K}\mathfrak{A} \oplus \mathfrak{G}\mathfrak{n}. \end{aligned}$$

Let $p: \mathfrak{G} \to \mathfrak{A}$ be the projection with respect to this decomposition. Since

$$\mathfrak{k}\mathfrak{G} = \mathfrak{k}\mathfrak{K}\mathfrak{A}\mathfrak{N} = \mathfrak{k}\mathfrak{K}\mathfrak{A}(k \cdot 1 + \mathfrak{N}\mathfrak{n}) \subset \mathfrak{k}\mathfrak{K}\mathfrak{A} + \mathfrak{G}\mathfrak{n},$$

we have

$$\mathfrak{G} = \mathfrak{A} \oplus (\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n}),$$

and p is also the projection to $\mathfrak{A}$ with respect to this decomposition.

Since $\mathfrak{a}$ is abelian, $\mathfrak{A}$ may be identified with the symmetric algebra $S(\mathfrak{a})$, and hence with the algebra of polynomial functions on $\mathfrak{a}^*$. Every affine automorphism T of $\mathfrak{a}^*$ gives rise to an algebra automorphism $T^{\wedge}$ of $\mathfrak{A} = S(\mathfrak{a})$, defined by $(T^{\wedge}f)(\lambda) = f(T^{-1}\lambda)$ for all $f \in \mathfrak{A}$, $\lambda \in \mathfrak{a}^*$. When T is translation by ρ, i.e., the map which takes $\lambda \in \mathfrak{a}^*$ to $\lambda + \rho$, we denote $T^{\wedge}$ by τ. Then $(\tau f)(\lambda) = f(\lambda - \rho)$ for all $f \in \mathfrak{A}$ and $\lambda \in \mathfrak{a}^*$, and τ may be characterized as the unique automorphism of $\mathfrak{A}$ which takes $a \in \mathfrak{a}$ to $a - \rho(a)$.

Now W is a group of linear automorphisms of $\mathfrak{a}^*$. For all $s \in W$, $s^{\wedge}$ is the unique automorphism of $\mathfrak{A}$ which acts on $\mathfrak{a}$ according to the contragredient of the action of s on $\mathfrak{a}^*$. Moreover, W acts as a group of automorphisms of $\mathfrak{A}$ in this way. Let $\mathfrak{A}^W$ be the algebra of W-invariants in $\mathfrak{A}$.

Let $\mathfrak{G}^{\mathfrak{k}}$ denote the centralizer of $\mathfrak{k}$ in $\mathfrak{G}$, and let p_* be the map $(\tau\circ p)|\mathfrak{G}^{\mathfrak{k}}$, so that $p_*:\mathfrak{G}^{\mathfrak{k}} \to \mathfrak{A}$.

Theorem 4.1. *The map* $p_*:\mathfrak{G}^{\mathfrak{k}} \to \mathfrak{A}$ *is an algebra homomorphism with kernel* $\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G} = \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}\mathfrak{k}$ *and image contained in* $\mathfrak{A}^W$.

Proof. The fact that p_* is a homomorphism is easy: Let $x, y \in \mathfrak{G}^{\mathfrak{k}}$, and write

$$x \equiv a \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})), \quad y \equiv b \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})),$$

where $a, b \in \mathfrak{A}$; then $a = p(x)$ and $b = p(y)$. We have

$$\begin{aligned} xy &\equiv xb \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})) \quad (\text{since } x \in \mathfrak{G}\ ) \\ &\equiv ab \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})), \end{aligned}$$

since $[\mathfrak{a}, \mathfrak{n}] \subset \mathfrak{n}$. Hence

$$xy = p(x)p(y) \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})),$$

and so $p(xy) = p(x)p(y)$. Since τ is a homomorphism, p_* is also a homomorphism.

Now $\operatorname{Ker} p_* = \operatorname{Ker} p|\mathfrak{G}^{\mathfrak{k}}$, and the fact that $\operatorname{Ker} p|\mathfrak{G}^{\mathfrak{k}} = \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G} = \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}\mathfrak{k}$ is proved in [1, Proposition 9.2.15]; the proof is essentially that of [5, Remark 4.6]. (Actually, the cited result deals with the projection to $\mathfrak{A}$ with respect to the decomposition $\mathfrak{G} = \mathfrak{A} \oplus (\mathfrak{G}\mathfrak{k} + \mathfrak{n}\mathfrak{G})$, but we get the desired result either by applying the transpose antiautomorphism of $\mathfrak{G}$ or by imitating the argument in [1] or [5] for the present map p.) The cited proof simplifies somewhat in the present special case. Also, in place of the argument in [5, Proof of Lemma 4.1] (see also [6] and [1, Lemma 9.2.7, part (b) of the proof]), which uses methods from the theory of Lie or algebraic groups, we can instead use the injectivity assertion in Theorem 3.1 above, whose proof of course does not involve Lie or algebraic groups. Incidentally, in the Appendix, we show how the injectivity argument in Theorem 3.1 can be used to give a proof of [1, Lemma 9.2.7(b)] in full generality, and even to generalize it, without algebraic groups. The cited proof of the equality $\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G} = \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}\mathfrak{k}$ is independent of the assertion about the kernel of p_*. None of the above requires k to be algebraically closed.

We must now show that $p_*(\mathfrak{G}^{\mathfrak{k}}) \subset \mathfrak{A}^W$. We shall do this first when $\dim \mathfrak{a} = 1$, in which case we shall also show that the image of p_* is exactly $\mathfrak{A}^W$. We shall finally reduce the general case to this case.

Assume now that $\dim \mathfrak{a} = 1$. In proving that $p_*(\mathfrak{G}^{\mathfrak{k}}) = \mathfrak{A}^W$, we may, and do, also assume that k is algebraically closed. In fact, however, this assumption will only be used in proving Lemmas 4.2, 4.3 and 4.4.

Let $\lambda: S(\mathfrak{g}) \to \mathfrak{G}$ be the canonical linear isomorphism from the symmetric algebra of $\mathfrak{g}$ to the universal enveloping algebra, so that λ is defined by the formula

$$\lambda(g_1 \cdots g_n) = \frac{1}{n!} \sum_{\sigma} g_{\sigma(1)} \cdots g_{\sigma(n)}$$

for all $n \in \mathbf{Z}_+$ and $g_i \in \mathfrak{g}$; here the product on the left is taken in $S(\mathfrak{g})$, the products on the right are taken in $\mathfrak{G}$, and σ ranges through the group of permutations of $\{1, \ldots, n\}$ (see [1, §2.4]). For all $g \in \mathfrak{g}$ and $n \in \mathbf{Z}_+$, $\lambda(g^n) = g^n$, and this condition determines λ since the powers of elements of $\mathfrak{g}$ span $S(\mathfrak{g})$ (see Lemma 3.5(ii)). Moreover, λ is a $\mathfrak{g}$-module isomorphism with respect to the natural actions of $\mathfrak{g}$ on $S(\mathfrak{g})$ and $\mathfrak{G}$ as derivations (see [1, §2.4.10]).

Let B be the Killing form of $\mathfrak{g}$, so that B is nonsingular on $\mathfrak{p}$. Let b_0 be the canonical quadratic element of $S(\mathfrak{p})^{\mathfrak{k}}$ associated with the restriction of B to $\mathfrak{p}$, as at the end of §3, and set $u_0 = \lambda(b_0) \in \lambda(S(\mathfrak{p})^{\mathfrak{k}}) \subset \mathfrak{G}^{\mathfrak{k}}$. Our goal now is to compute $p_*(u_0)$.

As in §3, we define the nonsingular symmetric form B_θ on $\mathfrak{g}$ by $B_\theta(x, y) = -B(x, \theta y)$ for all $x, y \in \mathfrak{g}$. Then B_θ is nonsingular on $\mathfrak{a} \oplus \mathfrak{n}$, and $B_\theta(\mathfrak{a}, \mathfrak{n}) = 0$ (Lemma 3.2).

Lemma 4.2. *Define the linear map* $f: \mathfrak{a} \oplus \mathfrak{n} \to \mathfrak{g}$ *by the conditions* $f = 1$ *on* $\mathfrak{a}$ *and* $f = 2^{-1/2}(1 - \theta)$ *on* $\mathfrak{n}$. *Then* $f(\mathfrak{a} \oplus \mathfrak{n}) \subset \mathfrak{p}$, *and* $f: \mathfrak{a} \oplus \mathfrak{n} \to \mathfrak{p}$ *is a linear isomorphism which is an isometry from* B_θ *to* B.

Proof. Clearly, $f(\mathfrak{a} \oplus \mathfrak{n}) \subset \mathfrak{p}$. From the Iwasawa decomposition, it follows that $(1 - \theta): \mathfrak{a} \oplus \mathfrak{n} \to \mathfrak{p}$ is a·linear isomorphism, and so $f: \mathfrak{a} \oplus \mathfrak{n} \to \mathfrak{p}$ is also a linear isomorphism, since $f = \frac{1}{2}(1 - \theta)$ on $\mathfrak{a}$ and $2^{-1/2}(1 - \theta)$ on $\mathfrak{n}$.

We must now show that for all $x, y \in \mathfrak{a} \oplus \mathfrak{n}$, $B(f(x), f(y)) = B_\theta(x, y)$. This is true if $x, y \in \mathfrak{a}$ since $B_\theta = B$ on $\mathfrak{a}$. Let $x \in \mathfrak{a}$, $y \in \mathfrak{n}$. Then $B_\theta(x, y) = 0$. But

$$B(f(x), f(y)) = 2^{-\frac{1}{2}} B(x, y - \theta y) = 2^{-\frac{1}{2}} B(x, y) - 2^{-\frac{1}{2}} B(x, \theta y) = 0,$$

so that the desired relation again holds. Finally, let $x, y \in \mathfrak{n}$. Then

$$B(f(x), f(y)) = \tfrac{1}{2} B(x - \theta x, y - \theta y) = -\tfrac{1}{2} B(x, \theta y) - \tfrac{1}{2} B(\theta x, y) = B_\theta(x, y).$$

The lemma follows from the bilinearity and symmetry of B_θ and B. Q.E.D.

Let $\alpha \in \Sigma_+$ be the (unique) simple restricted root, so that $\mathfrak{n} = \mathfrak{g}^{\alpha} \oplus \mathfrak{g}^{2\alpha}$, and $\mathfrak{g}^{2\alpha}$ may be zero. Since k is algebraically closed and B_θ is nonsingular on $\mathfrak{a}$, $\mathfrak{g}^{\alpha}$ and $\mathfrak{g}^{2\alpha}$ (Lemma 3.2), we may choose $e_1 \in \mathfrak{a}$ such that $B_\theta(e_1, e_1) = 1$ and B_θ-orthonormal bases $e_1^{\alpha}, \ldots, e_r^{\alpha}$ of $\mathfrak{g}^{\alpha}$ and $e_1^{2\alpha}, \ldots, e_s^{2\alpha}$ of $\mathfrak{g}^{2\alpha}$. The orthogonality of the decomposition $\mathfrak{a} \oplus \mathfrak{g}^{\alpha} \oplus \mathfrak{g}^{2\alpha}$ (Lemma 3.2) implies that $e_1, e_1^\alpha, \dots, e_r^\alpha, e_1^{2\alpha}, \dots, e_s^{2\alpha}$ is a B_θ-orthonormal basis of $\mathfrak{a} \oplus \mathfrak{n}$. Hence by Lemma 4.2, $f(e_1), f(e_1^\alpha), \dots, f(e_r^\alpha), f(e_1^{2\alpha}), \dots, f(e_s^{2\alpha})$ is a B-orthonormal basis of $\mathfrak{p}$. This basis is $e_1, 2^{-1/2}(e_1^\alpha - \theta e_1^\alpha), \dots, 2^{-1/2}(e_1^{2\alpha} - \theta e_1^{2\alpha}), \dots$. But if $x_1, \dots, x_t$ is any B-orthonormal basis of $\mathfrak{p}$, $b_0 = x_1^2 + \cdots + x_t^2$ in $S(\mathfrak{p})$, and hence $u_0 = \lambda(b_0) = x_1^2 + \cdots + x_t^2$ in $\mathfrak{G}$. Thus

$$u_0 = e_1^2 + \tfrac{1}{2}(e_1^\alpha - \theta e_1^\alpha)^2 + \cdots + \tfrac{1}{2}(e_r^\alpha - \theta e_r^\alpha)^2$$

$$+ \tfrac{1}{2}(e_1^{2\alpha} - \theta e_1^{2\alpha})^2 + \cdots + \tfrac{1}{2}(e_s^{2\alpha} - \theta e_s^{2\alpha})^2.$$

To compute $p_*(u_0)$, first note that $p_*(e_1^2) = (r \circ p)(e_1^2) = r(e_1^2) = (e_1 - \rho(e_1))^2$. Now let $e = e_i^\alpha (1 \leq i \leq r)$ or $e_j^{2\alpha} (1 \leq j \leq s)$. Then

$$\begin{aligned}
\tfrac{1}{2}(e - \theta e)^2 &= \tfrac{1}{2}(2e - (e + \theta e))^2 \\
&= \tfrac{1}{2}(4e^2 + (e + \theta e)^2 - 2e(e + \theta e) - 2(e + \theta e)e) \\
&\equiv -e(e + \theta e) \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})) \\
&\equiv -e\theta e \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})) \\
&\equiv -[e, \theta e] \ (\mathrm{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})).
\end{aligned}$$

Recall from §3 that x_α is the unique element of $\mathfrak{a}$ such that $B(x_\alpha, x) = \alpha(x)$ for all $x \in \mathfrak{a}$ and that $x_{2\alpha} = 2x_\alpha$ (if $2\alpha \in \Sigma$). Since $B_\theta(e, e) = 1$, Lemma 3.3 implies that $[e, \theta e] = -x_\alpha$ if $e \in \mathfrak{g}^\alpha$ and $[e, \theta e] = -2x_\alpha$ if $e \in \mathfrak{g}^{2\alpha}$. Thus from the above computation,

$$p(u_0) = e_1^2 + (r + 2s)x_\alpha = e_1^2 + (\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha})x_\alpha,$$

and hence

$$p_*(u_0) = (e_1 - \rho(e_1))^2 + (\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha})(x_\alpha - \rho(x_\alpha)).$$

Let w be the unique element of $\mathfrak{a}$ such that $\alpha(w) = 1$. Then by the definition of ρ,

$$\rho(w) = \tfrac{1}{2}(\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha}).$$

Let $w = ce_1$ and $x_\alpha = de_1$ $(c, d \in k)$. Then since $B(x_\alpha, w) = \alpha(w) = 1$ and $B(e_1, e_1) = B_\theta(e_1, e_1) = 1$, we have that $cd = 1$. Thus

$$\begin{aligned}
p_*(u_0) &= (e_1 - \rho(e_1))^2 + 2\rho(w)(x_\alpha - \rho(x_\alpha)) \\
&= (e_1 - \rho(e_1))^2 + 2cd\rho(e_1)(e_1 - \rho(e_1)) \\
&= (e_1 - \rho(e_1))^2 + 2\rho(e_1)(e_1 - \rho(e_1)) \\
&= e_1^2 - \rho(e_1)^2.
\end{aligned}$$

Summarizing, we have proved:

Lemma 4.3. *Assuming that* $\dim \mathfrak{a} = 1$ *and that* k *is algebraically closed, choose* $e_1 \in \mathfrak{a}$ *such that* $B(e_1, e_1) = 1$. *Then*

$$p_*(u_0) = e_1^2 - \rho(e_1)^2 = (e_1 + \rho(e_1))(e_1 - \rho(e_1)).$$

Since B is nonsingular on $\mathfrak{a}$, we can reformulate the last lemma as follows:

Lemma 4.4. *Assume* $\dim \mathfrak{a} = 1$, *and let* $e \in \mathfrak{a}$, $e \neq 0$. *Then* $B(e, e) \neq 0$, *and*

$$p_*(u_0) = (e^2 - \rho(e)^2)/B(e, e) = (e + \rho(e))(e - \rho(e))/B(e, e).$$

The point is that this holds even if k is not algebraically closed, and from now on we can drop the algebraic closure assumption.

Now clearly $e^2 - \rho(e)^2 \in \mathfrak{A}^W$, and since this element is quadratic (although not homogeneous), it generates $\mathfrak{A}^W$, and in fact $\mathfrak{A}^W = k[e^2 - \rho(e)^2]$ is the polynomial algebra generated by $e^2 - \rho(e)^2$. But $u_0 \in \mathfrak{G}^{\mathfrak{k}}$, and $p_*\colon \mathfrak{G}^{\mathfrak{k}} \to \mathfrak{A}$ is an algebra homomorphism. Hence we have:

Lemma 4.5. *The subalgebra* $k[u_0]$ *of* $\mathfrak{G}^{\mathfrak{k}}$ *generated by* u_0 *is isomorphic to the polynomial algebra generated by* u_0; $p_*(k[u_0]) \subset \mathfrak{A}^W$; *and* $p_*\colon k[u_0] \to \mathfrak{A}^W$ *is an algebra isomorphism. In particular,* $p_*(\mathfrak{G}^{\mathfrak{k}}) \supset \mathfrak{A}^W$.

To complete the proof that $p_*(\mathfrak{G}^{\mathfrak{k}}) = \mathfrak{A}^W$ when $\dim \mathfrak{a} = 1$, we need one last lemma:

Lemma 4.6. $\mathfrak{G}^{\mathfrak{k}} = (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) \oplus k[u_0]$.

Proof. Let $\mathfrak{G}_0 \subset \mathfrak{G}_1 \subset \mathfrak{G}_2 \subset \cdots$ be the standard filtration of $\mathfrak{G}$ and $S_0(\mathfrak{p}) \subset S_1(\mathfrak{p}) \subset S_2(\mathfrak{p}) \subset \cdots$ the standard filtration of $S(\mathfrak{p})$, so that for all $r \in \mathbf{Z}_+$, $S_r(\mathfrak{p}) = \coprod_{j=0}^{r} S^j(\mathfrak{p})$. The multiplication map in $\mathfrak{G}$ induces a linear isomorphism $\mathfrak{G} \simeq \mathfrak{K} \otimes \lambda(S(\mathfrak{p}))$, and $\mathfrak{G}_r \subset \mathfrak{K} \otimes \lambda(S_r(\mathfrak{p}))$ for all $r \in \mathbf{Z}_+$ (see [1, Proposition 2.4.15 and its proof]). Thus

$$\mathfrak{G}_r \subset (\mathfrak{k}\mathfrak{K} \oplus k \cdot 1) \otimes \lambda(S_r(\mathfrak{p})) \subset \mathfrak{k}\mathfrak{G} \oplus \lambda(S_r(\mathfrak{p})).$$

Since the decomposition on the right is a $\mathfrak{k}$-module decomposition,

$$\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}_r \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) \oplus \lambda(S(\mathfrak{p})^{\mathfrak{k}} \cap S_r(\mathfrak{p})).$$

But $S(\mathfrak{p})^{\mathfrak{k}} = k[b_0]$ (Corollary 3.11), and so

$$(*) \qquad \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}_r \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) \oplus \lambda(k[b_0] \cap S_r(\mathfrak{p})).$$

Now the sum $(\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0]$ in the statement of the lemma is direct by Lemma 4.5, since $\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G} \subset \operatorname{Ker} p_*$. Hence to prove the lemma it is sufficient to show that $\mathfrak{G}^{\mathfrak{k}} \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0]$. We shall show by induction on $r \in \mathbf{Z}_+$ that $\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}_r \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0]$. This is trivial if $r = 0$. Assume it is true for r. To prove it for $r + 1$, note that by $(*)$ it is sufficient to show that

$$\lambda(k[b_0] \cap S_{r+1}(\mathfrak{p})) \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0].$$

If r is even, we are done because $k[b_0] \cap S_{r+1}(\mathfrak{p}) = k[b_0] \cap S_r(\mathfrak{p})$, and the induction hypothesis implies the result. Suppose r is odd. In view of the induction hypothesis, it is sufficient to show that $\lambda(b_0^{(r+1)/2}) \in (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0]$. But

$$\lambda(b_0^{(r+1)/2}) \equiv \lambda(b_0^{(r-1)/2})\lambda(b_0) \pmod{\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{G}_r}.$$

(Indeed, for all $x \in S_m(\mathfrak{g})$, $y \in S_n(\mathfrak{g})$, we have $\lambda(xy) \equiv \lambda(x)\lambda(y) \pmod{\mathfrak{G}_{m+n-1}}$.) Again by the induction hypothesis, $\lambda(b_0^{(r-1)/2}) \subset (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0]$, so that

$$\lambda(b_0^{(r-1)/2})\lambda(b_0) = \lambda(b_0^{(r-1)/2})u_0 \in (\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}) + k[u_0].$$

A final application of the induction hypothesis proves the desired result. Q.E.D.

We now summarize our conclusions for the case $\dim \mathfrak{a} = 1$. From Lemmas 4.4, 4.5 and 4.6, we have:

Theorem 4.7. *Assume* $\dim \mathfrak{a} = 1$. *The homomorphism* $p_* : \mathfrak{G}^{\mathfrak{k}} \to \mathfrak{A}$ *has kernel* $\mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}$ *and image* $\mathfrak{A}^W$. *Let* b_0 *be the canonical quadratic element of* $S(\mathfrak{p})$ *associated with the restriction of the Killing form of* $\mathfrak{g}$ *to* $\mathfrak{p}$ *(see the end of* §3), *and let* $u_0 = \lambda(b_0)$, *so that* $u_0 \in \mathfrak{G}^{\mathfrak{k}}$. *Then the subalgebra* $k[u_0]$ *of* $\mathfrak{G}^{\mathfrak{k}}$ *generated by* u_0 *is isomorphic to the polynomial algebra generated by* u_0, *and* $p_* : k[u_0] \to \mathfrak{A}^W$ *is an algebra isomorphism. Moreover,*

$$p_*(u_0) = (e^2 - \rho(e)^2)/B(e, e),$$

where e *is an arbitrary nonzero element of* $\mathfrak{a}$.

Note that we did not have to refer to the general result on $\operatorname{Ker} p_*$ to show that $\operatorname{Ker} p_* = \mathfrak{G}^{\mathfrak{k}} \cap \mathfrak{k}\mathfrak{G}$ when $\dim \mathfrak{a} = 1$.

We must finally prove that $p_*(\mathfrak{G}^{\mathfrak{k}}) \subset \mathfrak{A}^W$ when $\dim \mathfrak{a}$ is arbitrary. We shall do this by applying Theorem 4.7 to certain semisimple subalgebras of $\mathfrak{g}$ associated with the simple restricted roots.

Assume then that $\dim \mathfrak{a}$ is arbitrary, and fix a simple restricted root α. Let $\mathfrak{m}$ be the centralizer of $\mathfrak{a}$ in $\mathfrak{k}$, and set

$$\mathfrak{g}_\alpha = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{j=\pm1,\pm2} \mathfrak{g}^{j\alpha} = \coprod_{j=-2}^{2} \mathfrak{g}^{j\alpha},$$

where $\mathfrak{g}^{2\alpha}$ and $\mathfrak{g}^{-2\alpha}$ might be zero. Then $\mathfrak{g}_\alpha$ is a subalgebra of $\mathfrak{g}$. Let Σ_α denote the set of positive restricted roots not proportional to α, and let

$$\mathfrak{n}^\alpha = \coprod_{\phi \in \Sigma_\alpha} \mathfrak{g}^\phi.$$

The simplicity of α implies that if $\beta \in \Sigma_\alpha$ and γ is either a positive restricted root or a restricted root proportional to α, then $\beta + \gamma \in \Sigma_\alpha$ if $\beta + \alpha$ is a restricted root. Hence $\mathfrak{n}^\alpha$ is a subalgebra of $\mathfrak{n}$, and $[\mathfrak{g}_\alpha, \mathfrak{n}^\alpha] \subset \mathfrak{n}^\alpha$. Also, setting $\mathfrak{n}_\alpha = \mathfrak{g}^\alpha \oplus \mathfrak{g}^{2\alpha}$, we have $\mathfrak{n} = \mathfrak{n}_\alpha \oplus \mathfrak{n}^\alpha$.

We claim that $\mathfrak{g}_\alpha$ is reductive in $\mathfrak{g}$. In fact, $\operatorname{Ker} \alpha$ is a subspace of $\mathfrak{a}$ and hence a subalgebra of $\mathfrak{g}$ reductive in $\mathfrak{g}$. But $\mathfrak{g}_\alpha$ is exactly the centralizer of $\operatorname{Ker} \alpha$ in $\mathfrak{g}$. The claim now follows from [1, Proposition 1.7.7].

Now $\mathfrak{g}_\alpha$ is stable under θ, so that $\mathfrak{g}_\alpha = \mathfrak{k}_\alpha \oplus \mathfrak{p}_\alpha$, where $\mathfrak{k}_\alpha = \mathfrak{g}_\alpha \cap \mathfrak{k}$ and $\mathfrak{p}_\alpha = \mathfrak{g}_\alpha \cap \mathfrak{p}$. Moreover, $\mathfrak{g}_\alpha$ is a reductive Lie algebra since it is reductive in $\mathfrak{g}$. Hence $\mathfrak{g}_1 = [\mathfrak{g}_\alpha, \mathfrak{g}_\alpha]$ is a semisimple Lie algebra and $\mathfrak{g}_\alpha = \mathfrak{g}_1 \oplus \mathfrak{c}$, where $\mathfrak{c}$ is the center of $\mathfrak{g}_\alpha$, and both $\mathfrak{g}_1$ and $\mathfrak{c}$ are stable under θ. Thus if we set $\theta_1 = \theta | \mathfrak{g}_1$, $\mathfrak{k}_1 = \mathfrak{g}_1 \cap \mathfrak{k}$, $\mathfrak{p}_1 = \mathfrak{g}_1 \cap \mathfrak{p}$, $\mathfrak{c}_+ = \mathfrak{c} \cap \mathfrak{k}$ and $\mathfrak{c}_- = \mathfrak{c} \cap \mathfrak{p}$, then $(\mathfrak{g}_1, \theta_1)$ is a semisimple symmetric Lie algebra with symmetric decomposition $\mathfrak{g}_1 = \mathfrak{k}_1 \oplus \mathfrak{p}_1$, and we also have $\mathfrak{c} = \mathfrak{c}_+ \oplus \mathfrak{c}_-$, $\mathfrak{k}_\alpha = \mathfrak{k}_1 \oplus \mathfrak{c}_+$ and $\mathfrak{p}_\alpha = \mathfrak{p}_1 \oplus \mathfrak{c}_-$.

Let $x_\alpha \in \mathfrak{a}$ be the unique element such that $B(x_\alpha, a) = \alpha(a)$ for all $a \in \mathfrak{a}$, where B is the Killing form of $\mathfrak{g}$. Then $\mathfrak{a} = kx_\alpha \oplus \operatorname{Ker} \alpha$.

Lemma 4.8. *We have*

$$\mathfrak{g}_1 = (\mathfrak{g}_1 \cap \mathfrak{m}) \oplus kx_\alpha \oplus \coprod_{j=\pm1,\pm2} \mathfrak{g}^{j\alpha}$$

and

$$\mathfrak{c} = (\mathfrak{c} \cap \mathfrak{m}) \oplus \operatorname{Ker} \alpha.$$

In particular, $\mathfrak{c}_+ = \mathfrak{c} \cap \mathfrak{m}$ *and* $\mathfrak{c}_- = \operatorname{Ker} \alpha$.

Proof. Clearly $\coprod \mathfrak{g}^{j\alpha} \subset \mathfrak{g}_1$, and so $\mathfrak{g}_1 = (\mathfrak{g}_1 \cap \mathfrak{m}) \oplus (\mathfrak{g}_1 \cap \mathfrak{a}) \oplus \coprod \mathfrak{g}^{j\alpha}$. To determine $\mathfrak{g}_1 \cap \mathfrak{a}$, recall that the symmetric bilinear form B_θ is nonsingular on $\mathfrak{g}^\alpha$ (see Lemma 3.2),and so we may choose $e \in \mathfrak{g}^\alpha$ such that $B_\theta(e, e) \neq 0$. But then Lemma 3.3 implies that $[e, \theta e]$ is a nonzero multiple of x_α. This shows that $kx_\alpha \subset \mathfrak{g}_1 \cap \mathfrak{a}$. On the other hand, $\operatorname{Ker} \alpha \subset \mathfrak{c}_-$, and $\mathfrak{c}_- \subset \mathfrak{a}$ because $\mathfrak{a}$ is its own centralizer in $\mathfrak{p}$. Since $\mathfrak{a} = kx_\alpha \oplus \operatorname{Ker} \alpha$ and $(\mathfrak{g}_1 \cap \mathfrak{a}) \cap \mathfrak{c}_- \subset \mathfrak{g}_1 \cap \mathfrak{c} = 0$, we must have $\mathfrak{g}_1 \cap \mathfrak{a} = kx_\alpha$ and $\mathfrak{c}_- = \operatorname{Ker} \alpha$. The rest of the lemma is clear. Q.E.D.

Lemma 4.9. *Let* $\mathfrak{a}_1 = kx_\alpha$. *Then* $\mathfrak{a}_1$ *is a splitting Cartan subspace of* $\mathfrak{p}_1$, *for the semisimple symmetric Lie algebra* $(\mathfrak{g}_1, \theta_1)$.

Proof. Clearly, $\mathfrak{a}_1$ is an abelian subspace of $\mathfrak{p}_1$ which is reductive in $\mathfrak{g}_1$. We must show that $\mathfrak{a}_1$ is its own centralizer in $\mathfrak{p}_1$. But from Lemma 4.8, the centralizer of $\mathfrak{a}_1$ in $\mathfrak{g}_1$ is $(\mathfrak{g}_1 \cap \mathfrak{m}) \oplus \mathfrak{a}_1$, and this implies the desired result. Q.E.D.

Let $\alpha_1 = \alpha|\mathfrak{a}_1$, so that $\alpha_1 \in \mathfrak{a}_1^*$. Then the restricted roots for $(\mathfrak{g}_1, \theta_1)$ with respect to $\mathfrak{a}_1$ are $\pm\alpha_1$ and possibly $\pm 2\alpha_1$ (depending on whether $\pm 2\alpha$ are roots for $\mathfrak{g}$). Choose α_1 (and possibly $2\alpha_1$) as the positive restricted roots, and let $\mathfrak{n}_1$ be the sum of the positive restricted root spaces in $\mathfrak{g}_1$. Then the corresponding Iwasawa decomposition of $\mathfrak{g}_1$ is $\mathfrak{g}_1 = \mathfrak{k}_1 \oplus \mathfrak{a}_1 \oplus \mathfrak{n}_1$. Moreover, $\mathfrak{n}_1 = \mathfrak{n}_\alpha$ as previously defined. Furthermore, the Iwasawa decomposition of $\mathfrak{g}_1$ is compatible with that of $\mathfrak{g}$, in the sense that $\mathfrak{k}_1 = \mathfrak{g}_1 \cap \mathfrak{k}$, $\mathfrak{a}_1 = \mathfrak{g}_1 \cap \mathfrak{a}$ and $\mathfrak{n}_1 = \mathfrak{g}_1 \cap \mathfrak{n}$.

Our goal now is to express the mapping $p: \mathcal{G} \to \mathcal{A}$ in a form which relates it to the corresponding mapping for $\mathfrak{g}_1$.

Let $\mathcal{G}_\alpha, \mathcal{K}_\alpha, \mathcal{N}_\alpha$ and $\mathcal{N}^\alpha$ denote the universal enveloping algebras of $\mathfrak{g}_\alpha$, $\mathfrak{k}_\alpha$, $\mathfrak{n}_\alpha$ and $\mathfrak{n}^\alpha$, respectively, regarded as canonically embedded in $\mathcal{G}$. Then regarding the following equalities as canonical linear isomorphisms, we have

$$\mathcal{G} = \mathcal{K} \otimes \mathcal{A} \otimes \mathcal{N} = \mathcal{K} \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \otimes \mathcal{N}^\alpha = \mathcal{K} \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \otimes (k \cdot 1 \oplus \mathcal{N}^\alpha \mathfrak{n}^\alpha)$$

$$= \mathcal{K} \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \oplus \mathcal{G}\mathfrak{n}^\alpha.$$

Now let $\mathfrak{r}$ be an arbitrary linear complement of $\mathfrak{k}_\alpha$ in $\mathfrak{k}$, let $\lambda: S(\mathfrak{g}) \to \mathcal{G}$ denote the canonical linear isomorphism, and let $S_*(\mathfrak{r})$ denote the ideal $\amalg_{r=1}^\infty S^r(\mathfrak{r})$ of $S(\mathfrak{r})$. Then

$$\mathcal{K} = \lambda(S(\mathfrak{r})) \otimes \mathcal{K}_\alpha$$

(see [1, proof of Proposition 2.4.15])

$$= \lambda(k \cdot 1 \oplus S_*(\mathfrak{r})) \otimes \mathcal{K}_\alpha = (k \cdot 1 \oplus \lambda(S_*(\mathfrak{r}))) \otimes \mathcal{K}_\alpha$$

$$= \mathcal{K}_\alpha \oplus \lambda(S_*(\mathfrak{r})) \otimes \mathcal{K}_\alpha.$$

Hence

$$\mathcal{G} = (\mathcal{K}_\alpha \oplus \lambda(S_*(\mathfrak{r})) \otimes \mathcal{K}_\alpha) \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \oplus \mathcal{G}\mathfrak{n}^\alpha$$

$$= \mathcal{K}_\alpha \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \oplus \lambda(S_*(\mathfrak{r})) \otimes K_\alpha \otimes \mathcal{A} \otimes \mathcal{N}_\alpha \oplus \mathcal{G}\mathfrak{n}^\alpha.$$

Since clearly $\mathfrak{g}_\alpha = \mathfrak{k}_\alpha \oplus \mathfrak{a} \oplus \mathfrak{n}_\alpha$, we have

$$\mathcal{G}_\alpha = \mathcal{K}_\alpha \otimes \mathcal{A} \otimes \mathcal{N}_\alpha,$$

and so

$$\mathfrak{G} = \mathfrak{G}_\alpha \oplus \lambda(S_*(\mathfrak{r})) \otimes \mathfrak{G}_\alpha \oplus \mathfrak{G}\mathfrak{n}^\alpha.$$

Let $q \colon \mathfrak{G} \to \mathfrak{G}_\alpha$ denote the projection map with respect to this decomposition. Then $\operatorname{Ker} q \subset \operatorname{Ker} p$, since $\lambda(S_*(\mathfrak{r})) \subset \mathfrak{k}\mathfrak{G}$ and $\mathfrak{G}\mathfrak{n}^\alpha \subset \mathfrak{G}\mathfrak{n}$, and so $p = p \circ q$.

Now $\mathfrak{g}_\alpha = \mathfrak{g}_1 \oplus \mathfrak{c}$, $\mathfrak{g}_1 = \mathfrak{k}_1 \oplus \mathfrak{a}_1 \oplus \mathfrak{n}_1$ and $\mathfrak{c} = \mathfrak{c}_+ \oplus \mathfrak{c}_-$. Letting $\mathfrak{G}_1$, $\mathfrak{A}_1$, $\mathfrak{C}$, $\mathfrak{C}_+$ and $\mathfrak{C}_-$ denote the universal enveloping algebras of $\mathfrak{g}_1$, $\mathfrak{a}_1$, $\mathfrak{c}$, $\mathfrak{c}_+$ and $\mathfrak{c}_-$, respectively, we have

$$\mathfrak{G}_1 = \mathfrak{A}_1 \oplus (\mathfrak{k}_1\mathfrak{G}_1 + \mathfrak{G}_1\mathfrak{n}_1)$$

and

$$\mathfrak{C} = \mathfrak{C}_+ \otimes \mathfrak{C}_- = (k \cdot 1 \oplus \mathfrak{c}_+\mathfrak{C}_+) \otimes \mathfrak{C}_- = \mathfrak{C}_- \oplus \mathfrak{c}_+\mathfrak{C}.$$

Let $p_1 \colon \mathfrak{G}_1 \to \mathfrak{A}_1$ and $p_2 \colon \mathfrak{C} \to \mathfrak{C}_-$ be the projections with respect to these decompositions, so that in particular, p_1 is the mapping for $\mathfrak{G}_1$ analogous to the mapping p for $\mathfrak{G}$. Now $\mathfrak{G}_\alpha = \mathfrak{G}_1 \otimes \mathfrak{C}$ and $\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{C}_-$, so we have a mapping $p_1 \otimes p_2 \colon \mathfrak{G}_\alpha \to \mathfrak{A}$.

Lemma 4.10. *The maps $p_1 \otimes p_2$ and $p|\mathfrak{G}_\alpha$ from $\mathfrak{G}_\alpha$ to $\mathfrak{A}$ are the same.*

Proof. Let $x \in \mathfrak{G}_1$, $y \in \mathfrak{C}$, and write $x \equiv a \,(\operatorname{mod}(\mathfrak{k}_1\mathfrak{G}_1 + \mathfrak{G}_1\mathfrak{n}_1))$ and $y \equiv b \,(\operatorname{mod} \mathfrak{c}_+\mathfrak{C})$, where $a \in \mathfrak{A}_1$ and $b \in \mathfrak{C}_-$. Then since $\mathfrak{C}$ centralizes $\mathfrak{G}_1$,

$$\begin{aligned} xy &\equiv ay \quad (\operatorname{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})) \\ &\equiv ab \quad (\operatorname{mod}(\mathfrak{k}\mathfrak{G} + \mathfrak{G}\mathfrak{n})), \end{aligned}$$

and so $p(xy) = ab$. Q.E.D.

Hence we have:

Lemma 4.11. *The map $p \colon \mathfrak{G} \to \mathfrak{A}$ can be expressed in the form $p = (p_1 \otimes p_2) \circ q$.*

In order to complete our proof, we have to be more specific about the choice of the complement $\mathfrak{r}$ of $\mathfrak{k}_\alpha$ in $\mathfrak{k}$.

Lemma 4.12. *The subalgebra $\mathfrak{k}_\alpha$ is reductive in $\mathfrak{g}$.*

Proof. Since $\operatorname{Ker} \alpha$ is a subalgebra of $\mathfrak{g}$ reductive in $\mathfrak{g}$ and since $\mathfrak{g}_\alpha$ is the centralizer of $\operatorname{Ker} \alpha$ in $\mathfrak{g}$, [1, Proposition 1.7.7] implies that the restriction to $\mathfrak{g}_\alpha$ of the Killing form B of $\mathfrak{g}$ is nonsingular and that the semisimple and nilpotent components (with respect to $\mathfrak{g}$) of an element of $\mathfrak{g}_\alpha$ belong to $\mathfrak{g}_\alpha$. Now $B(\mathfrak{k}_\alpha, \mathfrak{p}_\alpha) = 0$, so that B is nonsingular on $\mathfrak{k}_\alpha$. Let $x \in \mathfrak{k}_\alpha$, and let x_s and x_n be the semisimple and nilpotent components of x, respectively. Then $x_s, x_n \in \mathfrak{g}_\alpha$ by the above. But $x = \theta x = \theta x_s + \theta x_n$, and since θx_s is semisimple, θx_n is nilpotent and $[\theta x_s, \theta x_n] = \theta[x_s, x_n] = 0$, we must have $\theta x_s = x_s$ and $\theta x_n = x_n$. Hence $x_s \in \mathfrak{g}_\alpha \cap \mathfrak{k} = \mathfrak{k}_\alpha$ and $x_n \in \mathfrak{g}_\alpha \cap \mathfrak{k} = \mathfrak{k}_\alpha$. Thus $\mathfrak{k}_\alpha$ satisfies the conditions of [1, Proposition 1.7.6], and so $\mathfrak{k}_\alpha$ is reductive in $\mathfrak{g}$. Q.E.D.

By the lemma, $\mathfrak{k}_\alpha$ is reductive in $\mathfrak{k}$, and so we may choose $\mathfrak{r}$ above to be a $\mathfrak{k}_\alpha$-invariant complement of $\mathfrak{k}_\alpha$ in $\mathfrak{k}$. Then the three summands in the decomposition above which defines the projection q are all $\mathfrak{k}_\alpha$-stable (recall that $[\mathfrak{g}_\alpha, \mathfrak{n}^\alpha] \subset \mathfrak{n}^\alpha$), and so q is a $\mathfrak{k}_\alpha$-map. In particular, $q(\mathcal{G}^{\mathfrak{k}_\alpha}) = \mathcal{G}_\alpha^{\mathfrak{k}_\alpha}$, where superscript as usual denotes centralizer. Now since $\mathfrak{k}_\alpha = \mathfrak{k}_1 \oplus \mathfrak{c}_+$ and $\mathfrak{c}_+$ centralizes $\mathcal{G}_\alpha$, $\mathcal{G}_\alpha^{\mathfrak{k}_\alpha} = \mathcal{G}_\alpha^{\mathfrak{k}_1}$. But since $\mathcal{G}_\alpha = \mathcal{G}_1 \otimes \mathcal{C}$ and $\mathfrak{k}_1$ centralizes $\mathcal{C}$, $\mathcal{G}_\alpha^{\mathfrak{k}_1} = \mathcal{G}_1^{\mathfrak{k}_1} \otimes \mathcal{C}$. Hence from Lemma 4.11, we have

$$p(\mathcal{G}^{\mathfrak{k}_\alpha}) = (p_1 \otimes p_2)(q(\mathcal{G}^{\mathfrak{k}_\alpha})) = (p_1 \otimes p_2)(\mathcal{G}_1^{\mathfrak{k}_1} \otimes \mathcal{C})$$
$$= p_1(\mathcal{G}_1^{\mathfrak{k}_1}) \otimes p_2(\mathcal{C}) = p_1(\mathcal{G}_1^{\mathfrak{k}_1}) \otimes \mathcal{C}_-.$$

The conclusion is:

Lemma 4.13. *We have* $p(\mathcal{G}^{\mathfrak{k}_\alpha}) = p_1(\mathcal{G}_1^{\mathfrak{k}_1}) \otimes \mathcal{C}_-$.

We are now in a position to apply Theorem 4.7. Let

$$\rho_\alpha = \tfrac{1}{2}(\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha})\alpha$$

and let $\rho'_\alpha = \rho_\alpha | \mathfrak{a}_1$. Then ρ'_α is half the sum of the positive restricted roots (with multiplicities counted) for $\mathfrak{g}_1$, and $\rho_\alpha | \mathfrak{c}_- = 0$. Let σ_α be the affine automorphism of $\mathfrak{a}^*$ which takes $\lambda \in \mathfrak{a}^*$ to $s_\alpha(\lambda + \rho_\alpha) - \rho_\alpha$ (where s_α is the Weyl reflection with respect to α), and let $\gamma = \hat{\sigma_\alpha}$ (in the sense of the beginning of this section), so that γ is an automorphism of $\mathcal{A}$. Also, let σ'_α be the affine automorphism of $\mathfrak{a}_1^*$ which takes $\lambda \in \mathfrak{a}_1^*$ to $-\lambda - 2\rho'_\alpha$, and let $\delta = (\sigma'_\alpha)\hat{}: \mathcal{A}_1 \to \mathcal{A}_1$. (Here the symbol $\hat{}$ is used with respect to $\mathfrak{a}_1$ instead of $\mathfrak{a}$.) Denote by $\mathcal{A}^\gamma$ and $\mathcal{A}_1^\delta$ the respective algebras of invariants. By Theorem 4.7, $p_1(\mathcal{G}_1^{\mathfrak{k}_1}) = r_1^{-1}(\mathcal{A}_1^{W_1})$, where W_1 denotes the (two-element) Weyl group of $\mathfrak{g}_1$, and $r_1 = T\hat{}: \mathcal{A}_1 \to \mathcal{A}_1$, where $T: \mathfrak{a}_1^* \to \mathfrak{a}_1^*$ is translation by ρ'_α. But $r_1^{-1}(\mathcal{A}_1^{W_1})$ is exactly $\mathcal{A}_1^\delta$, so that $p_1(\mathcal{G}_1^{\mathfrak{k}_1}) = \mathcal{A}_1^\delta$. On the other hand, we have:

Lemma 4.14. *If we identify* $\mathcal{A}$ *with* $\mathcal{A}_1 \otimes \mathcal{C}_-$, *the automorphism* γ *of* $\mathcal{A}$ *equals* $\delta \otimes 1$.

Proof. Let s'_α be the linear automorphism of $\mathfrak{a}$ which is the transpose of s_α. Then s'_α is -1 on $\mathfrak{a}_1$ and 1 on $\mathfrak{c}_-$. Now γ is the automorphism of $\mathcal{A}$ determined by the condition $\gamma(a) = s'_\alpha(a) - 2\rho_\alpha(a)$ for all $a \in \mathfrak{a}$. Also, δ is the automorphism of $\mathcal{A}_1$ determined by the condition $\delta(a_1) = -a_1 - 2\rho'_\alpha(a_1) = -a_1 - 2\rho_\alpha(a_1)$ for all $a_1 \in \mathfrak{a}_1$. Let $a_1 \in \mathfrak{a}_1$ and $c \in \mathfrak{c}_-$. It is sufficient to show that $\gamma(a_1 + c) = \delta \otimes 1(a_1 \otimes 1 + 1 \otimes c)$ (regarding $\mathcal{A}$ and $\mathcal{A}_1 \otimes \mathcal{C}$ as identified). But

$$\gamma(a_1 + c) = s'_\alpha(a_1 + c) - 2\rho_\alpha(a_1 + c) = -a_1 + c - 2\rho_\alpha(a_1),$$

and

$$\delta \otimes 1(a_1 \otimes 1 + 1 \otimes c) = \delta(a_1) \otimes 1 + 1 \otimes c$$

$$= (-a_1 - 2\rho_\alpha(a_1)) \otimes 1 + 1 \otimes c.$$

Since these two elements identify with each other, the lemma is proved. Q.E.D.

In view of the lemma, $\mathcal{A}^\gamma = \mathcal{A}_1^\delta \otimes \mathcal{C}_-$, and so we can conclude from Lemma 4.13 and the discussion preceding Lemma 4.14:

Lemma 4.15. *We have* $p(\mathcal{G}^{\mathfrak{k}_\alpha}) = \mathcal{A}^\gamma$; *here* $\mathcal{A}^\gamma$ *denotes the algebra of invariants in* $\mathcal{A}$ *under the automorphism* $\gamma = \sigma_{\hat{\alpha}}$, *where* σ_α *is the affine automorphism of* $\mathfrak{a}^*$ *which takes* $\lambda \in \mathfrak{a}^*$ *to* $s_\alpha(\lambda + \rho_\alpha) - \rho_\alpha$.

We need one final lemma. Recall that $\rho = ½\, \Sigma_{\phi \in \Sigma_+}(\dim \mathfrak{g}^\phi)\phi$.

Lemma 4.16. *We have* $s_\alpha(\rho) - \rho = s_\alpha(\rho_\alpha) - \rho_\alpha$.

Proof. Let Σ_α denote the set of positive restricted roots not proportional to α. Then the simplicity of α implies that $s_\alpha \Sigma_\alpha = \Sigma_\alpha$. On the other hand, for all $\beta \in \Sigma$, $s_\alpha\beta \in \Sigma$ and in fact $\dim \mathfrak{g}^\beta = \dim \mathfrak{g}^{s_\alpha\beta}$ (see Lemma 2.5). Thus

$$s_\alpha(\rho) = -\frac{1}{2}(\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha})\alpha + \frac{1}{2} \sum_{\phi \in \Sigma_\alpha} (\dim \mathfrak{g}^\phi)\phi,$$

and so

$$s_\alpha(\rho) - \rho = -(\dim \mathfrak{g}^\alpha + 2 \dim \mathfrak{g}^{2\alpha})\alpha = -2\rho_\alpha = s_\alpha(\rho_\alpha) - \rho_\alpha. \quad \text{Q.E.D.}$$

By the last two lemmas, $p(\mathcal{G}^{\mathfrak{k}_\alpha}) = \mathcal{A}^\gamma$, where $\gamma = \sigma_{\hat{\alpha}}$ and σ_α is the affine automorphism of $\mathfrak{a}^*$ which takes $\lambda \in \mathfrak{a}^*$ to $s_\alpha(\lambda + \rho) - \rho$. Recall that $\tau = T\hat{}$: $\mathcal{A} \to \mathcal{A}$ where T: $\mathfrak{a}^* \to \mathfrak{a}^*$ is translation by ρ. Then $\tau(\mathcal{A}^\gamma)$ is the algebra of invariants for $s_{\hat{\alpha}}$. Denoting this algebra by $\mathcal{A}^{s_\alpha}$, we now have the following conclusion:

Theorem 4.17. *In the notation of the beginning of this section, let* $\alpha \in \Sigma$ *be an arbitrary simple restricted root, define the subalgebra*

$$\mathfrak{g}_\alpha = \mathfrak{m} \oplus \mathfrak{a} \oplus \coprod_{j=\pm1,\pm2} \mathfrak{g}^{j\alpha} = \coprod_{j=-2}^{2} \mathfrak{g}^{j\alpha},$$

where $\mathfrak{g}^{2\alpha}$ *and* $\mathfrak{g}^{-2\alpha}$ *might be zero, and let* $\mathfrak{k}_\alpha = \mathfrak{g}_\alpha \cap \mathfrak{k}$. *Denote by* $\mathcal{G}^{\mathfrak{k}_\alpha}$ *the centralizer of* $\mathfrak{k}_\alpha$ *in* $\mathcal{G}$, *and by* $\mathcal{A}^{s_\alpha}$ *the subalgebra of* $\mathcal{A}$ *consisting of the* *elements invariant under the natural action of the Weyl reflection* s_α *on* $\mathfrak{A}$. *Then* $(\tau \circ p)(\mathfrak{G}^{\mathfrak{k}_\alpha}) = \mathfrak{A}^{s_\alpha}$. *In particular*, $p_*(\mathfrak{G}^{\mathfrak{k}}) \subset \mathfrak{A}^{s_\alpha}$.

Since W is generated by the simple reflections s_α, we can conclude that $p_*(\mathfrak{G}^{\mathfrak{k}}) \subset \mathfrak{A}^W$, and Theorem 4.1 is proved. Q.E.D.

5. **Appendix.** Here we shall give a vector-valued generalization of the injectivity of the map F_* (see §3). In a class of important cases (of the module V, in the notation below), this generalization is already known (see [5, Lemma 4.1], [6] and [1, Lemma 9.2.7, part (b) of the proof]), but in addition to being more general, the present proof is elementary in that it does not require theory of Lie or algebraic groups. The argument presented here is G. McCollum's simplification of our original proof.

Let $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ be the symmetric decomposition of a semisimple symmetric Lie algebra over a field k of characteristic zero and let $\mathfrak{a}$ be a Cartan subspace of $\mathfrak{p}$. Then $\mathfrak{k}$ acts naturally on $\mathfrak{p}$, and thus on $\mathfrak{p}^*$ and on $S(\mathfrak{p}^*)$. Let V be an arbitrary (possibly infinite-dimensional) $\mathfrak{k}$-module. Then since $S(\mathfrak{p}^*)$ is naturally identified with the algebra of polynomial functions on $\mathfrak{p}$, the tensor product $\mathfrak{k}$-module $S(\mathfrak{p}^*) \otimes V$ may be identified with a space of V-valued functions on $\mathfrak{p}$. (In this section, $\otimes$ denotes tensor product over k.) Similarly, $S(\mathfrak{a}^*) \otimes V$ may be identified with a space of V-valued functions on $\mathfrak{a}$. Let $(S(\mathfrak{p}^*) \otimes V)^{\mathfrak{k}}$ be the space of $\mathfrak{k}$-annihilated vectors in $S(\mathfrak{p}^*) \otimes V$, and let $F_*^V : (S(\mathfrak{p}^*) \otimes V)^{\mathfrak{k}} \to S(\mathfrak{a}^*) \otimes V$ denote the natural restriction map.

Theorem 5.1. F_*^V *is injective.*

Proof. Let $f_0 \in (S(\mathfrak{p}^*) \otimes V)^{\mathfrak{k}}$ and suppose $F_*^V(f_0) = 0$. The homogeneous components of f_0 with respect to the decomposition

$$S(\mathfrak{p}^*) \otimes V = \coprod_{r=0}^{\infty} S^r(\mathfrak{p}^*) \otimes V$$

are annihilated by $\mathfrak{k}$, since the terms in this decomposition are $\mathfrak{k}$-stable. The components of f_0 also vanish on $\mathfrak{a}$; this follows from the fact that $\mathfrak{a}$ is stable under scalar multiplication. Hence it is sufficient to prove that if f_0 is a $\mathfrak{k}$-annihilated element of $S^r(\mathfrak{p}^*) \otimes V$ for some $r \in \mathbf{Z}_+$ and if the restriction of f_0 to $\mathfrak{a}$ is zero, then $f_0 = 0$.

Recall from §3 the pairing $\{\cdot, \cdot\}$ between $S^r(\mathfrak{p}^*)$ and $S^r(\mathfrak{p})$. Define a bilinear map $\omega : (S^r(\mathfrak{p}^*) \otimes V) \times S^r(\mathfrak{p}) \to V$ by the condition $g \otimes v, s \mapsto \{g, s\}v$ for all $g \in S^r(\mathfrak{p}^*)$, $v \in V$ and $s \in S^r(\mathfrak{p})$. In view of Lemma 3.6, ω is a $\mathfrak{k}$-map in the sense that $\omega(x \cdot f, s) + \omega(f, x \cdot s) = x \cdot \omega(f, s)$ for all $x \in \mathfrak{k}$, $f \in S^r(\mathfrak{p}^*) \otimes V$ and $s \in S^r(\mathfrak{p})$. Also, for all $f \in S^r(\mathfrak{p}^*) \otimes V$, $\omega(f, S^r(\mathfrak{p})) = 0$ implies $f = 0$. Indeed, let $\{v_i\}$ be a basis of V, and write $f = \Sigma_i \, g_i \otimes v_i$, where $g_i \in S^r(\mathfrak{p}^*)$.

Then

$$0 = \sum_i \omega(g_i \otimes v_i, S^r(\mathfrak{p})) = \sum_i \{g_i, S^r(\mathfrak{p})\}v_i$$

so that $\{g_i, S^r(\mathfrak{p})\} = 0$ for each i. By Lemma 3.5(i), each $g_i = 0$, and so $f = 0$.

Now let $T = \{t \in S^r(\mathfrak{p}) | \omega(f_0, t) = 0\}$. Then T is a $\mathfrak{k}$-submodule of $S^r(\mathfrak{p})$. In fact, if $t \in T$ and $x \in \mathfrak{k}$, then $\omega(f_0, x \cdot t) = x \cdot \omega(f_0, t) - \omega(x \cdot f_0, t) = 0$ since $t \in T$ and $x \cdot f_0 = 0$. But $S^r(\mathfrak{a}) \subset T$. Indeed, let $a \in \mathfrak{a}$, and write $f_0 = \sum_i g_i \otimes v_i$ for some $g_i \in S^r(\mathfrak{p}^*)$ and $v_i \in V$. Then

$$\omega(f_0, a^r) = \sum_i \{g_i, a^r\}v_i = \sum_i r!\, g_i(a)v_i = r!\, f_0(a) = 0$$

by hypothesis, and the fact that $S^r(\mathfrak{a}) \subset T$ follows from Lemma 3.5(ii). Thus T is a $\mathfrak{k}$-submodule of $S^r(\mathfrak{p})$ containing $S^r(\mathfrak{a})$, so that $T = S^r(\mathfrak{p})$ by Lemma 3.7. (Note that the field extension technique shows that Lemma 3.7 holds even when $\mathfrak{a}$ is not a splitting Cartan subspace.) That is, $\omega(f_0, S^r(\mathfrak{p})) = 0$, and so $f_0 = 0$ by the last paragraph. Q.E.D.

BIBLIOGRAPHY

1. J. Dixmier, *Algèbres enveloppantes*, Gauthier-Villars, Paris, 1974.

2. Harish-Chandra, (a) *Representations of semisimple Lie groups*. II, Trans. Amer. Math. Soc. 76 (1954), 26–65. MR 15, 398.

(b) *Spherical functions on a semisimple Lie group*. I, Amer. J. Math. 80 (1958), 241–310. MR 20 #925.

3. S. Helgason, *A duality for symmetric spaces with applications to group representations*, Advances in Math. 5 (1970), 1–154. MR 44 #8587.

4. B. Kostant, *On the existence and irreducibility of certain series of representations*, Publ. 1971 Summer School in Math., edited by I. M. Gel'fand, Bolyai-János Math. Soc., Budapest (to appear).

5. J. Lepowsky, *Algebraic results on representations of semisimple Lie groups*, Trans. Amer. Math. Soc. 176 (1973), 1–44.

6. C. Rader, *Spherical functions on semisimple Lie groups*, Thesis and unpublished supplements, University of Washington, 1971.

7. Séminaire Sophus Lie École Norm. Sup. 1954/55, *Théorie des algèbres de Lie. Topologies des groupes de Lie*, Secretariat mathématique, Paris, 1955. MR 17, 384.

8. G. Warner, *Harmonic analysis on semi-simple Lie groups*. I, Springer-Verlag, New York, 1972.

DEPARTMENT OF MATHEMATICS, YALE UNIVERSITY, NEW HAVEN, CONNECTICUT 06520