THE CLASSIFYING RING OF A CLASSICAL RANK ONE SEMISIMPLE LIE GROUP

A. BREGA, L. CAGLIERO, AND J. TIRAO

Abstract. Let G_o be a classical rank one semisimple Lie group and let K_o denote a maximal compact subgroup of G_o. Let $U(\mathfrak{g})$ be the complex universal enveloping algebra of G_o and let $U(\mathfrak{g})^K$ denote the centralizer of K_o in $U(\mathfrak{g})$. Also let $P : U(\mathfrak{g}) \longrightarrow U(\mathfrak{k}) \otimes U(\mathfrak{a})$ be the projection map corresponding to the direct sum $U(\mathfrak{g}) = \big(U(\mathfrak{k}) \otimes U(\mathfrak{a})\big) \oplus U(\mathfrak{g})\mathfrak{n}$ associated to an Iwasawa decomposition of G_o adapted to K_o. In this paper we give a characterization of the image of $U(\mathfrak{g})^K$ under the injective antihomorphism $P : U(\mathfrak{g})^K \longrightarrow U(\mathfrak{k}) \otimes U(\mathfrak{a})$.

Contents

1. Introduction 1
2. Outline and statement of results 4
3. The algebra B 17
4. The image of $U(\mathfrak{g})^K$ 19
5. Non commutative Gaussian elimination 23
6. The case SO(n,1) 28
7. The case SU(n,1) 32
7.1. Weyl group invariance of the leading term 39
7.2. Appendix 44
8. The case Sp(n,1) 47
8.1. Transversality results 57
8.2. An estimate of the Kostant degree 66
8.3. The main inductive argument 71
8.4. The coefficient matrix 81
8.5. The final stage. 87
References 102

1. Introduction

Let G_o be a connected, noncompact, real semisimple Lie group with finite center, and let K_o denote a maximal compact subgroup of G_o. We denote with $\mathfrak{g}_o$ and $\mathfrak{k}_o$ the Lie algebras of G_o and K_o, and $\mathfrak{k} \subset \mathfrak{g}$ will denote the

This paper is partially supported by CONICET grant PIP655-98.

respective complexified Lie algebras. Let $U(\mathfrak{g})$ be the universal enveloping algebra of $\mathfrak{g}$ and let $U(\mathfrak{g})^K$ denote the centralizer of K_o in $U(\mathfrak{g})$.

By the fundamental work of Harish-Chandra it is known that many deep questions concerning the infinite dimensional representation theory of G_o reduce to questions about the structure and finite dimensional representation theory of the algebra $U(\mathfrak{g})^K$, called the *classifying ring* of G_o (cf. Cooper [5]). For example, if π is an irreducible unitary representation of K_o and $\ker(\pi)$ denotes the kernel of π in $U(\mathfrak{k})$, then $I_\pi = U(\mathfrak{g})^K \cap U(\mathfrak{g}) \ker(\pi)$ is a two sided ideal of $U(\mathfrak{g})^K$, and there is a bijection between the set of all irreducible finite dimensional representations of the algebra $U(\mathfrak{g})^K/I_\pi$ and all the irreducible Harish-Chandra modules of G_o that contain π as a K-type (see [19] and [20]). In particular, if $\pi = 1$ is the trivial representation of K_o, by a theorem of Harish-Chandra (see [27]) it is known that $U(\mathfrak{g})^K/I_1$ is isomorphic to a polynomial ring in r variables, where r is the split rank of G_o. This result has been very useful in dealing with spherical irreducible representations of G_o (see Kostant [14]).

Also, since $U(\mathfrak{g})^K/I_1$ is isomorphic to the algebra of G_o-invariant differential operators on the symmetric space G_o/K_o, one obtains the structure of this algebra which plays an important role in the harmonic analysis of G_o/K_o. More generally $U(\mathfrak{g})^K/I_\pi$ is isomorphic to the algebra of all G_o-invariant differential operators on the equivariant vector bundle E_π over G_o/K_o. It is known that this algebra is finetely generated as a module over the center of $U(\mathfrak{g})$ (see [6]), but its full structure is known in very few cases.

Another instance where $U(\mathfrak{g})^K$ plays an important role is in the theory of spherical functions of the pair (G_o, K_o), since these functions are parameterized by the irreducible finite dimensional representations of $U(\mathfrak{g})^K$ which are continuous with respect to the weak topology defined by the K_o-central analytic functions on G_o (see [8], [22] and [7]).

There is no doubt of the importance of the classifying ring $U(\mathfrak{g})^K$. Unfortunately it is a very complex algebra and few things of its structure are known: If G_o is equal to SO(n,1) or SU(n,1) it is known that $U(\mathfrak{g})^K \simeq Z(\mathfrak{g}) \otimes Z(\mathfrak{k})$, where $Z(\mathfrak{g})$ and $Z(\mathfrak{k})$ denote the centers of $U(\mathfrak{g})$ and $U(\mathfrak{k})$, respectively; hence by the famous theorem of Harish-Chandra $U(\mathfrak{g})^K$ is a polynomial ring. This result was first proved by Cooper in [5] and his proof was later simplified by Howe in [10]. Also Johnson gave a proof for SU(n,1) in [11]. More generally, Knop (see [15]), studying actions of reductive groups on algebraic varieties, proved that the center of $U(\mathfrak{g})^K$ is always $Z(\mathfrak{g}) \otimes Z(\mathfrak{k})$.

In order to contribute to the understanding of $U(\mathfrak{g})^K$ Kostant suggested to consider the projection map $P : U(\mathfrak{g}) \longrightarrow U(\mathfrak{k}) \otimes U(\mathfrak{a})$, corresponding to the direct sum $U(\mathfrak{g}) = \big(U(\mathfrak{k}) \otimes U(\mathfrak{a})\big) \oplus U(\mathfrak{g})\mathfrak{n}$ associated to an Iwasawa decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{a} \oplus \mathfrak{n}$ adapted to $\mathfrak{k}$. In [19] Lepowsky studied the restriction of P to $U(\mathfrak{g})^K$ and proved, among other things, that one has the following exact sequence

$$0 \longrightarrow U(\mathfrak{g})^K \xrightarrow{P} U(\mathfrak{k})^M \otimes U(\mathfrak{a}),$$

where $U(\mathfrak{k})^M$ denotes the centralizer of M_o in $U(\mathfrak{k})$, M_o being the centralizer of A_o in K_o. Moreover if $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ is given the tensor product algebra structure then P becomes an antihomomorphism of algebras. Hence to go any further in this direction it is necessary to determine the image of P. This was accomplished by Tirao in [24] for SO(n,1) and SU(n,1). This result was later used in [26] to give a new proof of Cooper's result.

To characterize the image of P for any G_o, Kostant and Tirao introduced the subalgebra $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}$ of all elements in $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ which commute with certain intertwining operators (see 4.1 of [17]). Such operators are in a one to one correspondence with the elements of the Weyl group W of the pair $(\mathfrak{g}, \mathfrak{a})$ and are closely related to the intertwining operators considered in [21] and also to those studied in [13] and [18]. A result of Tirao shows that the image of $U(\mathfrak{g})^K$ under P is contained in $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}$ (Theorem 3.2 of [17]), however P is not onto $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}$. Nevertheless in [17] an element γ in $Z(\mathfrak{g})$ is chosen so that the map $P_\gamma : U(\mathfrak{g})^K_\gamma \longrightarrow \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}_{\gamma_o}$ induced by P, from the localization of $U(\mathfrak{g})^K$ with respect to γ to the localization of $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}$ with respect to $\gamma_o = P(\gamma)$, extends to a surjective anti-isomorphism between the completions of such localizations with respect to natural valuations on $U(\mathfrak{g})^K_\gamma$ and $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}_{\gamma_o}$ (Theorem 7.4 of [17]).

In order to determine the actual image $P(U(\mathfrak{g})^K)$, Tirao introduced in [24] a subalgebra B of $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ defined by a set of linear equations derived from certain embeddings between Verma modules, and considered the subalgebra $B^{\widetilde{W}} = B \cap \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^{\widetilde{W}}$. In [24] it is proved that $P(U(\mathfrak{g})^K)$ always lies in $B^{\widetilde{W}}$ and furthermore, for G_o equal to SO(n,1) or SU(n,1), that $P(U(\mathfrak{g})^K) = B^{\widetilde{W}}$. We point out that in these two cases $B^{\widetilde{W}}$ coincides with the subalgebra B^{W_ρ} of all elements in B that are invariant under the tensor product action of W on $U(\mathfrak{k})^M$ and the translated action of W on $U(\mathfrak{a})$ (see Corollary 3.3 in [17]).

In this paper we improve the results in [24] when $G_o = $ SO(n,1) or SU(n,1), and we prove a similar result when $G_o = $ Sp(n,1). In fact our main result is the following

Theorem 1.1. *If G_o is a classical rank one semisimple Lie group, then*

$$P(U(\mathfrak{g})^K) = \begin{cases} B^{W_\rho}, & \text{if } rank\,(G_o) \neq rank\,(K_o); \\ B, & \text{if } rank\,(G_o) = rank\,(K_o). \end{cases}$$

We conjecture that Theorem 1.1 is true for any rank one semisimple Lie group, but to achieve its proof it is still necessary to overcome some difficulties when G_o is the exceptional group F_4. Nevertheless most of the results in this paper are also true in this case.

2. Outline and statement of results

For convenience we summarize here the main steps and ideas leading to the proof of Theorem 1.1.

Let $\mathfrak{t}_o$ be a Cartan subalgebra of the Lie algebra $\mathfrak{m}_o$ of M_o. Set $\mathfrak{h}_o = \mathfrak{t}_o \oplus \mathfrak{a}_o$ and let $\mathfrak{h} = \mathfrak{t} \oplus \mathfrak{a}$ be the corresponding complexification. Choose a Borel subalgebra $\mathfrak{t} \oplus \mathfrak{m}^+$ of the complexification $\mathfrak{m}$ of $\mathfrak{m}_o$ and take $\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{m}^+ \oplus \mathfrak{n}$ as a Borel subalgebra of $\mathfrak{g}$. Let Δ and Δ^+ be, respectively, the corresponding sets of roots and positive roots of $\mathfrak{g}$. If $\langle\, , \,\rangle$ denotes the Killing form of $\mathfrak{g}$, for each $\alpha \in \Delta$ let $H_\alpha \in \mathfrak{h}$ be the unique element such that $\phi(H_\alpha) = 2\langle \phi, \alpha \rangle / \langle \alpha, \alpha \rangle$ for all $\phi \in \mathfrak{h}^*$. Also set $H_\alpha = Y_\alpha + Z_\alpha$ where $Y_\alpha \in \mathfrak{t}$ and $Z_\alpha \in \mathfrak{a}$, and let $P_+ = \{\alpha \in \Delta^+ : Z_\alpha \neq 0\}$. If $\alpha \in P_+$ let $\mathfrak{a}_\alpha = \{H \in \mathfrak{a} : \alpha(H) = 0\}$. Then $\mathfrak{a} = \mathfrak{a}_\alpha \oplus \mathbb{C} Z_\alpha$ and we can consider the elements in $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ as polynomials in Z_α with coefficients in $U(\mathfrak{k}) \otimes U(\mathfrak{a}_\alpha)$. For any $\alpha \in P_+$ consider the three dimensional simple Lie algebra $\mathfrak{u}_\alpha$ spanned by an $\mathfrak{s}$-triple of the form $\{H_\alpha, X_\alpha, X_{-\alpha}\}$ and set $E_\alpha = P(X_{-\alpha}) = X_{-\alpha} + \theta X_{-\alpha}$.

In Section 3 we state Theorem 3.1 which holds for any connected, noncompact, real semisimple Lie group, and whose proof is contained in Theorem 5 and Corollary 6 of [24]. Next we prove the following corollary.

Corollary 3.5. *If $\alpha \in P_+$ is a simple root and $n \in \mathbb{N}$, for all $u \in U(\mathfrak{g})^K$ $b = P(u)$ satisfies*

$$P_n(E_\alpha) b(n - Y_\alpha - 1) \equiv b(-n - Y_\alpha - 1) P_n(E_\alpha), \tag{1}$$

where the congruence is $\operatorname{mod}\big(U(\mathfrak{k})\mathfrak{m}^+ \otimes U(\mathfrak{a}_\alpha)\big)$.

Definition 3.6. Let B be the subalgebra of all elements $b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ satisfying (1) for all simple roots $\alpha \in P_+$ and all $n \in \mathbb{N}$.

We point out that the element $P_n(E_\alpha) \in U(\mathfrak{k})$ ocurring in equation (1) is obtained by evaluating at E_α the characteristic polynomial $P_n(t)$ of $\pi_{n-1}(E_\alpha)$, where π_{n-1} denotes the irreducible representation of $\mathfrak{u}_\alpha$ of dimension n. If $\alpha \in P_+$ is simple and $\lambda = \alpha|_{\mathfrak{a}}$ we let $\mathfrak{g}(\lambda)$ denote the real reductive rank one subalgebra of $\mathfrak{g}_o$ associated to λ. When $[\mathfrak{g}(\lambda), \mathfrak{g}(\lambda)] \simeq \mathfrak{sl}(2, \mathbb{R})$ we have $Y_\alpha = 0$ and the corresponding polynomial $P_n(t)$ is computed in Lemma 3.3. On the other hand, if $[\mathfrak{g}(\lambda), \mathfrak{g}(\lambda)] \not\simeq \mathfrak{sl}(2, \mathbb{R})$ we have $Y_\alpha \neq 0$ and $P_n(t) = t^n$ (see Proposition 3.4).

From now on we assume that G_o is a connected, noncompact real semisimple Lie group of split rank one. To prove Theorem 1.1 it is necessary to consider at certain points in the argument the different cases corresponding to the real root structure of G_o.

In Section 4 we first prove Theorem 1.1 when G_o is locally isomorphic to SL(2,$\mathbb{R}$). In this case $\mathfrak{m} = \{0\}$ and $U(\mathfrak{k})^M = U(\mathfrak{k})$ is abelian. This makes things sufficiently simple so that the theorem can be proved by direct computation.

For the remaining cases we have to work much more. To explain our approach we need to introduce some notation. Let G be the adjoint group of $\mathfrak{g}$ and let K be the connected Lie subgroup of G with Lie algebra $ad_{\mathfrak{g}}(\mathfrak{k})$. Also let $M = \mathrm{Centr}_K(\mathfrak{a})$, $M' = \mathrm{Norm}_K(\mathfrak{a})$ and $W = M'/M$. If H is a group and V a finite dimensional H-module over $\mathbb{C}$, let $S(V^*)$ denote the ring of all polynomial functions on V, and let $S(V^*)^H$ denote the subring of all H-invariant elements. Also let $S^n(V^*)$ denote the corresponding homogeneous subspace of $S(V^*)$ of degree n. We need to know the image of the homomorphism $\pi : S(\mathfrak{g}^*)^K \to S((\mathfrak{k}\oplus\mathfrak{a})^*) = S(\mathfrak{k}^*)\otimes S(\mathfrak{a}^*)$ induced by restriction from $\mathfrak{g}$ to $\mathfrak{k}\oplus\mathfrak{a}$.

Let Γ denote the set of all equivalence classes of irreducible holomorphic finite dimensional K-modules V_γ such that $V_\gamma^M \neq 0$. Any $\gamma\in\Gamma$ can be realized as a submodule of all harmonic polynomial functions on $\mathfrak{p}$, homogeneous of degree d for a uniquely determined $d = d(\gamma)$ (see Kostant [16]). If V is any K-module and $\gamma \in \hat{K}$ then V_γ will denote the isotypic component of V corresponding to γ.

Let $C = S(\mathfrak{k}^*)^M$ and let $C_d = \bigoplus S(\mathfrak{k}^*)^M_\gamma$, where the sum extends over all $\gamma\in\Gamma$ such that $d(\gamma)\le d$. Then $C = \bigcup_{d\ge 0} C_d$ is a nice ascending filtration of C. Moreover

$$D = \bigoplus_{d\ge 0}(C_d \otimes S^d(\mathfrak{a}^*))$$

is an algebra, and it is stable under the tensor product action of W on $S(\mathfrak{k}^*)^M\otimes S(\mathfrak{a}^*)$. If D^W denotes the ring of W-invariants in D, we have

Theorem 4.1. (See [23] and [1].) *The operation of restriction from $\mathfrak{g}$ to $\mathfrak{k}\oplus\mathfrak{a}$ induces an isomorphism of $S(\mathfrak{g}^*)^K$ onto D^W.*

Let $F = U(\mathfrak{k})^M$ and let $F_d = \bigoplus U(\mathfrak{k})^M_\gamma$, where the sum is over all $\gamma\in\Gamma$ such that $d(\gamma)\le d$. Then $F = \bigcup_{d\ge 0} F_d$ is a nice ascending filtration of F. If $b\in F$ we define $d(b) = \min\{d\in\mathbb{N}_o : b\in F_d\}$ and we call it the *Kostant degree* of b.

If $0\ne b\in U(\mathfrak{k})\otimes U(\mathfrak{a})$ we can write $b = b_m\otimes Z^m + \cdots + b_0$ in a unique way with $b_j\in U(\mathfrak{k})$ for $j = 0,\ldots,m$, $b_m\neq 0$ and $Z = Z_\alpha$ for any $\alpha\in P_+$ simple. We refer to b_m (resp. $\widetilde{b} = b_m\otimes Z^m$) as the *leading coefficient* (resp. *leading term*) of b and to m as the *degree* of b. In what follows $\big(U(\mathfrak{k})^M\otimes U(\mathfrak{a})\big)^W$ denotes the ring of W-invariants in $U(\mathfrak{k})^M\otimes U(\mathfrak{a})$ under the tensor product action of the Weyl group. At this point we quote the following property of the image $P(U(\mathfrak{g})^K)$, which follows from Theorem 4.5 of [17] and Theorem 9 of [24].

Proposition 4.3. *If $b = b_m\otimes Z^m + \cdots + b_0 \in P(U(\mathfrak{g})^K)$ then its leading term $\widetilde{b} = b_m\otimes Z^m \in \big(U(\mathfrak{k})^M\otimes U(\mathfrak{a})\big)^W$ and $d(b_m)\le m$.*

Now using Theorem 4.1 and taking a close and very technical look at the following diagram (which is only commutative at the highest degree level)

$$\begin{array}{ccc} U(\mathfrak{g})_n & \xrightarrow{\sigma^n} & S^n(\mathfrak{g}^*) \\ {\scriptstyle P}\big\downarrow & & \big\downarrow{\scriptstyle \pi} \\ \big(U(\mathfrak{k})\otimes U(\mathfrak{a})\big)_n & \xrightarrow{\sigma_o^n} & S^n\big((\mathfrak{k}\oplus\mathfrak{a})^*\big), \end{array}$$

we prove the following result.

Proposition 4.4. *If $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and $d(b_m) \le m$, then there exists $u \in U(\mathfrak{g})^K$ such that $\widetilde{b}$ is the leading term of $b = P(u)$.*

Finally, using Propositions 4.3 and 4.4, we finish Section 4 proving that the following theorem implies our main result (Theorem 1.1).

Theorem 4.5. *If $b \in B^{W_\rho}$ when rank$(G_o) \neq$ rank(K_o) or if $b \in B$ when rank$(G_o) =$ rank(K_o), then its leading term $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and $d(b_m) \le m$.*

Hence the rest of the paper is devoted to the proof of Theorem 4.5 for any classical rank one semisimple Lie group. Since at this point Theorem 1.1 has been already proved when G_o is locally isomorphic to $\mathrm{SL}(2,\mathbb{R})$, from now on it is assumed that G_o is a connected, noncompact real semisimple Lie group, of split rank one, not locally isomorphic to $\mathrm{SL}(2,\mathbb{R})$. Then, as we pointed out before, for any simple root $\alpha \in P_+$ we have $Y_\alpha \neq 0$. Therefore the algebra B (see Definition 3.6 and Proposition 3.4) is the set of all $b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ satisfying

$$E_\alpha^n b(n - Y_\alpha - 1) \equiv b(-n - Y_\alpha - 1)E_\alpha^n \tag{2}$$

$\mathrm{mod}\big(U(\mathfrak{k})\mathfrak{m}^+\big)$, for all simple roots $\alpha \in P_+$ and all $n \in \mathbb{N}$.

From now on we shall simply write $u \equiv v$ instead of $u \equiv v \mod \big(U(\mathfrak{k})\mathfrak{m}^+\big)$, for any $u, v \in U(\mathfrak{k})$. To simplify the notation we put $E = E_\alpha$, $Y = Y_\alpha$ and $Z = Z_\alpha$ for any simple root $\alpha \in P_+$. Notice that $[E, Y] = cE$ where $c = \alpha(Y_\alpha)$ and that E is $\mathfrak{m}^+$-dominant. Also observe that in the rank one case $c = 1$ when 2λ is not a restricted root and $c = \frac{3}{2}$ when it is (see Lemma 29 of [24]). In what follows we find it convenient to identify $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ with the polynomial ring in one variable $U(\mathfrak{k})[x]$, replacing Z by the indeterminate x. To study equation (2) we change $b(x) \in U(\mathfrak{k})[x]$ by $c(x) \in U(\mathfrak{k})[x]$ defined by

$$c(x) = b(x + H - 1), \tag{3}$$

where $H = 0$ if $c = 1$ and H is an appropriate vector in $\mathfrak{t}$, depending on the simple root $\alpha \in P_+$, such that $[H, E] = \frac{1}{2}E$ if $c = \frac{3}{2}$. Now if $\widetilde{Y} = Y + H$, we have $[E, \widetilde{Y}] = E$ in both cases. Then for $n \in \mathbb{N}$ the corresponding equation for $c(x) \in U(\mathfrak{k})[x]$ becomes

$$E^n c(n - \widetilde{Y}) \equiv c(-n - \widetilde{Y})E^n. \tag{4}$$

Observe that (4) is an equation in the noncommutative ring $U(\mathfrak{k})$.

If p is a polynomial in one indeterminate x with coefficients in a ring, let $p^{(n)}$ denote the n-th discrete derivative of p. In particular $p^{(1)}(x) = p(x+\frac{1}{2}) - p(x-\frac{1}{2})$. Also, if $X \in \mathfrak{k}$ we denote by $\dot{X}$ the derivation of $U(\mathfrak{k})$ induced by $\operatorname{ad}(X)$. Moreover if D is a derivation of $U(\mathfrak{k})$ we denote with the same symbol the unique derivation of $U(\mathfrak{k})[x]$ which extends D and such that $Dx = 0$. The main result of Section 5 is the following theorem where we obtain a triangularized version of the system of equations (4) that defines the algebra B.

Theorem 5.3. *Let $c \in U(\mathfrak{k})[x]$. Then the following systems of equations are equivalent:*
(i) $E^n c(n - \widetilde{Y}) \equiv c(-n - \widetilde{Y})E^n$, $(n \in \mathbb{N}_0)$;
(ii) $\dot{E}^{n+1}\big(c^{(n)}\big)(\frac{n}{2} + 1 - \widetilde{Y}) + \dot{E}^n\big(c^{(n+1)}\big)(\frac{n}{2} - \frac{1}{2} - \widetilde{Y})E \equiv 0$, $(n \in \mathbb{N}_0)$.

Moreover, if $c \in U(\mathfrak{k})[x]$ is a solution of one of the above systems, then for all $\ell, n \in \mathbb{N}_0$ we have
(iii) $(-1)^n \dot{E}^\ell\big(c^{(n)}\big)(-\frac{n}{2} + \ell - \widetilde{Y})E^n - (-1)^\ell \dot{E}^n\big(c^{(\ell)}\big)(-\frac{\ell}{2} + n - \widetilde{Y})E^\ell \equiv 0.$

Observe that if $c \in U(\mathfrak{k})[x]$ is of degree m and $c = c_m x^m + \cdots + c_0$, then all equations of the system (ii) corresponding to $n > m$ are trivial, because $c^{(n)} = 0$. Moreover the equation corresponding to $n = m$ reduces to $\dot{E}^{m+1}(c_m) \equiv 0$, and more generally the equation associated to $n = j$ only involves the coefficients $c_m, \dots, c_j$. In other words the system (ii) is a triangular system of $m+1$ linear equations in the $m+1$ unknowns $c_m, \dots, c_0$.

Since we are going to use equations (iii) of Theorem 5.3, it is convenient to consider a basis $\{\varphi_n\}_{n\geq 0}$ of the polynomial ring $\mathbb{C}[x]$ that behaves well under the discrete derivative. Let $\{\varphi_n\}_{n\geq 0}$ be the basis of $\mathbb{C}[x]$ defined by,

(i) $\qquad \varphi_0 = 1,$

(ii) $\qquad \varphi_n^{(1)} = \varphi_{n-1} \qquad$ if $n \geq 1$,

(iii) $\qquad \varphi_n(0) = 0 \qquad$ if $n \geq 1$.

In Section 6 we prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ with $n \geq 3$. If $n \geq 4$ there is only one simple root $\alpha_1 \in P_+$ and for $n = 3$ there are two α_1, α_2. In all cases we set $\alpha = \alpha_1$ and as before we put $E = E_\alpha$, $Y = Y_\alpha$ and $Z = Z_\alpha$. If $b(x) \in U(\mathfrak{k})[x]$, $b(x) \neq 0$, we write $b = \sum_{j=0}^m b_j x^j$, $b_j \in U(\mathfrak{k})$, $b_m \neq 0$, and the corresponding $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$. Then the vectors $(b_0, \dots, b_m)^t$ and $(c_0, \dots, c_m)^t$ are related by a rational nonsingular upper triangular matrix (see Lemma 6.1). Now it is easy to obtain, from Theorem 5.3, the following result.

Theorem 6.3. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{m+1}(b_j) \equiv 0$ for all $0 \leq j \leq m$.*

Another fundamental step in the proof of Theorem 1.1 is the following fact established in Theorem 3.11 of [2]. We refer to results of this kind as transversality results.

Theorem 6.4. *Let G_o be locally isomorphic to $SO(n,1)_e$, $n \geq 3$, or $SU(n,1)$ $n \geq 2$. Then the infinite sum $\sum_{j\geq 0} \dot{E}^j\big(U(\mathfrak{k})^M\big)$ is a direct sum and we have*

$$\Big(\sum_{j\geq 0} \dot{E}^j\big(U(\mathfrak{k})^M\big)\Big) \cap U(\mathfrak{k})\mathfrak{m}^+ = 0.$$

This result allows us to replace the congruence to zero $\mod \big(U(\mathfrak{k})\mathfrak{m}^+\big)$ in Theorem 6.3 by an equality. Hence we obtain the following corollary.

Corollary 6.5. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{m+1}(b_j) = 0$ for all $0 \leq j \leq m$.*

To establish Theorem 1.1 we still need some facts about the representations in Γ. First of all when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ or $\mathrm{SU}(n,1)$ we have an alternative and convenient description of the degree of $\gamma \in \Gamma$. In fact, let $\alpha \in P_+$ be a simple root and set $E = X_{-\alpha} + \theta X_{-\alpha}$ for any $X_{-\alpha} \neq 0$. If $\gamma \in \Gamma$ let

$$q(\gamma) = \max\{q \in \mathbb{N} : E^q(V_\gamma^M) \neq 0\}. \tag{5}$$

In Propositions 6.6 and 7.6 we prove that $d(\gamma) = q(\gamma)$ for $\mathrm{SO}(n,1)_e$ and that $d(\gamma) = 2q(\gamma)$ for $\mathrm{SU}(n,1)$, as well as other facts about the representations in Γ. This is one of the main differences between these cases and that of $\mathrm{Sp}(n,1)$. Some of these results where first established in [12], others were proved in [2] for G_o locally isomorphic to $\mathrm{SO}(n,1)_e$ or $\mathrm{SU}(n,1)$, and in [4] they were recently generalized to any real rank one semisimple Lie group. We are now in position to prove one of the conditions needed to establish Theorem 1.1 (see Theorem 4.5) when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$.

Theorem 6.7. *Assume that G_o is locally isomorphic to $SO(n,1)_e$, $n \geq 3$. Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $d(b_j) \leq m$ for all $0 \leq j \leq m$.*

To complete the proof of Theorem 1.1 we just need to show that when $\mathrm{rank}\,(G_o) = \mathrm{rank}\,(K_o)$ the algebra B does not contain elements of odd degree, because the non trivial element of W can be represented by an element in M_o' which acts on $\mathfrak{g}$ as the Cartan involution. As a consequence of (ii) and (iii) of Proposition 6.6 we obtain the following lemma, from where our final result follows.

Lemma 6.8. *If G_o is locally isomorphic to $SO(2p,1)_e$ and $b \in U(\mathfrak{k})^M$ is such that $\dot{E}^{2t}(b) = 0$ with $t \in \mathbb{N}$, then $\dot{E}^{2t-1}(b) = 0$.*

Theorem 6.9. *If G_o is locally isomorphic to $SO(2p,1)_e$, $p \geq 2$, and $b = b_m \otimes Z^m + \cdots + b_0 \in B$ with m odd, then $b_m = 0$.*

In Section 7 we prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SU}(n,1)$ with $n \geq 2$. In this case there are two simple roots $\alpha = \alpha_1, \alpha_n$ in P_+; in both cases $Y_\alpha \neq 0$. Set $E_1 = X_{-\alpha_1} + \theta X_{-\alpha_1}$, $E_2 = X_{-\alpha_n} + \theta X_{-\alpha_n}$, $Y_1 = Y_{\alpha_1}$, $Y_2 = Y_{\alpha_n}$ and $Z = Z_{\alpha_1} = Z_{\alpha_n}$. Also there is a unique $T \in \mathfrak{z}(\mathfrak{m})$

such that $[T, E_1] = E_1$ and $[T, E_2] = -E_2$. Now we define the vector H considered in (3) as follows,

$$H = \begin{cases} \frac{1}{2}T, & \text{if } \alpha = \alpha_1 \\ -\frac{1}{2}T, & \text{if } \alpha = \alpha_n, \end{cases}$$

and we write generically E for E_1 or E_2. In the first part of the section, using Theorem 5.3 and Theorem 6.4, the following fact is established.

Corollary 7.4. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{2m+1-j}(b_j) = 0$ for all $0 \le j \le m$.*

However to prove that if $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $d(b_m) \le m$ this is not enough. In fact it is necessary to establish that for such a b we have $\dot{E}^{[\frac{m}{2}]+1}(b_m) = 0$. To do this we need the folowing result.

Theorem 7.5. *Let $m, w, \alpha \in \mathbb{Z}$, $0 \le w, \alpha \le m$, $\alpha + w \ge m + 1$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and $\dot{E}^{m+\alpha+1-j}(b_j) \equiv 0$ for all $0 \le j \le m$, then*

$$\sum_{j=m-w}^{m} (-2)^{-j} j! \binom{\alpha + w}{j + w - m} \dot{E}^{m+\alpha-j}(b_j) E^j \equiv 0.$$

Next we prove Theorem 7.9 which plays a crucial role in the proof of Theorem 4.5 because it allows us to obtain from Theorem 7.5 two systems of linear equations and therefore doubling the number of equations. In fact from Theorems 7.5 and 7.9 we obtain, for each $1 \le \alpha \le m$, the following systems of linear equations

$$\sum_{\substack{m-w \le j \le m \\ j \text{ even (odd)}}} (-2)^{-j} j! \binom{\alpha + w}{j + w - m} \dot{E}^{m+\alpha-j}(b_j) E^j = 0,$$

for $m + 1 - \alpha \le w \le m$. Which, after an appropriate change of variables and indices, become

$$\sum_{\delta \le r \le [\frac{m+\delta}{2}]} \binom{2r}{s} y_r = 0,$$

for $\delta \le s \le \alpha + \delta - 1$ and $\delta = 0, 1$. We observe that the coefficient matrices of these systems are nonsingular (see Proposition 7.10). Now, by decreasing induction on α in the interval $[\frac{m}{2}] \le \alpha \le m$, we prove the following theorem.

Theorem 7.11. *Let G_o be locally isomorphic to $SU(n, 1)$, $n \ge 2$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{[\frac{m}{2}]+m+1-j}(b_j) = 0$ for all $0 \le j \le m$.*

As a corollary of this theorem we obtain one of the conditions needed to establish Theorem 1.1 (see Theorem 4.5).

Corollary 7.12. *Let G_o be locally isomorphic to $SU(n, 1)$, $n \ge 2$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $d(b_j) \le 3m - 2j$ for all $0 \le j \le m$. In particular $d(b_m) \le m$.*

To complete the proof of Theorem 1.1 we need to show that if $b \in B$ then its leading term $\widetilde{b} = b_m \otimes Z^m \in \left(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\right)^W$. To obtain this result it is enough to prove that m is even. This is done in Subsection 7.1.

To any $b(x) \in U(\mathfrak{k})[x]$ we associate $c(x) \in U(\mathfrak{k})[x]$ defined by $c(x) = b(x + H - 1)$. We refer to $c(x)$ as $c_1(x)$ or $c_2(x)$ according as $\alpha = \alpha_1$ or $\alpha = \alpha_n$. Also we write $c_i(x) = \sum_{j=0}^{m} c_{i,j}\varphi_j(x)$ with $c_{i,j} \in U(\mathfrak{k})$ for $i = 1, 2$. Then Proposition 7.13 is a consequence of Theorems 5.3 and 7.9. In order to get a better insight of it, for $r = 0, \dots, m+1$ we introduce the column vectors $\sigma_r = \sigma_r(b)$ and $\tau_r = \tau_r(b)$ of $m + r + 1$ entries defined by

$$\sigma_r = (0, \dots, 0, \dot{E}_1^r(c_{1,m})E_1^{m-r}, \dots, \dot{E}_1^{m-1}(c_{1,r+1})E_1, \dot{E}_1^m(c_{1,r}), 0, \dots, 0)^t,$$
$$\tau_r = (\underbrace{0, \dots, 0}_{r}, \underbrace{\dot{E}_1^r(c_{2,m})E_1^{m-r}, \dots, \dot{E}_1^{m-1}(c_{2,r+1})E_1, \dot{E}_1^m(c_{2,r})}_{m+1-r}, \underbrace{0, \dots, 0}_{r})^t.$$

Let us observe that by definition $\sigma_{m+1} = \tau_{m+1} = 0$, and that the last $m+1$ entries of σ_r and τ_r are respectively of the form $\dot{E}_1^{r+j}(c_{1,m-j})E_1^{m-r-j}$ and $\dot{E}_1^{r+j}(c_{2,m-j})E_1^{m-r-j}$ for $0 \le j \le m$, see Theorem 6.3 and Lemma 6.7.

Let J_{m+r} be the $(m + r + 1) \times (m + r + 1)$ matrix with ones in the skew diagonal and zeros everywhere else. In the following corollary we rephrase Proposition 7.13 in terms of the vectors σ_r and τ_r.

Corollary 7.14. *Let $r \in \mathbb{N}_o$, $0 \le r \le m$. If $b = b_m \otimes Z^m + \dots + b_0 \in B$ and $\sigma_{r+1} = \tau_{r+1} = 0$ then*

$$J_{m+r}\sigma_r = (-1)^{m+r}\sigma_r \qquad \text{and} \qquad J_{m+r}\tau_r = \tau_r.$$

The vectors σ_r and τ_r are nicely related by a Pascal matrix. Let P_k denote the $(k+1) \times (k+1)$ lower triangular matrix with the (i, j)-entry equal to $\binom{i}{j}$, for $0 \le i, j \le k$.

Proposition 7.15. *If $r \in \mathbb{N}_o$, $0 \le r \le m$ and $\sigma_{r+1} = 0$ then $P_{m+r}\sigma_r = \tau_r$.*

For $0 \le t \le n$ we also need to consider certain $(t+1) \times (t+1)$ submatrices A of a Pascal matrix P_n formed by any choice of $t+1$ consecutive rows and $t+1$ consecutive columns of P_n, with the only condition that A does not have zeros in its main diagonal. In Proposition 7.16 we collect some results about these matrices that are very important in the proof that the algebra B does not contain elements of odd degree.

After all this preparation we are in a position to complete the proof of Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SU}(n, 1)$, $n \ge 2$. This is accomplished by proving the following results.

Lemma 7.17. *Let $n \in \mathbb{N}_0$ be an even number and let $v \in U(\mathfrak{k})^M$ be such that $\dot{E}^{t+1}(v) = 0$. If $n \ge 2t$ then there exists $b \in B$ of degree n with $b_n = v$ and $\sigma_{t+1}(b) = 0$.*

Theorem 7.18. *If G_o is locally isomorphic to $SU(n, 1)$, $n \ge 2$, and $b = b_m \otimes Z^m + \dots + b_0 \in B$ with m odd, then $b_m = 0$. That is, B does not contain odd degree elements.*

In Section 8 we prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{Sp}(n,1)$, with $n \geq 2$. Let χ denote the Cayley transform of $\mathfrak{g}$ associated to the unique root $\mu \in P_+$ that vanishes on $\mathfrak{t}$ and set $\mathfrak{h}_\mathfrak{k} = \chi(\mathfrak{h})$. We begin the section by constructing a particular Borel subalgebra $\mathfrak{b}_\mathfrak{k} = \mathfrak{h}_\mathfrak{k} \oplus \mathfrak{k}^+$ of $\mathfrak{k}$, tightly related to the root structure of $(\mathfrak{g}, \mathfrak{h})$, that is used to establish some important properties of the K-modules V_γ for each $\gamma \in \Gamma$ (see Propositions 8.7 and 8.9).

Next we define an appropriate Lie subalgebra $\widetilde{\mathfrak{g}}$ of $\mathfrak{g}$ that is σ and θ stable and its real form $\widetilde{\mathfrak{g}_o} = \mathfrak{g}_o \cap \widetilde{\mathfrak{g}}$ is isomorphic to $\mathfrak{sp}(2,1)$. This subalgebra is very useful since most of the calculations depend on it. If $\widetilde{\mathfrak{k}} = \mathfrak{k} \cap \widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{p}} = \mathfrak{p} \cap \widetilde{\mathfrak{g}}$ then $\widetilde{\mathfrak{g}} = \widetilde{\mathfrak{k}} \oplus \widetilde{\mathfrak{p}}$ is a Cartan decomposition of $\widetilde{\mathfrak{g}}$. Moreover $\widetilde{\mathfrak{h}} = (\mathfrak{t} \cap \widetilde{\mathfrak{g}}) \oplus \mathfrak{a}$ is a Cartan subalgebra of $\widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{m}} = \mathfrak{m} \cap \widetilde{\mathfrak{k}}$ is the centralizer of $\mathfrak{a}$ in $\widetilde{\mathfrak{k}}$. If $\mathfrak{h}_{\widetilde{\mathfrak{k}}} = \chi(\widetilde{\mathfrak{h}})$ then $\mathfrak{h}_{\widetilde{\mathfrak{k}}}$ is a Cartan subalgebra of $\widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{k}}$. The positive system $\Delta^+(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})$ defines a positive system $\Delta^+(\widetilde{\mathfrak{k}}, \mathfrak{h}_{\widetilde{\mathfrak{k}}}) = \{\delta, \gamma_1, \gamma_2, \gamma_3 = \gamma_1 + \gamma_2, \gamma_4 = 2\gamma_1 + \gamma_2\}$. Thus $\widetilde{\mathfrak{k}} \simeq \mathfrak{sp}(1, \mathbb{C}) \times \mathfrak{sp}(2, \mathbb{C})$.

In this case there is only one simple root $\alpha \in P_+$ and $Y_\alpha \neq 0$. Set $E = E_\alpha$, $Y = Y_\alpha$ and $Z = Z_\alpha$. A simple calculation shows that E is a root vector in $\widetilde{\mathfrak{k}}^+$ corresponding to γ_3, hence we set $X_{\gamma_3} = E$. Also we choose X_{γ_4} and X_δ so that $X_{\gamma_4} - X_\delta \in \widetilde{\mathfrak{m}}^+$. This determines the pair $\{X_{\gamma_4}, X_\delta\}$ up to a constant. Moreover it is easy to see that $\widetilde{\mathfrak{m}}^+$ is generated by $\{X_{\gamma_2}, X_{\gamma_4} - X_\delta\}$. To simplify the notation we define $X_{\pm 1} = X_{\pm\gamma_1}$, $X_{\pm 2} = X_{\pm\gamma_2}$, $X_{\pm 3} = X_{\pm\gamma_3}$, $X_{\pm 4} = X_{\pm\gamma_4}$ and $X = X_\delta$. We choose $H_1 \in [\mathfrak{k}_{\gamma_1}, \mathfrak{k}_{-\gamma_1}]$ and normalize the root vectors X_1, X_{-1}, X_2 and X_4 so that $\{H_1, X_1, X_{-1}\}$ is an $\mathfrak{s}$-triple and the following commutation relations hold,

$$[X_1, X_2] = E, \quad [X_1, E] = X_4, \quad [X_{-1}, E] = 2X_2, \quad [X_{-1}, X_4] = 2E.$$

Also we choose $H_2 \in [\mathfrak{k}_{\gamma_2}, \mathfrak{k}_{-\gamma_2}]$ such that $\gamma_2(H_2) = 2$ and normalize X_{-2} so that $\{H_2, X_2, X_{-2}\}$ is an $\mathfrak{s}$-triple. Then we define the vector H considered in (3) by $H = \frac{1}{2}H_2$.

Then in the same way as in the previous section, except for the step where the congruence modulo $U(\mathfrak{k})\mathfrak{m}^+$ is replaced by an equality, we obtain Corollary 8.5. For later reference we rewrite equation (iii) of Theorem 5.3 in the following theorem.

Theorem 8.6. *Let $b = \sum_{j=0}^m b_j x^j \in U(\mathfrak{k})[x]$ and $c(x) = b(x + H - 1)$. If $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$ and $0 \leq \ell, n$ we set*

$$\begin{aligned}\epsilon(\ell, n) = (-1)^n &\sum_{n \leq i \leq m} \dot{E}^\ell(c_i)\varphi_{i-n}(-\tfrac{n}{2} + \ell - \widetilde{Y})E^n \\ &- (-1)^\ell \sum_{\ell \leq i \leq m} \dot{E}^n(c_i)\varphi_{i-\ell}(-\tfrac{\ell}{2} + n - \widetilde{Y})E^\ell.\end{aligned}$$

Then, if $b \in B$ we have $\epsilon(\ell, n) \equiv 0$ for all $0 \leq \ell, n$.

As we proved in Theorem 4.6, to establish Theorem 1.1 we need to show that Theorem 4.5 holds, that is, if $b = b_m \otimes Z^m + \cdots + b_0 \in B$ then $d(b_m) \leq m$

and m is even. In the rest of the paper we show how to obtain these results from the equations $\epsilon(\ell, n) \equiv 0$ of Theorem 8.6.

In Subsection 8.1 we establish several transversality results that allow us to replace the congruence modulo the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ by an equality. In the following theorem we prove an important result in this direction.

Set $\mathfrak{q}^+ = \mathfrak{k}^+ - \mathbb{C}X_{\gamma_1}$, since γ_1 is a simple root, $\mathfrak{q}^+$ is a subalgbra of $\mathfrak{k}^+$. We are interested in considering vectors $v \in U(\mathfrak{k})^{\mathfrak{q}^+}$ of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$ with $a, b, c \in \mathbb{Z}$. Two examples of such vectors are the following, $v = \dot{X}_{-1}^t(u)$ and $v = \sum_{j\geq 0} u_j E^j$, where $u, u_j \in U(\mathfrak{k})$ are $\mathfrak{k}^+$-dominant weight vectors of irreducible K-modules in Γ so that v is a weight vector.

Theorem 8.10. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $v \in U(\mathfrak{k})^{\mathfrak{q}^+}$ be a vector of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$ where $a, b, c \in \mathbb{Z}$. Then $v \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ if and only if $v \equiv 0 \mod (U(\mathfrak{k})X_2)$.*

We give an indication of the proof of this theorem. Assume that $n > 2$, the case $n = 2$ will be considered later. Let $\mathfrak{h}_\mathfrak{r} = \ker(\gamma_1) \cap \ker(\gamma_2) \cap \ker(\delta)$, and let $\mathfrak{q}$ be the subalgebra of $\mathfrak{k}$ defined as follows

$$\mathfrak{q} = \mathfrak{q}^+ \oplus \mathfrak{h}_\mathfrak{r} \oplus \mathfrak{q}^- \tag{6}$$

where

$$\mathfrak{q}^- = \langle \{X_{-\alpha} : X_\alpha \in \mathfrak{q}^+ \text{ and } [X_\alpha, X_{-\alpha}] \in \mathfrak{h}_\mathfrak{r}\} \rangle.$$

Lemma 8.11. *Let $\mathfrak{q}$ be the subalgebra of $\mathfrak{k}$ defined in (6). Then there exists a semisimple subalgebra $\mathfrak{r}$ and a nilpotent subalgebra $\mathfrak{u}$ of $\mathfrak{q}$ such that $\mathfrak{q} = \mathfrak{r} \oplus \mathfrak{u}$, $[\mathfrak{r}, \mathfrak{u}] \subset \mathfrak{u}$ and $\mathfrak{h}_\mathfrak{r}$ is a Cartan subalgebra of $\mathfrak{r}$. Also, if we set $\mathfrak{l} = \mathfrak{m}^+ \cap \mathfrak{u}$ we have $[\mathfrak{r}, \mathfrak{l}] \subset \mathfrak{l}$ and there exists a positive system of roots $\Delta^+(\mathfrak{r}, \mathfrak{h}_\mathfrak{r})$ such that $\mathfrak{m}^+ = \mathfrak{r}^+ \oplus \mathfrak{l}$.*

If $v \in U(\mathfrak{k})^{\mathfrak{q}^+}$ is a vector as in Theorem 8.10, first we use Proposition 8.13 to reduce the congruence $\mod (U(\mathfrak{k})\mathfrak{m}^+)$ to a congruence $\mod (U(\mathfrak{k})\mathfrak{l})$. Next, applying Proposition 8.15 we show that $v \in U(\mathfrak{k})\langle\{X_2, X_4 - X\}\rangle$ and, finally, using Lemma 8.16 we show that $v \in U(\mathfrak{k})X_2$.

When $n = 2$ Theorem 8.10 follows directly from Lemma 8.16.

Corollary 8.17. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$. Let $v = \dot{X}_{-1}^t(u)$ or $v = \sum_{j\geq 0} u_j E^j$ be a vector of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$, where $u, u_j \in U(\mathfrak{k})$ are $\mathfrak{k}^+$-dominant weight vectors of irreducible K-modules in Γ with $u_j \neq 0$ only for a finite number of j's. Then $v \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ if and only if $v \equiv 0 \mod (U(\mathfrak{k})X_2)$.*

We finish this subsection proving the following results, which, toghether with Corollary 8.17 allow as to pass from a congruence $\mod (U(\mathfrak{k})\mathfrak{m}^+)$ to an equality.

Proposition 8.18. *Let $u, v \in U(\mathfrak{k})$ be dominant vectors for the $\mathfrak{s}$-triple $\{H_1, X_1, X_{-1}\}$. If $u + vE \equiv 0 \mod (U(\mathfrak{k})X_2)$ then $u = v = 0$.*

Corollary 8.19. *Let $u \in U(\mathfrak{k})$ be a $\mathfrak{k}^+$-dominant vector of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$ where $a, b, c \in \mathbb{N}_o$. Then $u \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ implies $u = 0$.*

In Subsection 8.2, we prove the following theorem which gives a bound for the Kostant degrees of the coefficients b_j of an element $b = b_m \otimes Z^m + \cdots + b_0$ in B. The proof of this theorem rests on two very delicate technical results obtained in Theorems 8.21 and 8.23.

Theorem8.24. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $b \in U(\mathfrak{k})^M$ be such that $\dot{E}^{m+1}(b) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$. Then $d(b) \leq 2m$.*

Now from Corollary 8.5 and Theorem 8.24 we obtain,

Corollary 8.25. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $b = b_m \otimes Z^m + \cdots + b_0 \in B$. Then $d(b_r) \leq 2(2m - r)$ for every $0 \leq r \leq m$.*

This corollary implies, in particular, that $d(b_m) \leq 2m$. In Subsection 8.3 we set up an inductive process whose out put is to prove that $d(b_m) \leq m$ and that m is even, for every $b = b_m \otimes Z^m + \cdots + b_0 \in B$ with $b_m \neq 0$.

Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and set $d_r = 2m - r$ for every $0 \leq r \leq m$. Then, in view of Corollary 8.25, for each $0 \leq r \leq m$ we may write

$$b_r = \sum_{t=0}^{2d_r} \sum_{\max\{0,t-d_r\} \leq i \leq [t/2]} b^r_{2i,t-2i}, \tag{7}$$

where $b^r_{2i,t-2i}$ is an M-invariant element in $U(\mathfrak{k})$ of type $(2i, t-2i)$. To prove that $d(b_m) \leq m$ and that m is even we need to show that certain K-types are zero. To do this we consider, for $m - 1 \leq T \leq 4m$, the propositional function $P(T)$, associated to $b \in B$, defined as follows

$$P(T) : b_r = \sum_{t=0}^{\min\{T-r,2d_r\}} \sum_{\max\{0,t-d_r\} \leq i \leq [t/2]} b^r_{2i,t-2i}, \qquad 0 \leq r \leq m. \tag{8}$$

Observe that $P(m-1)$ is true precisely when $b_m = 0$ and that, in view of Corollary 8.25 and (7), $P(4m)$ holds. This is the starting point of a decreasing inductive process.

Assuming that $P(T)$ holds, we construct a homogeneous system of linear equations where the unknowns are $\mathfrak{k}^+$-highest weight vectors corresponding to the K-types that we want to prove to be zero. The first results are given in Propositions 8.27 and 8.28 which follow from Theorem 8.6.

Observe that the unknowns in equations (145) of Proposition 8.28 are not $\mathfrak{k}^+$-highest weight vectors, so we replace this system by an equivalent one where all the unknowns become $\mathfrak{k}^+$-highest weight vectors. To do this we let $\widetilde{\epsilon}(\ell, n)$, for $0 \leq \ell, n$, denote the left hand side of equation (145) and for a fixed $0 \leq n \leq \min\{2m, T\}$ we consider, for any $0 \leq L \leq \min\{2m, T\} - n$, the following linear combination

$$\mathcal{E}_L(n) = \sum_{\ell=0}^{L} (-2)^\ell \tbinom{L}{\ell} \widetilde{\epsilon}(\ell, n) E^{L-\ell} X_4^{\ell+n}.$$

Observe that under the hypothesis of Proposition 8.28 we have $\mathcal{E}_L(n) \equiv 0$. The following lemma plays an important role in the final expression of the system $\mathcal{E}_L(n) \equiv 0$ for $0 \le n \le \min\{2m, T\}$ and $0 \le L \le \min\{2m, T\} - n$.

Lemma 8.30. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \ge 2$ and let $b_{2i,j} \in U(\mathfrak{k})^M$ be an M-invariant element of type $(2i, j)$. For $0 \le k \le 2i$ set*

$$D_k(b_{2i,j}) = \Sigma_{\ell=0}^{k} (-2)^\ell \binom{k}{\ell} \binom{j+\ell}{\ell}^{-1} \dot{X}^{2i-\ell} \dot{E}^{j+\ell}(b_{2i,j}) E^{k-\ell} X_4^\ell.$$

Then $D_k(b_{2i,j})$ is a $\mathfrak{k}^+$-dominant vector of weight $i(\gamma_4 + \delta) + (j+k)\gamma_3$ with respect to $\mathfrak{h}_\mathfrak{k}$.

To prove that $P(T)$ implies $P(T-1)$ for a fixed $m \le T \le 4m$, we introduce another propositional function $Q(n)$ defined for $0 \le n \le \min\{T, 4m-T\}+1$ as follows:

$$Q(n): \quad b^r_{2i,T-r-2i} = 0 \quad if \quad 0 \le T - r - 2i < n \quad for \quad 0 \le r \le m. \tag{9}$$

Observe that $Q(0)$ is obviously true. Then we carry out an increasing induction on n in the range $0 \le n \le \min\{T, 4m - T\}$. To do this we use the system $\mathcal{E}_L(n) \equiv 0$ which is written in its final form in the following theorem.

Theorem 8.31. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and take $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m - T\}$. If $P(T)$ and $Q(n)$ are true then for all L such that $0 \le L \le \min\{2m, T\} - n$ we have*

$$\begin{aligned} &\sum_{\substack{r,k \\ T-n \ge 2k+r \ge T-L}} B_{r,k}(T,n,L) D_{L+2k+r-T}(b^r_{2k,T-r-2k})(XX_4)^{T-k} E^n \\ &\quad - \sum_{\substack{r,\ell \\ r \equiv T-n}} (-2)^\ell \binom{L}{\ell} \binom{T-n-\ell}{r-\ell} u^r_{T-r-n,n} (XX_4)^{(T+r+n)/2} E^L \equiv 0, \end{aligned} \tag{10}$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r} \dot{E}^n (b^r_{T-n-r,n})$ and

$$B_{r,k}(T,n,L) = r!(-1)^T 2^{T-r-2k} \binom{L}{T-r-2k} \binom{T-L-n}{r-n}.$$

At this point we are in a good position to derive from Theorem 8.31 the systems of equations that we use. For any $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m - T\}$ consider the following sets,

$L(T,n) = \{L \in \mathbb{N}_0 : 0 \le L \le \min\{2m, T\} - n,\ L \equiv n + 1\ (2)\}$,

$R(T,n) = \{r \in \mathbb{N}_0 : 0 \le r \le \min\{m, \min\{T, 4m - T\} - n\},\ r \equiv T - n\ (2)\}$.

Let $|L(T,n)|$ and $|R(T,n)|$ denote the cardinality of these sets. Now applying succesively Theorem 8.31, Corollary 8.17, Lemma 8.20 and Proposition 8.18 we obtain,

Theorem 8.32. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and take $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m - T\}$. If $P(T)$ and $Q(n)$ are true then for $L \in L(T,n)$ we have*

$$\sum_{r \in R(T,n)} \Big(\sum_{\ell} (-2)^\ell \binom{L}{\ell} \binom{T-n-\ell}{r-\ell} \Big) u^r_{T-r-n,n} (XX_4)^{(T+r+n)/2} = 0, \tag{11}$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r}\dot{E}^n(b^r_{T-n-r,n})$.

From this theorem we obtain a system of $|L(T,n)|$ linear equations in the $|R(T,n)|$ elements $u^r_{T-r-n,n}$. Let $A(T,n)$ denote the coefficient matrix of this system. In Lemma 8.33 we compare the cardinalities of the sets $|R(T,n)|$ and $|L(T,n)|$.

To study the coefficient matrix $A(T,n)$, in Subsection 8.4, we consider the following generalized version of $A(T,n)$. Given a sequence of integers $0 \le L_0 < \cdots < L_k$ and $\delta = 0, 1$ we consider the $(k+1) \times (k+1)$ matrix $A(s)$ with polynomial entries $A_{i,j}(s) \in \mathbb{C}[s]$ defined as follows

$$A_{ij}(s) = \sum_{0 \le \ell \le \min\{L_i, 2j+\delta\}} (-2)^\ell \binom{L_i}{\ell} \binom{s-\ell}{2j+\delta-\ell}. \tag{12}$$

Then the main result of this subsection is the following,

Theorem 8.39. *Given a sequence of integers $0 \le L_0 < L_1 < \cdots < L_k$ consider the set $R = \{L_i + L_j : 0 \le i < j \le k\}$ and for any $r \in R$ let*

$$m(r) = |\{(i,j) : 0 \le i < j \le k,\ r = L_i + L_j\}|.$$

Then
(i) If $\delta = 0$,

$$\det A(s) = c \prod_{r \in R} (s-r)^{m(r)}.$$

(ii) If $\delta = 1$,

$$\det A(s) = c \prod_{i=0}^{k} (s - 2L_i) \prod_{r \in R} (s-r)^{m(r)}.$$

Here c is a nonzero constant computed in Proposition 8.36.

We are particularly interested in the sequence $L_i = 2i + \epsilon$ for $0 \le i \le k$ and $\epsilon \in \{0, 1\}$. For q and k nonnegative integers we let $A(q)$ denote the $(k+1) \times (k+1)$ matrix obtain from $A(s)$ by evaluating at $s = q$. Then, from Theorem 8.39 we obtain the following corollary.

Corollary 8.40. *If $\epsilon, \delta \in \{0,1\}$, $k \ge 1$ and $L_i = 2i + \epsilon$ for $0 \le i \le k$ the matrix $A(q)$ is nonsingular if and only if $q \ge 2k + \delta$ and $q \ne 2k, 2k+2, \ldots, 4k + 2(\epsilon + \delta - 1)$.*

In Subsection 8.5 we prove Theorem 4.5 which in turns implies our main result (Theorem 1.1). We begin by considering the following linear subspace $\widetilde{B}$ of the algebra B,

$$\widetilde{B} = \{b \in B : b^{2r}_{2i,j} = 0 \text{ if } i + j \le r \text{ and } 0 \le 2r \le \deg(b)\}.$$

Then, using Proposition 4.4, we establish the following result.

Proposition 8.41. *Theorem 4.5 holds if and only if $\widetilde{B} = 0$.*

Given $b = b_m \otimes Z^m + \dots + b_0 \in \widetilde{B}$ we prove that $P(T)$ implies $P(T-1)$ for any $m \le T \le 4m$. Hence $P(m-1)$ is true, which implies that $b_m = 0$ and therefore that $b = 0$.

In view of the definition of $\widetilde{B}$, when $T-n \equiv 0$ we can change the index set $R(T,n)$ in (11) by a smaller set $\widetilde{R}(T,n)$ obtained by removing from $R(T,n)$ those indexes r for which $d(b^r_{T-r-n,n}) = T-r+n \le r$. Thus we define

$$\widetilde{R}(T,n) = \{r \in R(T,n) : r < \tfrac{T+n}{2} \text{ if } r \equiv 0\}.$$

Then Theorem 8.31 and Theorem 8.32 can be reformulated as follows.

Theorem 8.42. *Let $b = b_m \otimes Z^m + \dots + b_0 \in \widetilde{B}$ and take $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m-T\}$. If $P(T)$ and $Q(n)$ are true then for all L such that $0 \le L \le \min\{2m, T\} - n$ we have*

$$\begin{aligned}(13)\qquad &\sum_{\substack{r,k\\ T-n\ge 2k+r\ge T-L}} B_{r,k}(T,n,L) D_{L+2k+r-T}(b^r_{2k,T-r-2k})(XX_4)^{T-k}E^n \\ &\quad - \sum_{\substack{r,l\\ r\in\widetilde{R}(T,n)}} (-2)^l \tbinom{L}{l}\tbinom{T-n-l}{r-l} u^r_{T-r-n,n}(XX_4)^{(T+r+n)/2}E^L \equiv 0.\end{aligned}$$

Theorem 8.43. *Let $b = b_m \otimes Z^m + \dots + b_0 \in \widetilde{B}$ and take $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m-T\}$. If $P(T)$ and $Q(n)$ are true then for all $L \in L(T,n)$ we have*

$$(14)\qquad \sum_{r\in\widetilde{R}(T,n)} \Big(\sum_{\ell} (-2)^\ell \tbinom{L}{\ell}\tbinom{T-n-\ell}{r-\ell}\Big) u^r_{T-r-n,n}(XX_4)^{(T+r+n)/2} = 0,$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r}\dot{E}^n(b^r_{T-n-r,n})$.

Let $b = b_m \otimes Z^m + \dots + b_0 \in \widetilde{B}$ and $m \le T \le 4m$ be such that $P(T)$ is true. To prove that $P(T-1)$ holds we need to show that $Q(n)$ implies $Q(n+1)$ for every $0 \le n \le \min\{T, 4m-T\}$. Assume that $Q(n)$ holds. In view of Lemma 8.33 there are two possibilities:

$$(15)\qquad |\widetilde{R}(T,n)| \le |L(T,n)| \quad \text{or} \quad |\widetilde{R}(T,n)| = |L(T,n)| + 1.$$

In the first case we let $k = |\widetilde{R}(T,n)| - 1$ and consider the equations (14) corresponding to $\{L_i = 2i+\epsilon : 0 \le i \le k\} \subset L(T,n)$ where $\epsilon = (1+(-1)^n)/2$. Thus from Theorem 8.43 we obtain a $(k+1)\times(k+1)$ system of linear equations whose coefficient matrix $A(T,n)$ is exactly the matrix $A(T-n)$ defined in (12) for $s = T-n$, $\delta = \big(1-(-1)^{T-n}\big)/2$ and corresponding to the sequence $\{L_i = 2i+\epsilon : 0 \le i \le k\}$.

If $T-n \equiv 1$ it follows from Corollary 8.40 that $A(T-n)$ is nonsingular, hence we obtain $u^r_{T-r-n,n} = 0$ proving that $Q(n+1)$ holds. On the other hand, if $T-n \equiv 0$ the matrix $A(T-n)$ turns out, in general, to be singular. Therefore in order to prove that $Q(n+1)$ holds we need to consider another system of equations derived from Theorem 8.42. This is carried out in full detail in Proposition 8.44.

Now we use the system of equations obtained from Theorem 8.43 whenever it is nonsingular, and when it is singular we use Proposition 8.44 to establish the following result.

Proposition 8.45. *If $m \geq 1$ and $2m+1 \leq T \leq 4m$ then $P(T-1)$ follows from $P(T)$. Therefore $P(2m)$ holds.*

Now we consider the second possibility of (15). In this case Theorem 8.43 does not provide enough equations to form a square system. In order to obtain a nonsingular square system we consider, besides the equations (14), others taken from (13). This is carried out in the proof of the following proposition.

Proposition 8.46. *If $m \geq 1$ and $m \leq T \leq 2m$ then $P(T-1)$ follows from $P(T)$. Therefore $P(m-1)$ holds.*

As we noted before this proposition completes the proof of Theorem 1.1.

3. The algebra B

Let $\mathfrak{t}_o$ be a Cartan subalgebra of the Lie algebra $\mathfrak{m}_o$ of M_o. Set $\mathfrak{h}_o = \mathfrak{t}_o \oplus \mathfrak{a}_o$ and let $\mathfrak{h} = \mathfrak{t} \oplus \mathfrak{a}$ be the corresponding complexification. Then $\mathfrak{h}_o$ and $\mathfrak{h}$ are Cartan subalgebras of $\mathfrak{g}_o$ and $\mathfrak{g}$, respectively. Now we choose a Borel subalgebra $\mathfrak{t} \oplus \mathfrak{m}^+$ of the complexification $\mathfrak{m}$ of $\mathfrak{m}_o$ and take $\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{m}^+ \oplus \mathfrak{n}$ as a Borel subalgebra of $\mathfrak{g}$. Let Δ and Δ^+ be, respectively, the corresponding sets of roots and positive roots of $\mathfrak{g}$. As usual ρ is half the sum of the positive roots. Also if $\alpha \in \Delta$, X_α will be a nonzero root vector associated to α. Moreover, θ will denote the Cartan involution, and $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$ the Cartan decomposition of $\mathfrak{g}$ corresponding to (G_o, K_o).

If $\langle\, , \rangle$ denotes the Killing form of $\mathfrak{g}$, for each $\alpha \in \Delta$ let $H_\alpha \in \mathfrak{h}$ be the unique element such that $\phi(H_\alpha) = 2\langle \phi, \alpha\rangle / \langle \alpha, \alpha \rangle$ for all $\phi \in \mathfrak{h}^*$, and let $\mathfrak{h}_{\mathbb{R}}$ be the real span of $\{H_\alpha : \alpha \in \Delta\}$. Also set $H_\alpha = Y_\alpha + Z_\alpha$ where $Y_\alpha \in \mathfrak{t}$ and $Z_\alpha \in \mathfrak{a}$, and let $P_+ = \{\alpha \in \Delta^+ : Z_\alpha \neq 0\}$.

If $\alpha \in P_+$ let $\mathfrak{a}_\alpha = \{H \in \mathfrak{a} : \alpha(H) = 0\}$. Then $\mathfrak{a} = \mathfrak{a}_\alpha \oplus \mathbb{C}Z_\alpha$ and we can consider the elements in $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ as polynomials in Z_α with coefficients in $U(\mathfrak{k}) \otimes U(\mathfrak{a}_\alpha)$. Now we quote Theorem 5 and Corollary 6 of [24].

Theorem 3.1. *(i) If $\alpha \in P_+$ is a simple root and $n \in \mathbb{N}$, for all $u \in U(\mathfrak{g})^K$, $b = P(u)$ satisfies*

$$\begin{aligned} P(X_{-\alpha}^n)&(n - Y_\alpha - 1) b(n - Y_\alpha - 1) \\ &\equiv b(-n - Y_\alpha - 1) P(X_{-\alpha}^n)(n - Y_\alpha - 1), \end{aligned} \tag{16}$$

where the congruence is $\operatorname{mod}\big(U(\mathfrak{k})\mathfrak{m}^+ \otimes U(\mathfrak{a}_\alpha)\big)$.
(ii) Let $B = \{b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a}) : (16)$ holds for all $\alpha \in P_+$ simple, $n \in \mathbb{N}\}$. Then B is a subalgebra of $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$.

Let us now consider the symmetric pair (U_o, K_o)=(SL(2,$\mathbb{R}$),SO(2)), and let $U_o = K_oA_oN_o$ be the Iwasawa decomposition of U_o, where A_o and N_o are, respectively, the subgroups of all diagonal matrices and all upper triangular matrices in U_o. Let $\{H, X, Y\}$ be the usual $\mathfrak{s}$-triple in $\mathfrak{u}_o$ with $H \in \mathfrak{a}_o$ and $X \in \mathfrak{n}_o$. Let $P : U(\mathfrak{u}) \longrightarrow U(\mathfrak{k}) \otimes U(\mathfrak{a})$ be the projection map introduced above. We are interested in computing $P(Y^n)$.

Let (V_n, π_n) be the irreducible representation of $\mathfrak{u}$ of dimension $n+1$, and let $P_{n+1}(t)$ be the characteristic polynomial of $\pi_n(E)$, where $E = P(Y) = Y - X$.

Lemma 3.2. *If we view the elements in $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ as polynomials in H with coefficients in $U(\mathfrak{k})$, then $P(Y^{n+1})(n) = P_{n+1}(E)$ for all $n \in \mathbb{N}_o$.*

Proof. Let $v_n \neq 0$ be a dominant weight vector in V_n. Then

$$P(Y^{n+1})(n) \cdot v_n = Y^{n+1} \cdot v_n = 0. \tag{17}$$

By writing $Y = E + X$ it is easy to see that $P(Y^{n+1})(n) = E^{n+1} + a_nE^n + \cdots + a_0$, for some $a_i \in \mathbb{Z}$. Then from (17) it follows that

$$E^{n+1} \cdot v_n + a_nE^n \cdot v_n + \cdots + a_0v_n = 0. \tag{18}$$

Since $\{E^n \cdot v_n, E^{n-1} \cdot v_n, \dots, v_n\}$ is a basis of V_n it follows that the $(n+1)$-tuple $(a_n, \dots, a_0)$ is uniquely determined by (18).

Also $P_{n+1}(E) = E^{n+1}+b_nE^n+\cdots+b_0$ satisfies $P_{n+1}(E)\cdot V_n = 0$, therefore $b_i = a_i$ for $i = 0, \dots, n$; hence $P(Y^{n+1})(n) = P_{n+1}(E)$. This completes the proof of the lemma.

Lemma 3.3. *The characteristic polynomial of $\pi_n(E)$ is given by*

$$P_{n+1}(t) = \begin{cases} \prod_{j=1}^{k} \left(t^2 + (2j-1)^2\right), & \text{if } n = 2k-1 \\ t\prod_{j=1}^{k} \left(t^2 + (2j)^2\right), & \text{if } n = 2k. \end{cases} \tag{19}$$

Proof. The element E is conjugate to $\sqrt{-1}H$ by an element in SU(2), and the caracteristic polynomial of $\pi_n(\sqrt{-1}H)$ is given by

$$\det\left(t - \pi_n(\sqrt{-1}H)\right) = \prod_{j=0}^{n} \left(t - \sqrt{-1}(n-2j)\right).$$

From this the lemma follows.

Let us now go back to the general case where G_o is any connected, non-compact real semisimple Lie group with finite center. For any $\alpha \in P_+$ we shall consider the three dimensional simple Lie algebra $\mathfrak{u}_\alpha$ spanned by an $\mathfrak{s}$-triple of the form $\{H_\alpha, X_\alpha, X_{-\alpha}\}$. Also let (V_n, π_n) denote the irreducible representation of $\mathfrak{u}_\alpha$ of dimension $n+1$, and let $P_{n+1}(t)$ be the characteristic polynomial of $\pi_n(E_\alpha)$, where $E_\alpha = P(X_{-\alpha}) = X_{-\alpha} + \theta X_{-\alpha}$.

Proposition 3.4. *For all $\alpha \in P_+$ and all $n \in \mathbb{N}$, $P(X_{-\alpha}^n)(n - Y_\alpha - 1) = P_n(E_\alpha)$. Moreover:*
(i) If $Y_\alpha \neq 0$, then E_α is nilpotent, hence $P_n(t) = t^n$.

(ii) If $Y_\alpha = 0$*, then* E_α *is semisimple and we may assume that* $\theta X_\alpha = -X_{-\alpha}$*. In this case* $P_n(t)$ *is given by* (19)*.*

Proof. (i) Let σ denote the conjugation of $\mathfrak{g}$ with respect to the Lie algebra $\mathfrak{g}_o$ of G_o. Now define α^σ and α^θ by $\alpha^\sigma(H) = \overline{\alpha(\sigma H)}$, $\alpha^\theta(H) = \alpha(\theta H)$ ($H \in \mathfrak{h}$). Then α^σ and α^θ are again members of Δ. Moreover $\alpha^\sigma = -\alpha^\theta$, $-\alpha^\theta \in P_+$ and $\alpha^\sigma \neq \alpha$ because $Y_\alpha \neq 0$. (See [9], Lemma 3.3, p. 222.) Also $\alpha^\sigma - \alpha \notin \Delta$ ([28], Lemma 1.1.3.6, p. 25). Therefore $[X_{-\alpha}, \theta X_{-\alpha}] = 0$, hence E_α is nilpotent. Now since $[E_\alpha, \theta X_{-\alpha}] = [X_{-\alpha} + \theta X_{-\alpha}, \theta X_{-\alpha}] = 0$ we have $X_{-\alpha}^n = (E_\alpha - \theta X_{-\alpha})^n = \sum \binom{n}{j} E_\alpha^{n-j}(-\theta X_{-\alpha})^j$ which implies that $P(X_{-\alpha}^n) = E_\alpha^n = P_n(E_\alpha)$.

(ii) Since we are assuming that $Y_\alpha = 0$ we have $\alpha^\theta = -\alpha^\sigma = -\alpha$, thus $\theta(H_\alpha) = -H_\alpha$, and we may assume that $\theta X_\alpha = -X_{-\alpha}$. Now the linear map $\psi : \mathfrak{u}_\alpha \to \mathfrak{u}$ defined by $\psi(H_\alpha) = H$, $\psi(X_\alpha) = X$ and $\psi(X_{-\alpha}) = Y$ is a Lie algebra isomorphism commuting with the Cartan involutions. Then $\psi(E_\alpha) = E$, and the assertion follows from Lemmas (3.2) and (3.3).

Corollary 3.5. *If* $\alpha \in P_+$ *is a simple root and* $n \in \mathbb{N}$*, for all* $u \in U(\mathfrak{g})^K$ $b = P(u)$ *satisfies*

$$P_n(E_\alpha) b(n - Y_\alpha - 1) \equiv b(-n - Y_\alpha - 1) P_n(E_\alpha), \tag{20}$$

where the congruence is $\operatorname{mod}\big(U(\mathfrak{k})\mathfrak{m}^+ \otimes U(\mathfrak{a}_\alpha)\big)$*.*

Definition 3.6. Let B be the subalgebra of all elements $b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ satisfying (20) for all simple roots $\alpha \in P_+$ and all $n \in \mathbb{N}$.

4. The image of $U(\mathfrak{g})^K$

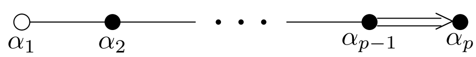
From now on we shall assume that G_o is a connected, noncompact real semisimple Lie group, with finite center and of split rank one. Observe that our main result Theorem 1.1 depends only on the local isomorphism class of the group G_o. From Cartan's classification we know that G_o is locally isomorphic to one and only one of the following groups: $\mathrm{SO}(n,1)_e$, $\mathrm{SU}(n,1)$, $\mathrm{Sp}(n,1)$, $n \geq 2$, and an exceptional group F_4.

The Dynkin-Satake diagrams of these groups are:

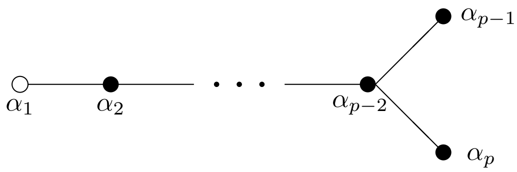
(i) $G_o = \mathrm{SO}(2,1)_e$.

(ii) $G_o = \mathrm{SO}(3,1)_e$.

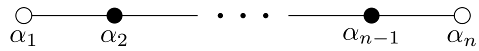
(iii) $G_o = \mathrm{SO}(2p,1)_e$, $p \geq 2$.



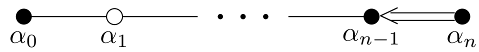
(iv) $G_o = \mathrm{SO}(2p-1,1)_e$, $p \geq 3$.



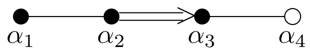
(v) $G_o = \mathrm{SU}(n,1)$, $n \geq 2$.



(vi) $G_o = \mathrm{Sp}(n,1)$, $n \geq 2$.



(vii) $G_o = \mathrm{F}_4$.



In all cases the simple roots α in P_+ are represented by a white circle, and $Y_\alpha \neq 0$, except in (i) where $Y_\alpha = 0$. Moreover in all cases, except in (iv), $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$.

We shall now prove Theorem 1.1 in case (i). The reason for doing this at this point is that this case does not fit into the general pattern that works for the other groups. The groups $\mathrm{SO}(2,1)_e$, SU(1,1) and SL(2,$\mathbb{R}$) are locally isomorphic. To prove the main theorem we prefer to take $G_o =$ SL(2,$\mathbb{R}$) and the Iwasawa decomposition $G_0 = K_oA_oN_o$ where $K_o = \mathrm{SO}(2)$, A_o is the subgroup of all diagonal matrices and N_o is the group of all upper triangular matrices with ones in the diagonal. The centralizer M_o of A_o in K_o is the group $\{\pm I\}$. Therefore $\mathfrak{h} = \mathfrak{a}$ is a Cartan subalgebra of $\mathfrak{g}$ and $\alpha(x(E_{11} - E_{22})) = 2x$ is the only positive root. Moreover $H_\alpha = E_{11} - E_{22}$, $Y_\alpha = 0$, and we set $Z = Z_\alpha = H_\alpha$. If we take $X_{-\alpha} = E_{21}$ then $E = X_{-\alpha} + \theta X_{-\alpha} = E_{21} - E_{12}$.

To compute $U(\mathfrak{g})^K$ it is convenient to choose an $\mathfrak{s}$-triple $\{h, e, f\}$ with $h \in \mathfrak{k}$. For example we may take $h = iE$, $e = \frac{1}{2}(-iE_{11} + E_{12} + E_{21} + iE_{22})$ and $f = \frac{1}{2}(iE_{11} + E_{12} + E_{21} - iE_{22})$. Then $U(\mathfrak{g})^K$ is the linear span of the basis elements $\{h^j(ef)^k\}$, that is the polynomial algebra $\mathbb{C}[h, ef]$.

In this case $U(\mathfrak{k})^M = U(\mathfrak{k}) = \mathbb{C}[E]$, therefore $P : U(\mathfrak{g})^K \longrightarrow U(\mathfrak{k}) \otimes U(\mathfrak{a})$ is an injective homomorphism of algebras. Thus its image is the polynomial algebra generated by the algebraically independent elements E and $Z(Z+2)$, since

$$P(h) = iE \quad \text{and} \quad P(ef) = \tfrac{1}{4}\big(H_\alpha(H_\alpha + 2) + E(E - 2i)\big).$$

On the other hand by Definition 3.6, the algebra B is the set of all elements $b \in U(\mathfrak{k}) \otimes U(\mathfrak{a})$, considered as polynomials in Z with coefficients in $U(\mathfrak{k})$, which satisfy the following system of equations

$$P_n(E)b(n-1) = b(-n-1)P_n(E), \quad n \in \mathbb{N}.$$

The polynomials $P_n(t)$ were computed in Lemma 3.3. But $P_n(E)$ commutes with the coefficients of b, therefore the above equations reduce to

$$b(n-1) = b(-n-1), \quad n \in \mathbb{N}.$$

Hence it is clear that B is the polynomial algebra generated by the constant polynomial E and $Z(Z+2)$, proving that $P\big(U(\mathfrak{g})^K\big) = B$.

To prove Theorem 1.1 in the other cases we have to work much more, in particular we need to quote a restriction theorem from [23] and Theorem 9 of [24]. To do this we introduce some notation.

Let G be the adjoint group of $\mathfrak{g}$ and let K be the connected Lie subgroup of G with Lie algebra $ad_{\mathfrak{g}}(\mathfrak{k})$. Also let $M = \mathrm{Centr}_K(\mathfrak{a})$, $M' = \mathrm{Norm}_K(\mathfrak{a})$ and $W = M'/M$. If H is a group and V a finite dimensional H-module over $\mathbb{C}$, let $S(V^*)$ denote the ring of all polynomial functions on V, and let $S(V^*)^H$ denote the subring of all H-invariants. Also let $S^n(V^*)$ denote the corresponding homogeneous subspace of $S(V^*)$ of degree n. We shall need to know the image of the homomorphism $\pi : S(\mathfrak{g}^*)^K \to S((\mathfrak{k} \oplus \mathfrak{a})^*) = S(\mathfrak{k}^*) \otimes S(\mathfrak{a}^*)$ induced by restriction from $\mathfrak{g}$ to $\mathfrak{k} \oplus \mathfrak{a}$.

Let Γ denote the set of all equivalence classes of irreducible holomorphic finite dimensional K-modules V_γ such that $V_\gamma^M \neq 0$. Any $\gamma \in \Gamma$ can be realized as a submodule of all harmonic polynomial functions on $\mathfrak{p}$, homogeneous of degree d, for a uniquely determined $d = d(\gamma)$ (Kostant, see [16]). If V is any K-module and $\gamma \in \hat{K}$ then V_γ will denote the isotypic component of V corresponding to γ.

Let $C = S(\mathfrak{k}^*)^M$ and let $C_d = \bigoplus S(\mathfrak{k}^*)_\gamma^M$, where the sum is over all $\gamma \in \Gamma$ such that $d(\gamma) \leq d$. Then $C = \bigcup_{d \geq 0} C_d$ is a nice ascending filtration of C. Now

$$D = \bigoplus_{d \geq 0} (C_d \otimes S^d(\mathfrak{a}^*))$$

is an algebra, precisely the Rees algebra associated to the filtration $C = \bigcup_{d \geq 0} C_d$. Moreover D is stable under the tensor product action of W on $S(\mathfrak{k}^*)^M \otimes S(\mathfrak{a}^*)$. Let D^W denote the ring of all W invariants in D.

Theorem 4.1. (See [23] and [1].) *The operation of restriction from $\mathfrak{g}$ to $\mathfrak{k} \oplus \mathfrak{a}$ induces an isomorphism of $S(\mathfrak{g}^*)^K$ onto D^W.*

Let $F = U(\mathfrak{k})^M$ and let $F_d = \bigoplus U(\mathfrak{k})_\gamma^M$, where the sum is over all $\gamma \in \Gamma$ such that $d(\gamma) \leq d$. Then $F = \bigcup_{d \geq 0} F_d$ is a nice ascending filtration of F. If $b \in F$ we define $d(b) = \min\{d \in \mathbb{N}_o : b \in F_d\}$ and we call it the *Kostant degree* of b.

If $0 \neq b \in U(\mathfrak{k}) \otimes U(\mathfrak{a})$ we can write $b = b_m \otimes Z^m + \cdots + b_0$ in a unique way with $b_j \in U(\mathfrak{k})$ for $j = 0, \ldots, m$, $b_m \neq 0$ and $Z = Z_\alpha$ for any $\alpha \in P_+$

simple. We shall refer to b_m (resp. $\widetilde{b} = b_m \otimes Z^m$) as the *leading coefficient* (resp. *leading term*) of b and to m as the *degree* of b. Also let 0 be the leading coefficient and the leading term of $b = 0$.

Now we rephrase Theorem 9 of [24] in the following way.

Theorem 4.2. *In the rank one case the following statements are equivalent:*
(i) For any $b \in B^{\widetilde{W}}$ there exists $u \in U(\mathfrak{g})^K$ such that $P(u) = b$.
(ii) If b_m is the leading coefficient of any $b \in B^{\widetilde{W}}$ then $d(b_m) \leq m$.

At this point it is convenient to point out the following property of the image $P(U(\mathfrak{g})^K)$, which follows from Theorem 4.5 of [17] and Theorem 4.2.

Proposition 4.3. *If $b = b_m \otimes Z^m + \cdots + b_0 \in P(U(\mathfrak{g})^K)$ then its leading term $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and $d(b_m) \leq m$.*

In what follows $\big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ will denote the ring of all W-invariants in $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$, under the tensor product action of the Weyl group.

Proposition 4.4. *If $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and $d(b_m) \leq m$, then there exits $u \in U(\mathfrak{g})^K$ such that $\widetilde{b}$ is the leading term of $b = P(u)$.*

Proof. We refer the reader to Section 3 of [24] for the unexplained notation. The proof is by induction on $\beta(\widetilde{b}) = \rho_o(\widetilde{b}) - m \geq 0$. If $\beta(\widetilde{b}) = 0$ then $\widetilde{b} \in \big(\mathbb{C} \otimes U^m(\mathfrak{a})\big)^W$ and $\sigma_o^m(\widetilde{b}) \in \big(\mathbb{C} \otimes S^m(\mathfrak{a}^*)\big)^W$. Thus from Theorem 4.1 there exists $\xi \in S^m(\mathfrak{g}^*)^K$ such that $\pi(\xi) = \sigma_o^n(\widetilde{b})$. Let $w = \sigma^{-1}(\xi) \in U(\mathfrak{g})^K_m$. Now $\sigma_o^m(\widetilde{F(w)}) = \sigma_o^m(\widetilde{b})$ and $\sigma_o^m(\widetilde{P(w)}) = \sigma_o^m(\widetilde{F(w)}) = \sigma_o^m(F(w)) = \sigma_o^m(\widetilde{b})$. Therefore $\rho_o(\widetilde{P(w)} - \widetilde{b}) < m$ which implies that $\widetilde{P(w)} = \widetilde{b}$.

Now assume that $\beta(\widetilde{b}) > 0$ and that the proposition is true for all $\widetilde{a} = a_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ such that $\beta(\widetilde{a}) < \beta(\widetilde{b})$. If $n = \rho_o(\widetilde{b})$ then, by hypothesis, $\sigma_o^n(\widetilde{b}) \in \big(C_m \otimes S^m(\mathfrak{a}^*)\big)^W$. Thus from Theorem 4.1 there exists $\xi \in S^n(\mathfrak{g}^*)^K$ such that $\pi(\xi) = \sigma_o^n(\widetilde{b})$. Let $w = \sigma^{-1}(\xi) \in U(\mathfrak{g})^K_n$. Now as before we have $\sigma_o^n(\widetilde{P(w)}) = \sigma_o^n(\widetilde{b})$. Therefore $\rho_o(\widetilde{b} - \widetilde{P(w)}) < \rho_o(\widetilde{b})$. If $\widetilde{b} = \widetilde{P(w)}$ we are done, if not $\widetilde{a} = \widetilde{b} - \widetilde{P(w)} \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ (cf.[17], Theorem 4.5), $d(\widetilde{a}) \leq m$ from Theorem 4.2 and $\beta(\widetilde{a}) < \beta(\widetilde{b})$. By the inductive hypothesis there is $v \in U(\mathfrak{g})^K$ such that $\widetilde{a} = \widetilde{P(v)}$. Then $u = v + w \in U(\mathfrak{g})^K$ and $\widetilde{P(u)} = \widetilde{b}$. This completes the proof of the proposition.

Finally we observe that to complete the proof of Theorem 1.1 it is sufficient to establish the following result.

Theorem 4.5. *If $b \in B^{W_\rho}$ when $rank(G_o) \neq rank(K_o)$ or if $b \in B$ when $rank(G_o) = rank(K_o)$, then its leading term $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and $d(b_m) \leq m$.*

Theorem 4.6. *Theorem 4.5 implies Theorem 1.1.*

Proof. We already know that $P(U(\mathfrak{g})^K) \subset B^{W_\rho}$ if $\operatorname{rank}(G_o) \neq \operatorname{rank}(K_o)$ and that $P(U(\mathfrak{g})^K) \subset B$ when $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$. The other inclusion will be established by induction on the degree m of b. If $m = 0$ then $b = b_0 \in \mathfrak{z}(U(\mathfrak{k}))$ since $d(\gamma) = 0$ implies that γ can be realized by constant polynomial functions on $\mathfrak{p}$; then $b_0 = P(b_0) \in P(U(\mathfrak{g})^K)$. If $m > 0$, from Proposition 4.4 we know that there exists $v \in U(\mathfrak{g})^K$ such that $\widetilde{P(v)} = \widetilde{b}$. Then $b - P(v)$ lies either in B^{W_ρ} or in B, depending on the case, and $d(b - P(v)) < m$. Thus by induction there exists $w \in U(\mathfrak{g})^K$ such that $P(w) = b - P(v)$. Therefore $b = P(v + w)$, completing the proof of the theorem.

The rest of the paper will be devoted to prove Theorem 4.5 for any classical rank one semisimple Lie group.

5. Non commutative Gaussian elimination

Since we have already established Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SL}(2,\mathbb{R})$, from now on we shall assume that G_o is a connected, noncompact real semisimple Lie group, with finite center and of split rank one, not locally isomorphic to $\mathrm{SL}(2,\mathbb{R})$. Then, as we pointed out before, for any simple root $\alpha \in P_+$ we have $Y_\alpha \neq 0$. Therefore the algebra B (see Definition 3.6 and Proposition 3.4) is the set of all $b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ satisfying

$$E_\alpha^n b(n - Y_\alpha - 1) \equiv b(-n - Y_\alpha - 1)E_\alpha^n \tag{21}$$

$\bmod\big(U(\mathfrak{k})\mathfrak{m}^+\big)$, for all simple roots $\alpha \in P_+$ and all $n \in \mathbb{N}$.

From now on we shall simply write $u \equiv v$ instead of $u \equiv v \mod \big(U(\mathfrak{k})\mathfrak{m}^+\big)$, for any $u, v \in U(\mathfrak{k})$. The following lemma was proved in Lemma 29 of [24] for G_o of any rank.

Lemma 5.1. *Let $\alpha \in P_+$ be a simple root. Set $H_\alpha = Y_\alpha + Z_\alpha$ ($Y_\alpha \in \mathfrak{t}$, $Z_\alpha \in \mathfrak{a}$) and $c = \alpha(Y_\alpha)$. If $\lambda = \alpha|_\mathfrak{a}$ and $m(\lambda)$ is the multiplicity of λ, then $c = 1$ when 2λ is not a restricted root and $m(\lambda)$ is even, or when $m(\lambda)$ is odd, and $c = \frac{3}{2}$ when 2λ is a restricted root and $m(\lambda)$ is even.*

Then $c = 1$ when G_o is locally isomorphic to SO(n,1), $n \geq 3$, and $c = \frac{3}{2}$ when G_o is locally isomorphic to SU(n,1) or Sp(n,1), $n \geq 2$, or F_4. In other words, in the rank one case $c = 1$ when 2λ is not a restricted root, and $c = \frac{3}{2}$ when it is.

To simplify the notation we set $E = E_\alpha$, $Y = Y_\alpha$ and $Z = Z_\alpha$ for any simple root $\alpha \in P_+$. Notice that $[E, Y] = cE$ where c is as in Lemma 5.1. Let us also keep in mind that E is $\mathfrak{m}^+$-dominant, because $E_\alpha = X_{-\alpha} + \theta X_{-\alpha}$ and α is a simple root in P_+.

In what follows we shall find it convenient to identify $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ with the polynomial ring in one variable $U(\mathfrak{k})[x]$, replacing Z by the indeterminate x. To study the equation (21) we shall change the unknown $b(x) \in U(\mathfrak{k})[x]$

by $c(x) \in U(\mathfrak{k})[x]$ defined by

$$c(x) = b(x + H - 1), \tag{22}$$

where $H = 0$ if $c = 1$, and if $c = \frac{3}{2}$ H is an appropriate vector in $\mathfrak{t}$ to be chosen later, depending on the simple root $\alpha \in P_+$ and such that $[H, E] = \frac{1}{2}E$. Now if $\widetilde{Y} = Y + H$, we have $[E, \widetilde{Y}] = E$. This is the main reason for introducing H, because it allows to treat (21) in a unified way in both cases, $c = 1, \frac{3}{2}$.

Then $b(x) \in U(\mathfrak{k})[x]$ satisfies (21) if and only if $c(x) \in U(\mathfrak{k})[x]$ satisfies

$$E^n c(n - \widetilde{Y}) \equiv c(-n - \widetilde{Y})E^n \tag{23}$$

for all $n \in \mathbb{N}$.

Now we introduce the following notation. If p is a polynomial in one indeterminate x with coefficients in a ring, then $p^{(n)}$ will denote the n-th discrete derivative of p. In particular $p^{(1)}(x) = p(x + \frac{1}{2}) - p(x - \frac{1}{2})$ and in general $p^{(n)}(x) = \sum_{j=0}^{n}(-1)^j \binom{n}{j} p(x + \frac{n}{2} - j)$. If $p = p_m x^m + \cdots + p_0$, then

$$p^{(n)}(x) = \begin{cases} 0, & \text{if } n > m \\ m! p_m, & \text{if } n = m. \end{cases} \tag{24}$$

Also, if $X \in \mathfrak{k}$ we shall denote with $\dot{X}$ the derivation of $U(\mathfrak{k})$ induced by $\operatorname{ad}(X)$. Moreover if D is a derivation of $U(\mathfrak{k})$ we shall denote with the same symbol the unique derivation of $U(\mathfrak{k})[x]$ which extends D and such that $Dx = 0$. Thus for $b \in U(\mathfrak{k})[x]$, $b = b_m x^m + \cdots + b_0$ we have $Db = (Db_m)x^m + \cdots + (Db_0)$. Observe that these derivations commute with the operation of taking the discrete derivative in $U(\mathfrak{k})[x]$.

Lemma 5.2. *Let $c(x) \in U(\mathfrak{k})[x]$. Then*
(i) $\dot{E}\big(c(x - \widetilde{Y})\big) = \dot{E}(c)(x - \widetilde{Y}) - c^{(1)}(x - \frac{1}{2} - \widetilde{Y})E,$

(ii) $E^n c(x - \widetilde{Y}) = \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(x - j - \widetilde{Y})E^j$ *for all* $n \in \mathbb{N}_0$.
(iii) $\sum_{j=0}^{n}(-1)^j \binom{n}{j} c^{(j)}(x - \frac{j}{2}) = c(x - n)$ *for all* $n \in \mathbb{N}_0$.

Proof. (i) Since $\dot{E}(\widetilde{Y}) = [E, \widetilde{Y}] = E$ by induction on n one easily get

$$\dot{E}\big((x - \widetilde{Y})^n\big) = -(x - \widetilde{Y})^n E + (x - \widetilde{Y} - 1)^n E.$$

This equality is precisely (i) for $c(x) = x^n$. Now for any $c(x)$ the assertion follows by linearity of $\dot{E}$ and from the Leibnitz rule.

(ii) The equality is obvious for $n = 0$. Let us assume that it is true for $n \geq 0$. Then

$$E^{n+1}c(x - \widetilde{Y}) = E \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(x - j - \widetilde{Y})E^j$$

$$= \dot{E}\Bigg(\sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(x - j - \widetilde{Y})E^j \Bigg) + \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(x - \widetilde{Y} - j)E^{j+1}$$

$$= \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n+1-j}(c)(x - j - \widetilde{Y})E^j + \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(x - j - 1 - \widetilde{Y})E^{j+1}$$

$$= \sum_{j=0}^{n+1} \binom{n+1}{j} \dot{E}^{n+1-j}(c)(x - j - \widetilde{Y})E^j,$$

which completes the inductive step.

(iii) For $n = 0$ the statement is obvious. Let us assume inductively that for $n \geq 0$ we have

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} c^{(j)}(x - \tfrac{j}{2}) = c(x - n). \tag{25}$$

By taking the discrete derivative on both sides of (25) we obtain

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} c^{(j+1)}(x - \tfrac{j}{2}) = c^{(1)}(x - n). \tag{26}$$

If we make the change of variable $x \mapsto x + \frac{1}{2}$ in (25) we have

$$c(x + \tfrac{1}{2}) + \sum_{j=0}^{n-1} (-1)^{j+1} \binom{n}{j+1} c^{(j+1)}(x - \tfrac{j}{2}) = c(x + \tfrac{1}{2} - n). \tag{27}$$

Now we subtract (26) from (27) to get

$$c(x + \tfrac{1}{2}) + \sum_{j=0}^{n-1} (-1)^{j+1} \binom{n+1}{j+1} c^{(j+1)}(x - \tfrac{j}{2})$$
$$+ (-1)^{n+1} \binom{n+1}{n+1} c^{(n+1)}(x - \tfrac{1}{2} - \tfrac{n}{2}) = c(x - \tfrac{1}{2} - n).$$

By changing back the variable x to $x - \frac{1}{2}$ we obtain

$$\sum_{j=0}^{n+1} (-1)^j \binom{n+1}{j} c^{(j)}(x - \tfrac{j}{2}) = c(x - 1 - n),$$

which completes the proof of (iii).

In the next theorem we give a triangularized version of system (23). The meaning of this will be clarified after the proof of the theorem.

Theorem 5.3. *Let $c \in U(\mathfrak{k})[x]$. Then the following systems of equations are equivalent:*
(i) $E^n c(n-\widetilde{Y}) \equiv c(-n-\widetilde{Y})E^n$, $(n \in \mathbb{N}_0)$;
(ii) $\dot{E}^{n+1}\big(c^{(n)}\big)(\frac{n}{2}+1-\widetilde{Y}) + \dot{E}^n\big(c^{(n+1)}\big)(\frac{n}{2}-\frac{1}{2}-\widetilde{Y})E \equiv 0$, $(n \in \mathbb{N}_0)$.

Moreover, if $c \in U(\mathfrak{k})[x]$ is a solution of one of the above systems, then for all $\ell, n \in \mathbb{N}_0$ we have
(iii) $(-1)^n \dot{E}^\ell\big(c^{(n)}\big)(-\frac{n}{2}+\ell-\widetilde{Y})E^n - (-1)^\ell \dot{E}^n\big(c^{(\ell)}\big)(-\frac{\ell}{2}+n-\widetilde{Y})E^\ell \equiv 0.$

Proof. For $\ell, n \in \mathbb{N}_0$ let

$$\epsilon(\ell,n) = (-1)^n \dot{E}^\ell\big(c^{(n)}\big)(-\tfrac{n}{2}+\ell-\widetilde{Y})E^n - (-1)^\ell \dot{E}^n\big(c^{(\ell)}\big)(-\tfrac{\ell}{2}+n-\widetilde{Y})E^\ell.$$

Let us first observe that the system $\epsilon(n,0) \equiv 0$, $(n \in \mathbb{N}_0)$ is equivalent to the system given in (i). In fact, if $c \in U(\mathfrak{k})[x]$ is a solution of $\epsilon(n,0) \equiv 0$, $(n \in \mathbb{N}_0)$, then from Lemma 5.2 (ii) and (iii) we get

(28)
$$\begin{aligned} E^n c(n-\widetilde{Y}) &= \sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(n-j-\widetilde{Y})E^j \\ &\equiv \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} c^{(n-j)}(-\tfrac{n-j}{2}-\widetilde{Y})E^n = c(-n-\widetilde{Y})E^n. \end{aligned}$$

Conversely, suppose that $c \in U(\mathfrak{k})[x]$ satisfies $E^n c(n-\widetilde{Y}) \equiv c(-n-\widetilde{Y})E^n$ for all $n \in \mathbb{N}_0$. Then from (28) we get

$$\sum_{j=0}^{n} \binom{n}{j} \dot{E}^{n-j}(c)(n-j-\widetilde{Y})E^j \equiv \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} c^{(n-j)}(-\tfrac{n-j}{2}-\widetilde{Y})E^n. \tag{29}$$

It is obvious that $\epsilon(0,0) \equiv 0$. Let us assume by induction that $\epsilon(\ell,0) \equiv 0$ for all $0 \le \ell \le n-1$, $n \ge 1$. Then from (29) we get $\epsilon(n,0) \equiv 0$, as we wanted to prove.

On the other hand it follows immediately that $\epsilon(n+1,n) \equiv 0$ is equivalent to $\dot{E}^{n+1}\big(c^{(n)}\big)(\frac{n}{2}+1-\widetilde{Y}) + \dot{E}^n\big(c^{(n+1)}\big)(\frac{n}{2}-\frac{1}{2}-\widetilde{Y})E \equiv 0$, for all $n \in \mathbb{N}_0$.

Now we shall prove that the following identity holds for all $\ell, n \in \mathbb{N}_0$:

$$\big(\dot{E}\epsilon(\ell,n) - \epsilon(\ell,n+1) - \epsilon(\ell+1,n)\big)E - \epsilon(\ell+1,n+1) = 0. \tag{30}$$

Using Lemma 5.2 (i) we get

$$\begin{aligned} \dot{E}\epsilon(\ell,n)E =& (-1)^n \dot{E}^{\ell+1}(c^{(n)})(-\tfrac{n}{2}+\ell-\widetilde{Y})E^{n+1} \\ &- (-1)^n \dot{E}^\ell(c^{(n+1)})(-\tfrac{n}{2}+\ell-\tfrac{1}{2}-\widetilde{Y})E^{n+2} \\ &- (-1)^l \dot{E}^{n+1}(c^{(\ell)})(-\tfrac{\ell}{2}+n-\widetilde{Y})E^{\ell+1} \\ &+ (-1)^\ell \dot{E}^n(c^{(\ell+1)})(-\tfrac{\ell}{2}+n-\tfrac{1}{2}-\widetilde{Y})E^{\ell+2}. \end{aligned} \tag{31}$$

We also have

$$-\epsilon(\ell,n+1)E =(-1)^n\dot{E}^{\ell}(c^{(n+1)})(-\tfrac{n}{2}+\ell-\tfrac{1}{2}-\widetilde{Y})E^{n+2} + (-1)^{\ell}\dot{E}^{n+1}(c^{(\ell)})(-\tfrac{\ell}{2}+n+1-\widetilde{Y})E^{\ell+1}, \tag{32}$$

$$-\epsilon(\ell+1,n)E =-(-1)^n\dot{E}^{\ell+1}(c^{(n)})(-\tfrac{n}{2}+\ell+1-\widetilde{Y})E^{n+1} - (-1)^{\ell}\dot{E}^{n}(c^{(\ell+1)})(-\tfrac{\ell}{2}+n-\tfrac{1}{2}-\widetilde{Y})E^{\ell+2}. \tag{33}$$

By using the definition of the discrete derivative we obtain

$$\begin{aligned} -\epsilon(\ell+1,n+1) =&(-1)^n\dot{E}^{\ell+1}(c^{(n+1)})(-\tfrac{n}{2}+\ell+\tfrac{1}{2}-\widetilde{Y})E^{n+1} \\ &- (-1)^{\ell}\dot{E}^{n+1}(c^{(\ell+1)})(-\tfrac{\ell}{2}+n+\tfrac{1}{2}-\widetilde{Y})E^{\ell+1} \\ =&(-1)^n\dot{E}^{\ell+1}(c^{(n)})(-\tfrac{n}{2}+\ell+1-\widetilde{Y})E^{n+1} \\ &- (-1)^n\dot{E}^{\ell+1}(c^{(n)})(-\tfrac{n}{2}+\ell-\widetilde{Y})E^{n+1} \\ &- (-1)^{l}\dot{E}^{n+1}(c^{(\ell)})(-\tfrac{\ell}{2}+n+1-\widetilde{Y})E^{\ell+1} \\ &+ (-1)^{\ell}\dot{E}^{n+1}(c^{(\ell)})(-\tfrac{\ell}{2}+n-\widetilde{Y})E^{\ell+1}. \end{aligned} \tag{34}$$

Now by adding up (31), (32), (33) and (34) it is easy to check (30).

To prove the theorem we shall see that under the hypothesis that $c \in U(\mathfrak{k})[x]$ satisfies either the system (i) or the system (ii) we have $\epsilon(\ell,n) \equiv 0$ for all $\ell, n \in \mathbb{N}_0$. This in particular implies that (i) and (ii) are equivalent. First of all let us observe that if $\epsilon(\ell,n) \equiv 0$ then $\dot{E}\epsilon(\ell,n) \equiv 0$ and $\epsilon(\ell,n)E \equiv 0$, this is so because E commutes with any element in $\mathfrak{m}^+$.

To follow the argument it helps a lot to visualize the set $\mathbb{N}_0^2$ in the plane. Then each identity (30) is associated to the four vertices of a unit square in $\mathbb{N}_0^2$. So, once we know that the equations $\epsilon(\ell,n) \equiv 0$ hold for three vertices of a unit square it holds for the other vertex. Also observe that the equations corresponding to the diagonal (n,n), $n \in \mathbb{N}_0$ are true by definition.

Now the system (i) implies that all the equations corresponding to the horizontal line $(\ell,0)$, $\ell \in \mathbb{N}_0$ hold. Then we can get first that $\epsilon(0,1) \equiv 0$ and then succesively that $\epsilon(\ell,1) \equiv 0$ for all $\ell \geq 2$, completing the second horizontal line of equations. Then in the same way we can assume inductively that for $n \in \mathbb{N}_0$, $\epsilon(\ell,n) \equiv 0$ for all $\ell \in \mathbb{N}_0$. Then starting from $\epsilon(n+1,n+1) \equiv 0$ we can move back to get $\epsilon(\ell,n+1) \equiv 0$ for all $\ell \in \mathbb{N}_0$, $0 \leq \ell \leq n$, and then move forward to get $\epsilon(\ell,n+1) \equiv 0$, for all $\ell \in \mathbb{N}_0$, $\ell > n+1$. In this way we get that $\epsilon(\ell,n) \equiv 0$ for all $\ell, n \in \mathbb{N}_0$.

Similarly, the system (ii) implies that all the equations corresponding to the diagonal $(n+1,n)$, $n \in \mathbb{N}_0$, below the main diagonal, hold. Then one can move inductively proving that all equations corresponding to points in all the diagonals parallel to the main one are true. This completes the proof of the theorem.

Let us observe that if $c \in U(\mathfrak{k})[x]$ is of degree m and $c = c_m x^m + \cdots + c_0$, then all equations of the system (ii) corresponding to $n > m$ are trivial, because $c^{(n)} = 0$. Moreover the equation corresponding to $n = m$ reduces to $\dot{E}^{m+1}(c_m) \equiv 0$, and more generally the equation associated to $n = j$ only involves the coefficients $c_m, \dots, c_j$. In other words the system (ii) is a triangular system of $m+1$ linear equations in the $m+1$ unknowns $c_m, \dots, c_0$.

Since we are going to use equations (iii) of Theorem 5.3, it is convenient to consider a basis $\{\varphi_n\}_{n\geq 0}$ of the polynomial ring $\mathbb{C}[x]$ that behaves well under the discrete derivative. Then let $\{\varphi_n\}_{n\geq 0}$ be the basis of $\mathbb{C}[x]$ defined by,

$$\varphi_0 = 1, \tag{i}$$

$$\varphi_n^{(1)} = \varphi_{n-1} \qquad \text{if } n \geq 1, \tag{ii}$$

$$\varphi_n(0) = 0 \qquad \text{if } n \geq 1. \tag{iii}$$

The existence and uniqueness of the family $\{\varphi_n\}_{n\geq 0}$ follows inductively from conditions (i), (ii) and (iii) above. Moreover it is easy to prove that such a family is given explicitly by

$$\varphi_n(x) = \tfrac{1}{n!}x(x + \tfrac{n}{2} - 1)(x + \tfrac{n}{2} - 2)\cdots(x - \tfrac{n}{2} + 1), \quad n \geq 1.$$

It is worth observing that the leading term of φ_n is $x^n/n!$.

6. The case SO(n,1)

In this section we shall prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ with $n \geq 3$. These are the only cases in which $c = 1$, where c is the constant defined in Lemma 5.1. Although the results in this section are mostly contained in [24], we include them here for completeness and to prove that $B^{W_\rho} = B$ when $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$ which is a new result.

Let us assume that G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ with $n \geq 3$. As we pointed out before, there is only one simple root $\alpha_1 \in P_+$ if $n \geq 4$ and there are two α_1, α_2 if $n = 3$. In all cases we set $\alpha = \alpha_1$ and as in the previous section we put $E = E_\alpha$, $Y = Y_\alpha$ and $Z = Z_\alpha$. Also as in (22), to any $b(x) \in U(\mathfrak{k})[x]$ we associate $c(x) \in U(\mathfrak{k})[x]$ defined by $c(x) = b(x-1)$. If $b(x) \in U(\mathfrak{k})[x]$, $b(x) \neq 0$, we shall find it convenient to write, in a unique way, $b = \sum_{j=0}^m b_j x^j$, $b_j \in U(\mathfrak{k})$, $b_m \neq 0$, and the corresponding $c = \sum_{j=0}^m c_j\varphi_j$ with $c_j \in U(\mathfrak{k})$. Then the following lemma establishes the relation between the coefficients b_j and c_j.

Lemma 6.1. *Let $b = \sum_{j=0}^m b_j x^j \in U(\mathfrak{k})[x]$ and set $c(x) = b(x-1)$. Then, if $c = \sum_{j=0}^m c_j\varphi_j$ with $c_j \in U(\mathfrak{k})$ we have*

$$c_i = \sum_{j=i}^{m} t_{ij} b_j \qquad 0 \leq i \leq m, \tag{35}$$

where t_{ij} are rational numbers and $t_{ii} = i!$. In other words, the vectors $(b_0, \dots, b_m)^t$ and $(c_0, \dots, c_m)^t$ are related by a rational nonsingular upper triangular matrix.

Proof. On the one hand we have

$$c^{(i)} = \sum_{j=0}^{m} c_j \varphi_j^{(i)} = \sum_{j=i}^{m} c_j \varphi_{j-i}.$$

Thus $c^{(i)}(0) = c_i$. On the other hand

$$c_i = c^{(i)}(0) = \sum_{j=0}^{m} b_j \big((x-1)^j\big)^{(i)}(0) = \sum_{j=0}^{m} t_{ij} b_j,$$

where we set $t_{ij} = \big((x-1)^j\big)^{(i)}(0)$. Now the lemma follows from (24) and the formula for the n-th discrete derivative given right before (24).

Lemma 6.2. *Let $u \in U(\mathfrak{k})$ and $X \in \mathfrak{k} - \mathfrak{m}^+$ be such that $\dot{X}(\mathfrak{m}^+) \subset \mathfrak{m}^+$. Then, if $n \in \mathbb{N}$ and $uX^n \equiv 0$ we have $u \equiv 0$.*

Proof. Choose a basis $\{Z_1, \dots, Z_q\}$ of $\mathfrak{m}^+$ and complete it to a basis of $\mathfrak{k}$ by adding vectors $X_1, \dots, X_p$ with $X_p = X$. Then by Poincaré-Birkhoff-Witt theorem the ordered monomials $X^I = X_1^{i_1} \cdots X_p^{i_p}$, $I = \{i_1, \dots, i_p\}$, and $Z^J = Z_1^{j_1} \cdots Z_p^{j_p}$, $J = \{j_1, \dots, j_p\}$, form a basis $\{X^I Z^J\}$ of $U(\mathfrak{k})$.

Clearly it is enough to prove the lemma for $n = 1$. If $u = \sum a_{I,J} X^I Z^J$ we have

$$uX = \sum a_{I,J} X^I X Z^J - \sum a_{I,J} X^I \dot{X}(Z^J).$$

Then, since $\dot{X}(Z^J) \equiv 0$ it follows that $uX \equiv \sum a_{I,J} X^I X Z^J$. Therefore $uX \equiv 0$ implies that $a_{I,J} = 0$ if $J = 0$. Hence the lemma follows.

We are now in a position to prove the following theorem.

Theorem 6.3. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{m+1}(b_j) \equiv 0$ for all $0 \le j \le m$.*

Proof. We regard b as a polynomial $b = \sum_{j=0}^{m} b_j x^j$ with $b_j \in U(\mathfrak{k})^M$ and let $c(x) = b(x-1) = \sum_{j=0}^{m} c_j \varphi_j(x)$ with $c_j \in U(\mathfrak{k})^M$. Then, since $b \in B$, c satisfies the system of equations (i) of Theorem 5.3 with $\widetilde{Y} = Y$. Therefore c satisfies equations (iii) of Theorem 5.3 for all $\ell, n \in \mathbb{N}_o$.

Hence, since $c^{(m+1)} = 0$, if we consider $\ell = m+1$ in equation (iii) of Theorem 5.3 and we use Lemma 6.2 with $X = E$ we obtain

$$\sum_{j=n}^{m} \dot{E}^{m+1}(c_j) \varphi_{j-n}\big(\tfrac{2m+2-n}{2} - Y\big) \equiv 0, \tag{36}$$

for $0 \le n \le m$. Now, taking into account that right multiplication by Y leaves invariant the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ because $Y \in \mathfrak{t}$, (36) together with decreasing induction on n starting from $n = m$ implies that $\dot{E}^{m+1}(c_j) \equiv 0$ for all $0 \le j \le m$. From this, applying $\dot{E}^{m+1}$ to (35), the theorem follows because the matrix (t_{ij}) is a nonsingular scalar matrix.

Another fundamental step in the proof of Theorem 1.1 is the following result established in Theorem 3.11 of [2].

Theorem 6.4. *Let G_o be locally isomorphic to $SO(n,1)_e$, $n \geq 3$, or $SU(n,1)$ $n \geq 2$. Then the infinite sum $\sum_{j\geq 0} \dot{E}^j\big(U(\mathfrak{k})^M\big)$ is a direct sum and we have*

$$\Big(\sum_{j\geq 0} \dot{E}^j\big(U(\mathfrak{k})^M\big)\Big) \cap U(\mathfrak{k})\mathfrak{m}^+ = 0.$$

This result allows us to replace the congruence to zero $\mod \big(U(\mathfrak{k})\mathfrak{m}^+\big)$ in Theorem 6.3 by an equality. Hence we obtain the following corollary.

Corollary 6.5. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{m+1}(b_j) = 0$ for all $0 \leq j \leq m$.*

To establish Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ we need to recall some facts about the representations in Γ. First of all when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$ or $\mathrm{SU}(n,1)$ we have an alternative and convenient description of the degree of $\gamma \in \Gamma$. In fact, let $\alpha \in P_+$ be a simple root and set $E = X_{-\alpha} + \theta X_{-\alpha}$ for any $X_{-\alpha} \neq 0$. If $\gamma \in \Gamma$ let

$$q(\gamma) = \max\{q \in \mathbb{N} : E^q(V_\gamma^M) \neq 0\}. \tag{37}$$

In the following proposition and in Proposition 7.6 we shall establish a relation between $q(\gamma)$ and $d(\gamma)$ for any $\gamma \in \Gamma$ as well as other facts about the representations in Γ. Some of these results where first established in [12], others were proved in [2] for G_o locally isomorphic to $\mathrm{SO}(n,1)_e$ or $\mathrm{SU}(n,1)$, and in [4] they were recently generalized to any real rank one semisimple Lie group.

Proposition 6.6. *Let G_o be locally isomorphic to $SO(n,1)_e$, $n \geq 3$. Then there exists a Borel subalgebra $\mathfrak{b}_\mathfrak{k} = \mathfrak{h}_\mathfrak{k} \oplus \mathfrak{k}^+$ of $\mathfrak{k}$ such that $\mathfrak{m}^+ \subset \mathfrak{k}^+$ and $E \in \mathfrak{k}^+$. For any such a Borel subalgebra there exists a fundamental weight ξ_o with the following properties:*
(i) For any $\gamma \in \hat{K}$ let ξ_γ denote its highest weight. Then $\gamma \in \Gamma$ if and only if for some $k \in \mathbb{N}_o$ we have $\xi_\gamma = k\xi_o$, when $n \geq 4$, and $\xi_\gamma = 2k\xi_o$, if $n = 3$.
(ii) If $rank(G_o) = rank(K_o)$, that is n even, the representation $\gamma \in \Gamma$ with highest weight $\xi_\gamma = k\xi_o$ occurs in $U(\mathfrak{k})$ if and only if k is even.
(iii) For any $\gamma \in \Gamma$ we have $E^{q(\gamma)}(V_\gamma^M) = V_\gamma^{\mathfrak{k}^+}$, $\xi_\gamma = q(\gamma)\xi_o$ if $n \geq 4$, and $\xi_\gamma = 2q(\gamma)\xi_o$ if $n = 3$. Moreover $d(\gamma) = q(\gamma)$.

For a construction of the Borel subalgebra $\mathfrak{b}_\mathfrak{k}$ we refer the reader to Section 3 of [4]; also (i) and (iii) are proved in Theorem 4.5 and Theorem 5.3 of [4]. On the other hand (ii) follows from well known general facts.

Observe that from (iii) of Proposition 6.6 it follows that if $b \in U(\mathfrak{k})^M$, $b \neq 0$, and $r = \max\{q \in \mathbb{N}_o : \dot{E}^q(b) \neq 0\}$ then $\dot{E}^r(b)$ is a highest weight vector of weight $\xi = r\xi_o$ if $n \geq 4$ or $\xi = 2r\xi_o$ if $n = 3$.

We are now in position to prove one of the conditions needed to establish Theorem 1.1 (see Theorem 4.5) when G_o is locally isomorphic to $\mathrm{SO}(n,1)_e$.

Theorem 6.7. *Assume that G_o is locally isomorphic to $SO(n,1)_e$, $n \geq 3$. Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $d(b_j) \leq m$ for all $0 \leq j \leq m$.*

Proof. Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then it follows from Corollary 6.5 that $\dot{E}^{m+1}(b_j) = 0$ for all $0 \le j \le m$. In view of (37) and (iii) of Proposition 6.6 this implies that $b_j \in \bigoplus U(\mathfrak{k})^M_\gamma$, where the sum extends over all $\gamma \in \Gamma$ such that $d(\gamma) \le m$. Therefore $d(b_j) \le m$ for all $0 \le j \le m$, as we wanted to prove.

Our next goal is to show that when $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$ the algebra B does not contain elements of odd degree. First of all, as a consequence of (ii) and (iii) of Proposition 6.6 we obtain the following result.

Lemma 6.8. *If G_o is locally isomorphic to $SO(2p,1)_e$ and $b \in U(\mathfrak{k})^M$ is such that $\dot{E}^{2t}(b) = 0$ with $t \in \mathbb{N}$ then $\dot{E}^{2t-1}(b) = 0$.*

Proof. If $\dot{E}^{2t-1}(b) \ne 0$ then $\dot{E}^{2t-1}(b)$ would be a highest weight vector of weight $\xi = (2t-1)\xi_o$, but this contradicts (ii) of Proposition 6.6.

Theorem 6.9. *If G_o is locally isomorphic to $SO(2p,1)_e$, $p \ge 2$, and $b = b_m \otimes Z^m + \cdots + b_0 \in B$ with m odd, then $b_m = 0$. That is, B does not contain odd degree elements.*

Proof. From Corollary 6.5 and Lemma 6.8 we obtain $\dot{E}^m(b_j) = 0$ for all $0 \le j \le m$. Then, from (35) we get $\dot{E}^m(c_j) = 0$ for all $0 \le j \le m$.

If we consider $\ell = m$ and $n = 0$ in equation (iii) of Theorem 5.3 we get

$$\sum_{j=0}^{m} \dot{E}^m(c_j)\varphi_j(m - Y) - m! b_m E^m \equiv 0,$$

which implies that $b_m \equiv 0$, and therefore $b_m = 0$ (Theorem 6.4) as we wanted to prove.

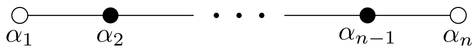
Corollary 6.10. *If G_o is locally isomorphic to $SO(n,1)_e$, $n \ge 3$, then the main result Theorem 1.1 holds.*

Proof. As we proved in Theorem 4.6 it is enough to establish Theorem 4.5. When n is odd it is clear that if $b \in B^{W_\rho}$ then its leading term $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$. If n is even from Theorem 6.9 we know that if $b \in B$ then its leading term $\widetilde{b} = b_m \otimes Z^m$ has m even. On the other hand, since in this case $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$, it is well known that the non trivial element of W can be represented by an element in M_o' which acts on $\mathfrak{g}$ as the Cartan involution. Thus $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$. Now Theorem 6.7 completes the proof of the corollary.

Remark. When G_o is locally isomorphic to $\mathrm{SO}(3,1)_e$ we used only one of the equations that define the algebra B. In other words if for each simple root $\alpha \in P_+$ we define B_α as the subalgebra of all elements $b \in U(\mathfrak{k}) \otimes U(\mathfrak{a})$ satisfying (20) for all $n \in \mathbb{N}$, then we proved that $P\big(U(\mathfrak{g})^K\big) = B^{W_\rho} = B_\alpha^{W_\rho}$. Moreover taking advantage of both equations it is not difficult to see that $B^{W_\rho} = B$.

7. The case SU(n,1)

In this section we shall prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SU}(n,1)$ with $n \geq 2$. Most of the results are contained in [24], but we include them here because some of them were presented without proofs, and to establish that $B^{W_\rho} = B$, which is a new result. The corresponding Dynkin-Satake diagram of $\mathfrak{g}$ is



It is well known that we can choose an orthonormal basis $\{\epsilon_i\}_{i=1}^{n+1}$ of $(\mathfrak{h}_\mathbb{R} \oplus \mathbb{R})^*$ in such a way that $\mathfrak{h}_\mathbb{R} = \{H \in \mathfrak{h}_\mathbb{R} \oplus \mathbb{R} : (\epsilon_1 + \cdots + \epsilon_{n+1})(H) = 0\}$, $\alpha_i = \epsilon_i - \epsilon_{i+1}$ if $1 \leq i \leq n$, $\epsilon_i^\sigma = -\epsilon_i$ if $2 \leq i \leq n$ and $\epsilon_1^\sigma = -\epsilon_{n+1}$. From the diagram we obtain that

$$\begin{aligned} \Delta^+(\mathfrak{g},\mathfrak{h}) &= \{\epsilon_i - \epsilon_j : 1 \leq i < j \leq n+1\}, \\ P_+ &= \{\epsilon_1 - \epsilon_j, \epsilon_j - \epsilon_{n+1} : 2 \leq j \leq n\} \cup \{\epsilon_1 - \epsilon_{n+1}\}, \\ P_- &= \{\epsilon_i - \epsilon_j : 2 \leq i < j \leq n\}, \end{aligned}$$

where P_- denotes the set of roots in $\Delta^+(\mathfrak{g},\mathfrak{h})$ that vanish on $\mathfrak{a}$.

In this case there are two simple roots $\alpha = \alpha_1, \alpha_n$ in P_+; in both cases $Y_\alpha \neq 0$. Set $E_1 = X_{-\alpha_1} + \theta X_{-\alpha_1}$, $E_2 = X_{-\alpha_n} + \theta X_{-\alpha_n}$, $Y_1 = Y_{\alpha_1}$, $Y_2 = Y_{\alpha_n}$ and $Z = Z_{\alpha_1} = Z_{\alpha_n}$. Let $T \in \mathfrak{t}_\mathbb{R}$ be defined by $\epsilon_2(T) = \cdots = \epsilon_n(T) = \frac{2}{n+1}$. Then $T \in \mathfrak{z}(\mathfrak{m})$ and $\dim(\mathfrak{z}(\mathfrak{m})) = 1$. Since $\epsilon_1(T) = \epsilon_{n+1}(T)$ and $(\epsilon_1 + \cdots + \epsilon_{n+1})(T) = 0$ we get $\epsilon_2(T) - \epsilon_1(T) = \epsilon_n(T) - \epsilon_{n+1}(T) = 1$; thus $[T, E_1] = E_1$ and $[T, E_2] = -E_2$. Now we define the vector H considered in (22) as follows,

$$H = \begin{cases} \frac{1}{2}T, & \text{if } \alpha = \alpha_1 \\ -\frac{1}{2}T, & \text{if } \alpha = \alpha_n, \end{cases} \tag{38}$$

and we write generically E, Y, and $\widetilde{Y} = Y + H$ for the corresponding vectors associated to a simple root $\alpha \in P_+$. Then $\dot{E}(H) = -\frac{1}{2}E$, and from Lemma 5.1 we get $\dot{E}(\widetilde{Y}) = E$.

Also as in (22), to any $b(x) \in U(\mathfrak{k})[x]$ we associate $c(x) \in U(\mathfrak{k})[x]$ defined by $c(x) = b(x + H - 1)$. If $b(x) \in U(\mathfrak{k})[x]$, $b(x) \neq 0$, we shall find it convenient to write, in a unique way, $b = \sum_{j=0}^m b_j x^j$, $b_j \in U(\mathfrak{k})$, $b_m \neq 0$, and the corresponding $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$. Then the following lemma establishes the relation between the coefficients b_j and c_j.

Lemma 7.1. *Let $b = \sum_{j=0}^m b_j x^j \in U(\mathfrak{k})[x]$ and set $c(x) = b(x + H - 1)$. Then, if $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$ we have*

$$c_i = \sum_{j=i}^m b_j t_{ij} \qquad 0 \leq i \leq m, \tag{39}$$

where

$$t_{ij}=\sum_{k=0}^{i}(-1)^k\binom{i}{k}(H+\tfrac{i}{2}-1-k)^j\in\mathfrak{z}\left(U(\mathfrak{m})\right). \tag{40}$$

Thus t_{ij} is a polynomial in H of degree $j-i$, in particular $t_{ii}=i!$. Moreover, if $b_j\in U(\mathfrak{k})^M$ for all $0\le j\le m$, then $c_j\in U(\mathfrak{k})^M$ for all $0\le j\le m$.

Proof. On the one hand we have

$$c_i=c^{(i)}(0)=\sum_{j=0}^{m}b_j\big((x+H-1)^j\big)^{(i)}(0)=\sum_{j=i}^{m}b_jt_{ij},$$

where we set $t_{ij}=\big((x+H-1)^j\big)^{(i)}(0)$. Now the lemma follows from (24) and the formula for the n-th discrete derivative given right before (24). The other statements are clear.

Lemma 7.2. *Let t_{ij} be defined by (40). Then*

$$\dot{E}^{j-i}(t_{ij})=\left(-\frac{1}{2}\right)^{j-i}j!E^{j-i}.$$

Proof. From Lemma 18 of [24] we know that if $\dot{H}(E)=cE$ and $a\in\mathbb{C}$, then

$$\dot{E}^m(H+a)^j=E^m\sum_{\ell=0}^{m}(-1)^\ell\binom{m}{\ell}(H+a+c\ell)^j. \tag{41}$$

From this and Lemma 13 of [24] we get

$$\dot{E}^{j-i}(H^{j-i})=E^{j-i}\sum_{\ell=0}^{j-i}(-1)^\ell\binom{j-i}{\ell}\left(H+\frac{\ell}{2}\right)^{j-i}=\left(-\frac{1}{2}\right)^{j-i}(j-i)!E^{j-i}.$$

Using (40) we can write

$$\begin{aligned}
t_{ij}&=\sum_{k=0}^{i}(-1)^k\binom{i}{k}\sum_{\ell=0}^{j}\binom{j}{\ell}\left(\frac{i}{2}-1-k\right)^\ell H^{j-\ell}\\
&=\sum_{\ell=i}^{j}\left(\sum_{k=0}^{i}(-1)^k\binom{i}{k}\left(\frac{i}{2}-1-k\right)^\ell\right)\binom{j}{\ell}H^{j-\ell}\\
&=\frac{j!}{(j-i)!}H^{j-i}+\cdots
\end{aligned}$$

Then

$$\dot{E}^{j-i}(t_{ij})=\frac{j!}{(j-i)!}\dot{E}^{j-i}(H^{j-i})=\left(-\frac{1}{2}\right)^{j-i}j!E^{j-i}.$$

Theorem 7.3. *If $b=b_m\otimes Z^m+\cdots+b_0\in B$, then $\dot{E}^{m+1}(c_j)=0$ for all $0\le j\le m$.*

Proof. Since $b \in B$, c satisfies the system of equations (i) of Theorem 5.3 with $\widetilde{Y} = Y + H$. Therefore c satisfies equations (iii) of Theorem 5.3 for all $\ell, n \in \mathbb{N}_o$. Hence, since $c^{(m+1)} = 0$, if we consider $\ell = m+1$ in equation (iii) of Theorem 5.3 and we use Lemma 6.2 with $X = E$ we obtain

$$\sum_{j=n}^{m} \dot{E}^{m+1}(c_j)\varphi_{j-n}\left(\frac{2m+2-n}{2} - \widetilde{Y}\right) \equiv 0, \tag{42}$$

for $0 \le n \le m$. Now, taking into account that right multiplication by $\widetilde{Y}$ leaves invariant the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ because $\widetilde{Y} \in \mathfrak{t}$, (42) together with decreasing induction on n starting from $n = m$ implies that $\dot{E}^{m+1}(c_j) \equiv 0$. Hence using Lemma 7.1 and Theorem 6.4 it follows that $\dot{E}^{m+1}(c_j) = 0$ for all $0 \le j \le m$.

Corollary 7.4. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{2m+1-j}(b_j) = 0$ for all $0 \le j \le m$.*

Proof. For $j = m$ the assertion follows directly from Theorem 7.3 since $c_m = m! b_m$ (Lemma 7.1). Now we proceed by decreasing induction on j. Thus let $0 \le j < m$ and assume that $\dot{E}^{2m+1-k}(b_k) = 0$ for all $j < k \le m$. Then, since $m+1 < 2m+1-j$, using Leibnitz rule, Lemma 7.2 and the inductive hypothesis we obtain

$$\dot{E}^{2m+1-j}(c_j) = \dot{E}^{2m+1-j}\Big(\sum_{k=j}^{m} b_k t_{jk}\Big) = j!\dot{E}^{2m+1-j}(b_j).$$

Since $\dot{E}^{2m+1-j}(c_j) = 0$ the proof of the corollary is completed.

The following result was proved in Theorem 30 of [24], in a different way.

Theorem 7.5. *Let $m, w, \alpha \in \mathbb{Z}$, $0 \le w, \alpha \le m$, $\alpha + w \ge m+1$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and $\dot{E}^{m+\alpha+1-j}(b_j) \equiv 0$ for all $0 \le j \le m$, then*

$$\sum_{j=m-w}^{m} (-2)^{-j} j! \binom{\alpha+w}{j+w-m} \dot{E}^{m+\alpha-j}(b_j)E^j \equiv 0.$$

Proof. From the previous theorem we know that $\dot{E}^{m+1}(c_j) \equiv 0$ for all $0 \le j \le m$. Since $w \ge 1$ we have $\dot{E}^{\alpha+w}(c_{m-w}) = 0$. Now using the Leibnitz rule and Lemma 7.2 we compute

$$\begin{aligned}
\dot{E}^{\alpha+w}(c_{m-w}) &= \dot{E}^{\alpha+w}\Big(\sum_{j=m-w}^{m} b_j t_{m-w,j}\Big) \\
&\equiv \sum_{j=m-w}^{m} \binom{\alpha+w}{j+w-m} \dot{E}^{m+\alpha-j}(b_j)\dot{E}^{j+w-m}(t_{m-w,j}) \\
&= \sum_{j=m-w}^{m} \binom{\alpha+w}{j+w-m} (-2)^{-(j+w-m)} j! \dot{E}^{m+\alpha-j}(b_j)E^{j+w-m}.
\end{aligned}$$

Therefore

$$\sum_{j=m-w}^{m} \binom{\alpha+w}{j+w-m}(-2)^{-(j+w-m)} j! \dot{E}^{m+\alpha-j}(b_j)E^{j+w-m} \equiv 0.$$

If we multiply the above equation on the right by $(-2)^{w-m}E^{m-w}$ we obtain the thesis.

In order to proceed any further with our argument we collect in the following proposition the results that we need about the representations in Γ. Some of these facts where first established in [12], others were proved in [2] and in [4] they were generalized to any real rank one semisimple Lie group. Since we shall mainly be concerned with those representations $\gamma \in \Gamma$ that occur as subrepresentations of $U(\mathfrak{k})$ we let

$$\Gamma_1 = \{\gamma \in \Gamma : \gamma \text{ is a subrepresentation of } U(\mathfrak{k})\}. \tag{43}$$

Proposition 7.6. *Let G_o be locally isomorphic to $SU(n,1)$, $n \geq 2$. Then for $E = E_1$ (respectively $E = E_2$) there exists a Borel subalgebra $\mathfrak{b}_\mathfrak{k} = \mathfrak{h}_\mathfrak{k} \oplus \mathfrak{k}^+$ of $\mathfrak{k}$ such that $\mathfrak{m}^+ \subset \mathfrak{k}^+$ and $E_1 \in \mathfrak{k}^+$ (respectively $E_2 \in \mathfrak{k}^+$). Moreover:*

(i) The Cartan complement $\mathfrak{p} = \mathfrak{p}_1 \oplus \mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are irreducible $\mathfrak{k}$-modules and $\mathfrak{p}_1 = \mathfrak{p}_2^*$.
(ii) Let ξ_1 and ξ_2 be the highest weights of $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively, and for any $\gamma \in \hat{K}$ let ξ_γ denote its highest weight. Then, $\gamma \in \Gamma$ if and only if $\xi_\gamma = k_1\xi_1 + k_2\xi_2$, $k_1, k_2 \in \mathbb{N}_o$ and $d(\gamma) = k_1 + k_2$.
(iii) We have $\gamma \in \Gamma_1$ if and only if $\xi_\gamma = k(\xi_1 + \xi_2)$, $k \in \mathbb{N}_o$.
(iv) Let $\gamma \in \Gamma_1$, $E = E_1$ (respectively $E = E_2$) and let $q(\gamma)$ be as in (37). Then $E^{q(\gamma)}(V_\gamma^M) = V_\gamma^{\mathfrak{k}^+}$, $\xi_\gamma = q(\gamma)(\xi_1 + \xi_2)$ and $d(\gamma) = 2q(\gamma)$.
(v) If we set $X = [E_1, E_2]$ then $X \neq 0$, $X \in \mathfrak{m}^+$ if $n \geq 3$ and $X \in \mathfrak{t} + \mathfrak{z}(\mathfrak{k})$ if $n = 2$. Moreover $[X, E_1] = [X, E_2] = 0$ if $n \geq 3$. For $\gamma \in \Gamma_1$ let $0 \neq b \in V_\gamma^M$, then $E_2^k E_1^\ell(b) = E_1^\ell E_2^k(b)$ for all $\ell, k \geq 0$ and $E_2^{q(\gamma)}E_1^{q(\gamma)}(b) \neq 0$.

For a construction of the Borel subalgebra $\mathfrak{b}_\mathfrak{k}$ we refer the reader to Section 3 of [4]; also (i), (ii), (iv) and (v) are proved in Proposition 4.4, Theorem 4.5 and Theorem 5.3 of [4]. On the other hand (iii) follows from well known general facts.

Lemma 7.7. *Let $k \in \mathbb{N}_o$ and $u \in U(\mathfrak{k})^M$. Then, $\dot{E}_i^k(u) \equiv 0$ for $i = 1$ or $i = 2$ if and only if $\dot{E}_i^k(u) = 0$ for every $i = 1, 2$.*

Proof. Let us assume that $\dot{E}_1^k(u) \equiv 0$, $k \geq 1$. Then Theorem 6.4 implies that $\dot{E}_1^k(u) = 0$. Hence, in view of Proposition 7.6, it follows that $u \in \bigoplus U(\mathfrak{k})_\gamma^M$ where the sum extends over all $\gamma \in \Gamma_1$ such that $q(\gamma) \leq k - 1$. Then since $q(\gamma)$ is independent of the choice of the simple root $\alpha = \alpha_1$ or $\alpha = \alpha_n$, we obtain $\dot{E}_2^k(u) = 0$ which completes the proof.

For further reference we now recall Lemma 1 of [26].

Lemma 7.8. *Let G_o be locally isomorphic to $SU(2,1)$ and set $Y = Y_{\alpha_1} = -Y_{\alpha_2}$. Also let $0 \neq D \in \mathfrak{z}(\mathfrak{k})$ and let ζ denote the Casimir element of $[\mathfrak{k}, \mathfrak{k}]$. Then $\{\zeta^i D^j\}_{i,j\geq 0}$ is a basis of $\mathfrak{z}(U(\mathfrak{k}))$ and $\{\zeta^i D^j Y^k\}_{i,j,k\geq 0}$ is a basis of $U(\mathfrak{k})^M$.*

The following theorem plays a crucial role in the proof of Theorem 4.5 because it allows us to obtain from Theorem 7.5 two systems of linear equations and therefore doubling the number of equations.

Theorem 7.9. *Let G_o be locally isomorphic to $SU(n,1)$, $n \geq 2$. Also let $m, k \in \mathbb{N}_o$, $m \leq k$, and let $b_j \in U(\mathfrak{k})^M$ be such that $\dot{E}^{k+1-j}(b_j) \equiv 0$ for all $0 \leq j \leq m$ and for $E = E_1$ or $E = E_2$. Then*

(i) If $\sum_{j=0}^m \dot{E}^{k-j}(b_j)E^j \equiv 0$ for $E = E_1$ and $E = E_2$ we obtain

$$\sum_{\substack{0\leq j\leq m \\ j \text{ even}}} \dot{E}^{k-j}(b_j)E^j = 0 = \sum_{\substack{0\leq j\leq m \\ j \text{ odd}}} \dot{E}^{k-j}(b_j)E^j.$$

(ii) If $\sum_{j=0}^m \dot{E}^{k-j}(b_j)E^j \equiv 0$ for $E = E_1$ or $E = E_2$ we have

$$\sum_{j=0}^m \dot{E}_i^{k-j}(b_j)E_i^j = 0 = \sum_{j=0}^m (-1)^j \dot{E}_{i'}^{k-j}(b_j)E_{i'}^j,$$

for $i' \neq i$ and $i, i' = 1, 2$.

Proof. At the beginning of this section we chose $T \in \mathfrak{z}(\mathfrak{m})$ in such a way that $[T, E_1] = E_1$ and $[T, E_2] = -E_2$. Then from (41) we have

$$\dot{E}^j(T^j) = E^j \sum_{\ell=0}^j (-1)^\ell \binom{j}{\ell} (T + \ell\epsilon)^j = (-\epsilon)^j j! E^j, \tag{44}$$

where $\epsilon = 1$ if $E = E_1$ and $\epsilon = -1$ if $E = E_2$.

Now Lemma 7.7 implies that $\dot{E}^{k+1-j}(b_j) = 0$ for $E = E_1$ and $E = E_2$. Then using Leibnitz rule and (44) we obtain

$$\dot{E}^k(b_j T^j) = \sum_{\ell=0}^k \binom{k}{\ell} \dot{E}^{k-\ell}(b_j)\dot{E}^\ell(T^j) = \binom{k}{j} \dot{E}^{k-j}(b_j)(-\epsilon)^j j! E^j. \tag{45}$$

Therefore

$$\sum_{j=0}^m \dot{E}^{k-j}(b_j)E^j = \dot{E}^k \sum_{j=0}^m \binom{k}{j}^{-1} (-\epsilon)^j (j!)^{-1} b_j T^j,$$

for both $E = E_1$ and $E = E_2$. Then, if we assume that the hypothesis in (i) holds, since $\sum_{j=0}^m \binom{k}{j}^{-1} (-\epsilon)^j (j!)^{-1} b_j T^j \in U(\mathfrak{k})^M$, applying Theorem 6.4 we obtain that $\sum_{j=0}^m \dot{E}^{k-j}(b_j)E^j = 0$ for $E = E_1$ and $E = E_2$. Moreover if we assume that the hypothesis in (ii) holds, applying Lemma 7.7 we complete the proof of (ii) for every $n \geq 2$.

In view of Proposition 7.6 (v) to prove (i) we shall consider two cases according as $n = 2$ or $n \geq 3$. Let us assume first that $n = 2$. It follows from Lemma 7.8 that we can write, in a unique way, $b_j = \sum_i a_{i,j} Y^i$ with $a_{i,j} \in \mathfrak{z}(U(\mathfrak{k}))$ and $0 \leq j \leq m$. On the other hand from Lemma 5.1 we have $\dot{E}(Y) = \frac{3\epsilon}{2} E$, hence from (41) and Lemma 13 of [26] we get

$$\dot{E}^t(Y^i) = \begin{cases} 0, & \text{if } t > i \\ (-1)^t t! \left(-\frac{3\epsilon}{2}\right)^t E^t, & \text{if } t = i. \end{cases} \tag{46}$$

Then, since in this case $\dot{E}^{k+1-j}(b_j) = 0$ for $0 \leq j \leq m$ and for $E = E_1$ or $E = E_2$, using (46) we obtain that $b_j = \sum_{i=0}^{k-j} a_{i,j} Y^i$. Therefore

$$\sum_{j=0}^{m} \dot{E}^{k-j}(b_j) E^j = E^k \sum_{j=0}^{m} \left(\tfrac{3\epsilon}{2}\right)^{k-j} a_{k-j,j} \tag{47}$$

for both $E = E_1$ and $E = E_2$. Hence if $\sum_{j=0}^{m} \dot{E}^{k-j}(b_j) E^j = 0$ for $E = E_1$ and $E = E_2$, using (47) we obtain (i) for $n = 2$.

Assume from now on that $n \geq 3$. Then from Proposition 7.6 (v) by a double induction on $\ell, k \geq 0$ we get

$$\dot{E}_1^\ell(E_2^k) = \binom{k}{\ell} \ell! E_2^{k-\ell} X^\ell, \quad \dot{E}_2^\ell(E_1^k) = \binom{k}{\ell} \ell! E_1^{k-\ell} (-X)^\ell. \tag{48}$$

From Proposition 7.6 (v) and (48) it follows that

$$\begin{aligned} \dot{E}_2^k \sum_{j=0}^{m} \dot{E}_1^{k-j}(b_j) E_1^j &= \sum_{\substack{0 \leq j \leq m \\ 0 \leq \ell \leq k}} \binom{k}{\ell} \dot{E}_2^{k-\ell} \dot{E}_1^{k-j}(b_j) \dot{E}_2^\ell(E_1^j) \\ &= \sum_{j=0}^{m} \binom{k}{j} \dot{E}_2^{k-j} \dot{E}_1^{k-j}(b_j) j! (-X)^j. \end{aligned}$$

Hence

$$\sum_{j=0}^{m} \binom{k}{j} j! \dot{E}_2^{k-j} \dot{E}_1^{k-j}(b_j)(-X)^j = 0. \tag{49}$$

Similarly we get

$$\sum_{j=0}^{m} \binom{k}{j} j! \dot{E}_1^{k-j} \dot{E}_2^{k-j}(b_j) X^j = 0. \tag{50}$$

Then, since $\dot{E}_1^{k-j} \dot{E}_2^{k-j}(b_j) = \dot{E}_2^{k-j} \dot{E}_1^{k-j}(b_j)$ (Proposition 7.6 (v)), from (49) and (50) we obtain

$$\dot{E}_2^k \sum_{\substack{0 \leq j \leq m \\ j \text{ even}}} \dot{E}_1^{k-j}(b_j) E_1^j = \sum_{\substack{0 \leq j \leq m \\ j \text{ even}}} \binom{k}{j} j! \dot{E}_2^{k-j} \dot{E}_1^{k-j}(b_j) X^j = 0.$$

Now by using (45) we can write $\sum_{0\le j\le m,\; j \text{ even}} \dot E_1^{k-j}(b_j)E_1^j = \dot E_1^k(u)$ with $u \in U(\mathfrak{k})^M$. Then $\dot E_2^k \dot E_1^k(u) = 0$ which implies that $\dot E_1^k(u) = 0$ (Proposition 7.6 (v)). Similarly we get $\sum_{0\le j\le m,\; j \text{ odd}} \dot E_1^{k-j}(b_j)E_1^j = 0$, and also $\sum_{0\le j\le m,\; j \text{ even}} \dot E_2^{k-j}(b_j)E_2^j = \sum_{0\le j\le m,\; j \text{ odd}} \dot E_2^{k-j}(b_j)E_2^j = 0$. This completes the proof of the theorem.

Taking into account Theorems 7.5 and 7.9 we are led to consider, for each $1 \le \alpha \le m$, the following systems of linear equations

$$\sum_{\substack{m-w\le j\le m \\ j \text{ even (odd)}}} (-2)^{-j} j! \binom{\alpha+w}{j+w-m} \dot E^{m+\alpha-j}(b_j)E^j = 0, \tag{51}$$

for $m+1-\alpha \le w \le m$.

If we put $x_j = \frac{(-2)^{-j} j!}{(\alpha+m-j)!} \dot E^{m+\alpha-j}(b_j)E^{j+w-m}$ and multiply (51) by $\frac{1}{(\alpha+w)!}$ we obtain

$$\sum_{\substack{m-w\le j\le m \\ j \text{ even (odd)}}} \frac{1}{(j+w-m)!} x_j = 0. \tag{52}$$

Now if we make the change of indices $j = 2r-\delta$, $m-w+\delta = s$ and put $y_r = \frac{x_{2r-\delta}}{(2r)!}$ then the systems (52) become

$$\sum_{\delta\le r\le [\frac{m+\delta}{2}]} \binom{2r}{s} y_r = 0, \tag{53}$$

for $\delta \le s \le \alpha+\delta-1$ and $\delta = 0, 1$.

Proposition 7.10. *For $\delta = 0, 1$ let M_δ be the matrix with entries defined by $M_{rs} = \binom{2r}{s}$ for $\delta \le r, s \le k$. Then*

$$\det(M_\delta) = 2^{k(k+1)/2}.$$

Proof. For each $\delta \le s \le k$ we let $\binom{2r}{s}$ denote the s-column of M_δ and we consider the determinant of M_δ as a multilinear function of their columns. Thus

$$\det(M_\delta) = \det\left(\binom{2r}{\delta}, \binom{2r}{\delta+1}, \dots, \binom{2r}{k}\right).$$

If we view the binomial coefficient $\binom{2r}{s}$ as a polynomial in the variable r of degree s we realize that we can write, in a unique way,

$$\binom{2r}{s} = 2^s \binom{r}{s} + a_{s-1}\binom{r}{s-1} + \dots + a_0,$$

in fact $a_j = 0$ for $j < \frac{s}{2}$. Then

$$\det(M) = \det\left(2^\delta \binom{r}{\delta}, 2^{\delta+1}\binom{r}{\delta+1}, \dots, 2^k\binom{r}{k}\right) = 2^{k(k+1)/2}.$$

This completes the proof of the proposition.

Theorem 7.11. *Let G_o be locally isomorphic to $SU(n,1)$, $n \geq 2$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{[\frac{m}{2}]+m+1-j}(b_j) = 0$ for all $0 \leq j \leq m$.*

Proof. We shall prove by decreasing induction on α in the interval $[\frac{m}{2}] \leq \alpha \leq m$ that $\dot{E}^{\alpha+m+1-j}(b_j) = 0$ for all $0 \leq j \leq m$. For $\alpha = m$ this result follows from Corollary 7.4 and Theorem 6.4. Thus assume that $[\frac{m}{2}] < \alpha \leq m$ and that $\dot{E}^{\alpha+m+1-j}(b_j) = 0$ for all $0 \leq j \leq m$. Then in view of Theorems 7.5 and 7.9 we have that the systems of linear equations (51) and their equivalent versions (52) and (53) hold.

Since $[\frac{m}{2}] + 1 \leq \alpha$ the number of unknowns in the system (53) is less or equal than the number of equations. Moreover, it follows from Proposition 7.10 that when $\delta = 0$ the rank of the coefficient matrix of the system (53) is $[\frac{m}{2}] + 1$ which it is equal to the number of unknowns. Thus $\dot{E}^{\alpha+m-j}(b_j) = 0$ for $0 \leq j \leq m$ and j even. Similarly , when $\delta = 1$ the rank of the coefficient matrix is $[\frac{m+1}{2}]$ which it is also equal to the number of unknowns. Therefore $\dot{E}^{\alpha+m-j}(b_j) = 0$ for $0 \leq j \leq m$ and j odd. The inductive hypothesis is completed and the theorem is proved.

We are now in a position to prove one of the conditions needed to establish Theorem 1.1 (see Theorem 4.5) when G_o is locally isomorphic to $\mathrm{SU}(n,1)$.

Corollary 7.12. *Let G_o be locally isomorphic to $SU(n,1)$, $n \geq 2$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $d(b_j) \leq 3m - 2j$ for all $0 \leq j \leq m$. In particular $d(b_m) \leq m$.*

Proof. Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then it follows from Theorem 7.11 that $\dot{E}^{[m/2]+m+1-j}(b_j) = 0$ for all $0 \leq j \leq m$. Hence in view of (37) and Proposition 7.6 it follows that $b_j \in \bigoplus U(\mathfrak{k})^M_\gamma$, where the sum extends over all $\gamma \in \Gamma_1$ such that $d(\gamma) \leq 3m - 2j$. Therefore $d(b_j) \leq 3m - 2j$ as we wanted to prove.

7.1. **Weyl group invariance of the leading term.** To complete the proof of Theorem 1.1 we need to show that if $b \in B$ then its leading term $\widetilde{b} = b_m \otimes Z^m \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ (see Theorem 4.5). In order to obtain this result it is enough to prove that m is even, because in this case $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$ and therefore the non trivial element of W can be represented by an element in M_o' which acts on $\mathfrak{g}$ as the Cartan involution.

As in the beginning of this section to any $b(x) \in U(\mathfrak{k})[x]$ we associate $c(x) \in U(\mathfrak{k})[x]$ defined by $c(x) = b(x + H - 1)$ where H is defined in (38). Recall that if $b(x) \in U(\mathfrak{k})^M[x]$ then $c(x) \in U(\mathfrak{k})^M[x]$, see Lemma 7.1. Whenever necessary we shall refer to $c(x)$ as $c_1(x)$ or $c_2(x)$ according as $\alpha = \alpha_1$ or $\alpha = \alpha_n$. On the other hand $c(x)$ will generically stand for $c_1(x)$ or $c_2(x)$. Also, as before, we shall find it convenient to write $c_i(x) = \sum_{j=0}^m c_{i,j}\varphi_j(x)$ with $c_{i,j} \in U(\mathfrak{k})$ for $i = 1, 2$.

Proposition 7.13. *Let $r \in \mathbb{N}_o$, $0 \le r \le m$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and $\dot{E}_1^{m+r+1-j}(c_{1,j}) = \dot{E}_1^{m+r+1-j}(c_{2,j}) = 0$ for $r+1 \le j \le m$ then*

$$\dot{E}_1^{m-j}(c_{1,r+j})E_1^j = (-1)^{m-r}\dot{E}_1^{r+j}(c_{1,m-j})E_1^{m-r-j}$$

and

$$\dot{E}_1^{m-j}(c_{2,r+j})E_1^j = \dot{E}_1^{r+j}(c_{2,m-j})E_1^{m-r-j}$$

for $j = 0, \dots, \left[\frac{m-r}{2}\right]$.

Proof. If we set $\ell = m - j$ and $n = r + j$ in equation (iii) of Theorem 5.3 we get

$$\begin{aligned}\dot{E}_1^{m-j}\big(c_1^{(r+j)}\big)&(-\tfrac{r+j}{2} + m - j - \widetilde{Y}_1)E_1^{r+j} \\ &- (-1)^{m-r}\dot{E}_1^{r+j}\big(c_1^{(m-j)}\big)(-\tfrac{m-j}{2} + r + j - \widetilde{Y}_1)E_1^{m-j} \equiv 0.\end{aligned}$$

By hypothesis $\dot{E}_1^{m-j}\big(c_1^{(r+j)}\big) = \sum_k \dot{E}_1^{m-j}(c_{1,k})\varphi_{k-r-j} = \dot{E}_1^{m-j}(c_{1,r+j})$, and the first assertion follows from Theorem 7.9 (i).

In a similar way we obtain

$$\dot{E}_2^{m-j}(c_{2,r+j})E_2^j = (-1)^{m-r}\dot{E}_2^{r+j}(c_{2,m-j})E_2^{m-r-j}.$$

Now the second assertion is a direct consequence of Theorem 7.9 (ii).

In order to get a better insight of Proposition 7.13, for $r = 0, \dots, m+1$ we introduce the column vectors $\sigma_r = \sigma_r(b)$ and $\tau_r = \tau_r(b)$ of $m + r + 1$ entries defined by

$$\sigma_r = (0, \dots, 0, \dot{E}_1^r(c_{1,m})E_1^{m-r}, \dots, \dot{E}_1^{m-1}(c_{1,r+1})E_1, \dot{E}_1^m(c_{1,r}), 0, \dots, 0)^t,$$

$$\tau_r = (\underbrace{0, \dots, 0}_{r}, \underbrace{\dot{E}_1^r(c_{2,m})E_1^{m-r}, \dots, \dot{E}_1^{m-1}(c_{2,r+1})E_1, \dot{E}_1^m(c_{2,r})}_{m+1-r}, \underbrace{0, \dots, 0}_{r})^t.$$

Let us observe that by definition $\sigma_{m+1} = \tau_{m+1} = 0$, and that the last $m+1$ entries of σ_r and τ_r are respectively of the form $\dot{E}_1^{r+j}(c_{1,m-j})E_1^{m-r-j}$ and $\dot{E}_1^{r+j}(c_{2,m-j})E_1^{m-r-j}$ for $0 \le j \le m$, see Theorem 6.3 and Lemma 6.7.

Let J_{m+r} be the $(m + r + 1) \times (m + r + 1)$ matrix with ones in the skew diagonal and zeros everywhere else, thus

$$J_{m+r} = \begin{pmatrix} 0 & & & 1 \\ & & \cdot & \\ & \cdot & & \\ \cdot & & & \\ 1 & & & 0 \end{pmatrix}. \tag{54}$$

In the following corollary we rephrase Proposition 7.13 in terms of the vectors σ_r and τ_r.

Corollary 7.14. *Let $r \in \mathbb{N}_o$, $0 \le r \le m$. If $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and $\sigma_{r+1} = \tau_{r+1} = 0$ then*

$$J_{m+r}\sigma_r = (-1)^{m+r}\sigma_r \qquad \textit{and} \qquad J_{m+r}\tau_r = \tau_r.$$

The vectors σ_r and τ_r are nicely related by a Pascal matrix. Let P_k denote the following $(k+1)\times(k+1)$ lower triangular matrix

$$P_k = \begin{pmatrix} 1 & & & & & & \\ 1 & 1 & & & & & \\ 1 & 2 & 1 & & & & \\ \cdot & & & \cdot & & & \\ \cdot & & & & \cdot & & \\ \cdot & & & & & \cdot & \\ \binom{k}{0} & \cdot & \cdot & \cdot & \cdot & \cdot & \binom{k}{k} \end{pmatrix}. \tag{55}$$

Proposition 7.15. *If $r \in \mathbb{N}_o$, $0 \le r \le m$ and $\sigma_{r+1} = 0$ then $P_{m+r}\sigma_r = \tau_r$, where P_{m+r} is the $(m+r+1)\times(m+r+1)$ Pascal matrix.*

Proof. Since $c_2(x) = c_1(x-T)$, for any $0 \le j \le m-r$ we have

$$c_{2,r+j} = c_2^{(r+j)}(0) = c_1^{(r+j)}(-T) = \sum_{s=0}^{m-r-j} c_{1,r+j+s}\varphi_s(-T).$$

On the other hand (44) implies that $\dot{E}_1^k((-T)^k) = k!E_1^k$ and $\dot{E}_1^t((-T)^k) = 0$ if $t > k$. Therefore, since $\varphi_k(-T) = \frac{1}{k!}(-T)^k + \cdots$, where the dots stand for lower degree terms in T, we have $\dot{E}_1^k(\varphi_k(-T)) = E_1^k$ and $\dot{E}_1^t(\varphi_k(-T)) = 0$ if $t > k$. Now the hypothesis $\sigma_{r+1} = 0$ together with Theorem 7.3 imply that $\dot{E}_1^{m+r+1-i}(c_{1,i}) = 0$ for every $0 \le i \le m$. Hence, for any $-r \le j \le m-r$ using the Leibnitz rule we obtain

$$\begin{aligned} \dot{E}_1^{m-j}(c_{2,r+j})E_1^j &= \sum_{s=0}^{m-r-j} \dot{E}_1^{m-j}(c_{1,r+j+s}\varphi_s(-T))E_1^j \\ &= \sum_{s=0}^{m-r-j}\sum_{\ell=0}^{m-j} \binom{m-j}{\ell} \dot{E}_1^{m-j-\ell}(c_{1,r+j+s})\dot{E}_1^{\ell}(\varphi_s(-T))E_1^j \\ &= \sum_{s=0}^{m-r-j} \binom{m-j}{s} \dot{E}_1^{m-j-s}(c_{1,r+j+s})E_1^{s+j}, \end{aligned}$$

which implies that the last $m+1$ components of $P_{m+r}\sigma_r$ and τ_r are equal. Since by definition the first r components of $P_{m+r}\sigma_r$ and τ_r are equal to 0 the proposition follows.

For $t \in \mathbb{N}_o$ we shall be interested in considering certain $(t+1)\times(t+1)$ submatrices of a Pascal matrix P_n formed by any choice of $t+1$ consecutive rows and $t+1$ consecutive columns of P_n, with the only condition that the submatrix does not have zeros in its main diagonal. To be precise, for any $0 \le a, b \le n$, $a, b \in \mathbb{N}_o$ such that $b \le a$ we shall be interested in submatrices

A of P_n of the following form

$$A = \begin{pmatrix} \binom{a}{b} & \binom{a}{b+1} & \cdots & \binom{a}{b+t} \\ \binom{a+1}{b} & \binom{a+1}{b+1} & \cdots & \binom{a+1}{b+t} \\ \vdots & \vdots & & \vdots \\ \binom{a+t}{b} & \binom{a+t}{b+1} & \cdots & \binom{a+t}{b+t} \end{pmatrix}. \tag{56}$$

In the following proposition we collect some results that will be very important in the proof of our goal, that is, that the algebra B does not contain elements of odd degree. The proof of this proposition will be given in an appendix at the end of this section.

Proposition 7.16. *If J_n and P_n are the matrices defined above we have,*
(i) If $v \in \mathbb{C}^{n+1}$ satisfies $J_n v = (-1)^n v$ and $J_n P_n v = P_n v$ then v begins and ends with the same number of coordinates, say k, equal to zero. Moreover, k is even or odd according as n is even or odd, respectively.
(ii) If A is a $(t+1)\times(t+1)$ submatrix of P_n of the form (56) then A is non-singular.

Lemma 7.17. *Let $n \in \mathbb{N}_0$ be an even number and let $v \in U(\mathfrak{k})^M$ be such that $\dot{E}^{t+1}(v) = 0$. If $n \geq 2t$ then there exists $b \in B$ of degree n with $b_n = v$ and $\sigma_{t+1}(b) = 0$.*

Proof. The proof will be by induction on n. If $n = 0$ the assertion follows from Proposition 7.6 and Proposition 4.4. Let us now take $n > 0$ even and consider $S = \{b \in B : \deg(b) = n \text{ and } b_n = v\}$. From Proposition 4.4 we get that S is nonempty, because from Proposition 7.6 we obtain $d(v) \leq 2t \leq n$. For each $b \in S$ let $r(b) \in \mathbb{N}_o$ be such that $\sigma_{r(b)+1}(b) = 0$ and $\sigma_{r(b)}(b) \neq 0$, and let $r = \min\{r(b) : b \in S\}$. We want to prove that $r \leq t$.

Let us assume that $r > t$ and let us take $b \in S$ such that $r(b) = r$. We have

$$\sigma_r(b) = (\underbrace{0,\dots,0}_{r}, \underbrace{\dot{E}_1^r(c_{1,n})E_1^{n-r}, \dots, \dot{E}_1^{n-1}(c_{1,r+1})E_1, \dot{E}_1^n(c_{1,r})}_{n+1-r}, \underbrace{0,\dots,0}_{r})^t,$$

$$J_{n+r}\sigma_r(b) = (-1)^{n+r}\sigma_r(b) \qquad \text{and} \qquad J_{n+r}P_{n+r}\sigma_r(b) = P_{n+r}\sigma_r(b).$$

Since $r > t$ the hypothesis $\dot{E}^{t+1}(v) = 0$ implies that the number of zeros with which $\sigma_r(b)$ starts is of the form $r + j_0$ with $j_0 \geq 1$. Thus we have

$$\sigma_r(b) = (\underbrace{0,\dots,0}_{r+j_0}, \underbrace{\dot{E}_1^{r+j_0}(c_{1,n-j_0})E_1^{n-j_0-r}, \dots, \dot{E}_1^{n-j_0}(c_{1,r+j_0})E_1^{j_0}}_{n+1-r-2j_0}, \underbrace{0,\dots,0}_{r+j_0})^t,$$

with j_0 even. From $\sigma_r(b) \neq 0$ we get $n+1-r-2j_0 > 0$ and from the definition of j_0 we obtain $\dot{E}_1^{r+j_0}(c_{1,n-j_0}) \neq 0$. Among all $b \in S$ with $\sigma_r(b) \neq 0$ we choose one with the largest j_0.

Let $n' = n - j_0$, $t' = r + j_0$, $v' = c_{1,n-j_0}$. Since $\sigma_{r+1}(b) = 0$ we have $\dot{E}_1^{t'+1}(v') = 0$. Now we consider the following two possibilities: $n' \geq 2t'$ and

$n' < 2t'$, and in both cases we will get a contradiction which will prove the lemma.

If $n' \geq 2t'$ then the inductive hypothesis implies that there exists $b' \in B$ of degree n' such that $b'_{n'} = v'$ and $\sigma_{t'+1}(b') = 0$, thus

$$(\underbrace{0,\ldots,0}_{r+j_0+1},\underbrace{\dot{E}_1^{r+j_0+1}(c'_{1,n-j_0})E_1^{n-2j_0-r-1},\ldots,\dot{E}_1^{n-j_0}(c'_{1,r+j_0+1})}_{n-r-2j_0},\underbrace{0,\ldots,0}_{r+j_0+1})^t = 0.$$

Therefore $\sigma_{r+1}(b-b') = 0$. This is a contradiction because either $\sigma_r(b-b')$ starts with more zeros than $\sigma_r(b)$ or $r(b-b') < r$.

On the other hand if $n' < 2t'$ then $n-r-2j_0 < r+j_0$. Let A be the submatrix of P_{n+r} formed by the elements in the last $n+1-r-2j_0$ rows and in the $n+1-r-2j_0$ central columns of P_{n+r}. From Proposition 7.16 we know that A is nonsingular.

Since $P_{n+r}\sigma_r(b) = \tau_r(b)$, $\tau_r(b)$ starts with $r+j_0$ zeros, and $J_{n+r}\tau_r(b) = \tau_r(b)$ implies that the last $r+j_0$ coordinates of $\tau_r(b)$ are also zeros. Therefore the equation $P_{n+r}\sigma_r(b) = \tau_r(b)$ implies that the vector u formed by the $n+1-r-2j_0$ central coordinates of $\sigma_r(b)$ satisfies $Au = 0$, since $n+1-r-2j_0 \leq r+j_0$. This is a contradiction because $\sigma_r(b) \neq 0$.

We are now in a position to prove that the algebra B does not have elements of odd degree, which will complete the proof of the Theorem 1.1 when G_o is locally isomorphic to $\mathrm{SU}(n,1)$, $n \geq 2$.

Theorem 7.18. *If G_o is locally isomorphic to $SU(n,1)$, $n \geq 2$, and $b = b_m \otimes Z^m + \cdots + b_0 \in B$ with m odd, then $b_m = 0$. That is, B does not contain odd degree elements.*

Proof. Let $B_o = \{b \in B : \deg(b) \text{ is odd}\}$ and let us assume that B_o is not empty. Now define $r = \min\{t \in \mathbb{N}_o : \sigma_{t+1}(b) = 0 \text{ and } b \in B_o\}$ and take $b \in B_o$ such that $\sigma_{r+1}(b) = 0$; clearly $\sigma_r(b) \neq 0$. Let $m = m(b)$ denote the degree of b. Then in view of Corollary 7.14 and Proposition 7.15 we have

$$J_{m+r}\sigma_r(b) = (-1)^{m+r}\sigma_r(b) \quad \text{and} \quad J_{m+r}P_{m+r}\sigma_r(b) = P_{m+r}\sigma_r(b). \tag{57}$$

Hence the vector $\sigma_r(b)$ satisfies the conditions of part (i) of Proposition 7.16, therefore if r is even $\sigma_r(b)$ begins (and ends) with an odd number of coordinates equal to zero and, on the other hand, if r is odd $\sigma_r(b)$ begins (and ends) with an even number of coordinates equal to zero.

We recall that the first and the last r coordinates of $\sigma_r(b)$ are zero and that the others are

$$\dot{E}_1^{r+j}(c_{1,m-j})E_1^{m-r-j}, \qquad j = 0,\ldots,m-r.$$

Therefore $\dot{E}_1^r(c_{1,m}) = 0$. Let $j_0(b) = \max\{j \in \mathbb{N}_o : \dot{E}_1^{r+t}(c_{1,m-t}) = 0 \text{ for all } 0 \leq t \leq j \leq m-r-1\}$. Then we know that $j_0(b)$ is even and that $m-r-2j_0(b)-1 > 0$ because $\sigma_r(b) \neq 0$, $\sigma_r(b)$ starts with $r+j_0(b)+1$ zeros and $J_{m+r}\sigma_r(b) = (-1)^{m+r}\sigma_r(b)$.

Among all $b \in B_o$ such that $\sigma_{r+1}(b) = 0$ we choose one such that $j_0 = j_0(b)$ is the largest possible. We also have $m - j_0 - 1 < 2(r + j_0 + 1)$, because from $m-j_0-1 \geq 2(r+j_0+1)$ and $\sigma_{r+1}(b)=0$ we would obtain $d(c_{1,m-j_0-1}) = 2(r+j_0+1) \leq m-j_0-1$. Hence from Lemma 7.17 we would know that there exist $\widetilde{b} = c_{1,m-j_0-1} \otimes Z^{m-j_0-1} + \cdots \in B$ such that $\sigma_{r+j_0+2}(\widetilde{b}) = 0$ and the element $b-\widetilde{b} \in B_o$ would contradict the maximality of j_0.

Let A be the submatrix of P_{m+r} formed by the elements in the last $m-r-2j_0-1$ rows and in the $m-r-2j_0-1$ central columns of P_{m+r}. From Proposition 7.16 we know that A is nonsingular. Since $P_{m+r}\sigma_r(b) = \tau_r(b)$, $\tau_r(b)$ starts with $r+j_0+1$ zeros and since $J_{m+r}\tau_r(b) = \tau_r(b)$ the last $r+j_0+1$ coordinates of $\tau_r(b)$ are also zeros. Therefore the equation $P_{m+r}\sigma_r(b) = \tau_r(b)$ implies that the vector u formed by the $m-r-2j_0-1$ central coordinates of $\sigma_r(b)$ satisfies $Au=0$, since $m-r-2j_0-1 \leq r+j_0+1$. This is a contradiction because $\sigma_r(b) \neq 0$. This completes the proof of the theorem.

7.2. **Appendix.** Our goal in this appendix is to prove Proposition 7.16. For any $n \in \mathbb{N}_o$ let J_n and P_n be the $(n+1)\times(n+1)$ matrices defined in (54) and (55), and let H_n be the following $(n+1)\times(n+1)$ diagonal matrix

$$H_n = \begin{pmatrix} (-1)^n & & & & & \\ & (-1)^{n-1} & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & -1 & \\ & & & & & & 1 \end{pmatrix}.$$

Let V denote the vector space over $\mathbb{C}$ of all polynomials in $\mathbb{C}[X]$ of degree less or equal to n. Then P_n, H_n and J_n are respectively the matrices of the linear operators on V given by

$$f(X) \mapsto f(X+1), \quad f(X) \mapsto f(-X), \quad f(X) \mapsto X^n f(\frac{1}{X}), \tag{58}$$

with respect to the ordered basis $\{\binom{n}{n}X^n, \binom{n}{n-1}X^{n-1}, \ldots, \binom{n}{0}\}$. We summarize in the following lemma some basic properties of the matrices P_n, H_n and J_n.

Lemma 7.19. *(i)* $J_n^2 = H_n^2 = I$ *and* $J_nH_n = (-1)^n H_nJ_n$.
(ii) $P_n^{-1} = H_nP_nH_n$.
(iii) J_n *and* P_nH_n *are conjugate, in fact* $J_n = (J_nP_nH_n)^{-1}P_nH_n(J_nP_nH_n)$. *Hence the eigenvectors of* P_nH_n *associated to the eigenvalue* $\lambda = \pm 1$ *are all of the form* $J_nP_nH_n(v)$ *where* v *is an eigenvector of* J_n *associated to the eigenvalue* λ.

Proof. It follows from a simple calculation with the linear operators given in (58).

Now let $k \in \mathbb{N}_o$ and let $v = (v_o, \ldots, v_n)$ be a vector in $\mathbb{C}^{n+1}$. We shall say that v begins with k coordinates equal to zero if $v_o = v_1 = \cdots = v_{k-1} = 0$

and $v_k \neq 0$. Similarly we shall say that v ends with k coordinates equal to zero if $v_{n-k+1} = v_{n-k+2} = \cdots = v_n = 0$ and $v_{n-k} \neq 0$. Also via the ordered basis $\{\binom{n}{n}X^n, \binom{n}{n-1}X^{n-1}, \dots, \binom{n}{0}\}$ we shall identify any vector $v = (v_o, \dots, v_n) \in \mathbb{C}^{n+1}$ with the polynomial $f_v(X) = v_0\binom{n}{n}X^n + v_1\binom{n}{n-1}X^{n-1} + \cdots + v_n$. In particular observe that v begins with k coordinates equal to zero if and only if the degree of f_v is $n-k$. In the following lemma we prove part (i) of Proposition 7.16.

Lemma 7.20. *If $v \in \mathbb{C}^{n+1}$ satisfies $J_n v = (-1)^n v$ and $J_n P_n v = P_n v$ then v begins and ends with the same number of coordinates, say k, equal to zero. Moreover, k is even or odd according as n is even or odd, respectively.*

Proof. Let $v \in \mathbb{C}^{n+1}$ be as in the statement of the lemma and assume that v begins with k coordinates equal to zero. If we identify v with the polynomial f_v defined above we claim that the degree of f_v is even. In fact from Lemma 7.19 it follows that $H_n(v)$ is an eigenvector of J_n associated to the eigenvalue 1, and that $J_n P_n H_n(H_n v) = J_n P_n v = P_n v$ is an eigenvector of $P_n H_n$ associated to the eigenvalue 1. Then $P_n H_n(P_n v) = P_n v$, which implies that $H_n P_n v = v$ or, equivalently, that $f_v(1-X) = f_v(X)$. Now if we define $g(X) = f_v(X + \frac{1}{2})$ we obtain $g(X) = g(-X)$, which in particular implies that the degree of g is even. Hence the degree of f_v is even. The other assertion is a direct consequence of $J_n v = (-1)^n v$.

We are now interested in proving part (ii) of Proposition 7.16. Let $t, a, b \in \mathbb{N}_o$ be such that $b \leq a \leq n$ and let A be the $(t+1) \times (t+1)$ submatrix, of the Pascal matrix P_n, defined in (56). Our objective is to prove that A is nonsingular. Associated to the parameters t, a, b we shall consider a $(t+1) \times (t+1)$ diagonal matrix D_x defined for $x \in \mathbb{N}_o$, $x \geq b$, as follows

$$D_x = \begin{pmatrix} \binom{x}{b} & & & & & \\ & \binom{x+1}{b} & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & \binom{x+t}{b} \end{pmatrix},$$

and a $(t+1) \times (t+1)$ matrix A_0 of the following form

$$A_0 = \begin{pmatrix} \binom{a-b}{0} & \cdot & \cdot & \cdot & \binom{a-b}{t} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \binom{a-b+t}{0} & \cdot & \cdot & \cdot & \binom{a-b+t}{t} \end{pmatrix}. \tag{59}$$

The following lemma contains the desired result about A, hence completing the proof of Proposition 7.16.

Lemma 7.21. *Let $t, a, b \in \mathbb{N}_o$ be such that $b \leq a \leq n$ and let A, D_x and A_0 be as above. Then* *(i)* $A = D_a A_0 D_b^{-1}$,

(ii) $\det A = \prod_{i=0}^{t} \binom{a+i}{b} \binom{b+i}{b}^{-1}$, *therefore* A *is nonsingular.*

Proof. (i) For $0 \le i, j \le t$ let $A_{i,j}$ denote the (i,j) entry of the matrix A, then we have

$$\begin{aligned} A_{i,j} = \binom{a+i}{b+j} &= \frac{(a+i)!}{(b+j)!(a-b+i-j)!} \\ &= \frac{(a+i)!}{b!(a-b+i)!} \frac{(a-b+i)!}{j!(a-b+i-j)!} \frac{b!j!}{(b+j)!} \\ &= \binom{a+i}{b} \binom{a-b+i}{j} \binom{b+j}{b}^{-1}. \end{aligned}$$

Since the right hand side of this equality is the (i,j) entry of the product $D_a A_0 D_b^{-1}$ (i) follows.

In view of (i) in order to prove (ii) it is enough to show that $\det A_0 = 1$ for any matrix A_0 as in (59). We proceed by induction on t. It is clear that the result holds for $t = 0$, so let us assume that it holds for any matrix as in (59) of size $t \times t$ and let A_0 be the $(t+1) \times (t+1)$ matrix defined in (59). Let $C_0, C_1, \dots, C_t$ denote the rows of A_0. Since for any $0 \le j \le t-1$ we have

$$\binom{a-b+j+1}{i} - \binom{a-b+j}{i} = \begin{cases} 0, & \text{if } i = 0 \\ \binom{a-b+j}{i-1}, & \text{if } 1 \le i \le t, \end{cases}$$

we obtain for any $0 \le j \le t-1$ that

$$C_{j+1} - C_j = \left(0, \binom{a-b+j}{0}, \dots, \binom{a-b+j}{t-1}\right).$$

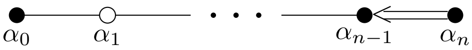
Hence if we regard $\det A_0$ as a multilinear function of the rows of A_0 we have

$$\begin{aligned} \det A_0 &= \det \left(C_0, C_1 - C_0, \dots, C_t - C_{t-1}\right) \\ &= \det \begin{pmatrix} \binom{a-b}{0} & \binom{a-b}{1} & \cdots & \binom{a-b}{t} \\ 0 & \binom{a-b}{0} & \cdots & \binom{a-b}{t-1} \\ \vdots & \vdots & & \vdots \\ 0 & \binom{a-b+t-1}{0} & \cdots & \binom{a-b+t-1}{t-1} \end{pmatrix} \\ &= \det \begin{pmatrix} \binom{a-b}{0} & \cdots & \binom{a-b}{t-1} \\ \vdots & & \vdots \\ \binom{a-b+t-1}{0} & \cdots & \binom{a-b+t-1}{t-1} \end{pmatrix} = 1, \end{aligned}$$

by the inductive hypothesis. This completes the proof of the lemma.

8. The case Sp(n,1)

In this section we shall prove Theorem 1.1 when G_o is locally isomorphic to $\mathrm{Sp}(n,1)$, with $n \geq 2$. The corresponding Dynkin-Satake diagram of $\mathfrak{g}$ is



It is well known that we can choose an orthonormal basis $\{\epsilon_i\}_{i=0}^n$ of $\mathfrak{h}_{\mathbb{R}}^*$ in such a way that $\alpha_i = \epsilon_i - \epsilon_{i+1}$ if $0 \leq i \leq n-1$, $\alpha_n = 2\epsilon_n$, $\epsilon_0^\sigma = \epsilon_1$, $\epsilon_1^\sigma = \epsilon_0$, and $\epsilon_i^\sigma = -\epsilon_i$ if $2 \leq i \leq n$. From the diagram we obtain that

$$\begin{aligned}\Delta^+(\mathfrak{g},\mathfrak{h}) &= \{\epsilon_i \pm \epsilon_j : 0 \leq i < j \leq n\} \cup \{2\epsilon_i : 0 \leq i \leq n\},\\ P_+ &= \{\epsilon_0 \pm \epsilon_j, \epsilon_1 \pm \epsilon_j : 2 \leq j \leq n\} \cup \{2\epsilon_0, 2\epsilon_1, \epsilon_0 + \epsilon_1\},\\ P_- &= \{\epsilon_i \pm \epsilon_j : 2 \leq i < j \leq n\} \cup \{2\epsilon_i : 2 \leq i \leq n\} \cup \{\epsilon_0 - \epsilon_1\},\end{aligned}$$

where P_- denotes the set of roots in $\Delta^+(\mathfrak{g},\mathfrak{h})$ that vanish on $\mathfrak{a}$. From this it is clear that $\mathfrak{m} \simeq \mathfrak{sp}(n-1,\mathbb{C}) \oplus \mathfrak{sp}(1,\mathbb{C})$.

In this case we have $\mathfrak{t} = \ker(\epsilon_0 + \epsilon_1)$ and $\mu = \epsilon_0 + \epsilon_1$ is the only root in P_+ that vanishes on $\mathfrak{t}$. Then $H_\mu = Z_\mu \in \mathfrak{a}$; we recall that H_μ was defined by $\phi(H_\mu) = 2\langle \phi, \mu\rangle / \langle \mu, \mu \rangle$ for all $\phi \in \mathfrak{h}^*$, where $\langle\, , \rangle$ denotes the bilinear form on $\mathfrak{h}^*$ induced by the Killing form $\langle\, , \rangle$ of $\mathfrak{g}$. We choose a root vector X_μ in such a way that $\langle X_\mu, \theta X_\mu \rangle = 1$ and define $X_{-\mu} = \theta X_\mu$. Then the ordered set $\{H_\mu, X_\mu, \theta X_\mu\}$ is an $\mathfrak{s}$-triple. This choice characterizes X_μ up to a sign. In order to fix this sign we observe that for any choice of nonzero vectors X_{α_1} and $X_{-\alpha_1}$ we have $[X_\mu, \theta X_{\alpha_1}] = tX_{\alpha_1}$ and $[X_\mu, X_{-\alpha_1}] = -t\theta X_{-\alpha_1}$ with $t^2 = 1$. Then we can choose X_μ in such a way that

$$[X_\mu, \theta X_{\alpha_1}] = -X_{\alpha_1} \quad \textit{and} \quad [X_\mu, X_{-\alpha_1}] = \theta X_{-\alpha_1}. \tag{60}$$

Now we consider the Cayley transform χ of $\mathfrak{g}$ defined by

$$\chi = Ad(\exp \tfrac{\pi}{4}(\theta X_\mu - X_\mu)). \tag{61}$$

It is easy to check that

$$Ad(\exp t(\theta X_\mu - X_\mu))H_\mu = \cos(2t)H_\mu + \sin(2t)(X_\mu + \theta X_\mu),$$

thus $\chi(H_\mu) = X_\mu + \theta X_\mu$. On the other hand, since $\mu_{|\mathfrak{t}} = 0$, χ fixes all elements of $\mathfrak{t}$. Therefore $\mathfrak{h}_{\mathfrak{k}} = \chi(\mathfrak{t} \oplus \mathfrak{a}) = \mathfrak{t} \oplus \mathbb{C}(X_\mu + \theta X_\mu) \subset \mathfrak{k}$ is a Cartan subalgebra of both $\mathfrak{g}$ and $\mathfrak{k}$.

Now for any $\phi \in \mathfrak{h}^*$ we define $\widetilde{\phi} \in \mathfrak{h}_{\mathfrak{k}}^*$ by $\widetilde{\phi} = \phi \cdot \chi^{-1}$. Then $\Delta(\mathfrak{g}, \mathfrak{h}_{\mathfrak{k}}) = \{\widetilde{\alpha} : \alpha \in \Delta(\mathfrak{g},\mathfrak{h})\}$ and $\mathfrak{g}_{\widetilde{\alpha}} = \chi(\mathfrak{g}_\alpha)$. Since $ad(\mathfrak{k})$ preserves the Cartan decomposition $\mathfrak{g} = \mathfrak{k} \oplus \mathfrak{p}$, the root spaces are contained either in $\mathfrak{k}$ or in $\mathfrak{p}$. A root $\widetilde{\alpha} \in \Delta(\mathfrak{g}, \mathfrak{h}_{\mathfrak{k}})$ is said to be compact (respectively noncompact) if $\mathfrak{g}_{\widetilde{\alpha}} \subset \mathfrak{k}$ (respectively $\mathfrak{g}_{\widetilde{\alpha}} \subset \mathfrak{p}$). Let $\Delta(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}})$ and $\Delta(\mathfrak{p}, \mathfrak{h}_{\mathfrak{k}})$ denote, respectively, the sets of compact and noncompact roots. With the aim of determining these sets we establish the following lemma.

Lemma 8.1. *The following hold:*
(i) $\theta \cdot \chi = \chi^{-1} \cdot \theta$,

(ii) $\widetilde{\alpha} \in \Delta(\mathfrak{g}, \mathfrak{h}_{\mathfrak{k}})$ *is compact (respectively noncompact) if and only if* $\theta(X_\alpha) = \chi^2(X_\alpha)$ *(respectively* $\theta(X_\alpha) = -\chi^2(X_\alpha)$*),*
(iii) $\widetilde{\mu}$ *is noncompact,*
(iv) If $\alpha \in \Delta(\mathfrak{g}, \mathfrak{h})$ *is strongly orthogonal to* μ *then* $\chi(X_\alpha) = X_\alpha$*.*

Proof. (i), (ii) and (iv) follow directly from the definitions. To prove (iii) we easily compute, taking into account that $\{H_\mu, X_\mu, \theta X_\mu\}$ is an $\mathfrak{s}$-triple, that

$$Ad\,(\exp t(\theta X_\mu - X_\mu))\, X_\mu = X_\mu - \frac{\sin(2t)}{2} H_\mu + \frac{\cos(2t)-1}{2}(X_\mu + \theta X_\mu).$$

Hence if $t = \frac{\pi}{2}$ we obtain $\chi^2(X_\mu) = -\theta(X_\mu)$ and the result follows.

Now since the roots α_i for $2 \le i \le n$ are roots of $\mathfrak{m}$ and they are strongly orthogonal to μ, Lemma 8.1 implies that $\widetilde{\alpha_i}$ for $2 \le i \le n$ are compact roots. Also since $\theta(X_{\alpha_0}) = X_{\alpha_0}$ and $\chi^2(X_{\alpha_0}) = -X_{\alpha_0}$ we get that $\widetilde{\alpha_0}$ is a noncompact root. Finally, since X_μ was chosen in such a way that (60) holds, we obtain that $\chi^2(X_{\alpha_1}) = -\theta(X_{\alpha_1})$ proving that $\widetilde{\alpha_1}$ is a noncompact root. From this it follows that

$$\begin{aligned}\Delta(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}}) &= \{\pm(\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j}) : 0 \le i < j \le n; i, j \ne 1\} \cup \{\pm 2\widetilde{\epsilon_i} : 0 \le i \le n\},\\ \Delta(\mathfrak{p}, \mathfrak{h}_{\mathfrak{k}}) &= \{\pm(\widetilde{\epsilon_0} \pm \widetilde{\epsilon_1}), \pm(\widetilde{\epsilon_1} \pm \widetilde{\epsilon_i}) : 2 \le i \le n\}.\end{aligned}$$

Our next task is to construct a particular Borel subalgebra $b_{\mathfrak{k}} = \mathfrak{h}_{\mathfrak{k}} \oplus \mathfrak{k}^+$ of $\mathfrak{k}$ that will be very useful later on to describe the set Γ of all equivalence classes of irreducible finite dimensional holomorphic K-modules V_γ such that $V_\gamma^M \ne 0$, as well as some of the properties of each $\gamma \in \Gamma$ (see Proposition 8.7). For more details on the construction of the subalgebra $b_{\mathfrak{k}}$ and its relation with Γ we refer the reader to [4].

Observe that $\alpha_1 = \epsilon_1 - \epsilon_2$ is the only simple root in P_+. As in the previous sections we consider the vector $E_{\alpha_1} = X_{-\alpha_1} + \theta X_{-\alpha_1}$ and set $E = E_{\alpha_1}$. Let $H_+ \in \mathfrak{t}_{\mathbb{R}}$ be such that $\alpha(H_+) > 0$ for all $\alpha \in \Delta^+(\mathfrak{m}, \mathfrak{t})$. We shall say that H_+ is a $\mathfrak{k}$-regular vector if in addition $\alpha(H_+) \ne 0$ for all α with $\widetilde{\alpha} \in \Delta(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}})$. Since μ is the only root in $\Delta^+(\mathfrak{g}, \mathfrak{h})$ that vanishes on $\mathfrak{t}$ and since $\widetilde{\mu}$ is a noncompact root, it follows that $\mathfrak{k}$-regular vectors exist. Given a $\mathfrak{k}$-regular vector H_+ we consider the positive system

$$\Delta^+(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}}) = \{\widetilde{\alpha} \in \Delta(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}}) : \alpha(H_+) > 0\}.$$

Now if $\lambda_0 = \alpha_1|_{\mathfrak{a}}$ is the simple restricted root and H_+ is a $\mathfrak{k}$-regular vector we consider the following set

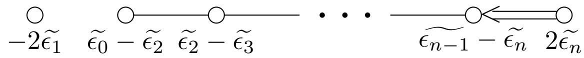
$$P_+(\lambda_0)^- = \{\alpha \in P_+ : \alpha|_{\mathfrak{a}} = \lambda_0 \text{ and } \alpha(H_+) < 0\}.$$

Definition 8.2. A positive system $\Delta^+(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}})$ defined by a $\mathfrak{k}$-regular vector H_+ is said to be compatible with E if $\alpha - \alpha_1$ is a root for every $\alpha \in P_+(\lambda_0)^-$ such that $\alpha \ne \alpha_1$.

If $\mathfrak{g}_o \simeq \mathfrak{sp}(n, 1)$ with $n \ge 2$ the $\mathfrak{k}$-regular vectors are all of the form $H_+ = (t_0, -t_0, t_2, \dots, t_n)$ with $t_0 > 0$, $t_2 > t_3 > \dots > t_n > 0$ and $t_0 \ne t_j$ for every $j \ge 2$. Different vectors H_+ define different positive systems and they depend only on how many $j \geq 2$ satisfy $t_j > t_0$. If either $t_0 > t_2$ or $t_2 > t_0 > t_3$ the positive systems obtained are both compatible with E, however the positive systems obtained when $t_3 > t_0$ are not compatible with E. From now on we fix a $\mathfrak{k}$-regular vector $H_+ = (t_0, -t_0, t_2, \dots, t_n)$ with $t_0 > t_2 > t_3 > \cdots > t_n > 0$. Then the corresponding positive system is

$$\Delta^+(\mathfrak{k}, \mathfrak{h}_\mathfrak{k}) = \{\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j} : 0 \leq i < j \leq n; i, j \neq 1\} \cup \{-2\widetilde{\epsilon_1}, 2\widetilde{\epsilon_i} : 0 \leq i \leq n, i \neq 1\}.$$

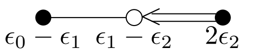
Let $b_\mathfrak{k} = \mathfrak{h}_\mathfrak{k} \oplus \mathfrak{k}^+$ be the associated Borel subalgebra. The Dynkin diagram corresponding to this positive system is

(62) 

therefore $\mathfrak{k} \simeq \mathfrak{sp}(1, \mathbb{C}) \oplus \mathfrak{sp}(n, \mathbb{C})$. Moreover by direct inspection of $\Delta(\mathfrak{p}, \mathfrak{h}_\mathfrak{k})$ it follows that $\mathfrak{p}$ is an irreducible $\mathfrak{k}$-module with highest weight $\widetilde{\epsilon_0} - \widetilde{\epsilon_1}$.

Our next goal is to define an appropriate Lie subalgebra $\widetilde{\mathfrak{g}}$ of $\mathfrak{g}$ in such a way that it be both σ and θ stable and that its real form $\widetilde{\mathfrak{g}_o} = \mathfrak{g}_o \cap \widetilde{\mathfrak{g}}$ be isomorphic to $\mathfrak{sp}(2, 1)$. This subalgebra will be very useful in this section since most of the calculations will depend on it.

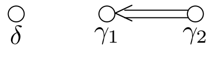
Observe that α_1 is the only simple root in P_+ and that $\nu = 2\epsilon_0$ is the maximal root in $\Delta^+(\mathfrak{g}, \mathfrak{h})$. Let $\widetilde{\mathfrak{g}}$ be the complex Lie subalgebra of $\mathfrak{g}$ generated by the nonzero root vectors $X_{\pm\alpha_0} = X_{\pm(\epsilon_0 - \epsilon_1)}$, $X_{\pm\alpha_1} = X_{\pm(\epsilon_1 - \epsilon_2)}$ and $X_{\pm(\nu^\theta + 2\alpha_1)} = X_{\pm 2\epsilon_2}$. Then $\widetilde{\mathfrak{g}}$ is a simple Lie algebra stable under σ and θ. Therefore $\widetilde{\mathfrak{g}}$ is the complexification of the real subalgebra $\widetilde{\mathfrak{g}_o} = \mathfrak{g}_o \cap \widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{g}} = \widetilde{\mathfrak{k}} \oplus \widetilde{\mathfrak{p}}$ is a Cartan decomposition of $\widetilde{\mathfrak{g}}$, where $\widetilde{\mathfrak{k}} = \mathfrak{k} \cap \widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{p}} = \mathfrak{p} \cap \widetilde{\mathfrak{g}}$. Moreover $\widetilde{\mathfrak{h}} = (\mathfrak{t} \cap \widetilde{\mathfrak{g}}) \oplus \mathfrak{a}$ is a Cartan subalgebra of $\widetilde{\mathfrak{g}}$ and $\widetilde{\mathfrak{m}} = \mathfrak{m} \cap \widetilde{\mathfrak{k}}$ is the centralizer of $\mathfrak{a}$ in $\widetilde{\mathfrak{k}}$. The Dynkin-Satake diagram of $\widetilde{\mathfrak{g}_o}$ is



Thus $\widetilde{\mathfrak{g}_o} \simeq \mathfrak{sp}(2, 1)$.

Since $\mu \in \Delta(\widetilde{\mathfrak{g}}, \widetilde{\mathfrak{h}})$ the root vectors X_μ and θX_μ are in $\widetilde{\mathfrak{g}}$, hence $\widetilde{\mathfrak{g}}$ is stable under the Cayley transform χ of $(\mathfrak{g}, \mathfrak{h})$. Moreover the restriction of χ to $\widetilde{\mathfrak{g}}$ is the Cayley transform associated to $(\widetilde{\mathfrak{g}}, \widetilde{\mathfrak{h}})$. Let $\mathfrak{h}_{\widetilde{\mathfrak{k}}} = \chi(\widetilde{\mathfrak{h}}) = \mathfrak{h}_\mathfrak{k} \cap \widetilde{\mathfrak{k}}$, then $\mathfrak{h}_{\widetilde{\mathfrak{k}}}$ is a Cartan subalgebra of $\widetilde{\mathfrak{k}}$ and $\widetilde{\mathfrak{g}}$.

Let us recall that we have already chosen a positive system $\Delta^+(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})$ in the set of compact roots $\Delta(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})$. This determines a positive system $\Delta^+(\widetilde{\mathfrak{k}}, \mathfrak{h}_{\widetilde{\mathfrak{k}}}) = \{\widetilde{\alpha}_{|\mathfrak{h}_{\widetilde{\mathfrak{k}}}} \in \Delta(\widetilde{\mathfrak{k}}, \mathfrak{h}_{\widetilde{\mathfrak{k}}}) : \widetilde{\alpha} \in \Delta^+(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})\}$. Now if we set $\gamma_1 = \widetilde{\nu} + \widetilde{\alpha_1^\theta} = \widetilde{\epsilon_0} - \widetilde{\epsilon_2}$, $\gamma_2 = -\widetilde{\nu^\theta} - 2\widetilde{\alpha_1} = 2\widetilde{\epsilon_2}$ and $\delta = \widetilde{\nu^\theta} = -2\widetilde{\epsilon_1}$ it follows that $\{\gamma_1, \gamma_2, \delta\}$ is a simple system of roots in $\Delta^+(\widetilde{\mathfrak{k}}, \mathfrak{h}_{\widetilde{\mathfrak{k}}})$ and the Dynkin diagram is



Thus $\widetilde{\mathfrak{k}} \simeq \mathfrak{sp}(1,\mathbb{C}) \times \mathfrak{sp}(2,\mathbb{C})$. Notice that $\Delta^+(\widetilde{\mathfrak{k}}, \mathfrak{h}_{\widetilde{\mathfrak{k}}}) = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4, \delta\}$ where $\gamma_3 = \gamma_1 + \gamma_2 = -\widetilde{\alpha_1^\theta} = \widetilde{\epsilon_0} + \widetilde{\epsilon_2}$ and $\gamma_4 = 2\gamma_1 + \gamma_2 = \widetilde{\nu} = 2\widetilde{\epsilon_0}$. These roots and their corresponding root vectors, suitably normalized, will play a crucial role in what follows.

A simple calculation shows that $\chi(\theta X_{-\alpha_1}) = \frac{\sqrt{2}}{2}E$, thus E is a root vector in $\widetilde{\mathfrak{k}}^+$ corresponding to the root γ_3. Then we set $X_{\gamma_3} = E$. Now fix a nonzero root vector X_{α_0} and set $X_\nu = [X_\mu, X_{\alpha_0}]$ where $\nu = 2\epsilon_0$ is the maximal root in $\Delta(\mathfrak{g}, \mathfrak{h})$. Using that $[X_{-\mu}, X_\nu] = 2X_{\alpha_0} \in \mathfrak{m}^+ \cap \widetilde{\mathfrak{k}} = \widetilde{\mathfrak{m}}^+$ it is easy to show that $[X_\mu, [X_\mu, \theta X_\nu]] = 2X_\nu$. From this it follows that $\chi(X_\nu) = \frac{1}{2}(2X_{\alpha_0} + X_\nu + \theta X_\nu)$ and $\chi(\theta X_\nu) = \frac{1}{2}(-2X_{\alpha_0} + X_\nu + \theta X_\nu)$. Hence we can define X_{γ_4} and X_δ in such a way that $X_{\gamma_4} - X_\delta \in \widetilde{\mathfrak{m}}^+$. Observe that this fact determines the pair $\{X_{\gamma_4}, X_\delta\}$ up to a constant. Moreover it is easy to see that $\widetilde{\mathfrak{m}}^+$ is generated by $\{X_{\gamma_2}, X_{\gamma_4} - X_\delta\}$. For any such a pair $\{X_{\gamma_4}, X_\delta\}$ we choose $H_4 \in [\mathfrak{k}_{\gamma_4}, \mathfrak{k}_{-\gamma_4}]$ and $H_\delta \in [\mathfrak{k}_\delta, \mathfrak{k}_{-\delta}]$ in such a way that $\gamma_4(H_4) = 2$ and $\delta(H_\delta) = 2$, and normalize $X_{-\gamma_4}$ and $X_{-\delta}$ so that $\{H_4, X_{\gamma_4}, X_{-\gamma_4}\}$ and $\{H_\delta, X_\delta, X_{-\delta}\}$ become $\mathfrak{s}$-triples. Then, since $\gamma_4(H_\delta) = \delta(H_{\gamma_4}) = 0$, it follows that $\{H_4 + H_\delta, X_{\gamma_4} - X_\delta, X_{-\gamma_4} - X_{-\delta}\}$ is an $\mathfrak{s}$-triple.

In order to simplify the notation from now on we shall set $X_{\pm 1} = X_{\pm\gamma_1}$, $X_{\pm 2} = X_{\pm\gamma_2}$, $X_{\pm 3} = X_{\pm\gamma_3}$, $X_{\pm 4} = X_{\pm\gamma_4}$ and $X = X_\delta$. Let $H_1 \in [\mathfrak{k}_{\gamma_1}, \mathfrak{k}_{-\gamma_1}]$ be such that $\gamma_1(H_1) = 2$. Then we can normalize X_1 and X_{-1} in such a way that $\{H_1, X_1, X_{-1}\}$ becomes an $\mathfrak{s}$-triple. Next we normalize X_2 and X_4, and accordingly X_δ (so that $X_4 - X_\delta \in \widetilde{\mathfrak{m}}^+$), in such a way that

$$[X_1, X_2] = E \quad \textit{and} \quad [X_1, E] = X_4. \tag{63}$$

From this, and the fact that $\gamma_2(H_1) = -2$, it follows that

$$[X_{-1}, E] = 2X_2 \quad \textit{and} \quad [X_{-1}, X_4] = 2E. \tag{64}$$

Now choose $H_2 \in [\mathfrak{k}_{\gamma_2}, \mathfrak{k}_{-\gamma_2}]$ such that $\gamma_2(H_2) = 2$ and normalize X_{-2} so that $\{H_2, X_2, X_{-2}\}$ becomes an $\mathfrak{s}$-triple. Observe that $[\mathfrak{k}_{\gamma_2}, \mathfrak{k}_{-\gamma_2}] \subset \mathfrak{t}$ because $2\epsilon_2$ is a root of $\mathfrak{m}$ strongly orthogonal to μ. Then, since $\gamma_1(H_2) = -1$, if we define $H = \frac{1}{2}H_2$ we obtain a vector $H \in \mathfrak{t}$ such that $\dot{H}(E) = \frac{1}{2}E$. This vector H is the one introduced abstractly in the change of variables (22). Also, since $\delta(H_2) = 0$, we have $[X, H] = 0$.

As in the previous sections we set $Z = Z_{\alpha_1}$, $Y = Y_{\alpha_1}$ and $\widetilde{Y} = Y + H$. From Lemma 5.1 it follows that $\dot{E}(Y) = \frac{3}{2}E$ hence $\dot{E}(\widetilde{Y}) = E$, this is the main reason for using $\widetilde{Y}$ instead of Y itself (see Section 5). Now observe that $[Y, X] = \nu(Y)X$. On the other hand, since $\nu(H_{\alpha_1}) = 0$, we have $\nu(Y) = -\nu(Z) = -1$ because $\nu|_{\mathfrak{a}} = 2\alpha_1|_{\mathfrak{a}}$ and $\alpha_1(Z) = \frac{1}{2}$ (see Lemma 5.1). Therefore $\dot{X}(Y) = X$ from where it follows that $\dot{X}(\widetilde{Y}) = X$.

Let us recall now the definition of the subalgebra B of $U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ introduced in Section 3.6 (Definition 3.6). In this section the algebra B (see (21)) is the set of all $b \in U(\mathfrak{k})^M \otimes U(\mathfrak{a})$ that satisfy

$$E^n b(n - Y - 1) \equiv b(-n - Y - 1)E^n \qquad \mod (U(\mathfrak{k})\mathfrak{m}^+), \tag{65}$$

for all $n \in \mathbb{N}$. As before we identify $U(\mathfrak{k}) \otimes U(\mathfrak{a})$ with the polynomial ring in one variable $U(\mathfrak{k})[x]$ by changing $Z \in \mathfrak{a}$ by the indeterminate x. Also as in (22), to any $b(x) \in U(\mathfrak{k})[x]$ we associate $c(x) \in U(\mathfrak{k})[x]$ defined by $c(x) = b(x + H - 1)$ where H is as above. Then $b(x) \in U(\mathfrak{k})[x]$ satisfies (65) if and only if $c(x) \in U(\mathfrak{k})[x]$ satisfies

$$E^n c(n - \widetilde{Y}) \equiv c(-n - \widetilde{Y}) E^n \qquad \mod (U(\mathfrak{k})\mathfrak{m}^+), \tag{66}$$

for all $n \in \mathbb{N}$. On the other hand, in view of Theorem 5.3 $c(x)$ satisfies (66) if and only if it satisfies equations (iii) of Theorem 5.3 for all $n, \ell \in \mathbb{N}_o$.

If $b(x) \in U(\mathfrak{k})[x]$ and $b(x) \neq 0$ we shall find it convenient to write, in a unique way, $b = \sum_{j=0}^m b_j x^j$ with $b_j \in U(\mathfrak{k})$, $b_m \neq 0$, and $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$. Here $\{\varphi_n\}_{n \geq 0}$ is the basis of $\mathbb{C}[x]$ defined at the beginning of Section 6. The following lemma is the analogue of Lemma 7.1 and its proof is exactly the same.

Lemma 8.3. *Let $b = \sum_{j=0}^m b_j x^j \in U(\mathfrak{k})[x]$ and set $c(x) = b(x + H - 1)$. Then, if $c = \sum_{j=0}^m c_j \varphi_j$ with $c_j \in U(\mathfrak{k})$ we have*

$$c_i = \sum_{j=i}^{m} b_j t_{ij} \qquad 0 \leq i \leq m, \tag{67}$$

where

$$t_{ij} = \sum_{k=0}^{i} (-1)^k \binom{i}{k} (H + \tfrac{i}{2} - 1 - k)^j. \tag{68}$$

Thus t_{ij} is a polynomial in H of degree $j - i$, in particular $t_{ii} = i!$.

Also observe that Lemma 7.2 hold for the case at hand (i.e. Sp(n,1)) exactly as it is stated in the previous section. From this result and Theorem 5.3 we obtain the following theorem whose proof is the same as that of Theorem 7.3 except for the step where the congruence modulo $U(\mathfrak{k})\mathfrak{m}^+$ is replaced by an equality.

Theorem 8.4. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{m+1}(c_j) \equiv 0$ for all $0 \leq j \leq m$.*

From this theorem we obtain the following result whose proof is exactly the same as that of Corollary 7.4 except that all the equalities have to be replaced by congruence modulo the left ideal $U(\mathfrak{k})\mathfrak{m}^+$.

Corollary 8.5. *If $b = b_m \otimes Z^m + \cdots + b_0 \in B$, then $\dot{E}^{2m+1-j}(b_j) \equiv 0$ for all $0 \leq j \leq m$.*

For later reference we shall now rewrite equation (iii) of Theorem 5.3. First observe that given $b = \sum_{j=0}^m b_j x^j \in B$ and $c(x) = b(x+H-1)$ it follows from Theorem 8.4 that equation (iii) of Theorem 5.3 is satisfied if $\ell > m$ or $n > m$. Moreover such equation is trivial when $\ell = n$. Also note that the equation corresponding to (n, ℓ) is equivalent to that one corresponding to (ℓ, n).

Theorem 8.6. *Let* $b = \sum_{j=0}^{m} b_j x^j \in U(\mathfrak{k})[x]$ *and* $c(x) = b(x + H - 1)$. *If* $c = \sum_{j=0}^{m} c_j \varphi_j$ *with* $c_j \in U(\mathfrak{k})$ *and* $0 \le \ell, n$ *we set*

$$\begin{aligned}\epsilon(\ell, n) = (-1)^n &\sum_{n \le i \le m} \dot{E}^\ell(c_i)\varphi_{i-n}(-\tfrac{n}{2} + \ell - \widetilde{Y})E^n \\ - (-1)^\ell &\sum_{\ell \le i \le m} \dot{E}^n(c_i)\varphi_{i-\ell}(-\tfrac{\ell}{2} + n - \widetilde{Y})E^\ell.\end{aligned}$$

Then, if $b \in B$ *we have* $\epsilon(\ell, n) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ *for all* $0 \le \ell, n$.

Proof. The assertion follows from equation (iii) of Theorem 5.3 and the fact that $c^{(k)} = \sum_{i=k}^{m} c_i \varphi_{i-k}$ for all $0 \le k \le m$.

As we proved in Theorem 4.6, in order to establish our main result (Theorem 1.1) we need to show that Theorem 4.5 holds, that is, if $b = b_m \otimes Z^m + \cdots + b_0 \in B$ we have to prove that $d(b_m) \le m$ and that its leading term $\widetilde{b} = b_m \otimes Z^m$ is invariant under the Weyl group W of (G_o, K_o). Since in the case under consideration $\operatorname{rank}(G_o) = \operatorname{rank}(K_o)$, to prove the second assertion it is enough to show that m is even. In the rest of this paper we shall show how to obtain these results from the equations $\epsilon(\ell, n) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$, $0 \le \ell, n$, of Theorem 8.6.

We begin by collecting in the following proposition several results that we shall need about the representations in Γ or Γ_1 (see (43)).

Proposition 8.7. *Let* G_o *be locally isomorphic to* $Sp(n, 1)$ *with* $n \ge 2$ *and let* $\mathfrak{b}_\mathfrak{k} = \mathfrak{h}_\mathfrak{k} \oplus \mathfrak{k}^+$ *be the Borel subalgebra of* $\mathfrak{k}$ *defined at the beginning of this section. Then* $\mathfrak{m}^+ \subset \mathfrak{k}^+$ *and* E *is a root vector in* $\mathfrak{k}^+$. *Moreover:*
(i) For any $\gamma \in \hat{K}$ *let* ξ_γ *denote its highest weight. Then,* $\gamma \in \Gamma$ *if and only if* $\xi_\gamma = \frac{k}{2}(\gamma_4 + \delta) + \ell\gamma_3$ *with* $k, \ell \in \mathbb{N}_o$. *In this context we write* $\gamma = \gamma_{k,\ell}$, $\xi_\gamma = \xi_{k,\ell}$ *and* $V_{k,\ell}$ *for the corresponding representation space. Also we shall refer to any* $v \in V_{k,\ell}^M$ *as an* M*-invariant element of type* (k, ℓ).
(ii) For any $\gamma_{k,\ell} \in \Gamma$ *we have* $d(\gamma_{k,\ell}) = k + 2\ell$.
(iii) If $\gamma \in \Gamma$ *we have* $\gamma \in \Gamma_1$ *if and only if* $\xi_\gamma = \xi_{k,\ell}$ *with* k *even.*
(iv) For any $\gamma_{k,\ell} \in \Gamma$ *we have* $X^k E^\ell(V_{k,\ell}^M) = V_{k,\ell}^{\mathfrak{k}^+}$ *and* $X^p E^q(V_{k,\ell}^M) = \{0\}$ *if and only if* $p > k$ *or* $p + q > k + \ell$.

For a proof of this proposition we refer the reader to [4]. In fact, the construction of the Borel subalgebra $\mathfrak{b}_\mathfrak{k}$ is contained in Section 3 of [4] and the statements in (i), (ii) and (iv) follow from Proposition 4.4, Theorem 4.5 and Theorem 5.3 of [4]. On the other hand (iii) is a consequence of well known general facts.

Lemma 8.8. *If* u *is a dominant vector in the irreducible finite dimensional* $\{H_1, X_1, X_{-1}\}$*-module* V_n *of dimension* $n + 1$, *then for all* $0 \le i \le j \le n$ *we have*

$$X_1^{j-i} X_{-1}^j(u) = \frac{j!(n-i)!}{i!(n-j)!} X_{-1}^i(u). \tag{69}$$

Proposition 8.9. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$. Let $\gamma_{k,\ell} \in \Gamma$ and let $V_{k,\ell}$ be a K-module in the class $\gamma_{k,\ell}$. If $0 \neq v \in V_{k,\ell}^M$ then:*
(i) $v = \sum_{i=0}^{k} v_i$, with v_i a non trivial vector of weight $\frac{1}{2}(k-2i)(\gamma_4 - \delta)$ with respect to $\mathfrak{h}_{\mathfrak{k}}$. Moreover

$$v_i = (i!)^2 (k!)^{-2} \binom{k}{i} X_4^{k-i} X_{-\delta}^{k-i}(v_k), \tag{70}$$

for $0 \leq i \leq k$.
(ii) The set $\{X^{k-j}E^{\ell+j}(v) : 0 \leq j \leq k\}$ is a basis of the $\{H_1, X_1, X_{-1}\}$ irreducible module of dimension $k+1$ generated by any non trivial highest weight vector of $V_{k,\ell}$. Moreover the vector $X^{k-j}E^{\ell+j}(v)$ has weight $\xi_{k,\ell} - j\gamma_1$ and we have:

$$X_1 X^{k-j} E^{\ell+j}(v) = \frac{(j+\ell)}{2} X^{k-j+1} E^{\ell+j-1}(v) \qquad 0 \leq j \leq k, \tag{71}$$

$$X_{-1} X^{k-j} E^{\ell+j}(v) = \frac{2(j+1)(k-j)}{\ell+j+1} X^{k-j-1} E^{\ell+j+1}(v) \qquad 0 \leq j \leq k, \tag{72}$$

and

$$X_{-1}^{j}(u_{k,\ell}) = 2^j j! \binom{k}{j} \binom{\ell+j}{\ell}^{-1} X^{k-j} E^{\ell+j}(v) \qquad 0 \leq j \leq k, \tag{73}$$

where $u_{k,\ell}$ is the highest weight vector $X^k E^\ell(v)$.

Proof. First of all from Proposition 8.7 (i) it follows that given representations $\gamma_{r,s}$ and $\gamma_{r',s'}$ in Γ we can realize the representation $\gamma_{r+r',s+s'}$ as the Cartan product of $\gamma_{r,s}$ and $\gamma_{r',s'}$. Let $V_{r,s}$ and $V_{r',s'}$ be K-modules in the classes $\gamma_{r,s}$ and $\gamma_{r',s'}$, respectively. If we choose $0 \neq w \in V_{r,s}^M$ and $0 \neq w' \in V_{r',s'}^M$ then $w \otimes w' \in (V_{r,s} \otimes V_{r',s'})^M$ and

$$w \otimes w' = w'' + \cdots, \qquad w'' \in V_{r+r',s+s'}^M,$$

the dots stand for M-invariant elements of type (i,j) with either $i < r+r'$ or $i+j < r+r'+s+s'$. The only thing we have to prove is that $w'' \neq 0$, and this follows, in view of Proposition 8.7 (iv), from

$$\begin{aligned} X^{r+r'}E^{s+s'}(w'') &= X^{r+r'}E^{s+s'}(w \otimes w') \\ &= \binom{r+r'}{r}\binom{s+s'}{s} X^r E^s(w) \otimes X^{r'} E^{s'}(w') \neq 0. \end{aligned}$$

(i) By direct inspection of $\Delta(\mathfrak{p}, \mathfrak{h}_{\mathfrak{k}})$ it follows that $\mathfrak{p}$ is an irreducible K-module with highest weight $\xi_{1,0} = \frac{1}{2}(\gamma_4 + \delta) = \widetilde{\epsilon}_0 - \widetilde{\epsilon}_1$. On the other hand $\mathfrak{p}^M = \mathbb{C}H_\mu$, and a simple calculation shows that $H_\mu = -X_{\widetilde{\mu}} - X_{-\widetilde{\mu}}$ where $X_{\widetilde{\mu}} = \chi(X_\mu)$ and $X_{-\widetilde{\mu}} = \chi(\theta X_\mu)$. Therefore the $\mathfrak{h}_{\mathfrak{k}}$-weights of any M-invariant element of type $(1,0)$ are $\pm\widetilde{\mu} = \pm\frac{1}{2}(\gamma_4 - \delta)$.

We consider now the representation class $\gamma_{0,1}$ with highest weight $\xi_{0,1} = \gamma_3$ and let $0 \neq v \in V_{0,1}^M$. Then v is a vector of weight zero because the only

$\mathfrak{h}_{\mathfrak{k}}$-weights that vanish on $\mathfrak{t}$ are multiples of $\widetilde{\mu}$ and $\xi_{0,1} - c\widetilde{\mu}$ can not be written as a sum of positive roots for any value of $c \neq 0$.

Since any representation in the class $\gamma_{k,\ell} \in \Gamma$ can be realized as the Cartan product of representations in the classes $\gamma_{k,0}$ and $\gamma_{0,\ell}$, it follows that the weights of any $0 \neq v \in V_{k,\ell}^M$ are contained in $\{\frac{1}{2}(k-2i)(\gamma_4-\delta) : i = 0, \dots, k\}$.

Our next goal is to show that all these weights do occur in v. Write $v = \sum_{i=0}^{k} v_i$ where v_i is a vector of weight $\frac{1}{2}(k-2i)(\gamma_4-\delta)$. Then, since the root vectors X_4, $X = X_\delta$ and E commute with each other and $X - X_4 \in \mathfrak{m}$, for every $0 \leq j \leq k$ we have

$$0 \neq X^k E^\ell(v) = X_4^j X^{k-j} E^\ell(v) = \sum_{i=0}^{k} X_4^j X^{k-j} E^\ell(v_i). \tag{74}$$

In particular, in view of Proposition 8.7 (iv), $X_4^j X^{k-j} E^\ell(v)$ is a $\mathfrak{k}^+$-dominant vector of weight $\xi_{k,\ell} = \frac{k}{2}(\gamma_4 + \delta) + \ell\gamma_3$ for every $0 \leq j \leq k$. Now, since the vector $X_4^j X^{k-j} E^\ell(v_i)$ in (74) has weight $\xi_{k,\ell} + (i-j)(\delta - \gamma_4)$, we conclude that $v_i \neq 0$ for every $0 \leq i \leq k$.

We shall now prove the second assertion of (i). Let $0 \neq v \in V_{k,\ell}^M$ and write $v = \sum_{i=0}^{k} v_i$ where v_i is a non trivial vector of weight $\frac{1}{2}(k-2i)(\gamma_4 - \delta)$. We note that

$$\mathfrak{m}^+ = \langle \{X_{\widetilde{\epsilon}_i \pm \widetilde{\epsilon}_j} : 2 \leq i < j \leq n\} \cup \{X_{2\widetilde{\epsilon}_i} : 2 \leq i \leq n\} \cup \{X_4 - X_\delta\} \rangle, \tag{75}$$

where $\langle X \rangle$ denotes the linear space spanned by the set X. For any root ϕ in $\Phi = \{\widetilde{\epsilon}_i \pm \widetilde{\epsilon}_j : 2 \leq i < j \leq n\} \cup \{2\widetilde{\epsilon}_i : 2 \leq i \leq n\}$ choose X_ϕ, $X_{-\phi}$ and H_ϕ in such a way that $\{H_\phi, X_\phi, X_{-\phi}\}$ is an $\mathfrak{s}$-triple. Also recall that $\{H_4 + H_\delta, X_4 - X_\delta, X_{-4} - X_{-\delta}\}$ is an $\mathfrak{s}$-triple. Then we have

$$\mathfrak{m} = \bigoplus_{\phi \in \Phi} \langle \{H_\phi, X_\phi, X_{-\phi}\} \rangle \oplus \langle \{H_4 + H_\delta, X_4 - X_\delta, X_{-4} - X_{-\delta}\} \rangle. \tag{76}$$

Since v is M-invariant we have $X_4(v) = X_\delta(v)$, hence comparing weights in this equality we obtain that

$$X_4(v_i) = X_\delta(v_{i-1}) \tag{77}$$

for $1 \leq i \leq k$, and

$$X_4(v_0) = X_\delta(v_k) = 0. \tag{78}$$

For further reference we observe that (77) and (78) imply that

$$X_4^{k+1}(v_k) = X_\delta^k X_4(v_0) = 0. \tag{79}$$

Also, since $\{H_\delta, X_\delta, X_{-\delta}\}$ is an $\mathfrak{s}$-triple, it follows that

$$X_\delta X_{-\delta}^j = j X_{-\delta}^{j-1}(H_\delta - j + 1) + X_{-\delta}^j X_\delta \tag{80}$$

for every $j \geq 1$.

Now consider the element $\widetilde{v} \in V_{k,\ell}$ defined as follows,

$$\widetilde{v} = \sum_{i=0}^{k} c_i X_4^{k-i} X_{-\delta}^{k-i}(v_k)$$

where $c_i = (i!)^2(k!)^{-2}\binom{k}{i}$ for $0 \leq i \leq k$. Our next objective is to show that $\widetilde{v} \in V_{k,\ell}^M$. Let $\phi \in \Phi$, since $X_{\pm\phi}(v) = 0$, it follows that $X_{\pm\phi}(v_k) = 0$. Then, since $X_{\pm\phi}$ commute with X_4 and $X_{-\delta}$, we obtain that $X_{\pm\phi}(\widetilde{v}) = 0$. Hence $\widetilde{v}$ is annihilated by the $\mathfrak{s}$-triple $\{H_\phi, X_\phi, X_{-\phi}\}$.

Now using (78), (79), (80), and the fact that $\gamma_4(H_\delta) = \delta(H_4) = 0$ it follows that

$$(X_4 - X_\delta)(\widetilde{v}) = \sum_{i=0}^{k-1}(c_{i+1} - (k-i)(i+1)c_i) X_4^{k-i} X_{-\delta}^{k-i}(v_k) = 0,$$

because $c_{i+1} = (k-i)(i+1)c_i$ for every $0 \leq i \leq k-1$. On the other hand, since $X_4^{k-i} X_{-\delta}^{k-i}(v_k)$ is a vector of weight $\frac{1}{2}(k-2i)(\gamma_4 - \delta)$ for $0 \leq i \leq k$ and $(\gamma_4 - \delta)(H_4 + H_\delta) = 0$, it follows that $(H_4 + H_\delta)(\widetilde{v}) = 0$. Hence $\widetilde{v}$ is annihilated by $\{X_4 - X_\delta, H_4 + H_\delta, X_{-4} - X_{-\delta}\}$. Therefore it follows from (76) that $\widetilde{v} \in V_{k,\ell}^M$. Then, since $\dim(V_{k,\ell}^M) = 1$, we have $\widetilde{v} = cv$ where $c \in \mathbb{C}$. Now, since the components of weight $-\frac{k}{2}(\gamma_4 - \delta)$ in $\widetilde{v}$ and v are the same, we conclude that $c = 1$ and therefore $v_i = c_i X_4^{k-i} X_{-\delta}^{k-i}(v_k)$ for $0 \leq i \leq k$, as we wanted to prove.

(ii) We begin by proving (71) and the statement about the weights of the vectors $X^{k-j}E^{\ell+j}(v)$ where $0 \leq j \leq k$. Our approach will consist in establishing first these results for the K-modules in the classes $\gamma_{k,0}$ and $\gamma_{0,\ell}$ of Γ, and then extending them to every class $\gamma_{k,\ell}$ by realizing a K-module in $\gamma_{k,\ell}$ as the Cartan product of a K-module in $\gamma_{k,0}$ and a K-module in $\gamma_{0,\ell}$.

Observe that for any K-module in $\gamma_{k,\ell}$ the equality (71) always holds for $j = 0$ since, in view of Proposition 8.7 (iv), the left hand side as well as the right hand side of (71) are equal to zero. This observation also apply to the statement about the weight of $X^{k-j}E^{\ell+j}(v)$ when $j = 0$, since in this case $X^kE^\ell(v)$ is a $\mathfrak{k}^+$-highest weight vector. In particular this implies that (71) as well as the weight statement hold for any K-module in $\gamma_{0,\ell}$.

Consider now a K-module in $\gamma_{k,0}$ and let $0 \neq v \in V_{k,0}^M$. We shall prove by induction on $k \in \mathbb{N}$ that (71)holds for $\gamma_{k,0}$ and that $X^{k-j}E^j(v)$ is a vector of weight $\xi_{k,0} - j\gamma_1$. Let us consider first $k = 1$. Then we need to show that

$$X_1E(v) = \tfrac{1}{2}X(v), \tag{81}$$

for any $v \in V_{1,0}^M$. Since v is M-invariant we have $X(v) = X_4(v)$, hence using (63) we conclude that proving (81) is equivalent to show that

$$X_1E(v) = -EX_1(v), \tag{82}$$

for any $v \in V_{1,0}^M$.

Since $\mathfrak{p}$ is an irreducible K-module in Γ with highest weight $\xi_{1,0} = \widetilde{\epsilon_0} - \widetilde{\epsilon_1}$, we can assume that $V_{1,0} = \mathfrak{p}$. Then $\mathfrak{p}^M = \mathbb{C}(X_{\widetilde{\mu}} + X_{-\widetilde{\mu}})$ and we may take $v = X_{\widetilde{\mu}} + X_{-\widetilde{\mu}}$ where $\widetilde{\mu} = \widetilde{\epsilon_0} + \widetilde{\epsilon_1}$. Also recall that $X_1 = X_{\gamma_1}$ and $E = X_{\gamma_3}$ where $\gamma_1 = \widetilde{\epsilon_0} - \widetilde{\epsilon_2}$ and $\gamma_3 = \widetilde{\epsilon_0} + \widetilde{\epsilon_2}$. Then equation (82), and therefore (81), is equivalent to

$$[X_{\gamma_1}, [X_{\gamma_3}, X_{-\widetilde{\mu}}]] = -[X_{\gamma_3}, [X_{\gamma_1}, X_{-\widetilde{\mu}}]]. \tag{83}$$

We know that there exists $c \neq 0$ such that

$$[X_{\gamma_1}, [X_{\gamma_3}, X_{-\widetilde{\mu}}]] = c[X_{\gamma_3}, [X_{\gamma_1}, X_{-\widetilde{\mu}}]]. \tag{84}$$

Now, since $[X_{\widetilde{\mu}}, X_{\gamma_1}] = [X_{\widetilde{\mu}}, X_{\gamma_3}] = 0$, multiplying (84) on the left by $X_{\widetilde{\mu}}$ we obtain

$$[X_{\gamma_1}, [X_{\widetilde{\mu}}, [X_{-\widetilde{\mu}}, X_{\gamma_3}]]] = c[X_{\gamma_3}, [X_{\widetilde{\mu}}, [X_{-\widetilde{\mu}}, X_{\gamma_1}]]]. \tag{85}$$

Then, since $[X_{\widetilde{\mu}}, [X_{-\widetilde{\mu}}, X_{\gamma_3}]] = X_{\gamma_3}$ and $[X_{\widetilde{\mu}}, [X_{-\widetilde{\mu}}, X_{\gamma_1}]] = X_{\gamma_1}$, we conclude that $c = -1$ which proves (83), and therefore the proof of (81) is complete. We observe now that $E(v) = [X_{\gamma_3}, X_{-\widetilde{\mu}}]$ is a weight vector with respect to $\mathfrak{h}_{\mathfrak{k}}$ and that, in view of (81), its weight is equal to $\xi_{1,0} - \gamma_1$ as we wanted to prove. This completes the case $k = 1$.

Let us assume now that (71) holds for the K-module $\gamma_{k,0}$ and that for any $0 \neq v \in V_{k,0}^M$ the vectors $X^{k-j}E^j(v)$ have weight $\xi_{k,0} - j\gamma_1$ for every $0 \leq j \leq k$. We realize the K-module $\gamma_{k+1,0}$ as the Cartan product of $\gamma_{k,0}$ and $\gamma_{1,0}$, that is we take $V_{k+1,0}$ to be the irreducible submodule of $V_{k,0} \otimes V_{1,0}$ with highest weight $\xi_{k,0} + \xi_{1,0} = \xi_{k+1,0}$. Choose non trivial elements $v' \in V_{k,0}^M$, $v'' \in V_{1,0}^M$ and let v denote the isotypic component of $v' \otimes v''$ in $V_{k+1,0}^M$. Also for $0 \leq j \leq k+1$ we have

$$\begin{aligned} X^{k+1-j}E^j(v) &= X^{k+1-j}E^j(v' \otimes v'') \\ &= jX^{k+1-j}E^{j-1}(v') \otimes E(v'') + (k+1-j)X^{k-j}E^j(v') \otimes X(v''). \end{aligned} \tag{86}$$

Now applying X_1 to (86) and using that (71) holds for the K-modules $\gamma_{k,0}$ and $\gamma_{1,0}$ we obtain

$$\begin{aligned} X_1 X^{k+1-j}E^j(v) = \frac{j(j-1)}{2} X^{k+2-j}E^{j-2}(v') \otimes E(v'') \\ + \frac{j(k+2-j)}{2} X^{k+1-j}E^{j-1}(v') \otimes X(v'') = \frac{j}{2} X^{k+2-j}E^{j-1}(v), \end{aligned}$$

as we wanted to prove. This completes the proof of (71) for any K-module $\gamma_{k,0}$. Also formula (86) together with the inductive hypothesis and the results obtained for the K-module $\gamma_{1,0}$ imply that the vector $X^{k+1-j}E^j(v)$ has weight $\xi_{k+1,0} - j\gamma_1$ for every $0 \leq j \leq k$.

Let us consider now a K-module $\gamma_{k,\ell} \in \Gamma$ with $k, \ell \in \mathbb{N}$. Realize $\gamma_{k,\ell}$ as the Cartan product of $\gamma_{k,0}$ and $\gamma_{0,\ell}$, that is we take $V_{k,\ell}$ to be the irreducible submodule of $V_{k,0} \otimes V_{0,\ell}$ with highest weight $\xi_{k,0} + \xi_{0,\ell} = \xi_{k,\ell}$. Choose non-trivial elements $v' \in V_{k,0}^M$, $v'' \in V_{0,\ell}^M$ and let v denote the isotypic component of $v' \otimes v''$ in $V_{k,\ell}$. We know that $v \neq 0$ and that $v \in V_{k,\ell}^M$. Also for $0 \leq j \leq k$ we have

$$X^{k-j}E^{\ell+j}(v) = \binom{\ell+j}{\ell} X^{k-j}E^j(v') \otimes E^\ell(v''). \tag{87}$$

Now, using that (71) holds for $\gamma_{k,0}$ and that $E^\ell(v'')$ is a $\mathfrak{k}^+$-dominant vector, we obtain that

$$\begin{aligned} X_1 X^{k-j}E^{\ell+j}(v) &= \frac{j}{2}\binom{\ell+j}{\ell} X^{k+1-j}E^{j-1}(v') \otimes E^\ell(v'') \\ &= \frac{1}{2}(\ell+j)X^{k+1-j}E^{\ell+j-1}(v), \end{aligned}$$

which proves (71) for any K-module $\gamma_{k,\ell}$ in Γ. On the other hand it follows from (87) that $X^{k-j}E^{\ell+j}(v)$ is a vector of weight $\xi_{k,0}+\xi_{0,\ell}-j\gamma_1 = \xi_{k,\ell}-j\gamma_1$, as we wanted to prove.

Consider now any K-module $\gamma_{k,\ell} \in \Gamma$ with $k, \ell \in \mathbb{N}_0$, $0 \neq v \in V_{k,\ell}^M$ and set $u_{k,\ell} = X^k E^\ell(v)$. In view of Proposition 8.7 (iv) $u_{k,\ell}$ is a $\mathfrak{k}^+$-dominant vector of weight $\xi_{k,\ell}$. Now for any $0 \leq j \leq k$ the vectors $X_{-1}^j(u_{k,\ell})$ and $X^{k-j}E^{\ell+j}(v)$ have both weight $\xi_{k,\ell} - j\gamma_1$. Since γ_1 is a simple root the weight space corresponding to $\xi_{k,\ell} - j\gamma_1$ has dimension one. Then there exists a non trivial constant c such that

$$X_{-1}^j(u_{k,\ell}) = cX^{k-j}E^{\ell+j}(v). \tag{88}$$

Now, applying X_1^j to (88) and using Lemma 8.8 and (71), we obtain that $c = 2^j j! \binom{k}{j} \binom{\ell+j}{\ell}^{-1}$, completing the proof of (73). This also implies that $\{X^{k-j}E^{\ell+j}(v) : 0 \leq j \leq k\}$ is a basis of the $\{H_1, X_1, X_{-1}\}$ irreducible module of dimension $k+1$ generated by the highest weight vector $u_{k,\ell}$.

Finally (72) is a direct consequence of (73). This completes the proof of the proposition.

8.1. **Transversality results.** Our next goal is to establish several transversality results that will allow us to deal with the congruence modulo the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ which occurs in the definition of the algebra B.

Set $\mathfrak{q}^+ = \mathfrak{k}^+ - \mathbb{C}X_{\gamma_1}$; since γ_1 is a simple root in $\Delta^+(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})$ it follows that $\mathfrak{q}^+$ is a subalgbra of $\mathfrak{k}^+$. We are interested in considering vectors $v \in U(\mathfrak{k})^{\mathfrak{q}^+}$ of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$ with $a, b, c \in \mathbb{Z}$. Two examples of such vectors are the following: $v = \dot{X}_{-1}^t(u)$ and $v = \sum_{j\geq 0} u_j E^j$ where $u, u_j \in U(\mathfrak{k})$ are $\mathfrak{k}^+$-dominant weight vectors of irreducible K-modules in Γ_1, $u_j \neq 0$ only for a finite number of j's, and v is a weight vector.

The proof of the following theorem will be the consequence of several results that will be proved in what follows.

Theorem 8.10. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $v \in U(\mathfrak{k})^{\mathfrak{q}^+}$ be a vector of weight $\xi = a\gamma_1 + b\gamma_2 + c\delta$ where $a, b, c \in \mathbb{Z}$. Then $v \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ if and only if $v \equiv 0 \mod (U(\mathfrak{k})X_2)$.*

We begin by setting up the necessary background. We will assume from now on that $n > 2$, the case $n = 2$ will be considered later. Let $\mathfrak{h}_{\mathfrak{r}} = \ker(\gamma_1) \cap \ker(\gamma_2) \cap \ker(\delta)$, and let $\mathfrak{q}$ be the subalgebra of $\mathfrak{k}$ defined as follows

$$\mathfrak{q} = \mathfrak{q}^+ \oplus \mathfrak{h}_{\mathfrak{r}} \oplus \mathfrak{q}^- \tag{89}$$

where

$$\mathfrak{q}^- = \langle \{X_{-\alpha} : X_\alpha \in \mathfrak{q}^+ \text{ and } [X_\alpha, X_{-\alpha}] \in \mathfrak{h}_{\mathfrak{r}}\} \rangle.$$

Recall that the simple roots in $\Delta^+(\mathfrak{g}, \mathfrak{h}_{\mathfrak{k}})$ are $\widetilde{\alpha_i} = \widetilde{\epsilon_i} - \widetilde{\epsilon_{i+1}}$ for $0 \leq i \leq n-1$ and $\widetilde{\alpha_n} = 2\widetilde{\epsilon_n}$. Also it follows from (62) that the set of simple roots in $\Delta^+(\mathfrak{k}, \mathfrak{h}_{\mathfrak{k}})$ is $\Pi = \{\delta, \gamma_1, \widetilde{\alpha_2}, \ldots, \widetilde{\alpha_n}\}$. Then, if for each $\alpha \in \Pi$ we let $H_\alpha \in [\mathfrak{k}_\alpha, \mathfrak{k}_{-\alpha}]$ be such that $\alpha(H_\alpha) = 2$, it is easy to see that

$$\mathfrak{h}_{\mathfrak{r}} = \langle \{H_{\widetilde{\alpha_i}} : 3 \leq i \leq n\} \rangle. \tag{90}$$

From this it follows that

$$\mathfrak{q}^- = \langle \{X_{-(\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j})} : 3 \leq i < j \leq n\} \cup \{X_{-2\widetilde{\epsilon_i}} : 3 \leq i \leq n\} \rangle. \tag{91}$$

Lemma 8.11. *Let $\mathfrak{q}$ be the subalgebra of $\mathfrak{k}$ defined in* (89). *Then there exists a semisimple subalgebra $\mathfrak{r}$ and a nilpotent subalgebra $\mathfrak{u}$ of $\mathfrak{q}$ such that $\mathfrak{q} = \mathfrak{r} \oplus \mathfrak{u}$, $[\mathfrak{r}, \mathfrak{u}] \subset \mathfrak{u}$ and $\mathfrak{h}_{\mathfrak{r}}$ is a Cartan subalgebra of $\mathfrak{r}$. Also, if we set $\mathfrak{l} = \mathfrak{m}^+ \cap \mathfrak{u}$ we have $[\mathfrak{r}, \mathfrak{l}] \subset \mathfrak{l}$ and there exists a positive system of roots $\Delta^+(\mathfrak{r}, \mathfrak{h}_{\mathfrak{r}})$ such that $\mathfrak{m}^+ = \mathfrak{r}^+ \oplus \mathfrak{l}$.*

Proof. We define

$$\mathfrak{r} = \langle \mathfrak{h}_{\mathfrak{r}} \cup \{X_{\pm(\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j})} : 3 \leq i < j \leq n\} \cup \{X_{\pm 2\widetilde{\epsilon_i}} : 3 \leq i \leq n\} \rangle$$

and

$$\mathfrak{u} = \langle \{X_{\widetilde{\epsilon_0} + \widetilde{\epsilon_2}}, X_{\widetilde{\epsilon_0} \pm \widetilde{\epsilon_j}}, X_{\widetilde{\epsilon_2} \pm \widetilde{\epsilon_j}} : 3 \leq j \leq n\} \cup \{X_4, X, X_2\} \rangle.$$

Then $\mathfrak{r}$ is a semisimple subalgebra of $\mathfrak{k}$, in fact $\mathfrak{r} \simeq \mathfrak{sp}(n-2, \mathbb{C})$. Also, $\mathfrak{u}$ is a nilpotent subalgebra of $\mathfrak{k}$, $[\mathfrak{r}, \mathfrak{u}] \subset \mathfrak{u}$ and it follows from (89) and (91) that $\mathfrak{q} = \mathfrak{r} \oplus \mathfrak{u}$. It is also clear that $\mathfrak{h}_{\mathfrak{r}}$ is a Cartan subalgebra of $\mathfrak{r}$ and that

$$\Delta^+(\mathfrak{r}, \mathfrak{h}_{\mathfrak{r}}) = \{\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j} : 3 \leq i < j \leq n\} \cup \{2\tilde{\epsilon}_i : 3 \leq i \leq n\} \tag{92}$$

is a positive system of $\Delta(\mathfrak{r}, \mathfrak{h}_{\mathfrak{r}})$. Moreover from (75) it follows that

$$\mathfrak{l} = \langle \{X_{\widetilde{\epsilon_2} \pm \widetilde{\epsilon_j}} : 3 \leq j \leq n\} \cup \{X_2, X_4 - X\} \rangle.$$

Hence it is clear that $\mathfrak{m}^+ = \mathfrak{r}^+ \oplus \mathfrak{l}$. This completes the proof of the lemma.

Let Q be the connected Lie subgroup of K with Lie algebra $\mathfrak{q}$. Also let R and U be the connected Lie subgroups of Q with Lie algebras $\mathfrak{r}$ and $\mathfrak{u}$, respectively, and let L be the connected Lie subgroup of U with Lie algebra $\mathfrak{l}$. Then L is a unipotent subgroup of K and, in view of Lemma 8.11, R normalizes L.

Now, in order to proceed any further, we need to state the following result of Tirao; we refer to [25] for its proof. Let G be a reductive linear algebraic group over $\mathbb{C}$ and let $\mathfrak{g}$ be its Lie algebra. Let $\hat{G}$ denote the set of all equivalence classes of holomorphic irreducible finite dimensional representations of G and let V_π denote a fixed G-module in the class π for each $\pi \in \hat{G}$. If U is a connected unipotent subgroup of G and $\mathfrak{u}$ denotes its Lie algebra we have

Theorem 8.12. *Let $a \in U(\mathfrak{g})$. Then $a \in U(\mathfrak{g})\mathfrak{u}$ if and only if $\pi(a)(V_\pi^U) = 0$ for every $\pi \in \hat{G}$.*

Let R and L be the connected Lie subgroups of K defined above. We are now in a position to start proving Theorem 8.10. The following result allows to reduce, under appropriate conditions, a congruence $\bmod\ (U(\mathfrak{k})\mathfrak{m}^+)$ to a congruence $\bmod\ (U(\mathfrak{k})\mathfrak{l})$, see Proposition 3.8 of [2].

Proposition 8.13. *We have*

$$U(\mathfrak{k})^R \cap U(\mathfrak{k})\mathfrak{m}^+ = U(\mathfrak{k})^R \cap U(\mathfrak{k})\mathfrak{l}.$$

Proof. Let $a \in U(\mathfrak{k})^R \cap U(\mathfrak{k})\mathfrak{m}^+$. In view of Theorem 8.12 we need to show that $\pi(a)\big(V_\pi^L\big) = 0$ for every $\pi \in \hat{K}$. Fix $\pi \in \hat{K}$, since R normalizes L, V_π^L is an R-module. Let $W \subset V_\pi^L$ be an irreducible R-module and let $w \in W$ be a non-zero $\mathfrak{r}^+$-dominant vector, with respect to the positive system defined in Lemma 8.11. Since $a \in U(\mathfrak{k})^R$ the map $\pi(a) : W \to V_\pi^L$ is R-equivariant. Hence $\ker(\pi(a)) = 0$ or W. Now, since $\mathfrak{m}^+ = \mathfrak{r}^+ \oplus \mathfrak{l}$, we have $\pi(X)w = 0$ for every $X \in \mathfrak{m}^+$. Then, since $a \in U(\mathfrak{k})\mathfrak{m}^+$, it follows that $\pi(a)w = 0$ with $w \neq 0$. This implies that $\pi(a)(W) = 0$ for every irreducible R-module $W \subset V_\pi^L$, thus $\pi(a)\big(V_\pi^L\big) = 0$ as we wanted to prove.

The next step in proving Theorem 8.10 will consist in establishing that $U(\mathfrak{k})^R \cap U(\mathfrak{k})\mathfrak{l} = U(\mathfrak{k})^R \cap U(\mathfrak{k})X_2$, this will be done mainly by applying the Poincaré-Birkhoff-Witt theorem several times. Before starting with this part of the argument we need to state a very general lemma.

Let $\mathfrak{k}$ be a finite dimensional complex Lie algebra and let $\mathfrak{l}$ be a subalgebra of $\mathfrak{k}$. If $\{X_1, \dots, X_r\}$ is an ordered basis of $\mathfrak{l}$ we complete it to an ordered basis $\{Y_1, \dots, Y_s, X_1, \dots, X_r\}$ of $\mathfrak{k}$. Then if $I = \{i_1, \dots, i_s\}$ and $J = \{j_1, \dots, j_r\}$ we set $Y^I X^J = Y_1^{i_1} \times \cdots \times Y_s^{i_s} \times X_1^{j_1} \times \cdots \times X_r^{j_r}$ in $U(\mathfrak{k})$. For a proof of the following result we refer the reader to Lemma 3.5 of [2].

Lemma 8.14. *Any $u \in U(\mathfrak{k})\mathfrak{l}$ can be written in a unique way as $u = a_1X_1 + \cdots + a_rX_r$ where*

$$a_k = \sum a_{I,j_1,\dots,j_k} Y^I X_1^{j_1} \cdots X_k^{j_k} \quad \textit{for} \quad k = 1, \dots, r.$$

We shall now define a certain subalgebra $\mathfrak{s}$ of $\mathfrak{k}$ that will be very useful in what follows. Let $\{\widetilde{H_j} : 0 \le j \le n\} \subset \mathfrak{h}_\mathfrak{k}$ be the dual basis of $\{\widetilde{\epsilon_j} : 0 \le j \le n\}$ and set $H_\mathfrak{s} = \widetilde{H_2} - \widetilde{H_1}$. Then, if $\operatorname{centr}_\mathfrak{k}(H_\mathfrak{s})$ denotes the centralizer of $H_\mathfrak{s}$ in $\mathfrak{k}$ we define

$$\mathfrak{s} = \operatorname{centr}_\mathfrak{k}(H_\mathfrak{s}) \oplus \sum_{\widetilde{\alpha}(H_s) < 0} \mathfrak{k}_{\widetilde{\alpha}}, \tag{93}$$

where $\mathfrak{k}_{\widetilde{\alpha}}$ is the root space corresponding to the root $\widetilde{\alpha} \in \Delta(\mathfrak{k}, \mathfrak{h}_\mathfrak{k})$. Now using the explicit description of $\mathfrak{k}^+$ given at the beginning of this section and that of $\mathfrak{l}$ given in Lemma 8.11 it is easy to verify that,

$$\mathfrak{k} = \mathfrak{s} \oplus \mathbb{C}X_{-1} \oplus \mathbb{C}E \oplus \mathfrak{l}. \tag{94}$$

Next we introduce the following notation $S_j = X_{\tilde{\epsilon_2}+\tilde{\epsilon_j}}$ and $T_j = X_{\tilde{\epsilon_2}-\tilde{\epsilon_j}}$ where $3 \le j \le n$. With this notation at hand we have

$$\mathfrak{l} = \langle \{S_j, T_j : 3 \le j \le n\} \cup \{X_2, X_4 - X\}\rangle. \tag{95}$$

We assume that the root vectors S_j and T_j are normalized in such a way that $[S_j, T_j] = X_2$ for every $3 \le j \le n$. Also by direct inspection it follows that all the other brackets among the basis elements of $\mathfrak{l}$ are zero.

Now it follows from (64) that

$$[X_{-1}, X_4 - X] = 2E \quad \textit{and} \quad [X_{-1}, E] = 2X_2. \tag{96}$$

On the other hand, direct inspection shows that the brackets between X_{-1} (respectively E) and all the remainig basis elements of $\mathfrak{l}$ are zero.

If $\{Z_1, \dots, Z_p\}$ is an ordered basis of $\mathfrak{s}$, in view of (94) the following set

$$\{Z_1, \dots, Z_p, X_{-1}, E, S_3, \dots, S_n, T_3, \dots, T_n, X_2, X_4 - X\} \tag{97}$$

is an ordered basis of $\mathfrak{k}$. In order to simplify the notation and motivated by Lemma 8.14 we define $U_j(\mathfrak{k})$, for $3 \le j \le n$, as the subspace of $U(\mathfrak{k})$ formed by those elements whose monomials, when written in the Poincaré-Birkhoff-Witt basis of $U(\mathfrak{k})$ corresponding to (97), end with S_j or before. Similarly, for $3 \le j \le n$, we define $U^j(\mathfrak{k})$ as the subspace of $U(\mathfrak{k})$ formed by those elements whose monomials end with T_j or before. Also, let $U_2(\mathfrak{k})$ denote the subspace of $U(\mathfrak{k})$ formed by those elements whose monomials end with X_2 or before. We are now in position to establish the following result.

Proposition 8.15. *If Q is the subgroup of K introduced before, we have*

$$U(\mathfrak{k})^Q \cap U(\mathfrak{k})\mathfrak{l} = U(\mathfrak{k})^Q \cap U(\mathfrak{k})\langle\{X_2, X_4 - X\}\rangle.$$

Proof. Let $v \in U(\mathfrak{k})^Q \cap U(\mathfrak{k})\mathfrak{l}$. Then in view of Lemma 8.14, we can write

$$v = \sum_{j=3}^{n} a_j S_j + \sum_{j=3}^{n} b_j T_j + cX_2 + d(X_4 - X),$$

where $a_j \in U_j(\mathfrak{k})$, $b_j \in U^j(\mathfrak{k})$, $c \in U_2(\mathfrak{k})$ and $d \in U(\mathfrak{k})$. Our objective in this proof is to show that $a_j = b_j = 0$ for every $3 \le j \le n$. For this purpose we set $V_j = X_{\tilde{\epsilon_0}-\tilde{\epsilon_j}}$ for every $3 \le j \le n$. Then $V_j \in \mathrm{centr}_{\mathfrak{k}}(H_{\mathfrak{s}}) \subset \mathfrak{s}$, thus $\dot{V}_j(U(\mathfrak{s})) \subset U(\mathfrak{s})$. From the definition of $\mathfrak{u}$ in Lemma 8.11 it follows that $V_j \in \mathfrak{u} \subset \mathfrak{q}$. Hence $\dot{V}_j(v) = 0$. Also, using (96), it is easy to see that V_j can be normalized in such a way that

$$\dot{V}_j(S_j) = E \quad \textit{and} \quad \dot{V}_j(X_{-1}) = 2T_j, \tag{98}$$

for every $3 \le j \le n$. On the other hand, by direct inspection it follows that $\dot{V}_j(S_i) = 0$ if $i \ne j$, $\dot{V}_j(T_i) = 0$ for every $3 \le i, j \le n$ and $\dot{V}_j(E) = \dot{V}_j(X_2) = \dot{V}_j(X_4 - X) = 0$ for every $3 \le j \le n$.

Now let us assume that the set $\{j : a_j \neq 0\}$ is not empty and set $r = \min\{j : a_j \neq 0\}$. Then it follows, from (98) and from the action of $\dot{V}_r$ on the other basis elements of $\mathfrak{l}$, that

$$\begin{aligned} 0 =& \dot{V}_r(a_r)S_r + a_r E + \sum_{j=r+1}^{n} \dot{V}_r(a_j)S_j + \sum_{j=3}^{n} \dot{V}_r(b_j)T_j \\ &+ \dot{V}_r(c)X_2 + \dot{V}_r(d)(X_4 - X). \end{aligned} \tag{99}$$

On the other hand, since $[S_j, T_j] = X_2$ for every $3 \leq j \leq n$, it follows that

$$T_j S_j^k = S_j^k T_j - k S_j^{k-1} X_2 \tag{100}$$

for every $3 \leq j \leq n$. Then using (98) and (100) it is easy to verify that for every $j \geq r$ we have $\dot{V}_r a_j = u_0 + u_1 T_r + u_2 X_2$ where $u_i \in U_j(\mathfrak{k})$ for $i = 0, 1, 2$. Similarly, for every $3 \leq j \leq n$ one obtains $\dot{V}_r b_j = v_0 + v_1 T_r + v_2 X_2$ where $v_i \in U^j(\mathfrak{k})$ for $i = 0, 1, 2$. Also (98) and (100) imply that $\dot{V}_r(U_2(\mathfrak{k})) \subset U_2(\mathfrak{k})$. Using all this information in (99), together with Poincaré-Birkhoff-Witt theorem, we conclude that every monomial of a_r must contain S_r, that is $a_r = a'_r S_r$ with $a'_r \in U_r(\mathfrak{k})$. Therefore we have

$$v = a'_r S_r^2 + \sum_{j=r+1}^{n} a_j S_j + \sum_{j=3}^{n} b_j T_j + c X_2 + d(X_4 - X).$$

Applying $\dot{V}_r$ to v again, the same argument gives that every monomial of a'_r must contain S_r, that is $a'_r = a''_r S_r$. Hence $a_r = a''_r S_r^2$. Now by induction we conclude that a_r is a multiple of any power of S_r. This implies that $a_r = 0$, which is contradiction. Therefore we have $a_j = 0$ for every $3 \leq j \leq n$. Hence

$$v = \sum_{j=3}^{n} b_j T_j + c X_2 + d(X_4 - X). \tag{101}$$

Now in order to prove that $b_j = 0$ for $3 \leq j \leq n$ we set $W_j = X_{\tilde{\epsilon}_0 + \tilde{\epsilon}_j}$. Then $W_j \in \mathrm{centr}_{\mathfrak{k}}(H_{\mathfrak{s}}) \subset \mathfrak{s}$, and from the definition of $\mathfrak{u}$ it follows that $W_j \in \mathfrak{u} \subset \mathfrak{q}$. Hence $\dot{W}_j(v) = 0$ and $\dot{W}_j(U(\mathfrak{s})) \subset U(\mathfrak{s})$ for every $3 \leq j \leq n$. Also, as before, it is easy to see that W_j can be normalized in such a way that

$$\dot{W}_j(T_j) = E \quad \textit{and} \quad \dot{W}_j(X_{-1}) = -2S_j, \tag{102}$$

for $3 \leq j \leq n$. Also by direct inspection it follows that $\dot{W}_j(E) = \dot{W}_j(X_2) = \dot{W}_j(X_4 - X) = 0$ for every $3 \leq j \leq n$.

As above, let us assume that the set $\{j : b_j \neq 0\}$ is not empty and set $r = \min\{j : b_j \neq 0\}$. Then it follows from (101), (102) and from the action of $\dot{W}_r$ on the other basis elements of $\mathfrak{l}$ that

$$0 = \dot{W}_r(b_r)T_r + b_r E + \sum_{j=r+1}^{n} \dot{W}_r(b_j)T_j + \dot{W}_r(c)X_2 + \dot{W}_r(d)(X_4 - X). \tag{103}$$

From the above description of the action of $\dot{W}_r$ it follows that $\dot{W}_r(U^j(\mathfrak{k})) \subset U^j(\mathfrak{k})$ for every $j \geq r$ and $\dot{W}_r(U_2(\mathfrak{k})) \subset U_2(\mathfrak{k})$. Then (103) together with Poincaré-Birkhoff-Witt theorem imply that $(\dot{W}_r b_r)T_r + b_r E = 0$, which in turns implies that every monomial of b_r must contain T_r, that is, $b_r = b_r' T_r$ with $b_r' \in U^r(\mathfrak{k})$. Hence

$$v = b_r' T_r^2 + \sum_{j=r+1}^{n} b_j T_j + cX_2 + d(X_4 - X).$$

Applying $\dot{W}_r$ to v again we obtain $\dot{W}_r(b_r')T_r + 2b_r' E = 0$, from where it follows that $b_r' = b_r'' T_r$ with $b_r'' \in U^r(\mathfrak{k})$. Hence $b_r = b_r'' T_r^2$. Now by induction we conclude that b_r is a multiple of any power of T_r. This implies that $b_r = 0$, which is a contradiction. Therefore we have that $b_j = 0$ for every $3 \leq j \leq n$. Hence $v = cX_2 + d(X_4 - X)$, as we wanted to prove.

Next we prove a lemma that will be needed in what follows.

Lemma 8.16. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $\langle\{X_2, X_4 - X\}\rangle$ be the abelian subalgebra of $\mathfrak{m}^+$ spanned by $\{X_2, X_4 - X\}$. Then if $v \in U(\mathfrak{k})\langle\{X_2, X_4 - X\}\rangle$ is a weight vector we have $v \in U(\mathfrak{k})X_2$.*

Proof. We find convenient to take as an ordered basis of $\mathfrak{k}$ one of the following form

$$\{X_{-1}, \dots, X_{-m}, H_1, \dots, H_\ell, X_1, \dots, X_{m-3}, X_4, X_2, X_4 - X\},$$

where X_{-j} is a negative root vector for each $1 \leq j \leq m$, $\{H_1, \dots, H_\ell\}$ is a basis of $\mathfrak{h}_\mathfrak{k}$ and X_j are positive root vectors such that they are not multiples of X_4, X_2 or X, for all $1 \leq j \leq m-3$. By hypothesis we may assume that v is a vector of weight λ and that can be writen, in a unique way, as

$$v = aX_2 + \sum_{j=1}^{p} b_j (X_4 - X)^j,$$

where a and each b_j are sums of Poincaré-Birkhoff-Witt monomials not including the basis vector $X_4 - X$. Moreover we can certainly assume that $p \geq 1$ and that $b_p \neq 0$. Then

$$v = aX_2 + \sum_{j=1}^{p} b_j X_4^j + \sum_{i=1}^{p} (-1)^i \Big(\sum_{j=i}^{p} \tbinom{j}{i} b_j X_4^{j-i} \Big) X^i. \tag{104}$$

If we look at the summand $b_p X^p$ expressed as a sum of PBW-monomials we observe that $b_p = d_{\lambda - p\delta}$ is an element in $U(\mathfrak{k})$ of weight $\lambda - p\delta$ and such that all its PBW-monomials do not include the basis vector $X_4 - X$. Similarly, if $p > 1$ and we look at the summand $\big(\binom{p}{p-1} b_p X_4 + b_{p-1}\big) X^{p-1}$ we see that $d_{\lambda-(p-1)\delta} = \binom{p}{p-1} b_p X_4 + b_{p-1}$ is a vector of weight $\lambda - (p-1)\delta$ all whose PBW-monomials do not include the basis vector $X_4 - X$. Thus $b_{p-1} = d_{\lambda-(p-1)\delta} - \binom{p}{p-1} b_p X_4$. Now by decreasing induction on j we can prove that there exists a unique sequence $\{d_{\lambda-j\delta}\}$, $1\le j\le p$, of elements $d_{\lambda-j\delta}\in U(\mathfrak{k})$ such that

$$b_j=\sum_{r=0}^{p-j}(-1)^r\tbinom{j+r}{r}d_{\lambda-(j+r)\delta}X_4^r. \tag{105}$$

Moreover $d_{\lambda-(j+r)\delta}$ is a vector of weight $\lambda-(j+r)\delta$ such that all its PBW-monomials do not include the basis vector X_4-X. In fact (105) is true for $j=p$. Now assume that for each $1<i\le p$ we have a unique $d_{\lambda-j\delta}$, with the stated properties, such that

$$b_j=\sum_{r=0}^{p-j}(-1)^r\tbinom{j+r}{r}d_{\lambda-(j+r)\delta}X_4^r. \tag{106}$$

If we look at the summand $(-1)^{i-1}\Big(\sum_{j=i-1}^{n}\binom{j}{i-1}b_jX_4^{j-i+1}\Big)X^{i-1}$ in (104) we realize that

$$d_{\lambda-(i-1)\delta}=\sum_{j=i-1}^{p}\tbinom{j}{i-1}b_jX_4^{j-i+1}$$

is a vector of weight $\lambda-(i-1)\delta$ and all its PBW-monomials do not include the basis vector X_4-X. Thus

$$d_{\lambda-(i-1)\delta}=b_{i-1}+\sum_{\substack{i\le j\le p\\0\le r\le p-j}}\tbinom{j}{i-1}(-1)^r\tbinom{j+r}{r}d_{\lambda-(j+r)\delta}X_4^{r+j-i+1}. \tag{107}$$

If we introduce a new summation index $k=r+j$ we get

$$\begin{aligned}d_{\lambda-(i-1)\delta}&=b_{i-1}+\sum_{\substack{i\le k\le p\\0\le r\le k-i}}\tbinom{k-r}{i-1}(-1)^r\tbinom{k}{r}d_{\lambda-k\delta}X_4^{k-i+1}\\&=b_{i-1}+\sum_{i\le k\le p}(-1)^{k-i}\tbinom{k}{i-1}d_{\lambda-k\delta}X_4^{k-i+1},\end{aligned} \tag{108}$$

since $\sum_{0\le r\le k-i}(-1)^r\binom{k-r}{i-1}\binom{k}{r}=(-1)^{k-i}\binom{k}{i-1}$.

Therefore

$$\begin{aligned}b_{i-1}&=\sum_{i-1\le k\le p}(-1)^{k-i+1}\tbinom{k}{i-1}d_{\lambda-k\delta}X_4^{k-i+1}\\&=\sum_{0\le r\le p-i+1}(-1)^r\tbinom{i-1+r}{r}d_{\lambda-(i-1+r)\delta}X_4^r,\end{aligned} \tag{109}$$

as we wanted to prove.

Now we want to express (104) in terms of the weight vectors $d_{\lambda-j\delta}$ instead of the vectors b_j. We have

$$\begin{aligned}\sum_{j=i}^{p}\tbinom{j}{i}b_jX_4^{j-i} &= \sum_{\substack{i\le j\le p\\0\le r\le p-j}}\tbinom{j}{i}(-1)^r\tbinom{j+r}{r}d_{\lambda-(j+r)\delta}X_4^{j+r-i}\\ &=\sum_{i\le k\le p}\Big(\sum_{0\le r\le k-i}(-1)^r\tbinom{k-r}{i}\tbinom{k}{r}\Big)d_{\lambda-k\delta}X_4^{k-i}\\ &= d_{\lambda-i\delta},\end{aligned}\tag{110}$$

since

$$\sum_{0\le r\le k-i}(-1)^r\tbinom{k-r}{i}\tbinom{k}{r}=\begin{cases}0, & \text{if } k>i\\ 1, & \text{if } k=i.\end{cases}$$

On the other hand we have,

$$\begin{aligned}\sum_{j=1}^{p}b_jX_4^{j} &= \sum_{\substack{1\le j\le p\\0\le r\le p-j}}(-1)^r\tbinom{j+r}{r}d_{\lambda-(j+r)\delta}X_4^{j+r}\\ &=\sum_{1\le k\le p}\Big(\sum_{0\le r\le k-1}(-1)^r\tbinom{k}{r}\Big)d_{\lambda-k\delta}X_4^{k}\\ &=\sum_{1\le k\le p}(-1)^{k-1}d_{\lambda-k\delta}X_4^k.\end{aligned}\tag{111}$$

Now using (110) and (111) we obtain

$$v=aX_2+\sum_{1\le k\le p}(-1)^{k-1}d_{\lambda-k\delta}X_4^k+\sum_{1\le i\le p}(-1)^i d_{\lambda-i\delta}X^i.\tag{112}$$

We observe that each term $d_{\lambda-k\delta}X_4^k$ is a vector of weight $\lambda+k(\gamma_4-\delta)\neq\lambda$ for $1\le k\le p$. Therefore, each PBW-monomial of these terms must cancel with a corresponding PBW-monomial of aX_2, since they do no appear in the other summands. Hence $d_{\lambda-k\delta}X_4^k=a_kX_2$, but this implies that $d_{\lambda-k\delta}=c_kX_2$, since X_2 and X_4 commutes. Thus we finally obtain

$$v=\Big(a+\sum_{1\le k\le p}(-1)^{k-1}c_kX_4^k+\sum_{1\le i\le p}(-1)^kc_iX^i\Big)X_2.$$

This completes the proof of the lemma.

Proof of Theorem 8.10. Let us consider first $n=2$. In this case we have $\mathfrak{m}^+=\langle\{X_2,X_4-X\}\rangle$, then the theorem follows from a direct application of Lemma 8.16. Now let $n>2$ and v be as in Theorem 8.10. It follows from the definition of the group Q that $v\in U(\mathfrak{k})^Q\cap U(\mathfrak{k})\mathfrak{m}^+$. On the other hand, since $R\subset Q$, it follows from Proposition 8.13 that $U(\mathfrak{k})^Q\cap U(\mathfrak{k})\mathfrak{m}^+=U(\mathfrak{k})^Q\cap U(\mathfrak{k})\mathfrak{l}$. Therefore, in view of Proposition 8.15, it follows that $v\in U(\mathfrak{k})^Q\cap U(\mathfrak{k})\langle\{X_2,X_4-X\}\rangle$. Finally, since v is a weight vector, Lemma 8.16 implies that $v\equiv 0 \mod (U(\mathfrak{k})X_2)$, as we wanted to prove. $\square$

The next result follows directly from Theorem 8.10.

Corollary 8.17. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$. Let $v = \dot{X}_{-1}^t(u)$ or $v = \sum_{j\geq 0} u_j E^j$ be a vector of weight $\lambda = a\gamma_1 + b\gamma_2 + c\delta$, where $u, u_j \in U(\mathfrak{k})$ are $\mathfrak{k}^+$-dominant weight vectors of irreducible K-modules in Γ_1 and $u_j \neq 0$ only for a finite number of j's. Then $v \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ if and only if $v \equiv 0 \mod (U(\mathfrak{k})X_2)$.*

Remark. The only hypothesis needed on the u_j is that they are $\mathfrak{k}^+$-dominant.

The following two results are derived by restricting our attention to the subalgebra $\widetilde{\mathfrak{g}_o} \simeq \mathfrak{sp}(2,1)$.

Proposition 8.18. *Let $u, v \in U(\mathfrak{k})$ be dominant vectors for the $\mathfrak{s}$-triple $\{H_1, X_1, X_{-1}\}$. If $u + vE \equiv 0 \mod (U(\mathfrak{k})X_2)$ then $u = v = 0$.*

Proof. Let $u+vE = wX_2$ for some $w \in U(\mathfrak{k})$. Then applying $\dot{X}_1$ successively we obtain

$$vX_4 = \dot{X}_1(w)X_2 + wE \tag{113}$$

and

$$0 = \dot{X}_1^k(w)X_2 + k\dot{X}_1^{k-1}(w)E + \frac{k(k-1)}{2}\dot{X}_1^{k-2}(w)X_4, \tag{114}$$

for all $k \geq 2$. If k is sufficiently large we have $\dot{X}_1^k(w) = 0$. But then from (114), by decreasing induction on k, we get that $w = 0$. Thus from (113) we obtain $v = 0$ and therefore $u = 0$, completing the proof of the proposition.

From Theorem 8.10 and Proposition 8.18 the following corollary follows.

Corollary 8.19. *Let $u \in U(\mathfrak{k})$ be a $\mathfrak{k}^+$-dominant vector of weight $\lambda = a\gamma_1 + b\gamma_2 + c\delta$ where $a, b, c \in \mathbb{N}_o$. Then $u \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ implies $u = 0$.*

Before stating the next lemma we define $\Delta = 2X_4X_2 - E^2$ and observe that, since X_2, X_4 and E commute with each other, it is easy to show that $(-1)^j\Delta^j \equiv E^{2j} \mod (U(\mathfrak{k})X_2)$.

Lemma 8.20. *Let $\{\eta_j : j \in \mathbb{N}_0\}$ be a sequence in $U(\mathfrak{k})$ such that $\eta_j \neq 0$ only for a finite number of j's, $\dot{X}_1(\eta_j) = 0$ for every $j \in \mathbb{N}_0$ and $\sum_{j\geq 0} \eta_j E^j \equiv 0 \mod (U(\mathfrak{k})X_2)$. Then*

$$\sum_{i\geq 0} \eta_{2i}E^{2i} \equiv 0 \quad \textit{and} \quad \textstyle\sum_{i\geq 0} \eta_{2i+1}E^{2i+1} \equiv 0,$$

where in both cases the congruence is $\mod (U(\mathfrak{k})X_2)$.

Proof. Let $\widetilde{\eta_0} = \sum_{i\geq 1}(-1)^{i+1}\eta_{2i}\Delta^i$ and $\widetilde{\eta_1} = \sum_{i\geq 1}(-1)^{i+1}\eta_{2i+1}\Delta^i$. We shall first show that

$$\widetilde{\eta_0} + \widetilde{\eta_1}E + \sum_{j\geq 2} \eta_j E^j \equiv 0 \qquad \mod (U(\mathfrak{k})X_2). \tag{115}$$

In fact,

$$\widetilde{\eta_0} + \sum_{i\geq 1} \eta_{2i} E^{2i} = \sum_{i\geq 1} \eta_{2i}\big((-1)^{i+1}\Delta^i + E^{2i}\big) \equiv 0 \tag{116}$$

and similarly

$$\widetilde{\eta_1} E + \sum_{i\geq 1} \eta_{2i+1} E^{2i+1} = \sum_{i\geq 1} \eta_{2i+1}\big((-1)^{i+1}\Delta^i E + E^{2i+1}\big) \equiv 0, \tag{117}$$

where in both cases the congruence is $\mod (U(\mathfrak{k})X_2)$. Hence (115) follows.

Now, since $\sum_{j\geq 2} \eta_j E^j \equiv -\eta_0 - \eta_1 E \mod (U(\mathfrak{k})X_2)$, it follows from (115) that

$$(\widetilde{\eta_0} - \eta_0) + (\widetilde{\eta_1} - \eta_1)E \equiv 0 \qquad \mod (U(\mathfrak{k})X_2). \tag{118}$$

Since $\dot{X}_1(\Delta) = 0$ it follows that $\dot{X}_1(\widetilde{\eta_0}) = \dot{X}_1(\widetilde{\eta_1}) = 0$. Thus from Proposition 8.18 we obtain that $\widetilde{\eta_0} = \eta_0$ and $\widetilde{\eta_1} = \eta_1$. Going back to (116) and (117) we get respectively $\sum_{i\geq 0} \eta_{2i} E^{2i} \equiv 0$ and $\sum_{i\geq 0} \eta_{2i+1} E^{2i+1} \equiv 0 \mod (U(\mathfrak{k})X_2)$. This completes the proof of the lemma.

8.2. **An estimate of the Kostant degree.** Our next objective is to prove a theorem that gives a bound on the Kostant degree of the coefficients b_j of an element $b = b_m \otimes Z^m + \cdots + b_0$ in B. This bound will be the starting point of an inductive process that will lead to the proof of Theorem 4.5.

Theorem 8.21. *Let $u \in U(\mathfrak{k})$ be a nonzero dominant vector of weight n for the $\mathfrak{s}$-triple $\{H_1, X_1, X_{-1}\}$ and such that $\dot{X}_{-1}^{t+1}(u) \equiv 0 \mod (U(\mathfrak{k})X_2)$ for some $t \in \mathbb{N}_o$. Then*
(i) $n \leq 2t$,
(ii) if $t \leq n$ we have $u = vX_4^{n-t}$ where v is a dominant vector of weight $2t - n$ for the $\mathfrak{s}$-triple $\{H_1, X_1, X_{-1}\}$.

Proof. We proceed by induction on $t \geq 0$. If $t = 0$ we have $\dot{X}_{-1}(u) = wX_2$. Then applying $\dot{X}_1$ successively we obtain

$$nu = \dot{X}_1(w)X_2 + wE \tag{119}$$

and

$$0 = \dot{X}_1^k(w)X_2 + k\dot{X}_1^{k-1}(w)E + \frac{k(k-1)}{2}\dot{X}_1^{k-2}(w)X_4, \tag{120}$$

for all $k \geq 2$. If k is sufficiently large we have $\dot{X}_1^k(w) = 0$. But then from (120), by decreasing induction on k, we get that $w = 0$. Thus from (119) we obtain $n = 0$ which proves (i) in this case. On the other hand, since $n = t = 0$ (ii) holds.

Take now $t \geq 1$ and suppose that (i) and (ii) are true for $t - 1$, and that $\dot{X}_{-1}^{t+1}(u) = wX_2$. Also we may assume that $t < n$ since the statements we want to prove are obviously true for $t \geq n$. Then applying $\dot{X}_1$ successively we obtain

$$\dot{X}_1^{t+1}\dot{X}_{-1}^{t+1}(u) = \dot{X}_1^{t+1}(w)X_2 + (t+1)\dot{X}_1^{t}(w)E + \frac{(t+1)t}{2}\dot{X}_1^{t-1}(w)X_4, \tag{121}$$

and

$$0=\dot X_1^k(w)X_2+k\dot X_1^{k-1}(w)E+\frac{k(k-1)}{2}\dot X_1^{k-2}(w)X_4, \tag{122}$$

for all $k\geq t+2$. If k is sufficiently large we have $\dot X_1^k(w)=0$. But then from (122), by decreasing induction on k, we get that $\dot X_1^t(w)=0$. Thus from (121) and Lemma 8.8 we obtain $u=u'X_4$. It is clear that u' is a dominant vector of weight $n-2$ for the $\mathfrak{s}$-triple $\{H_1,X_1,X_{-1}\}$.

By induction on k it follows that

$$\dot X_{-1}^k(u)=\dot X_{-1}^k(u')X_4+2k\dot X_{-1}^{k-1}(u')E+2k(k-1)\dot X_{-1}^{k-2}(u')X_2. \tag{123}$$

Therefore

$$0\equiv\dot X_{-1}^k(u')X_4+2k\dot X_{-1}^{k-1}(u')E \qquad \mod (U(\mathfrak{k})X_2), \tag{124}$$

for all $k\geq t+1$. If k is sufficiently large we have $\dot X_{-1}^k(u')=0$. But then from (124), by decreasing induction on k, we get that $\dot X_1^t(u')\equiv 0 \mod (U(\mathfrak{k})X_2)$. Thus from the inductive hypothesis applied to u' we obtain that $n-2\leq 2(t-1)$ which is equivalent to (i). Also, since $t-1\leq n-2$ we get $u'=vX_4^{n-t-1}$ where v is a dominant vector of weight $2t-n$ for the $\mathfrak{s}$-triple $\{H_1,X_1,X_{-1}\}$. Hence $u=vX_4^{n-t}$ as we wanted to prove. This completes the proof of the theorem.

Next we shall need to consider the roots $\{\widetilde{\epsilon_2}\pm\widetilde{\epsilon_j}:3\leq j\leq n\}\subset\Delta^+(\mathfrak{k},\mathfrak{h}_{\mathfrak{k}})$. For each $\phi\in\{\widetilde{\epsilon_2}\pm\widetilde{\epsilon_j}:3\leq j\leq n\}$ we fix nonzero root vectors X_ϕ and $X_{-\phi}$. The proof of the following lemma follows by induction.

Lemma 8.22. *Let $Y\in\mathfrak{k}$ stand for any one of the following root vectors: X_1, X_{-2}, X_{-3}, $X_{-\delta}$ or $X_{-\phi}$ with $\phi\in\{\widetilde{\epsilon_2}\pm\widetilde{\epsilon_j}:3\leq j\leq n\}$. Then for every $0\leq k\leq\ell$ we have*

$$\dot Y^k(X_2^\ell)=wX_2^{\ell-k}, \tag{125}$$

for some $w\in U(\mathfrak{k})$.

Theorem 8.23. *Let $u\in U(\mathfrak{k})$ be a nonzero $\mathfrak{k}^+$-dominant vector of weight $\lambda=(i+\ell)(\gamma_4+\delta)+j\gamma_3$ where $i,j,\ell\in\mathbb{N}_o$. Let $V_{2(i+\ell),j}$ be the irreducible K-module generated by u and let $b\in V^M_{2(i+\ell),j}$. Then, if $u=vX_4^\ell$ with $v\in U(\mathfrak{k})$ we have*

$$\dot E^{2i+\ell+j+1}(b)\equiv 0 \qquad \mod (U(\mathfrak{k})X_2). \tag{126}$$

Proof. We shall first show that $\dot X_{-1}^{2(i+\ell)}(u)=aX_2^\ell$ for a nonzero vector $a\in U(\mathfrak{k})$. Let us observe that v and X_4^ℓ are, respectively, $\mathfrak{k}^+$-dominant vectors of weights $2i$ and 2ℓ with respect to the $\mathfrak{s}$-triple $\{H_1,X_1,X_{-1}\}$. Then, using Leibnitz's rule and the fact that

$$\dot X_{-1}^{2\ell}(X_4^\ell)=2^\ell(2\ell)!X_2^\ell \quad\text{and}\quad \dot X_{-1}^{2\ell+1}(X_4^\ell)=0,$$

we obtain

$$\begin{aligned}\dot X_{-1}^{2(i+\ell)}(u) &= \sum_{t=2\ell}^{2(i+\ell)} \tbinom{2(i+\ell)}{t} \dot X_{-1}^{2(i+\ell)-t}(v)\dot X_{-1}^{t}(X_4^\ell)\\ &= 2^\ell(2\ell)!\tbinom{2(i+\ell)}{2\ell}\dot X_{-1}^{2i}(v)X_2^\ell = aX_2^\ell,\end{aligned}$$

where $a \in U(\mathfrak{k})$ is nonzero.

If $\ell = 0$ in view of Proposition 8.7 (iv) we have $\dot E^{2i+j+1}(b) = 0$, hence (126) holds. Therefore from now on we shall assume that $\ell \geq 1$. Now from Proposition 8.9 (i) it follows that

$$\dot E^{2i+\ell+j+1}(b) = \sum_{r=0}^{\ell-1} w_r, \tag{127}$$

where w_r is a nonzero vector in $V_{2(i+\ell),j}$ of weight $\lambda_r = (i+\ell-r)(\delta-\gamma_4) + (2i+\ell+j+1)\gamma_3$. Our next objective is to show that $w_0 \equiv 0 \mod (U(\mathfrak{k})X_2)$.

Since γ_1 is a simple root in $\Delta^+(\mathfrak{k},\mathfrak{h}_\mathfrak{k})$ it follows that $\dot X_{-1}^{2(i+\ell)}(u)$ is annihilated by every positive root vector X_α with $\alpha \neq \gamma_1$. Then, since we also have $\dot X_{-1}\dot X_{-1}^{2(i+\ell)}(u) = 0$, we conclude that $\dot X_{-1}^{2(i+\ell)}(u)$ is a dominant vector in $V_{2(i+\ell),j}$ with respect to the positive system $s_{\gamma_1}\big(\Delta^+(\mathfrak{k},\mathfrak{h}_\mathfrak{k})\big)$, where s_{γ_1} is the reflection associated to the simple root γ_1. Recall that if $\{\phi_1,\dots,\phi_k\}$ denote the roots in $\Delta^+(\mathfrak{k},\mathfrak{h}_\mathfrak{k})$ different from γ_1 we have $s_{\gamma_1}\big(\Delta^+(\mathfrak{k},\mathfrak{h}_\mathfrak{k})\big) = \{-\gamma_1,\phi_1,\dots,\phi_k\}$.

It is now convenient to consider the following subsets of $\{\phi_1,\dots,\phi_k\}$.

$$\begin{aligned} I_1 &= \{\phi_1,\dots,\phi_{k_1}\} = \{\widetilde{\epsilon_i} \pm \widetilde{\epsilon_j} : 3 \leq i < j \leq n\} \cup \{2\widetilde{\epsilon_i} : 3 \leq i \leq n\},\\ I_2 &= \{\phi_{k_1+1},\dots,\phi_{k_2}\} = \{\widetilde{\epsilon_2} \pm \widetilde{\epsilon_j} : 3 \leq j \leq n\} \cup \{\delta,\gamma_2,\gamma_3\},\\ I_3 &= \{\phi_{k_2+1},\dots,\phi_{k}\} = \{\widetilde{\epsilon_0} \pm \widetilde{\epsilon_j} : 3 \leq j \leq n\} \cup \{\gamma_4\},\end{aligned}$$

where $1 < k_1 < k_2 < k$. For any $\phi \in \{\phi_1,\dots,\phi_k\}$ fix a nonzero root vector $X_{-\phi}$ corresponding to the root $-\phi$.

Since $w_0 \in V_{2(i+\ell),j}$ is of weight $\lambda_0 = (i+\ell)(\delta-\gamma_4) + (2i+\ell+j+1)\gamma_3$, we know that w_0 can be written as a linear combination of vectors of the following form

$$\dot X_{-\phi_k}^{a_k}\cdots \dot X_{-\phi_{k_2+1}}^{a_{k_2+1}}\dot X_1^b \dot X_{-\phi_{k_2}}^{a_{k_2}}\cdots \dot X_{-\phi_1}^{a_1}\big(\dot X_{-1}^{2(i+\ell)}(u)\big), \tag{128}$$

where the nonnegative integers $a_1,\dots,a_k$ and b are such that

$$\sum_{i=1}^{k} a_i\phi_i - b\gamma_1 = (\ell-1)\gamma_3. \tag{129}$$

In order to prove that $w_0 \equiv 0 \mod (U(\mathfrak{k})X_2)$ we are going to show that if the condition (129) is satisfied then any vector of the form (128) belongs to the ideal $U(\mathfrak{k})X_2$.

First of all we observe that if we take the scalar product with $\widetilde{\alpha_1} = \widetilde{\epsilon_1} - \widetilde{\epsilon_2}$ on both sides of (129) we obtain that

$$\sum_{i=k_1+1}^{k_2} a_i + b \leq \ell - 1. \tag{130}$$

On the other hand, in view of (73) there exists a constant $c \neq 0$ such that

$$\dot{X}_{-1}^{2(i+\ell)}(u) = c\dot{E}^{2(i+\ell)+j}(b).$$

Then, since for any $\phi \in I_1$ the root vector $X_{-\phi}$ commutes with E and belongs to $\mathfrak{m}$, for any integer $t \geq 1$ we have

$$\dot{X}_{-\phi}^t\big(\dot{X}_{-1}^{2(i+\ell)}(u)\big) = c\dot{E}^{2(i+\ell)+j}\dot{X}_{-\phi}^t(b) = 0.$$

Also for any $\phi \in I_3$ the derivation $\dot{X}_{-\phi}$ leaves the left ideal $U(\mathfrak{k})X_2$ invariant. Therefore, in order to show that any vector of the form (128) belongs to $U(\mathfrak{k})X_2$ if the condition (129) holds, it is enough to show that

$$\dot{X}_1^b\dot{X}_{-\phi_{k_2}}^{a_{k_2}} \cdots \dot{X}_{-\phi_{k_1+1}}^{a_{k_1+1}}\big(\dot{X}_{-1}^{2(i+\ell)}(u)\big) \in U(\mathfrak{k})X_2.$$

This follows from the fact that $\dot{X}_{-1}^{2(i+\ell)}(u) = aX_2^\ell$ with $a \in U(\mathfrak{k})$ by using Lemma 8.22 together with (130). This proves that $w_0 \equiv 0 \mod (U(\mathfrak{k})X_2)$.

Now it follows from (70) that there exists a nonzero constant c_r such that $w_r = c_r\dot{X}_4^r X_{-\delta}^r(w_0)$ for every $0 \leq r \leq \ell - 1$. Then, since $w_0 \equiv 0 \mod (U(\mathfrak{k})X_2)$ and the left ideal $U(\mathfrak{k})X_2$ is invariant under $\dot{X}_4$ and $\dot{X}_{-\delta}$ it follows that $w_r \equiv 0 \mod (U(\mathfrak{k})X_2)$ for every $0 \leq r \leq \ell - 1$. Hence in view of (127) the proof of the theorem is completed.

We are now in position to reach the advertised objective of obtaining a bound on the Kostant degree of an M-invariant element in $U(\mathfrak{k})$.

Theorem 8.24. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $b \in U(\mathfrak{k})^M$ be such that $\dot{E}^{m+1}(b) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$. Then $d(b) \leq 2m$.*

Proof. First of all we observe that in view of Proposition 8.7 we may decompose any $b \in U(\mathfrak{k})^M$ in a finite sum of the form

$$b = \sum b_{2i,j}, \tag{131}$$

where each $b_{2i,j}$ is an M-invariant element of type $(2i,j)$ uniquely determined by b. In order to prove that $d(b) \leq 2m$ we need to show that $b = \sum_{i+j\leq m} b_{2i,j}$, in fact, this implies $d(b) = \max\{d(b_{2i,j}) : b_{2i,j} \neq 0\} = \max\{2(i+j) : b_{2i,j} \neq 0\} \leq 2m$.

Let $t = \max\{j : b_{2i,j} \neq 0 \textit{ for some } i\}$ and set $r = \max\{i : b_{2i,t} \neq 0\}$. If $t \geq m+1$, since $\dot{E}^{m+1}(b) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ and the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ is invariant under the derivations $\dot{X}$ and $\dot{E}$, we get

$$\dot{X}^{2r}\dot{E}^t(b_{2r,t}) = \dot{X}^{2r}\dot{E}^t(b) \equiv 0 \qquad \mod (U(\mathfrak{k})\mathfrak{m}^+).$$

Hence from Proposition 8.7 (iv) and Corollary 8.19 it follows that $b_{2r,t} = 0$. Thus $t \le m$, in other words we have

$$b = \sum_{j \le m} b_{2i,j}.$$

Next set $s = \max\{2i + j : b_{2i,j} \neq 0\}$ and $p = [s/2]$. If $s \le m$ there is nothing to prove, hence we may assume that $s \ge m+1$. Since $\dot{E}^{m+1}(b) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ it follows from Proposition 8.7 (iv) that for every $0 \le k \le s-m-1$ we have

$$\sum_{\substack{2i+j=s \\ j \le m}} \dot{X}^{s-m-k-1} \dot{E}^{m+k+1}(b_{2i,j}) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+). \tag{132}$$

Now we multiply (132) by X^p on the right and then we change in the ith-term X^p by $X^{p-i}X_4^i$. Observe that this can be done because the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ is stable under right multiplication by X and $X_4 - X \in \mathfrak{m}^+$. Then (132) becomes

$$\sum_{\substack{2i+j=s \\ j \le m}} \dot{X}^{s-m-k-1} \dot{E}^{m+k+1}(b_{2i,j}) X^{p-i} X_4^i \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+). \tag{133}$$

Now we are going to apply Theorem 8.10 to the left hand side of (133). From (73) and from the fact that X and X_4 are $\mathfrak{k}^+$-dominant weight vectors, it follows that the left hand side of (133) is a vector in $U(\mathfrak{k})^{\mathfrak{q}^+}$ of weight $(s-m-k-1)\gamma_4 + (m+k+1)\gamma_3 + p\delta$. Then we have

$$\sum_{\substack{2i+j=s \\ j \le m}} \dot{X}^{s-m-k-1} \dot{E}^{m+k+1}(b_{2i,j}) X^{p-i} X_4^i \equiv 0 \mod (U(\mathfrak{k})X_2), \tag{134}$$

for every $0 \le k \le s-m-1$. Our next objective is to prove that

$$\dot{X}^{s-m-k-1} \dot{E}^{m+k+1}(b_{2i,j}) \equiv 0 \mod (U(\mathfrak{k})X_2), \tag{135}$$

for every $(2i, j)$ such that $2i + j = s$ and every $0 \le k \le s-m-1$. In order to do this we proceed by decreasing induction on k in the range $0 \le k \le s-m-1$.

Let $k = s-m-1$, then from (134) we get

$$\sum_{i=0}^{p} \dot{E}^s(b_{2i,s-2i}) X^{p-i} X_4^i \equiv 0 \mod (U(\mathfrak{k})X_2). \tag{136}$$

On the other hand from (72) it follows that $\dot{X}_{-1}\dot{E}^s(b_{2i,s-2i}) = 0$ for every $0 \le i \le p$. Also we have $\dot{X}_{-1}^{\ell}(X_4^{\ell}) \equiv 2^{\ell}\ell! E^{\ell}$ and $\dot{X}_{-1}^{\ell+1}(X_4^{\ell}) \equiv 0 \mod (U(\mathfrak{k})X_2)$. Then, since the left ideal $U(\mathfrak{k})X_2$ is stable under the derivation $\dot{X}_{-1}$, applying $\dot{X}_{-1}^{p}$ to (136) we obtain $\dot{E}^s(b_{2p,s-2p}) \equiv 0 \mod (U(\mathfrak{k})X_2)$. Next applying $\dot{X}_{-1}^{p-1}$ we obtain $\dot{E}^s(b_{2p-2,s-2p+2}) \equiv 0 \mod (U(\mathfrak{k})X_2)$. Continuing in this way we get that $\dot{E}^s(b_{2i,s-2i}) \equiv 0 \mod (U(\mathfrak{k})X_2)$ for every $0 \le i \le p$. This completes the proof of (135) for $k = s-m-1$.

Assume now that (135) holds for a fixed $0 < k \leq s-m-1$ and let us prove it for $k-1$. If we replace k by $k-1$ in (134) we obtain

$$\sum_{\substack{2i+j=s\\ j\leq m}} \dot{X}^{s-m-k}\dot{E}^{m+k}(b_{2i,j})X^{p-i}X_4^i \equiv 0 \qquad \text{mod } (U(\mathfrak{k})X_2). \tag{137}$$

Now it follows from (72) and from (135) that $\dot{X}_{-1}\dot{X}^{s-m-k}\dot{E}^{m+k}(b_{2i,j}) \equiv 0$ mod $(U(\mathfrak{k})X_2)$ for every $(2i,j)$ such that $2i+j=s$. Then applying appropriate powers of $\dot{X}_{-1}$ to (137), as we did in the first step of this inductive process, we get $\dot{X}^{s-m-k}\dot{E}^{m+k}(b_{2i,j}) \equiv 0 \mod (U(\mathfrak{k})X_2)$ for every $(2i,j)$ such that $2i+j=s$, which proves (135) for $k-1$. Hence (135) holds for all $0 \leq k \leq s-m-1$.

Taking $k=0$ and using (73) we get $\dot{X}_{-1}^{m+1-j}(u_{2i,j}) \equiv 0 \mod (U(\mathfrak{k})X_2)$ for every $(2i,j)$ such that $2i+j=s$. Therefore from Theorem 8.21 (i) we get that $i+j \leq m$ for every $(2i,j)$ such that $2i+j=s$, and from Theorem 8.21 (ii) we obtain that $u_{2i,j} = v_{2(m-j-i),j}X_4^{2i+j-m}$. Hence Theorem 8.23 implies that $\dot{E}^{m+1}(b_{2i,j}) \equiv 0 \mod (U(\mathfrak{k})X_2)$ for all $(2i,j)$ such that $2i+j=s$.

Finally if $b' = \sum_{2i+j=s} b_{2i,j}$ we have $\dot{E}^{m+1}(b-b') \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ and $b-b' = \sum_{2i+j<s} b_{2i,j}$, thus by decreasing induction on s it follows that $b = \sum_{i+j\leq m} b_{2i,j}$, which completes the proof of the theorem.

The next result follows directly from Theorem 8.5 and Theorem 8.24.

Corollary 8.25. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \geq 2$ and let $b = b_m \otimes Z^m + \cdots + b_0 \in B$. Then $d(b_r) \leq 2(2m-r)$ for every $0 \leq r \leq m$.*

8.3. **The main inductive argument.** From Corollary 8.25 we know, in particular, that $d(b_m) \leq 2m$. The purpose of this subsection is to improve this estimate to reach our main goal of proving that $d(b_m) \leq m$ for every $b = b_m \otimes Z^m + \cdots + b_0 \in B$. In order to do this we shall set up an inductive process which will lead to the proof of Theorem 4.5 from which our main result (Theorem 1.1) follows.

Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and set $d_r = 2m - r$ for every $0 \leq r \leq m$. Then, in view of (131) and Corollary 8.25, for each $0 \leq r \leq m$ we may write

$$b_r = \sum_{t=0}^{2d_r} \sum_{\max\{0,t-d_r\}\leq i\leq [t/2]} b^r_{2i,t-2i}, \tag{138}$$

where $b^r_{2i,t-2i}$ is an M-invariant element in $U(\mathfrak{k})$ of type $(2i, t-2i)$. To follow the incoming argument we find it convenient to have in mind the following array of the K-types of each b_r.

(139)

$$\begin{array}{llllllllllll}
b_r = b^r_{2d_r,0} & + & b^r_{2d_r-2,1} & + & b^r_{2d_r-4,2} & + & b^r_{2d_r-6,3} & + & \cdot\ \cdot\ \cdot & + & b^r_{0,d_r} \\
 & + & b^r_{2d_r-2,0} & + & b^r_{2d_r-4,1} & + & b^r_{2d_r-6,2} & + & \cdot\ \cdot\ \cdot & + & b^r_{0,d_r-1} \\
 & & & + & b^r_{2d_r-4,0} & + & b^r_{2d_r-6,1} & + & \cdot\ \cdot\ \cdot & + & b^r_{0,d_r-2} \\
 & & & & & + & b^r_{2d_r-6,0} & + & \cdot\ \cdot\ \cdot & + & b^r_{0,d_r-3} \\
 & & & & & & & & \cdot\ \cdot\ \cdot & & \cdot \\
 & & & & & & & & \ \ \cdot\ \cdot & & \cdot \\
 & & & & & & & & \ \ \ \ \cdot & & \cdot \\
 & & & & & & & & & + & b^r_{0,0}\ .
\end{array}$$

Observe that in this context the parameter t used in (138) may be regarded as a label for the skew diagonals of the array (139). More precisely, for $0 \le t \le 2d_r$ we may consider the set $\{b^r_{2i,t-2i} : \max\{0, t-d_r\} \le i \le [t/2]\}$ as the skew diagonal associated to t. Also note that the Kostant degree is constant along the rows of the array (139). In particular if we consider $r = m$ the Kostant degree takes the values $2m, 2m-2, \dots, 0$ from the top row of the array corresponding to b_m. Hence in order to prove that $d(b_m) \le m$ (see Theorem 4.5) we need to show that all the M-invariant elements that occur in the first $m/2$ rows if m is even, or the $[m/2]+1$ rows if m is odd, are equal to zero. To prove that the above mentioned K-types of b_m are equal to zero we will have to deal simultaneously with all the coefficients b_r, $0 \le r \le m$, of b. If we let T denote the label of the skew diagonals in the array corresponding to b_0, our approach will mainly consist in doing a decreasing induction on T in the range $m-1 \le T \le 4m$.

Let $T \in \mathbb{N}_o$ be as above and such that $m-1 \le T \le 4m$. We consider the propositional function $P(T)$ associated to $b \in B$ defined as follows,

$$P(T) : b_r = \sum_{t=0}^{\min\{T-r, 2d_r\}} \sum_{\max\{0,t-d_r\} \le i \le [t/2]} b^r_{2i,t-2i}, \qquad 0 \le r \le m. \tag{140}$$

Observe that $P(m-1)$ is true precisely when $b_m = 0$ and that, in view of Corollary 8.25 and (138), $P(4m)$ holds. This is the starting point of our argument.

Let H, X, Y and $\widetilde{Y} = Y + H$ be as in the beginning of this section. Recall that $[E, H] = -\frac{1}{2}E$, $[X, H] = 0$ and that $[E, X] = 0$. In the following lemma we prove some simple properties of the derivations $\dot{E}$ and $\dot{X}$.

Lemma 8.26. *(i)* $\dot{E}^k(H^k) = k!(-\frac{1}{2}E)^k$ *and* $\dot{E}^k(H^j) = 0$ *if* $k > j$.
(ii) $\dot{E}^k \varphi_k(H) = (-\frac{1}{2}E)^k$.
(iii) $\dot{X}^k((-\widetilde{Y})^k) = k!(-X)^k$ *and* $\dot{X}^k((-\widetilde{Y})^j) = 0$ *if* $k > j$.
(iv) $\dot{X}^k \varphi_k(a - \widetilde{Y}) = (-X)^k$ *for any* $a \in C$.

Proof. (i) The first statement will be prove by induction on k. If $k = 1$ the result follows from the choice of H, as we pointed out before. Now

$\dot{E}^k(H^k) = k!(-\frac{1}{2}E)^k$ implies that

$$\begin{aligned}\dot{E}^{k+1}(H^{k+1}) &= \dot{E}\dot{E}^k(H^kH) = \dot{E}\left(k!(-\frac{1}{2}E)^kH + k\dot{E}^{k-1}(H^k)(-\frac{1}{2}E)\right)\\ &= k!(-\frac{1}{2}E)^{k+1} + kk!(-\frac{1}{2}E)^{k+1} = (k+1)!(-\frac{1}{2}E)^{k+1}.\end{aligned}$$

The second assertion follows directly from the first.

(ii) This is a consequence of (i) and that $\varphi_k(H) = (k!)^{-1}H^k + \cdots$, where the dots stand for lower degree terms in H. In a similar way one proves (iii) and (iv).

Proposition 8.27. *Let $m \le T \le 4m$, $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and assume that $P(T)$ holds. Then for every (ℓ, n) such that $0 \le \ell, n$ and $\ell + n \le T$ we have*

$$(-1)^n\Sigma_1E^n - (-1)^\ell\Sigma_2E^\ell \equiv 0 \qquad \mathrm{mod}\ (U(\mathfrak{k})\mathfrak{m}^+), \tag{141}$$

where

$$\begin{aligned}\Sigma_1 &= \sum_{(i,r)\in I_1} A_{i,r}(T,n,\ell)\dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b_r)E^{r-i}X^{i-n},\\ \Sigma_2 &= \sum_{(i,r)\in I_2} A_{i,r}(T,\ell,n)\dot{X}^{T-n-i}\dot{E}^{n+i-r}(b_r)E^{r-i}X^{i-\ell},\end{aligned} \tag{142}$$

and

$$A_{i,r}(T,n,\ell) = (-\tfrac{1}{2})^{r-i}(-1)^{i-n}r!\tbinom{T-n-\ell}{i-n}\tbinom{\ell}{r-i},$$

$$I_1 = \{(i,r) \in N_0^2 : n \le i \le \min\{m, T-\ell\}, i \le r \le \min\{m, i+\ell\}\},$$

$$I_2 = \{(i,r) \in N_0^2 : \ell \le i \le \min\{m, T-n\}, i \le r \le \min\{m, i+n\}\}.$$

Proof. Let (ℓ, n) be such that $0 \le \ell, n$ and $\ell + n \le T$. If we apply $\dot{X}^{T-n-\ell}$ to $\epsilon(\ell, n)$ of Theorem 8.6 we obtain two sums Σ_1 and Σ_2 which will be analyzed separately. Using Leibnitz rule in the first sum of $\epsilon(\ell, n)$ we have

$$\Sigma_1 = \sum_{i,j}\tbinom{T-n-\ell}{j}\dot{X}^{T-n-\ell-j}\dot{E}^\ell(c_i)\dot{X}^j\varphi_{i-n}(\ell - \tfrac{n}{2} - \widetilde{Y}). \tag{143}$$

Next, using (67) and the fact that $\dot{X}(H) = 0$ we obtain

$$\dot{X}^{T-n-\ell-j}\dot{E}^\ell(c_i) = \sum_{i\le r\le m}\sum_s \tbinom{\ell}{s}\dot{X}^{T-n-\ell-j}\dot{E}^{\ell-s}(b_r)\dot{E}^s(t_{i,r}). \tag{144}$$

Now in view of (iv) of Lemma 8.26 we have $j \le i - n$ in (143). On the other hand, since $P(T)$ holds, in (144) we have $T - n - \ell - j + \ell - s \le \min\{T - r, 2d_r\} \le T - r$, and in view of Lemma 7.2 in (144) we also have $s \le r - i$. All these conditions imply that $j = i - n$ in (143) and $s = r - i$ in (144). Then the first sum Σ_1 becomes,

$$\Sigma_1 = \sum_{(i,r)\in I_1}(-\tfrac{1}{2})^{r-i}(-1)^{i-n}r!\tbinom{T-n-\ell}{i-n}\tbinom{\ell}{r-i}\dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b_r)E^{r-i}X^{i-n},$$

where

$$I_1 = \{(i,r) \in N_0^2 : n \le i \le \min\{m, T-\ell\}, i \le r \le \min\{m, i+\ell\}\}.$$

If we interchange n and ℓ we obtain Σ_2. On the other hand equation (141) follows from the fact that $\epsilon(\ell, n) \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$ (see Theorem 8.6). This completes the proof of the proposition.

Proposition 8.28. *Let $m \le T \le 4m$, $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and assume that $P(T)$ holds. Then for every (ℓ, n) such that $0 \le \ell, n$ and $\ell + n \le T$ we have*

$$(-1)^n \Sigma_1 E^n - (-1)^\ell \Sigma_2 E^\ell \equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+), \tag{145}$$

where

$$\Sigma_1 = \sum_{\substack{(i,r)\in I_1 \\ \max\{0,T-r-d_r\} \le k \le [\frac{T-r}{2}]}} A_{i,r}(T,n,\ell)\dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b^r_{2k,T-r-2k}) \times E^{r-i}X^{T-k}X_4^{k+i-n},$$

$$\Sigma_2 = \sum_{\substack{(i,r)\in I_2 \\ \max\{0,T-r-d_r\} \le k \le [\frac{T-r}{2}]}} A_{i,r}(T,\ell,n)\dot{X}^{T-n-i}\dot{E}^{n+i-r}(b^r_{2k,T-r-2k}) \times E^{r-i}X^{T-k}X_4^{k+i-\ell},$$

with the understanding that the K-types $b^r_{2k,T-r-2k}$ that do not occur in b_r are assumed to be zero. Moreover (145) has the advantage that all terms in the left hand side are weight vectors of weight $(2T-\ell-n)\gamma_1 + T(\gamma_2+\delta)$.

Proof. We first replace b_r in (142), $0 \le r \le m$, by what is obtained from the hypothesis (140):

$$b_r = \sum_{t=0}^{\min\{T-r, 2d_r\}} \sum_{\max\{0,t-d_r\} \le k \le [t/2]} b^r_{2k,t-2k}.$$

Using Proposition 8.7 (iv) the sums Σ_1 and Σ_2 simplify a bit because $\dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b^r_{2k,t-2k}) = 0$ unless $T-r \le t$, but on the other hand $t \le T-r$ which forces $t = T-r$. Thus we get

$$\Sigma_1 = \sum_{\substack{(i,r)\in I_1 \\ \max\{0,T-r-d_r\} \le k \le [\frac{T-r}{2}]}} A_{i,r}(T,n,\ell)\dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b^r_{2k,T-r-2k}) \times E^{r-i}X^{i-n},$$

$$\Sigma_2 = \sum_{\substack{(i,r)\in I_2 \\ \max\{0,T-r-d_r\} \le k \le [\frac{T-r}{2}]}} A_{i,r}(T,\ell,n)\dot{X}^{T-n-i}\dot{E}^{n+i-r}(b^r_{2k,T-r-2k}) \times E^{r-i}X^{i-\ell}.$$

Now we multiply both sums on the right by X^T and then we change in each term a certain number of X's by the same number of X_4's, so that Σ_1 and Σ_2 become weight vectors with respect to $\mathfrak{h}_\mathfrak{k}$ of weights $(2T-\ell-2n)\gamma_1+(T-n)\gamma_2+T\delta$ and $(2T-n-2\ell)\gamma_1+(T-\ell)\gamma_2+T\delta$, respectively. Observe that the equation (Proposition 8.27)

$$(-1)^n\Sigma_1E^n-(-1)^\ell\Sigma_2E^\ell\equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+), \tag{146}$$

is preserved under this change, because the left ideal $U(\mathfrak{k})\mathfrak{m}^+$ is invariant by right multiplication by X and $X\equiv X_4 \mod (U(\mathfrak{k})\mathfrak{m}^+)$. Thus we obtain the first part of the proposition. Moreover it is clear that all terms of $(-1)^n\Sigma_1E^n-(-1)^l\Sigma_2E^l$ are weight vectors with respect to $\mathfrak{h}_\mathfrak{k}$ of weight $(2T-\ell-n)\gamma_1+T(\gamma_2+\delta)$. This completes the proof of the proposition.

Observe that the equations (145) of Proposition 8.28 may be regarded as a system of linear equations where the unknowns $\dot X^{T-j-i}\dot E^{j+i-r}(b^r_{2k,T-r-2k})$ are certain derivatives of the K-types that occur in the $T-r$ skew diagonal of the coefficient b_r of b (see the array (139)). Since the unknowns in this system are in general not $\mathfrak{k}^+$-dominant we shall find it very convenient to replace this system by an equivalent one where all the unknowns become $\mathfrak{k}^+$-dominant vectors associated to the K-types $b^r_{2k,T-r-2k}$.

In order to do this we let $\widetilde\epsilon(\ell,n)$, for $0\le\ell,n$, denote the left hand side of equation (145) and for a fixed $0\le n\le\min\{2m,T\}$ we consider, for any $0\le L\le\min\{2m,T\}-n$, the following linear combination

$$\mathcal{E}_L(n)=\sum_{\ell=0}^{L}(-2)^\ell\tbinom{L}{\ell}\widetilde\epsilon(\ell,n)E^{L-\ell}X_4^{\ell+n}. \tag{147}$$

Observe that under the hypothesis of Proposition 8.28 we have $\mathcal{E}_L(n)\equiv 0 \mod (U(\mathfrak{k})\mathfrak{m}^+)$. We also set

$$\mathcal{E}^1_L(n)=\sum_{\ell=0}^{L}(-2)^\ell\tbinom{L}{\ell}\Sigma_1E^{L-\ell}X_4^{\ell+n} \quad \textit{and} \quad \mathcal{E}^2_L(n)=\textstyle\sum_{\ell=0}^{L}2^\ell\binom{L}{\ell}\Sigma_2X_4^{\ell+n}.$$

With this notation it is easy to see that

$$\mathcal{E}_L(n)=(-1)^n\mathcal{E}^1_L(n)E^n-\mathcal{E}^2_L(n)E^L. \tag{148}$$

To improve the system $\mathcal{E}_L(n)\equiv 0$ for $0\le n\le\min\{2m,T\}$ and $0\le L\le\min\{2m,T\}-n$ a bit more, we need to use the following lemmas.

Lemma 8.29. *For any $b,c,d\in\mathbb{N}$ we have*

$$\sum_{0\le j\le d}(-1)^j\binom{c+d}{j}\binom{b+d-j}{b}=\binom{b-c}{d}. \tag{149}$$

Proof. The proof of this lemma will be based on the following identity

$$\binom{m}{n}=\frac{1}{2\pi i}\oint\frac{(1+w)^m}{w^{n+1}}dw, \tag{150}$$

which holds for any $m, n \in \mathbb{N}_o$. Then

$$\begin{aligned}\sum_{0\le j\le d} &(-1)^j \tbinom{c+d}{j}\tbinom{b+d-j}{b} \\ &= \frac{1}{(2\pi i)^2}\oint\oint \sum_{0\le j}(-1)^j \frac{(1+w)^{c+d}(1+z)^{b+d-j}}{w^{j+1}z^{b+1}}dwdz \\ &= \frac{1}{(2\pi i)^2}\oint\oint \frac{(1+w)^{c+d}(1+z)^{b+d}}{wz^{b+1}}\sum_{0\le j}(-w(1+z))^{-j}dwdz,\end{aligned}$$

where the domain of integration is the torus $\{w : |w| = 4\} \times \{z : |z| = \frac{1}{2}\}$. Hence $|w(1+z)| \ge 2$, which implies that

$$\sum_{0\le j}(-w(1+z))^{-j} = \frac{w(1+z)}{1+w(1+z)}.$$

Then the first integral we have to compute gives

$$\frac{1}{2\pi i}\oint_{|w|=4}\frac{(1+w)^{c+d}}{1+w(1+z)}dw = \frac{z^{c+d}}{(1+z)^{c+d+1}},$$

since $\mathrm{R}es_{w=-(1+z)^{-1}}\left(\frac{(1+w)^{c+d}}{1+w(1+z)}\right) = \frac{z^{c+d}}{(1+z)^{c+d+1}}$. Therefore using (150) again we obtain

$$\begin{aligned}\sum_{0\le j\le d}(-1)^j\tbinom{c+d}{j}\tbinom{b+d-j}{b} &= \frac{1}{(2\pi i)}\oint_{|z|=\frac{1}{2}}\frac{(1+z)^{b+d}z^{c+d}}{z^{b+1}(1+z)^{c+d}}dz \\ &= \frac{1}{(2\pi i)}\oint_{|z|=\frac{1}{2}}\frac{(1+z)^{b-c}}{z^{b-c-d+1}}dz = \tbinom{b-c}{b-c-d} = \tbinom{b-c}{d},\end{aligned}$$

which completes the proof of the lemma.

Lemma 8.30. *Let G_o be locally isomorphic to $Sp(n,1)$ with $n \ge 2$ and let $b_{2i,j} \in U(\mathfrak{k})^M$ be an M-invariant element of type $(2i,j)$. For $0 \le k \le 2i$ set*

$$D_k(b_{2i,j}) = \Sigma_{\ell=0}^{k}(-2)^\ell\tbinom{k}{\ell}\tbinom{j+\ell}{\ell}^{-1}\dot{X}^{2i-\ell}\dot{E}^{j+\ell}(b_{2i,j})E^{k-\ell}X_4^\ell. \tag{151}$$

Then $D_k(b_{2i,j})$ is a $\mathfrak{k}^+$-dominant vector of weight $i(\gamma_4+\delta)+(j+k)\gamma_3$ with respect to $\mathfrak{h}_\mathfrak{k}$.

Proof. A set of simple roots in $\Delta^+(\mathfrak{k},\mathfrak{h}_\mathfrak{k})$ is $\{\delta,\gamma_1,\widetilde{\alpha_2},\dots,\widetilde{\alpha_n}\}$ (see (62)), hence it is enough to prove that $D_k(b_{2i,j})$ is annihilated by X, X_1 and $X_{\widetilde{\alpha_i}}$ for $2 \le i \le n$.

Using Proposition 8.7 (iv) and the fact that X commutes with E and X_4 it follows that $\dot{X}(D_k(b_{2i,j})) = 0$. Similarly, since $X_{\widetilde{\alpha_i}} \in \mathfrak{m}^+$ for $2 \le i \le n$, and because each one of these vectors commutes with X, E and X_4 we obtain that $\dot{X}_{\widetilde{\alpha_i}}(D_k(b_{2i,j})) = 0$.

Next we shall show that $\dot{X}_1(D_k(b_{2i,j})) = 0$. First of all we recall that from (71) we have

$$\dot{X}_1\dot{X}^{2i-\ell}\dot{E}^{j+\ell}(b_{2i,j}) = \frac{j+\ell}{2}\dot{X}^{2i-\ell+1}\dot{E}^{j+\ell-1}(b_{2i,j}), \tag{152}$$

for every $0 \leq \ell \leq 2i$. Then, since $\dot{X}_1(E) = X_4$ and $\dot{X}_1(X_4) = 0$, using (152) we obtain

$$\begin{aligned}
\dot{X}_1(D_k(b_{2i,j})) &= \sum_{\ell=0}^{k}(-2)^\ell\tbinom{k}{\ell}\tbinom{j+\ell}{\ell}^{-1}\tfrac{j+\ell}{2}\dot{X}^{2i-\ell+1}\dot{E}^{j+\ell-1}(b_{2i,j})E^{k-\ell}X_4^\ell \\
&\quad+\sum_{\ell=0}^{k}(-2)^\ell\tbinom{k}{\ell}\tbinom{j+\ell}{\ell}^{-1}(k-\ell)\dot{X}^{2i-\ell}\dot{E}^{j+\ell}(b_{2i,j})E^{k-\ell-1}X_4^{\ell+1} \\
&= \sum_{\ell=0}^{k-1}\Big[(-2)^{\ell+1}\tbinom{k}{\ell+1}\tbinom{j+\ell+1}{\ell+1}^{-1}\tfrac{j+\ell+1}{2}+(-2)^\ell\tbinom{k}{\ell}\tbinom{j+\ell}{\ell}^{-1}(k-\ell)\Big] \\
&\quad\times \dot{X}^{2i-\ell}\dot{E}^{j+\ell}(b_{2i,j})E^{k-\ell-1}X_4^{\ell+1} = 0,
\end{aligned}$$

since $\dot{X}^{2i+1}\dot{E}^{j-1}(b_{2i,j}) = 0$ and the bracket is also zero. That each term of $D_k(b_{2i,j})$ is of weight $i(\gamma_4+\delta)+(j+k)\gamma_3$ it is clear. This completes the proof of the lemma.

For a fixed $m \leq T \leq 4m$ in order to prove that $P(T)$ implies $P(T-1)$ we need to show that

$$b^r_{2i,T-r-2i} = 0 \quad \text{if} \quad 0 \leq T-r-2i \leq \min\big\{T, 4m-T\big\} - r, \tag{153}$$

for every $0 \leq r \leq m$.

For this purpose we introduce another inductive hypothesis $Q(n)$ define for $0 \leq n \leq \min\big\{T, 4m-T\big\}+1$ as follows: all types $b^r_{2i,j}$ on the skew diagonal $T-r$ of b_r with $j<n$ are zero for all $0 \leq r \leq m$. In other words

$$Q(n): \quad b^r_{2i,T-r-2i} = 0 \quad \text{if} \quad 0 \leq T-r-2i < n. \tag{154}$$

Observe that $Q(0)$ is obviously true. We also note that we already know that (154) holds if $T-2i > \min\big\{T, 4m-T\big\}$, see Corollary 8.25.

Theorem 8.31. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in B$ and take $m \leq T \leq 4m$ and $0 \leq n \leq \min\big\{T, 4m-T\big\}$. If $P(T)$ and $Q(n)$ are true then for all L such that $0 \leq L \leq \min\{2m, T\} - n$ we have*

$$\begin{aligned}
&\sum_{\substack{r,k \\ T-n\geq 2k+r\geq T-L}} B_{r,k}(T,n,L)D_{L+2k+r-T}(b^r_{2k,T-r-2k})(XX_4)^{T-k}E^n \\
&\quad - \sum_{\substack{r,\ell \\ r\equiv T-n}} (-2)^\ell\tbinom{L}{\ell}\tbinom{T-n-\ell}{r-\ell}u^r_{T-r-n,n}(XX_4)^{(T+r+n)/2}E^L \equiv 0,
\end{aligned} \tag{155}$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r}\dot{E}^n(b^r_{T-n-r,n})$, *the congruence is module the left ideal* $U(\mathfrak{k})\mathfrak{m}^+$ *and*

$$B_{r,k}(T,n,L) = r!(-1)^T 2^{T-r-2k}\tbinom{L}{T-r-2k}\tbinom{T-L-n}{r-n}. \tag{156}$$

Proof. We start from the linear combination $\mathcal{E}_L(n) = (-1)^n\mathcal{E}^1_L(n)E^n - \mathcal{E}^2_L(n)E^L$ (see (148)) of the equations (ℓ, n) given in Proposition 8.28.

We have

$$\begin{aligned}\mathcal{E}^1_L(n) =& \sum_{\ell=0}^{L}(-2)^\ell\tbinom{L}{\ell}\Sigma_1 E^{L-\ell}X_4^{\ell+n}\\ =& \sum_{i,r,k,\ell} r!(-2)^\ell(-\frac{1}{2})^{r-i}(-1)^{i-n}\tbinom{L}{\ell}\tbinom{T-n-\ell}{i-n}\tbinom{\ell}{r-i}\\ &\times \dot{X}^{T-\ell-i}\dot{E}^{\ell+i-r}(b^r_{2k,T-r-2k})E^{L+r-\ell-i}X^{T-k}X_4^{k+i+\ell}.\end{aligned} \tag{157}$$

If we change the index ℓ by $s = 2k+\ell+i-T$ we obtain

$$\begin{aligned}\mathcal{E}^1_L(n) =&(-1)^n\sum_{r,k,s} r!(-\frac{1}{2})^{r+2k-T-s}\\ &\times\Big(\sum_{n\le i\le r}(-1)^i\tbinom{L}{T+s-i-2k}\tbinom{2k+i-n-s}{i-n}\tbinom{T+s-i-2k}{r-i}\Big)\\ &\times \dot{X}^{2k-s}\dot{E}^{T+s-r-2k}(b^r_{2k,T-r-2k})E^{L+2k+r-T-s}X_4^s(XX_4)^{T-k}.\end{aligned} \tag{158}$$

To simplify the sum over i in the above expression we let $a = T+s-n-2k$, $b = 2k-s$, $c = L-a$, $d = r-\alpha$ and $j = i-n$. Then

$$\begin{aligned}&\sum_{n\le i\le r}(-1)^i\tbinom{L}{T+s-i-2k}\tbinom{2k+i-n-s}{i-n}\tbinom{T+s-i-2k}{r-i}\\ &\qquad\qquad=(-1)^n\sum_{0\le j\le d}(-1)^j\tbinom{L}{a-j}\tbinom{b+j}{j}\tbinom{a-j}{d-j}.\end{aligned}$$

But

$$\tbinom{L}{a-j}\tbinom{a-j}{d-j} = \tfrac{L!}{(L-a+d)!(a-d)!}\tbinom{L-a+d}{d-j}.$$

Therefore

$$\begin{aligned}&\sum_{n\le i\le r}(-1)^i\tbinom{L}{T+s-i-2k}\tbinom{2k+i-\alpha-s}{i-n}\tbinom{T+s-i-2k}{r-i}\\ &\qquad=\frac{(-1)^nL!}{(L-a+d)!(a-d)!}\sum_{0\le j\le d}(-1)^j\tbinom{L-a+d}{d-j}\tbinom{b+j}{j}\\ &\qquad=\frac{(-1)^{n+d}L!}{(L-a+d)!(a-d)!}\sum_{0\le j\le d}(-1)^j\tbinom{c+d}{j}\tbinom{b+d-j}{b}.\end{aligned}$$

Now using Lemma 8.29 and replacing a, b, c, d by their definitions we get

$$\begin{aligned}\sum_{n\le i\le r}(-1)^i\tbinom{L}{T+s-i-2k}\tbinom{2k+i-\alpha-s}{i-\alpha}\tbinom{T+s-i-2k}{r-i}&\\ =&\frac{(-1)^{n+d}L!}{(L-a+d)!(a-d)!}\tbinom{b-c}{d}\\ =&(-1)^r\tbinom{L}{T+s-2k-r}\tbinom{T-L-n}{r-n}\\ =&(-1)^r\tbinom{L}{T-2k-r}\tbinom{T-L-n}{r-n}\tbinom{L+2k+r-T}{s}\tbinom{T+s-2k-r}{s}^{-1}.\end{aligned}$$

Then if we go back to (158) and we use the definitions (151) and (156) we finally obtain

$$\begin{aligned}\mathcal{E}_L^1(n)=&(-1)^n\sum_{r,k,s}r!(-\tfrac{1}{2})^{r+2k-T-s}\\ &\times(-1)^r\tbinom{L}{T-2k-r}\tbinom{T-L-n}{r-n}\tbinom{L+2k+r-T}{s}\tbinom{T+s-2k-r}{s}^{-1}\\ &\times\dot{X}^{2k-s}\dot{E}^{T+s-r-2k}(b^r_{2k,T-r-2k})E^{L+2k+r-T-s}X_4^s(XX_4)^{T-k}\\ =&(-1)^n\sum_{r,k}r!(-\tfrac{1}{2})^{r+2k-T}(-1)^r\tbinom{L}{T-2k-r}\tbinom{T-L-n}{r-n}\\ &\times D_{L+2k+r-T}(b^r_{2k,T-2k-r})(XX_4)^{T-k}\\ =&(-1)^n\sum_{r,k}B_{r,k}(T,n,L)D_{L+2k+r-T}(b^r_{2k,T-r-2k})(XX_4)^{T-k}.\end{aligned}\tag{159}$$

From the second summand of (148) we obtain

$$\begin{aligned}\mathcal{E}_L^2(n)=&\sum_{\ell=0}^{L}2^\ell\tbinom{L}{\ell}\Sigma_2X_4^{\ell+n}\\ =&\sum_{i,r,k,\ell}r!2^\ell(-\tfrac{1}{2})^{r-i}(-1)^{i-\ell}\tbinom{L}{\ell}\tbinom{T-n-\ell}{i-\ell}\tbinom{n}{r-i}\\ &\times\dot{X}^{T-n-i}\dot{E}^{n+i-r}(b^r_{2k,T-r-2k})E^{r-i}X^{T-k}X_4^{k+i+n}.\end{aligned}$$

In the above sum, taking into account the hypothesis $Q(n)$, we have $T-r-2k\ge n$, $r\ge i$ and $T-n-i\le 2k$. Therefore $n\ge T-i-2k\ge T-r-2k\ge n$. Hence $i=r$ and $2k=T-r-n$. Thus

$$\mathcal{E}_L^2(n)=\sum_{\substack{r,\ell\\ r\equiv T-n}}(-2)^\ell\tbinom{L}{\ell}\tbinom{T-n-\ell}{r-\ell}u^r_{T-r-n,n}(XX_4)^{(T+r+n)/2},$$

where we put $u^r_{T-r-n,n}=r!(-1)^r\dot{X}^{T-n-r}\dot{E}^n(b^r_{T-n-r,n})$. This completes the proof of the theorem.

We are now in a good position to obtain from Theorem 8.31 the system of equations that we are looking for. For any T and n such that $m\le T\le 4m$

and $0 \le n \le \min\{T, 4m-T\}$ we consider the following sets,

(160)
$$\begin{aligned} L(T,n) &= \{L \in \mathbb{N}_0 : 0 \le L \le \min\{2m, T\} - n, \quad L \equiv n+1\}, \\ R(T,n) &= \{r \in \mathbb{N}_0 : 0 \le r \le \min\{m, \min\{T, 4m-T\} - n\},\ r \equiv T-n\}\,, \end{aligned}$$

where the congruence is $\bmod (2)$.

Let $|L(T,n)|$ and $|R(T,n)|$ denote the cardinality of these sets. In the following theorem we establish the system of equations that we shall work with from now on.

Theorem 8.32. *Let $b = b_m \otimes Z^m + \dots + b_0 \in B$ and take $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m-T\}$. If $P(T)$ and $Q(n)$ are true then for $L \in L(T,n)$ we have*

$$\sum_{r \in R(T,n)} \Big(\sum_{\ell} (-2)^{\ell} \tbinom{L}{\ell} \tbinom{T-n-\ell}{r-\ell} \Big) u^r_{T-r-n,n} (XX_4)^{(T+r+n)/2} = 0, \tag{161}$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r} \dot{E}^n (b^r_{T-n-r,n})$.

Proof. At this stage the proof follows by applying successively Theorem 8.31, Corollary 8.17, Lemma 8.20 and finally Proposition 8.18.

We observe that Theorem 8.32 gives a system of $|L(T,n)|$ linear equations in the $|R(T,n)|$ unknowns $u^r_{T-r-n,n}$. One of the main advantages of this system is that the unknowns are all $\mathfrak{k}^+$-dominant vectors corresponding to K-types on the $T-r$ skew diagonal of the coefficient b_r of b, see (139). Let $A(T,n)$ denote the coefficient matrix of this system. In the next subsection we are going to carry out a through study of this matrix.

Next we compute, for any $m \le T \le 4m$, the cardinality of the sets $L(T,n)$ and $R(T,n)$. As far as $L(T,n)$ is concerned it is easy to see that

(162)
$$2|L(T,n)| = \begin{cases} 2m - n + \frac{1}{2}(1-(-1)^n), & 2m < T \le 4m \\ T - n - m + \frac{1}{2}(1-(-1)^n) + \frac{1}{2}(1-(-1)^T), & m \le T \le 2m, \end{cases}$$

for any $0 \le n \le \min\{T, 4m-T\}$. On the other hand to compute $|R(T,n)|$ we need to consider two cases. If $0 \le n \le \min\{T, 4m-T\} - m$ we have

$$|R(T,n)| = \begin{cases} \left[\frac{m}{2}\right] + 1, & \text{if } T-n \equiv 0 \\ \left[\frac{m-1}{2}\right] + 1, & \text{if } T-n \equiv 1, \end{cases} \tag{163}$$

and for $\min\{T, 4m-T\} - m + 1 \le n \le \min\{T, 4m-T\}$ we get

$$2|R(T,n)| = \min\{T, 4m-T\} - n + 1 + \tfrac{1}{2}\big(1 + (-1)^{T-n}\big). \tag{164}$$

With this calculations at hand we can now compare the number of equations $|L(T,n)|$ with the number of unknowns $|R(T,n)|$ in the linear system of Theorem 8.32.

Lemma 8.33. *Let $m \geq 1$, $m \leq T \leq 4m$ and $0 \leq n \leq \min\{T, 4m - T\}$. Then if $m \leq T \leq 2m$, $T - m \leq n \leq T$ and $T \equiv n \equiv 0$ we have $|R(T,n)| = |L(T,n)| + 1$. In all other cases we get $|R(T,n)| \leq |L(T,n)|$.*

Proof. Let us assume first that $2m+1 \leq T \leq 4m$. In this case we have $0 \leq n \leq 4m - T$. We need to consider two cases. If $0 \leq n \leq 3m - T$ it follows from (162) and (163) that $|R(T,n)| \leq |L(T,n)|$. On the other hand if $3m - T + 1 \leq n \leq 4m - T$ and $T - n \equiv 0$ it follows from (162) and (164) that

$$2|L(T,n)| - 2|R(T,n)| = T - 2m - 2 + \tfrac{1}{2}\big(1 - (-1)^n\big) \geq 0,$$

for every T and n in the given ranges. If $T - n \equiv 1$ a similar calculation shows that $|R(T,n)| \leq |L(T,n)|$. Hence we conclude that for every $2m+1 \leq T \leq 4m$ and every $0 \leq n \leq 4m - T$ we have $|R(T,n)| \leq |L(T,n)|$.

We consider now $m \leq T \leq 2m$. Then, since $\min\{T, 4m - T\} = T$, it follows that $0 \leq n \leq T$. As before we need to consider two cases. Let us assume first that $0 \leq n \leq T - m$. If $T \equiv n \equiv 0$ it follows from (162) and (163) that

$$2|L(T,n)| - 2|R(T,n)| = \begin{cases} T - n - m - 2, & \text{if } m \equiv 0 \\ T - n - m - 1, & \text{if } m \equiv 1. \end{cases}$$

Hence if $0 \leq n < T - m$ we obtain $|R(T,n)| \leq |L(T,n)|$ and if $n = T - m$ we have $|R(T,n)| = |L(T,n)| + 1$. On the other hand a similar calculation shows that if $T \equiv n \equiv 1$, or if $T - n \equiv 1$ we have $|R(T,n)| \leq |L(T,n)|$.

Next we consider $T - m + 1 \leq n \leq T$. In this case it follows from (162) and (164) that

$$2|L(T,n)| - 2|R(T,n)| = -1 + \tfrac{1}{2}\big(1 - (-1)^n\big) + \tfrac{1}{2}\big(1 - (-1)^T\big) - \tfrac{1}{2}\big(1 + (-1)^{T-n}\big).$$

Hence, if $T \equiv n \equiv 0$ we have $|R(T,n)| = |L(T,n)| + 1$, and in all other cases we get $|R(T,n)| = |L(T,n)|$. This completes the proof of the lemma.

8.4. **The coefficient matrix.** Let $A(T,n)$ denote the coefficient matrix of the system given by Theorem 8.32. Our next goal is to study the matrix $A(T,n)$ as thoroughly as possible. For this purpose we shall consider a generalized version of it.

Given a sequence of integers $0 \leq L_0 < \cdots < L_k$ and $\delta = 0, 1$ we consider the $(k+1) \times (k+1)$ matrix $A(s)$ with polynomial entries $A_{i,j}(s) \in \mathbb{C}[s]$ defined as follows

$$A_{ij}(s) = \sum_{0 \leq \ell \leq \min\{L_i, 2j+\delta\}} (-2)^\ell \binom{L_i}{\ell} \binom{s - \ell}{2j + \delta - \ell}, \tag{165}$$

where for $m > 0$,

$$\binom{s-\ell}{m} = \frac{(s-\ell)(s-\ell-1)\cdots(s-\ell-m+1)}{m!} \quad \textit{and} \quad \binom{s-\ell}{0} = 1.$$

Our first objective will be to determine the degree of the polynomial $\det A(s)$. To obtain this result we shall need to use the following lemmas.

Lemma 8.34. *Let $(i_0, i_1, \ldots, i_k)$ be a $(k+1)$-tuple of integers such that $i_j \leq 2j+\delta$ for $j = 0, \ldots, k$ and $i_0+\cdots+i_k > (k+\delta)(k+\delta+1)/2$. Then there exists a pair of indexes a, b such that $0 \leq a < b \leq k$ and $i_b - i_a = 2(b-a)$.*

Proof. Let $t_j = 2j+\delta-i_j \geq 0$. Hence $t_0+\cdots+t_k < (k+\delta)(k+1-\delta)/2 = k(k+1)/2$. Then there are two indexes a, b such that $0 \leq a < b \leq k$ and $t_a = t_b$, because the sum of $k+1$ different nonnegative integers is greater or equal to $k(k+1)/2$. Thus $i_b - i_a = 2(b-a)$ as asserted.

Lemma 8.35. *Given a sequence of integral numbers $0 \leq L_0 \leq \cdots \leq L_k$ and $\delta = 0, 1$ let N and D denote the $(k+1)\times(k+1)$ matrices defined as follows: for $0 \leq i, j \leq k$ we set $N_{ij} = 0$ if $j > 2i+\delta$ and $N_{ij} = 1/(2i+\delta-j)!$ in all the other cases, and $D_{ij} = \binom{L_i}{j}$. Then*

$$\det D = \prod_{j=0}^{k} \frac{1}{j!} \prod_{0\leq i<j\leq k} (L_i - L_j),$$

$$\det N = 2^{(k+\delta)(k+\delta+1)/2} \Big(\prod_{s=\delta}^{k+\delta} s!\Big)\Big(\prod_{r=\delta}^{k+\delta} \frac{1}{(2r)!}\Big).$$

Proof. We begin by computing $\det D$. Let D' be the matrix defined by $D'_{ij} = L_i(L_i-1)\cdots(L_i-j+1)$ for $0 \leq i, j \leq k$. Then

$$\det D = \Big(\prod_{j=0}^{k} \frac{1}{j!}\Big) \det D'.$$

If we look closely at the columns of D' and use the multilinearity of the determinant as a function of the columns of a matrix we realize that $\det D'$ is equal to the determinant of the transpose of a Van Dermonde matrix with second row equal to $(L_0, L_1, \ldots, L_k)$. Thus $\det D' = \prod_{0\leq i<j\leq k}(L_j - L_i)$.

Now let $M_\delta = (M_{rs})$ be the matrix introduced in Proposition 7.10. If we make the change of indexes $i = r-\delta$, $j = s-\delta$ we see that $N_{ij} = M_{rs} s!/(2r)!$. From this the second assertion in the lemma follows directly from Proposition 7.10.

Before stating the next result we find it convenient to introduce the following notation: for any $p \in \mathbb{C}[s]$ and $i \in \mathbb{N}$ we set $(p)_i = p(p+1)\cdots(p+i-1)$, also set $(p)_0 = 1$.

Proposition 8.36. *For any sequence of integers $0 \leq L_0 < \cdots < L_k$ and $\delta = 0, 1$ let $A(s)$ be the $(k+1)\times(k+1)$ matrix defined in* (165)*. Then*

$$\det A(s) = c s^{(k+\delta)(k+\delta+1)/2} + \cdots,$$

where the dots stand for lower degree terms in s and the leading coefficient is given by

$$c = (-2)^{k(k+1)/2} (\det N)(\det D).$$

Proof. For $0 \leq j \leq k$ let $A^j(s)$ denote the j-column of the matrix $A(s)$. It follows from the definition of $A(s)$ that

$$A^j(s) = \sum_{\ell=0}^{2j+\delta} (s-2j-\delta+1)_\ell B^j_\ell,$$

where B^j_ℓ is the constant column vector whose i-entry is $(-2)^{2j+\delta-\ell}\binom{L_i}{2j+\delta-\ell}\ell!$. Using the multilinearity of the determinant as a function of the columns of a matrix, we have

$$\begin{aligned}
\det A(s) &= \det\Big(A^0(s), A^1(s), \ldots, A^k(s)\Big) \\
&= \det\Big(\sum_{i_0=0}^{\delta}(s-\delta+1)_{i_0}B^0_{i_0}, \ldots, \sum_{i_k=0}^{2k+\delta}(s-2k-\delta+1)_{i_k}B^k_{i_k}\Big) \\
&= \sum_{\substack{i_0,\ldots,i_k \\ 0\leq i_j\leq 2j+\delta}} (s-\delta+1)_{i_0}\cdots(s-2k-\delta+1)_{i_k}\det\Big(B^0_{i_0},\ldots,B^k_{i_k}\Big).
\end{aligned}$$

Now, if $i_0+\cdots+i_k > (k+\delta)(k+\delta+1)/2$ it follows from Lemma 8.34 that there exists a pair of indexes a, b such that $0 \leq a < b \leq k$ and $i_b - i_a = 2(b-a)$. Hence $\binom{L_i}{2a+\delta-i_a} = \binom{L_i}{2b+\delta-i_b}$ and the column vectors $B^a_{i_a}$ and $B^b_{i_b}$ turn out to be proportional. Therefore

$$\begin{aligned}
\det A(s) = &\sum_{\substack{0\leq i_j\leq 2j+\delta \\ i_0+\cdots+i_k\leq(k+\delta)(k+\delta+1)/2}} (s-\delta+1)_{i_0}\cdots(s-2k-\delta+1)_{i_k} \\
&\times \det\Big(B^0_{i_0},\ldots,B^k_{i_k}\Big).
\end{aligned}$$

Hence, since the degree of $(s-\delta+1)_{i_0}\cdots(s-2k-\delta+1)_{i_k}$ is $i_0+\cdots+i_k$, it follows that the degree of $\det A(s)$ is less or equal to $(k+\delta)(k+\delta+1)/2$ and that the leading coefficient is given by

$$c = \sum_{\substack{0\leq i_j\leq 2j+\delta \\ i_0+\cdots+i_k=(k+\delta)(k+\delta+1)/2}} \det\Big(B^0_{i_0},\ldots,B^k_{i_k}\Big).$$

We can reparametrize the constant column vector $B^j_{i_j}$ in terms of the parameter $t_j = 2j+\delta-i_j$. In other words let $C^j_{t_j}$ be the constant column vector whose i-entry is $(-2)^{t_j}\binom{L_i}{t_j}/(2j+\delta-t_j)!$. Then

$$c = \sum_{\substack{0\leq t_j\leq 2j+\delta \\ t_0+\cdots+t_k=k(k+1)/2}} \det\Big(C^0_{t_0},\ldots,C^k_{t_k}\Big).$$

If $t_i = t_j$ then $C^i_{t_i}$ and $C^j_{t_j}$ are proportional. Therefore we may assume that in the above sum $t_j = \sigma(j)$, where σ is an element of the permutation group

S_{k+1} of the set $\{0,1,\dots,k\}$. Thus

$$c=\sum_{\substack{\sigma\in S_{k+1}\\ \sigma(j)\le 2j+\delta}} \det\left(C^0_{\sigma(0)},\dots,C^k_{\sigma(k)}\right).$$

Now if we let D_j denote the column vector whose i-entry is $\binom{L_i}{j}$, we have

$$C^j_{\sigma(j)}=\frac{(-2)^{\sigma(j)}}{(2j+\delta-\sigma(j))!}D_{\sigma(j)}.$$

Therefore using Lemma 8.35 we obtain

$$\begin{aligned} c&=(-2)^{k(k+1)/2}\Big(\sum_{\substack{\sigma\in S_{k+1}\\ \sigma(j)\le 2j+\delta}} \operatorname{sign}(\sigma)\prod_{j=0}^{k}\frac{1}{(2j+\delta-\sigma(j))!}\Big)\det(D_0,\dots,D_k)\\ &=(-2)^{k(k+1)/2}(\det N)(\det D). \end{aligned}$$

This completes the proof of the proposition.

Next we go on to find enough roots of $\det A(s)$ as to factor it into a product of simple polynomials. For this purpose the corollary of the following lemma will be useful. We recall that we use the convention of considering the combinatorial numbers $\binom{p}{q}$ as defined for all $p,q\in\mathbb{Z}$ by

$$\binom{p}{q}=\begin{cases}\frac{p!}{q!(p-q)!} & \text{for } 0\le q\le p,\\ 0 & \text{in all other cases.}\end{cases}$$

Lemma 8.37. *If a,b,c are nonnegative integers, then*

$$\sum_{\ell}(-2)^{\ell}\binom{a}{\ell}\binom{a+b-\ell}{c-\ell}=\sum_{\ell}(-1)^{\ell}\binom{a}{\ell}\binom{b}{c-\ell}.$$

Proof. Using the identity (150) we have,

$$\begin{aligned} &\sum_{\ell}(-2)^{\ell}\binom{a}{\ell}\binom{a+b-\ell}{c-\ell}\\ &\qquad=\frac{1}{(2\pi i)^2}\oint\oint\sum_{0\le\ell}(-2)^{\ell}\frac{(1+z)^a(1+w)^{a+b-\ell}}{z^{\ell+1}w^{c-\ell+1}}dzdw\\ &\qquad=\frac{1}{(2\pi i)^2}\oint\oint\frac{(1+z)^a(1+w)^{a+b}}{zw^{c+1}}\sum_{0\le\ell}\left(\frac{-2w}{z(1+w)}\right)^{\ell}dzdw\\ &\qquad=\frac{1}{(2\pi i)^2}\oint\oint\frac{(1+z)^a(1+w)^{a+b+1}}{w^{c+1}(z(1+w)+2w)}dzdw. \end{aligned}$$

We take as domain of integration the torus $\{z:|z|=3\}\times\{w:|w|=\frac12\}$, where the geometric series converges absolutely and uniformely. Now

$$\frac{1}{2\pi i}\oint_{|z|=3}\frac{(1+z)^a}{z(1+w)+2w}dz=\frac{(1-w)^a}{(1+w)^{a+1}},$$

since $\mathrm{R}es_{z=-2w(1+w)^{-1}}\left(\frac{(1+z)^a}{z(1+w)+2w}\right) = \frac{(1-w)^a}{(1+w)^{a+1}}$. Therefore

$$\sum_\ell (-2)^\ell \binom{a}{\ell}\binom{a+b-\ell}{c-\ell} = \frac{1}{(2\pi i)}\oint_{|w|=\frac{1}{2}} \frac{(1-w)^a(1+w)^b}{w^{c+1}}dw.$$

To compute $\mathrm{R}es_{w=0}\left(\frac{(1-w)^a(1+w)^b}{w^{c+1}}\right)$ we write

$$\frac{(1-w)^a(1+w)^b}{w^{c+1}} = \frac{1}{w^{c+1}}\sum_{\ell,k}\binom{a}{\ell}\binom{b}{k}(-w)^\ell w^k,$$

which gives

$$\sum_\ell (-2)^\ell \binom{a}{\ell}\binom{a+b-\ell}{c-\ell} = \sum_\ell (-1)^\ell \binom{a}{\ell}\binom{b}{c-\ell}.$$

This completes the proof of the lemma.

Corollary 8.38. *If a, b, c are nonnegative integers, then*

$$\sum_\ell (-2)^\ell \binom{a}{\ell}\binom{a+b-\ell}{c-\ell} = (-1)^c \sum_\ell (-2)^\ell \binom{b}{\ell}\binom{a+b-\ell}{c-\ell}.$$

Theorem 8.39. *Given a sequence of integers $0 \le L_0 < L_1 < \cdots < L_k$ consider the set $R = \{L_i + L_j : 0 \le i < j \le k\}$ and for any $r \in R$ let*

$$m(r) = |\{(i,j) : 0 \le i < j \le k,\ r = L_i + L_j\}|.$$

Then
(i) If $\delta = 0$,

$$\det A(s) = c\prod_{r\in R}(s-r)^{m(r)}.$$

(ii) If $\delta = 1$,

$$\det A(s) = c\prod_{i=0}^{k}(s-2L_i)\prod_{r\in R}(s-r)^{m(r)}.$$

Here c is the same constant as in Proposition 8.36.

Proof. Let $A_i(s)$ denote the i-row of the matrix $A(s)$ and let r be any non negative integer. Then from Corollary 8.38 we obtain

$$\begin{aligned} A_{i,j}(r) &= \sum_\ell (-2)^\ell \binom{L_i}{\ell}\binom{r-\ell}{2j+\delta-\ell} \\ &= (-1)^\delta \sum_\ell (-2)^\ell \binom{r-L_i}{\ell}\binom{r-\ell}{2j+\delta-\ell} = (-1)^\delta A_{r(i),j}(r), \end{aligned}$$

where $0 \le r(i) \le k$ is such that $L_{r(i)} = r - L_i$. For a fix $r \in R$ let us write $A_i(s) = A_i(r) + (s-r)B_i(s)$ where $B_i(s)$ is a row vector with coefficients in $\mathbb{C}[s]$ and set $m = m(r)$. Suppose we have indexes $0 \le a_1 < \cdots < a_m < b_m < \cdots < b_1 \le k$ such that $L_{b_j} = r - L_{a_j}$ for $1 \le j \le m$. Then by induction on

j we shall prove that $\det A(s) = (s-r)^{m(r)} f(s)$ for some $f(s) \in \mathbb{C}[s]$. For $1 \le j \le m(r)$ let $P(j)$ be the following propositional function:

$$\det A(s) = (s-r)^{j-1} F_{j-1}(A_0(s), \dots, A_{a_j}(s), \dots, A_{b_j}(s), \dots, A_k(s)),$$

where F_{j-1} is a multilinear alternating function on $k+3-2j$ variables (those corresponding to $a_1, \dots, a_{j-1}, b_{j-1}, \dots, b_1$ are missing) with values in $\mathbb{C}[s]$. Then $P(1)$ is obviously true. If $P(j)$ is true for $1 \le j < m$, then

$$\begin{aligned}\det A(s) =&(s-r)^{j-1}\\ &\times F_{j-1}(\dots, A_{a_j}(r) + (s-r)B_{a_j}(s), \dots, A_{b_j}(r) + (s-r)B_{b_j}(s), \dots)\\ =&(s-r)^{j-1}\big[(s-r)F_{j-1}(\dots, A_{a_j}(r), \dots, B_{b_j}(s), \dots)\\ &+ (s-r)F_{j-1}(\dots, B_{a_j}(s), \dots, A_{b_j}(r), \dots)\\ &+ (s-r)^2 F_{j-1}(\dots, B_{a_j}(s), \dots, B_{b_j}(s), \dots)\big]\\ =&(s-r)^j F_j(\dots, A_{a_{j+1}}(s), \dots, A_{b_{j+1}}(s), \dots),\end{aligned}$$

where F_j is a multilinear alternating function on $k+1-2j$ variables (those corresponding to the indexes $a_1, \dots, a_j, b_j, \dots, b_1$ are missing) with values in $\mathbb{C}[s]$. Hence $P(j+1)$ is also true. Therefore $P(m(r))$ is true. Since $\mathbb{C}[s]$ is a unique factorization domain it follows that

$$\det A(s) = c(s) \prod_{r \in R} (s-r)^{m(r)},$$

where $c(s) \in \mathbb{C}[s]$. Now since $\sum_{r \in R} m(r) = |\{(i,j) : 0 \le i < j \le k\}| = k(k+1)/2$, it follows from Proposition 8.36 that when $\delta = 0$ we obtain $c(s) = c \in \mathbb{C}$ which proves part (i) of the theorem.

When $\delta = 1$ we also obtain from Corollary 8.38 that $A_i(s) = (s-2L_i)A_i'(s)$ for $0 \le i \le k$. In fact,

$$A_{ij}(2L_i) = \sum_{\ell} (-2)^{\ell} \binom{L_i}{\ell} \binom{2L_i - \ell}{2j+1-\ell} = -\sum_{\ell} (-2)^{\ell} \binom{L_i}{\ell} \binom{2L_i - \ell}{2j+1-\ell}$$

says that $A_{ij}(2L_i) = 0$. Then, for $r \in R$ and $1 \le j \le m(r)$ we can change the propositional function $P(j)$ introduced before by

$$\begin{aligned}\det A(s) =&(s-r)^{j-1} \left(\prod_{i=0}^{k} (s-2L_i) \right)\\ &\times F_{j-1}(A_0'(s), \dots, A_{a_j}'(s), \dots, A_{b_j}'(s), \dots, A_k'(s)).\end{aligned}$$

Hence when we write $A_i'(s) = A_i'(r) + (s-r)B_i'(s)$, from $A_{a_j}(r) = -A_{b_j}(r)$ we get

$$(r - 2L_{a_j})A_{a_j}'(r) = -(r - 2L_{b_j})A_{b_j}'(r),$$

which implies that $A'_{a_j}(r)$ and $A'_{b_j}(r)$ are linearly dependent. As before this implies that $P(m(r))$ is true. Therefore

$$\det A(s) = c(s)\prod_{i=0}^{k}(s-2L_i)\prod_{r\in R}(s-r)^{m(r)},$$

for some $c(s)\in\mathbb{C}[s]$. But we have $k+1+k(k+1)/2=(k+1)(k+2)/2$ simple factors, so Proposition 8.36 implies that $c(s)=c\in\mathbb{C}$. This completes the proof of the theorem.

We are particularly interested in the sequence $L_i=2i+\epsilon$ for $0\le i\le k$ and $\epsilon\in\{0,1\}$. In this case it is easy to see that $R=\{2(\epsilon+j):1\le j\le 2k-1\}$ if $k\ge 1$ and $R=\emptyset$ if $k=0$. On the other hand, if $k\ge 1$ and $2\nu\in R$ the multiplicity of 2ν as a root of $\det A(s)$ is given by

$$m(2\nu)=\begin{cases}\left[\frac{\nu+1-\epsilon}{2}\right], & \text{if } 1+\epsilon\le\nu\le k+\epsilon\\ \left[\frac{2k+1+\epsilon-\nu}{2}\right], & \text{if } k+\epsilon+1\le\nu\le 2k+\epsilon-1.\end{cases}\tag{166}$$

For q and k nonnegative integers we let $A(q)$ denote the $(k+1)\times(k+1)$ matrix obtain from $A(s)$ by evaluating at $s=q$. Then, from Theorem 8.39 we obtain the following corollary.

Corollary 8.40. *If $\epsilon,\delta\in\{0,1\}$, $k\ge 1$ and $L_i=2i+\epsilon$ for $0\le i\le k$ the matrix $A(q)$ is nonsingular if and only if $q\ge 2k+\delta$ and $q\ne 2k,2k+2,\dots,4k+2(\epsilon+\delta-1)$.*

Proof. If $q<2k+\delta$ then $\binom{q-\ell}{2k+\delta-\ell}=0$ for all ℓ, hence the k-column of $A(q)$ is zero and $A(q)$ is singular. When $q\ge 2k+\delta$ Theorem 8.39 implies that $A(q)$ is nonsingular if and only if $q\notin\{2L_i:0\le i\le k\}\cup\{L_i+L_j:0\le i<j\le k\}=\{2(\epsilon+j):1-\delta\le j\le 2k+\delta-1\}$. Hence the corollary follows.

Remark. When $k=0$ the following cases arise: (i) if $(\epsilon,\delta)=(0,0)$ *or* $(1,0)$, then $A(q)$ is non singular for every $q\ge 0$; (ii) if $(\epsilon,\delta)=(0,1)$, then $A(q)$ is non singular if and only if $q\ge 1$; (iii) if $(\epsilon,\delta)=(1,1)$, then $A(q)$ is non singular if and only if $q\ge 1$ and $q\ne 2$.

8.5. **The final stage.** We are now in a good position to start proving Theorem 4.5. To do this we need to show that if $b=b_m\otimes Z^m+\cdots+b_0\in B$, $b_m\ne 0$, then $d(b_m)\le m$ and m is even.

We begin by making an important observation on which our proof will rely heavily. If $b=b_m\otimes Z^m+\cdots+b_0\in B$ we know from (138) that for every $0\le r\le m$ we have

$$b_r=\sum_{t=0}^{2d_r}\sum_{\max\{0,t-d_r\}\le i\le[\frac{t}{2}]} b^r_{2i,t-2i},\tag{167}$$

where $b^r_{2i,t-2i}$ is an M-invariant element in $U(\mathfrak{k})$ of type $(2i, t-2i)$. Set $p = 2[m/2]$ and define

$$c_p = \sum_{t=0}^{p} \sum_{\max\{0,t-d_p\} \le i \le [\frac{t}{2}]} b^p_{2i,t-2i}.$$

Clearly $c_p \in U(\mathfrak{k})^M$ and a simple calculation shows that $d(c_p) \le p$. In fact, c_p contains all the K-types of Kostant degree smaller or equal to p that occur in b_p. Now, since p is even $c_p \otimes Z^p \in \big(U(\mathfrak{k})^M \otimes U(\mathfrak{a})\big)^W$ and therefore, by Proposition 4.4, $c_p \otimes Z^p$ is the leading term of an element $b'_p = c_p \otimes Z^p + \cdots \in P(\mathrm{U}(\mathfrak{g})^K) \subset B$. Next let us define $b^p = b - b'_p \in B$. Then all the K-types that occur in the p-coefficient of b^p have Kostant degree greater than p. Now by looking at the $(p-2)$-coefficient of b^p we can construct in a similar way an element $b'_{p-2} \in P(\mathrm{U}(\mathfrak{g})^K)$ such that the coefficients of $b^{p-2} = b^p - b'_{p-2}$ corresponding to degrees greater than $p-2$ are the same as those of b^p, and all the K-types that occur in the $(p-2)$-coefficient of b^{p-2} have Kostant degree greater than $p-2$. Continuing in this way we can define inductively a sequence $b^p, b^{p-2} \dots, b^0$ of elements of degree at most m in B such that $\widetilde{b} = b^0$ has the property that the K-types that occur in all the even coefficients $\widetilde{b}_{2k}$ of $\widetilde{b}$ have Kostant degree greater than $2k$, and moreover if m is odd $\widetilde{b}_m = b_m$ and if m is even then $d(b_m - \widetilde{b}_m) \le m$.

Now let us consider the linear subspace $\widetilde{B}$ of B consisting of all elements $b \in B$ such that, the K-types $b^{2r}_{2i,j}$ that occur in the $2r$-coefficient of b have Kostant degree greater than $2r$ for all r with $0 \le 2r \le m$. Thus

$$\widetilde{B} = \{b \in B : b^{2r}_{2i,j} = 0 \text{ if } i + j \le r \text{ and } 0 \le 2r \le \deg(b)\}. \tag{168}$$

Then when G_o is locally isomorphic to $\mathrm{Sp}(n, 1)$ we have

Proposition 8.41. *Theorem 4.5 holds if and only if $\widetilde{B} = 0$.*

Proof. Suppose first that Theorem 4.5 holds and let $0 \ne b \in \widetilde{B}$ be an element of degre m. Then we know that m is even and that $d(b_m) \le m$. But on the other hand $b \in \widetilde{B}$ implies that all K-types that occur in b_m have Kostant degree greater than m. Therefore $b_m = 0$ which is a contradiction, thus $\widetilde{B} = 0$.

Conversely, suppose that $\widetilde{B} = 0$ and let $0 \ne b \in B$ be an element of degree m. If m is odd there exists $0 \ne \widetilde{b} \in \widetilde{B}$ of degree m such that $\widetilde{b}_m = b_m$. This contradicts the hypothesis $\widetilde{B} = 0$. Therefore m is even, in this case we know that there exists $0 \ne \widetilde{b} \in \widetilde{B}$ of degree at most m such that $d(b_m - \widetilde{b}_m) \le m$. But since $\widetilde{b} = 0$ we conclude that $d(b_m) \le m$ and the proposition follows.

The advantage of working with $\widetilde{b} \in \widetilde{B}$ instead of $b \in B$ is that the coefficients of $\widetilde{b}$ corresponding to even powers of Z have a smaller number of K-types than those of b. This fact is very important since it implies that we shall have to handle a smaller number of unknowns when dealing with the system (161), which in some cases it is also necessary to assure that one can obtain a nonsingular square subsystem of (161).

Hence from now on we shall assume that $b = b_m \otimes Z^m + \cdots + b_0$ is in $\widetilde{B}$ and, in view of Proposition 8.41, we need to show that $b = 0$. Our approach to this problem will consist in proving that $P(T)$ implies $P(T-1)$ for $m \leq T \leq 4m$, where $P(T)$ is the propositional function associated to b and defined in (140). Observe that if m is even it is enough to show that $P([\frac{3m}{2}])$ holds while if m is odd we must show that $P(m-1)$ is true, because in both cases this implies that $b_m = 0$.

When $T-n \equiv 0$ we can change the index set $R(T,n)$ in (161) by a smaller set $\widetilde{R}(T,n)$ obtained by removing from $R(T,n)$ those indexes r such that $d(b^r_{T-r-n,n}) = T - r + n \leq r$. Thus we introduce the new index set

$$\widetilde{R}(T,n) = \{r \in R(T,n) : r < \tfrac{T+n}{2} \text{ if } r \equiv 0\}. \tag{169}$$

Observe that $\widetilde{R}(T,n) = R(T,n)$ if $T-n \equiv 1$. On the other hand if $T-n \equiv 0$ it follows from (169) that

$$|\widetilde{R}(T,n)| = \begin{cases} |R(T,n)| - \max\{0, \left[\frac{m}{2}\right] - \frac{T+n-4}{4}\}, & \text{if } T-n \equiv 0 \\ |R(T,n)| - \max\{0, \left[\frac{m}{2}\right] - \frac{T+n-2}{4}\}, & \text{if } T-n \equiv 2, \end{cases} \tag{170}$$

where the congruence is $\mod (4)$.

Now Theorem 8.31 and Theorem 8.32 can be reformulated as follows.

Theorem 8.42. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in \widetilde{B}$ and take $m \leq T \leq 4m$ and $0 \leq n \leq \min\{T, 4m-T\}$. If $P(T)$ and $Q(n)$ are true then for all L such that $0 \leq L \leq \min\{2m, T\} - n$ we have*

$$\begin{aligned} &\sum_{\substack{r,k \\ T-n \geq 2k+r \geq T-L}} B_{r,k}(T,n,L) D_{L+2k+r-T}(b^r_{2k,T-r-2k})(XX_4)^{T-k}E^n \\ &\quad - \sum_{\substack{r,l \\ r \in \widetilde{R}(T,n)}} (-2)^l \tbinom{L}{l} \tbinom{T-n-l}{r-l} u^r_{T-r-n,n}(XX_4)^{(T+r+n)/2}E^L \equiv 0, \end{aligned} \tag{171}$$

where the congruence is $\mod (U(\mathfrak{k})\mathfrak{m}^+)$.

Theorem 8.43. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in \widetilde{B}$ and take $m \leq T \leq 4m$ and $0 \leq n \leq \min\{T, 4m-T\}$. If $P(T)$ and $Q(n)$ are true then for all $L \in L(T,n)$ we have*

$$\sum_{r \in \widetilde{R}(T,n)} \Big(\sum_{\ell} (-2)^\ell \tbinom{L}{\ell} \tbinom{T-n-\ell}{r-\ell} \Big) u^r_{T-r-n,n} (XX_4)^{(T+r+n)/2} = 0, \tag{172}$$

where $u^r_{T-r-n,n} = r!(-1)^r \dot{X}^{T-n-r}\dot{E}^n(b^r_{T-n-r,n})$.

From now on we shall assume that $b \in \widetilde{B}$ is of degree m, satisfies the hypothesis of Theorem 8.43 and that $|\widetilde{R}(T,n)| \leq |L(T,n)|$. Then if we set $k = |\widetilde{R}(T,n)| - 1$ and consider the equations (172) corresponding to

$\{L_i = 2i + \epsilon : 0 \le i \le k\} \subset L(T, n)$ where $\epsilon = (1 + (-1)^n)/2$, we obtain a $(k+1) \times (k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ whose coefficient matrix $A(T, n)$ is exactly the matrix $A(T-n)$ defined in (165) by evaluating at $s = T - n$, corresponding to the sequence $\{L_i = 2i + \epsilon : 0 \le i \le k\}$ and $\delta = \left(1 - (-1)^{T-n}\right)/2$.

We will show later on that whenever $T-n \equiv 1$ Corollary 8.40 implies that the matrix $A(T-n)$ is nonsingular, hence we obtain $u^r_{T-r-n,n} = 0$ proving that $Q(n+1)$ is true. On the other hand, if $T-n \equiv 0$ the matrix $A(T-n)$ will turn out, in general, to be singular. Therefore in order to prove that $u^r_{T-r-n,n} = 0$ we need to consider another system of equations derived from Theorem 8.42 which it be nonsingular. We describe next how to obtain this new system.

Assume that $T - n = 2\nu$ with $1 \le k \le \nu \le 2k + \epsilon - 1$. Then in view of Corollary 8.40 the matrix $A(2\nu)$ is singular. Moreover if $A_i(2\nu)$ denotes the i-row of the matrix $A(2\nu)$ it follows from the proof of Theorem 8.39 that $A(2\nu)$ is singular because $A_i(2\nu) = A_{\nu-i-\epsilon}(2\nu)$ for $\nu - k - \epsilon \le i \le \nu - k - \epsilon + m(2\nu) - 1$ if $k+1 \le \nu$ and $0 \le i \le m(2\nu) - 1$ if $\nu = k$. Where $m(2\nu)$ is the multiplicity of 2ν as a root of $\det A(s)$ and is given by (166). That is, the square system obtained from Theorem 8.43 is singular because it has $m(2\nu)$ pairs of equal equations. Hence our strategy will consist in replacing one of the equations in each one of these pairs by a new equation taken from Theorem 8.42. These new equations will be chosen as follows. Set

$$L'(T, n) = \{L : 0 \le L < \min\{n, \min\{2m, T\} - n + 1\},\ L \equiv n\}. \tag{173}$$

Then for each $L \in L'(T, n)$ the first sum in equation (171) of Theorem 8.42 is empty, therefore the second sum of (171), after using Corollary 8.19, gives rise to a new equation in the elements $u^r_{T-r-n,n}$ with $r \in \widetilde{R}(T, n)$. In order to assure that we have sufficiently many new equations we need to show, in each case, that $m(2\nu) \le |L'(T, n)|$. If this is the case we consider the equations corresponding to the first $m(2\nu)$ elements of $L'(T, n)$ and use them to replace the equations corresponding to the rows $A_i(2\nu)$ for $k + 1 - m(2\nu) \le i \le k$ if $\nu \ge k + 1$ and $k + 1 - m(2k) - \epsilon \le i \le k - \epsilon$ if $\nu = k$. If we let $A'(T-n)$ denote the coefficient matrix of this new $(k+1) \times (k+1)$ system of linear equations it follows that $A'(T-n)$ is defined as in (165) with $s = T-n$, $\delta = 0$ and corresponding to the sequence of nonnegative integers $\{L'_i : 0 \le i \le k\}$ defined as follows. If $k + 1 \le \nu$, $\nu + \epsilon \equiv 1$ and $\epsilon' = 1 - \epsilon$ we set

$$L'_i = \begin{cases} 2i + \epsilon, & 0 \le i \le k - m(2\nu) \\ 2(i - \nu + k + \epsilon - m(2\nu)) + \epsilon', & k + 1 - m(2\nu) \le i \le k; \end{cases} \tag{174}$$

and if $\nu + \epsilon \equiv 0$ set

$$L'_i = \begin{cases} 2i + \epsilon, & 0 \le i \le k - m(2\nu) \\ 2(i - \nu + k + \epsilon - m(2\nu) - 1) + \epsilon', & k + 1 - m(2\nu) \le i \le k. \end{cases} \tag{175}$$

On the other hand, if $\nu = k$ and $k+\epsilon \equiv 1$ we define,

$$L'_i = \begin{cases} 2(i - m(2k)) + \epsilon', & k+1-m(2k)-\epsilon \le i \le k-\epsilon \\ 2i+\epsilon, & \text{all other } i\text{'s}; \end{cases} \tag{176}$$

and if $k+\epsilon \equiv 0$ we set

$$L'_i = \begin{cases} 2(i - m(2k) - 1) + \epsilon', & k+1-m(2k)-\epsilon \le i \le k-\epsilon \\ 2i+\epsilon, & \text{all other } i\text{'s}. \end{cases} \tag{177}$$

In the following proposition we show that the system of equations considered above is nonsingular.

Proposition 8.44. *Let $b = b_m \otimes Z^m + \cdots + b_0 \in \widetilde{B}$, $m \le T \le 4m$ and $0 \le n \le \min\{T, 4m-T\}$ be such that $P(T)$ and $Q(n)$ are true. Assume that $|\widetilde{R}(T,n)| \le |L(T,n)|$ and set $k = |\widetilde{R}(T,n)| - 1$. Then if $T - n = 2\nu$ with $1 \le k \le \nu \le 2k + \epsilon - 1$ and $m(2\nu) \le |L'(T,n)|$ the coefficient matrix $A'(T-n)$ of the system defined above is nonsingular. In particular $Q(n+1)$ is true.*

Proof. It follows from Theorem 8.39 that $A'(2\nu)$ is nonsingular if and only if $2\nu \notin R \cap 2\mathbb{Z}$ where $R = \{L'_i + L'_j : 0 \le i < j \le k\}$. To establish this fact we consider first $k+1 \le \nu$. If $\nu + \epsilon \equiv 1$ it follows from (166) that $m(2\nu) = (2k+1+\epsilon-\nu)/2$, hence using (174) we get

$$\begin{aligned} &\max(R \cap 2\mathbb{Z}) \\ &\quad = \max\{4(\nu - k - \epsilon + m(2\nu)) + 2\epsilon - 6, 4(2k - \nu + \epsilon - m(2\nu)) - 2\epsilon\} \\ &\quad = \max\{2\nu - 4, 4k - 2\nu - 2\} = 2\nu - 4. \end{aligned}$$

On the other hand, if $\nu + \epsilon \equiv 0$ it follows from (166) that $m(2\nu) = (2k + \epsilon - \nu)/2$, hence from (175) we get

$$\begin{aligned} &\max(R \cap 2\mathbb{Z}) \\ &\quad = \max\{4(\nu - k - \epsilon + m(2\nu)) + 2\epsilon - 2, 4(2k - \nu + \epsilon - m(2\nu)) - 2\epsilon - 4\} \\ &\quad = \max\{2\nu - 2, 4k - 2\nu - 4\} = 2\nu - 2. \end{aligned}$$

In both cases $2\nu \notin R \cap 2\mathbb{Z}$.

Now consider $\nu = k$. If $k + \epsilon \equiv 1$ it follows from (166) that $m(2k) = (k+1-\epsilon)/2$, hence using (176) we obtain $\{L'_i : 0 \le i \le k\} = \{0, 1, \ldots, k\}$ if $\epsilon = 0$ and $\{L'_i : 0 \le i \le k\} = \{0, 1, \ldots, k-1, 2k+1\}$ if $\epsilon = 1$. Therefore,

$$R \cap 2\mathbb{Z} = \begin{cases} \{2j : 1 \le j \le k-1\}, & \text{if } \epsilon = 0 \\ \{2j : 1 \le j \le k-2\} \cup \{2j : k+1 \le j \le 3k/2\}, & \text{if } \epsilon = 1. \end{cases}$$

On the other hand, if $k+\epsilon \equiv 0$ it follows from (166) that $m(2k) = (k-\epsilon)/2$, hence it follows from (177) that $\{L'_i : 0 \le i \le k\} = \{0, 1, \ldots, k\}$ if $\epsilon = 0$ and $\{L'_i : 0 \le i \le k\} = \{0, 1, \ldots, k-3, k-2, k, 2k+1\}$ if $\epsilon = 1$. Hence,

$$R \cap 2\mathbb{Z} = \begin{cases} \{2j : 1 \le j \le k-1\}, & \text{if } \epsilon = 0 \\ \{2j : 1 \le j \le k-1\} \cup \{2j : k+1 \le j \le (3k+1)/2\}, & \text{if } \epsilon = 1. \end{cases}$$

Therefore in both cases it is clear that $2k \notin R \cap 2\mathbb{Z}$, as we wanted to prove. This completes the proof of the proposition.

Let $b = b_m \otimes Z^m + \cdots + b_0$ in $\widetilde{B}$. As we indicated before our goal is to show that $b_m = 0$, which certainly implies that $\widetilde{B} = 0$. Our approach to this problem will consist in proving that $P(T)$ implies $P(T-1)$ for $m \leq T \leq 4m$. This will be done in two steps, $2m+1 \leq T \leq 4m$ and $m \leq T \leq 2m$ by proving in each case that $Q(n)$ implies $Q(n+1)$ for $0 \leq n \leq \min\{T, 4m-T\}$. To do this we shall use the system of equations obtained from Theorem 8.43 whenever it is nonsingular, and when it is singular we shall prove that we are in the hypothesis of Proposition 8.44.

Proposition 8.45. *If $m \geq 1$ and $2m+1 \leq T \leq 4m$ then $P(T-1)$ follows from $P(T)$. Therefore $P(2m)$ holds.*

Proof. For any $2m+1 \leq T \leq 4m$ to prove that $P(T-1)$ holds we must show that $b^r_{T-r-n,n} = 0$ or, equivalently, that $u^r_{T-r-n,n} = 0$ for every $0 \leq n \leq 4m-T$ and every $r \in \widetilde{R}(T,n)$. To do this we will show that $Q(n)$ implies $Q(n+1)$, where $Q(n)$ is the propositional function defined in (154).

We begin by observing that for $T \geq 2m+1$ we have $4[m/2]-T < 0$, hence from (170) we obtain that $\widetilde{R}(T,n) = R(T,n)$ for every $0 \leq n \leq 4m-T$. On the other hand, in view of Lemma 8.33, we have that $|R(T,n)| \leq |L(T,n)|$. Thus if we set $k = |R(T,n)| - 1$ and we consider in the system (172) the equations corresponding to $\{L_i = 2i+\epsilon : 0 \leq i \leq k\} \subset L(T,n)$ where $\epsilon = (1+(-1)^n)/2$, we obtain a $(k+1)\times(k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ whose coefficient matrix is the matrix $A(T-n)$ defined in (165) for $s = T-n$, corresponding to the sequence $\{L_i = 2i+\epsilon : 0 \leq i \leq k\}$ and $\delta = \left(1-(-1)^{T-n}\right)/2$.

Let us first assume that $3m \leq T \leq 4m$. Then it follows from (163) and (164) that $2|R(T,n)| = 4m - T - n + 1 + \left(1-(-1)^{T-n}\right)/2$ for every $0 \leq n \leq 4m-T$. Hence $4k+2(\epsilon+\delta-1) = 8m+2\epsilon-2(T+n)-2$ and therefore $T-n = 3T+n-2(T+n) \geq m+4k+2(\epsilon+\delta-1) \geq 1+4k+2(\epsilon+\delta-1)$. Then in view of Corollary 8.40 the matrix $A(T-n)$ is nonsingular, therefore $u^r_{T-r-n,n} = 0$ for every $r \in R(T,n)$, proving that $Q(n+1)$ holds.

Next assume that $2m+1 \leq T \leq 3m-1$. To analyze the matrix $A(T-n)$ we shall consider two cases: $T-n \equiv 1$ and $T-n \equiv 0$. If n is such that $T-n \equiv 1$ it follows from (163) and (164) that

$$2k+\delta = \begin{cases} 2[\frac{m-1}{2}]+1, & \text{if } 0 \leq n \leq 3m-T \\ 4m-T-n, & \text{if } 3m-T+1 \leq n \leq 4m-T. \end{cases}$$

Then if $0 \leq n \leq 3m-T$ we have $T-n \geq 2T-3m \geq m+2 > 2k+\delta$. On the other hand if $3m-T+1 \leq n \leq 4m-T$ we get $T-n = 4m-T-n+2(T-2m) > 2k+\delta$. Hence for every $0 \leq n \leq 4m-T$ we have $T-n > 2k+\delta$, which is one of the conditions of Corollary 8.40. Furthermore, since $T-n \equiv 1$ it follows from the same corollary that the matrix $A(T-n)$ is nonsingular, therefore $u^r_{T-r-n,n} = 0$ for every $r \in R(T,n)$, proving that $Q(n+1)$ holds.

We assume now that n is such that $T-n\equiv 0$. In this case $\delta=0$ and from (163) and (164) we obtain

$$2k+\delta=\begin{cases}2[\frac{m}{2}]+1, & \text{if } 0\le n\le 3m-T\\ 4m-T-n, & \text{if } 3m-T+1\le n\le 4m-T.\end{cases}\tag{178}$$

Then, as in the previous case, a simple calculation shows that $T-n\ge 2(k+1)$ for every $0\le n\le 4m-T$. Hence if we set $T-n=2\nu$ we get $\nu\ge k+1$. Also it is easy to verify that $\nu\le 2k+\epsilon-1$ if and only if $n\ge T+2-4k-2\epsilon$. Hence if $0\le n<T+2-4k-2\epsilon$ it follows from Corollary 8.40 that the matrix $A(T-n)$ is nonsingular, therefore for these values of n we have $u^r_{T-r-n,n}=0$ for every $r\in R(T,n)$, proving that $Q(n+1)$ holds.

Let us assume now that n is such that $k+1\le\nu\le 2k+\epsilon-1$. In this case the matrix $A(T-n)$ is singular, then to show that $Q(n+1)$ holds we are going to use Proposition 8.44. To do this we need to check that $m(2\nu)\le|L'(T,n)|$, where $L'(T,n)$ is the set defined in (173). We begin by observing that for $T\ge 2m+1$ we have

$$|L'(T,n)|=\begin{cases}\left[\frac{n}{2}\right], & \text{if } 0\le n\le m\\ \frac{2m+1+\epsilon-n}{2}, & \text{if } m+1\le n\le 4m-T.\end{cases}\tag{179}$$

On the other hand from (166) we obtain that $m(2\nu)=[(2k+1+\epsilon-\nu)/2]$.

Let us first consider $0\le n\le 3m-T$. Then, since $T\ge 2m+1$, we have $n<m$ and therefore $|L'(T,n)|=[n/2]$. Also it follows from (178) that

$$m(2\nu)=\left[\frac{4[m/2]+2+2\epsilon+n-T}{4}\right]\le\left[\frac{n+1+2\epsilon}{4}\right]\le\left[\frac{n}{2}\right]=|L'(T,n)|,$$

as we wanted to prove.

Now consider $3m-T+1\le n\le 4m-T$. Then it follows from (178) that

$$m(2\nu)=\left[\frac{8m+2+2\epsilon-3T-n}{4}\right]\le\left[\frac{n+\epsilon}{2}\right]=\left[\frac{n}{2}\right].$$

Also, since $T\ge 2m+1$ and $n\le 4m-T$, we get $4m-3T+n<0$ which in turns implies that

$$m(2\nu)=\left[\frac{8m+2+2\epsilon-3T-n}{4}\right]<\frac{2m+1+\epsilon-n}{2}.$$

Hence in view of (179) we obtain that $m(2\nu)\le|L'(T,n)|$. This completes the proof of the proposition.

Proposition 8.46. *If $m\ge 1$ and $m\le T\le 2m$ then $P(T-1)$ follows from $P(T)$. Therefore $P(m-1)$ holds.*

Proof. For any $m\le T\le 2m$ we have $0\le n\le T$. Hence, as in the previous proposition, we need to show that $u^r_{T-r-n,n}=0$ for every $0\le n\le T$ and every $r\in\widetilde{R}(T,n)$. To do this we will show that $Q(n)$ implies $Q(n+1)$.

Let $m\le T\le 2m$ and assume that n is such that $T-n\equiv 1$. Then it follows from Lemma 8.33 that $|R(T,n)|\le|L(T,n)|$. Hence if we set

$k = |R(T,n)| - 1$ and we consider the equations (172) associated to the sequence $\{L_i = 2i + \epsilon : 0 \le i \le k\} \subset L(T,n)$ where $\epsilon = (1 + (-1)^n)/2$, we obtain a $(k+1) \times (k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ whose coefficient matrix is the matrix $A(T-n)$ defined in (165) for $s = T - n$, $\delta = 1$ and the sequence $\{L_i = 2i + \epsilon : 0 \le i \le k\}$.

Now it follows from (163) and (164) that

$$2k + \delta = \begin{cases} 2\left[\frac{m-1}{2}\right] + 1, & \text{if } 0 \le n \le T - m \\ T - n, & \text{if } T - m + 1 \le n \le T. \end{cases}$$

Then, if $0 \le n \le T - m$ we get $T - n \ge m \ge 2k + \delta$, and for $T - m + 1 \le n \le T$ we have $T - n = 2k + \delta$. Hence for every $0 \le n \le T$ the first condition of Corollary 8.40 is satisfied. Furthermore, since $T - n \equiv 1$ it follows from the same corollary that the matrix $A(T-n)$ is nonsingular, therefore $u^r_{T-r-n,n} = 0$ for every $r \in R(T,n)$, proving that $Q(n+1)$ holds.

From now on we shall assume that $m \le T \le 2m$ and that n is such that $T - n \equiv 0$. In this case it is convenient to consider the following situations:
(i) $0 \le n < T - m$,
(ii) $n = T - m$ and $n \equiv 1$,
(iii) $T - m + 1 \le n \le T$ and $n \equiv 1$,
(iv) $T - m \le n \le T$ and $n \equiv 0$.

We begin by observing that in cases (i), (ii) and (iii) Lemma 8.33 implies that $|\widetilde{R}(T,n)| \le |L(T,n)|$. Hence if we set $k = |\widetilde{R}(T,n)| - 1$ and consider the equations (172) associated to the sequence $\{L_i = 2i + \epsilon : 0 \le i \le k\} \subset L(T,n)$ where $\epsilon = (1 + (-1)^n)/2$, we obtain a $(k+1) \times (k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ whose coefficient matrix is the matrix $A(T-n)$ defined in (165) for $s = T - n$, $\delta = 0$ and corresponding to the sequence $\{L_i = 2i + \epsilon : 0 \le i \le k\}$. This is the system of equations that we shall use in the cases (i), (ii) and (iii). If the coefficient matrix $A(T-n)$ is nonsingular we shall obtain that $Q(n+1)$ holds right away, however if $A(T-n)$ is singular we shall need to apply Proposition 8.44. In order to analyze the matrix $A(T-n)$ we shall consider each one of the first three cases separately.

(i) We consider first $0 \le n < T - m$. In view of (170) we need to consider two cases according as $T + n \equiv 0 \mod (4)$ or $T + n \equiv 2 \mod (4)$. Also for each one of these cases we have two different situations, $|\widetilde{R}(T,n)| < |R(T,n)|$ or $|\widetilde{R}(T,n)| = |R(T,n)|$.

Let us assume that $T + n \equiv 0 \mod (4)$ and that $|\widetilde{R}(T,n)| < |R(T,n)|$. It follows from (170) that this case holds if and only if $m+1 \le T \le 4[m/2]$ and $0 \le n \le \min\{T - m - 1, 4[m/2] - T\}$. Then we have $|\widetilde{R}(T,n)| = (T+n)/4$ and $k = (T + n - 4)/4$. Hence, if $T \ge [(3m+2)/2]$ we have

$$T - n \ge 2T - 4\left[\tfrac{m}{2}\right] \ge 2m + 2 - 2\left[\tfrac{m}{2}\right] \ge 2\left[\tfrac{m}{2}\right] + 2 > 2k + \delta.$$

On the other hand, if $T \leq [3m/2]$ it is easy to see that $T - m < (T+2)/3$. Thus for every $0 \leq n < T - m$ we have $n < (T+2)/3$, which implies that $2k + \delta < T - n$. Therefore the first condition of Corollary 8.40 is satisfied.

Next set $T - n = 2\nu$. Since $2k + \delta < T - n$ and $\delta = 0$ we have $\nu \geq k + 1$. Also, using Corollary 8.40, a simple calculation shows that 2ν is a root of $\det A(s)$ if and only if $2 \leq n < T - m$. Thus if $n = 0, 1$ the matrix $A(T-n)$ is nonsingular, hence for these values of n we have $u^r_{T-r-n,n} = 0$ for all $r \in \widetilde{R}(T, n)$, proving that $Q(1)$ and $Q(2)$ hold.

On the other hand, if $2 \leq n < T - m$ we have $k + 1 \leq \nu \leq 2k + \epsilon - 1$. In this case the matrix $A(T - n)$ is singular (Corollary 8.40). Then in order to show that $Q(n + 1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \leq |L'(T, n)|$, where $L'(T, n)$ is the set defined in (173). Since $T \leq 2m$ it follows that

$$|L'(T,n)| = \begin{cases} \left[\frac{n}{2}\right], & \text{if } \min\{n, T-n+1\} = n \\ \frac{T-n+2\epsilon}{2}, & \text{if } \min\{n, T-n+1\} = T-n+1, \end{cases} \tag{180}$$

where $\epsilon = (1 + (-1)^n)/2$. Now, since $T \leq 2m$, if $0 \leq n \leq T - m$ we have $n \leq T - m \leq m < T - n + 1$, therefore from (180) we get $|L'(T, n)| = [n/2]$. On the other hand since $\nu \geq k + 1$ it follows from (166) that

$$m(2\nu) = \left[\tfrac{2k+\epsilon+1-\nu}{2}\right] = \left[\tfrac{n+\epsilon-1}{2}\right] = \left[\tfrac{n}{2}\right] = |L'(T,n)|.$$

Hence it follows from Proposition 8.44 that $Q(n + 1)$ holds.

We assume now that $T + n \equiv 0 \mod (4)$ and that $|\widetilde{R}(T, n)| = |R(T, n)|$. This occurs if and only if $(4[m/2]+m+5)/2 \leq T \leq 2m$ and $4[m/2]+4-T \leq n \leq T - m - 1$ (see (170)). Then $|\widetilde{R}(T, n)| = [m/2] + 1$ and $k = [m/2]$. Now, since $n < T - m$ and $\delta = 0$, we obtain $T - n > m \geq 2k + \delta$, which is the first condition of Corollary 8.40. Moreover, if we set $T - n = 2\nu$ then $\nu \geq k + 1$.

On the other hand a simple calculation shows that $k+1 \leq \nu \leq 2k+\epsilon-1$ if and only if $T + 2 - 4[m/2] - 2\epsilon \leq n \leq T - m - 1$. Hence, taking into account that n and T are both even or both odd, it follows that $2k + \epsilon - 1 < \nu$ only when $m \equiv 1$ and $(T, n) = (2m, 0)$ or $(T, n) = (2m - 1, 1)$. For these values of T and n it follows from Corollary 8.40 that the matrix $A(T - n)$ is nonsingular. Then, whenever $m \equiv 1$, it follows that $Q(1)$ holds if $T = 2m$, and $Q(2)$ holds if $T = 2m - 1$.

Let us assume now that T and n are such that $k+1 \leq \nu \leq 2k+\epsilon-1$. In this case $A(T-n)$ is singular, then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \leq |L'(T, n)|$. In fact, since $4[m/2] + 4 - T \leq n$, from (166) we get

$$m(2\nu) = \left[\tfrac{2k+\epsilon+1-\nu}{2}\right] \leq \left[\tfrac{4[m/2]+n+4-T}{4}\right] \leq \left[\tfrac{n}{2}\right] = |L'(T,n)|.$$

Then from Proposition 8.44 it follows that $Q(n + 1)$ holds. This completes the analysis when $T + n \equiv 0 \mod (4)$.

Let us assume that $T + n \equiv 2 \mod (4)$ and that $|\widetilde{R}(T, n)| < |R(T, n)|$. It follows from (170) that this case holds if and only if $m + 1 \leq T \leq 4[m/2] - 2$

and $0 \le n \le \min\{T-m-1, 4[m/2]-2-T\}$. Then $|\widetilde{R}(T,n)| = (T+n+2)/4$ and $k = (T+n-2)/4$. Hence, if $T \ge [(3m+2)/2]$ we have

$$T - n \ge 2T + 2 - 4\left[\tfrac{m}{2}\right] \ge 2m + 4 - 2\left[\tfrac{m}{2}\right] \ge 2\left[\tfrac{m}{2}\right] + 4 > 2k + \delta.$$

On the other hand, if $T \le [3m/2]$ it is easy to see that $T - m < (T+2)/3$. Thus for every $0 \le n < T - m$ we have $n < (T+2)/3$ which in turn implies that $2k + \delta < T - n$. Therefore the first condition of Corollary 8.40 is satisfied.

Next set $T - n = 2\nu$. Since $2k + \delta < T - n$ and $\delta = 0$ we have $\nu \ge k+1$. Also, using Corollary 8.40, a simple calculation shows that 2ν is a root of $\det A(s)$ if and only if $2 \le n < T - m$. Thus if $n = 0, 1$ the matrix $A(T-n)$ is nonsingular, hence for these values of n we have $u^r_{T-r-n,n} = 0$ for all $r \in \widetilde{R}(T,n)$, proving that $Q(1)$ and $Q(2)$ hold.

On the other hand, if $2 \le n < T - m$ we have $k + 1 \le \nu \le 2k + \epsilon - 1$. In this case the matrix $A(T-n)$ is singular (Corollary 8.40). Then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \le |L'(T,n)|$. Now since $\nu \ge k+1$ it follows from (166) that

$$m(2\nu) = \left[\tfrac{2k+\epsilon+1-\nu}{2}\right] = \left[\tfrac{n+\epsilon}{2}\right] = \left[\tfrac{n}{2}\right] = |L'(T,n)|.$$

Hence it follows from Proposition 8.44 that $Q(n+1)$ holds.

We assume now that $T + n \equiv 2 \mod (4)$ and that $|\widetilde{R}(T,n)| = |R(T,n)|$. This occurs if and only if $(4[m/2]+m+3)/2 \le T \le 2m$ and $4[m/2]+2-T \le n \le T-m-1$ (see (170)). Then $|\widetilde{R}(T,n)| = [m/2]+1$ and $k = [m/2]$. Now, since $n < T - m$ and $\delta = 0$, we obtain $T - n > m \ge 2k + \delta$, which is the first condition of Corollary 8.40. Moreover, if we set $T - n = 2\nu$ then $\nu \ge k+1$.

On the other hand a simple calculation shows that $k+1 \le \nu \le 2k+\epsilon-1$ if and only if $T+2-4[m/2]-2\epsilon \le n \le T-m-1$. Hence, taking into account that n and T are both even or both odd, it follows that $2k + \epsilon - 1 < \nu$ only when $m \equiv 1$ and $(T,n) = (2m,0)$ or $(T,n) = (2m-1,1)$. For these values of T and n it follows from Corollary 8.40 that the matrix $A(T-n)$ is nonsingular. Then, whenever $m \equiv 1$, it follows that $Q(1)$ holds if $T = 2m$, and $Q(2)$ holds if $T = 2m-1$.

Let us assume now that T and n are such that $k+1 \le \nu \le 2k+\epsilon-1$. In this case $A(T-n)$ is singular, then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \le |L'(T,n)|$. In fact, since we are assuming that $T + n \equiv 2 \mod (4)$, from (166) we get

$$m(2\nu) = \left[\tfrac{2k+\epsilon+1-\nu}{2}\right] = \begin{cases} \frac{4[m/2]+n+2-T}{4}, & \text{if } n \equiv 0 \\ \frac{4[m/2]+n-T}{4}, & \text{if } n \equiv 1. \end{cases}$$

Thus, from $4[m/2] + 2 - T \le n$, it follows that $m(2\nu) \le [n/2] = |L'(T,n)|$. Then from Proposition 8.44 we obtain that $Q(n+1)$ holds. This completes the analysis when $T + n \equiv 2 \mod (4)$, completing the proof of the proposition in case (i).

(ii) We consider now the case $n = T - m$ and $n \equiv 1$. Then, since $T - n \equiv 0$, we have $T \equiv 1$ and $m \equiv 0$. In this case we need to consider two different situations according as $m \leq T \leq 3m/2$ or $(3m+2)/2 \leq T \leq 2m$.

Let us assume first that $(3m+2)/2 \leq T \leq 2m$. Then it follows from (170) and (163) that $|\widetilde{R}(T,n)| = |R(T,n)| = \frac{m}{2}+1$. Hence $k = |\widetilde{R}(T,n)| - 1 = m/2$ and therefore $T - n = m = 2k$, which is the first condition of Corollary 8.40. Moreover it follows from the same corollary that the matrix $A(T-n)$ is singular for every $(3m+2)/2 \leq T \leq 2m$. Thus in order to prove that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2k) \leq |L'(T,n)|$. In fact, since $(3m+2)/2 \leq T$ it follows that $(m+2)/4 \leq n/2$. Then from (166) we obtain

$$m(2k) = \left[\tfrac{k+1}{2}\right] = \left[\tfrac{m+2}{4}\right] \leq \left[\tfrac{n}{2}\right] = |L'(T,n)|.$$

Hence Proposition 8.44 implies that $Q(n+1)$ is true.

We assume now that $m \leq T \leq 3m/2$. Then it follows from (170) and (163) that $|\widetilde{R}(T,n)| < |R(T,n)|$ and that

$$|\widetilde{R}(T,n)| = \begin{cases} \frac{T+n}{4}, & \text{if } T+n \equiv 0 \mod (4) \\ \frac{T+n+2}{4} & \text{if } T+n \equiv 2 \mod (4). \end{cases} \tag{181}$$

Now, since $T \leq 3m/2$, it follows from (181) that $T - n > 2k + \delta$, which is the first condition of Corollary 8.40. Moreover, if we set $T - n = 2\nu$ then $\nu \geq k+1$. Also, using the same corollary, a simple calculation shows that 2ν is a root of $\det A(s)$ if and only if $m+3 \leq T \leq 3m+2$. Thus if $T = m+1$ and $n = 1$ the matrix $A(m)$ is nonsingular, therefore we obtain that $u^r_{m-r,1} = 0$ for every $r \in \widetilde{R}(m+1,1)$, proving that $Q(2)$ holds.

On the other hand if $m+3 \leq T \leq 3m/2$ we have $k+1 \leq \nu \leq 2k-1$. Hence it follows from Corollary 8.40 that the matrix $A(T-n)$ is singular, then to prove that $Q(n+1)$ holds we must check that $m(2\nu) \leq |L'(T,n)|$.

Since $T \leq 2m$ and $n = T - m$, it follows from (180) that $|L'(T,n)| = [n/2]$. Then, since $\nu \geq k+1$, from (166) we get

$$m(2\nu) = \left[\tfrac{2k+1-\nu}{2}\right] = \left[\tfrac{n}{2}\right] = |L'(T,n)|.$$

Hence Proposition 8.44 implies that $Q(n+1)$ holds. This completes the proof of the proposition in case (ii).

(iii) We consider now $T - m + 1 \leq n \leq T$ and $n \equiv 1$. Since $T - n \equiv 0$ we have $T \equiv 1$, hence we may assume that $2[m/2] + 1 \leq T \leq 2m - 1$. Now in view of (170) we need to consider two cases according as $T + n \equiv 0 \mod (4)$ or $T + n \equiv 2 \mod (4)$. Also for each one of these cases we have two different situations, $|\widetilde{R}(T,n)| < |R(T,n)|$ or $|\widetilde{R}(T,n)| = |R(T,n)|$.

Let us assume that $T + n \equiv 0 \mod (4)$ and that $|\widetilde{R}(T,n)| = |R(T,n)|$. It follows from (170) that this case holds if and only if $2[m/2]+3 \leq T \leq 2m-1$ and $\max\{T - m + 1, 4[m/2] + 4 - T\} \leq n \leq T$. Moreover from (164) we get $|\widetilde{R}(T,n)| = (T-n+2)/2$ and therefore $k = (T-n)/2$.

Observe that if $n=T$ we have $k=0$, therefore the corresponding matrix $A(0)$ is clearly nonsingular. Hence for every $2[m/2]+3\le T\le 2m-1$ and $n=T$ we obtain $u^0_{0,T}=0$ as we wished to prove.

Then from now on we may assume that $n\le T-2$. Since $T-n=2k$ with $k\ge 1$ it follows from Corollary 8.40 that $A(T-n)$ is singular, then in order to prove that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu)\le |L'(T,n)|$. We begin by observing that from (180) we get

$$|L'(T,n)| = \begin{cases} \frac{n-1}{2}, & \text{if } n\le \frac{T+1}{2} \\ \frac{T-n}{2}, & \text{if } \frac{T+1}{2}<n, \end{cases} \tag{182}$$

and from (166) we obtain that $m(2k)=[(k+1)/2]=(T-n+2)/4$. Now since $n\le T-2$ it follows that $m(2k)\le (T-n)/2$. On the other hand it is easy to see that $(T+4)/3\le \max\{T-m+1, 4[m/2]+4-T\}$ for every T. Then we have $(T+4)/3\le n$ which in turns implies that $m(2k)\le (n-1)/2$. Therefore, in view of (182), we have $m(2\nu)\le |L'(T,n)|$ as we wanted to prove. Hence Proposition 8.44 implies that $Q(n+1)$ is true.

We assume now that $T+n\equiv 0 \mod (4)$ and that $|\widetilde{R}(T,n)|<|R(T,n)|$. Then it follows from (170) that $n<4[m/2]+4-T$. More precisely, since $T\equiv n\equiv 1$ and $T+n\equiv 0 \mod (4)$ we conclude that this case holds if and only if $2[m/2]+1\le T\le [3m/2]-1$ and $T-m+1\le n\le 4[m/2]-T$. Moreover from (164) and (170) we get $|\widetilde{R}(T,n)|=(3T-n-4[m/2])/4$.

Now since $n\le 4[m/2]-T$ it follows that $T-n\ge 2(k+1)$ where $k=|\widetilde{R}(T,n)|-1$. This implies that the first condition of Corollary 8.40 holds. Moreover if we set $T-n=2\nu$, using the same corollary, it follows that 2ν is a root of $\det A(s)$ if and only if $2[m/2]+3\le T\le [3m/2]-1$ and $T-m+1\le n\le 4[m/2]-T$. Hence if $T=2[m/2]+1$ and $2[m/2]-m+2\le n\le 2[m/2]-1$ the matrix $A(T-n)$ is nonsingular. Therefore $u^r_{T-r-n,n}=0$ for all $r\in \widetilde{R}(T,n)$, proving that $Q(n+1)$ holds.

If $T\ge 2[m/2]+3$ the matrix $A(T-n)$ is singular for every $T-m+1\le n\le 4[m/2]-T$, then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu)\le |L'(T,n)|$, where $|L'(T,n)|$ is given by (182). On the other hand, since $\nu\ge k+1$, $\epsilon=0$ and $T\equiv 1$, it follows from (166) that

$$m(2\nu)=\left[\tfrac{2k+1-\nu}{2}\right]=\tfrac{T-2[m/2]-1}{2}. \tag{183}$$

Then, since $T-m+1\le n$, we have $T-2[m/2]-1\le n-1$ which implies that $m(2\nu)\le (n-1)/2$. Also, since $n\le 4[m/2]-T$ and $T\ge 2[m/2]+3$, it follows that $n<2[m/2]+1$, therefore $m(2\nu)<(T-n)/2$. Hence in view of (182) we obtain that $m(2\nu)\le |L'(T,n)|$. Then Proposition 8.44 implies that $Q(n+1)$ is true.

Assume now that $T+n\equiv 2 \mod (4)$ and that $|\widetilde{R}(T,n)|=|R(T,n)|$. It follows from (170) that this case holds if and only if $2[m/2]+1\le T\le 2m-1$

and $\max\{T-m+1, 4[m/2]+2-T\} \le n \le T$. Moreover from (164) we get $|\widetilde{R}(T,n)| = (T-n+2)/2$ and therefore $k = (T-n)/2$.

Observe that if $n = T$ we have $k = 0$ therefore the corresponding matrix $A(0)$ is clearly nonsingular. On the other hand it follows from (160) that $\widetilde{R}(T,n) = R(T,n) = \{0\}$, hence for every $2[m/2]+1 \le T \le 2m-1$ and $n = T$ we obtain $u^0_{0,T} = 0$ as we wanted to prove.

Then from now on we may assume that $n \le T-2$. Since $T-n = 2k$ with $k \ge 1$ it follows from Corollary 8.40 that $A(T-n)$ is singular, then in order to prove that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2k) \le |L'(T,n)|$. Now, since $T+n \equiv 2 \mod (4)$ and $n \equiv 1$ we obtain that $T-n \equiv 0 \mod (4)$. Hence, since $\epsilon = 0$, from (166) we get

$$m(2k) = \left[\tfrac{k+1}{2}\right] = \tfrac{T-n}{4}.$$

Clearly $m(2k) < (T-n)/2$. On the other hand it is easy to see that $(T+2)/3 \le \max\{T-m+1, 4[m/2]+2-T\}$ for every T. Then we have $(T+2)/3 \le n$ which in turn implies that $m(2k) \le (n-1)/2$. Therefore, in view of (182), we have $m(2k) \le |L'(T,n)|$ as we wanted to prove. Hence Proposition 8.44 implies that $Q(n+1)$ is true.

Next we assume that $T+n \equiv 2 \mod (4)$ and that $|\widetilde{R}(T,n)| < |R(T,n)|$. Then it follows from (170) that this case holds if and only if $2[m/2]+1 \le T \le [(3m-4)/2]$ and $T-m+1 \le n \le 4[m/2]-2-T$. Moreover from (164) and (170) we get $|\widetilde{R}(T,n)| = (3T-n-4[m/2]+2)/4$.

Now since $n \le 4[m/2]-2-T$ it follows that $T-n \ge 2(k+1)$ where $k = |\widetilde{R}(T,n)|-1$. This implies that the first condition of Corollary 8.40 holds. Moreover if we set $T-n = 2\nu$, and since $T \equiv 1$, using the same corollary it follows that 2ν is a root of $\det A(s)$ if and only if $2[m/2]+3 \le T \le [(3m-4)/2]$ and $T-m+1 \le n \le 4[m/2]-2-T$. Hence if $T = 2[m/2]+1$ and $2[m/2]-m+2 \le n \le 2[m/2]-3$ the matrix $A(T-n)$ is nonsingular. Therefore $u^r_{T-r-n,n} = 0$ for all $r \in \widetilde{R}(T,n)$, proving that $Q(n+1)$ holds.

If $T \ge 2[m/2]+3$ the matrix $A(T-n)$ is singular for every $T-m+1 \le n \le 4[m/2]-2-T$, then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \le |L'(T,n)|$, where $|L'(T,n)|$ is given by (182). However in this case $m(2\nu)$ is also given by (183), hence the same calculation that we did right after (183) shows that $m(2\nu) \le |L'(T,n)|$. Then Proposition 8.44 implies that $Q(n+1)$ is true. This completes the proof of the proposition in case (iii).

(iv) Let us now assume that $T-m \le n \le T$ and $n \equiv 0$. Then since $T-n \equiv 0$ we also have $T \equiv 0$. We are going to consider two different situations according $|\widetilde{R}(T,n)| < |R(T,n)|$ or $|\widetilde{R}(T,n)| = |R(T,n)|$.

We begin by considering $|\widetilde{R}(T,n)| < |R(T,n)|$. It follows from (170) that this situation occurs if and only if $T-m \le n \le 4[m/2]-T$ if $T+n \equiv 0 \mod (4)$ or $T-m \le n \le 4[m/2]-2-T$ if $T+n \equiv 2 \mod (4)$. Moreover from (163), (164) and (170) we get

$$|\widetilde{R}(T,n)| = \begin{cases} \frac{3T-n-4[m/2]}{4}, & \text{if } T+n \equiv 0 \mod (4) \\ \frac{3T+2-n-4[m/2]}{4}, & \text{if } T+n \equiv 2 \mod (4). \end{cases} \tag{184}$$

Now in view of Lemma 8.33 we have $|\widetilde{R}(T,n)| \leq |R(T,n)|-1 = |L(T,n)|$. Hence if we set $k = |\widetilde{R}(T,n)|-1$ and consider the equations (172) associated to the sequence $\{L_i = 2i+1 : 0 \leq i \leq k\} \subset L(T,n)$ we obtain a $(k+1) \times (k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ whose coefficient matrix $A(T,n)$ is the matrix $A(T-n)$ defined in (165) for $s = T-n$, $\delta = 0$ and corresponding to the sequence $\{L_i = 2i+1 : 0 \leq i \leq k\}$.

Set $T - n = 2\nu$. Since $n \leq 4[m/2] - T$ if $T+n \equiv 0 \mod (4)$ or $n \leq 4[m/2]-2-T$ if $T+n \equiv 2 \mod (4)$ it follows from (184) that $T-n \geq 2(k+1)$, hence the first condition of Corollary 8.40 is satisfied. Also from the same corollary it follows that 2ν is a root of $\det A(s)$ if and only if $T \geq 2[m/2]+2$, independently of the value of n. Observe that the only value of T that is not included in this range is $T = m$ whenever m is even. In this case the matrix $A(m-n)$ is nonsingular for all the corresponding values of n, hence $u^r_{T-r-n,n} = 0$ for every $r \in \widetilde{R}(T,n)$, proving that $Q(n+1)$ is true for $T = m$.

If $T \geq 2[m/2]+2$ the matrix $A(T-n)$ is singular for all the corresponding values of n, then in order to show that $Q(n+1)$ holds we need to use Proposition 8.44. To do this we must check that $m(2\nu) \leq |L'(T,n)|$. We begin by observing that from (180) we get

$$|L'(T,n)| = \begin{cases} \frac{n}{2}, & \text{if } T-m \leq n \leq \frac{T}{2} \\ \frac{T-n+2}{2} & \text{if } \frac{T}{2} < n \leq T. \end{cases} \tag{185}$$

On the other hand, since $\nu \geq k+1$, $\epsilon = 1$ and $T \equiv 0$, from (166) we get

$$m(2\nu) = \left[\tfrac{2k+2-\nu}{2}\right] = \tfrac{T-2[m/2]}{2}.$$

Then since n is even and $T - m \leq n$ it follows that $T - 2[m/2] \leq n$ which implies that $m(2\nu) \leq n/2$. Also, since $n \leq 4[m/2]-T$ and $T \geq 2[m/2]+2$, we get that $n < 2[m/2]+2$ which in turn implies that $m(2\nu) < (T-n+2)/2$. Therefore, in view of (185), we have $m(2\nu) \leq |L'(T,n)|$ as we wanted to prove. Hence Proposition 8.44 implies that $Q(n+1)$ is true.

Let us assume now that $|\widetilde{R}(T,n)| = |R(T,n)|$. It follows from (170) that this situation occurs if and only if $2[m/2]+2 \leq T \leq 2m$ and $\max\{T-m, 4[m/2]+4-T\} \leq n \leq T$ if $T+n \equiv 0 \mod (4)$ or $\max\{T-m, 4[m/2]+2-T\} \leq n \leq T$ if $T+n \equiv 2 \mod (4)$.

Now in view of Lemma 8.33 we have $|\widetilde{R}(T,n)| = |L(T,n)|+1$, therefore Theorem 8.43 does not provide us with enough equations to form a square system of linear equations in the elements $u^r_{T-r-n,n}$ with $r \in \widetilde{R}(T,n)$. In order to obtain such a system we need to add to equations (172) one more equation associated to some element $L \in L'(T,n)$. To do this we must check that $|L'(T,n)| \geq 1$ for every T and n we are considering. However this follows from (185) together with the fact that n is even and that $\max\{T-m, 4[m/2]+2-T\} \geq 1$ for all $m \geq 1$ and all T.

Then it follows from the definition of $L'(T,n)$, see (173), that $0 \in L'(T,n)$. Therefore if we consider $L = 0$ in Theorem 8.42, the first sum in equation (171) is empty, implying that the second sum gives rise to a new equation in the elements $u^r_{T-r-n,n}$ with $r \in \widetilde{R}(T,n)$. If we add this new equation to the equations obtained in Theorem 8.43 we obtain a $(k+1)\times(k+1)$ system of linear equations in the elements $u^r_{T-r-n,n}$ where $k = |\widetilde{R}(T,n)| - 1$. The coefficient matrix of this system is the matrix $A(T-n)$ defined in (165) for $s = T-n$, $\delta = 0$ and corresponding to the sequence $L(T,n) \cup \{0\} = \{0, 1, 3, \ldots, 2k-1\}$.

Next we shall analyze the matrix $A(T-n)$. It follows from (162) that $|\widetilde{R}(T,n)| = (T-n+2)/2$, therefore $T-n = 2k$. If $n = T$ or $n = T-2$ it is easy to see that the coefficient matrix of the system considered above is nonsingular, therefore we get $u^r_{T-r-n,n} = 0$ for every $r \in \widetilde{R}(T,n)$, as we wanted to prove.

Assume now that $n \leq T-4$. Then it follows from Theorem 8.39 (i) that $T-n = 2k$ is a root of $\det A(s)$ of multiplicity $m(2k) = [k/2]$, hence the matrix $A(2k)$ is singular. Moreover, if $A_i(2k)$ denotes the i-row of $A(2k)$, it follows from the proof Theorem 8.39 that $A_i(2k) = A_{k-i+1}(2k)$ for $1 \leq i \leq m(2k)$. Then, as we did in Proposition 8.44, we shall replace one row in each one of these pairs of equal rows by rows coming from new equations associated to elements $L \in L'(T,n)$. To do this we must check that $m(2k) \leq |L'(T,n) - \{0\}|$, since we have already used the equation corresponding to $L = 0$.

We begin by observing that

$$m(2k) = \begin{cases} \frac{T-n}{4}, & \text{if } T+n \equiv 0 \mod (4) \\ \frac{T-n-2}{4}, & \text{if } T+n \equiv 2 \mod (4). \end{cases}$$

Then, in view of (185), to prove that $m(2k) \leq |L'(T,n) - \{0\}|$ it is enough to show that $m(2k) \leq (n-2)/2$.

Now if $T+n \equiv 0 \mod (4)$ it is easy to see that every even n such that $n \geq \max\{T-m, 4[m/2]+4-T\}$ satisfies $n \geq (T+4)/3$ which in turns implies that $m(2k) \leq (n-2)/2$ as we wanted to prove. Similarly if $T+n \equiv 2 \mod (4)$ every even n such that $n \geq \max\{T-m, 4[m/2]+2-T\}$ satisfies $n \geq (T+2)/3$ which implies that $m(2k) \leq (n-2)/2$. Then in both cases we have $m(2k) \leq |L'(T,n) - \{0\}|$.

Then we use the equations corresponding to elements $L \in L'(T,n) - \{0\}$ to replace the equations associated to the rows $A_i(2k)$ of $A(2k)$ for $k - m(2k) + 1 \leq i \leq k$. If $A'(T,n)$ denotes the $(k+1)\times(k+1)$ coefficient matrix of this new linear system of equations in the elements $u^r_{T-r-n,n}$ with $r \in \widetilde{R}(T,n)$, it follows from Theorem 8.39 (i) that $A'(T,n)$ is nonsingular.

This implies that $u^r_{T-r-n,n} = 0$ for every $r \in \widetilde{R}(T,n)$ proving that $Q(n+1)$ holds. This completes the proof of Proposition 8.46.

References

[1] N. Andruskiewitsch and J. Tirao, *A restriction theorem for modules having a spherical submodule,* Trans. Amer. Math. Soc. **331, no. 2** (1992), 705-725.

[2] A. Brega and J. Tirao, *A transversality property of a derivation of the universal enveloping algebra U(k), for SO(n,1) and SU(n,1),* Manuscripta math. **74** (1992), 195-215.

[3] L. Cagliero, *Los residuos de los operadores de entrelazamiento de Kunze-Stein y el anillo clasificante de un grupo de Lie semisimple de rango uno,* Ph.D. Thesis (1998), Univ. N. de Córdoba.

[4] L. Cagliero and J. Tirao, *(K,M)-spherical modules of a rank one semisimple Lie group G_o,* Manuscripta math. **113** (2004), 107-124.

[5] A. Cooper, *The classifying ring of groups whose classifying ring is commutative,* Ph.D. Thesis (1975), MIT.

[6] A. Deitmar, *Invariant operators on higher K-types,* J. reine ungew. Math. **412** (1990), 97-107.

[7] R. Gangolli and V. S. Varadarajan, *Harmonic analysis of spherical functions on real reductive groups,* Ergeb. Math. Grenzgeb. 101, Springer-Verlag, Berlin, 1988.

[8] R. Godement, *A theory of spherical functions I,* Trans. Amer. Math. Soc. **73** (1952), 496-556.

[9] S. Helgason, *Differential geometry and symmetric spaces,* Academic Press, New York, 1964.

[10] R. Howe, *Some highly symmetrical dynamical systems,* preprint (unpublished).

[11] K. Johnson, *The centralizer of a Lie algebra in an envelopiing algebra,* J. reine ungew. Math. **395** (1989), 196-201.

[12] K. Johnson and N. Wallach, *Composition series and intertwining operators for the spherical principal series I,* Trans. Amer. Math. Soc. **229** (1977), 137-173.

[13] A. Knapp and E. Stein, *Intertwining operators for semisimple Lie groups,* Ann. of Math. **93** (1971), 489-578.

[14] B. Kostant, *On the existence and irreducibility of certain series of representations,* 1971 Summer School in Math. edited by I. M. Gelfand.

[15] F. Knop, *A Harish-Chandra homomorphism for reductive group actions,* Ann. of Math. **140** (1994), 253-288.

[16] B. Kostant and S. Rallis, *Orbits and representations associated with symmetric spaces,* Amer. J. Math. **93** (1971), 753-809.

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

[18] R. Kunze and E. Stein, *Uniformly bounded representations III. Intertwining operators for the principal series on semisimple groups,* Amer. J. Math. **89** (1967), 385-442.

[19] J. Lepowsky, *Algebraic results on representations of semisimple Lie groups,* Trans. Amer. Math. Soc. **176** (1973), 1-44.

[20] J. Lepowsky and G. W. McCollum, *On the determination of irreducible modules by restriction to a subalgebra,* Trans. Amer. Math. Soc. **176** (1973), 45-57.

[21] G. Schiffmann, *Integrales d'entrelacement et fonctiones de Whittaker,* Bull. Soc. Math. France **99** (1971), 3-72.

[22] J. Tirao, *Spherical functions,* Rev. Un. Mat. Argentina **28** (1977), 75-98.

[23] J. Tirao, *A restriction theorem for semisimple Lie groups of rank one,* Trans. Amer. Math. Soc. **279, no. 2** (1983), 651-660.

[24] J. Tirao, *On the centralizer of K in the universal enveloping algebra of* $\mathrm{SO}(n,1)$ *and* $\mathrm{SU}(n,1)$*,* Manuscripta math. **85** (1994), 119-139.

[25] J. Tirao, *On the left ideal in the universal enveloping algebra of a Lie group generated by a complex Lie subalgebra,* Proc. Amer. Math. Soc. **121, no. 4** (1994), 1257-1266.

[26] J. Tirao, *On the structure of the classifying ring of* $\mathrm{SO}(n,1)$ *and* $\mathrm{SU}(n,1)$*,* Rev. Unión Mat. Arg. **40** (1996), 15-31.

[27] N. Wallach, *Real Reductive groups I,* Academic Press, San Diego, 1988. Series title: Pure and Applied Mathematics, **132**.

[28] G. Warner, *Harmonic analysis on semi-simple Lie groups I,* Springer-Verlag, Berlin, 1972.

CIEM-FaMAF, Universidad Nacional de Córdoba, Córdoba 5000, Argentina
E-mail address: `brega@mate.uncor.edu`

CIEM-FaMAF, Universidad Nacional de Córdoba, Córdoba 5000, Argentina
E-mail address: `cagliero@mate.uncor.edu`

CIEM-FaMAF, Universidad Nacional de Córdoba, Córdoba 5000, Argentina
E-mail address: `tirao@mate.uncor.edu`