Astérisque

BERTRAM KOSTANT

The McKay correspondence, the Coxeter element and representation theory

Astérisque, tome S131 (1985), p. 209-255

<http://www.numdam.org/item?id=AST_1985__S131__209_0>

Société Mathématique de France
Astérisque, hors série, 1985, p. 209-255

THE McKAY CORRESPONDENCE, THE COXETER ELEMENT AND REPRESENTATION THEORY

BY

Bertram KOSTANT*

1.1. **Introduction.** — A fundamental question in harmonic analysis is : given a locally compact group G, a closed subgroup H, and an irreducible representation π of G, how does the restriction $\pi|H$ decompose. Consider this question in the following very basic situation : $G = SU(2)$ and $H = \Gamma$ is any finite subgroup of $SU(2)$. The classification of all finite subgroups Γ of $SU(2)$ is classical and well known. See e.g. [12] or [13]. Let $S(\mathbf{C}^2) = \bigoplus_{n=0}^{\infty} S^n(\mathbf{C}^2)$ be the symmetric algebra over $\mathbf{C}^2$ and let π_n be the representation of $SU(2)$ on $S^n(\mathbf{C}^2)$ induced by its action on $\mathbf{C}^2$. One knows π_n is irreducible for all n and the set of equivalence classes $\{\pi_n\}$, $n = 0, \ldots,$ defines the unitary dual of $SU(2)$. Now let $\Gamma \subseteq SU(2)$ be any finite group. The question then in this case is : how does $\pi_n|\Gamma$ decompose for any $n \in \mathbf{Z}_+$. The question is particularly interesting in the light of the McKAY correspondence. The latter sets up a bijection between $\widehat{\Gamma}$, the unitary dual of Γ, with the nodes of the extended Dynkin diagram of a simple Lie algebra $\mathbf{g}$, of type A, D or E. Thus, the question becomes : what is the multiplicity of a particular node for any $n \in \mathbf{Z}_+$.

The problem above has arisen recently in connection with the resolution of certain algebraic singularities. One way of dealing with it is by the use of the theory of complex reflection groups. The latter enables one to decompose polynomials into a sum of products of "invariants" and "harmonics". This is an old technique and its appropriateness in the present context was pointed out by P. SLODOWY. This approach has been carried out by G. GONZALEZ-SPRINBERG and J.-L. VERDIER in [2] and H. KNÖRRER in [5]. An effective

* Supported in part by NSF grant MCS 8105633.

method for computing these multiplicities is achieved and consequently one obtains an explanation of the McKay correspondence. However the multiplicities are not significantly related to $\mathbf{g}$ itself.

In this paper the whole matter is viewed in a completely different way. We accept the McKay correspondence; thereby setting up a bijection of all such Γ and all simple complex Lie algebras $\mathbf{g} = \mu(\Gamma)$ of type A, D and E. The question we ask is : in what way does Γ and the multiplicities in $\pi_n|\Gamma$ "see" the structure of $\mathbf{g}$ and vice versa. What we show is that these multiplicities come in a beautiful way from the root structure of $\mathbf{g}$. More explicitly they come from the orbit structure of the Coxeter element σ on the set of roots of $\mathbf{g}$. In fact the "harmonics" come from intersecting the orbits of σ with the roots of a distinguished Heisenberg subalgebra $\mathbf{n}$ of $\mathbf{g}$ and the "invariants" come from the scalar product of those roots in that orbit of σ which contains the highest root ψ. (The degree of the minimal "invariant" appears then as twice the coefficient of ψ at the branch point.) Besides making connection with $\pi_n|\Gamma$, new results in the orbit structure of σ are obtained. We remark that all the results are obtained using Lie theoretic principles and there is no reliance on empirical observations. Also, the decomposition itself into "invariants" times "harmonics" is seen in the root structure and there is no need for recourse to reflection group theory.

1.2. — Let $\Gamma \subseteq SU(2)$ be a non-trivial finite subgroup of $SU(2)$ and let $\{\gamma_0, \ldots, \gamma_l\} = \widehat{\Gamma}$ be the set of equivalence classes of irreducible finite dimensional complex representations of Γ. Then if $\gamma : \Gamma \to SU(2)$ is the given 2-dimensional representation one defines an $(l+1) \times (l+1)$ matrix $A(\Gamma)$ with entries in $\mathbf{Z}_+$ by decomposing the tensor product

$$\gamma_j \otimes \gamma = \Sigma_i A(\Gamma)_{ij} \gamma_i$$

into irreducible components. John McKay has made the remarkable observation (see [6] and [7]) that there exists a complex simple Lie algebra $\mathbf{g} = \mu(\Gamma)$ of rank l such that

$$A(\Gamma) = 2 - C(\widetilde{\mathbf{g}}),$$

where $\widetilde{\mathbf{g}}$ is the affine Kac-Moody Lie algebra associated to $\mathbf{g}$ and $C(\widetilde{\mathbf{g}})$ is a Cartan matrix of $\widetilde{\mathbf{g}}$. Moreover the correspondence $\Gamma \to \mu(\Gamma) = \mathbf{g}$ sets up a bijection between the set of all isomorphism classes of such subgroups $\Gamma \subseteq SU(2)$ and the set of all isomorphism classes of complex Lie algebras of type A, D and E.

The Cartan matrix $C(\widetilde{\mathbf{g}})$ is with respect to an ordered set of simple roots $\alpha_i \in \widetilde{\mathbf{h}}'$, $i = 0, \ldots, l$, where $\mathbf{h} \subseteq \widetilde{\mathbf{h}}$ are, respectively, Cartan subalgebras of $\mathbf{g} \subseteq \widetilde{\mathbf{g}}$. The indexing may be chosen so that γ_0 is the trivial representation of Γ and $\alpha_0 \in \widetilde{\mathbf{h}}'$ is the added simple root corresponding to the negative of the highest root $\psi \in \mathbf{h}'$ of $\mathbf{g}$. Now if

$$\pi_n \mid \Gamma = \sum_{i=0}^{l} m_i \gamma_i,$$

we associate to $\pi_n|\Gamma$ the element $v_n \in \widetilde{\mathbf{h}}'$ in the root lattice defined by putting

$$v_n = \sum_{i=0}^{l} m_i \alpha_i .$$

The problem we set for ourselves is then the determination of the generating function $P_\Gamma(t)$, with coefficients in $\widetilde{\mathbf{h}}'$, defined by putting

$$P_\Gamma(t) = \sum_{n=0}^{\infty} v_n t^n .$$

We restrict our attention to the cases where the Coxeter number $h = 2g$ of $\mathbf{g}$ is even (so that $g \in \mathbf{Z}_+$). This excludes only the case where Γ is a cyclic group of odd order. (The latter case is readily dealt with by considering first the cyclic group $\Gamma \times \mathbf{Z}_2$ of even order where $\mathbf{Z}_2 = \{\pm I\}$.) We can now speak of the special node i_* of the Dynkin diagram of $\mathbf{g}$. If $\mathbf{g} \not\cong A_l$ then i_* is the branch point. If $\mathbf{g} \cong A_{2m-1}$ (A_{2m} has been excluded) then i_* is the midpoint. Our main results will be stated in the following sequence of six theorems.

Remark. — In the light of Slodowy's observation (see § 1.1) the following result (THEOREM 1.3) is not new. However, the product decomposition in THEOREM 1.3 arises not from reflection group theory but from a study of the Coxeter element. As a consequence the numbers involved are directly related to the root structure of $\mathbf{g} = \mu(\Gamma)$. But then if one proceeds to make the connection with the reflection group theory one obtains as a theorem (not just an observation) that the numbers of reflecting hyperplanes is given in terms of the Coxeter number and the lesser degree of the two fundamental invariants is given in terms of the highest coefficient of the maximal root of $\mathbf{g}$.

THEOREM 1.3. — *There exist $z_i \in \widetilde{\mathbf{h}}'$, $i = 0, \ldots, h$, and even integers $2 \le a \le b \le h$ such that*

$$P_\Gamma(t) = \frac{\sum_{i=0}^{h} z_i t^i}{(1-t^a)(1-t^b)} . \tag{1.3.1}$$

The integers a and b are determined by the next result. The table of these values is given in THEOREM 5.17.

THEOREM 1.4. — *One has $a = 2d$ where $d = d_{i_*}$ is the coefficient of the highest root ψ corresponding to the special node i_* (1 for A_l, 2 for D_l, 3 for E_6, 4 for E_7 and 6 for E_8). Furthermore b is given by*

$$b = h + 2 - a. \tag{1.4.1}$$

In addition one has

$$ab = 2\,|\Gamma|\,. \tag{1.4.2}$$

If W is the (finite) Weyl group of $(\mathbf{h}, \mathbf{g})$ then one knows that there is a Coxeter element $\sigma \in W$ corresponding to $\Pi = \{\alpha_1, \ldots, \alpha_l\}$ such that $\sigma = \tau_2\tau_1$ where $\tau_2, \tau_1 \in W$ have order at most 2 and correspond to a decomposition $\Pi = \Pi_1 \cup \Pi_2$ into orthogonal sets. The order may be chosen so that $\tau_2\psi = \psi$. For $n \in \mathbf{Z}_+$ let $\tau_n = \tau_1$ if n is odd and $\tau_n = \tau_2$ if n is even. Also let $\tau^{(n)}$ be the alternating decreasing product $\tau^{(n)} = \tau_n\tau_{n-1}\cdots\tau_1$. Let $e = b/2$. The vectors z_i are determined in

THEOREM 1.5. — *One has $z_0 = z_h = \alpha_0$. For $n = 1, \ldots, h-1$, one has $z_n \in \mathbf{h}'$ (not just $\widetilde{\mathbf{h}}'$) and z_n is given by*

$$z_n = \tau^{(n-1)}\psi - \tau^{(n)}\psi, \tag{1.5.1}$$

where ψ is the highest root of $(\mathbf{h}, \mathbf{g})$. Furthermore

$$z_g = 2\alpha_{i_*} \tag{1.5.2}$$

and in general one has the symmetry

$$z_{g+k} = z_{g-k} \tag{1.5.3}$$

for $k = 1, \ldots, g$. Finally if $n = 1, \ldots, g-1$ there exists distinct $\alpha_{i_1}, \ldots, \alpha_{i_r} \in \Pi_j$, $j \in \{1, 2\}$, where $j \equiv n \bmod 2$ such that

$$z_n = \alpha_{i_1} + \cdots + \alpha_{i_r}. \tag{1.5.4}$$

Moreover

$$r = \begin{cases} 1 & \text{if } 1 \le n \le d-1\,; \\ 2 & \text{if } d \le n \le e-1\,; \\ 3 & \text{if } e \le n \le g-1\,; \end{cases} \tag{1.5.5.}$$

and in fact $r = 1, 2$, *or* 3 *according as to whether* $(\tau^{(n)}\psi, \tau^{(n-1)}\psi)$ *is positive, zero, or negative. For* $n = g+1, \ldots, h-1$ *the number* r *is then given by the symmetry* (1.5.3).

Remark 1.6. — Instead of generating z_n by the highest root ψ the z_n's can be generated in a manner similar to (1.5.1) using the simple root α_{i_*} instead of ψ. (See THEOREM 5.15).

1.7. — Now the Poincaré series $P_\Gamma(t)_i$ for the individual representations γ_i is obviously obtained by considering only the i^{th} coefficient of the vectors v_n. Clearly by THEOREM 1.3, using the subscript i for this coefficient

$$P_\Gamma(t)_i = \frac{z(t)_i}{(1-t^a)(1-t^b)},$$

where

$$z(t) = \sum_{n=0}^{h} z_n t^n.$$

Thus to determine $P_\Gamma(t)_i$ we have only to determine $z(t)_i$. Consider first the case $i = 0$. One notes that $P_\Gamma(t)_0$ is the Poincaré series for the algebra of invariants $S(\mathbf{C}^2)^\Gamma$. The following is known although probably not expressed in terms of the Coxeter number h of $\mathbf{g}$ and the largest coefficient $d = a/2$ of the highest root ψ of $(\mathbf{h}, \mathbf{g})$. It is an immediate consequence of THEOREM 1.5.

THEOREM 1.8. — *One has* $z(t)_0 = 1 + t^h$ *so that*

$$P_\Gamma(t)_0 = \frac{1+t^h}{(1-t^a)(1-t^b)}. \tag{1.8.1}$$

Next consider the case where $i = i_*$. One notes that γ_{i_*} is an irreducible representation of maximal dimension of Γ and is the unique such in case $\mu(\Gamma) = E_6$, E_7 or E_8. Observe that the coefficient of t^g is 2 in the following result. This is the only occurrence of a coefficient greater than 1 for any $z(t)_i$.

THEOREM 1.9. — *One has*

$$z(t)_{i_*} = \sum_{j=0}^{d-1} t^{g-2j} + \sum_{j=0}^{d-1} t^{g+2j}. \tag{1.9.1}$$

In particular $z(1)_{i_*} = a = 2d_{i_*}$.

1.10. — Now let Φ be the set of roots φ of $(\mathbf{h},\mathbf{g})$ such that $(\varphi,\psi)>0$; One has

$$\mathrm{Card}\Phi = 2h-3 \tag{1.10.1}$$

and one may refer to Φ as a Heisenberg system since a set of corresponding roots vectors span a Heisenberg Lie subalgebra of $\mathbf{g}$, of dimension $2h-3$. By intersecting Φ with the l orbits (naturally parametrized by Π) of the Coxeter element σ one obtains a partition

$$\Phi = \bigcup_{i=1}^{l} \Phi^i. \tag{1.10.2}$$

One proves

$$\mathrm{Card}\,\Phi^i = \begin{cases} 2d_i, & \text{if } i \neq i_* \\ 2d_i - 1, & \text{if } i = i_* \end{cases} \tag{1.10.3}$$

where the d_i are the coefficients of the highest root. That is

$$\psi = \sum_{i=1}^{l} d_i\alpha_i.$$

On the other hand there is a natural function $\varphi \mapsto n(\varphi) \in \mathbf{Z}_+$ on the set of positive roots defined using the $\tau^{(n)}$. Among other things it is injective on each Φ^i. The case for the remaining nodes is settled by

THEOREM 1.11. — *If $i \neq 0$ or i_* then*

$$z(t)_i = \sum_{\varphi\in\Phi^i} t^{n(\varphi)} \tag{1.11.1}$$

so that in particular all the coefficients of $z(t)_i$ are either 1 or 0. Furthermore the coefficients of t^{g-k} and t^{g+k} are equal for $k = 1,\ldots,g$ and vanish for $k=0$. Finally, (by (1.10.3)), $z(1)_i = 2d_i$.

2.1. **The McKay Correspondence.** — Let $\Gamma \subseteq SU(2)$ be any finite subgroup of $SU(2)$. Let $\widehat{\Gamma}$ be its representation dual (i.e., $\widehat{\Gamma}$ is the set of equivalence classes of complex, irreducible finite dimensional representations of Γ). Write $l+1$ for the cardinality of $\widehat{\Gamma}$ and order the elements of $\widehat{\Gamma}$ so that

$$\widehat{\Gamma} = \{\gamma_0,\gamma_1,\ldots,\gamma_l\}$$

where γ_0 is the 1-dimensional trivial representation of Γ. One now defines an $(l+1)\times(l+1)$ matrix $A(\Gamma)$ with non-negative integer entries as follows : The group Γ is given as a subgroup of $SU(2)$ so that the embedding $\Gamma \to SU(2)$ defines a distinguished 2-dimensional representation γ. (Note that γ is not necessarily irreducible.) If $1 \le i, j \le l+1$ let $a_{ij} \in \mathbf{Z}_+$ be defined by the tensor product decomposition

$$\gamma_j \otimes \gamma = \sum_{i=1}^{l+1} a_{ij}\gamma_i.$$

Then $A(\Gamma)$ is given by

$$(A(\Gamma))_{ij} = a_{ij}. \tag{2.1.1}$$

2.2. — Now let $\mathbf{g}$ be a complex simple Lie algebra of rank l and let $\mathbf{h}$ be a Cartan subalgebra of $\mathbf{g}$. Let $\mathbf{h}'$ be the dual space to $\mathbf{h}$ and let $\alpha_i \in \mathbf{h}'$, $i = 1, \ldots, l$, be an ordered set of simple positive roots with respect to some choice of a positive root system. The corresponding Cartan matrix $C(\mathbf{g})$ is the $l \times l$ matrix with integral entries defined by putting

$$(C(\mathbf{g}))_{ij} = \frac{2(\alpha_i, \alpha_j)}{(\alpha_i, \alpha_i)}, \tag{2.2.1}$$

where, as usual, the bilinear form, B, on $\mathbf{h}'$ is induced by the Killing form on $\mathbf{g}$. The Weyl group W of $(\mathbf{h}, \mathbf{g})$ will be regarded as operating on $\mathbf{h}'$.

Now associated to $\mathbf{g}$ is the corresponding affine Kac-Moody Lie algebra $\widetilde{\mathbf{g}}$ considered here, however, modulo the central extension. See e.g. [3]. (We will only use elementary facts about the root system of $\widetilde{\mathbf{g}}$.) We recall that the Cartan subalgebra $\widetilde{\mathbf{h}}$ of $\widetilde{\mathbf{g}}$ has dimension $l+1$. Also, we can regard $\mathbf{h}' \subseteq \widetilde{\mathbf{h}}'$ when $\widetilde{\mathbf{h}}'$ is the dual space to $\widetilde{\mathbf{h}}$ and an ordered set of simple (positive) roots $\alpha_i \in \widetilde{\mathbf{h}}'$, $i = 0, 1, \ldots, l$, of $(\widetilde{\mathbf{h}}, \widetilde{\mathbf{g}})$ includes the ordered set $(i > 0)$ of simple positive roots of $(\mathbf{h}, \mathbf{g})$. The α_i, $i \ge 0$, are a basis of $\widetilde{\mathbf{h}}'$ and one extends the bilinear form B to a symmetric (but singular) bilinear form $\widetilde{B}$ on $\widetilde{\mathbf{h}}'$ by putting

$$(\alpha_0, \alpha_i) = (-\psi, \alpha_i), \tag{2.2.2}$$

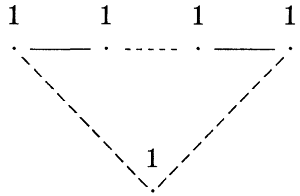
$i = 1, \ldots, l$, where ψ is the highest positive root of $(\mathbf{h}, \mathbf{g})$, and putting

$$(\alpha_0, \alpha_0) = (\psi, \psi). \tag{2.2.3}$$

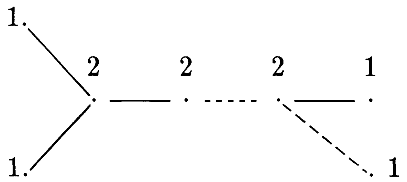
The Weyl group $\widetilde{W}$ of $(\widetilde{\mathbf{h}}, \widetilde{\mathbf{g}})$ — the so-called affine Weyl group — is the group, operating linearly on $\widetilde{\mathbf{h}}'$, generated by the reflections corresponding to the simple positive roots α_i, $i \geq 0$. (Note that $(\alpha_i, \alpha_i) > 0$ for $i \geq 0$.) In particular then we can regard $W \subseteq \widetilde{W}$ so that the action of W is now extended from an action on $\mathbf{h}'$ to an action on $\widetilde{\mathbf{h}}'$. The following well-known fact is immediate from (2.2.2) and (2.2.3).

PROPOSITION 2.3. — *The vector $\alpha_0 + \psi \in \widetilde{\mathbf{h}}'$ is $\widetilde{B}-$ orthogonal to every vector in $\widetilde{\mathbf{h}}'$ and consequently $\alpha_0 + \psi$ is fixed under the action of $\widetilde{W}$.*

2.4. — The Cartan matrix $C(\widetilde{\mathbf{g}})$ of $\widetilde{\mathbf{g}}$ is the $(l+1) \times (l+1)$ matrix defined by (2.2.1) for $i, j = 0, \ldots, l$, so that it contains $C(\mathbf{g})$ as an $l \times l$ principal minor. It is explicitly determined by the extended Dynkin diagram — a graph where the nodes correspond to the simple roots. We will only be concerned in this paper with the case where $\mathbf{g}$ is simply laced. That is, the case where (α_i, α_i) is independent of i — the A, D, E family. Then (2.2.1), if not zero, is -1 and this is indicated by a line segment joining the i^{th} and j^{th} nodes. We write down the extended Dynkin diagrams of the A, D, E family and include the coefficients of the $\widetilde{W}$-fixed vector $\alpha_0 + \psi$, relative to the simple roots, as superscripts above or to the side of the nodes. For clarity, the line segments joined to the 0^{th} node is made of dashes.

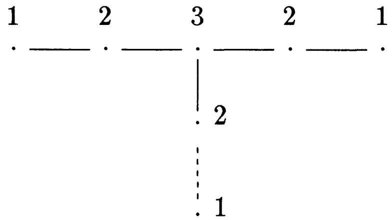


A_l

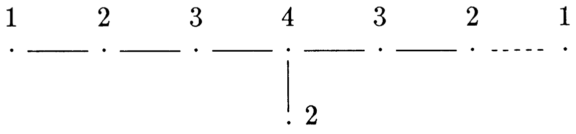


D_l

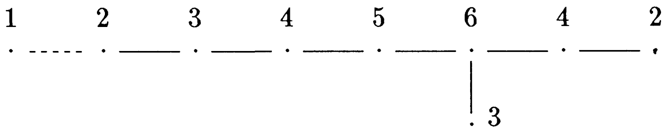
(2.4.1)



E_6



E_7



E_8

John McKAY made a remarkable observation relating the finite subgroups Γ of $SU(2)$ with the complex simple Lie algebras of type A, D and E. See [6] and [7]. The relation is established by an equality of matrices involving $A(\Gamma)$ on one hand and $C(\widetilde{\mathbf{g}})$ on the other.

THEOREM 2.5 (McKay correspondence). — *Let Γ be a non-trivial (i.e.,* $\operatorname{Card}\Gamma > 1$*) subgroup of $SU(2)$ and let the notation be as above. In particular, $A(\Gamma)$ is the $(l+1) \times (l+1)$ matrix defined by* (2.1.1). *Then there exists a complex simple Lie algebra $\mathbf{g}$ of rank l and of type A, D or E, unique up to isomorphism, and an ordering of the simple positive roots of the associated affine Kac-Moody Lie algebra $\widetilde{\mathbf{g}}$ together with a bijection $\{\gamma_j\} \mapsto \{\alpha_j\}$, $\gamma_j \mapsto \alpha_j$ (so that $\gamma_0 \to \alpha_0$) such that*

$$A(\Gamma) = 2I - C(\widetilde{\mathbf{g}}).$$

Here I is the $(l+1) \times (l+1)$ identity matrix. Moreover, the correspondence $\Gamma \mapsto \mathbf{g}$ sets up a bijection between the set of isomorphism classes of non-trivial finite subgroups of $SU(2)$ and the isomorphism classes of complex simple Lie algebras of type A, D and E.

Since the finite subgroups of $SU(2)$ and their representatives are well known, THEOREM 2.5 may be proved simply by checking. Among other results, a classification-free proof of THEOREM 2.5 has been given by STEINBERG in [11] and by ARTIN-VERDIER in [1]. See also SLODOWY, [8], Appendix III and [9].

2.6. — Let μ denote the McKay correspondence so that $\mathbf{g} = \mu(\Gamma)$ in the notation of THEOREM 2.5. If $\Gamma \subseteq SU(2)$ is a finite subgroup and j is a node in the extended Dynkin diagram D of $\mu(\Gamma)$ let $N(j)$ be the set of all nodes in D which are joined to j by a line segment. Note that $j \notin N(j)$. A well-known immediate consequence of THEOREM 2.5 is

COROLLARY 2.7. — *Let the notation be as in* THEOREM 2.5. *Then*

$$\gamma_j \otimes \gamma = \sum_{k \in N(j)} \gamma_k. \tag{2.7.1}$$

Now, recalling PROPOSITION 2.3, write

$$\alpha_0 + \psi = \sum_{i=0}^{l} d_i \alpha_i \tag{2.7.2}$$

so that the d_i are the integers appearing in the diagrams (2.4.1). Another well-known easy consequence of THEOREM 2.5 is

COROLLARY 2.8. — *Let the notation be as in* THEOREM 2.5 *and let* $\dim \gamma_j$ *be the dimension of the representation* γ_j. *Then*

$$\dim \gamma_j = d_j \tag{2.8.1}$$

for all $j = 0, \ldots, l$.

Proof. — A vector $x = \{x_j\} \in \mathbf{R}^{l+1}$, $j = 0, \ldots, l$, is an eigenvector of $A(\Gamma)$ with eigenvalue 2 if and only if for all j

$$2x_j = \sum_{k \in N(j)} x_k. \tag{2.8.2}$$

But $d = \{d_j\}$ satisfies this condition since $\alpha_0 + \psi$ is $\widetilde{W}$ invariant and $e = \{\dim \gamma_j\}$ satisfies this condition by Corollary (2.7.1). However, $d_0 = e_0 = 1$. Thus $d = e$ since 2 as an eigenvalue of $A(\Gamma)$ has multiplicity at most 1. This is clear because $C(\tilde{\mathbf{g}}) = 2I - A(\Gamma)$ has the non-singular $C(\mathbf{g})$ as a principal $l \times l$ minor. ∎

2.9. — Now for any $n = 2, 3, \ldots$, let (1) $\mathbf{Z}_n$ be a cyclic group of order n, (2) Δ_n be a dihedral group of order $2n$, (3) A_4 be an alternating group on 4 letters so that $|A_4| = 12$ (vertical lines denotes order), (4) S_4 be a symmetric group on 4 letters so that $|S_4| = 24$ and, finally, (5) A_5 be an alternating group on 5 letters so that $|A_5| = 60$.

The following is a well-known classical result. (See e.g., [12], § 2.6 or [13], Chap. I, § 6.)

THEOREM 2.10. — *A non-trivial finite group admits a faithful embedding in* $SO(3)$ *if and only if it is isomorphic to one of the groups above. In particular, then, the list above breaks up the set of non-trivial finite subgroups of* $SO(3)$ *into 5 distinct types.*

Now let

$$SU(2) \to SO(3) \tag{2.10.1}$$

be the usual double covering. If $F \subseteq SO(3)$ is a finite subgroup let $F^* \subseteq SU(2)$ be its inverse image so that

$$|F^*| = 2\,|F|\,. \tag{2.10.2}$$

Except for one special family all subgroups $\Gamma \subseteq SU(2)$ are of the form F^* for $F \subseteq SO(3)$.

PROPOSITION 2.11. — *Let $\Gamma \subseteq SU(2)$ then $\Gamma = F^*$ for some (necessarily unique) $F \subseteq SO(3)$ if and only if Γ is not a cyclic group of odd order.*

Proof. — One notes that Γ is of the form F^* for $F \subseteq SO(3)$ if and only if minus the identity is contained in Γ. But clearly this is the case if and only if $|\Gamma|$ is even. On the other hand, if $|\Gamma|$ is odd, Γ injects faithfully into $SO(3)$ under the map (2.10.1) but then Γ is cyclic of odd order by THEOREM 2.10. ∎

2.12. — In this paper we are primarily interested in only those subgroups of $SU(2)$ which are of the form F^* for $F \subseteq SO(3)$.The groups $\mathbf{Z}_n$, Δ_n, A_4, S_4 and A_5 listed above will henceforth (THEOREM 2.10) be regarded as subgroups of $SO(3)$ and hence $\mathbf{Z}_n^*$, Δ_n^*, A_4^*, S_4^* and A_5^* are subgroups of $SU(2)$.

PROPOSITION 2.13. — *With regard to the McKay correspondence one has*

$$\begin{array}{ll} (1) & \mu(\mathbf{Z}_n^*) = A_{2n-1}\,; \\ (2) & \mu(\Delta_n^*) = D_{n+2}\,; \\ (3) & \mu(A_4^*) = E_6\,; \\ (4) & \mu(S_4^*) = E_7\,; \\ (5) & \mu(A_5^*) = E_8. \end{array} \tag{2.13.1}$$

Proof. — This is stated in the McKay correspondence. However granting only THEOREM 2.5, the proof follows easily from the bijectivity in THEOREM 2.5 together with a comparison of (2.4.1) with the following well-known facts : (1) the numbers, $\dim\gamma$, where $\gamma \in \widehat{F}$, and $F = A_4$, S_4 and A_5 and (2) the commutativity of $\mathbf{Z}_n^*$ and the non-commutativity of Δ_n^*, as well as Card $\widehat{F}^*$ in these two cases. ∎

Remark 2.14. — It may also be noted that if $\Gamma \subseteq SU(2)$ is a cyclic group of order m, then $\mu(\Gamma) = A_{m-1}$. This then includes the case (m odd) not considered in PROPOSITION 2.13.

2.15. — Let $\mathbf{g}$ be a complex simple Lie algebra and let $h = h(\mathbf{g})$ be its Coxeter number. By definition h is the order of the Coxeter element in a Weyl group of $\mathbf{g}$. If $l = \operatorname{rank} \mathbf{g}$, we recall (see [4] THEOREM 8.4), that l divides $\dim \mathbf{g}$ and, in fact.

$$\dim \mathbf{g} = (h+1)l. \tag{2.15.1}$$

For the cases that concern us, we record

PROPOSITION 2.16.

(1) $h(A_m) = m + 1$,

so that in particular $h(A_{2n-1}) = 2n$;

(2) $h(D_{n+2}) = 2n + 2$;

(3) $h(E_6) = 12$;

(4) $h(E_7) = 18$;

(5) $h(E_8) = 30$.

With regard to the McKay correspondence one has

PROPOSITION 2.17. — *Let* $\Gamma \subseteq SU(2)$ *be any non-trivial subgroup. Put* $h = h(\mu(\Gamma))$ *then*

$$h = \sum_{\gamma \in \widehat{\Gamma}} \dim \gamma. \tag{2.17.1}$$

Proof. — It is a well-known fact that $h(\mathbf{g})$ is the sum of the coefficients (relative to the simple roots) of the highest root plus 1. (See [4], THEOREM 8.4.) The result then follows from (2.8.1). ∎

The reason for restricting ourselves to Γ of the form F^* for $F \subseteq SO(3)$ has to do with the parity of h. The significance of this will be apparent later on. The following proposition could be proved by comparing PROPOSITIONS 2.13 and 2.16. However a proof follows from general representation theoretic considerations.

PROPOSITION 2.18. — *Let the notation be as in* PROPOSITION 2.17. *Then h is even if and only if Γ is of the form F^* where $F \subseteq SO(3)$.*

Proof. — For any finite group E one knows that $\sum_{\gamma \in \widehat{E}} \dim \gamma$ is even if and only if $|E|$ is even (because $(\dim \gamma)^2 \equiv \dim \gamma \bmod 2$). The result then follows from PROPOSITION 2.17 and the proof of PROPOSITION 2.11. ∎

3.1. **The vectors v_n and the affine Coxeter element.** — Now let $S(\mathbf{C}^2)$ be the symmetric algebra over $\mathbf{C}^2$ and, for any $n \in \mathbf{Z}_+$, let $S^n(\mathbf{C}^2) \subseteq S(\mathbf{C}^2)$ be the subspace of homogeneous elements of degree n. The action of $SU(2)$ on $\mathbf{C}^2$ extends naturally to an action of $SU(2)$ on $S^n(\mathbf{C}^2)$ defining an irreducible representation π_n of $SU(2)$. Clearly $\dim \pi_n = n+1$ and one knows that the unitary dual, $S\widehat{U}(2)$, of $SU(2)$ may be described by

$$S\widehat{U}(2) = \{\pi_n\}, \quad n = 0, 1, \ldots$$

Now let $\Gamma \subseteq SU(2)$ be a non-trivial finite group and let the notation be as in § 2. The main problem we wish to consider in the paper is the determination of the restriction representation $\pi_n|\Gamma$ for any $n \in \mathbf{Z}_+$. This means determining the non-negative integers $m_j(n)$, $j = 0, 1, \ldots, l$, so that

$$\pi_n|\Gamma = \sum_{j=0}^{l} m_j(n)\gamma_j.$$

We can clearly deal with this question by considering instead the corresponding vector $v_n(\Gamma) = v_n$ in the dual $\widetilde{\mathbf{h}}'$ of the Cartan subalgebra $\widetilde{\mathbf{h}}$ of the affine Kac-Moody Lie algebra $\widetilde{\mathbf{g}}$. The vector v_n is defined by putting

$$v_n = \sum_{j=0}^{l} m_j(n)\alpha_j. \tag{3.1.1}$$

Note that if $\Lambda \subseteq \widehat{\mathbf{h}}'$, is the $\mathbf{Z}$-span of the roots — that is, the root lattice — then $v_n \in \Lambda$. Introducing a generating function $P_\Gamma(t)$ our problem then is the determination of the power series

$$P_\Gamma(t) = \sum_{n=0}^{\infty} v_n t^n \tag{3.1.2}$$

with elements of Λ as coefficients.

Remark 3.2. — One notes that in considering only the i^{th} component, $(v_n)_i$, of v_n one obtains the Poincaré series $P_\Gamma(t)_i$ for the representation $\gamma_i \in \widehat{\Gamma}$ with respect to the action of Γ on $S(\mathbf{C}^2)$. In particular for $i = 0$ this is just the Poincaré series for the algebra of invariants $S(\mathbf{C}^2)^\Gamma$.

3.3. — Now if V denotes the $\mathbf{C}$-vector space of all formal power series

$$x = \sum_{n=0}^{\infty} x_n t^n,$$

where $x_n \in \widetilde{\mathbf{h}}'$ then we may regard $B \in \operatorname{End} V$ where B is a formal power series

$$\sum_{t=0}^{\infty} B_n t^n$$

with $B_n \in \operatorname{End} \widetilde{\mathbf{h}}'$; one obtains Bx just as in the multiplication of scalar power series except that $B_j x_k \in \widetilde{\mathbf{h}}'$ replaces what would normally be a product of scalars.

Now let $A \in \operatorname{End} \widetilde{\mathbf{h}}'$ be the operator whose matrix with respect to the simple roots α_i, $i = 0, \ldots, l$, is just $A(\Gamma)$. One notes that

$$Av_n = v_{n+1} + v_{n-1} \tag{3.3.1}$$

for all $n \in \mathbf{Z}_+$ where $v_{-1} = 0$. This is clear from the definition of $A(\Gamma)$ (see 2.1.1) since by the Clebsch-Gordon formula for $SU(2)$ one has

$$\pi_n \otimes \pi_1 = \pi_{n+1} + \pi_{n-1}$$

where π_{-1} is the zero representation.

LEMMA 3.4. — *For any $n \in \mathbf{Z}_+$ one has*

$$v_n = \left[\sum_{j=0}^{[n/2]} (-1)^j \binom{n-j}{j} A^{n-2j}\right] \alpha_0. \tag{3.4.1}$$

Proof. — For convenience put $x = P_\Gamma(t) \in V$. Then by (3.3.1) one has

$$tAx = (1+t^2)x - v_0.$$

Thus $(1-(tA-t^2))x = v_0$. But since t factors out of $tA - t^2$ it is clear that $1-(tA-t^2)$ is invertible in $\operatorname{End} V$ and that

$$x = \sum_{k=0}^{\infty} B^k v_0,$$

where $B = tA - t^2 = t(A-t)$. Thus

$$B^k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} A^{k-j} t^{k+j}.$$

Putting $k+j=n$ we collect the coefficient of t^n in $\sum_{k=0}^{\infty} B^k$. One has $k=n-j$ and $k-j=n-2j$. Thus

$$\sum_{k=0}^{\infty} B^k = \sum_{n=0}^{\infty} \sum_{j=0}^{[n/2]} \left[(-1)^j \binom{n-j}{j} A^{n-2j}\right] t^n.$$

The result then follows since $v_0 = \alpha_0$. ∎

3.5. — Now let $\widetilde{P}$ be the set of integers $0,1,\ldots,l$, and let P be the subset with 0 deleted. Then as one knows (see e.g. [10] for details) we may partition P (in fact uniquely) as a disjoint union $P_1 \cup P_2$ so that for $j=1,2$ the set $\Pi_j = \{\alpha_i \mid i \in P_j\}$ consists of mutually orthogonal roots. If $P_j = \{i_1, i_2, \ldots, i_k\}$ let $\tau_j \in W$ be defined by putting

$$\tau_j = s_{i_1} s_{i_2} \cdots s_{i_k} \tag{3.5.1}$$

where $s_i \in \widetilde{W}$ for $i=0,\ldots,l$, is the reflection corresponding to the simple root α_i. The order in (3.5.1) is immaterial since the reflections in the product (3.5.1) commute with one another. In particular, one has

$${\tau_1}^2 = {\tau_2}^2 = e \text{ (the identity of } \widetilde{W}). \tag{3.5.2}$$

Now assume that Γ is of the form F^* where $F \subseteq SO(3)$. By Proposition 2.13 one notes that the extended Dynkin diagram contains no cycle of odd length. (This is also deducible from the parity of h.) In particular α_0 is orthogonal to all the elements in Π_1 or Π_2. Since we haven't fixed the labelling we now fix it so that α_0 is orthogonal to all the elements of Π_2. Let $\widetilde{\Pi}_2 = \Pi_2 \cup \{\alpha_0\}$ and let $\widetilde{\Pi}_1 = \Pi_1$. Also let $\widetilde{P}_2 = P_2 \cup \{0\}$ and $\widetilde{P}_1 = P_1$.

Now $-1 \in F^*$ where 1 here is the identity element in $SU(2)$. Given any $i \in \widetilde{P}$ one has $\gamma_i(-1) = \pm I$ where I is the identity operator on the module of γ_i. If $\gamma_i(-1) = I$ we may regard γ_j as a representation of F. The following proposition determines the sign and gives preliminary information on the non-zero components of v_n.

Proposition 3.6. — *Let the notation be as above. Then* $\gamma_i(-1) = (-1)^j I$ *where* $j \in \{1,2\}$ *is such that* $i \in \widetilde{P}_j$. *In particular*

$$\widehat{F} = \{\gamma_j \mid j \in \widetilde{P}_2\}. \tag{3.6.1}$$

Furthermore if we write for any $n \in \mathbf{Z}_+$,

$$v_n = \sum_{i=0}^{l} m_i(n) \alpha_i$$

then $m_i(n) = 0$ *for all* $i \in \widetilde{P}_j$ *where* $j - 1 \equiv n \bmod 2$.

Proof. — If $j \in \{1,2\}$ let $\widehat{j} \in \{1,2\}$ be such that set-wise $\{j, \widehat{j}\} = \{1,2\}$. Also let $Q_j \subseteq \widetilde{P}$ be defined by

$$Q_j = \{i \in \widetilde{P} | \gamma_i(-1) = (-1)^j I\}.$$

Now recalling (2.7.1) one has

$$N(i) \subseteq Q_{\widehat{j}} \tag{3.6.2}$$

for any i where j is such that $i \in Q_j$. (We are identifying $\widetilde{P}$ with the set of nodes of the extended Dynkin diagram.) This is clear since $\gamma(-1) = -1$. But (3.6.2) implies that the set of roots $\{\alpha_k | k \in Q_j\}$ are mutually orthogonal. However $0 \in Q_2$. By uniqueness one has $Q_j = \widetilde{P}_j$. This proves the first statement. The second follows immediately since $\pi_n(-1) = (-1)^n I$. ∎

3.7. — Now let $r_2 = s_0 \tau_2 = \tau_2 s_0$ and let $r_1 = \tau_1$. One clearly has

$$r_1{}^2 = r_2{}^2 = e. \tag{3.7.1}$$

The statement in the next lemma is implicit in [10] and even more so in [11].

LEMMA 3.8. — *One has*

$$A = r_1 + r_2. \tag{3.8.1}$$

Proof. — Let $i \in \widetilde{P}$. Then $i \in \widetilde{P}_j$ for some $j \in \{1,2\}$. Clearly $r_j \alpha_i = -\alpha_i$. But, using the notation in the proof of PROPOSITION 3.6,

$$r_{\widehat{j}} \alpha_i = \alpha_i - \sum \frac{2(\alpha_k, \alpha_i)}{(\alpha_k, \alpha_k)} \alpha_k$$

where the sum is over $k \in \widetilde{P}_{\widehat{j}}$. But then since the sum for $k \in \widetilde{P}_j$ of the $(2(\alpha_k, \alpha_i)/(\alpha_k, \alpha_k))\alpha_k$ is equal to $2\alpha_i$, and $\widetilde{P}_j \cup \widetilde{P}_{\widehat{j}} = \{0, \ldots, l\}$, one has

$$(r_1 + r_2)\alpha_i = 2\alpha_i - \sum_{k=0}^{l} \frac{2(\alpha_k, \alpha_i)}{(\alpha_k, \alpha_k)} \alpha_k.$$

Thus $(r_1 + r_2)\alpha_i = A\alpha_i$ since $A(\Gamma) = 2I - C(\widetilde{\mathfrak{g}})$ by THEOREM 2.5. ∎

3.9. — Let $c = r_2 r_1$ so that c is a Coxeter element of $\widetilde{W}$. It is *not* a Coxeter element of W. By (3.7.1) and (3.8.1) one has

$$A^2 = c + c^{-1} + 2I \tag{3.9.1}$$

where I here is the identity operator on $\widetilde{\mathfrak{h}}'$.

LEMMA 3.10. — *For any $m \in \mathbf{Z}_+$ one has*

$$A^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} c^{k-m}. \tag{3.10.1}$$

Proof. — Let $a = c + I$ and $b = c^{-1} + I$ so that $A^2 = a + b$ by (3.9.1). But clearly $a + b = ab$ and a and b commute. Thus

$$A^{2m} = a^m b^m$$

But $b = ac^{-1}$. Thus $A^{2m} = a^{2m} c^{-m}$. However,

$$a^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} c^k. \quad \blacksquare$$

We can now make an improvement on Lemma 3.4. We first need some relations involving binomial coefficients.

LEMMA 3.11. — *Let $j, n \in \mathbf{Z}_+$, where $j \le n$. Then*

$$\sum_{i=0}^{j} (-1)^i \binom{n-2i}{j-i} \binom{n-i}{i} = 1 \tag{3.11.1}$$

and

$$\sum_{i=0}^{j} (-1)^i \binom{n-2i}{j-i} \binom{n+1-i}{i} = \begin{cases} 1 & \textit{if } j \text{ is even,} \\ 0 & \textit{if } j \text{ is odd.} \end{cases} \tag{3.11.2}$$

Proof. — Because of the cancellation of $(n-2i)!$ the i^{th} term on the left side of (3.11.1) may be written $\binom{j}{i} \binom{n-i}{j}$. Therefore to prove (3.11.1) it suffices to establish

$$\sum_{i=0}^{j} (-1)^i \binom{j}{i} \binom{n-i}{j} = 1. \tag{3.11.3}$$

But as one knows

$$\frac{1}{(1-t)^{j+1}} = \sum_{k=j}^{\infty} \binom{k}{j} t^{k-j},$$

so that the left side of (3.11.3) is just the computation of the coefficient of t^{n-j} in the product $(1-t)^j/(1-t)^{j+1}$. But this product is just $\Sigma_{i=0}^{\infty} t^i$. This proves (3.11.1).

We will prove (3.11.2) by induction on j. It is clearly true if $j = 0$. Hence assume $j > 0$ and the result is true for smaller values. Clearly the result is true for $n = j$. Assume $n > j$. We may write

$$\binom{n+1-i}{i} = \binom{n-i}{i} + \binom{n-i}{i-1}, \tag{3.11.4}$$

so that the left side of (3.11.2) decomposes into two sums. But one of the sums is just the left side of (3.11.1) and hence by (3.11.1) we have to show that

$$\sum_{i=1}^{j} (-1)^i \binom{n-2i}{j-i} \binom{n-i}{i-1} = \begin{cases} 0 & \text{if } j \text{ is even,} \\ -1 & \text{if } j \text{ is odd.} \end{cases} \tag{3.11.5}$$

But putting $i - 1 = k$ and $n - 2 = m$ the left side of (3.11.5) is just

$$-\sum_{k=0}^{j-1} (-1)^k \binom{m-2k}{j-1-k} \binom{m+1-k}{k}.$$

But this is just the negative of the left side of (3.11.2) where m replaces n and $j-1 \leq m$ replaces j. The result then follows by the induction assumption. ∎

If $n = 2m$ is even, the following result expresses v_n as a partial sum of the elements in the orbit of α_0 under the action of the extended Coxeter element $c \in \widetilde{W}$. Since, among other things, c does not have finite order the result is still not yet clarifying.

If $n = 2m + 1$ is odd, we must replace $\alpha_0 = v_0$ by v_1. Note that in this case the partial sum involves every other power of c rather than consecutive powers.

PROPOSITION 3.12. — *If $n = 2m$ is even then*

$$v_n = \left[\sum_{j=0}^{2m} c^{j-m}\right] \alpha_0 \tag{3.12.1}$$

and if $n = 2m + 1$ is odd then

$$v_n = \left[\sum_{j=0}^{m} c^{2j-m}\right] v_1. \tag{3.12.2}$$

Proof. — If $n = 2m$, then by (3.4.1)

$$v_n = \sum_{i=0}^{m}(-1)^i \binom{n-i}{i} A^{2(m-i)}\alpha_0.$$

But then substituting $m - i$ for m in Lemma 3.10 we have, by (3.10.1),

$$v_n = \sum_{i=0}^{m}(-1)^i \binom{n-i}{i} \sum_{k=0}^{n-2i} \binom{n-2i}{k} c^{k+i-m}\alpha_0. \tag{3.12.3}$$

Writing $j = k + i$ and substituting $j - i$ for k in (3.12.3) it is clear that j takes all values from 0 to n and that we can regard i as taking all values from 0 to j. Thus

$$v_n = \sum_{j=0}^{n}\left[\sum_{i=0}^{j}(-1)^i \binom{n-i}{i}\binom{n-2i}{j-i}\right] c^{j-m}\alpha_0.$$

The result (3.12.1) then follows from (3.11.1). Now assume $n = 2m + 1$. Put $n_0 = 2m$. Clearly $A\alpha_0 = v_1$ by (3.3.1). Thus by (3.4.1)

$$v_n = \sum_{i=0}^{m}(-1)^i \binom{n_0+1-i}{i} A^{2(m-i)} v_1$$

and hence by (3.10.1)

$$v_n = \sum_{i=0}^{m}(-1)^i \binom{n_0+1-i}{i} \sum_{k=0}^{n_0-2i} \binom{n_0-2i}{k} c^{k+i-m} v_1.$$

Again putting $j = k + i$ we may take i and j arbitrary such that $0 \leq i \leq j \leq n_0$ and, hence, we may write

$$v_n = \sum_{j=0}^{2m}\left[\sum_{i=0}^{j}(-1)^i \binom{n_0+1-i}{i}\binom{n_0-2i}{j-i}\right] c^{j-m} v_1.$$

The result then follows from (3.11.2). ∎

4.1. The Coxeter element $\sigma \in W$ and the product formula for $P_\Gamma(t)$. We now consider the element $\sigma = \tau_2\tau_1 \in W$. Clearly σ is a Coxeter element in W. One thus has $\sigma^h = e$ where h as in § 2.15, is the Coxeter number of $\mathbf{g}$. Since $s_0\tau_2 = r_2$ and $\tau_1 = r_1$ we note also that

$$c = s_0\sigma. \tag{4.1.1}$$

Recalling the bilinear form $\widetilde{B}$ on $\widetilde{\mathbf{h}}'$ let $a_0 = 1$ and put, for positive $k \in \mathbf{Z}_+$,

$$a_k = 2\frac{(\sigma^k\alpha_0, \alpha_0)}{(\alpha_0, \alpha_0)}. \tag{4.1.2}$$

Then $a_k \in \mathbf{Z}$ since $\sigma^k\alpha_0$ is in the root lattice. Since $\sum_{k=0}^{\infty} a_k t^k$ is invertible in the ring of all such power series, we can define a sequence $b_k \in \mathbf{Z}$, $k = 0, 1, \ldots$, by inversion. That is, the sequence is defined, so that

$$\sum_{k=0}^{\infty} a_k\, t^k \sum_{j=0}^{\infty} b_j\, t^j = 1. \tag{4.1.3}$$

We may thus define b_k inductively so that for positive k

$$b_k = -\sum_{j=0}^{k-1} b_j\, a_{k-j} \tag{4.1.4}$$

and $b_0 = 1$.

We proceed now to convert from c to σ in PROPOSITION (3.12). We first observe

LEMMA 4.2. — *For any $k \in \mathbf{Z}_+$ one has*

$$c^k\alpha_0 = \sum_{j=0}^{k} b_j\, \sigma^{k-j}\alpha_0. \tag{4.2.1}$$

Proof. — The proof will be by induction on k. It is clearly true for $k = 0$. Hence, assume $k > 0$ and that the result is true for smaller values. Since it is then true for $k-1$ we have upon applying c to both sides of (4.2.1), where $k-1$ replaces k,

$$c^k\alpha_0 = \sum_{j=0}^{k-1} b_j\, s_0\, \sigma^{k-j}\alpha_0$$

because $c = s_0\sigma$. But $s_0\sigma^{k-j}\alpha_0 = \sigma^{k-j}\alpha_0 - a_{k-j}\alpha_0$. Thus

$$c^k\alpha_0 = \sum_{j=0}^{k-1} b_j\,\sigma^{k-j}\alpha_0 - \left[\sum_{j=0}^{k-1} b_j\,a_{k-j}\right]\alpha_0.$$

But then the result follows from (4.1.4). ∎

Now note that for any $k \in \mathbf{Z}_+$ and $i = 1, 2$ that

(4.2.2) $$c^k r_i = r_i c^{-k}.$$

We also note that

(4.2.3) $$c^k r_1 = c^{k-1} r_2$$

and

(4.2.4) $$r_2 c^k = r_1 c^{k-1}.$$

LEMMA 4.3. — *For any positive $k \in \mathbf{Z}_+$ one has*

$$c^{-k}\alpha_0 = -\sum_{j=0}^{k-1} b_j\,\tau_1\sigma^{k-1-j}\,\alpha_0.$$

Proof. — Clearly (see § 3.5)

(4.3.1) $$\tau_2\alpha_0 = \alpha_0$$

so that, since $r_2 = s_0\tau_2 = \tau_2 s_0$,

(4.3.2) $$r_2\alpha_0 = -\alpha_0.$$

But then $c^{-k}\alpha_0 = -c^{-k}r_2\alpha_0 = -r_2c^k\alpha_0$ by (4.2.2) and hence $c^{-k}\alpha_0 = -r_1c^{k-1}\alpha_0$ by (4.2.4). But $r_1 = \tau_1$. Thus $c^{-k}\alpha_0 = -\tau_1c^{k-1}\alpha_0$. The result then follows from (4.2.1). ∎

4.4. — Now for any $n \in \mathbf{Z}_+$ let

(4.4.1) $$\tau_n = \begin{cases} \tau_1 & \text{if } n \text{ is odd,} \\ \tau_2 & \text{if } n \text{ is even.} \end{cases}$$

Also put $\tau^{(0)} = e$ and for n positive let

$$\tau^{(n)} = \tau_n \tau_{n-1} \cdots \tau_2 \tau_1 \tag{4.4.2}$$

so that $\tau^{(n)}$ is an alternating product of τ_2 and τ_1 with n factors. In particular if $n = 2m$ is even then

$$\tau^{(n)} = \sigma^m, \tag{4.4.3}$$

and if $n = 2m + 1$ is odd then

$$\tau^{(n)} = \tau_1 \sigma^m. \tag{4.4.4}$$

Now let $u_n \in \widetilde{\mathbf{h}}'$ be defined by putting

$$u_n = \tau^{(n)} \alpha_0. \tag{4.4.5}$$

Remark 4.5. — If $D(\sigma) \subseteq W$ is the subgroup generated by τ_1 and τ_2 note that $D(\sigma)$ is isomorphic to the dihedral group of order $2h$ having the cyclic group $D_+(\sigma)$ generated by σ as a normal subgroup of order h. Thus we have that

$$D(\sigma)\alpha_0 = \{u_n \mid n = 0, 1, \ldots\}.$$

Also, since α_0 is a root of $(\widetilde{\mathbf{h}}, \widetilde{\mathbf{g}})$, note that u_n is a root of $(\widetilde{\mathbf{h}}, \widetilde{\mathbf{g}})$ for all $n \in \mathbf{Z}_+$.

Now let $w_0 = u_0 = \alpha_0$ and for $n \in \mathbf{Z}_+$ positive let

$$w_n = u_n - u_{n-1}. \tag{4.5.1}$$

Also for any $n \in \mathbf{Z}_+$ let

$$f_n = \sum_{i=0}^{n} b_i. \tag{4.5.2}$$

LEMMA 4.6. — *For any $n \in \mathbf{Z}_+$ one has*

$$v_n = \sum_{j=0}^{[n/2]} f_j w_{n-2j}. \tag{4.6.1}$$

Proof. — First assume that $n = 2m$ is even. Then by Lemmas 4.2 and 4.3 one has

$$c^k \alpha_0 + c^{-k} \alpha_0 = b_k \alpha_0 + \sum_{j=0}^{k-1} b_j (\sigma^{k-j} \alpha_0 - \tau_1 \sigma^{k-j-1} \alpha_0)$$

for any positive $k \in \mathbf{Z}_+$. But $u_{2(k-j)} = \sigma^{k-j}\alpha_0$ and $u_{2(k-j)-1} = \tau_1\sigma^{k-j-1}\alpha_0$ by (4.4.3) and (4.4.4). Thus

$$c^k\alpha_0 + c^{-k}\alpha_0 = \sum_{j=0}^{k} b_j\, w_{2k-2j}.$$

Summing for $k = 1, \ldots, m$ and adding $\alpha_0 = b_0 w_0$ one has

$$v_n = \sum_{k=0}^{m}\sum_{j=0}^{k} b_j\, w_{2k-2j} \tag{4.6.2}$$

by (3.12.1). Now putting $i = m - k + j$ so that $2k - 2j = n - 2i$ then, in the sum (4.6.2), i ranges from 0 to m and j, fixing i, ranges from 0 to i. Thus we may rewrite

$$v_n = \sum_{i=0}^{m}\left[\sum_{j=0}^{i} b_j\right] w_{n-2i}.$$

The result then follows for $n = 2m$ by (4.5.2).

Now assume $n = 2m + 1$ is odd. Recall that $v_1 = Av_0 = A\alpha_0$ by (3.3.1). But $A = r_1 + r_2$ by (3.8.1). Let $k \in \mathbf{Z}_+$ be positive. Then $c^k v_1 = c^k r_1\alpha_0 + c^k r_2\alpha_0 = c^{k-1} r_2\alpha_0 + c^k r_2\alpha_0$ by (4.2.3). But then by (4.3.2)

$$c^k v_1 = -c^{k-1}\alpha_0 - c^k\alpha_0. \tag{4.6.3}$$

But now $c^{-k}v_1 = c^{-k}r_1\alpha_0 + c^{-k}r_2\alpha_0 = r_1 c^k\alpha_0 + r_2 c^k\alpha_0$ by (4.2.2). However $r_2 c^k = r_1 c^{k-1}$ by (4.2.4). Since $r_1 = \tau_1$ we have

$$c^{-k}v_1 = \tau_1 c^{k-1}\alpha_0 + \tau_1 c^k\alpha_0. \tag{4.6.4}$$

Thus adding (4.6.3) and (4.6.4) and recalling (4.2.1)

$$\begin{aligned} c^k v_1 + c^{-k} v_1 &= (\tau_1 c^{k-1} - c^{k-1})\alpha_0 + (\tau_1 c^k - c^k)\alpha_0 \\ &= \sum_{j=0}^{k-1} b_j(\tau_1\sigma^{k-1-j} - \sigma^{k-1-j})\alpha_0 + \sum_{j=0}^{k} b_j(\tau_1\sigma^{k-j} - \sigma^{k-j})\alpha_0 \\ &= \sum_{j=0}^{k-1} b_j w_{2(k-1-j)+1} + \sum_{j=0}^{k} b_j w_{2(k-j)+1} \end{aligned}$$

by (4.4.3), (4.4.4) and (4.5.1).

Now summing over the values $k = 1, 3, \ldots, m$, in case m is odd and $k = 2, 4, \ldots, m$, in case m is even and adding, in the latter case, $v_1 = r_1\alpha_0 + r_2\alpha_0 = \tau_1\alpha_0 - \alpha_0 = w_1 = b_0 w_1$ one has, by (3.12.2),

$$v_n = \sum_{k=0}^{m}\sum_{j=0}^{k} b_j\, w_{2(k-j)+1}.$$

Now, as before, put $i = m - k + j$ so that $2(k-j)+1 = n - 2i$. Then i ranges from 0 to $m = [n/2]$ and j from 0 to i and we may write

$$v_n = \sum_{i=0}^{m}\left[\sum_{j=0}^{i} b_j\right] w_{n-2i}$$

and hence the result follows from (4.5.2). ∎

We may express Lemma 4.6 in a more convenient form. Let

$$f(t) = \sum_{j=0}^{\infty} f_j t^{2j}$$

and let

$$w(t) = \sum_{i=0}^{\infty} w_i t^i.$$

We recall also the definition of the generating function $P_\Gamma(t)$ (see § 3.1). Then the following factorization of $P_\Gamma(t)$ is a restatement of LEMMA 4.6. The "product" is well defined since the coefficients of $f(t)$ are scalars and the coefficients of $w(t)$ are vectors in $\widetilde{\mathbf{h}}'$.

LEMMA 4.7. — *One has*

$$P_\Gamma(t) = f(t)w(t).$$

4.8. — Now let $\kappa \in W$ be the long element of the Weyl group W so that, in particular, $\kappa^2 = e$. The element κ takes the positive roots of $(\mathbf{h}, \mathbf{g})$ to the negative roots and hence in particular.

$$\kappa\psi = -\psi, \tag{4.8.1}$$

where, we recall, ψ is the highest root.

We recall (see PROPOSITION 2.18) that the Coxeter number h is even. Let $h/2 = g \in \mathbf{Z}_+$. The following is well known and due to STEINBERG.

LEMMA 4.9. — *One has $\sigma^g = \kappa$.*

Proof. — This is in fact implicit in [10]. Using the notation of THEOREM 6.3 in [10] one has that $\sigma^g = (R_1 \cdots R_n)^{h/2}$. But then THEOREM 6.3 in [10] asserts that σ^g carries all the positive roots into negative roots. Thus $\sigma^g = \kappa$. ∎

We note, by LEMMA 4.9 and (4.8.1), that

$$\sigma^g \psi = -\psi. \tag{4.9.1}$$

4.10. — Now for $i = 0, 1, \ldots, h-1$, let

$$z_i = w_i \tag{4.10.1}$$

but we put

$$z_0 = \alpha_0 \tag{4.10.2}$$

so that z_n is defined for $n = 0, \ldots, h$. The following observation will later be important for us. It asserts in effect that the α_0-component of z_n vanishes for $1 \le n \le h-1$.

LEMMA 4.11. — *One has $z_0 = z_h = \alpha_0$ but $z_n \in \mathbf{h}'$ for $1 \le n \le h-1$.*

Proof. — By definition $z_0 = z_h = \alpha_0$. But now since $\tau_j \in W$ for $j = 1, 2$ it follows that

$$u_n - \alpha_0 \in \mathbf{h}'$$

for any $n \in \mathbf{Z}_+$. (See (4.4.5).) Thus $w_n \in \mathbf{h}'$ for all $n \ge 1$. ∎

Let

$$z(t) = \sum_{i=0}^{h} z_i t^i. \tag{4.11.1}$$

The next lemma is a key point. It asserts that we can reduce $w(t)$ to a finite sum.

LEMMA 4.12. — *One has*

$$w(t) = \frac{z(t)}{1 + t^h}.$$

Proof. — Let $u(t) = \sum_{j=0}^{\infty} u_j t^j$. By definition of w_j one clearly has

$$w(t) = (1-t)u(t). \tag{4.12.1}$$

But now obviously

$$u_h = \sigma^g \alpha_0.$$

Write $\alpha_0 = (\alpha_0 + \psi) - \psi$. But then by PROPOSITION 2.3 and (4.9.1) one has

$$u_h = \alpha_0 + 2\psi = 2(\alpha_0 + \psi) - \alpha_0 \tag{4.12.2}$$

and hence $u_0 + u_h = 2(\alpha_0 + \psi)$. But then by PROPOSITION 2.3 this element is invariant under W and hence, upon applying τ_1 and τ_2 alternately, we have

$$u_j + u_{j+h} = 2(\alpha_0 + \psi) \tag{4.12.3}$$

for any $j \in \mathbf{Z}_+$. Thus if $\overline{u}(t)$ is the finite sum $\sum_{i=0}^{h-1} u_i t^i$ then

$$u(t)(1 + t^h) = \overline{u}(t) + 2(\alpha_0 + \psi)\frac{t^h}{1-t}. \tag{4.12.4}$$

Now let $\overline{w}(t)$ be the finite sum $\sum_{i=0}^{h-1} w_i t^i$. Then clearly

$$(1-t)\overline{u}(t) = \overline{w}(t) - u_{h-1}t^h. \tag{4.12.5}$$

But now

$$\tau_2 \psi = \psi \tag{4.12.6}$$

by (4.3.1), since $\psi = (\alpha_0 + \psi) - \alpha_0$ (recalling PROPOSITION 2.3). But since $u_h = \alpha_0 + 2\psi$ by (4.12.2) it follows from both (4.3.1) and (4.12.6) that u_h is fixed by τ_2. However $u_h = \tau_2 u_{h-1}$ since h is even and hence $u_{h-1} = \tau_2 u_h$. Thus we also have

$$u_{h-1} = \alpha_0 + 2\psi. \tag{4.12.7}$$

Now multiplying (4.12.4) by $1 - t$ it then follows from (4.12.1), (4.12.5) and (4.12.7) that

$$\begin{aligned} w(t)(1 + t^h) &= \overline{w}(t) - (\alpha_0 + 2\psi)t^h + 2(\alpha_0 + \psi)t^h \\ &= \overline{w}(t) + \alpha_0 t^h. \end{aligned}$$

But $\overline{w}(t) + \alpha_0 t^h = z(t)$ by definition of $z(t)$. This proves the lemma. ∎

4.13. — We now proceed to express $f(t)$ in terms of polynomials. Let $a(t) = \sum\limits_{j=0}^{\infty} a_j t^{2j}$ and $b(t) = \sum\limits_{i=0}^{\infty} b_i t^{2i}$ so that, by (4.1.3), $b(t) = 1/a(t)$. But now, by definition, clearly $f(t) = b(t)/(1 - t^2)$ and hence

$$f(t) = \frac{1}{(1-t^2)a(t)}. \tag{4.13.1}$$

Now if $g > 1$ put, for $i = 1, \ldots, g-1$,

$$c_i = \frac{2(\sigma^i\psi, \psi)}{(\psi, \psi)} \tag{4.13.2}$$

and in any case put

$$c_0 = 1 \text{ and } c_g = -1. \tag{4.13.3}$$

Thus in any case we can define a polynomial $c(t)$ of degree h by putting $c(t) = \sum_{j=0}^{g} c_j t^{2j}$.

LEMMA 4.14. — *One has*

$$(1 + t^h)a(t) = c(t).$$

Proof. — We note first that for any $j \geq 1$

$$a_j = \frac{2(\sigma^j\psi, \psi)}{(\psi, \psi)}. \tag{4.14.1}$$

Indeed we may write $\alpha_0 = (\alpha_0 + \psi) - \psi$. But since $\alpha_0 + \psi$ is $\widetilde{B}$ orthogonal to $\widetilde{\mathfrak{h}}'$ one obtains (4.14.1) by substituting $(\alpha_0 + \psi) - \psi$ for α_0 in (4.1.2). But now by (4.9.1) one has

$$a_{j+g} + a_j = 0 \tag{4.14.2}$$

for all positive j and $a_g + a_0 = -1$. Thus if $\overline{a}(t) = \sum_{j=0}^{g-1} a_j t^{2j}$ one has

$$(1 + t^h)a(t) = \overline{a}(t) - t^h.$$

But $\overline{a}(t) - t^h$ is just $c(t)$ by (4.13.2) and (4.13.3). ∎

4.15. — What is significant is the "jumps" in the numbers c_i. Let $q_0 = q_{g+1} = 1$ and for $j = 1, \ldots, g$, let

$$q_i = c_i - c_{i-1}. \tag{4.15.1}$$

One then defines a polynomial $q(t)$ of degree $h + 2$ by putting

$$q(t) = \sum_{i=0}^{g+1} q_i t^{2i}. \tag{4.15.2}$$

It will later be seen that $q(t)$ has a particularly simple form.

LEMMA 4.16. — *One has*

$$q(t) = (1 - t^2)c(t).$$

Proof. — This is obvious from the definition. One has only to notice that the coefficient of t^{h+2} equals 1 in the product since $c_g = -1$. ∎

The following lemma summarizes much of the above. It reduces the generating function $P_\Gamma(t)$ to a quotient of explicit finite sums.

LEMMA 4.17. — *One has*

$$P_\Gamma(t) = \frac{z(t)}{q(t)}.$$

Proof. — By LEMMA 4.7 one has $P_\Gamma(t) = f(t)w(t)$. But then by LEMMA 4.12 one has

$$P_\Gamma(t) = \frac{f(t)z(t)}{1+t^h}$$

and hence by (4.13.1)

$$P_\Gamma(t) = \frac{z(t)}{(1+t^h)(1-t^2)a(t)}.$$

But $(1+t^h)a(t) = c(t)$ by LEMMA 4.14 and hence the result follows from LEMMA 4.16. ∎

5.1. The root structure of $\mathfrak{g}$ and the simplification of the product formula for $P_\Gamma(t)$. — We now wish to be much more explicit about the polynomial $q(t)$ and the vectors $z_i \in \mathbf{h}'$ for $i = 1, \ldots, h-1$.

Let $\Delta \subseteq \mathbf{h}'$ be the set of roots of $(\mathbf{h}, \mathbf{g})$ and let $\Delta_+ \subseteq \Delta$ be that set of positive roots such that $\Pi \subseteq \Delta_+$. We recall (see THEOREM 8.4 in [4]) that $\dim \mathbf{g} = (h+1)l$ or that $\operatorname{Card} \Delta = hl$ and hence

$$\operatorname{Card} \Delta_+ = gl. \tag{5.1.1}$$

Let $\tau^{(n)}$ for $n \in \mathbf{Z}_+$ be as in (4.4.2). Also let

$$L : W \longrightarrow \mathbf{Z}_+$$

be the length function with respect to Π.

LEMMA 5.2. — *If $h \geq n \geq k \geq 0$ then in the Bruhat ordering of W one has $\tau^{(n)} \geq \tau^{(k)}$.*

Proof. — Clearly $\tau^{(h)} = \sigma^g = \kappa$ by LEMMA 4.9. Thus $L(\tau^{(h)}) = gl$ by (5.1.1). However upon substituting the product (3.5.1) for (τ_j), for $j = 1, 2$, in (4.4.2) it is clear that (4.4.2) for $m = h$ becomes a product of gl elementary reflections (since $\tau_2\tau_1$ involves l such reflections). Thus (4.4.2) becomes a minimal way of writing κ as a product of elementary reflections. It follows therefore that if $s \in W$ is obtained from this product by deleting p left-most such reflections then the remaining product is minimal also for s and $L(s) = gl - p$. The lemma then follows immediately from well-known properties of the Bruhat ordering. ∎

The proof of Lemma 5.2 and (4.4.3) and (4.4.1) clearly implies that if $h \geq n \geq 0$ one has

$$L(\tau^{(n)}) = \begin{cases} lm, & \text{if } n = 2m \text{ is even,} \\ \operatorname{Card} \Pi_1 + lm, & \text{if } n = 2m+1 \text{ is odd.} \end{cases} \tag{5.2.1}$$

Recall that $\psi \in \Delta_+$ is the highest root.

LEMMA 5.3. — *For $n = 1, \ldots, h-1$, one has*

$$z_n = \tau^{(n-1)}\psi - \tau^{(n)}\psi. \tag{5.3.1}$$

Proof. — By definition (see (4.5.1), (4.10.1) and (4.4.5)) one has $z_n = u_n - u_{n-1} = \tau^{(n)}\alpha_0 - \tau^{(n-1)}\alpha_0$. But, by PROPOSITION 2.3, $\tau^{(j)}(\alpha_0 + \psi) = \alpha_0 + \psi$. Thus $\tau^{(j)}(\alpha_0) - \alpha_0 = \psi - \tau^{(j)}\psi$ and hence $\tau^{(n)}(\alpha_0) - \tau^{(n-1)}\alpha_0 = \tau^{(n-1)}\psi - \tau^{(n)}\psi$. ∎

5.4. — It is obvious from the definition of the vectors $v_n \in \widetilde{\mathfrak{h}}'$ that the entries of v_n are non-negative. However this is not obvious for z_n since, in fact, the polynomial $q(t)$ does not have positive coefficients (see LEMMA 5.7). The following result establishes that not only are the coefficients of the z_n non-negative they are, in fact, of a very special type. Also there is symmetry around the middle ($n = g$) and the middle one, z_g, which is different from the others can be completely described isolating a particular node (later seen as the branch point or the middle point, in the case of A_{2m-1}, of the Dynkin diagram) in P.

LEMMA 5.5. — *One has $z_n \neq 0$ and*

$$z_n = z_{h-n} \tag{5.5.1}$$

for $n = 1, \ldots, h-1$. *Furthermore there exists* $i_* \in P_j$, $j = 1, 2$, *with* j *congruent to* g mod 2 *such that*

$$z_g = 2\alpha_{i_*}. \tag{5.5.2}$$

If however $n \neq g$ *then all the coefficients of* z_n *are either* 1 *or* 0. *In fact if* $j \in \{1, 2\}$ *is congruent to* n mod 2 *there exists distinct* $i_1, i_2, \ldots, i_r \in P_j$ *such that*

$$z_n = \alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_r}, \tag{5.5.3}$$

where $r = 1$, 2 *or* 3 *and these three cases occur, respectively, according as* $(\tau^{(n)}\psi, \tau^{(n-1)}\psi)$ *is positive, zero, or negative.*

Proof. — Consider the partial ordering in $\mathbf{h}'$ defined so that $x \geq y$ if $x - y$ is in the $\mathbf{Z}_+$-cone spanned by the positive roots. In case $u \in \mathbf{h}'$ is a dominant element of the weight lattice and s, $t \in W$, where $s \geq t$ in the Bruhat ordering, then one knows that $tu \geq su$ in the partial ordering of $\mathbf{h}'$. Thus $\tau^{(n-1)}\psi \geq \tau^{(n)}\psi$ by LEMMA 5.2 and hence all the coefficients of z_n, by (5.3.1), are in $\mathbf{Z}_+$.

Now clearly $z_1 \neq 0$ by definition (see § 3.5) of the sets P_1 and P_2. Assume $z_n = 0$ where $2 \leq n \leq h-1$. Then $\tau^{(n)}\psi = \tau^{(n-1)}\psi$. Applying τ_{n+1} we clearly have $\tau^{(n+1)}\psi = \tau^{(n-2)}\psi$ (since $\tau_{n+1} = \tau_{n-1}$). But $\tau^{(n-2)}\psi \geq \tau^{(n-1)}\psi \geq \tau^{(n)}\psi \geq \tau^{(n+1)}\psi$. Therefore equalities hold. But $\tau^{(n-1)}\psi = \tau^{(n+1)}\psi$ implies that this non-zero element is fixed by σ. Since 1 is not an eigenvalue of σ we have a contradiction so that $z_n \neq 0$. In particular the $\tau^{(n)}\psi$, for $n = 0, \ldots, h-1$, are distinct and simply ordered.

The argument above would fail for $n = h$. In fact $\tau^{(h)}\psi = \kappa\psi = -\psi$. But $\tau_h = \tau_2$ and $\tau_2\psi = \psi$ by (4.12.6). Thus $\tau^{(h)}\psi = \tau^{(h-1)}\psi = -\psi$. From the latter it is clear there exists $1 \leq k \leq h-1$ such that $\tau^{(k-1)}\psi \in \Delta_+$ but $\tau^{(k)}\psi \in -\Delta_+$. Put $\beta = \tau^{(k-1)}\psi$ and $\gamma = \tau^{(k)}\psi$. One thus has $\tau_j\beta = \gamma$ when $j \in \{1, 2\}$ and j has the same parity as k. But the only positive roots which change sign under τ_j are clearly the elements of Π_j. Thus $\beta \in \Pi_j$ and $\gamma = -\beta$. That is, there exists a node $i_* \in P_j$ such that

$$\tau^{(k-1)}\psi = \alpha_{i_*} \tag{5.5.4}$$

and

$$\tau^{(k)}\psi = -\alpha_{i_*}. \tag{5.5.5}$$

Clearly then

$$z_k = 2\alpha_{i_*}. \tag{5.5.6}$$

Now if $2 \leq k \leq h-2$ then applying τ_{k+1} to both (5.5.4) and (5.5.5) we have that $\tau^{(k-2)}\psi = -\tau^{(k+1)}\psi$. Iterating this way it is clear, since the $\tau^{(n)}\psi$ are distinct for $n = 0, \ldots, h-1$, that (5.5.4) and (5.5.5) can only happen if $k = g$. Also the iteration yields

$$\tau^{(g-j)}\psi = -\tau^{(g+j-1)}\psi \tag{5.5.7}$$

for $j = 1, \ldots, g$. But (5.5.7) clearly implies (5.5.1).

Now since the entries of z_n are non-negative for $n = 1, \ldots, h-1$ it follows for $j \in \{1,2\}$, where j has the same parity as n, that (since $\tau^{(n)}\psi = \tau_j\tau^{(n-1)}\psi$)

$$(\tau^{(n-1)}\psi, \alpha) \geq 0 \tag{5.5.8}$$

for any $\alpha \in \Pi_j$. Note that, even though $\tau^{(n-1)}\psi$ might be negative simple, (5.5.8) implies $\tau^{(n-1)}\psi \notin \Pi_j$. But then if $\tau^{(n-1)}\psi \notin \Pi_j$ one must have

$$\frac{2(\tau^{(n-1)}\psi, \alpha)}{(\alpha,\alpha)} = 0, 1 \tag{5.5.9}$$

for any $\alpha \in \Pi_j$. Since the $\tau^{(j)}\psi$ are simply ordered it follows from (5.5.4) that $\tau^{(n-1)}\psi \notin \Pi_j$ if $n \neq k = g$. Thus in this case the coefficients of z_n are either 0 or 1. That is, if $n \neq g$, there exists distinct $i_1, i_2, \ldots, i_r \in P_j$ such that

$$\tau^{(n-1)}\psi - \alpha_{i_1} - \alpha_{i_2} - \cdots - \alpha_{i_r} = \tau^{(n)}\psi \tag{5.5.10}$$

and one has $K(\tau^{(n-1)}\psi, \alpha_{i_j}) = 1$, where $K = \frac{2}{(\psi,\psi)}$, for $j = 1, \ldots, r$. Taking the inner product of both sides of (5.5.10) with $K\tau^{(n-1)}\psi$ it follows that $K(\tau^{(n-1)}\psi, \tau^{(n)}\psi) = 2 - r$. This proves the lemma since the distinctness of the $\tau^{(j)}\psi$ implies that $2 - r = 1, 0, -1$ or -2. However -2 cannot occur by (5.5.7) since $n \neq g$. ∎

For later use we record in the next proposition some facts established in the proof above. We recall that ψ is the highest root, $\tau^{(n)}$ is defined by (4.4.2), and $h = 2g$ is the Coxeter number which is assumed to be even.

PROPOSITION 5.6. — *For $n = 0, \ldots, h-1$ the roots $\tau^{(n)}\psi$ are distinct and simply ordered with respect to the $\mathbf{Z}_+$-cone spanned by Δ_+ with $\tau^{(0)}\psi = \psi$ highest and*

$$\tau^{(h-1)}\psi = -\psi \tag{5.6.1}$$

lowest. Moreover if $j \in \{1,2\}$ has the same parity as g

$$\tau^{(g-1)}\psi = \alpha_{i_*} \in \Pi_j \tag{5.6.2}$$

where $i_* \in P$ *is the node picked out in* LEMMA 5.5. *Thus* $\tau^{(n)}\psi \in \Delta_+$ *if* $n = 0, \ldots, g-1$. *Finally*

$$\tau^{(g-j)}\psi = -\tau^{(g+j-1)}\psi$$

for $j = 1, \ldots, g$.

We can now pretty much pin down the polynomial $q(t)$. The following result together with LEMMA 4.17 completes the proof of THEOREM 1.3.

LEMMA 5.7. — *There exists even integers* a *and* b *with* $2 \le a \le b \le h$ *such that* $a + b = h + 2$ *and*

$$q(t) = (1 - t^a)(1 - t^b). \tag{5.7.1}$$

Proof. — Now $q(t) = \Sigma_{i=0}^{g+1} q_i t^{2i}$ with $q_0 = q_{g+1} = 1$, recalling § 4.15. Also $c_0 = 1$ and $c_g = -1$. Thus if $g = 1$ then one has $q_0 = q_2 = 1$ and $q_1 = c_g - c_0 = -2$ and hence $q(t) = (1 - t^2)^2$. That is $a = b = 2$. Assume $g > 1$. Then since $\sigma^{g-1} = \sigma^{-1}\kappa$ one has $\sigma^{g-1}\psi = -\sigma^{-1}\psi$ so that, by (4.15.1), (4.13.2) and (4.13.3),

$$q_1 = q_g = \frac{2(\sigma\psi, \psi)}{(\psi, \psi)} - 1.$$

But since $\sigma\psi \ne \psi$ one has $q_1 = q_g \le 0$. But also $q_i \le 0$ for $i = 2, \ldots, g-1$, by PROPOSITION 5.6 since ψ is dominant and for these values

$$q_i = \frac{2(\sigma^i\psi - \sigma^{i-1}\psi, \psi)}{(\psi, \psi)}$$

by (4.13.2) and (4.15.1).

On the other hand $(\sigma^i\psi, \psi) = -(\sigma^i\psi, \sigma^g\psi)$ and hence

$$(\sigma^i\psi, \psi) = -(\sigma^{g-i}\psi, \psi).$$

Thus $(\sigma^i\psi - \sigma^{i-1}\psi, \psi) = (\sigma^{g+1-i}\psi - \sigma^{g-i}\psi, \psi)$ for $i = 2, \ldots, g-1$, so that

$$q_i = q_{g+1-i} \tag{5.7.2}$$

for $i = 1, \ldots, g$. But now, by (4.13.3) and (4.15.1), $\Sigma_{i=1}^{g} q_i = c_g - c_0 = -2$. Thus, since the q_i are non-positive integers, there exists by (5.7.2) a unique positive integer d where $1 \le d \le (g+1)/2$ such that $q_d < 0$. Also $q_d = q_e$ where $e = g + 1 - d$. We can also conclude that $q_d = -1$ if $d < (g+1)/2$ and $q_d = -2$ if $d = (g+1)/2$. That is in any case $q(t) = 1 - t^a - t^b + t^{h+2} = (1 - t^a)(1 - t^b)$ where $a = 2d$ and $b = 2e$. ∎

Let d and e be as in the proof above so that $a = 2d$ and $b = 2e$ and

$$d + e = g + 1. \tag{5.7.3}$$

As an immediate corollary, recalling (4.13.2) and (4.15.1), one obtains the values of $\frac{2(\sigma^n\psi,\psi)}{(\psi,\psi)}$ for $0 \le n \le g$. In the following result one is to ignore those intervals (e.g., if $d - 1 = 0$) which do not make sense.

THEOREM 5.8. — *One has*

$$\frac{2(\sigma^n\psi,\psi)}{(\psi,\psi)} = \begin{cases} 2 & \textit{if } n = 0, \\ 1 & \textit{if } 1 \le n \le d-1, \\ 0 & \textit{if } d \le n \le e-1, \\ -1 & \textit{if } e \le n \le g-1, \\ -2 & \textit{if } n = g. \end{cases} \tag{5.8.1}$$

We now observe

LEMMA 5.9. — *One has for any positive $n \in \mathbf{Z}_+$*

$$(\tau^{(n-1)}\psi, \tau^{(n)}\psi) = (\sigma^n\psi, \psi). \tag{5.9.1}$$

Proof. — Let $\tau^{(-n)}$ denote $(\tau^{(n)})^{-1}$. Clearly $\tau^{(-n)}\tau^{(n-1)} = \tau^{(2n-1)}$. Thus

$$(\tau^{(n-1)}\psi, \tau^{(n)}\psi) = (\tau^{(2n-1)}\psi, \psi). \tag{5.9.2}$$

But $\tau_2\tau^{(2n-1)} = \tau^{(2n)} = \sigma^n$. On the other hand $\tau_2\psi = \psi$ by (4.12.6). Thus one obtains (5.9.1) by applying τ_2 to both terms on the right side of (5.9.2). ∎

We can now determine, in terms of d and e, the integer r in LEMMA 5.5. We recall that r is the number of non-zero entries in z_n where $n \neq g$. Write $r = r(n)$. Again in the following lemma an interval is to be ignored if it makes no sense.

LEMMA 5.10. — *One has*

$$r(n) = \begin{cases} 1 & \textit{if } 1 \le n \le d-1, \\ 2 & \textit{if } d \le n \le e-1, \\ 3 & \textit{if } e \le n \le g-1, \end{cases} \tag{5.10.1}$$

and (by symmetry)

$$r(n) = \begin{cases} 3 & \textit{if } g+1 \le n \le h-e, \\ 2 & \textit{if } h-e+1 \le n \le h-d, \\ 1 & \textit{if } h-d+1 \le n \le h-1. \end{cases} \tag{5.10.2}$$

Proof. — This follows immediately from LEMMA 5.9, THEOREM 5.8 and the final statement of LEMMA 5.5. ∎

Remark. — It should be noted that z_n is a root only if $r(n) = 1$.

Now let $\lambda_i \in \mathbf{h}'$, $i = 1, \ldots, l$, be the highest weights of the fundamental representations of $\mathbf{g}$. That is, the λ_i are defined so that $\frac{2(\lambda_i, \alpha_i)}{(\alpha_j, \alpha_j)} = \delta_{ij}$. Also if $n \in \mathbf{Z}_+$ then as in the proof of LEMMA 5.9 let $\tau^{(-n)} = (\tau^{(n)})^{-1}$.

LEMMA 5.11. — *Let $1 \leq i \leq l$ and let $j \in \{1, 2\}$ be such that $i \in P_j$. Let $n \in \mathbf{Z}_+$. Then, if j and n have opposite parity,*

$$\tau^{(-(n-1))}\lambda_i - \tau^{(-n)}\lambda_i = 0, \tag{5.11.1}$$

whereas if j and n have the same parity

$$\tau^{(-(n-1))}\lambda_i - \tau^{(-n)}\lambda_i = \tau^{(-(n-1))}\alpha_i. \tag{5.11.2}$$

Proof. — By definition $\tau^{(n)} = \tau_n \tau^{(n-1)}$ so that $\tau^{(-n)} = \tau^{(-(n-1))}\tau_n$. Hence the left side of (5.11.1) or (5.11.2) is just $\tau^{(-(n-1))}(\lambda_i - \tau_n \lambda_i)$. But, clearly, if j and n have opposite parity then $\tau_n \lambda_i = \lambda_i$ whereas if they have the same parity $\tau_n \lambda_i = \lambda_i - \alpha_i$. ∎

Let $\nu_i \in \mathbf{h}'$, $i = 1, \ldots, l$, be the basis of $\mathbf{h}'$ which is dual to the simple roots. Clearly

$$\nu_i = \frac{2}{(\alpha_i, \alpha_i)}\lambda_i. \tag{5.11.3}$$

The following lemma will enable us to determine d and e (and hence a and b).

LEMMA 5.12. — *Let $k \in \mathbf{Z}_+$ be such that $0 \leq k \leq (g-1)/2$. Then*

$$\frac{2(\sigma^k \psi, \psi)}{(\psi, \psi)} = (\nu_{i_*}, z_{g-2k}), \tag{5.12.1}$$

where, we recall, $i_* \in P$ is the special node picked out in LEMMA 5.5 *or* PROPOSITION 5.6.

Proof. — If $2k < g - 1$ we can clearly write as an increasing product

$$\tau^{(2k)} = \tau_{2k+1} \cdots \tau_{g-1} \tau^{(g-1)}.$$

However, since $2k + 1$ is odd, we note that $\tau_{2k+1} \cdots \tau_{g-1} = \tau^{(-(g-2k-1))}$. Thus in any case we have

$$\tau^{(2k)} = \tau^{(-(g-2k-1))}\tau^{(g-1)}. \tag{5.12.2}$$

But now $\tau^{(2k)} = \sigma^k$. On the other hand $\tau^{(g-1)}\psi = \alpha_{i_*}$ by (5.6.2). Thus applying both sides of (5.12.2) to ψ we have

$$\sigma^k\psi = \tau^{(-(g-2k-1))}\alpha_{i_*}. \tag{5.12.3}$$

However if $j \in \{1,2\}$ is such that $i_* \in P_j$ then, by PROPOSITION 5.6 j has the same parity as g or $g-2k$. Thus LEMMA 5.11 applies and we can write

$$\sigma^k\psi = \tau^{(-(g-2k-1))}\lambda_{i_*} - \tau^{(-(g-2k))}\lambda_{i_*}.$$

But then taking the inner product with ψ and moving the Weyl group elements to the other side we have

$$(\sigma^k\psi, \psi) = (\lambda_{i_*}, \tau^{(g-2k-1)}\psi - \tau^{(g-2k)}\psi). \tag{5.12.4}$$

But the difference term on the right side of (5.12.4) is just z_{g-2k}. The result then follows from (5.11.3) since ψ and α_{i_*} are W-conjugate. (Of course in the case at hand $\mathbf{g}$ is simply laced and the last argument is unnecessary. However the argument applies more generally to any $\mathbf{g}$ where h is even.) ∎

Remark 5.13. — We note that

$$(\nu_{i_*}, z_{g-j}) = 0 \tag{5.13.1}$$

for any $0 \leq j \leq g-1$ where j is odd. Indeed it is clear from the definition of z_n that

$$< \nu_i, z_n >= 0 \tag{5.13.2}$$

if $i \in P_j$ where j and n have opposite parities. But i_* and g have the same parity proving (5.13.1). Thus (5.12.1) and (5.13.1) determine the coefficients of α_{i_*} for any z_n.

Recall (see (2.7.2)) that $d_i, i = 1, \ldots, l$, are the coefficients of the highest root ψ relative to the simple roots α_i. We can now prove

LEMMA 5.14. — *One has*

$$d = d_{i_*} \tag{5.14.1}$$

where $d = a/2$ and a is given by LEMMA 5.7.

Proof. — If $g = 1$, then $d = a/2 = 1$, as established in the proof of LEMMA 5.7. This proves (5.14.1) in this case since $\mathbf{g} \cong A_1$. Now assume $g > 1$. By definition of the z_n one has

$$\psi - \tau^{(g-1)}\psi = \sum_{n=1}^{g-1} z_n. \tag{5.14.2}$$

But then by (5.6.2) one has

$$\psi - \alpha_{i_*} = \sum_{n=1}^{g-1} z_n. \tag{5.14.3}$$

But then taking the inner product of both sides with ν_{i_*} one has by LEMMA 5.12 and REMARK 5.13

$$d_{i_*} - 1 = \sum_{k=1}^{[(g-1)/2]} \frac{2(\sigma^k\psi, \psi)}{(\psi, \psi)}. \tag{5.14.4}$$

But now recalling the proof of LEMMA 5.7 one has $1 \leq d \leq [(g+1)/2]$ and hence $d - 1 \leq [(g-1)/2]$. On the other hand $e = g + 1 - d$ so that $e - 1 = g - d \geq g - [(g+1)/2] \geq [(g-1)/2]$. But then by (5.8.1) the sum on the right side of (5.14.4) is just $d - 1$. Thus $d_{i_*} = d$. ∎

Now we have only to identify the node i_*. First, however, we observe that the z_n can be generated in a simple way from the simple root α_{i_*}. Let $n \in \mathbf{Z}_+$. Put $\tau^{[n]} = e$ if $n = 0$ and for n positive let $\tau^{[n]} = \tau_{g+n} \cdots \tau_{g+1}$. (One notes of course that $\tau^{[n]} = \tau^{(n)}$ in case g is even.)

THEOREM 5.15. — *One has for* $n = 1, \ldots, g-1$

$$z_{g-n} = z_{g+n} = \tau^{[n]}\alpha_{i_*} - \tau^{[n-1]}\alpha_{i_*}. \tag{5.15.1}$$

Proof. — Note that for $k = 0, \ldots, g-1$

$$\tau^{(k)} = \tau^{[g-k-1]}\tau^{(g-1)}. \tag{5.15.2}$$

Indeed if $k = g - 1$ this is obvious. But for $k < g - 1$ one has $\tau^{(k)} = \tau_{k+1} \cdots \tau_{g-1}\tau^{(g-1)}$. However, clearly, $\tau_{k+1} \cdots \tau_{g-1} = \tau^{[g-k-1]}$ and this establishes (5.15.2). Thus by (5.6.2)

$$\tau^{(k)}\psi = \tau^{[g-k-1]}\alpha_{i_*}. \tag{5.15.3}$$

But $z_{g-n} = \tau^{(g-n-1)}\psi - \tau^{(g-n)}\psi$. The result then follows from (5.15.3) and the symmetry (5.5.1). ∎

We now have

LEMMA 5.16. — *If* $\mathbf{g}$ *is not isomorphic to* A_{2m+1} *(i.e.,* F^* *is not cyclic) then* i_* *is the branch point of the Dynkin diagram of* $\mathbf{g}$. *If* $\mathbf{g} \cong A_{2m+1}$ *then* i_* *is the midpoint of the Dynkin diagram of* $\mathbf{g}$.

Proof. — If $\mathbf{g}$ is not isomorphic to A_{2m-1} then the extended Dynkin diagram is a tree and hence, in the notation of § 2.6, $N(0)$ consists of only one point. Thus $z_1 = \psi - \tau_1\psi$ is a simple root (since again $\mathbf{g} \not\cong A_1$). That is, $r(1) = 1$ in the notation of LEMMA 5.10. But then $d > 1$ by (5.10.1) and since $d + e = g + 1$ this implies $e < g$. But then

$$r(g-1) = 3 \tag{5.16.1}$$

by (5.10.1). However, since $\tau^{(g-2)}\psi = \tau_{g-1}\tau^{(g-1)}\psi$,

$$z_{g-1} = \tau_{g-1}\alpha_{i_*} - \alpha_{i_*} \tag{5.16.2}$$

by (5.6.2). But since $r(g-1) = 3$ it follows that Card $N(i_*) = 3$. Thus i_* is the branch point.

Now assume $\mathbf{g} \cong A_{2m-1}$. We also assume that the nodes are ordered in the natural way given by the diagram. Clearly then

$$\tau^{(k)}\psi = \alpha_{k+1} + \alpha_{k+2} + \cdots + \alpha_{2m-1-k} \tag{5.16.3}$$

for $0 \leq k \leq g - 1 = m - 1$. But then in particular $\tau^{g-1}\psi = \alpha_m$. The result then follows from (5.6.2). ∎

Since $a = 2d$ and $b = h + 2 - a$ we can now write down, using (2.4.1), the table of a and b values for the five types of subgroups $F^* \subseteq SU(2)$.

THEOREM 5.17. — *One has*

F^*	$\mathbf{g}$	a	b	h
$\mathbf{Z}_n^*$	A_{2n-1}	2	$2n$	$2n$
Δ_n^*	D_{n+2}	4	$2n$	$2n+2$
A_4^*	E_6	6	8	12
S_4^*	E_7	8	12	18
A_5^*	E_8	12	20	30

The following result may be observed empirically from the table above. However it is more interesting to derive it from the general theory.

THEOREM 5.18. — *One has*

$$ab = 2\,|F^*|\,. \tag{5.18.1}$$

Proof. — Let $\chi : \widetilde{\mathbf{h}}' \to \mathbf{C}$ be the linear map defined so that $\chi(\alpha_i) = \dim \gamma_i$. Thus, in the notation of (2.7.2), $\chi(\alpha_i) = d_i$ by (2.8.1).

By operating on the coefficients we extend χ so that it maps power series with coefficients in $\widetilde{\mathbf{h}}'$ to ordinary power series with coefficients in $\mathbf{C}$.

Now by LEMMAS 4.17 and 5.7

$$z(t) = (1-t^a)(1-t^b)P_\Gamma(t),$$

where $\Gamma = F^*$. But clearly

$$\chi(P_\Gamma(t)) = \sum_{n=0}^{\infty} \dim S^n(\mathbf{C}^2)t^n = \sum_{n=0}^{\infty}(n+1)t^n = \frac{1}{(1-t)^2}. \tag{5.18.2}$$

Thus

$$\begin{aligned} \chi(z(t)) &= \frac{(1-t^a)}{(1-t)}\frac{(1-t^b)}{(1-t)}, \\ &= \left[\sum_{j=0}^{a-1} t^j\right]\left[\sum_{i=0}^{b-1} t^i\right]. \end{aligned} \tag{5.18.3}$$

Evaluating at $t=1$ one has

$$\left(\chi(z(t))\right)(1) = ab. \tag{5.18.4}$$

On the other hand, by definition of $z(t)$, one has

$$\left(\chi(z(t))\right)(1) = \sum_{n=0}^{h} \chi(z_n).$$

But

$$\sum_{n=0}^{h} z_n = 2(\alpha_0 + \psi) \tag{5.18.5}$$

since $z_0 = z_h = \alpha_0$ (see LEMMA 4.11) and the sum (5.18.5) taken from 1 to $h-1$ equals 2ψ by (5.3.1) and (5.6.1). But clearly

$$\chi(\alpha_0 + \psi) = \sum_{i=0}^{l} {d_i}^2 \tag{5.18.6}$$

by (2.7.2) and (2.8.1). Thus $ab = 2|F^*|$ by (5.1.4). ∎

Now, recalling LEMMAS 5.7 and 5.14, the proof of THEOREM 1.4 is complete. Furthermore, recalling (5.3.1) and LEMMAS 5.5 and 5.10, the proof of THEOREM 1.5 is complete.

6.1. The Poincaré series $P_\Gamma(t)_i$, for the individual representations γ_i. — We now consider the question of determining the Poincaré series $P_\Gamma(t)_i$ for the individual representations $\gamma_i \in \widehat{\Gamma}$ where $\Gamma = F^*$. If $z(t)_i$ is the polynomial obtained from $z(t)$ by considering only the i^{th} component then it follows from (1.3.1) that

$$P_\Gamma(t)_i = \frac{z(t)_i}{(1-t^a)(1-t^b)}. \tag{6.1.1}$$

Thus it suffices only to determine $z(t)_i$. We first observe

LEMMA 6.2. — *The sum of the coefficients of $z(t)_i$ is $2d_i$ where d_i is the coefficient of $\alpha_0 + \psi$ corresponding to the simple root α_i. Furthermore if $i \neq i_*$ then all the non-zero coefficients of $z(t)_i$ are equal to 1. This is also the case for $i = i_*$ except that the coefficient of t^g is 2. Finally, in any case the coefficient of t^{g+k} is equal to the coefficient of t^{g-k} for $k = 0, \ldots, g$ and it vanishes if $k = 0$ when $i \neq i_*$.*

Proof. — The first statement follows from (5.18.5). The next two statements follow from LEMMA 5.5. ∎

More explicitly consider first the case where $i = 0$. Note that $P_\Gamma(t)_0$ is just the Poincaré series for the algebra of invariants $S(\mathbf{C}^2)^\Gamma$. The next result is a restatement of THEOREM 1.8.

THEOREM 6.3. — *One has $z(t)_0 = 1 + t^h$ so that by* THEOREM 1.3

$$P_\Gamma(t)_0 = \frac{1+t^h}{(1-t^a)(1-t^b)}.$$

Proof. — This is an immediate consequence of LEMMA 4.11. ∎

Remark 6.4. — The relation (5.18.1) is now subject to another interpretation. One knows that the subgroup $F \subseteq SO(3)$ may be embedded as a normal subgroup of index 2 in a reflection group $G \subseteq O(3)$. One then has

$$|F^*| = |G|. \tag{6.4.1}$$

Indeed if $F = \mathbf{Z}_n$ then G is the dihedral group operating in the same plane as F but leaving the perpendicular vector fixed. If $F = \Delta_n$ then F operates in a plane but half the elements of F map a perpendicular vector $v \neq 0$ into its negative. The group G is generated by F and the reflection defined by v. The groups A_4, S_4 and A_5 may be regarded, respectively, as the groups of proper rotations of the tetrahedron, cube and icosahedron. The group G is then the corresponding group of improper rotations.

Now from the general theory of reflection groups one knows that the algebra, $S(\mathbf{C}^3)^G$, of G-invariants is generated by 3 algebraically independent homogeneous polynomials. Since G leaves invariant a non-singular symmetric bilinear form, one of these generators, I_2, has degree 2. If δ and ϵ, with $\delta \le \epsilon$, are the degrees of the other two, then the Poincaré series of $S(\mathbf{C}^3)^G$ is clearly

$$Q(t) = \left[\frac{1}{1-t^2}\right]\left[\frac{1}{1-t^\delta}\right]\left[\frac{1}{1-t^\epsilon}\right]$$

and from the general theory of reflection groups

$$|G| = 2\delta\epsilon. \tag{6.4.2}$$

On the other hand if r is the number of reflecting hyperplanes then again from this general theory $t^r Q(t)$ is the Poincaré series for the sign representation of G. Since only the identity and the sign representations are trivial on F it follows that $(1+t^r)Q(t)$ is the Poincaré series of $S(\mathbf{C}^3)^F$. However if $H = \oplus_{n=0}^{\infty} H^n$ is the space of harmonic polynomials on $\mathbf{C}^3$ then as a G-module

$$S(\mathbf{C}^3) = \mathbf{C}[I_2] \otimes H.$$

Thus if $P(t)$ is the Poincaré series of H^F one has

$$P(t) = \frac{1+t^r}{(1-t^\delta)(1-t^\epsilon)}$$

since the Poincaré series of $\mathbf{C}[I_2]$ is $1/(1-t^2)$.

But now, using the notation of § 3.1, $\pi_n|F^*$ has no non-trivial invariants if n is odd since $-1 \in F^*$. On the other hand, π_{2n}, defines a representation $\overline{\pi}_{2n}$ of $SO(3)$. This implies that (1.8.1) is just the Poincaré series defined by the representations $\overline{\pi}_{2n}|F$. But one knows that the representation of $SO(3)$ on H^n is equivalent to $\overline{\pi}_{2n}$. Thus (1.8.1) is equal to $P(t^2)$ or

$$\frac{1+t^h}{(1-t^a)(1-t^b)} = \frac{1+t^{2r}}{(1-t^{2\delta})(1-t^{2\epsilon})}.$$

But then it is easy to see that $r = g = h/2$, $\delta = d = a/2$, and $\epsilon = e = b/2$. Indeed from the general theory of reflection groups one knows that $(2-1)+(\delta-1)+(\epsilon-1) = r$ or $\delta+\epsilon = r+1$. Thus $\delta \le r$ and $\epsilon \le r$. But also $a \le h$ and $b \le h$. By clearing denominators and considering primitive

$2h$ and $4r$ roots of 1 it follows that $h = 2r$ and then, similarly, $\delta = d$ and $\epsilon = e$. We have thus proved from general principles the following empirically observed facts.

THEOREM 6.5. — *One has*

$$g = r \text{ and } \delta = d.$$

That is, the number of reflecting hyperplanes for the reflection group $G \subseteq O(3)$ is equal to one half the Coxeter number of $\mathbf{g}$. *Also excluding a quadratic invariant the lesser degree of the two remaining fundamental symmetric invariants of G is equal to the coefficient of the highest root of* $\mathbf{g}$ *corresponding to the branch point (or mid-point, in the case of $\mathbf{Z}_n$) of the Dynkin diagram of* $\mathbf{g}$.

After the case where $i = 0$ another distinguished case is where $i = i_*$. One notes that γ_{i_*} is an irreducible representation of maximal dimension. For the cases A_4^*, S_4^* and A_5^* it is the unique such representation. The following result is a restatement of THEOREM 1.9.

THEOREM 6.6. — *One has*

$$z(t)_{i_*} = \sum_{i=0}^{d-1} t^{g-2i} + \sum_{i=0}^{d-1} t^{g+2i}. \tag{6.6.1}$$

In particular $z(1)_{i_*} = 2d = a$.

Proof. — This is immediate from (5.12.1) and (5.8.1). ∎

6.7. — The expression (6.6.1) was derived basically by studying that orbit of the Coxeter element σ which contains α_{i_*}. More generally we will see that $z(t)_i$ may be obtained from that orbit of σ which is "associated" with α_i.

Let $\Delta_- = -\Delta_+$ and for any $t \in W$ let

$$\Psi_t = t^{-1}\Delta_- \cap \Delta_+ \tag{6.7.1}$$

so that Ψ_t is the set of positive roots which become negative upon applying t. One knows that

$$\operatorname{Card} \Psi_t = L(t) \tag{6.7.2}$$

where, as in § 5.1, L is the length function on W.

The sets $\Psi_{\tau^{(n)}}$, $n = 1, \ldots, h$, have a particularly nice form. For any $n \in \mathbf{Z}$ let $\Pi_n = \Pi_2$ if n is even and Π_1 if n is odd. If $n \in \mathbf{Z}_+$ recall that $\tau^{(-n)} = (\tau^{(n)})^{-1}$.

PROPOSITION 6.8. — *For $n = 1,\ldots,h$, one has $\tau^{(-(n-1))}\Pi_n \subseteq \Delta_+$ and*

$$\Psi_{\tau^{(n)}} = \bigcup_{j=1}^{n} \tau^{(-(j-1))}\Pi_j \tag{6.8.1}$$

is a disjoint union. In particular

$$\Delta_+ = \bigcup_{n=1}^{h} \tau^{(-(n-1))}\Pi_n \tag{6.8.2}$$

is a disjoint union. Also if $h \geq n \geq m \geq 1$ then

$$\Psi_{\tau^{(m)}} \subseteq \Psi_{\tau^{(n)}}. \tag{6.8.3}$$

Proof. — If $s,t \in W$ where $L(st) = L(s) + L(t)$ then one knows that

$$\Psi_{st} = t^{-1}\Psi_s \cup \Psi_t \tag{6.8.4}$$

is a disjoint union. Indeed upon writing $s^{-1}\Delta_- = \Psi_s \cup (s^{-1}\Delta_- \cap \Delta_-)$ it follows that the left side of (6.8.4) is contained in the right side for any $s,t \in W$. But then (6.8.4) follows from (6.7.2).

Now we may write $\tau^{(n)} = \tau_n\tau^{(n-1)}$. Furthermore it is clear from (5.2.1) that $L(\tau^{(n)}) = L(\tau_n) + L(\tau^{(n-1)})$ when we note that $L(\tau_n) = \mathrm{Card}\,\Pi_n$. But then by (6.8.4)

$$\Psi_{\tau^{(n)}} = \tau^{(-(n-1))}\Psi_{\tau_n} \cup \Psi_{\tau^{(n-1)}} \tag{6.8.5}$$

is a disjoint union. But clearly $\Psi_{\tau_n} = \Pi_n$. The result then follows by induction since Π_e is empty. ∎

6.9. — Now for any $\varphi \in \Delta_+$ let $n(\varphi) \in \mathbf{Z}_+$, where $1 \leq n(\varphi) \leq h$, be defined by the condition that for $n = n(\varphi)$

$$\varphi \in \tau^{(-(n-1))}\Pi_n. \tag{6.9.1}$$

This is well defined by (6.8.2).

Obviously, from (6.9.1), if $n = n(\varphi)$ then $\tau^{(n-1)}\varphi \in \Pi_n$. Let $i(\varphi) \in P$ be defined so that

$$\tau^{(n-1)}\varphi = \alpha_{i(\varphi)} \in \Pi_n. \tag{6.9.2}$$

Remark 6.10. — If $\varphi_1, \varphi_2 \in \Delta_+$ note that $\varphi_1 = \varphi_2$ if and only if $n(\varphi_1) = n(\varphi_2)$ and $i(\varphi_1) = i(\varphi_2)$.

Now one knows (see COROLLARY 8.2 (COLEMAN) in [4]) that each orbit of σ, acting on Δ, has exactly h elements. Consequently, there are exactly l orbits, Δ^i, $i = 1, \ldots, l$, because $\operatorname{Card}\Delta = hl$.

Let $\Delta^i_+ = \Delta^i \cap \Delta_+$.

PROPOSITION 6.10. — *One has* $\operatorname{Card}\Delta^i_+ = g$, $i = 1, \ldots, l$, *and the indexing may be chosen so that*

$$\Delta^i_+ = \{\varphi \in \Delta_+ \mid i(\varphi) = i\}. \tag{6.10.1}$$

Proof. — Let $R^i \subseteq \Delta_+$ be the subset defined by the right side of (6.10.1). If $j \in \{1, 2\}$ is such that $i \in \Pi_j$, then $n(\varphi)$ has the same parity as j for all $\varphi \in R^i$ by (6.9.2). It follows then easily from (6.9.2) that any two elements of R^i lie in the same σ-orbit. On the other hand R^i has exactly g elements by (6.8.2). But, since $\operatorname{Card}\Delta_+ = gl$, to prove the proposition it suffices only to observe that Δ^i_+ is not empty. But this is clear since the sum of the elements in Δ^i is necessarily zero (because 1 is not an eigenvalue of σ). ∎

Remark 6.11. — One notes from the argument above that the correspondence $\varphi \to n(\varphi)$ defines a bijection of Δ^i_+ with the set of all integers from 1 to h which have the same parity as $j \in \{1, 2\}$ where $i \in \Pi_j$.

Now let $\Phi = \{\varphi \in \Delta \mid (\varphi, \psi) > 0\}$ where, we recall, $\psi \in \Delta_+$ is the highest root. Clearly $\psi \in \Phi$. Let $\Phi_o = \Phi - \{\psi\}$.

The following proposition is true, as the proof clearly shows, for any simple Lie algebra, simply laced or not.

PROPOSITION 6.12. — *One has* $\Phi \subseteq \Delta_+$ *and*

$$\frac{2(\varphi, \psi)}{(\psi, \psi)} = 1 \tag{6.12.1}$$

for all $\varphi \in \Phi$. *Furthermore* $\operatorname{Card}\Phi_o$ *is even and in fact there exists a fixed point free involution* $\varphi \to \widehat{\varphi}$ *of* Φ_o *such that*

$$\psi = \varphi + \widehat{\varphi} \tag{6.12.2}$$

for any $\varphi \in \Phi_o$. *Finally if* $\varphi_i \in \Phi$, $i = 1, 2$, *then* $\varphi_1 + \varphi_2$ *is not a root unless* $\varphi_1, \varphi_2 \in \Phi_o$ *and* $\varphi_2 = \widehat{\varphi}_1$.

Proof. — Since ψ is the highest root it is of maximal length (this is redundant in our case but it applies for a general **g**) and hence one has (6.12.1). But also $\Phi \subseteq \Delta_+$ since ψ is dominant. If $\varphi \in \Phi_o$ then $\psi - \varphi \in \Delta$

since $(\varphi,\psi)>0$. But $(\psi,\psi-\varphi)>0$ by (6.12.1) and hence $\psi-\varphi\in\Phi_o$. Put $\psi-\varphi=\widehat{\varphi}$. One has $\varphi\neq\widehat{\varphi}$ since 2φ is not a root. Finally, given $\varphi_1,\varphi_2\in\Phi$, then $(\psi,\varphi_1+\varphi_2)\geq(\psi,\psi)$ by (6.12.1) so that unless $\varphi_1+\varphi_2=\psi$ one has $\varphi_1+\varphi_2\notin\Delta$ again by (6.12.1). ∎

We will refer to Φ as the Heisenberg subsystem of Δ_+.

Remark 6.13. — If, for any $\varphi\in\Delta$, $e_\varphi\in\mathbf{g}$ is a corresponding root vector, it is clear from PROPOSITION 6.12 that the span $\mathbf{n}(\Phi)$ of the e_φ, for $\varphi\in\Phi$, is a Heisenberg Lie algebra having $\mathbf{C}e_\psi$ as its center. One notes that $\mathbf{n}(\Phi)$ is the nilradical of that parabolic subalgebra of $\mathbf{g}$ which, under the adjoint representation, stabilizes $\mathbf{C}e_\psi$.

Now put $\Phi^i=\Phi\cap\Delta^i$ for $i=1,\ldots,l$. We note that $\Phi^i\subseteq\Delta^i_+$ by PROPOSITION 6.12.

The polynomial $z(t)_i$ has already been given for $i=0$ and $i=i_*$. For the remaining values one can prove

LEMMA 6.14. — *For $i=1,\ldots,l$, where $i\neq i_*$, one has*

$$z(t)_i=\sum_{\varphi\in\Phi^i}t^{n(\varphi)}. \tag{6.14.1}$$

Proof. — Let b_n here, for $n=0,\ldots,h$, be the coefficient of t^n in $z(t)_i$. One has $b_0=b_h=0$ by LEMMA 4.11. Assume $n=1,\ldots,h-1$. Then in the notation of (5.11.3) one has $b_n=(z_n,\nu_i)$. Thus

$$\begin{aligned}b_n&=(\tau^{(n-1)}\psi-\tau^{(n)}\psi,\nu_i),\\&=K(\psi,\tau^{-(n-1)}\lambda_i-\tau^{(n)}\lambda_i),\end{aligned}$$

where $K=2/(\alpha_i,\alpha_i)$, by (5.11.3).

But now if $j\in\{1,2\}$ is such that $i\in\Pi_j$ then $b_n=0$ by (5.11.1) if j and n have opposite parities and by (5.11.2)

$$b_n=K(\psi,\tau^{-(n-1)}\alpha_i), \tag{6.14.2}$$

if j and n have the same parity. Assuming the latter

$$b_n=\frac{2(\psi,\varphi)}{(\psi,\psi)}$$

where $\varphi=\tau^{-(n-1)}\alpha_i$ since $\mathbf{g}$ is simply laced. Clearly $\varphi\in\Delta^i_+$ and $n(\varphi)=n$ by (6.9.1) and PROPOSITION 6.10. But then $\varphi\neq\psi$ since $i(\psi)=i_*$ by (5.6.2). Thus $b_n=1$ or 0 according as to whether $\varphi\in\Phi^i$ or not. Recalling REMARK 6.11 this proves (6.14.1). ∎

Remark 6.15. — It follows immediately from (5.18.5) and (6.14.1) that for $i \neq i_*$

$$\text{Card}\,\Phi^i = 2d_i. \tag{6.15.1}$$

The argument in the proof above would apply to $i = i_*$ except when $n = g$. In that case $\varphi = \psi$ and $b_g = 2$. Thus one has

$$\text{Card}\,\Phi^{i_*} = 2d_{i_*} - 1. \tag{6.15.2}$$

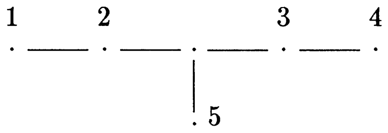
But then since $\Sigma_{i=1}^{l} d_i = h - 1$ by (2.7.2) one has

$$\text{Card}\,\Phi = 2h - 3. \tag{6.15.3}$$

This together with (5.5.1) completes the proof of THEOREM 1.11.

6.16. — We compile a table of the polynomials $z(t)_i$, $i \neq i_*$, for the cases A_4^*, S_4^*, and A_5^*. To do this we have to label the nodes. We have found the computation simplest by using (5.15.1).

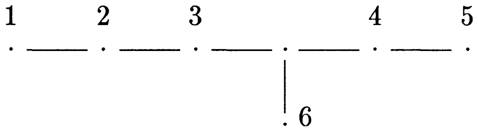
A_4^*



(E_6)

$$\begin{aligned}
z(t)_1 &= t^4 + t^8\\
z(t)_2 &= t^3 + t^5 + t^7 + t^9\\
z(t)_3 &= t^3 + t^5 + t^7 + t^9\\
z(t)_4 &= t^4 + t^8\\
z(t)_5 &= t + t^5 + t^7 + t^{11}
\end{aligned}$$

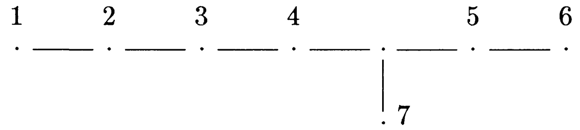
S_4^*



(E_7)

$$
\begin{aligned}
z(t)_1 &= t^6 + t^{12} \\
z(t)_2 &= t^5 + t^7 + t^{11} + t^{13} \\
z(t)_3 &= t^4 + t^6 + t^8 + t^{10} + t^{12} + t^{14} \\
z(t)_4 &= t^2 + t^6 + t^8 + t^{10} + t^{12} + t^{16} \\
z(t)_5 &= t + t^7 + t^{11} + t^{17} \\
z(t)_6 &= t^4 + t^8 + t^{10} + t^{14}
\end{aligned}
$$

A_5^*



(E_8)

$$
\begin{aligned}
z(t)_1 &= t + t^{11} + t^{19} + t^{29} \\
z(t)_2 &= t^2 + t^{10} + t^{12} + t^{18} + t^{20} + t^{28} \\
z(t)_3 &= t^3 + t^9 + t^{11} + t^{13} + t^{17} + t^{19} + t^{21} + t^{27} \\
z(t)_4 &= t^4 + t^8 + t^{10} + t^{12} + t^{14} + t^{16} + t^{18} + t^{20} + t^{22} + t^{26} \\
z(t)_5 &= t^6 + t^8 + t^{12} + t^{14} + t^{16} + t^{18} + t^{22} + t^{24} \\
z(t)_6 &= t^7 + t^{13} + t^{17} + t^{23} \\
z(t)_7 &= t^6 + t^{10} + t^{14} + t^{16} + t^{20} + t^{24}
\end{aligned}
$$

REFERENCES

[1] ARTIN (M.) and VERDIER (J.-L.). — Reflexive modules over rational doublepoints. Preprint..

[2] GONZALEZ-SPRINBERG (G.) and VERDIER (J.-L.). — Construction géométrique de la correspondance de McKay, *Ann. Sci. Ecole Norm. Sup.*, t. **16,** n°3, 1983, p. 410–449.

[3] KAC (V.). — *Infinite Dimensional Lie algebras.* — Boston, Birkhaüser, 1983.

[4] KOSTANT (B.). — The principal three dimensional subgroups and the Betti numbers of a complex Lie group, *Amer. J. Math*, t. **81**, 1959, p. 973–1032.

[5] KNÖRRER (H.). — Group representation and resolutions of rational double points, *Proc. Conf. Finite Groups*, Concordia, edited by J. McKay (to appear).

[6] MCKAY (J.). — Graphs, singularities, and finite groups, *Proc. Symp. Pure math.*, t. **37**, 1980, p. 183–186.

[7] MCKAY (J.). — Cartan matrices, finite groups of quaternions, and Kleinian singularities *Proc. A.M.S.* 1981, p. 153–154.

[8] SLODOWY (P.). — *Simple singularities and simple algebraic groups.* — Berlin and New York, Springer-Verlag, 1981, (*Lecture Notes in Math.*, **815**).

[9] SLODOWY (P.). — *Platonic solids, Kleinian singularities and Lie groups.* — Berlin, Springer-Verlag, 1983, (*Lecture Notes in Math.*, **1008**, p. 102–138).

[10] STEINBERG (R.). — Finite reflection groups, *Trans. Amer. Math. Soc.*, t. **91**, 1959, p. 493–504.

[11] STEINBERG (R.). — Subgroups of $SU(2)$ and Dynkin diagrams, Preprint.

[12] WOLF (J.). — *Spaces of Constant Curvature.* — New York, McGraw-Hill, 1967.

[13] ZASSENHAUS (H.). — *The Theory of Groups.* — New York, Chelsea, 1958.

Bertram KOSTANT,
Department of Mathematics,
Massachusetts Institute of Technology,
Cambridge, Massachusetts 02139, U.S.A.