COADJOINT ACTION OF A SEMI-SIMPLE ALGEBRAIC GROUP AND THE CENTER OF THE ENVELOPING ALGEBRA IN CHARACTERISTIC p

BY

V. KAC AND B. WEISFEILER

(Communicated by Prof. T. A. SPRINGER at the meeting of June 28, 1975)

1. INTRODUCTION

The aim of the present note is to extend to fields of arbitrary non-zero characteristic the theorem on the connection between characters of the center of the universal enveloping algebra of a classical Lie algebra and weights of irreducible representations (Theorem 2). Unlike known precedents we work completely in characteristic p (and do not use reduction modulo p from characteristic zero, compare [2], [4], [10]). Hence for characteristics between 2 and the Coxeter number our results are new, at least for algebras of type different from A_n. At the same time our approach is not constructive.

Three points should be emphasized in the present paper. First, we consider our Lie algebras as Lie algebras of algebraic groups. The action of the corresponding algebraic group gives to the object under study the desired rigidity. Second, our argument, at least at crucial points, is local in the sense that it uses only Lie sub-algebras and algebraic sub-groups of type A_1, normalized by some maximal torus. Third, most assertions below are standard and the only points where a result is obtained by an argument which seems to be not completely standard are Lemmas 4.2, 4.3, 5.2.

Let k be an algebraically closed field of characteristic $p>0$, $\mathscr{G}$ be a connected almost-simple algebraic k-group. For an algebraic group $\mathscr{H}$ we denote by H or by Lie $\mathscr{H}$ the Lie algebra of $\mathscr{H}$, endowed with the p-operation $x \to x^{[p]}$. Let now $\mathscr{B}$ (resp. $\mathscr{N}^+$, $\mathscr{N}^-$, $\mathscr{T}$) be a Borel subgroup of $\mathscr{G}$ (resp. the maximal unipotent subgroup of $\mathscr{B}$, a maximal unipotent subgroup opposite to $\mathscr{B}$, the maximal torus normalizing $\mathscr{B}$ and $\mathscr{N}^-$). We suppose (as we can) that all these groups are defined over $\mathbf{F}_p$. Put $B=\text{Lie } \mathscr{B}$, $N^+=\text{Lie } \mathscr{N}^+$, $N^-=\text{Lie } \mathscr{N}^-$, $T=\text{Lie } \mathscr{T}$. Let W be the Weyl group of $\mathscr{G}$ (with respect to $\mathscr{T}$), and let $X(\mathscr{T})$ be the character group of $\mathscr{T}$.

Attention: we denote throughout by the same letter the characters of $\mathscr{T}$ (in particular roots of $\mathscr{T}$ in $\mathscr{G}$ and G) and their differentials, con-

sidered as linear forms on T. However ϱ denotes the half sum of the positive roots considered as element of $X(\mathscr{T})$ (when it belongs to $X(\mathscr{T})$, cf. 2.4) and also the linear form equal to the half sum of the differentials of all positive roots if $p \neq 2$ or the differential of $\varrho \in X(\mathscr{T})$ if ϱ belongs to $X(\mathscr{T})$. The distinction between the former linear form and the differential of $\varrho \in X(\mathscr{T})$ is void if $\mathscr{G}$ is simply connected.

For a vector space V over k we put $V^* = \mathrm{Hom}_k(V, k)$, $S(V)$ stands for the symmetric algebra of V and $k[V]$ for the ring of polynomials on V. We denote by $U(H)$ the universal enveloping algebra of a Lie algebra H. Then we have $U(G) = U(N^-) \otimes U(N^+) \otimes U(T)$. We identify $U(T)(\simeq S(T))$ with $k[T^*]$. Let Z be the center of $U(G)$. Let further $\beta: U(T) \to U(T)$ be the extension to $U(T)$ of the map $t \to t + \varrho(t)$, $t \in T$ (which is given in $k[T^*]$ by the simpler formula $\beta(\varphi(\lambda)) = \varphi(\lambda + \varrho)$, $\lambda \in T^*$, $\varphi \in k[T^*]$). If $u \in U(G)$ is written in the form $u = \varphi_0 + \sum_{i>0} u_i^- u_i^+ \varphi_i$ with $\varphi_i \in k[T^*](\simeq U(T))$, $u_i^\pm \in U(N^\pm)$ and $u_i^- u_i^+ \neq 0$, we put $\gamma_1(u) = \varphi_0$. It is a map $\gamma_1: U(G) \to U(T)$. Set $\gamma = \beta \circ \gamma_1$. Denote by $A^{\mathscr{H}}$ the ring of $\mathscr{H}$-invariants of a ring A with an automorphism group $\mathscr{H}$. Our main result:

THEOREM 1. *Let either $p \neq 2$ or $\varrho \in X(\mathscr{T})$. Then $\gamma(Z^{\mathscr{G}}) = U(T)^W$ and $\gamma: Z^{\mathscr{G}} \to U(T)^W$ is a ring isomorphism.*

Using now results of [3] (Cor. of Th. 3) one can get conditions under which $Z^{\mathscr{G}}$ is a ring of polynomials (cf. [10] for more results):

COROLLARY. *If p does not divide $n+1$ for A_n, 2 for B_n, C_n, D_n, 6 for E_6, E_7, G_2, F_4, 30 for E_8 then $Z^{\mathscr{G}}$ is a ring of polynomials.*

Denote now by χ_λ the character (the homomorphism of Z into k) of the irreducible representation of G with the highest weight $\lambda \in T^*$. Let W_λ be the stabilizer of the image of λ in the W-module $T^*(k)/T^*(\mathbf{F}_p)$.

THEOREM 2. *Under the assumptions of Theorem 1 one has $\chi_\lambda = \chi_\mu$ iff $\mu = w(\lambda + \varrho) - \varrho$ for some $w \in W_\lambda$.*

For any finite-dimensional $k-\mathscr{G}$-module V we denote by $[V]$ its image in the Grothendieck group of finite-dimensional $k-\mathscr{G}$-modules. Let M_λ denote an irreducible $k-\mathscr{G}$-module with the highest weight $\lambda \in X(\mathscr{T})$, the character group of $\mathscr{T}$. For each $\lambda \in X(\mathscr{T})$, let $\overline{V}_\lambda$ denote the reduction from characteristic 0 of the standard irreducible module with the highest weight λ. The results below follow from [4], Th. 5.1.

THEOREM 3. *Let moreover $\mathscr{G}$ be simply connected. If V is an indecomposable $k-\mathscr{G}$-module and $[V] = \sum_{\lambda \in X(\mathscr{T})} n_\lambda [M_\lambda]$ then $n_\lambda \neq 0$, $n_\mu \neq 0$ implies that $\lambda + \varrho \equiv w(\mu + \varrho) \pmod{p}$ for some $w \in W$. The module $\overline{V}_\lambda$ is indecomposable. In particular, if $\mathrm{Hom}(\overline{V}_\lambda, \overline{V}_\mu) \neq 0$ then $\lambda + \varrho \equiv w(\mu + \varrho) \pmod{p}$ for some $w \in W$.*

Here ϱ is considered as an element of $X(\mathscr{T})$. For $\mathscr{G}$ of type A_n Theorem 3 is proved in ([2], Th. 3.8).

Let now $U_{\mathbf{Z}}$ denote the universal $\mathbf{Z}$-algebra, described for example in [9] and let $V_{\mathbf{Z}}$ be a $U_{\mathbf{Z}}$-module which is irreducible as $U_{\mathbf{Z}} \otimes \mathbf{Q}$ module. Let $V'_{\mathbf{Z}}$ be a $U_{\mathbf{Z}}$-submodule in $V_{\mathbf{Z}}$ and $p_1, p_2, \ldots, p_m$ be the prime divisors of the torsion of $V_{\mathbf{Z}}/V'_{\mathbf{Z}}$. The next result follows immediately from Theorem 3.

COROLLARY. *Let λ, μ be the highest weights of $U_{\mathbf{Z}}$ on $V_{\mathbf{Z}}/V'_{\mathbf{Z}}$. Then there exists a sequence of weights of $V_{\mathbf{Z}}$ $\lambda = \mu_1, \ldots, \mu_s = \mu$ and a sequence of primes $p_{i_1}, \ldots, p_{i_s} \in \{p_1, \ldots, p_m\}$ such that $\mu_j + \varrho \equiv w_j(\mu_{j+1} + \varrho) \pmod{p_{i_j}}$ for some $w_j \in W$.*

Our uttermost thanks are due to T. A. Springer who read the manuscript and made a number of corrections and ameliorations.

We are thankful also to J. E. Humphreys who read a preliminary version of the note and asked us to give a complete proof of Theorem 4i in Section 3. It led us to more results on the $\mathscr{G}$-module G^*, which we included here since we thought that they have an independent interest and might be used in future research. In particular those results have enabled us to drop the assumption of non-degeneracy of the Killing form in [11], Th. 2, cf. Theorem 5 in 3.13.

2. On normal and pathological behaviour

Three questions are discussed in this Section. First the structure of three-dimensional simple subalgebras, normalized by a maximal torus (cf. 2.1). Second, the description of the kernel of W on $T = \mathrm{Lie}\, \mathscr{T}$ (cf. 2.3). Third, the conditions under which ϱ belongs to T^* (cf. 2.4).

Let Σ be the root system of $\mathscr{G}$ with respect to $\mathscr{T}$. Let $x_\alpha(t)$, $\alpha \in \Sigma$, be a parametrization of the root subgroup (isomorphic to G_a) of $\mathscr{G}$ corresponding to α. We assume that the parameters t agree with one another in the standard manner. For $\alpha \in \Sigma$ we denote by $\mathscr{G}_\alpha$ the algebraic subgroup of $\mathscr{G}$, generated by $x_\alpha(t)$ and $x_{-\alpha}(t)$, $t \in k$. Then G_α stands for Lie $\mathscr{G}_\alpha$.

2.1. PROPOSITION. i) *If $\mathscr{G}$ is not isomorphic to $SO(2n+1)$, $n \geqslant 1$*

$$PGL(2) \simeq SO(3),\ PSp(4) \simeq SO(5),$$

then $\mathscr{G}_\alpha \simeq SL(2)$ for all $\alpha \in \Sigma$. If $\mathscr{G} \simeq SO(2n+1)$, $n \geqslant 1$, then $\mathscr{G}_\alpha \simeq SL(2)$ if α is a long root and $\mathscr{G}_\alpha \simeq PGL(2)$ if α is a short root.

ii) *If $p \neq 2$ or $\mathscr{G}$ is not isomorphic to $SO(2n+1)$, then $G_\alpha \simeq$ Lie $SL(2)$.*

PROOF. Let $\tilde{\mathscr{G}}$ be the universal covering of $\mathscr{G}$. Then the groups $\tilde{\mathscr{G}}_\alpha$ are simply connected (cf. [7], II, 5.4), i.e. $\tilde{\mathscr{G}}_\alpha \simeq SL(2)$. Let $\tilde{C}$ be the center of $\tilde{\mathscr{G}}$. If $\tilde{C} \cap \tilde{\mathscr{G}}_\alpha = 1$, then the image $\mathscr{G}_\alpha$ of $\tilde{\mathscr{G}}_\alpha$ in $\mathscr{G}$ is isomorphic to $\tilde{\mathscr{G}}_\alpha \simeq SL(2)$. If $\tilde{C} \cap \tilde{\mathscr{G}}_\alpha \neq 1$, then $2 | \langle \beta, \alpha \rangle$, $V\beta \in \Sigma$, i.e. $2(\beta, \alpha)/(\alpha, \alpha) \in 2\mathbf{Z}$, $V\beta \in \Sigma$ (cf. [9], p. 43). The last condition holds only when α is a short root of a root system Σ of type B_n, i.e. i) is proved.

To prove ii) it is sufficient to note that Lie $PGL(2) \simeq$ Lie $SL(2)$ if $p \neq 2$ and apply i).

REMARK. In the proof above the center $\tilde{C}$, the intersection $\tilde{C} \cap \tilde{\mathcal{G}}_\alpha$ and all isomorphisms are taken of course in the scheme-theoretic sense.

2.2. Let us consider now W as acting on T and let $Z_W(T)$ be the set of elements of W which act trivially. Let w_α stand for the reflection in $\alpha \in \Sigma$.

LEMMA. $T^* \simeq X(\mathcal{T}) \otimes k$ *(as W-modules).*

PROOF. Evidently $X(\mathcal{T}) \otimes k$ has the same dimension as T^*. The isomorphism is given by the differential (which turns each character of $\mathcal{T}$ into a linear form on T).

2.3. PROPOSITION. i) *If $p \neq 2$ then $Z_W(T) = 1$.*

ii) *If $p = 2$ and $\mathcal{G} \simeq Sp(2n)$ $(n \geqslant 1)$, $SO(n)$ $(n \geqslant 5)$, then $Z_W(T)$ is the abelian normal subgroup of W consisting of "sign changes".*

iii) *If $p = 2$ and $\mathcal{G}$ is not isomorphic to any one of the groups from* ii), *then $Z_W(T) = \{\pm 1\} \cap W$.*

This Proposition is not used in the sequel except for illustrations (cf. Sections 8, 9). So we only indicate how the proof can be conducted. First of all if $w \in W$ is of prime order q, then there exists in Σ a w-invariant subsystem $\tilde{\Sigma}$ of type A_{q-1} on which w acts naturally. Using this fact it can be easily checked that $w \in Z_W(T)$ only if $p = 2$ and $q = 2$. For $A_n (n \geqslant 2,\ n \neq 3)$ and $E_n (n = 6,\ 7,\ 8)$ the assertion is derived from the simplicity of a big subgroup of W. Using the result for A_n and plates from [1] one can check the validity of our assertion in the remaining cases.

2.4. Let us denote now by $\mathbb{Z}\Sigma$ the lattice of roots and by Π the lattice of weights of Σ. Let $\varrho \in \Pi$ be the half-sum of the positive roots and let $\tilde{\Pi}$ denote the lattice, generated by ϱ and $\mathbb{Z}\Sigma$ in Π.

PROPOSITION. i) $\tilde{\Pi} = \mathbb{Z}\Sigma$ *if Σ is of type A_{2m}, C_{4m}, C_{4m+3}, D_{4m}, D_{4m+1}, G_2, F_4, E_6, E_8.*

ii) $\tilde{\Pi} = \Pi$ *if Σ is of type B_m, C_{4d+1}, $C_{4d+2} (d > 0)$, E_7.*

iii) $[\tilde{\Pi} : \mathbb{Z}\Sigma] = 2$, $\tilde{\Pi} \neq \Pi$ *if Σ is of type $A_{2m-1} (m \geqslant 2)$, D_{4m+2}, $D_{4m+3} (m \geqslant 1)$.*

iv) $\varrho \in T^*$ *if either $p \neq 2$ or $\tilde{\Pi} \subset X(\mathcal{T})$.*

PROOF. Remark that $[\tilde{\Pi} : \mathbb{Z}\Sigma] = 1$ or 2 since $2\varrho \in \mathbb{Z}\Sigma$. Then use plates from [1] giving the structure of $\Pi/\mathbb{Z}\Sigma$ and the expression of ϱ in terms of roots. So one obtains i)–iii). To obtain iv) remark that for $p = 2$ iv) follows from 2.2. If $p \neq 2$ then $2\varrho \in \mathbb{Z}\Sigma \otimes k$ and since 2 is invertible in k our result is immediate.

3. Action of $\mathcal{G}$ on G^*

We assume in this section that either $p \neq 2$ or $\mathcal{G}$ is not isomorphic to $SO(2n+1)$, $n \geqslant 1$. The aim of the section is to establish elementary properties of the $\mathcal{G}$-module G^*.

It should be pointed out from the beginning that the properties of the $\mathcal{G}$-module G^* are close to those of the Lie algebra of the adjoint group. Hence our results resemble the results of [7], II. 3.17′, III. 1.10, etc. Some additional complications are caused by the absence of a Lie algebra structure.

Let us denote by Σ the root system of $\mathcal{G}$ with respect to $\mathcal{T}$, by Σ^+, Σ^-, Δ the system of positive, negative and simple roots corresponding to the choice of Borel subgroup $\mathcal{B}$.

We choose a system of Chevalley generators $\{e_\alpha, h_\alpha\}$, $\alpha \in \Sigma$, for G_α. It follows from our assumptions on $\mathcal{G}$ that $[e_\alpha, e_{-\alpha}] = h_\alpha$, $\forall \alpha > 0$ and $\alpha(h_\alpha) = 2$. We consider T^*, B^*, N^* as imbedded into G^*. Namely $T^* = \{l \in G^* : l(N^+ \oplus N^-) = 0\}$, $B^* = \{l \in G^* : l(N^+) = 0\}$, $N^* = \{l \in G^* : l(B^*) = 0\}$.

For a reductive subgroup $\mathcal{H}$ of $\mathcal{G}$, which contains a maximal torus of $\mathcal{G}$ denote by H^* the subspace of G^* consisting of $l \in G^*$ such that $l(e_\alpha) = 0$ if $x_\alpha(t) \notin \mathcal{H}$. (This definition, given after T. A. Springer, doesn't depend on the choice of a maximal torus since all such tori are conjugate). These embeddings are isomorphisms of the corresponding $N_{\mathcal{G}}(\mathcal{T})$-, $\mathcal{B}$-, $\mathcal{B}$- and $\mathcal{H}$-modules respectively. We say that $l \in G^*$ is semi-simple (resp. nilpotent) if $\mathcal{G} \cdot l \cap T^* \neq \emptyset$ (resp. $\mathcal{G} \cdot l \cap N^* \neq \emptyset$). For an $l \in G^*$ a decomposition $l = l_s + l_n$ is called a *Jordan decomposition* if there exists a $g \in \mathcal{G}$ such that $g \cdot l_s \in T^*$, $g \cdot l_n \in N^*$ and $[g \cdot l_s(h_\alpha) \neq 0$ implies $g \cdot l_n(e_{\pm\alpha}) = 0]$. The group $N_{\mathcal{G}}(\mathcal{T})$ acts on T^*. We denote by $Z_{\mathcal{G}}(T^*)$ the pointwise stabilizer of T^* (and T) and by $\overline{W}$ the factor-group $N_{\mathcal{G}}(\mathcal{T})/Z_{\mathcal{G}}(T) \simeq W/Z_W(T)$. We set $\Omega = \{l \in T^* \subset G^* : l(h_\alpha) \neq 0, \forall \alpha \in \Sigma\}$ (regular semi-simple elements) and $\Omega_1 = \{l \in \Omega : \bar{w}l \neq l, \forall \bar{w} \in \overline{W}\}$ (strongly regular elements, compare [8]). Clearly $Z_W(l) = Z_W(T)$, $\forall l \in \Omega_1$.

Finally, we set $P = \operatorname{Spec} k[G^*]^{\mathcal{G}}$, and let $\varphi : G^* \to P$ be the map induced by the inclusion $k[G^*]^{\mathcal{G}} \to k[G^*]$.

Theorem 4. *Suppose that $\mathcal{G}$ is almost simple and that either $p \neq 2$ or $\mathcal{G}$ is not isomorphic to $SO(2n+1)$, $n \geqslant 1$. Then*

i) *The natural map $k[G^*]^{\mathcal{G}} \to k[T^*]^W$ induced by the imbedding $T^* \to G^*$ is an isomorphism of algebras.*

ii) *Closed orbits are precisely orbits of semi-simple elements.*

iii) *An element $l \in G^*$ is nilpotent iff $P(l) = 0$ $\forall P \in k[G^*]^{\mathcal{G}}$, N^* is the set of nilpotent elements of B^*.*

iv) *Every $l \in G^*$ admits a unique Jordan decomposition.*

v) *(T. A. Springer) For $l \in G^*$ a decomposition $l = l_s + l_n$ is a Jordan decomposition if and only if l_s is semi-simple, l_n is nilpotent and $l_n \in Z_G(l_s)^*$.*

vi) *The complement of $\mathcal{G} \cdot \Omega$ in G^* is a divisor. If $\mathcal{G}$ is simply connected, irreducible components of that divisor correspond to lengths of roots of Σ*

(that is, it is irreducible for Σ of type A_n, D_n, E_n and has two irreducible components for Σ of type B_n, C_n, F_4, G_2).

vii) *The support of the fibers of the map $\varphi: G^* \to P$ is irreducible.*

The proof of the Theorem 4 is given in steps.

3.1. LEMMA. *Let $l \in T^*$.*

i) *$Z_G(l)$ and $Z_{\mathscr{G}}(l)$ are $\mathscr{T}$-stable. In particular, there exists a closed subsystem $\Sigma_1 \subseteq \Sigma$ such that $Z_G(l)$ is spanned by T and e_α, $\alpha \in \Sigma_1$.*

ii) *$\alpha \in \Sigma_1$ if and only if $l(h_\alpha) = 0$.*

iii) *$Z_G(l)$ is reductive.*

iv) *$Z_G(l) = Lie\, Z_{\mathscr{G}}(l)$.*

v) *If $gl_1 = l_2$ for $l_1, l_2 \in \Omega$ and $g \in \mathscr{G}$ then $g \in N_{\mathscr{G}}(\mathscr{T})$.*

PROOF. The first assertion of i) is evident, and the second follows from the first. If $l(h_\alpha) \neq 0$,then $e_\alpha \cdot l(e_{-\alpha}) \neq 0$ whence $e_\alpha \notin Z_G(l)$. If $l(h_\alpha) = 0$; then we have $e_\alpha \cdot l(h) = l(\lambda e_\alpha) = 0$ for all $h \in T$, $e_\alpha \cdot l(e_\beta) = l(N_{\alpha,\beta} e_{\alpha+\beta}) = 0$ for $\beta \neq -\alpha$, $e_\alpha \cdot l(e_{-\alpha}) = l(h_\alpha) = 0$ by the assumption. So $e_\alpha \cdot l = 0$ in this case which proves ii). iii) follows from ii) since by ii) $\alpha \in \Sigma_1$ iff $-\alpha \in \Sigma_1$. The same argument as in the proof of ii) establishes that $x_\alpha(t) \in Z_{\mathscr{G}}(l)$ iff $l(h_\alpha) = 0$, whence iv). To prove v) note that by ii) and iv) $Z_{\mathscr{G}}(l_1)^\circ = Z_{\mathscr{G}}(l_2)^\circ = \mathscr{T}$ which implies that $g \in N_{\mathscr{G}}(\mathscr{T})$.

3.2. LEMMA. *$\mathscr{G} \cdot \Omega$ contains an open subset of G^*.*

PROOF. By 3.1. ii), T is the kernel of the differential of $\pi: \mathscr{G} \times \Omega \to \to G^*(\pi(g \cdot l) = g \cdot l)$ at $l \in \Omega$. Since $\mathscr{T}$ is the stabilizer of l, we are done.

3.3. LEMMA. *For any $l \in G^*$ one has $\mathscr{G} \cdot l \cap B^* \neq \emptyset$.*

PROOF. Consider the subset D of $G^* \times \mathscr{G}/\mathscr{B}$ of pairs $(l', \mathscr{B}')$ such that $\mathscr{B}'$ is a Borel subgroup and l' ([Lie $\mathscr{B}'$, Lie $\mathscr{B}'$]) $= 0$. D is evidently closed. Since $\mathscr{G}/\mathscr{B}$ is complete, the image of D in G^* is closed and by 3.2 it is open. So $D = G^*$ and our assertion follows from the conjugacy of Borel subgroups.

3.4. LEMMA. *If $l = l_1 + l_2$, $l_1 \in T^*$, $l_2 \in N^*$, then l_1 belongs to the closure of the orbit $\mathscr{T} \cdot l$. In particular the closure of any orbit of $\mathscr{G}$ in G^* intersects T^* and closed orbits consist of semi-simple elements.*

PROOF. The mappings $\mathscr{T} \to \mathscr{T} \cdot l \subsetneq G^*$ define a $\mathscr{T}$-invariant mapping $\pi: k[G^*] \to k[\mathscr{T}] = k[x_i, x_i^{-1}, i = 1, 2, \ldots, r]$. It may be assumed that the x_i^{-1}'s afford negative characters of $\mathscr{T}$ (in the ordering defined by $\mathscr{B}$). Since the characters of $\mathscr{T}$ on N^* are also negative we have $\pi(k[G^*]) \subseteq \subseteq k[x_i^{-1}, i = 1, 2, \ldots, r]$.

This means that $\mathscr{T} \to \mathscr{T} \cdot l \subsetneq G^*$ can be extended to a morphism $\tilde{\pi}: \mathbb{A}_k^r = \operatorname{Spec} k[x_i^{-1}, i = 1, \ldots, r] \to G^*$. The point $\tilde{\pi}(0)$ is stable under $\mathscr{T}$ whence $\tilde{\pi}(0) \in T^*$. Since $\mathscr{T} \cdot l_1 = l_1$ we have $\tilde{\pi}(0) = l_1$, as asserted by the first part of Lemma. The second part follows immediately from 3.3.

3.5. PROOF OF i). By Rosenlicht's theorem [6] there exists an open $\mathscr{G}$-stable subset $V \subset G^*$ such that a geometric quotient $V/\mathscr{G}$ exists. By 3.2 V can be chosen so that $M = V \cap T^* \subseteq \Omega$. The quotient $V \cap T^*/N_{\mathscr{G}}(\mathscr{T})$ exists automatically since it is a quotient for the action of the finite group $\overline{W}$. By 3.4 and 3.1 the embedding $M \subsetneq V$ induces isomorphism $k[V]^{\mathscr{G}} \to k[M]^W$. Hence we get an isomorphism $k(G^*)^{\mathscr{G}} \to k(T^*)^W$ of fields of rational functions.

Therefore $k[G^*]^{\mathscr{G}} \to k[T^*]^W$ is injective. The last step is now the same as the last step of the proof of Th. II. 3.17′ from [7].

3.6. PROOF OF ii). By 3.4 it is sufficient to prove that any orbit $\mathscr{G} \cdot l$, $l \in T^*$, is closed. Suppose that it is not closed. Then $\mathscr{G} \cdot l$ contains a closed orbit $\mathscr{G} \cdot l_1$, and by 3.4 we can take $l_1 \in T^*$. Then l and l_1 cannot be distinguished by polynomials from $k[G^*]^{\mathscr{G}}$ and by i) by polynomials from $k[T^*]^W$. This is a contradiction since orbits of the finite group $\overline{W}$ on T^* can be distinguished by invariant polynomials, by Serre's theorem.

3.7. PROOF OF iii). If l is nilpotent one can assume that $l \in N^*$. But then $0 \in$ Closure of $\mathscr{T} \cdot l$. Hence $R(l) = 0$, $\forall R \in k[G^*]^{\mathscr{G}}$. If $l \in G^*$ and $R(l) = 0$, $\forall R \in k[G^*]^{\mathscr{G}}$, one can assume that $l \in B^*$, $l = l_1 + l_2$, $l_1 \in T^*$, $l_2 \in N^*$. Then $l_1 \in$ Closure of $\mathscr{T} \cdot l$. Hence $R(l_1) = 0$, $\forall R \in k[T^*]^W$ whence by Serre's theorem $l_1 = 0$, that is $l \in N^*$ as asserted.

3.8. PROOF OF iv). By 3.3 one can assume that $l \in B^*$. Let

$$\Pi = \{\alpha \in \Sigma^+ : l(h_\alpha) \neq 0\}.$$

Let $\beta_1, \ldots, \beta_m$ be an ordering of all roots from Π such that $i > j$ implies that the height of β_i with respect to Δ is greater than the height of β_j. We shall conjugate T by $x_\beta(t)$, $\beta \in \Pi$, so that the value of l on the new $e_{-\beta}$ will be zero. Suppose that for $i = 1, 2, \ldots, m$, we achieved the equality $l(e_{-\beta_i}) = 0$, $\forall i \leqslant m$, $l(e_\gamma) = 0$, $\forall \gamma > 0$. Set $g(t) = x_{\beta_{m+1}}(t)$. Then

$$g(t) e_\gamma = e_\gamma + \sum_{s>0} \lambda_s(t)\, e_{\gamma + s\beta_{m+1}}$$

for $\gamma \neq -\beta_{m+1}$ and $g(t) e_{-\beta_{m+1}} = e_{-\beta_{m+1}} + t h_{\beta_{m+1}} - t^2 e_{\beta_{m+1}}$. Since $\beta_{m+1} > 0$ we have $g(t) \cdot l \in B^*$. We have further $(g(t) \cdot l)(e_{-\beta_i}) = 0$, $i = 1, 2, \ldots, m$ since the height of $-\beta_i + s\beta_{m+1}$ is not negative for $s \geqslant 1$ so that $(g(t) \cdot l)(e_{-\beta_i}) = l(e_{-\beta_i})$ and by the inductive assumptions $l(e_{-\beta_i}) = 0$. Finally $(g(t) \cdot l)(e_{-\beta_{m+1}}) = tl(h_{\beta_{m+1}}) + l(e_{-\beta_{m+1}})$ and since $l(h_{\beta_{m+1}}) \neq 0$ the parameter t can be chosen so that $(g(t_1) l)(e_{-\beta_{m+1}}) = 0$. This completes the induction step and establishes the existence of a Jordan decomposition.

Unicity is proved in three steps.

i) If $l \in B^*$, $b \in \mathscr{B}$, $l = l_s + l_n$ is a Jordan decomposition for l, then $b \cdot l = l$ implies $b \cdot l_s = l_s$.

PROOF. We can assume that $l_s \in T^*$. Let $m = |\{\alpha \in \Sigma^+ : l(h_\alpha) \neq 0\}|$. Consider the map $\mathscr{B} \to \mathbb{H}^m$ which puts into correspondence to $b \in \mathscr{B}$ the

e_α^*-coordinates, $h(\alpha)\neq 0$, of $b\cdot l$. We have a) $Z_{\mathscr{G}}(l_s)$ is the fiber of this map over $0\in \mathbb{H}^m$. b) This map is surjective (it follows from the proof of existence of Jordan decomposition since it is proved there that for any m-tuple of values $\{a_\alpha\}$ a form l with $l(e_\alpha)=a_\alpha$, $l(h_\alpha)\neq 0$, can be brought into a form with $l(e_\alpha)=0$ if $l(h_\alpha)\neq 0$). c) It is separable (since $Z_B(l_s)=$ $=\mathrm{Lie}\, Z_{\mathscr{G}}(l_s)$). Hence the induced map $\mathscr{B}/Z_{\mathscr{G}}(l_s)\to \mathbb{H}^m$ is an isomorphism, whence our assertion.

ii) If $l=l_s+l_n$ is any Jordan decomposition then $Z_{\mathscr{G}}(l)^\circ\subseteq Z_{\mathscr{G}}(l_s)^\circ$.

Proof. Let $\mathscr{H}$ be a solvable connected subgroup of $Z_{\mathscr{G}}(l)$. Since the set of Borel subgroups $\mathscr{B}$ such that $l([\mathrm{Lie}\,\mathscr{B},\mathrm{Lie}\,\mathscr{B}])=0$ is closed in $\mathscr{G}/\mathscr{B}$ and, consequently, complete, $\mathscr{H}$ has a fixed point in this set. Hence $\mathscr{H}$ normalizes some $\mathscr{B}=\mathscr{B}(\mathscr{H},l)$ such that $l([\mathrm{Lie}\,\mathscr{B},\mathrm{Lie}\,\mathscr{B}])=0$. In particular, $\mathscr{H}\subseteq\mathscr{B}(\mathscr{H},l)$. Since $l=h\cdot l=h\cdot l_s+h\cdot l_n$ is a Jordan decomposition for l, we have by i), where we put $\mathscr{B}=\mathscr{B}(\mathscr{H},l)$, that $h\cdot l_s=l_s$. Since $Z_{\mathscr{G}}(l)^\circ$ is generated by the connected solvable subgroups which it contains, we have our assertion.

iii) End of the proof of unicity. It follows from 3.1 iii) that $C(Z_{\mathscr{G}}(l_s)^\circ)\subseteq C(Z_{\mathscr{G}}(l)^\circ)$. Hence the groups $C(Z_{\mathscr{G}}(l_s')^\circ)$ generate, when l_s' ranges over the semi-simple parts of l, a connected commutative subgroup of $C(Z_{\mathscr{G}}(l)^\circ)$. By 3.1 iii) this group, say $\mathscr{T}(l)$, is of multiplicative type. Now l is contained in $Z_G(\mathscr{T}(l))^*$ and all l_s' belong to $Z_G(\mathscr{T}(l))^*$ and are stable under $[Z_{\mathscr{G}}(\mathscr{T}(l)),Z_{\mathscr{G}}(\mathscr{T}(l))]$. Since all nilpotent parts are spanned by e_α^*, where α is a root of $Z_{\mathscr{G}}(\mathscr{T}(l))$, we should have from $l_s+l_n=l_s'+l_n'$ that $l_s=l_s'$.

3.9. The proof of v) follows immediately from the definition of Jordan decomposition and from 3.1 ii), iv).

3.10. Proof of vii). Take $l=l_1+l_2$, $l_1\in T^*$, $l_2\in N^*$. By 3.4 the irreducible set l_1+N^* is contained in the same fiber of φ as l. By 3.3, i) and the fact that $\overline{W}$-invariant polynomials on T^* distinguish points of T^*, we have that the set of points of the fiber of l is the orbit of l_1+N^* under $\mathscr{G}$. Since $\mathscr{G}\times(l_1+N^*)$ is irreducible we get our assertion.

3.11. Proof of vi). Consider $R=\prod_{\alpha\in\Sigma^+}h_\alpha$ as a polynomial on T^*. Then $T^*-\Omega=\{l\in T^*\colon R(l)=0\}$. By i) R can be extended to a $\mathscr{G}$-invariant polynomial $\tilde{R}\in k[G^*]$. Set $\tilde{\Omega}=\{x\in G^*\colon \tilde{R}(x)\neq 0\}$. We shall prove that $\tilde{\Omega}=\mathscr{G}\cdot\Omega$. Certainly $\mathscr{G}\cdot\Omega\subseteq\tilde{\Omega}$. Let us prove that $\tilde{\Omega}\subseteq\mathscr{G}\cdot\Omega$. Take $x\in\tilde{\Omega}$ and let $x=x_s+x_n$ be its Jordan decomposition. It can be assumed that $x_s\in T^*$, $x_n\in N^*$. Since $\tilde{R}(x)=\tilde{R}(x_s)$ (by 3.4) we have $\tilde{R}(x_s)=R(x_s)\neq 0$. Hence $x_s\in\Omega$. By the definition of a Jordan splitting we have $x_n=0$, whence $x\in\Omega$. This proves the first part of vi). To prove the second part it is sufficient to note that in the case under consideration the set of zeros of R is the set of walls of a Weyl chamber. They correspond to roots, and roots of equal length are permuted transitively by W.

3.11.1. REMARK. It follows from Theorem 4 vi) that a rational function having no singularities on the set of all semi-simple elements is regular.

3.12. Let us give now the statement of Th. 2 from [11], adjusted to all characteristics. So take $l \in G^*$ and let $l = l_s + l_n$ be its Jordan splitting. Let us suppose (by Theorem 4 this is not a restriction), that $l_s(h_\alpha) \neq 0$ implies $l_n(e_\alpha) = l_n(e_{-\alpha}) = 0$. Put $\Sigma' = \{\alpha \in \Sigma : l(h_\alpha) = 0\}$, $\Sigma_0 = \Sigma \cap \mathbf{Q}\Sigma'$. Set $P = T + \sum_{\alpha > 0} ke_\alpha + \sum_{\alpha \in \Sigma_0} ke_\alpha$. Then P is a parabolic subalgebra in G.

Let $U_l(G)$ be the quotient of $U(G)$ by the ideal generated by $g^p - g^{[p]} - l^p(g)$, $g \in G$.

THEOREM 5. *Let V be a simple $U_l(G)$-module, V' be a simple P-submodule of V. Then $V = U_l(G) \otimes_{U_l(P)} V'$. In particular,*

$$\dim V = p^{\dim N} \cdot \dim V',$$

V' is the unique simple p-submodule of V and the dimension of any simple $U_l(G)$-module is divisible by $p^{(|\Sigma| - |\Sigma_0|)/2}$.

The proof is the same as in [11] since it uses only the properties a) [$l_s(h_\alpha) \neq 0$ implies $l_n(e_\alpha) = l_n(e_{-\alpha}) = 0$] and b) $G_\alpha \simeq \text{Lie } SL(2)$.

4. LEMMAS ON THE STRUCTURE OF Z

Let $\mathcal{G}$ be a connected almost simple group. Assume here that either $\varrho \in X(\mathcal{T})$ or $p \neq 2$. (The case $p = 2$, $\mathcal{G} \simeq SO(2n+1)$ is excluded since $\varrho \notin X(\mathcal{T})$ in this case, cf. 2.4).

Let Z be the center of $U(G)$, Z_0 be the subalgebra of Z, generated by $g^p - g^{[p]}$, $g \in G$. Then by [12] both Z and Z_0 are finitely generated, integrally closed and $\mathcal{G}$-stable. The map $g \to g^p - g^{[p]}$, $g \in G$, commutes with the action of $\mathcal{G}$.

Let us denote for a schema X over k by X^p the same schema twisted by the Frobenius morphism (the structure sheaf is exponentiated to the p-th power). Let us denote by $\bar{A}$ the quotient field of an integral domain A.

4.1. LEMMA. $Z_0 \simeq k[G^{*p}]$.

PROOF. (An explicit isomorphism is given in [11], Prop. 1.1). Set $\bar{e}_\alpha = (Adx_{-\alpha}(1))e_\alpha = e_\alpha - h_\alpha - e_{-\alpha}$. Then e_α, $\alpha \in \Sigma$, $\bar{e}_\alpha$, $\alpha \in \Delta$, form a base of G. We have $e_\alpha^{[p]} = \bar{e}_\alpha^{[p]} = 0$, $\forall \alpha \in \Sigma$. By [12], $Z_0 = k[x_1^p - x_1^{[p]}, \ldots, x_n^p - x_n^{[p]}]$, where $\{x_i\}$ is a base of G. So in our case $Z_0 = k[e_\alpha^p, \alpha \in \Sigma, \bar{e}_\alpha^p, \alpha \in \Delta]$. Hence $Z_0 = S(G^p) \simeq k[G^{*p}]$ as asserted.

4.2. LEMMA. *$\bar{Z}$ is separable over $\bar{Z}_0$ and $[\bar{Z} : \bar{Z}_0] = p^r$.*

PROOF. Since $\dim T = r$ the equation $\lambda^p - \lambda = l^p$ with $\lambda \in T^*$ admits p^r solutions. (Namely the set of solutions is $\lambda_0 + T^*(\mathbf{F}_p)$, where λ_0 is one solution).

For each such λ denote by V_λ the representation of G with the highest weight λ induced (in the sense of [11], cf. also 3.12) from the one-dimensional representation of B given by $(h+n)(v)=\lambda(h)v$, $\forall h \in T$, $\forall n \in N^+$. By ([11], Th. 2) (cf. also Th. 5 in 3.12) v is the only eigenvector (up to scalar multiple) for B in V_λ if $l \in \Omega$. Hence for $l \in \Omega$ all V_λ, $\lambda^p-\lambda=l^p$, are irreducible and $V_\lambda \not\simeq V_\mu$ if $\lambda \neq \mu$, $\lambda^p-\lambda=\mu^p-\mu=l^p$. Since they are irreducible we have: $\dim V_\lambda = p^{\dim G - \dim B} = p^{(n-r)/2}$. Since they are not equivalent and since $\mathcal{G}\cdot\Omega$ is open (cf. 3.1) we have that the separable degree of $\bar{Z}$ over $\bar{Z}_0$ is $\geqslant p^r$ (cf. [11], [12]). Now by [11] we should have $(\dim V_\lambda)^2 \cdot [\bar{Z}:\bar{Z}_0] \leqslant p^{\dim G}$ whence our assertion.

REMARK. In the case of a simply connected group $\mathcal{G}$ we can avoid the use of the complicated Theorem 5. Namely, by existence of the Steinberg representation (of dimension $p^{\dim G - \dim B}$) we conclude that the dimension of representations in general position is $\geqslant p^{\dim G - \dim B}$. On the other hand the same argument as above shows that the separable degree of $\bar{Z}$ over $\bar{Z}_0$ is $\geqslant p^r$, whence our assertion.

4.3. We study here the action of W on points of Spec Z over $\Omega^p \subseteq$ Spec Z_0. As in 4.2 we consider those points as representations V_λ with the highest weight $\lambda \in T^*$, $\lambda^p-\lambda \in \Omega^p$. (Recall that the V_λ are induced from one-dimensional representations.) The action of $\mathcal{G}$ on representations is given by $F^g(x)=F(gxg^{-1})$, where $F: G \to \mathrm{Hom}\,(V, V)$ is some representation. In our case $\mathcal{T}$ enters into the stabilizers of all points of Ω^p whence the action of $N_{\mathcal{G}}(\mathcal{T})$ factors to an action of W. We shall write $V_{\underset{\sim}{w}\lambda}$ for the image of V_λ under $w \in W$. (The proof below shows the sense of this notation.) For $w \in W$ set $\Sigma(w)=\{\alpha \in \Sigma^+ : w^{-1}\alpha \in \Sigma^-\}$ and

$$s(w)=\sum_{\alpha \in \Sigma(w)} \alpha.$$

LEMMA.

a) $\underset{\sim}{w}\cdot\lambda = w\cdot\lambda - s(w)$

b) $s(w)=\varrho - w\cdot\varrho$

c) *if* $w \in Z_W(T)$ *then* $\underset{\sim}{w}\cdot\lambda=\lambda$, $\forall \lambda \in T^*$.

PROOF. We shall write $V_{\lambda, B}$ to emphasize the dependence of V_λ on B. Then $w \in W$ moves $V_{\lambda, B}$ into $V_{w\lambda, B^w}$. Indeed, if v is a highest vector for B in $V_{\lambda, B}$, then $(t+n)v=\lambda(t)v$ for $t \in T$, $n \in N^+$. Hence $(w(t+n)w^{-1})v = \lambda(t)\cdot v$ in $V_{w\lambda, B^w}$ whence our assertion.

The space $V_{w\lambda, B^w}$ has a unique (up to collinearity) eigenvector for B (since $e_\alpha^p=0$, $\forall \alpha$ in our case). So $V_{w\lambda, B^w} \simeq V_{\lambda(w), B}$ for some $\lambda(w) \in T^*$. Let v be a non-zero eigenvector for B^w in $V_{w\lambda, B^w}$. It is evident (and easy to check) that $(\prod_{\alpha \in \Sigma(w)} e_\alpha^{p-1})v$ is a non-zero eigenvector for B in $V_{w\lambda, B^w}$. Then we have $t(\prod_{\alpha \in \Sigma(w)} e_\alpha^{p-1} v) = (w\cdot\lambda - \sum_{\alpha \in \Sigma(w)} \alpha)\ (t)\ (\prod_{\alpha \in \Sigma(w)} e_\alpha^{p-1} v)$, whence $\underset{\sim}{w}\cdot\lambda = \lambda(w) = w\cdot\lambda - s(w)$, i.e. a) is proved. b) is easily proved by the induction beginning with $s(w_\alpha)=\alpha=\varrho - w_\alpha\cdot\varrho$. c) follows immediately from a) and b).

4.4. LEMMA. $[\bar{Z}^{\mathcal{G}}: \bar{Z}_0^{\mathcal{G}}] = p^r$.

PROOF. The imbedding $Z_0 \subsetneq Z$ induces a finite $\mathcal{G}$-morphism

$$\varphi: \operatorname{Spec} Z \to \operatorname{Spec} Z_0.$$

By 4.2 it is separable of degree p^r. Since (cf. 4.3 c) the stabilizer of $l \in \Omega_1$, acts trivially in the fiber over l and since $\mathcal{G} \cdot \Omega_1$ is open in G^*, the morphism of the orbit spaces (in Rosenlicht's sense [6]) is also separable and of the same degree as φ.

4.5. LEMMA. *The algebras* $Z^{\mathcal{G}}$, $Z_0^{\mathcal{G}}$, $U(T)^W$, $(U(T) \cap Z_0)^W$ *are integrally closed.*

PROOF. We shall prove the general assertion: let A be an integrally closed ring and $\mathcal{H}$ a group of automorphisms. Then $A^{\mathcal{H}}$ is integrally closed.

Take d from the integral closure of $A^{\mathcal{H}}$. Then $d \in \overline{A^{\mathcal{H}}}$. Since A is integrally closed, we have $d \in A$. Therefore $d \in A \cap \overline{A^{\mathcal{H}}} = A$. q.e.d.

4.6. LEMMA. i) $\bar{Z}_0^{\mathcal{G}} = \overline{Z_0^{\mathcal{G}}}$.
ii) $\bar{Z}^{\mathcal{G}} = \overline{Z^{\mathcal{G}}}$.

PROOF. Since $Z_0 = k[G^{*p}]$, part i) follows from the evident fact:

Let V be a vector space (in our case $V = G^*$) and f a rational function on V invariant under a connected linear group having only trivial characters. Then f is a quotient of two invariant polynomials.

Let us prove ii). Let A be the integral closure of $Z_0^{\mathcal{G}}$ in $\bar{Z}^{\mathcal{G}}$. Since Z is integrally closed we have $A \subseteq Z$. Hence $A \subseteq Z \cap \bar{Z}^{\mathcal{G}} = Z^{\mathcal{G}}$, i.e., $A \subseteq Z^{\mathcal{G}}$ Therefore $\bar{A} \subseteq \overline{Z^{\mathcal{G}}}$. On the other hand $\bar{A} = \bar{Z}^{\mathcal{G}}$ (since the quotient field of the integral closure in a finite extension ($\bar{Z}^{\mathcal{G}} / \bar{Z}_0^{\mathcal{G}}$ in our case) is that extension). Adding to the last two relations the evident one $\overline{Z^{\mathcal{G}}} \subseteq \bar{Z}^{\mathcal{G}}$ we get

$$\bar{A} \subseteq \overline{Z^{\mathcal{G}}} \subseteq \bar{Z}^{\mathcal{G}} = \bar{A}$$

whence our assertion.

4.7. LEMMA. Z_0 *and* $Z^{\mathcal{G}}$ *generate* Z.

PROOF. Let Z_1 be the subalgebra of Z generated by Z_0 and $Z^{\mathcal{G}}$. The inclusions $Z_0 \subsetneq Z_1 \subsetneq Z$ induce finite separable morphisms

$$\operatorname{Spec} Z \xrightarrow{\varphi_1} \operatorname{Spec} Z_1 \xrightarrow{\varphi_2} \operatorname{Spec} Z_0.$$

Take $x \in \varphi_2^{-1}(\mathcal{G} \cdot \Omega_1) \subseteq \operatorname{Spec} Z_1$. Let $\{x_1, \ldots, x_m\} = \varphi_1^{-1}(x)$, $y = \varphi_2(x)$. By Theorem 4 i) and Rosenlicht's theorem regular invariants distinguish orbits in general position on Spec Z. Now $Z^{\mathcal{G}} \subseteq Z_1$, $x_1, \ldots, x_m$, are contained in one orbit. Hence $\mathcal{G}_x$ (the stabilizer of x) permutes them transitively. Evidently $\mathcal{G}_x \subseteq \mathcal{G}_y$. Since by 4.3. c) $\mathcal{G}_y$ acts trivially on the fiber over y of $\varphi_2 \circ \varphi_1$, the same is true for $\mathcal{G}_x$. Hence $m = 1$ as asserted.

5. Lemmas on γ

We assume here that either $\varrho \in X(\mathscr{T})$ or $p \neq 2$.

5.1. Lemma. *$\gamma: U(G)^{\mathscr{T}} \to U(T)$ is a homomorphism of algebras.*

Proof. It is sufficient to prove that γ_1 is a homomorphism since evidently β is one. Let $z_1 z_2 \in U(G)$ and $t z_i t^{-1} = z_i$, $\forall t \in \mathscr{T}$. Then

$$z_i = \varphi_i(\lambda) + \sum_{\substack{\alpha<0 \\ m>0}} e_\alpha^m P_{i,\alpha,m},\ P_{i,\alpha,m} \in U(G).$$

(The sum is taken over $m>0$, since z_i has zero weight with respect to $\mathscr{T}$ and therefore if it contains some e_β, $\beta>0$, it should be compensated by some e_γ, $\gamma<0$). We have

$$z_1 \cdot z_2 = \varphi_1(\lambda)\,\varphi_2(\lambda) + \varphi_1(\lambda) \sum e_\alpha^m P_{2,\alpha,m} + \sum e_\alpha^m P_{1,\alpha,m}\,\varphi_2(\lambda) + \sum e_\alpha^m P_{1,\alpha,m}\, e_\beta^q P_{2,\beta,q}.$$

Obviously

$$\gamma_1(\varphi_1(\lambda) \sum_{m>0} e_\alpha^m P_{2,\alpha,m}) = \gamma_1(\sum_{m>0} e_\alpha^m \tilde{P}_{2,\alpha,m}) = 0,\ \tilde{P}_{2,\alpha,m} = \psi_m(\lambda)\, P_{2,\alpha,m}$$

and also

$$\gamma_1(\sum_{m>0} e_\alpha^m P_{1,\alpha,m}\,\varphi_2(\lambda)) = 0.$$

Let us consider $\gamma_1(e_\alpha^m P_{1,\alpha,m} e_\beta^q P_{2,\varrho,q})$ where $\alpha<0$, $\beta<0$, $m>0$. To compute it we should bring it into the form $\sum u_j^- u_j^+ \varphi_j(\lambda)$. Obviously we shall have then a sum of expressions of the form $e_\alpha^d \overline{P}_{\alpha,d}$, where $d \geqslant k > 0$. Hence $\gamma_1(e_\alpha^m P_{1,\alpha,m} e_\beta^q P_{2,\beta,q}) = 0$. Therefore $\gamma_1(z_1 z_2) = \varphi_1(\lambda) \cdot \varphi_2(\lambda) = \gamma_1(z_1) \cdot \gamma_1(z_2)$.

5.2. Lemma. *For $n_w \in N_{\mathscr{G}}(\mathscr{T})$, a representative of $w \in W$, we have $\gamma(n_w z n_w^{-1}) = w(\gamma(z))\, w^{-1}$ for all $z \in Z$. In particular, $\gamma(Z^{N_{\mathscr{G}}(\mathscr{T})}) \subseteq U(T)^W$.*

Proof. Let $z = \varphi_0(\lambda) + \sum u_i^- u_i^+ \varphi_i(\lambda) \in Z$, $u_i^- u_i^+ \neq 0$. Then z acts as a scalar multiple of the identity operator upon V_λ, $\lambda^p - \lambda \in \Omega^p$ (since V_λ is irreducible). We denote the image of z by $\chi_\lambda(z) \cdot id$. If v is a highest weight vector for V_λ, then we evidently have $z \cdot v = \varphi_0(\lambda) v +$ (terms, containing only $\prod_{\Sigma n_\alpha > 0,\, \alpha \in \Sigma^-} e_\alpha^{n_\alpha} v$). So we have $\chi_\lambda(z) = \varphi_0(\lambda) = \gamma(z)$. Our assertion follows now from Lemma 4.3 a), b). Namely by this Lemma and remark above, $n_w z n_w^{-1} = \varphi_0(\underline{w} \cdot \lambda) + \sum \tilde{u}_i^- \tilde{u}_i^+ \tilde{\varphi}_i(\lambda)$, $\tilde{u}_i^- \tilde{u}_i^+ \neq 0$, and $\underline{w} \cdot \lambda = w(\lambda + \varrho) - \varrho$.

5.3. Lemma. *$\gamma: Z^{\mathscr{G}} \subsetneq U(T)^W$ is a monomorphism of algebras.*

Proof. By 5.2, $\gamma(Z^{\mathscr{G}}) \subseteq U(T)^W$ and by 5.1, γ is a homomorphism. It remains to prove that $\gamma(z) = 0$, $z \in Z^{\mathscr{G}}$, implies $z = 0$. By Theorem 4 i), $k[G^*]^{\mathscr{G}} \to k[T^*]^W$ is a monomorphism. Since $Z_0 \simeq k[G^{*p}]$ (cf. 4.1) and since γ coincides with γ_1 (that is, with the restriction homomorphism) on Z_0, we get that γ is a monomorphism on $Z_0^{\mathscr{G}}$. Take now $z \in Z^{\mathscr{G}}$, $z \neq 0$, and set $m = p^r$. Since $[\overline{Z}^{\mathscr{G}} : \overline{Z}_0^{\mathscr{G}}] = m$, z satisfies an equation $a_0 z^m + \ldots + a_m = 0$,

$a_m \neq 0$, $a_i \in Z_0^{\mathcal{G}}$. Applying γ to that equation we get by 5.1 the equation $\sum \gamma(a_i)\gamma(z)^i = 0$. Since $\gamma(a_m) \neq 0$ (as shown above), we have $\gamma(z) \neq 0$ as asserted.

5.4. LEMMA. $\gamma(Z^{\mathcal{G}}) = U(T)^W$.

PROOF. By Zassenhaus' theorem [12], $U(T)$ is integral over $U(T) \cap Z_0$. Hence (cf. 4.5) $U(T)^W$ is integral over $(U(T) \cap Z_0)^W$. By Theorem 4 i) and since γ coincides with the restriction homomorphism on Z_0 we have $(U(T) \cap Z_0)^W = \gamma(Z_0^{\mathcal{G}})$. Hence $U(T)^W$ is integral over $\gamma(Z_0^{\mathcal{G}})$. Since $Z^{\mathcal{G}}$ is integral over $Z_0^{\mathcal{G}}$, $U(T)^W$ is integral over $\gamma(Z^{\mathcal{G}})$. Evidently

$$[\overline{U(T)^W} : \overline{(U(T) \cap Z_0)^W}] < p^r.$$

From 4.4, 4.6 and 5.3 we get $\overline{U(T)^W} = \overline{\gamma(Z^{\mathcal{G}})}$. Since both $U(T)^W$ and $\gamma(Z^{\mathcal{G}})$ are integrally closed we get $U(T)^W = \gamma(Z^{\mathcal{G}})$ as desired.

6. PROOF OF THEOREMS 1, 2 AND COROLLARY TO THEOREM 1

6.1. Theorem 1 is contained in 5.1, 5.4.

6.2. PROOF OF COROLLARY TO THEOREM 1. Under the assumptions of that corollary the W-module T is irreducible and therefore it is isomorphic to the reduction modulo p of the W-module of weights of Σ. By [3] (Cor. of Th. 3) the symmetric algebra over the latter module is an algebra of polynomials. These two statements together give our Corollary.

6.3. PROOF OF THEOREM 2. If $\mu = w(\lambda + \varrho) - \varrho$, $w \in W_\lambda$, then χ_λ and χ_μ coincide on $Z^{\mathcal{G}}$ and on Z_0. Therefore the equality $\chi_\lambda = \chi_\mu$ follows from 4.7.

Suppose that $\chi_\lambda = \chi_\mu$. By Theorem 1 and since regular invariants distinguish orbits of finite group on an affine variety, we get $\mu = w(\lambda + \varrho) - \varrho$ $w \in W$. Let us extend λ and μ from T to $U(T)$. Since $\varrho(T(\mathbf{F}_p)) \subseteq \mathbf{F}_p$ and $w \cdot \varrho(T(\mathbf{F}_p)) \subseteq \mathbf{F}_p$, the equality $w \cdot \lambda = \mu$ holds on $U(T) \cap Z_0$. Restricting $\chi_\lambda = \chi_\mu$ to Z_0 we see $\lambda = \mu = w(\lambda)$ on $U(T) \cap Z_0$, which implies that $w \in W_\lambda$.

7. REMARK ON THE EXTENSION $\bar{Z}^{\mathcal{G}} / \bar{Z}_0^{\mathcal{G}}$

Suppose that $\mathcal{G}$ is connected, almost simple and simply connected. We shall show that the extension $\bar{Z}^{\mathcal{G}}$ of $\bar{Z}_0^{\mathcal{G}}$ is not Galois if either $p \neq 2$ or $\mathcal{G} \not\simeq SL(2)$.

Indeed the extension $\overline{U(T)} / \overline{U(T) \cap Z_0}$ is normal and

$$\Gamma = \mathrm{Gal}\,(\overline{U(T)} / \overline{U(T) \cap Z_0}) \simeq T^*(\mathbf{F}_p)$$

and consists of mappings $h \in T \to h + l(h)$, $l \in T^*(\mathbf{F}_p)$. (It should be recalled that $U(T) \cap Z_0$ is generated by $h^p - h$, $h \in T(\mathbf{F}_p)$). The Weyl group W acts on $\Gamma = T^*(\mathbf{F}_p)$. Therefore $\Gamma \times W$ is an "extended Weyl group". We

have $\Gamma \times W = \mathrm{Gal}\,(\overline{U(T)}/(\overline{U(T) \cap Z_0})^W)$. Since W is not a normal subgroup of $\Gamma \times W$, both extensions $\overline{U(T)}^W/(\overline{U(T) \cap Z_0})^W = \bar{Z}^{\mathcal{G}}/\bar{Z}_0^{\mathcal{G}}$ are not normal.

However, in the case $p=2$, $\mathcal{G}=SL(2)$ the group acts trivially upon Γ whence the extension is normal. But this was clear from the outset since $[\bar{Z}^{\mathcal{G}}: \bar{Z}_0^{\mathcal{G}}]=2$ and $\bar{Z}^{\mathcal{G}}/\bar{Z}_0^{\mathcal{G}}$ is separable in this case.

8. Removing the assumption $\varrho \in T^*$

We discuss below what happens in the case of algebras Lie $\mathcal{G}$ excluded in the preceding sections. In this Section we assume $p \neq 2$ or $\mathcal{G}$ is not isomorphic to $SO(2n+1)$.

8.1. Theorems 1 and 2 have no sense if $\varrho \notin T^*$. However, their statements could be corrected so that they would make sense. Namely, let us take γ_1 in place of γ and define the action of W on $U(T) \simeq k[T^*]$ by the formula $\underset{\sim}{w} \cdot \lambda = w \cdot \lambda - s(w)$. Then a corrected version of Theorem 1 is

Theorem 1 bis. *If $p \neq 2$ or $\mathcal{G}$ is not isomorphic to $SO(2n+1)$, then $\gamma_1(Z^{\mathcal{G}}) = U(T)^W$ and $\gamma_1 : Z^{\mathcal{G}} \to U(T)^W$ is an isomorphism.*

The proof is the same as that of Theorem 1. However, Lemmas 4.4, 4.7 do not hold in general. To get the result it is sufficient yet to note that $[\bar{Z}^{\mathcal{G}}: \bar{Z}_0^{\mathcal{G}}] = [\overline{U(T)}^W : (\overline{U(T) \cap Z_0})^W]$ by Lemmas 4.3, 5.2. So 5.4 goes through.

8.2. If $\varrho \in X(\mathcal{T})$ and $Z_W(T) \neq 1$, the action of $Z_W(T)$ given by $\lambda \to w \cdot \lambda - s(w)$ induces a nontrivial action of $Z_W(T)$ on the fibers of $\mathrm{Spec}\, Z \to \mathrm{Spec}\, Z_0$. By 2.3, 2.4 the group $PSp(8d+2)$, $d \geqslant 1$, can be taken as example. We have $Z_W(T) = \{\pm 1\}$, $\underset{\sim}{w} \cdot \lambda = \lambda - 2\varrho$. By [1], plate III, $2\varrho = (4d+1)(2d+1)\alpha_n \notin 2X(\mathcal{T})$, whence $2\varrho \neq 0$. Hence $\lambda \to \lambda - \alpha_n$ is a nontrivial action of $Z_W(T)$ in the fiber over $\lambda^p - \lambda \in \Omega_1^p$. So $[\bar{Z}^{\mathcal{G}}: \bar{Z}_0^{\mathcal{G}}] = 2^{r-1}$. The corrected version of Theorem 2 is

Theorem 2 bis. *Assume that $p \neq 2$ or $\mathcal{G} \not\simeq SO(2n+1)$.*

a) *If $\chi_\lambda = \chi_\mu$ then $\mu = w \cdot \lambda - s(w)$, $w \in W_\lambda$.*
b) *If $w \in W_\lambda$, $\mu = w \cdot \lambda - s(w)$, then either $\chi_\lambda = \chi_\mu$ or $\chi_{\lambda - 2\varrho} = \chi_\mu$.*
c) *If either $Z_W(T) = 1$ or $\varrho \in X(T)$ the case $\chi_{\lambda-2\varrho} = \chi_\mu$ in* b) *cannot occur.*

9. The case $p=2$, $\mathcal{G} \simeq SO(2n+1)$

9.1. For $SO(2n+1)$ the whole picture gets distorted already in Section 3. Namely 3.2 does not hold, that is, semi-simple elements do not form an open set and Sections 4 and 5 could not be even approached. And for good reason since it can be easily seen that $q = \sum_{\alpha \text{ short}} e_{-\alpha} e_\alpha$ (Casimir element) belongs to Z. The extension $Z_0(q)$ of Z_0 is clearly purely inseparable (since $q^2 \in Z_0$).

To prove that $q \in Z$ let us remark that q commutes with all e_β, β short, and q is invariant under $N_{\mathcal{G}}(\mathcal{T})$. Since $N_{\mathcal{G}}(\mathcal{T})$ acts transitively on long roots it is sufficient to check that $[e_\beta, q]=0$ for some long $\beta \in \Sigma$. So we can assume $\mathcal{G}=PSp(4)$, $\beta=\alpha_2$, $q=e_{-\alpha_1}e_{\alpha_1}+e_{-\alpha_1-\alpha_2}e_{\alpha_1+\alpha_2}$. We have $[e_{\alpha_2}, e_{\alpha_1+\alpha_2}]=0$. Hence $[e_{\alpha_2}, q]=e_{-\alpha_1}e_{\alpha_1+\alpha_2}+e_{-\alpha_1}e_{\alpha_1+\alpha_2}=0$, as asserted.

It is easy to check that also $q \in Z^{\mathcal{G}}$.

9.2. The proof of Theorem 2 from [11] does not go through for G since there is an induction based on Lie $SL(2)$.

For Lie $PGL(2)$ irreducible representations with a linear form l such that $l(e_\alpha)=l(e_{-\alpha})=0$ have dimension one ($\{e_\alpha, e_{-\alpha}\}$ is an ideal and goes into zero). So in 4.2 we would have dim $V_\lambda = p^{-r+\dim N}$ which, together with the non-openness of $\mathcal{G}\cdot\Omega$, is an obstruction to our proof.

9.3. The next interesting point is that $U(T)^W=(U(T)\cap Z_0)^W$. To show this let us remark first that $Z_W(T)=\langle w_\alpha, \alpha \text{ short}\rangle$ (cf. [1], table II). Since $X(\mathcal{T})=\mathbb{Z}\Sigma$ and $\mathbb{Z}\Sigma=\sum_{\alpha \text{ short}}\mathbb{Z}\alpha$ in our case it follows that $Z_W(T)$ acts transitively on the fiber over $l \in \Omega_1^p$ of the (separable) map: Spec $U(T) \to$ Spec $(U(T)\cap Z_0)$. So the degree of

$$\text{Spec } U(T)^W \to \text{Spec } (U(T)\cap Z_0)$$

is one as asserted.

9.4. To sum up the deviations of $SO(2n+1)$ for $p=2$ (about which we know) we have

a) The G_α, α short, are Lie $PGL(2)$.
b) $\mathcal{G}\cdot\Omega$ is not open in G^*.
c) Z is not separable over Z_0.
d) $\gamma_1: Z^{\mathcal{G}} \to U(T)$ has a non-trivial kernel.
e) $U(T)^W \subseteq U(T)\cap Z_0$.

Institute for Advanced Study,
Princeton, N.J. 08540, U.S.A.

REFERENCES

1. Bourbaki, N., Groupes et algèbres de Lie, ch. IV–VI, Hermann, Paris, 1968.
2. Carter, R. W. and G. Lusztig, On the modular representations of the general linear and symmetric groups, Math. Z. **136**, 193–242 (1974).
3. Demazure, M., Invariants symétriques entiers des groupes de Weyl et torsion, Invent. Math. **21**, 287–301 (1973).
4. Humphreys, J. E., Modular representations of classical Lie algebras and semi-simple groups, J. algebra, **19**, 51–79 (1971).
5. Jantzen, J. C., Zur Charakterformel gewisser Darstellungen halfeinfacher Gruppen und Lie-algebren, Math. Zeits. **140**, 127–150 (1974).

6. ROSENLICHT, M., A note on orbit spaces, Anais. Acad. brasil cienc. **35**, 487–489 (1963).
7. SPRINGER, T. A. and R. STEINBERG, Conjugacy classes, in Seminar on alg. groups and related finite groups, Lecture Notes in Math., vol. **131**, Springer Verlag, Berlin 1971.
8. STEINBERG, R., Regular elements of semi-simple algebraic groups, Publ. Math. IHES, **25**, 49–80 (1965).
9. ————, Lectures on Chevalley groups, Yale Univ., 1967.
10. VELDKAMP, F. D., The center of the universal enveloping algebra of a Lie algebra in characteristic p, Ann. Scient. Ec. Norm. Sup, 4-é série, **5**, 217–240 (1972).
11. WEISFEILER, B. YU. and V. G. KAC, On irreducible representations of Lie p-algebras (in Russian), Funct. analysis and its appl. **5**, No. 2, 28–36 (1971).
12. ZASSENHAUS, H., The representations of Lie algebras of prime characteristic, Proc. Glasgow Math. Ass. **21**, 1–36 (1954).