ERIC M. FRIEDLANDER
BRIAN J. PARSHALL

Rational actions associated to the adjoint representation

Annales scientifiques de l'É.N.S. 4e série, tome 20, nº 2 (1987), p. 215-226
<http://www.numdam.org/item?id=ASENS_1987_4_20_2_215_0>

Ann. scient. Éc. Norm. Sup.,
4^e^ série, t. 20, 1987, p. 215 à 226.

RATIONAL ACTIONS ASSOCIATED TO THE ADJOINT REPRESENTATION

BY ERIC M. FRIEDLANDER (1), (2) AND BRIAN J. PARSHALL (1)

In this paper we investigate the G-module structure of the universal enveloping algebra $U(\mathscr{G})$ of the Lie algebra $\mathscr{G}$ of a simple algebraic group G, by relating its structure to that of the symmetric algebra $S(\mathscr{G})$ on $\mathscr{G}$. We provide a similar analysis for the hyperalgebra hy(G) of G in positive characteristic. In each of these cases, the algebras involved are regarded as rational G-algebras by extending the adjoint action of G on $\mathscr{G}$ in the natural way.

We prove the existence of a G-equivariant isomorphism of coalgebras $U(\mathscr{G}) \to S(\mathscr{G})$ in Section 1. (Our proof requires some restriction on the characteristic p of the base field k.) This theorem, inspired by the very suggestive paper of Mil'ner [12], can be viewed as a G-equivariant Poincaré-Birkhoff-Witt theorem. As a noteworthy consequence, this implies each short exact sequence $0 \to U^{n-1} \to U^n \to S^n(\mathscr{G}) \to 0$ of rational G-modules is split. Then in Section 2, we provide an analogous identification (in positive characteristic) of the hyperalgebras of G and its infinitesimal kernels G_r in terms of divided power algebras on $\mathscr{G}$.

Motivated by the main result of Section 1, we study in Sections 3 and 4 the invariants of $S(\mathscr{G})$ [and of $U(\mathscr{G})$] under the actions of the infinitesimal kernels $G_r \subset G$. For $r=1$, Veldkamp [14] studied the invariants in $U(\mathscr{G})$, regarded as the center of $U(\mathscr{G})$. We adopt his methods and extend his results. We achieve this by considering the field of fractions of the G_r-invariants of $S(\mathscr{G})$ in Section 3. Our identification of $S(\mathscr{G})^{G_r}$ and $U(\mathscr{G})^{G_r}$ given in Section 4 has a form quite analogous to Veldkamp's description of the center of $U(\mathscr{G})$. As we show in (4.5), this portrayal illustrates an interesting phenomenon concerning "good filtrations" (in the sense of Donkin [6]) of rational G-modules.

The present paper has its origins in the authors' unsuccessful attempts to understand the proof of Mil'ner's main theorem in [12], which asserts the existence of a (filtration preserving) isomorphism $U(\mathscr{G}) \to S(\mathscr{G})$ of $\mathscr{G}$-modules for an arbitrary restricted Lie algebra $\mathscr{G}$. We are most grateful to Robert L. Wilson for providing us with the example following (1.4) below, which gives a counterexample to the key step in Mil'ner's argument ([12], Proposition 5).

(1) Research supported in part by N.S.F.

(2) The first author gratefully acknowledges the support of the Institute for Advanced Study.

1. A G-invariant form of the P-B-W-theorem

Let $\mathscr{G}$ be a Lie algebra over a field k with universal enveloping algebra $U(\mathscr{G})$. Recall that $U(\mathscr{G})$ has a natural (increasing) filtration $\{U^n\}$, where U^n denotes the subspace of $U(\mathscr{G})$ spanned by all products of at most n elements of $\mathscr{G}$. Also, $U(\mathscr{G})$ carries the structure of a cocommutative Hopf algebra in which the elements of $\mathscr{G}$ are primitive for the comultiplication $\Delta: U(\mathscr{G}) \to U(\mathscr{G}) \otimes U(\mathscr{G})$. Note that each U^n is actually a subcoalgebra of $U(\mathscr{G})$. The adjoint representation of $\mathscr{G}$ extends to an action of $\mathscr{G}$ on $U(\mathscr{G})$ by derivations. If $\mathscr{G}$ is the Lie algebra of a linear algebraic group G, then the adjoint action of G on $\mathscr{G}$ defines in an evident way a rational action of G on $U(\mathscr{G})$ by Hopf algebra automorphisms.

If V is an arbitrary vector space over k, the symmetric algebra $S(V)$ on V carries a Hopf algebra structure in which the elements of V are primitive under the comultiplication $\Delta: S(V) \to S(V) \otimes S(V)$. For $n \geqq 0$, we denote by $S^{\leqq n}(V)$ the sum of the homogeneous components $S^i(V)$ of $S(V)$ with $i \leqq n$. Note that $\{S^{\leqq n}(V)\}$ is filtration of $S(V)$ by subcoalgebras.

In particular, we consider the Hopf algebra $S(U(\mathscr{G}))$ based on the vector space $U(\mathscr{G})$. The following result gives our interpretation (and strengthening) of Mil'ner's ([12], Proposition 1).

(1.1) LEMMA. — *There exists a coalgebra morphism*

$$\varphi: \quad U(\mathscr{G}) \to S(U(\mathscr{G}))$$

in which $\varphi|_{\mathscr{G}}$ *identifies with the natural inclusion of* $\mathscr{G} \subset U(\mathscr{G})$ *into* $S^1(U(\mathscr{G})) = U(\mathscr{G})$ *and* $\varphi(x_1 \ldots x_n) \equiv \varphi(x_1) \ldots \varphi(x_n)$ (mod $S^{\leqq n-1}(U(\mathscr{G}))$) *for* $x_1, \ldots, x_n \in \mathscr{G}$. *The morphism* φ *is* $\mathscr{G}$*-equivariant for the adjoint action of* $\mathscr{G}$ *on* $U(\mathscr{G})$ *and its extension* (*by derivations*) *to* $S(U(\mathscr{G}))$. *Finally,* φ *is* G*-equivariant if* $\mathscr{G} = Lie(G)$ *is the Lie algebra of a linear algebraic group* G *over* k.

Proof. — If $\mathbf{x} = \{x_1, \ldots, x_n\}$ is an ordered sequence of elements of $\mathscr{G}$, for $I = \{i_1 < \ldots < i_k\} \subset N = \{1, \ldots, n\}$ we set $x_I = x_{i_1} \ldots x_{i_k} \in U(\mathscr{G})$. Consider the element

$$\psi(\mathbf{x}) \equiv \sum x_{I_1} \ldots x_{I_k} \in S(U(\mathscr{G})),$$

where the summation extends over all partitions $I_1 \cup \ldots \cup I_k$ of N into nonempty disjoint ordered subsets. (Each I_j is an ordered subset of the ordered set N, whereas the different orderings of $I_1, \ldots, I_k$ are not distinguished.) On the right hand side of the above expression, the product of the x_{I_j} is taken in $S(U(\mathscr{G}))$. Thus, in $S(U(\mathscr{G}))$, x_{I_j} has homogeneous degree 1, so that $x_{I_1} \ldots x_{I_k}$ has homogeneous degree k. In particular, the image of $\psi(\mathbf{x})$ in $S^{\leqq n}(U(\mathscr{G}))/S^{\leqq n-1}(U(\mathscr{G}))$ is $x_{\{1\}} \ldots x_{\{n\}}$. Suppose $1 \leqq j < n$ and $x_{j+1} x_j = x_j x_{j+1} + \xi$, for $\xi \in \mathscr{G}$. Set

$$\mathbf{y} = \{x_1, \ldots, x_{j-1}, x_{j+1}, x_j, x_{j+2}, \ldots, x_n\}$$

and

$$\mathbf{z} = \{x_1, \ldots, x_{j-1}, \xi, x_{j+2}, \ldots, x_n\},$$

and let P be the set of partitions of N in which j and $j+1$ occur in the same ordered subset (which we index to be I_1). Using the surjective order preserving map $N \rightarrow N-1=\{1, \ldots, n-1\}$ sending j and $j+1$ to j to identify P with the set of partitions of $N-1$, we conclude the equalities

$$\psi(\mathbf{y})-\psi(\mathbf{x})=\sum_{P}(y_{I_1}-x_{I_1})\, x_{I_2} \ldots x_{I_k}=\sum z_{I_1} \ldots z_{I_k}=\psi(\mathbf{z}).$$

It follows from the definition of $U(\mathscr{G})$ as a quotient of the tensor algebra based on $\mathscr{G}$ that ψ defines a linear map $\varphi: U(\mathscr{G}) \rightarrow S(U(\mathscr{G}))$ by setting $\varphi(1)=1$ and $\varphi(x_N) \equiv \varphi(x_1 \ldots x_n)=\psi(\mathbf{x})$ for any $\mathbf{x}=(x_1, \ldots, x_n)$. To see that φ is a coalgebra morphism, we note that for a sequence $\mathbf{x}=\{x_1, \ldots, x_n\}$ of elements in $\mathscr{G}$, we have

$$(\varphi \otimes \varphi)\, \Delta(x_1 \ldots x_n)=(\varphi \otimes \varphi)\left(\sum x_I \otimes x_{N \setminus I}\right)=\sum x_{I_1} \ldots x_{I_k} \otimes x_{J_1} \ldots x_{J_l}.$$

In this expression, I runs over all ordered subsets of the ordered set N, while the last summation runs over all such I and all partitions $I_1, \ldots, I_k$ (respectively, $J_1, \ldots, J_l$) of such I (resp., $N \setminus I$). (By convention, we set $x_{\varnothing}=1$.) This term clearly equals

$$\Delta \varphi(x_1 \ldots x_n)=\Delta\left(\sum x_{K_1} \ldots x_{K_t}\right).$$

whence it follows that φ defines a coalgebra morphism. It is immediate, from its definition, that φ has the required equivariance properties. □

Making use of this result, we easily obtain the following theorem, inspired by the main theorem of Mil'ner [12] [*cf.* remarks following (1.4) below].

(1.2) THEOREM. — *Let $\mathscr{G}$ be a Lie algebra over a field k. There is a $\mathscr{G}$-equivariant, filtration preserving isomorphism of coalgebras*

$$\beta: U(\mathscr{G}) \rightarrow S(\mathscr{G})$$

if and only if the natural inclusion $\mathscr{G} \subset U(\mathscr{G})$ splits relative to the adjoint action of $\mathscr{G}$ on $U(\mathscr{G})$. Furthermore, if $\mathscr{G}=\operatorname{Lie}(G)$ is the Lie algebra of a linear algebraic group G, β can be taken to be G-equivariant if and only if the inclusion $\mathscr{G} \subset U(\mathscr{G})$ splits as rational G-modules. When β exists, the associated graded map $\operatorname{gr}(\beta): \operatorname{gr}(U(\mathscr{G})) \rightarrow \operatorname{gr}(S(\mathscr{G})) \cong S(\mathscr{G})$ is an isomorphism of Hopf algebras.

Proof. — If the isomorphism β exists, it maps $\mathscr{G} \subset U(\mathscr{G})$ isomorphically to $\mathscr{G}=S^1(\mathscr{G})$ since $\mathscr{G}$ is the space of primitive elements contained in $S^{\leqq 1}(\mathscr{G})$. It follows that $\mathscr{G} \subset U(\mathscr{G})$ splits for $\mathscr{G}$ (or G if applicable). Conversely, assume that the inclusion $\mathscr{G} \subset U(\mathscr{G})$ splits for the action of $\mathscr{G}$ on $U(\mathscr{G})$. Thus, there exists an equivariant projection $p: U(\mathscr{G}) \rightarrow \mathscr{G}$ of $\mathscr{G}$-modules, which induces an equivariant morphism $S(p): S(U(\mathscr{G})) \rightarrow S(\mathscr{G})$ of Hopf algebras. It follows that if φ is as in (1.1), then $\beta=S(p) \circ \varphi: U(\mathscr{G}) \rightarrow S(\mathscr{G})$ is an equivariant, filtration preserving morphism of coalgebras. By (1.1), β induces an isomorphism $\operatorname{gr}(\beta): U^n/U^{n-1} \rightarrow S^{\leqq n}(\mathscr{G})/S^{\leqq n-1}(\mathscr{G})$, so that β itself is necessarily an isomorphism. This establishes the first part of the theorem, while the second is obtained similarly, using (1.1). The final assertion follows from the property $\varphi(x_1 \ldots x_n) \equiv \varphi(x_1) \ldots \varphi(x_n)$ $(\operatorname{mod} S^{\leqq n-1}(U(\mathscr{G})))$ for φ as in (1.1). □

We proceed to investigate circumstances under which an isomorphism β in (1.2) exists. If k has characteristic 0, the mapping $\eta: S(\mathscr{G}) \to U(\mathscr{G})$ defined by

$$\eta(x_1 \ldots x_n) = 1/n! \sum x_{\tau(1)} \ldots x_{\tau(n)} \qquad (x_1, \ldots, x_n \in \mathscr{G})$$

(where τ runs over permutations of $\{1, \ldots, n\}$) is clearly equivariant. By [2] (Ch. II, § 1, No. 5, Proposition 9), η is an isomorphism of coalgebras, and we can therefore put $\beta = \eta^{-1}$.

For the rest of this paper we assume therefore that k is an algebraically closed field of positive characteristic p.

If $\mathscr{G}$ is a restricted Lie algebra over k with p-operator $x \to x^{[p]}$, we denote its restricted enveloping algebra by $V(\mathscr{G})$. Thus, $V(\mathscr{G})$ is a finite dimensional Hopf algebra which is obtained from $U(\mathscr{G})$ by factoring out the ideal generated by elements of the form $x^{[p]} - x^p$, $x \in \mathscr{G}$. The adjoint action of $\mathscr{G}$ defines an action by derivations of $\mathscr{G}$ on $V(\mathscr{G})$. Also, if $\mathscr{G}$ is the Lie algebra of a linear algebraic group G, the adjoint action of G on $\mathscr{G}$ extends to a rational action of G on $V(\mathscr{G})$ by Hopf algebra automorphisms.

Recall that the bad primes p for a simple, simply connected algebraic group G defined and split over k are as follows:

none if G is of type A_l;

$p = 2$ if G is of type B_l, C_l, or D_l;

$p = 2$ or 3 if G is of type G_2, F_4, E_6, or E_7;

$p = 2$, 3, or 5 if G is of type E_8.

If a prime p is not bad for G, it is called good. Then we have the following result.

(1.3) LEMMA. — *Suppose $G = GL_n$ or that G is a simple, simply connected algebraic group defined over an algebraically closed field k of positive characteristic p which is good for G. If $G = SL_n$, assume also that p does not divide n. Then the natural inclusion $\mathscr{G} \subset V(\mathscr{G})$ of rational G-modules is split.*

Proof. — Let I be the ideal of functions in the coordinate ring $k[G]$ of G which vanish at the identity 1. Then $\mathscr{G}$ identifies with the linear dual $(I/I^2)^*$. It follows from [1] (4.4, p. 505) that, under the hypotheses of the lemma, we may assume that the quotient map $\pi: k[G] \to \mathscr{G}^* \cong k[G]/(I^2 \oplus k)$ admits a G-equivariant section s. Let G_1 be the infinitesimal subgroup of G of height $\leqq 1$ with $\mathrm{Lie}(G_1) = \mathscr{G}$ ([5], II, § 7, No. 4.3). If $\sigma: k[G] \to k[G_1]$ is the restriction map on coordinate rings, the quotient map $\pi_1: k[G_1] \to \mathscr{G}^*$ admits $\sigma \circ s$ as a G-equivariant section. Moreover, in the identification of the dual Hopf algebra $k[G_1]^*$ with $V(\mathscr{G})$ ([5], II, § 7, No. 4.2), the dual mapping π_1^* identifies with the natural inclusion $\mathscr{G} \subset V(\mathscr{G})$. This establishes the lemma. □

We use this result in proving the following G-equivariant P-B-W theorem.

(1.4) THEOREM. — *Assume that G is a linear algebraic group over k of one of the following types:* (i) $G \cong GL_n$; (ii) *G is a simple, simply connected algebraic group not of type A_l and p is good for G;* (iii) *G is of type A_l and p does not divide $l+1$. Then there is a G-equivariant, filtration preserving isomorphism*

$$\beta: \quad U(\mathscr{G}) \to S(\mathscr{G})$$

of coalgebras, whose induced morphism gr(β) *is an isomorphism of* G-*Hopf algebras.*

Proof. — By (1.3), the natural inclusion $\mathcal{G} \subset V(\mathcal{G})$ splits for the action of G on $V(\mathcal{G})$. Composing a G-equivariant projection $V(\mathcal{G}) \to \mathcal{G}$ with the natural quotient morphism $U(\mathcal{G}) \to V(\mathcal{G})$, we obtain that the inclusion $\mathcal{G} \subset U(\mathcal{G})$ also splits for the action of G. Thus, the theorem follows from (1.2). □

Robert Wilson has kindly given us the following example which shows that the conclusion of Lemma 1.3 is false for a general restricted Lie algebra. Let $\mathcal{G}$ be the central extension of sl_2 with basis e, h, f, z satisfying $[e, f]=h$, $[h, e]=2e$, $[h, f]=-2f$, $[\mathcal{G}, z]=0$. We make $\mathcal{G}$ into a restricted Lie algebra by defining $e^{[p]}=z$, $h^{[p]}=h$, $f^{[p]}=0$, $z^{[p]}=0$. Assume that $p > 3$, and put $w=e^{p-3}h^3 \in V(\mathcal{G})$. Then $w \notin \mathcal{G}$ and $(\operatorname{ad} e)^3 w=-48z$. Since $(\operatorname{ad} e)^3 \mathcal{G}=0$, if w_1 is the projection of w into any subspace of $V(\mathcal{G})$ which is a complement to $\mathcal{G}$ in $V(\mathcal{G})$, we obtain that $(\operatorname{ad} e)^3 w_1=(\operatorname{ad} e)^3 w$ is a nonzero element in $\mathcal{G}$. Thus, the inclusion $\mathcal{G} \subset V(\mathcal{G})$ does not split for the action of $\mathcal{G}$ as claimed by Mil'ner ([12], Proposition 5). For $p=2$ and $\mathcal{G}=sl_2$, a similar example can be given replacing w by ef and $(\operatorname{ad} e)^3$ by $(\operatorname{ad} f)(\operatorname{ad} e)$. Note in this case that the monomials $e^a h^b f^c$ of degree > 1 in $U(\mathcal{G})$ span an $\operatorname{ad}(\mathcal{G})$-invariant subspace, providing an isomorphism $U(\mathcal{G}) \to S(\mathcal{G})$ of coalgebras which is equivariant relative to the adjoint action of $\mathcal{G}$.

2. A G-equivariant P-B-W theorem for hyperalgebras

In this section we obtain results analogous to those of Section 1 for the hyperalgebras of certain algebraic groups. The reader is referred to [3] for a more detailed discussion concerning the theory of hyperalgebras which we require.

Let k be an algebraically closed field of positive characteristic p, and let G be a connected, linear algebraic group defined over the prime field $\mathbf{F}_p$. For $r \geqq 1$, G_r denotes the group-scheme theoretic kernel of the r-th power of the Frobenius morphism $\sigma: G \to G$. The coordinate ring $k[G_r]$ of G_r is a finite dimensional commutative Hopf algebra. By definition, the hyperalgebra $\operatorname{hy}(G_r)$ of G_r is the Hopf algebra dual of $k[G_r]$. The natural inclusions $G_r \subset G_{r+1}$ provide Hopf algebra embeddings $\operatorname{hy}(G_r) \subset \operatorname{hy}(G_{r+1})$, and the hyperalgebra of G is realized as the limit

$$\operatorname{hy}(G)=\varinjlim \operatorname{hy}(G_r).$$

As such, hy(G) is a cocommutative, infinite dimensional (if $G \neq e$) Hopf algebra. The conjugation action of G on itself induces a natural (rational) G-action on each $\operatorname{hy}(G_r)$ and hence on hy(G) by Hopf algebra automorphisms.

For example, suppose G is the d-dimensional vector group $V=G_a^{\times d}$. If $x_1, \ldots, x_d$ is a basis for $V(\mathbf{F}_p)$, hy(V) has a k-basis on symbols $x_1^{(m_1)} \ldots x_d^{(m_d)}$, $m_1, \ldots, m_d \geqq 0$. Since hy(V) is commutative, the rules $x_i^{(a)} x_i^{(b)}=\binom{a+b}{a} x_i^{(a+b)}$ specify its multiplication. Also, the comultiplication is given by $\Delta(x_i^{(a)})=\sum_{b+c=a} x_i^{(b)} \otimes x_i^{(c)}$. Thus, the $x_i^{(m)}$ behave like the divided powers $x_i^m/m!$ [and $\mathrm{hy}(V)$ identifies with the graded dual $S(V^*)^{*gr}$ of the symmetric algebra $S(V^*)$]. Note that $\mathrm{hy}(V)$ is naturally graded by setting $\mathrm{hy}^m(V)$ equal to the linear span of all monomials $x_1^{(m_1)} \ldots x_d^{(m_d)}$ satisfying $m = m_1 + \ldots + m_d$. This defines an increasing filtration $\{\mathrm{hy}^{\leqq n}(V)\}$ on $\mathrm{hy}(V)$ by subcoalgebras in which the associated graded Hopf algebra $\mathrm{gr}(\mathrm{hy}(V))$ identifies with $\mathrm{hy}(V)$. For $r \geqq 1$, the hyperalgebra $\mathrm{hy}(V_r)$ of the infinitesimal subgroup scheme V_r corresponds to the subspace of $\mathrm{hy}(V)$ spanned by those monomials above satisfying $m_i < p^r$, $1 \leqq i \leqq d$. Finally, GL_d acts naturally on $\mathrm{hy}(V)$ by Hopf algebra automorphisms, preserving the grading, etc.

If G is a simple, simply connected algebraic group defined and split over $\mathbf{F}_p$, $\mathrm{hy}(G)$ has a basis consisting of monomials

$$x_{-\beta_1}^{a_1}/a_1! \ldots x_{-\beta_N}^{a_N}/a_N! \binom{h_1}{b_1} \ldots \binom{h_l}{b_l} x_{\beta_1}^{c_1}/c_1! \ldots x_{\beta_N}^{c_N}/c_N!$$

(usual notation, *cf.* [3; 5.1]). Observe that $\mathrm{hy}(G)$ is graded by setting $\mathrm{hy}^n(G)$ to be the linear span of those monomials of total degree $\sum a_i + \sum b_j + \sum c_k = n$, and we obtain an increasing filtration $\{\mathrm{hy}^{\leqq n}(G)\}$ of $\mathrm{hy}(G)$ by subcoalgebras, stable under the action of G on $\mathrm{hy}(G)$. We do not go into further details here, but refer instead to [3] (§ 5), [2] (Ch. 8, § 12, No. 3).

We now prove the following companion theorem to Theorem 1.4. In the statement of this result, $\mathrm{hy}(\mathscr{G})$ denotes the hyperalgebra of $\mathscr{G}$ regarded as a vector group defined over $\mathbf{F}_p$. For simplicity we omit the case of GL_n; the interested reader should have no trouble supplying the modifications to handle this group.

(2.1) THEOREM. — *Let* G *be a simple, simply connected algebraic group defined and split over* $\mathbf{F}_p$. *Assume that* p *is good for* G *and that if* G *is of type* A_l *then* p *does not divide* $l+1$. *Then there exists a* G*-equivariant, filtration preserving isomorphism of coalgebras*

$$\beta: \quad \mathrm{hy}(G) \to \mathrm{hy}(\mathscr{G})$$

with the property that the induced map $\mathrm{gr}(\beta): \mathrm{gr}(\mathrm{hy}(G)) \to \mathrm{hy}(\mathscr{G})$ *is a* G*-isomorphism of Hopf algebras. Moreover, for each* $r \geqq 1$, β *restricts to a* G*-equivariant, filtration preserving isomorphism of coalgebras*

$$\beta_r: \quad \mathrm{hy}(G_r) \to \mathrm{hy}(\mathscr{G}_r)$$

for which $\mathrm{gr}(\beta_r)$ *is a* G*-equivariant isomorphism of Hopf algebras.*

Proof. — As noted in the proof of (1.3), the natural quotient map $k[G] \to \mathscr{G}^*$ admits a G-equivariant section $\mathscr{G}^* \to k[G]$. Composing this map with the restriction homomorphism $k[G] \to k[G_r]$ provides a G-equivariant section $s_r: \mathscr{G}^* \to k[G_r]$ to the quotient map $k[G_r] \to \mathscr{G}^*$. Since $k[G_r]$ identifies with a truncated polynomial algebra $k[T_1, \ldots, T_d]/(T_1^{p^r}, \ldots, T_d^{p^r})$, $d = \dim G$, by [3] (§ 9.1), [5] (III, § 3, No. 6.4), it follows that s_r identifies $k[G_r]$ G-equivariantly with $S(\mathscr{G}^*)/\mathscr{G}^{*p^r}$ as commutative algebras. Taking duals, we obtain the desired G-equivariant isomorphism β_r: $hy(G_r) \to hy(\mathscr{G}_r)$ of coalgebras. Because the s_r are by construction compatible, it follows that the β_r define a G-equivariant isomorphism $\beta: hy(G) \to hy(\mathscr{G})$ of coalgebras. Furthermore, using the usual basis of hy(G) we easily see that $gr(\beta)$ is an isomorphism of Hopf algebras. □

Further information concerning the G-module structure of hy(G) will be given in paragraph 4 below.

3. Fraction fields and their invariants

Let G be a linear algebraic group defined over $\mathbf{F}_p$, as in Section 2 above. In this section, we investigate the invariants of the field of fractions of $S(\mathscr{G})$ under the action of the infinitesimal subgroups G_r. (Recall that a rational module V for an affine k-group H is, by definition, a comodule for the coordinate ring $k[H]$ of H. If $\Delta_V: V \to k[H] \otimes V$ is the corresponding comodule map, then the subspace of invariants is defined by $V^H = \{ v \in V : \Delta_V(v) = 1 \otimes v \}$ ([3], 1.1). From an equivalent functorial point of view ([5], II, § 2, No. 1), V^H consists of those $v \in V$ such that $v \otimes 1 \in V \otimes R$ is H(R)-fixed for all commutative k-algebras R.)

Let $\rho: G \to GL(V)$ be a finite dimensional rational $\mathbf{F}_p$-representation. Let $A = S(V)$ and set K equal to the field of fractions of A. In general, K is *not* a rational G-module since it need not be locally finite for the action of G. However, it is interesting to note that each infinitesimal subgroup G_r does act rationally on K. To see this, first observe that relative to a fixed basis for $V(\mathbf{F}_p)$, any $x \in G_r(R)$ (R a commutative k-algebra) is represented on $V \otimes R$ by a matrix of the form $I + D$, where the matrix entries in D have p^r-power equal to 0. Thus, for $v \in V$, the element

$$\rho(x)(v \otimes 1) - v \otimes 1 = D(v \otimes 1) \in V \otimes R \subset S(V) \otimes R \cong S(V \otimes R),$$

satisfies the relation $[\rho(x)(v \otimes 1) - v \otimes 1]^{p^r} = 0$. Hence, given any $f \in S(v)$ and $x \in G(R)$, we have $(\rho(x)(f \otimes 1))^{p^r} = f^{p^r} \otimes 1$. This shows that $K \otimes R$ is isomorphic to the localization of $A \otimes R$ relative to the multiplicative subset generated by $\rho(G_r(R))(A^\times \otimes 1)$, and hence $K \otimes R$ is a $R - G_r(R)$-module, functorial in R. By [5] (II, § 2.1), K is a rational G_r-module. Of course, when $r = 1$, this merely amounts to the familiar procedure of extending an action of the Lie algebra $\mathscr{G}$ on A by derivations to an action (by derivations) on the fraction field K by the quotient rule of calculus.

We can now state the following result concerning invariants.

(3.1) Proposition. — *Let* G *be a linear algebraic group defined over* $\mathbf{F}_p$ *and let* $\rho: G \to GL(V)$ *be a finite dimensional rational* $\mathbf{F}_p$*-representation. Let* K *denote the field of fractions of* $A = S(V)$ *and let* K_r *denote the field of fractions of the algebra of invariants* A^{G_r}. *Then* K_r *equals* K^{G_r} *for any* $r > 0$, *where* K *is given the structure of a rational* G_r-*module described above.*

Proof. — Clearly, $K_r \subset K^{G_r}$. Conversely, if $\lambda = x/s \in K^{G_r}$ with x, $s \in A$, then $s^{p^r} \in A^{G_r}$ and $\lambda = xs^{p^r-1}/s^{p^r} \in K_r$. □

Now fix a simple, simply connected algebraic group G defined and split over $\mathbf{F}_p$. Assume that p does not divide the order of the Weyl group W of G. In particular, this implies that the Killing form on $\mathscr{G}$ is non-degenerate, and we thereby identify $\mathscr{G} \cong \mathscr{G}^*$ as rational G-modules. Let $\mathscr{H} = \mathrm{Lie}(T) \subset \mathscr{G} = \mathrm{Lie}(G)$ be the Lie algebra of a maximal split torus T of G. Then $S(\mathscr{G})^G \cong S(\mathscr{H})^W$ [13] is isomorphic to a polynomial ring J on homogeneous generators $T_1, \ldots, T_l$ ($l = \mathrm{rank}\ G$) of degrees $m_1+1, \ldots, m_l+1$ where the m_i are the exponents of the root system of T in G [4]. Let K be the field of fractions of $S(\mathscr{G})$. Extending arguments of Veldkamp [14] for $r=1$, we identify $K_r = K^{G_r}$ using this polynomial algebra J. We first require the following result.

(3.2) LEMMA. — *Fix an ordered basis* $\{X_1, \ldots, X_n\}$ *of* $\mathscr{G}$ *and let* C *be the* $n \times n$ K-*matrix* (a_{ij}), *where* $a_{ij} = [X_i, X_j] \in K$. *Then* $\mathrm{rank}(C) \geqq \dim G/T = n - l$.

Proof. — Let Φ be the root system of T in $\mathscr{G}$, and for $\alpha \in \Phi$, let e_α be a nonzero root vector of weight α. Since the rank of C is independent of the choice of basis for $\mathscr{G}$, we may assume that $\{e_\alpha\}_{\alpha \in \Phi}$ is part of our basis $\{X_i\}$. It is therefore enough to show that the submatrix $B = ([e_\alpha, e_\beta])$ of C is nonsingular. Let $\tau: S(\mathscr{G}) \to S(\mathscr{H})$ be the algebra homomorphism defined by $\tau(e_\alpha) = 0$ for all $\alpha \in \Phi$ and $\tau(h) = h$ for all $h \in \mathscr{H}$. Since G is simply connected, each $[e_\alpha, e_{-\alpha}]$, $\alpha \in \Phi$, is a nonzero element of $\mathscr{H}$. Hence, $\tau(B)$ has exactly one nonzero entry in each row and column, and so is nonsingular. Hence, B is nonsingular. □

(3.3) THEOREM. — *Let* G *be a simple, simply connected algebraic group defined and split over* $\mathbf{F}_p$ *of dimension n and* rank *l with the property that p is prime to the order of the Weyl group* W *of* G. *For each positive integer r, the natural* G-*map* $S(\mathscr{G}^{(r)}) \otimes_{J^{(r)}} J \to S(\mathscr{G})^{G_r}$ *is an injection and induces an isomorphism on associated fields of fractions*

$$\mathrm{frac}(S(\mathscr{G}^{(r)}) \otimes_{J^{(r)}} J) \cong K_r.$$

Here $S(\mathscr{G}^{(r)})$(*respectively,* $J^{(r)}$) *is the subalgebra of* $S(\mathscr{G})$ (*resp.,* J) *generated by the* p^r-*th powers of the homogeneous generators of* $S(\mathscr{G})$ (*resp.,* J) *and* $J = S(\mathscr{G})^G$.

Proof. — We first assert that the monomials $T_1^{a_1} \ldots T_l^{a_l}$, $0 \leqq a_i < p^r$, in $S(\mathscr{G})$ are linearly independent over $S(\mathscr{G}^{(r)})$. Fix a basis $\{X_i\}$ of $\mathscr{G}$. We recall from [14] (7.1) that the Jacobian matrix $(\partial T_i/\partial X_j)$ has rank l at $\varphi \in \mathscr{G}^* \cong \mathscr{G}$ if and only if φ is regular. Since the regular elements of $\mathscr{G}$ form an open dense subset, $(\partial T_i/\partial X_j)$ has rank l. As argued in [14] this establishes our assertion when $r=1$. The general case then follows by an easy inductive argument on r.

Thus, the natural map $S(\mathscr{G}^{(r)}) \otimes_{J^{(r)}} J \to S(\mathscr{G})^{G_r}$ is injective, and we let K_r' be the field of fractions of the image domain. Since J is a free $J^{(r)}$-module of rank p^{rl}, we conclude that K_r' is a subfield of K_r which is an extension of degree p^{rl} over K^{p^r}. Hence, $[K : K_r'] = p^{r(n-l)}$. To prove the inclusion $K_r' \subset K_r$ is actually an equality, it suffices to prove that $[K : K_r] \geqq p^{r(n-l)}$. We proceed to prove that $[K_s : K_{s+1}] \geqq p^{n-l}$ for each s, $0 \leqq s < r$ (with $K_0 = K$).

By Proposition 3.1, $K_{s+1}=K_s^{G_{s+1}/G_s}$. Identifying G_{s+1}/G_s with G_1, and the G_{s+1}/G_s-module K_s with the corresponding "untwisted" G_1-module $K_s^{(-s)}$ [3] (3.3), we obtain that $K_{s+1}\cong(K_s^{(-s)})^{G_1}=(K_s^{(-s)})^{\mathscr{G}}$. Thus, the Jacobson-Bourbaki theorem ([10], Theorem 19, p. 186) implies that $[K_s:K_{s+1}]=p^{[\mathscr{G}_s:K_s^{(-s)}]}$ where $\mathscr{G}_s$ denotes the $K_s^{(-s)}$-span of the image of $\mathscr{G}$ in the derivation algebra Der $(K_s^{(-s)})$. For X, $Y\in\mathscr{G}$, the derivation of $K_s^{(-s)}$ defined by X maps $(Y^{p^s})^{(-s)}\in K_s^{(-s)}$ to $([X,Y]^{p^s})^{(-s)}$. Thus, $[\mathscr{G}_s:K_s^{(-s)}]$ equals at least the rank of the matrix C of (3.2). Thus, by (3.2), $[K_s:K_{s+1}]\geqq p^{n-l}$ as required. □

In the course of the above proof we have also established the following result which may be of independent interest.

(3.4) COROLLARY. — *Let* G *be as in* (3.3). *Then the matrix* C *of* (3.2) *has rank exactly equal to* dim G/T. *Furthermore, if* $K\mathscr{G}$ *is the* K-*span of the image of* $\mathscr{G}$ *in the derivation algebra* Der (K), *then* $K\mathscr{G}$ *has dimension equal to* dim G/T *over* K. □

We also obtain the following corollary from (the proof of) Theorem 3.3.

(3.5) COROLLARY. — *Let* G *be as in* (3.3). *Then* K *is purely inseparable of dimension* $p^{r(n-l)}$ *over* $K_r=K^{G_r}$, *whereas* K_r *is purely inseparable of dimension* p^{rl} *over* $\operatorname{frac} S(\mathscr{G}^{(r)})=K^{p^r}$. □

It is amusing to observe that the extension analogous to K_1/K^p in the context of $U(\mathscr{G})$ is separable. Namely, the field of fractions of the center of $U(\mathscr{G})$ [which we may view as $U(\mathscr{G})^{G_1}$ to preserve the analogy with $S(\mathscr{G})$] is separable over the field of fractions of the central subalgebra $\mathscr{O}\cong S(\mathscr{G}^{(1)})$ [11], Lemma 4.2) (*see* also Proposition 4.5 below).

4. Infinitesimally invariant subalgebras

In Theorem 4.1 below we identify for a simple, simply connected algebraic group G defined and split over $\mathbf{F}_p$ the G_r-invariants of $S(\mathscr{G})$ in terms of $S(\mathscr{G}^{(r)})=S(\mathscr{G})^{p^r}$ and the polynomial subalgebra $J=S(\mathscr{G})^G\subset S(\mathscr{G})$. We then use this result to provide a corresponding identification of the G_r-invariants of $U(\mathscr{G})$, thereby extending Veldkamp's determination of the center of $U(\mathscr{G})$ [14]. Our proofs are modifications of Veldkamp's original arguments. In Proposition 4.5, we interpret the information given by Theorem 4.1 in the light of the existence of a "good filtration" on $S(\mathscr{G})$.

(4.1) THEOREM. — *Let* G *be a simple algebraic group defined and split over* $\mathbf{F}_p$ *of dimension n and rank l with the property that p does not divide the order of the Weyl group* W *of* G. *For each positive integer r, there is a natural isomorphism*

$$S(\mathscr{G}^{(r)})\otimes_{J^{(r)}}J\cong S(\mathscr{G})^{G_r}$$

of rational G-*algebras.*

Proof. — For notational convenience, let $A_r'=S(\mathscr{G}^{(r)})\otimes_{J^{(r)}}J$ and let $A_r=S(\mathscr{G})^{G_r}$. By Theorem 3.3, the natural map $A_r'\to A_r$ is an inclusion which induces an isomorphism on the corresponding fields of fractions. Since $A_r'\to A_r$ is clearly a finite map, it suffices to prove that A'_r is integrally closed. We explicitly write the extension $J \to A'_r$ as

$$k[T_1, \ldots, T_l] \to k[T_1, \ldots, T_l][x_1^{p^r}, \ldots, x_n^{p^r}]/(T_i^{p^r} - t_i(x_1^{p^r}, \ldots, x_n^{p^r}), 1 \leq i \leq l).$$

The Jacobian matrix $(\partial t_i/\partial x_j)$ has rank l at an element φ of $\mathcal{G}^*$ (naturally homeomorphic to the maximal ideal space of A'_r) if and only if $\varphi \in \mathcal{G}^*$ ($\cong \mathcal{G}$ via the Killing form) is regular. Hence, A'_r is regular in codimension 2. As presented above, A'_r is clearly a complete intersection of hypersurfaces in affine $n+l$ space. Hence, Serre's normality criterion ([9], 5.8.6) implies that A'_r is normal as required. □

Identifying $\mathcal{G}$ with $\mathcal{G}^*$ via the Killing form, we can restate Theorem 4.1 in geometric language as follows.

(4.2) COROLLARY. — *For* G *as in* (4.1), *there is a natural isomorphism of* G-*schemes*

$$\mathcal{G}/G_r \cong \mathcal{G}^{(r)} \times_{(\mathcal{G}/G)^{(r)}} \mathcal{G}/G.$$

Because the isomorphism $U(\mathcal{G}) \cong S(\mathcal{G})$ of Section 1 is not multiplicative, a description of $U(\mathcal{G})^{G_r}$ analogous to that of $S(\mathcal{G})^{G_r}$ in Theorem 4.1 requires a little effort. We recall the central G-subalgebra $\mathcal{O} \subset U(\mathcal{G})$ given as the (isomorphic) image of the G-algebra map $S(\mathcal{G}^{(1)}) \to U(\mathcal{G})$ sending $X \in \mathcal{G}^{(1)}$ to $X^p - X^{[p]} \in U(\mathcal{G})$. We define $\mathcal{O}^r$ to be

$$\mathcal{O}_r = S(\operatorname{span}\{e_\alpha^{p^r}, (h_\beta^p - h_\beta)^{p^{r-1}}; \alpha \in \Phi, \beta \in \Pi\}).$$

Here Φ denotes the root system of G, Π is a set of simple roots, and $\{e_\alpha, h_\beta; \alpha \in \Phi, \beta \in \Pi\}$ is a standard (Chevalley) basis for $\mathcal{G}$. The following corollary is a generalization to $r > 1$ of Veldkamp's description of the center $U(\mathcal{G})^{G_1}$ of $U(\mathcal{G})$ [14; 3.1].

(4.3) COROLLARY. — *For* G *as in* (4.1) *and* $r \geq 1$, $U(\mathcal{G})^{G_r}$ *is isomorphic as a rational* G-*module to a direct sum of* p^{rl} *copies of* $\mathcal{O}_r$. *More precisely, if* $S_1, \ldots, S_l$ *are* G-*invariant elements of* $U(\mathcal{G})$ *whose representatives in* $\operatorname{gr}(U(\mathcal{G})) \cong S(\mathcal{G})$ *are the homogeneous generators* $T_1, \ldots, T_l$ *of* $S(\mathcal{G})^G$, *then the natural map*

$$\mathcal{O}_r[s_1, \ldots, s_l] \to U(\mathcal{G})^{G_r}, \qquad s_i \to S_i$$

restricts to an isomorphism from the submodule $\mathcal{O}_r[s_1, \ldots, s_l; p^r]$ *of polynomials of degree* $< p^r$ *in each of the* s_i *onto* $U(\mathcal{G})^{G_r}$.

Proof. — Because $\mathcal{O}_r \subset U(\mathcal{G})$ has the property that its associated graded group (with respect to the filtration $\{U^n\}$ on $U(\mathcal{G})$) is $S(\mathcal{G}^{(r)}) \subset S(\mathcal{G})$, we conclude using Theorem 4.1 that the associated graded group of the image of $\mathcal{O}_r[s_1, \ldots, s_l; p^r] \to U(\mathcal{G})^{G_r}$ is $S(\mathcal{G})^{G_r} \subset S(\mathcal{G})$. Hence, $\mathcal{O}_r[s_1, \ldots, s_l; p^r] \to U(\mathcal{G})^{G_r}$ is surjective. On the other hand, the associated graded group of $\mathcal{O}_r[s_1, \ldots, s_l; p^r]$ maps injectively to $S(\mathcal{G})^{G_r}$, so that $\mathcal{O}_r[s_1, \ldots, s_l; p^r] \to U(\mathcal{G})^{G_r}$ must be injective as well. □

We conclude by investigating one aspect of the G-extensions occuring in $S(\mathcal{G})$. Let G be as in (4.1), and let T be a maximal split torus contained in a fixed Borel subgroup $B \subset G$. For any dominant weight λ, denote by $I(\lambda)$ the rational G-module obtained by inducing to G the one-dimensional rational B-module defined by the character $w_0(\lambda)$.

An increasing filtration by rational G-modules of a given rational G-module M is said to be *good* if its sections are of the form $I(\lambda)$, *cf.* [6]. Then we have the following result.

(4.4) PROPOSITION. — *Let* G *be a simple, simply connected algebraic group defined and split over* $\mathbf{F}_p$ *as above. Assume that p does not divide the order of the Weyl group of* G. *Then:*

(*a*) $S(\mathcal{G})$ *has a good filtration;*

(*b*) $U(\mathcal{G})$ *has a good filtration; and*

(*c*) $hy(G)$ *does not have a good filtration.*

In particular, $U(\mathcal{G})$ *is not isomorphic to* $hy(G)$ *as a rational* G-*module.*

Proof. — (*a*) follows from [1] (4.4) (improving the bounds in [8]), and (*b*) is clear from Theorem 1.4. To prove (*c*) it is enough by Theorem 2.1 to prove that $hy(\mathcal{G})$ does not have a good filtration. We assert that the component $hy^p(\mathcal{G})$ does not admit a good filtration. First, observe that if ν is the maximal root in the root system Φ of G, then $p\nu$ is the maximal dominant weight in $hy^p(\mathcal{G})$, so that if $hy^p(\mathcal{G})$ admits a good filtration, there exists a surjective G-module homomorphism $hy^p(\mathcal{G}) \to I(p\nu)$ [6]. On the other hand, the subspace V of $hy^p(\mathcal{G})$ spanned by those monomials $x_1^{(a_1)} \dots x_n^{(a_n)}$ with $0 \leqq a_i < p$ is clearly G-stable and $hy^p(\mathcal{G})/V \cong \mathcal{G}^{(1)}$. It follows from universal mapping that if there exists a surjective G-module homomorphism $hy^p(\mathcal{G}) \to I(p\nu)$, then this map must factor through $\mathcal{G}^{(1)}$. This is not possible since $\mathcal{G}^{(1)} \neq I(p\nu)$ identifies with the socle of $I(p\nu)$. □

The following question (originally asked by S. Donkin) is of considerable interest. If M is a rational G-module with a good filtration and $r > 1$, then does $(M^{G_r})^{(-r)}$ also have a good filtration? An easy universal mapping property argument gives a positive answer to this question in the very special case of a rational G-module with a split good filtration: $I(p^r\lambda)^{G_r} \cong I(\lambda)^{(r)}$, whereas $I(\mu)^{G_r} = 0$ if $\mu \neq p^r\lambda$ for some dominant weight λ. Our next result gives additional examples for which the answer to Donkin's question is positive.

(4.5) PROPOSITION. — *Let* G *be a simple algebraic group defined and split over* $\mathbf{F}_p$ *and assume that p does not divide the order of the Weyl group of* G. *Then* $(S(\mathcal{G})^{G_r})^{(-r)}$ *has a good filtration for any* $r > 0$. *On the other hand, let* ν *be the maximal root. For any* $n < p$ *for which the induced module* $I(n\nu)$ *is not self-dual, the good filtration on* $S^n(\mathcal{G})$ *does not split.*

Proof. — By Theorem 4.1, $(S(\mathcal{G})^{G_r})^{(-r)}$ is isomorphic as a G-module to a direct sum of copies of $S(\mathcal{G})$ and thus also has a good filtration by (4.4*a*). If the good filtration of $S^n(\mathcal{G})$ splits, one and only one summand is isomorphic to $I(n\nu)$ since $n\nu$ occurs with multiplicity one in $S^n(\mathcal{G})$. For $n < p$, $S^n(\mathcal{G})$ is self dual so that a splitting of the good filtration for $S^n(\mathcal{G}) \cong (S^n(\mathcal{G}))^*$ would imply that $I(n\nu)$ is likewise self-dual. □

REFERENCES

[1] H. ANDERSEN and J. JANTZEN, *Cohomology of Induced Representations of Algebraic Groups* (*Math. Ann.* Vol. 269, 1984, pp. 487-525).

[2] N. BOURBAKI, *Groupes et algèbres de Lie*, Chap. 2, 3, . . . , Hermann, Paris, (1972. . .).
[3] E. CLINE, B. PARSHALL and L. SCOTT, *Cohomology, Hyperalgebras, and Representations* (*J. Algebra*, Vol. 63, 1980, pp. 98-123).
[4] M. DEMAZURE, *Invariants symétriques entiers des groupes de Weyl et torsion* (*Inv. Math.*, Vol. 21, 1973, pp. 287-301).
[5] M. DEMAZURE and P. GABRIEL, *Groupes Algébriques*, I, North-Holland, 1970.
[6] S. DONKIN, *Rational Representations of Algebraic Groups: Tensor Products and Filtrations* (*Lec. Notes in Math.*, No. 1140, Springer, 1985).
[7] E. FRIEDLANDER and B. PARSHALL, *On the Cohomology of Algebraic and Related Finite Groups* (*Inv. Math.*, Vol. 4, 1983, pp. 85-117).
[8] E. FRIEDLANDER and B. PARSHALL, *Cohomology of Lie Algebras and Algebraic Groups* (*Amer. J. Math.*, Vol. 108, 1986, pp. 235-253).
[9] A. GROTHENDIECK, *Éléments de géométrie algébrique*, IV, (*Publ. Math. I.H.E.S.*, Vol. 24, 1965).
[10] N. JACOBSON, *Lectures in AbstractAlgebra*, III, Van Nostrand, 1964.
[11] V. KAC and B. WEISFEILER, *Coadjoint Action of a Semi-Simple Algebraic Group and the Center of the Enveloping Algebra in Characteristic p* (*Indag. Math.*, Vol. 38, 1976, pp. 135-151).
[12] A. A. MIL'NER, *Maximal Degree of Irreducible Lie Algebra Representations Over a Field of Positive Characteristic* (*Funks. Anal.*, Vol. 14, No. 2, 1980, pp. 67-68).
[13] T. SPRINGER and R. STEINBERG, *Conjugacy Classes* (*Lec. Notes in Math.*, No. 131, Springer, 1970, pp. 167-266).
[14] F. VELDKAMP, *The Center of the Universal Enveloping Algebra of a Lie Algebra in Characteristic p* (*Ann. scient. Ec. Norm. Sup.*, 1972, pp. 217-240).

(Manuscrit reçu le 12 mai 1986,
révisé le 12 décembre 1986).

Eric M. FRIEDLANDER,
Department of Mathematics,
Northwestern University,
Evanston, IL 60201;

Brian J. PARSHALL,
Department of Mathematics,
University of Virginia,
Charlottesville, VA 22903.