Eric M. Friedlander
Brian J. Parshall

Rational actions associated to the adjoint representation


<http://www.numdam.org/item?id=ASENS_1987_4_20_2_215_0>
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 $U(\mathcal{G})$ of the Lie algebra $\mathcal{G}$ of a simple algebraic group $G$, by relating its structure to that of the symmetric algebra $S(\mathcal{G})$ on $\mathcal{G}$. We provide a similar analysis for the hyperalgebra $\text{hy}(G)$ 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 $\mathcal{G}$ in the natural way.

We prove the existence of a $G$-equivariant isomorphism of coalgebras $U(\mathcal{G}) \to S(\mathcal{G})$ 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 $0 \to U^{n-1} \to U^n \to S^s(\mathcal{G}) \to 0$ 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 $\mathcal{G}$.

Motivated by the main result of Section 1, we study in Sections 3 and 4 the invariants of $S(\mathcal{G})$ [and of $U(\mathcal{G})$] under the actions of the infinitesimal kernels $G_r \subset G$. For $r = 1$, Veldkamp [14] studied the invariants in $U(\mathcal{G})$, regarded as the center of $U(\mathcal{G})$. We adopt his methods and extend his results. We achieve this by considering the field of fractions of the $G_r$-invariants of $S(\mathcal{G})$ in Section 3. Our identification of $S(\mathcal{G})^{G_r}$ and $U(\mathcal{G})^{G_r}$ given in Section 4 has a form quite analogous to Veldkamp's description of the center of $U(\mathcal{G})$. 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 $U(\mathcal{G}) \to S(\mathcal{G})$ of $\mathcal{G}$-modules for an arbitrary restricted Lie algebra $\mathcal{G}$. 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 $\mathfrak{g}$ be a Lie algebra over a field $k$ with universal enveloping algebra $U(\mathfrak{g})$. Recall that $U(\mathfrak{g})$ has a natural (increasing) filtration $\{U^n\}$, where $U^n$ denotes the subspace of $U(\mathfrak{g})$ spanned by all products of at most $n$ elements of $\mathfrak{g}$. Also, $U(\mathfrak{g})$ carries the structure of a cocommutative Hopf algebra in which the elements of $\mathfrak{g}$ are primitive for the comultiplication $\Delta: U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$. Note that each $U^n$ is actually a subcoalgebra of $U(\mathfrak{g})$. The adjoint representation of $\mathfrak{g}$ extends to an action of $\mathfrak{g}$ on $U(\mathfrak{g})$ by derivations. If $\mathfrak{g}$ is the Lie algebra of a linear algebraic group $G$, then the adjoint action of $G$ on $\mathfrak{g}$ defines in an evident way a rational action of $G$ on $U(\mathfrak{g})$ 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 $n \geq 0$, we denote by $S^\leq n(V)$ the sum of the homogeneous components $S^i(V)$ of $S(V)$ with $i \leq n$. Note that $\{S^\leq n(V)\}$ is filtration of $S(V)$ by subcoalgebras.

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

1.1. Lemma. — There exists a coalgebra morphism

$$\varphi: U(\mathfrak{g}) \to S(U(\mathfrak{g}))$$

in which $\varphi|_\mathfrak{g}$ identifies with the natural inclusion of $\mathfrak{g} \subset U(\mathfrak{g})$ into $S^1(U(\mathfrak{g})) = U(\mathfrak{g})$ and

$$\varphi(x_1 \cdots x_n) \equiv \varphi(x_1) \cdots \varphi(x_n) \pmod{S^\leq n(U(\mathfrak{g}))}$$

for $x_1, \ldots, x_n \in \mathfrak{g}$. The morphism $\varphi$ is $\mathfrak{g}$-equivariant for the adjoint action of $\mathfrak{g}$ on $U(\mathfrak{g})$ and its extension (by derivations) to $S(U(\mathfrak{g}))$. Finally, $\varphi$ is $G$-equivariant if $\mathfrak{g} = \text{Lie}(G)$ 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 $\mathfrak{g}$, for $I = \{i_1 < \ldots < i_k\} \subset N = \{1, \ldots, n\}$ we set $x_I = x_{i_1} \cdots x_{i_k} \in U(\mathfrak{g})$. Consider the element

$$\psi(x) = \sum x_{I_1} \cdots x_{I_k} \in S(U(\mathfrak{g})),$$

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 $S(U(\mathfrak{g}))$. Thus, in $S(U(\mathfrak{g}))$, $x_{I_j}$ has homogeneous degree $\ell$, so that $x_{I_1} \cdots x_{I_k}$ has homogeneous degree $\ell$. In particular, the image of $\psi(x)$ in $S^\leq n(U(\mathfrak{g}))/S^\leq n-1(U(\mathfrak{g}))$ is $x_{(1)} \cdots \hat{x_{(n)}}$. Suppose $1 \leq j < n$ and $x_{j+1} x_j = x_j x_{j+1} + \xi$, for $\xi \in \mathfrak{g}$. 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 $I_j$). Using the surjective order preserving map $N \to N-1 = \{1, \ldots, n-1\}$ sending $j$ and $j+1$ to $j$ to identify $P$ with the set of partitions of $N-1$, we conclude the equalities

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

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

$$\varphi \otimes \varphi \Delta(x_1 \ldots x_n) = (\varphi \otimes \varphi)(\sum x_{I_1} \otimes x_{N \setminus I_1}) = \sum x_{I_1} \ldots x_{I_k} \otimes x_{I_1} \ldots x_{I_k},$$

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

$$\Delta(\varphi(x_1 \ldots x_n)) = \Delta(\sum x_{I_1} \ldots x_{I_k}).$$

whence it follows that $\varphi$ defines a coalgebra morphism. It is immediate, from its definition, that $\varphi$ has the required equivariance properties. \qed

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 $\mathcal{G}$ be a Lie algebra over a field $k$. There is a $\mathcal{G}$-equivariant, filtration preserving isomorphism of coalgebras

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

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

Proof. — If the isomorphism $\beta$ exists, it maps $\mathcal{G} \subset U(\mathcal{G})$ isomorphically to $\mathcal{G} = S^1(\mathcal{G})$ since $\mathcal{G}$ is the space of primitive elements contained in $S^1(\mathcal{G})$. It follows that $\mathcal{G} \subset U(\mathcal{G})$ splits for $\mathcal{G}$ (or $G$ if applicable). Conversely, assume that the inclusion $\mathcal{G} \subset U(\mathcal{G})$ splits for the action of $\mathcal{G}$ on $U(\mathcal{G})$. Thus, there exists an equivariant projection $p: U(\mathcal{G}) \to \mathcal{G}$ of $\mathcal{G}$-modules, which induces an equivariant morphism $S(p): S(U(\mathcal{G})) \to S(\mathcal{G})$ of Hopf algebras. It follows that if $\varphi$ is as in (1.1), then $\beta = S(p) \circ \varphi: U(\mathcal{G}) \to S(\mathcal{G})$ is an equivariant, filtration preserving morphism of coalgebras. By (1.1), $\beta$ induces an isomorphism $\text{gr}(\beta): U^n/U^{n-1} \to S^1(\mathcal{G})/S^1(\mathcal{G})$, so that $\beta$ 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 $\varphi(x_1 \ldots x_n) \equiv \varphi(x_1) \ldots \varphi(x_n) \pmod{S \cdot 1(\mathcal{G})}$ for $\varphi$ as in (1.1). \qed

Annales Scientifiques de l'École Normale Supérieure
We proceed to investigate circumstances under which an isomorphism $\beta$ in (1.2) exists. If $k$ has characteristic 0, the mapping $\eta: S(\mathcal{G}) \to U(\mathcal{G})$ defined by

$$\eta(x_1 \ldots x_n) = \frac{1}{n!} \sum_{\tau \in S(n)} x_{\tau(1)} \ldots x_{\tau(n)} \quad (x_1, \ldots, x_n \in \mathcal{G})$$

(where $\tau$ runs over permutations of $\{1, \ldots, n\}$) is clearly equivariant. By [2] (Ch. II, §1, No. 5, Proposition 9), $\eta$ 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 $\mathcal{G}$ is a restricted Lie algebra over $k$ with $p$-operator $x \mapsto x^{[p]}$, we denote its restricted enveloping algebra by $V(\mathcal{G})$. Thus, $V(\mathcal{G})$ is a finite dimensional Hopf algebra which is obtained from $U(\mathcal{G})$ by factoring out the ideal generated by elements of the form $x^{[p]} - x^p, \quad x \in \mathcal{G}$. The adjoint action of $\mathcal{G}$ defines an action by derivations of $\mathcal{G}$ on $V(\mathcal{G})$. Also, if $\mathcal{G}$ is the Lie algebra of a linear algebraic group $G$, the adjoint action of $G$ on $\mathcal{G}$ extends to a rational action of $G$ on $V(\mathcal{G})$ 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 $A_i$;

$p=2$ if $G$ is of type $B_p$, $C_p$, or $D_p$;

$p=2$ 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 $\mathcal{G} \subset V(\mathcal{G})$ 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 $\mathcal{G}$ 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 $\pi: k[G] \to \mathcal{G}^* \cong k[G]/(I^2 \oplus k)$ admits a $G$-equivariant section $s$. Let $G_1$ be the infinitesimal subgroup of $G$ of height $\leq 1$ with $Lie(G_1) = \mathcal{G}$ ([5], II, §7, No. 4.3). If $\sigma: k[G] \to k[G_1]$ is the restriction map on coordinate rings, the quotient map $\pi_1: k[G_1] \to \mathcal{G}^*$ admits $\sigma \circ s$ as a $G$-equivariant section. Moreover, in the identification of the dual Hopf algebra $k[G_1]^*$ with $V(\mathcal{G})$ ([5], II, §7, No. 4.2), the dual mapping $\pi_1^*$ identifies with the natural inclusion $\mathcal{G} \subset V(\mathcal{G})$. This establishes the lemma. \hfill $\square$

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 $A_1$ and $p$ is good for $G$; (iii) $G$ is of type $A_1$ and $p$ does not divide $l + 1$. Then there is a $G$-equivariant, filtration preserving isomorphism

$$\beta: U(\mathcal{G}) \to S(\mathcal{G})$$
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 $\mathfrak{sl}_2$ be the central extension of $\mathfrak{sl}^\mathfrak{g}$ with basis $e, h, f, z$ satisfying 
\[[e, f] = h, \quad [h, e] = 2e, \quad [h, f] = -2f, \quad [g, z] = 0.\]
We make $\mathcal{G}$ into a restricted Lie algebra by defining $e^{[p]} = z, \quad h^{[p]} = h, \quad f^{[p]} = 0, \quad z^{[p]} = 0$. Assume that $p > 3$, and put $w = e^{p-3}h^3 \in V(\mathcal{G})$. Then $w \notin \mathcal{G}$ and $(ad e)^3 w = -48z$. Since $(ad e)^3 \mathcal{G} = 0$, 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 $(ad e)^3 w_1 = (ad e)^3 w$ 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 $\mathcal{G} = \mathfrak{sl}_2$, a similar example can be given replacing $w$ by $ef$ and $(ad e)^3$ by $(ad f) (ad e)$. Note in this case that the monomials $e^a h^b f^c$ of degree $> 1$ in $U(\mathcal{G})$ span an $(ad (\mathcal{G}))$-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 $F_p$. For $r \geq 1$, $G_r$ 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 $h(y)(G_r)$ 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 $h(y)(G_r) \subset h(y)(G_{r+1})$, and the hyperalgebra of $G$ is realized as the limit

$$h(y)(G) = \lim_{\to} h(y)(G_r).$$

As such, $h(y)(G)$ 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 $h(y)(G_r)$ and hence on $h(y)(G)$ by Hopf algebra automorphisms.

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

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

\[
x_1^{a_1} x_2^{a_2} / a_1! \cdots x_r^{a_r} / a_r! \left(\begin{array}{c} h_1 \\ b_1 \end{array}\right) \cdots \left(\begin{array}{c} h_i \\ b_i \end{array}\right) x_1^{c_1} / c_1! \cdots x_r^{c_r} / c_r!
\]

(usual notation, cf. [3; 5.1]). Observe that \(h(G)\) is graded by setting \(h^m(G)\) 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 \(\{h_i^\leq s(G)\}\) of \(h(G)\) by subcoalgebras, stable under the action of \(G\) on \(h(G)\). 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, \(h(\mathcal{G})\) denotes the hyperalgebra of \(\mathcal{G}\) regarded as a vector group defined over \(\mathbf{F}_p\). For simplicity we omit the case of \(GL_d\); 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 \(A_i\) then \(p\) does not divide \(i+1\). Then there exists a \(G\)-equivariant, filtration preserving isomorphism of coalgebras

\[
\beta : h(G) \to h(\mathcal{G})
\]

with the property that the induced map \(\text{gr}(\beta) : \text{gr}(h(G)) \to h(\mathcal{G})\) is a \(G\)-isomorphism of Hopf algebras. Moreover, for each \(r \geq 1\), \(\beta\) restricts to a \(G\)-equivariant, filtration preserving isomorphism of coalgebras

\[
\beta_r : h(G_r) \to h(\mathcal{G}_r)
\]

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

Proof. — As noted in the proof of (1.3), the natural quotient map \(k[G] \to \mathcal{G}^*\) admits a \(G\)-equivariant section \(\mathcal{G}^* \to k[G]\). Composing this map with the restriction homomorphism \(k[G] \to k[G_r]\) provides a \(G\)-equivariant section \(s_r : \mathcal{G}^* \to k[G_r]\) to the quotient map \(k[G_r] \to \mathcal{G}^*\). Since \(k[G_r]\) identifies with a truncated polynomial algebra \(k[T_1, \ldots, T_d]/(T_1^{p_1}, \ldots, T_d^{p_d}), d = \dim G\), by [3] (§9.1), [5] (III, §3, No. 6.4), it follows that \(s_r\) identifies \(k[G_r]\) \(G\)-equivariantly with \(S(\mathcal{G}^*)/\mathcal{G}^{*p'_d}\) as commutative algebras. Taking
duals, we obtain the desired $G$-equivariant isomorphism $\beta_r : \text{hy}(G_r) \to \text{hy}(\mathcal{G}_r)$ of coalgebras. Because the $s_r$ are by construction compatible, it follows that the $\beta_r$, define a $G$-equivariant isomorphism $\beta : \text{hy}(G) \to \text{hy}(\mathcal{G})$ of coalgebras. Furthermore, using the usual basis of $\text{hy}(G)$ we easily see that $\text{gr}(\beta)$ is an isomorphism of Hopf algebras. □

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

3. Fraction fields and their invariants

Let $G$ be a linear algebraic group defined over $F_p$, as in Section 2 above. In this section, we investigate the invariants of the field of fractions of $S(\mathcal{G})$ 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 $\rho : G \to \text{GL}(V)$ be a finite dimensional rational $F_p$-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 $V(F_r)$, 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 $x \in G_r(R)$, 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 $\rho(G_r(R)) (A^+ \otimes 1)$, 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 $\mathcal{G}$ 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 $F_p$ and let $\rho : G \to \text{GL}(V)$ be a finite dimensional rational $F_p$-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 $\mathfrak{g}$ is non-degenerate, and we thereby identify $\mathfrak{g} \cong \mathfrak{g}^*$ as rational $G$-modules. Let $\mathcal{H} = \text{Lie}(T) \subset \mathfrak{g} = \text{Lie}(G)$ be the Lie algebra of a maximal split torus $T$ of $G$. Then $S(\mathfrak{g}^G_r) \cong S(\mathcal{H}^W) [13]$ is isomorphic to a polynomial ring $J$ on homogeneous generators $T_1, \ldots, T_l$ ($l = \text{rank } G$) 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 $S(\mathfrak{g})$. 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 $\mathfrak{g}$ and let $C$ be the $n \times n$ $K$-matrix $(a_{ij})$, where $a_{ij} = [X_i, X_j] \in K$. Then $\text{rank}(C) \leq \dim G/T = n - 1$.

Proof. — Let $\Phi$ be the root system of $T$ in $\mathfrak{g}$, and for $\alpha \in \Phi$, let $e_\alpha$ be a nonzero root vector of weight $\alpha$. Since the rank of $C$ is independent of the choice of basis for $\mathfrak{g}$, 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 $\tau: S(\mathfrak{g}) \to S(\mathcal{H})$ be the algebra homomorphism defined by $\tau(e_\alpha) = 0$ for all $\alpha \in \Phi$ and $\tau(h) = h$ for all $h \in \mathcal{H}$. Since $G$ is simply connected, each $[e_\alpha, e_\beta], \alpha \in \Phi$, is a nonzero element of $\mathcal{H}$. 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 $S(\mathfrak{g}^{(r)}) \otimes_{J^G_{r-1}} J \to S(\mathfrak{g})^{G_r}$ is an injection and induces an isomorphism on associated fields of fractions

\[ \frac{\text{frac}(S(\mathfrak{g}^{(r)}) \otimes_{J^G_{r-1}} J)}{K_r} \cong K_r. \]

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

Proof. — We first assert that the monomials $T_{i_1} \cdots T_{i_l}, 0 \leq a_i < p^r$, in $S(\mathfrak{g})$ are linearly independent over $S(\mathfrak{g})$. Fix a basis $\{X_i\}$ of $\mathfrak{g}$. We recall from [14] (7.1) that the Jacobian matrix $(\partial T_{i_j}/\partial X_{i_j})$ has rank $l$ at $\varphi \in \mathcal{H}^* \cong \mathfrak{g}$ if and only if $\varphi$ is regular. Since the regular elements of $\mathfrak{g}$ form an open dense subset, $(\partial T_{i_j}/\partial X_{i_j})$ 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 $S(\mathfrak{g}^{(r)}) \otimes_{J^{(r-1)}} J \to S(\mathfrak{g})^{G_r}$ is injective, and we let $K_r \subset K_r$ be the field of fractions of the image domain. Since $J$ is a free $J^{(r)}$-module of rank $p^r$, we conclude that $K_r$ is a subfield of $K_r$ which is an extension of degree $p^r$ over $K^{G_r}$. Hence, $[K:K_r] = p^r(a^m - 1)$. To prove the inclusion $K_r \subset K_r$ is actually an equality, it suffices to prove that $[K:K_r] \geq p^{r-1}$ for each $s, 0 \leq s < r$ (with $K_0 = K$).
By Proposition 3.1, $K_{s+1} = K_{s+1}^G$. Identifying $G_{s+1}/G_s$ with $G_s$, and the $G_{s+1}/G_s$-module $K_s$ with the corresponding “untwisted” $G_s$-module $K_s^{(-s)}[3](3.3)$, we obtain that $K_{s+1} \cong (K_s^{(-s)})^G = (K_s^{(-s)})^G$. Thus, the Jacobson-Bourbaki theorem ([10], Theorem 19, p. 186) implies that $[K_s : K_{s+1}] = p^{[\mathcal{G}_s : K_s^{(-s)}]}$ where $\mathcal{G}_s$ denotes the $K_s^{(-s)}$-span of the image of $\mathcal{G}$ in the derivation algebra $\text{Der}(K)$. For $X, Y \in \mathcal{G}$, the derivation of $K_s^{(-s)}$ defined by $X$ maps $(Y^{(s)})^{(-s)} \in K_s^{(-s)}$ to $([X, Y])^{(-s)}$. Thus, $[\mathcal{G} : K_s^{(-s)}]$ equals at least the rank of the matrix $C$ of (3.2). Thus, by (3.2), $[K_s : K_{s+1}] \geq p^{s-1}$ 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 $K \mathcal{G}$ is the $K$-span of the image of $\mathcal{G}$ in the derivation algebra $\text{Der}(K)$, then $K \mathcal{G}$ 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 $p^{(n-r)}$ over $K_r = K^G_r$, whereas $K_s$ is purely inseparable of dimension $p^s$ over $\text{frac}(S(\mathcal{G}^{(r)})) = K_s^F$. □

It is amusing to observe that the extension analogous to $K_1/K^F$ in the context of $U(\mathcal{G})$ is separable. Namely, the field of fractions of the center of $U(\mathcal{G})$ [which we may view as $U(\mathcal{G})^G$ to preserve the analogy with $S(\mathcal{G})$] is separable over the field of fractions of the central subalgebra $\mathcal{Q} \cong S(\mathcal{G}^{(1)})$ [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 $F_p$ the $G_r$-invariants of $S(\mathcal{G})$ in terms of $S(\mathcal{G}^{(r)}) = S(\mathcal{G})^F$ and the polynomial subalgebra $J = S(\mathcal{G}^G) \subset S(\mathcal{G})$. We then use this result to provide a corresponding identification of the $G_r$-invariants of $U(\mathcal{G})$, thereby extending Veldkamp’s determination of the center of $U(\mathcal{G})$ [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 $S(\mathcal{G})$.

(4.1) THEOREM. — Let $G$ be a simple algebraic group defined and split over $F_p$ 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

$$S(\mathcal{G}^{(r)}) \otimes_{\mathcal{G}^r} J \cong S(\mathcal{G})^G,$$

of rational $G$-algebras.

Proof. — For notational convenience, let $A_r = S(\mathcal{G}^{(r)}) \otimes_{\mathcal{G}^r} J$ and let $A_r = S(\mathcal{G})^G$. 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

$$ k[T_1, \ldots, T_r] \to k[T_1, \ldots, T_r][x_{1}', \ldots, x_{r}']/(T_r' - t_r(x_{1}', \ldots, x_{r}'), 1 \leq i \leq l). $$

The Jacobian matrix $(\partial t_i/\partial x_j)$ has rank $l$ at an element $\varphi$ of $\mathfrak{g}^*$ (naturally homeomorphic to the maximal ideal space of $A'_r$) if and only if $\varphi \in \mathfrak{g}^*$ (isomorphic 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 $\mathfrak{g}$ with $\mathfrak{g}^*$ 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

$$ \mathfrak{g}/G_r \cong (\mathfrak{g}^{(1)})^G \times (\mathfrak{g}/G)^G. $$

Because the isomorphism $U(\mathfrak{g}) \cong S(\mathfrak{g})$ of Section 1 is not multiplicative, a description of $U(\mathfrak{g})^{G_r}$ analogous to that of $S(\mathfrak{g})^{G_r}$ in Theorem 4.1 requires a little effort. We recall the central $G$-subalgebra $\mathcal{O} \subset U(\mathfrak{g})$ given as the (isomorphic) image of the $G$-algebra map $S(\mathfrak{g}^{(1)}) \to U(\mathfrak{g})$ sending $X \in \mathfrak{g}^{(1)}$ to $X^2 - X^{[2]} \in U(\mathfrak{g})$. We define $\mathcal{O}'$ to be

$$ \mathcal{O}' = S(\text{span}\{ e_{\alpha}', (h_p^\alpha - h_p)\alpha^{-1}; \alpha \in \Phi, \beta \in \Pi \}). $$

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

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

$$ \mathcal{O}', [s_1, \ldots, s_l] \to U(\mathfrak{g})^{G_r}, \quad s_i \to S_i $$

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

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

We conclude by investigating one aspect of the $G$-extensions occuring in $S(\mathfrak{g})$. 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 $\lambda$, denote by $I(\lambda)$ the rational $G$-module obtained by inducing to $G$ the one-dimensional rational $B$-module defined by the character $w_0(\lambda)$. 

4e série — tome 20 — 1987 — n° 2
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 $\mathbb{F}_p$ 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) $\mathrm{hy}(G)$ does not have a good filtration.

In particular, $U(\mathcal{G})$ is not isomorphic to $\mathrm{hy}(G)$ 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 $\mathrm{hy}(\mathcal{G})$ does not have a good filtration. We assert that the component $\mathrm{hy}^p(\mathcal{G})$ does not admit a good filtration. First, observe that if $\nu$ is the maximal root in the root system $\Phi$ of $G$, then $p \nu$ is the maximal dominant weight in $\mathrm{hy}^p(\mathcal{G})$, so that if $\mathrm{hy}^p(\mathcal{G})$ admits a good filtration, there exists a surjective $G$-module homomorphism $\mathrm{hy}^p(\mathcal{G}) \to I(p \nu)$ [6]. On the other hand, the subspace $V$ of $\mathrm{hy}^p(\mathcal{G})$ spanned by those monomials $x_1^{a_1} \ldots x_n^{a_n}$ with $0 \leq a_i < p$ is clearly $G$-stable and $\mathrm{hy}^p(\mathcal{G})/V \cong \mathcal{G}^{(1)}$ (1). It follows from universal mapping that if there exists a surjective $G$-module homomorphism $\mathrm{hy}^p(\mathcal{G}) \to I(p \nu)$, 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 $(M^G)^{(-r)}$ 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: $I(p' \lambda)^G \cong I(\lambda)^G$, whereas $I(\mu)^G = 0$ if $\mu \neq p' \lambda$ for some dominant weight $\lambda$.

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

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

REFERENCES


ANNALES SCIENTIFIQUES DE L'ÉCOLE NORMALE SUPÉRIEURE

(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.