ALGEBRAIC GROUPS AND HOPF ALGEBRAS

BY

G. HOCHSCHILD

1. Introduction

We consider affine algebraic groups over a fixed algebraically closed base field of characteristic 0. The totality of all polynomial functions on such a group is the underlying set of a Hopf algebra over the base field, and the group is recoverable from this Hopf algebra structure. Similarly, a Hopf algebra is attached to a Lie algebra. The elements of this Hopf algebra are the representative functions on the universal enveloping algebra of the Lie algebra.

The main theme of this paper is the comparison of the Hopf algebra of an algebraic group with the Hopf algebra of its Lie algebra. Within the theory of algebraic groups, this theme is very closely tied to that of group coverings. In particular, we shall exhibit the use of Hopf algebras in constructing universal coverings in the category of affine algebraic groups. An affine algebraic group has such a universal covering if and only if its radical is unipotent. Our procedure also yields a direct description of the "simply connected" affine algebraic group belonging to a given Lie algebra L such that $L = [L, L]$ in terms of the universal enveloping algebra of L.

I wish to thank Calvin Moore for his helpful comments and suggestions both, in direct conversation, and in Chapter I of his forthcoming paper [8].

2. Algebraic group coverings

Let F be an algebraically closed field of characteristic 0, and let G and H be connected affine algebraic groups over F. Suppose that $\eta : H \to G$ is a surjective rational group homomorphism with finite kernel. Then we say that (H, η) is a *group covering* of G. We call G *simply connected* if every group covering of G is an isomorphism.

LEMMA 2.1. *Suppose that G is simply connected, and that K is a connected normal algebraic subgroup of G. Then G/K is simply connected.*

Proof. Let γ denote the canonical epimorphism $G \to G/K$, and consider a group covering $\eta : H \to G/K$. We must show that the kernel, A say, of η is trivial. Let us form the fibered product $P = H \times_{(\eta,\gamma)} G$, i.e., the algebraic subgroup of $H \times G$ consisting of all elements (h, g) such that $\eta(h) = \gamma(g)$. Clearly, K may be identified with a normal algebraic subgroup of P, and P/K is isomorphic with H. Since H and K are connected, it follows that P is connected. Now consider the canonical projection epimorphism $\rho : P \to G$. The kernel of ρ evidently coincides with the canonical isomorphic image of A

Received January 9, 1968.

in P, and (P, ρ) is a group covering of G. Since G is simply connected, the kernel of ρ must be trivial, so that A must be trivial.

LEMMA 2.2. *If G is simply connected then the radical of G is unipotent.*

Proof. Here, an affine algebraic group is called unipotent if every finite-dimensional rational representation sends it onto a unipotent group of linear automorphisms. This will be the case provided only that there is some faithful finite-dimensional rational representation of the group by unipotent linear automorphisms. Now let R denote the radical of G, i.e., the maximum connected solvable normal algebraic subgroup. This contains the *unipotent radical* N, i.e., the maximum unipotent normal algebraic subgroup. We have the standard semidirect product decomposition $G = N \cdot P$, where P is a fully reducible connected algebraic subgroup of G [9, Th. 7.1]. Here, an affine algebraic group is called fully reducible if every rational representation of it is semisimple. This will be so provided only that the group has some faithful finite-dimensional semisimple rational representation.

By considering the Lie algebra of P and using the well-known structure theorem of Jacobson for fully reducible Lie algebras of linear endomorphisms, one sees that the commutator subgroup $[P, P]$ of P is semisimple, and that $P = [P, P]Q$, where Q is the connected component of the identity in the center of P. Clearly, $[P, P] \cap Q$ is zero-dimensional, and thus a finite central subgroup T of P. Moreover, Q is a fully reducible connected algebraic group, and therefore is an algebraic toroid, i.e., a direct product of copies of the multiplicative group of our base field F [1, Prop. 7.4 & Remark 7.5(2)]. Since G is simply connected and P is isomorphic with G/N, it follows from Lemma 2.1 that P is simply connected. On the other hand, it is clear from the above that P is isomorphic with the factor group of $[P, P] \times Q$ mod a finite central subgroup that is isomorphic with T. Hence we may conclude that T must actually be trivial, so that P is isomorphic with $[P, P] \times Q$. Now Q is isomorphic with $P/[P, P]$ and hence, by Lemma 2.1, is simply connected. Being an algebraic toroid, it must therefore be trivial. Thus $P = [P, P]$ and is therefore semisimple. Since $G = N \cdot P$, it follows that $R = N$, so that Lemma 2.2 is proved.

The following theorem reduces the consideration of simple connectedness to the case of semisimple groups.

THEOREM 2.3. *Let G be a connected affine algebraic group over the algebraically closed field F of characteristic 0. Let R denote the radical of G. Then G is simply connected if and only if R is unipotent and G/R is simply connected.*

Proof. The necessity of the conditions has already been established by Lemmas 2.2 and 2.1. Now suppose that the conditions are satisfied. Let $\eta : H \rightarrow G$ be a group covering, and let K denote the finite kernel of η. Let R^* denote the connected component of the identity in $\eta^{-1}(R)$. Then R^* is a normal connected algebraic subgroup of H, and η induces a rational surjective group homomorphism η' of H/R^* onto G/R. The kernel of η' is the finite group $(KR^*)/R^*$. Since G/R is simply connected, this kernel must therefore be trivial, so that $K \subset R^*$. Now the restriction of η to R^* is a group covering of R with kernel K. We have a semidirect product decomposition $R^* = N \cdot P$, where N is unipotent and P is fully reducible. Since the image of a fully reducible group by a rational homomorphism is fully reducible and since the unipotent group R has no non-trivial fully reducible subgroup, we have $P \subset K$. But P is connected, and K is finite. Hence P must be trivial, so that R^* is unipotent. Therefore, R^* has no non-trivial finite subgroup. Hence K must be trivial, and Theorem 2.3 is proved.

THEOREM 2.4. *Let P be a connected normal algebraic subgroup of the simply connected affine algebraic group G. Then P is simply connected.*

Proof. Let R denote the radical of G. Then $P \cap R$ is a normal algebraic subgroup of P, and $P/(P \cap R)$ may be identified with the corresponding connected normal algebraic subgroup of the semisimple group G/R. The Lie algebra of $P/(P \cap R)$ is an ideal of the semisimple Lie algebra of G/R. Hence it is semisimple and a direct summand of the Lie algebra of G/R. As in the proof of Lemma 2.2, it follows that there is a connected normal algebraic subgroup Q of G/R such that G/R is isomorphic with the factor group of $(P/(P \cap R)) \times Q$ mod a finite central subgroup T. Since G/R is simply connected, T must be trivial, so that G/R is isomorphic with $(P/(P \cap R)) \times Q$. Hence $P/(P \cap R)$ is isomorphic with a factor group of G/R mod a connected normal algebraic subgroup (isomorphic with Q). By Lemma 2.1, $P/(P \cap R)$ is therefore simply connected. By Lemma 2.2, R is unipotent, whence also $P \cap R$ is unipotent. Since $P/(P \cap R)$ is semisimple, $P \cap R$ is therefore the radical of P, and we have from Theorem 2.3 that P is simply connected. This completes the proof of Theorem 2.4.

Note that the condition of normality in Theorem 2.4 is not superfluous. For example, if $\mathbf{C}$ is the field of complex numbers, the subgroup $SO(3, \mathbf{C})$ of $SL(3, \mathbf{C})$ is *not* simply connected, although $SL(3, \mathbf{C})$ *is* simply connected.

By a *universal group covering* of the connected affine algebraic group G we mean a group covering $\gamma : G^* \to G$ with the property that, for every group covering $\eta : H \to G$, there is one and only one group covering $\eta^* : G^* \to H$ such that $\eta \circ \eta^* = \gamma$. This is easily seen to simply that G^* is simply connected, and it is clear from Theorem 2.3 that G can have a universal group covering only if its radical is unipotent. We shall prove that, if the radical of G is unipotent, then a universal group covering for G actually exists, and we shall construct it explicitly from the Lie algebra of G. In order to do this, we must first discuss the Hopf algebra structures that are associated with groups and Lie algebras.

3. Hopf algebras

Throughout, we shall consider groups, associative algebras, and Lie algebras over the fixed algebraically closed base field F of characteristic 0.

All associative algebras will have identity elements, and all algebra homomorphisms will send identity elements onto identity elements.

By an *affine Hopf algebra* over F we shall mean the following structure. There is given a finitely generated F-algebra H that is an integral domain. Thus, in the usual terminology, H is an affine F-algebra. We denote by $\mu : F \to H$ the canonical injection, i.e., the *unit* of the F-algebra H. There is also given a *counit* $c : H \to F$, i.e., an algebra homomorphism of H onto F, so that $c \circ u$ is the identity map on F. Furthermore, H is endowed with a comultiplication $\gamma : H \to H \otimes H$, which is assumed to be an algebra homomorphism and to be coassociative, in the sense that $(i \otimes \gamma) \circ \gamma = (\gamma \otimes i) \circ \gamma$ where i stands for the identity map on H. Finally, it is assumed that $(c \otimes i) \circ \gamma = i = (i \otimes c) \circ \gamma$. Here, if $\mu : H \otimes H \to H$ denotes the algebra multiplication of H, we identify $F \otimes H$ and $H \otimes F$ with H, via $\mu \circ (u \otimes i)$ and $\mu \circ (i \otimes u)$, respectively.

The general notion of a Hopf algebra is obtained from the above by allowing H to be an arbitrary F-algebra. Our notation is that of [7, II.3], which may be consulted for more details on the formalism we use here, in the case where H is commutative. A *symmetry* of a Hopf algebra H is a linear endomorphism η of H such that $\mu \circ (\eta \otimes i) \circ \gamma = u \circ c = \mu \circ (i \otimes \eta) \circ \gamma$. In all the cases we shall meet here, the symmetries are actually algebra anti-automorphisms. If α and β are algebra homomorphisms $H \to F$ then one defines their product $\alpha\beta$ by $\alpha\beta = (\alpha \otimes \beta) \circ \gamma$. This multiplication of homomorphisms is associative, and has c as a neutral element. If there is a symmetry η, then this is actually a group multiplication; the inverse of the homomorphism α is given by $\alpha^{-1} = \alpha \circ \eta$. Thus, if H is a Hopf algebra with symmetry, then the algebra homomorphisms $H \to F$ constitute a group, which we denote by $\mathbf{G}(H)$.

Now let G be a connected affine algebraic group over F. Then G determines an affine Hopf algebra $\mathbf{H}(G)$ over F as follows. As an F-algebra, $\mathbf{H}(G)$ is the algebra of all polynomial functions of the algebraic variety structure of G. The counit c is the evaluation $f \to f(1)$ at the neutral element 1 of G. The comultiplication γ is given by identifying $\mathbf{H}(G) \otimes \mathbf{H}(G)$ with $\mathbf{H}(G \times G)$ and putting $\gamma(f)(x, y) = f(xy)$. This Hopf algebra has a symmetry η, where $\eta(f)(x) = f(x^{-1})$. It is immediate from the definition of affine algebraic group over F (as given, for example, in [1, I.2], or in [2, Ch. II]) that the map that associates with each element x of G the evaluation x° at x, is an isomorphism of G onto $\mathbf{G}(\mathbf{H}(G))$. Conversely, if H is any affine Hopf algebra with symmetry over F then the group $\mathbf{G}(H)$, as defined above, is a connected affine algebraic group, with H as the algebra of all polynomial functions. Thus, the Hopf algebra $\mathbf{H}(\mathbf{G}(H))$ may be identified with the given Hopf algebra H.

The Lie Algebra of the group $\mathbf{G}(H)$ may be identified with the Lie algebra of all *differentiations* $H \to F$, by which we mean the F-linear maps $\delta : H \to F$ such that $\delta(fg) = c(f)\delta(g) + \delta(f)c(g)$ for all f and g in H. The Lie product $[\sigma, \tau]$ of two such differentiations is given by $[\sigma, \tau] = (\sigma \otimes \tau - \tau \otimes \sigma) \circ \gamma$.

We shall say that a linear endomorphism σ of H is *proper* if $\gamma \circ \sigma =$

$(i \otimes \sigma) \circ \gamma$. One verifies directly that the maps $\sigma \to c \circ \sigma$ and $\delta \to (i \otimes \delta) \circ \gamma$ are mutually inverse linear isomorphisms between the space dual to H and the space of all proper linear endomorphisms of H. In particular, the Lie algebra of $\mathbf{G}(H)$ may therefore be viewed also as the Lie algebra of all proper derivations of H, and the group $\mathbf{G}(H)$ may be identified with the group of all proper algebra automorphisms of H. If H is viewed as the function algebra $\mathbf{H}(\mathbf{G}(H))$, then the proper linear endomorphisms of H are precisely those linear endomorphisms which commute with the right translations $f \to f \cdot x$, where $(f \cdot x)(y) = f(xy)$, that are effected by the elements x of G. The verification of this fact is straightforward. In particular, $\mathbf{G}(H)$ thus becomes the group of all left translations $f \to x \cdot f$, where $(x \cdot f)(y) = f(yx)$, and the Lie algebra of $\mathbf{G}(H)$ appears as the Lie algebra of all those derivations of H that commute with every right translation.

Now let L be a finite-dimensional Lie algebra over F. Denote the universal enveloping algebra of L by $\mathbf{U}(L)$. We recall that $\mathbf{U}(L)$ is a (non-commutative) Hopf algebra, the comultiplication, d say, being the algebra homomorphism $\mathbf{U}(L) \to \mathbf{U}(L) \otimes \mathbf{U}(L)$ that extends the map $x \to x \otimes 1 + 1 \otimes x$ of L into $\mathbf{U}(L) \otimes \mathbf{U}(L)$. A linear functional f on $\mathbf{U}(L)$ is called a *representative function* if it annihilates some two-sided ideal of finite codimension in $\mathbf{U}(L)$. The comultiplication d on $\mathbf{U}(L)$ dualizes to a commutative and associative multiplication of representative functions, with which the space $\mathbf{U}(L)$ of all representative functions becomes an integral domain (for this, see [4, Section 2], for example). Moreover, $\mathbf{H}(L)$ has a coalgebra structure

$$\gamma : \mathbf{H}(L) \to \mathbf{H}(L) \otimes \mathbf{H}(L),$$

with which it becomes a Hopf algebra. The comultiplication γ is characterized by $\gamma(f)(x \otimes y) = f(xy)$, where we identify $\mathbf{H}(L) \otimes \mathbf{H}(L)$ with the corresponding algebra of linear functionals on $\mathbf{U}(L) \otimes \mathbf{U}(L) = \mathbf{U}(L \oplus L)$. It is easy to see that this actually identifies $\mathbf{H}(L) \otimes \mathbf{H}(L)$ with $\mathbf{H}(L \oplus L)$.

Let σ denote the algebra anti-automorphism of $\mathbf{U}(L)$ that extends the map $x \to -x$ of L into $\mathbf{U}(L)$. Then σ is a symmetry of the Hopf algebra $\mathbf{U}(L)$, and its dual η is a symmetry of the Hopf algebra $\mathbf{H}(L)$.

Now suppose that the radical, A say, of L is nilpotent. An element f of $\mathbf{H}(L)$ is called *basic* if it annihilates some power of the ideal generated by A. The basic representative functions are precisely the functions associated with those finite-dimensional representations of L whose restrictions to A are nilpotent. These functions make up a Hopf sub-algebra $\mathbf{B}(L)$ of $\mathbf{H}(L)$. It is known that $\mathbf{B}(L)$ is a finitely generated F-algebra [4, Sections 5–7], so that, with the restriction of γ as the comultiplication, it constitutes an affine Hopf algebra. Moreover, $\mathbf{B}(L)$ is stable under the symmetry η of $\mathbf{H}(L)$, so that it is a Hopf algebra with symmetry. We call $\mathbf{B}(L)$ the *canonical basic subalgebra* of $\mathbf{H}(L)$. By [4, Th. 7], we have $\mathbf{H}(L) = C \otimes \mathbf{B}(L)$, where C is the algebra of the *trigonometric functions*, in the sense of [4]; these are the representative functions associated with the semisimple finite-dimensional representations of $L/[L, L]$. *In particular,* $\mathbf{B}(L) = \mathbf{H}(L)$ *if and only if* $L = [L, L]$.

We shall write $\mathbf{G}(L)$ for $\mathbf{G}(\mathbf{B}(L))$. By what we have seen above, $\mathbf{G}(L)$ is a connected affine algebraic group whose algebra of polynomial functions may be identified with $\mathbf{B}(L)$, and whose Lie algebra may be identified with the Lie algebra of all proper derivations of $\mathbf{B}(L)$.

THEOREM 3.1. *Let L be a finite-dimensional Lie algebra over F whose radical is nilpotent. Then the group $\mathbf{G}(L)$ is simply connected, and its Lie algebra may be identified with L. Moreover, if G is a connected affine algebraic group over F with unipotent radical, and if σ is a surjective homomorphism of L onto the Lie algebra of G, then there is a rational group homomorphism $\sigma^+ : \mathbf{G}(L) \to G$ whose differential coincides with σ.*

Proof. Since the radical of L is nilpotent, L is an algebraic Lie algebra, and the map that sends each element x of L onto the left translation effected by x on $\mathbf{B}(L)$ is an isomorphism of L onto the Lie algebra of all proper derivations of $\mathbf{B}(L)$ (see the end of [4]). Hence the Lie algebra of $\mathbf{G}(L)$ may be identified with L. Since the action of the radical of L by left translations on $\mathbf{B}(L)$ is locally nilpotent, it follows that the action of the radical of $\mathbf{G}(L)$ by proper automorphisms on $\mathbf{B}(L)$ is locally unipotent. Hence it is clear that the radical of $\mathbf{G}(L)$ is unipotent.

Now let G be a connected affine algebraic group over F with unipotent radical, and let G° denote the Lie algebra of G. Suppose that σ is a surjective Lie algebra homomorphism of L onto G°. Let us view G° as the Lie algebra of all proper derivations of $\mathbf{H}(G)$. Then σ extends uniquely to an algebra homomorphism of $\mathbf{U}(L)$ into the algebra of all proper linear endomorphisms of $\mathbf{H}(G)$. Let us denote this extension of σ by the same letter σ. Now we define a map σ^* of $\mathbf{H}(G)$ into $\mathbf{H}(L)$ by putting $\sigma^*(f)(a) = \sigma(a)(f)(1)$ for every element f of $\mathbf{H}(G)$ and every element a of $\mathbf{U}(L)$. The standard formal facts concerning rational representations and their differentials (see [2] and [3]) show that σ^* is a homomorphism of Hopf algebras.

The restriction of σ to the radical of L is a surjective Lie algebra homomorphism of the radical of L onto that of G°. Since the radical of G is unipotent, the action of the radical of G° by proper derivations on $\mathbf{H}(G)$ is locally nilpotent. One sees immediately from this that σ^* sends $\mathbf{H}(G)$ into the Hopf subalgebra $\mathbf{B}(L)$ of $\mathbf{H}(L)$. Hence, by dualization, σ^* defines a group homomorphism $\sigma^+ : \mathbf{G}(L) \to \mathbf{G}(\mathbf{H}(G)) = G$. It is clear from the definition that σ^+ is a rational homomorphism, and that its differential coincides with σ. This proves the second part of Theorem 3.1. If this result is applied to a group covering $\rho : G \to \mathbf{G}(L)$, it shows that ρ is necessarily an isomorphism. Hence $\mathbf{G}(L)$ is simply connected, and the proof of Theorem 3.1 is complete.

Note that Theorem 3.1 implies that every simply connected affine algebraic group whose Lie algebra is isomorphic with L is, itself, isomorphic with $\mathbf{G}(L)$.

It follows that simply connected groups have the expected lifting property for rational homomorphisms, as expressed in the following corollary.

COROLLARY 3.2. *Let $\eta : H \to G$ be a group covering. Let T be a simply connected affine algebraic group, and let τ be a rational homomorphism of T into G. Then there is one and only one rational homomorphism $\tau^\eta : T \to H$ such that $\eta \circ \tau^\eta = \tau$.*

Proof. By Theorem 3.1, we may identify T with $\mathbf{G}(T^\circ)$. The image $\tau(T)$ is a connected algebraic subgroup of G, and there is evidently a connected algebraic subgroup K of H such that the restriction of η to K is a group covering $K \to \tau(T)$. Hence we may suppose that τ is surjective which implies that the radical of G, and hence that of H, is unipotent. Now the differential η° of η is a Lie algebra isomorphism $H^\circ \to G^\circ$, and $(\eta^\circ)^{-1} \circ \tau^\circ$ is a surjective Lie algebra homomorphism $T^\circ \to H^\circ$. Hence we may apply Theorem 3.1 to conclude that there is a rational group homomorphism $\tau^\eta : \mathbf{G}(T^\circ) \to H$ whose differential is $(\eta^\circ)^{-1} \circ \tau^\circ$. It follows that $\eta \circ \tau^\eta = \tau$. This, and the uniqueness of τ^η, are clear from the fact that a rational homomorphism of connected algebraic groups over a field of characteristic 0 is determined by its differential.

4. The affine algebra of a simply connected group

If B is a commutative ring and A is a subring of B then we shall say that B is *unramified* over A if, for every B-module M, the only A-linear derivation of B into M is the zero map. If, moreover, A and B are affine F-algebras (i.e., integral domains that are finitely generated as F-algebras), and B is finitely generated as an A-module, then we call B an *affine unramified extension* of A.

Let $\eta : H \to G$ be a group covering of connected affine algebraic groups over F. Then it is easy to see that $\mathbf{H}(H)$ is an affine unramified extension of $\mathbf{H}(G)$. The proof of this is contained in the proof of [6, Th. 3.2]. We wish to establish the following algebraic-geometric criterion of simple connectedness for affine algebraic groups.

THEOREM 4.1. *Let G be a connected affine algebraic group over the algebraically closed field F of characteristic 0. Then G is simply connected if and only if $\mathbf{H}(G)$ has no proper affine unramified extensions.*

Proof. By our last remark above, the condition is sufficient. It remains to be shown that if G is simply connected then $\mathbf{H}(G)$ has no proper affine unramified extensions. In order to do this, we transfer the problem to the case where the base field F is the field of complex numbers, in which case we may apply topological considerations in order to obtain the result.

Suppose that G is simply connected, write P for $\mathbf{H}(G)$, and let Q be an affine unramified extension of P. We must show that $Q = P$. Choose a finite system of F-algebra generators for P, and a finite system of P-module generators of Q. The products of pairs of elements of the system of P-module generators of Q, and the images of the F-algebra generators of P under the comultiplication, may be written so as to involve, altogether, only a finite set of coefficients in F. Let F_0 denote the algebraic closure in F of the field obtained by adjoining this finite set of coefficients to the prime field of F. Let P_0 be the F_0-subalgebra of P that is generated over F_0 by our system of F-algebra generators of P, and similarly define the F_0-subalgebra Q_0 of Q. Then P_0 and Q_0 are affine F_0-algebras, and Q_0 contains P_0 and is finitely generated as a P_0-module. Moreover, the comultiplication of P sends P_0 into $P_0 \otimes_{F_0} P_0$, so that P_0 has the structure of an affine Hopf algebra over F_0. We have $P = P_0 \otimes_{F_0} F$ and $Q = Q_0 \otimes_{F_0} F$. Since Q is unramified over P, it follows that Q_0 is unramified over P_0 [6, Section 2]. Thus Q_0 is an affine unramified extension of P_0.

Since F_0 is an algebraic closure of a finitely generated extension field of the field of rational numbers, we may regard it as a subfield of the field $\mathbf{C}$ of complex numbers. Let $P_1 = P_0 \otimes_{F_0} \mathbf{C}$ and $Q_1 = Q_0 \otimes_{F_0} \mathbf{C}$. Then P_1 is an affine Hopf algebra over $\mathbf{C}$, Q_1 is an affine $\mathbf{C}$-algebra containing P_1, and Q_1 is finitely generated as a P_1-module. Moreover, since Q_0 is unramified over P_0, we have that Q_1 is unramified over P_1 [6, Section 2].

Now it will suffice to show that the algebraic variety whose algebra of polynomial functions is P_1 is simply connected in the topological sense. For then it follows from a simple topological consideration that we must have $Q_1 = P_1$ (see [6, end of Section 2]), whence $Q_0 = P_0$, and $Q = P$.

Since G is simply connected, we have $P = \mathbf{H}(G^\circ)$. Since P_0 is finitely generated as an F_0-algebra and $P = P_0 \otimes_{F_0} F$, it is clear that, as the Lie algebra of all differentiations $P \to F$, G° appears in the form $L \otimes_{F_0} F$, where L is the Lie algebra of all differentiations $P_0 \to F_0$. Hence we have $\mathbf{B}(L) \otimes_{F_0} F = \mathbf{B}(G^\circ)$, and we know from Section 3 that P may be identified with $\mathbf{B}(G^\circ)$. It follows that the canonical map $P_0 \to \mathbf{B}(L)$ is an isomorphism, so that we may identify P_0 with $\mathbf{B}(L)$. Tensoring with $\mathbf{C}$ relative to F_0, we see from this that P_1 may be identified with $\mathbf{B}(L \otimes_{F_0} \mathbf{C})$, which shows that $\mathbf{G}(P_1)$ is simply connected as an affine complex algebraic group. But this implies that $\mathbf{G}(P_1)$ is simply connected also in the topological sense, and our proof is now complete.

Our results so far contain a characterization of the affine Hopf algebras arising from Lie algebras with nilpotent radical. This may be stated as follows. *Let (H, μ, u, γ, c) be an affine Hopf algebra with symmetry over the algebraically closed field F of characteristic 0. Then this is the Hopf algebra $\mathbf{B}(L)$ of a finite-dimensional Lie algebra L over F with nilpotent radical if and only if the affine F-algebra H has no proper affine unramified extensions.*

If (H, μ, u, γ, c) is any affine Hopf algebra with symmetry over F then the algebra units of H are precisely the non-zero scalar multiples of the rational homomorphisms of $\mathbf{G}(H)$ into the multiplicative group of F, by [5, end]. On the other hand, one sees easily from the proof of Lemma 2.2 above that a connected affine algebraic group over F has no non-trivial rational homomorphism into the multiplicative group of F if and only if its radical is unipotent. Hence, if H has no units other than the scalar multiples of the identity element, then $\mathbf{G}(H)$ has unipotent radical, and therefore has a universal group covering. If L is the Lie algebra of all differentiations $H \to F$, there is therefore a finite abelian group A of algebra automorphisms of $\mathbf{B}(L)$ such that H may be identified, by the canonical map $H \to \mathbf{B}(L)$, with the A-fixed part $\mathbf{B}(L)^A$ of $\mathbf{B}(L)$. The group A is the kernel of the universal group covering of $\mathbf{G}(H)$, i.e., the *fundamental group* of $\mathbf{G}(H)$.

5. The universal enveloping algebra

Let L be a finite-dimensional Lie algebra over a field F of characteristic 0 (we need not assume here that F is algebraically closed). We recall a basic result due to Harish-Chandra, according to which the elements of $\mathbf{U}(L)$ are separated by the finite-dimensional representations or, equivalently, by the functions belonging to $\mathbf{H}(L)$. The proof is as follows. By Ado's theorem, L has a faithful finite-dimensional representation. Adjoining a suitable 1-dimensional L-module as a direct summand to the representation space of such a representation, we obtain a finite-dimensional faithful L-module V such that every element of L acts on V as a linear endomorphism of trace 0. Choose a basis $(x_1, \cdots, x_n)$ of L over F, and let $e_1, \cdots, e_n$ be the corresponding linear endomorphisms of V. Since these are linearly independent and of trace 0, we can complete this set to a basis $(e_0, e_1, \cdots, e_k)$ of the space $E(V)$ of all linear endomorphisms of V such that e_0 is the identity map on V and each e_i with $i \neq 0$ has trace 0. For every non-negative integer r, let $V^{(r)}$ denote the rth tensor power of the L-module V. Then $E(V^{(r)})$ has a basis consisting of the r-fold tensor products of the e_i's. Now let u be an element of $\mathbf{U}(L)$, and suppose that, when written as an ordered polynomial in the x_i's, u is of degree r. Then we have $u = v + p$, where v is a non-zero homogeneous ordered polynomial of degree r in $x_1, \cdots, x_n$, and p is an ordered polynomial of degree less than r. Now one sees directly that the canonical image of u in $E(V^{(r)})$ is a sum $v^* + q$, where v^* is the tensor polynomial in $e_1, \cdots, e_n$ that is obtained from v by replacing each x_i with e_i, and then applying all permutations of the tensor factors and adding up, while q is a tensor polynomial in $e_0, e_1, \cdots, e_k$ each term of which has at least one factor e_0. Clearly, this implies that the image of u in $E(V^{(r)})$ is different from 0 whenever $u \neq 0$, so that the proof of Harish-Chandra's result is complete.

Now we topologize $\mathbf{U}(L)$ by making the two-sided ideals of finite codimension a fundamental system of neighborhoods of 0. Then, if F is given the discrete topology, $\mathbf{H}(L)$ consists precisely of the *continuous* linear functionals on $\mathbf{U}(L)$. Harish-Chandra's result above means that *our topology on* $\mathbf{U}(L)$ *is a Hausdorff topology.* The tensor product algebra $\mathbf{U}(L) \otimes \mathbf{U}(L)$, which we may identify with $\mathbf{U}(L \oplus L)$, is topologized in the same way. Then both the multiplication, and the comultiplication d, of the Hopf algebra $\mathbf{U}(L)$ are continuous. Hence they extend to yield the structure of a topological algebra on the completion $\mathbf{U}(L)^*$ of $\mathbf{U}(L)$, and a topological algebra homomorphism $d^* : \mathbf{U}(L)^* \to (\mathbf{U}(L) \otimes \mathbf{U}(L))^*$. Moreover, the tensor product $\mathbf{U}(L)^* \otimes \mathbf{U}(L)^*$ may be identified with a subalgebra of $(\mathbf{U}(L) \otimes \mathbf{U}(L))^*$, in the obvious fashion.

We may view $\mathbf{H}(L)$ also as the algebra of all continuous linear functionals on $\mathbf{U}(L)^*$. With this understanding, we claim that *the map that sends each element u of $\mathbf{U}(L)^*$ onto the evaluation $f \to f(u)$ of $\mathbf{H}(L)$ at u is a linear isomorphism of $\mathbf{U}(L)^*$ onto the dual space of $\mathbf{H}(L)$.*

In order to prove this, note that $\mathbf{U}(L)^*$ may be regarded as the projective limit of the system of the factor algebras $\mathbf{U}(L)/I$, where I ranges over the two-sided ideals of finite codimension, with the canonical epimorphisms $\mathbf{U}(L)/I \to \mathbf{U}(L)/J$ for $I \subset J$; by Harish-Chandra's result, the intersection of the family of these ideals is (0), so that the canonical map of $\mathbf{U}(L)$ into $\mathbf{U}(L)^*$ is injective. If u is any non-zero element of $\mathbf{U}(L)^*$, there is a two-sided ideal I of finite codimension in $\mathbf{U}(L)$ such that the canonical image of u in $\mathbf{U}(L)/I$ is different from 0. Hence there is a linear functional f^I on $\mathbf{U}(L)/I$ such that $f^I(u) \neq 0$. Now f^I defines an element f of $\mathbf{H}(L)$ that vanishes on I, and we have $f(u) = f^I(u) \neq 0$. Thus our above map is injective.

Now let τ be any linear functional on $\mathbf{H}(L)$. For every ideal I of finite codimension in $\mathbf{U}(L)$, let $\mathbf{H}(L)^I$ denote an annihilator of I in $\mathbf{H}(L)$. Then $\mathbf{H}(L)^I$ is finite-dimensional, whence there is an element τ_I in $\mathbf{U}(L)$ such that $f(\tau_I) = \tau(f)$ for every element f of $\mathbf{H}(L)^I$. Clearly, the coset $\tau_I + I$ is uniquely determined by τ and I. Now one sees easily that the family of these cosets, as I ranges over the family of all two-sided ideals of finite codimension in $\mathbf{U}(L)$, defines an element τ^* of $\mathbf{U}(L)^*$ such that $f(\tau^*) = \tau(f)$ for every element f of $\mathbf{H}(L)$. This shows that our above map is also surjective, so that our assertion is proved.

Since $\mathbf{U}(L) \otimes \mathbf{U}(L)$ may be identified with $\mathbf{U}(L \oplus L)$ and $\mathbf{H}(L) \otimes \mathbf{H}(L)$ may be identified with $\mathbf{H}(L \oplus L)$, we can show in exactly the same way that *$(\mathbf{U}(L) \otimes \mathbf{U}(L))^*$ is isomorphic with the dual space of $\mathbf{H}(L) \otimes \mathbf{H}(L)$.*

PROPOSITION 5.1. *A linear functional τ on $\mathbf{H}(L)$ is a differentiation if and only if the corresponding element τ^* of $\mathbf{U}(L)^*$ lies in $L\mathbf{U}(L)^*$ and satisfies $d^*(\tau^*) = \tau^* \otimes 1 + 1 \otimes \tau^*$. The linear functional τ is an algebra homomorphism into F if and only if $\tau^* \in 1 + L\mathbf{U}(L)^*$ and $d^*(\tau^*) = \tau^* \otimes \tau^*$.*

Proof. This follows immediately from the above and from the definition of the multiplication on $\mathbf{H}(L)$.

The elements u of $\mathbf{U}(L)^*$ such that $d^*(u) = u \otimes 1 + 1 \otimes u$ are called the *Lie algebra-like* elements of $U(L)^*$; necessarily, they lie in $L\mathbf{U}(L)^*$. The elements u in $1 + L\mathbf{U}(L)^*$ such that $d^*(u) = u \otimes u$ are called the *group-like* elements. The group-like elements constitute a subgroup of the group of units of $\mathbf{U}(L)^*$, and the map to the dual space of $\mathbf{H}(L)$ is a group isomorphism of the group of the group-like elements onto $\mathbf{G}(\mathbf{H}(L))$. Similarly, the Lie algebra-like elements constitute a Lie subalgebra of $\mathbf{U}(L)^*$, and the map to the dual space of $\mathbf{H}(L)$ is a Lie algebra isomorphism of this Lie algebra onto the Lie algebra of all differentiations of $\mathbf{H}(L)$.

It is interesting to note that *the only group-like element in* $\mathbf{U}(L)$ *is the identity element.* For, suppose that u is a group like element in $\mathbf{U}(L)$, and write $u = 1 + v$, with v in $L\mathbf{U}(L)$. Then we have

$$d(v) = v \otimes 1 + 1 \otimes v + v \otimes v.$$

If v is written as an ordered polynomial in given basis elements of L then $d(v)$ is seen to be a linear combination of elements $x \otimes y$, where x and y are ordered monomials in the given basis elements, and the sum of the degrees of x and y is no greater than the degree of v. Hence, if v is different from 0, then the terms of highest degree of $v \otimes v$ cannot appear in $d(v)$, which proves our assertion.

The most interesting case is the case where $L = [L, L]$. Then we have $\mathbf{H}(L) = \mathbf{B}(L)$, so that *the group of the group-like elements of* $\mathbf{U}(L)^*$ *may be identified with the simply connected affine algebraic group whose Lie algebra is* $L = [L, L]$. Moreover, in this case, we have that the only differentiations of $\mathbf{H}(L)$ are the evaluations at the elements of L. Hence, *if* $L = [L, L]$, *then the only Lie algebra-like elements of* $\mathbf{U}(L)^*$ *are the elements of* L.

6. Some representation-theoretical facts

The purpose of this section is to display the significance of certain known facts concerning the representations of Lie algebras and algebraic groups for the structure of the Hopf algebras treated above.

THEOREM 6.1. *Let L be a finite-dimensional Lie algebra over the field F of characteristic* 0. *Then the following five properties are mutually equivalent.*

(1) $L = [L, L]$.

(2) *The image of every finite-dimensional representation of L is an algebraic linear Lie algebra.*

(3) *The canonical map of L into the space of all differentiations of* $\mathbf{H}(L)$ *is surjective.*

(4) $\mathbf{H}(L)$ *is finitely generated as an F-algebra.*

(5) *Every unit of* $\mathbf{H}(L)$ *is an F-multiple of the identity element.*

Proof. It is a standard result that the commutator subalgebra of every linear Lie algebra is an algebraic linear Lie algebra [2, p. 177, Th. 15], so that (1) implies (2). On the other hand, if $L \neq [L, L]$, then one can easily write down a representation of $L/[L, L]$, and so of L, whose image is not an algebraic linear Lie algebra. In order to do this, it suffices to exhibit a one-dimensional Lie algebra of linear endomorphisms of a finite-dimensional F-space that is not an algebraic linear Lie algebra. For example, the Lie algebra consisting of all F-multiples of the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ is not algebraic, because the semisimple and nilpotent components of this matrix are $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, respectively, and these would have to belong to the Lie algebra if the Lie algebra were algebraic. Thus (1) and (2) are equivalent.

The equivalence of (1) and (4) is known from the structure theory of $\mathbf{H}(L)$ [4, Section 5 and Th. 5]. The equivalence of (1) and (3) follows from Theorems 5 and 6, loc. cit., upon applying the isomorphism between the Lie algebra of all differentiations of $\mathbf{H}(L)$ and the Lie algebra of all proper derivations.

Finally, by [5, Th. 5], the units of $\mathbf{H}(L)$ are the non-zero F-multiples of the F-algebra homomorphisms $\mathbf{U}(L) \to F$, and one sees easily that there are such homomorphisms other than the canonical projection if and only if $L \neq [L, L]$ (see [4, p. 518]). Thus (1) and (5) are equivalent.

THEOREM 6.2. *Let L be a finite-dimensional Lie algebra over the field F of characteristic 0. Then L is semisimple if and only if there is a linear functional J on $\mathbf{H}(L)$ such that $J \circ u$ is the identity map on F, and $u \circ J = (J \otimes i) \circ \gamma$, where u is the unit of $\mathbf{H}(L)$ and γ is the comultiplication.*

Proof. First, suppose that L is semisimple. Consider $\mathbf{H}(L)$ as an L-module, with L operating by proper derivations on $\mathbf{H}(L)$. Then $\mathbf{H}(L)$ is a locally finite and hence semisimple L-module. Hence there is an L-module projection of $\mathbf{H}(L)$ onto its L-annihilated part, which is $u(F)$. Let J denote the composite of this L-module projection with the counit c. Then $J \circ u$ is evidently the identity map on F. The canonical L-module decomposition of $\mathbf{H}(L)$ that corresponds to J is $\mathbf{H}(L) = u(F) \oplus L \cdot \mathbf{H}(L)$. Hence, if t is any element of $\mathbf{U}(L)$, and f is any element of $\mathbf{H}(L)$, we have

$$J(t \cdot f) = u(1)(t)J(f).$$

Write $\gamma(f) = \sum_k g_k \otimes h_k$. Then $t \cdot f = \sum_k h_k(t) g_k$. Hence

$$J(t \cdot f) = \sum_k h_k(t) J(g_k),$$

so that

$$u(1)(t)J(f) = \sum_k h_k(t)J(g_k) = (J \otimes i)(\gamma(f))(t).$$

Since $(u \circ J)(f) = J(f)u(1)$, this shows that $u \circ J = (J \otimes i) \circ \gamma$.

Conversely, suppose that there is a linear functional J satisfying the conditions of the theorem. The first part of this proof has shown that these conditions mean that J is a $\mathbf{U}(L)$-module projection $\mathbf{H}(L) \to F$. By elementary representation theory, this implies that, for every finite-dimensional $\mathbf{U}(L)$-module M, there is a $\mathbf{U}(L)$-module projection of M onto its L-annihilated part M^L. In turn, this implies that every finite-dimensional $\mathbf{U}(L)$-module is semisimple (the group analogue of this is carried out in [7, II.2]; see also [7, XI.2]). Thus L is semisimple, and Theorem 6.2 is proved.

One calls a linear functional J on a Hopf algebra (H, μ, u, γ, c) such that $J \circ u$ is the identity map on F and $u \circ J = (J \otimes i) \circ \gamma$ a *gauge* of the Hopf algebra. Proceeding in the same way as in the proof of Theorem 6.2, one finds that *an affine algebraic group is fully reducible if and only if its Hopf algebra of polynomial functions has a gauge.*

In the case of semisimple Lie algebras, and in the case of fully reducible algebraic groups, one has orthogonality relations for representative functions, exactly like those for compact groups (see [7, Ch. II, Ths. 2.4 and 2.5]), with the gauge J taking the place of the Haar integral.

If L is a finite-dimensional semisimple Lie algebra over the field F of characteristic 0, then one can obtain an explicit description of the gauge J on $\mathbf{H}(L)$ as the evaluation at a certain element of $\mathbf{U}(L)^*$, as follows.

Let t denote the Casimir element of $\mathbf{U}(L)$ that is associated with the adjoint representation of L (see [7, XI.2]). Then t lies in the center of $L\mathbf{U}(L)$ and has the following property. If M is any finite-dimensional non-trivial simple L-module then the linear endomorphism of M that corresponds to t is a positive rational multiple of the identity map (if F is algebraically closed, this can be written down explicitly in terms of the highest weight of M and the positive roots of L). Now let I be any proper two-sided ideal of finite codimension in $\mathbf{U}(L)$. Then $\mathbf{U}(L)/I$ is a finite-dimensional semisimple algebra over F. It follows that $I = P_1 \cap \cdots \cap P_k$, where the P_i's are all the maximal two-sided ideals of $\mathbf{U}(L)$ that contain I. Each P_i is the kernel of a simple representation ρ_i of $\mathbf{U}(L)$, namely the representation of $\mathbf{U}(L)$ on a minimal left ideal of $\mathbf{U}(L)/P_i$. The representation ρ_i is trivial only if $P_i = L\mathbf{U}(L)$. Hence, for each i such that $P_i \neq L\mathbf{U}(L)$, $\rho_i(t)$ is the scalar multiplication by a positive rational number $|P_i|$. Hence the element $1 - |P_i|^{-1}t$ of the center of $\mathbf{U}(L)$ belongs to the kernel P_i of ρ_i. We define an element u_I of the center of $\mathbf{U}(L)$ by putting $u_I = \prod_{P_i \neq L\mathbf{U}(L)} (1 - |P_i|^{-1}t)$.

Let I' be another two-sided ideal of finite codimension in $\mathbf{U}(L)$, and suppose that $I' \subset I$. Then we have $I' = I \cap K$, where K is the intersection of a finite set of maximal two-sided ideals distinct from the P_i's and of finite codimension in $\mathbf{U}(L)$. Hence $u_{I'} = u_I u_K$, and $u_{I'} - u_I = u_I(u_K - 1)$. Since $u_K - 1 \in L\mathbf{U}(L)$, we see from this that $u_{I'} - u_I \in I$. It is clear from this that, as I ranges over the two-sided ideals of finite codimension in $\mathbf{U}(L)$, the family of u_I's defines an element u^* of $\mathbf{U}(L)^*$. It is readily seen from this construction that the evaluation of $\mathbf{H}(L)$ at u^* is an L-module projection $\mathbf{H}(L) \to F$, and thus is the gauge of $\mathbf{H}(L)$.

References

1. A. Borel, *Groupes linéaires algébriques*, Ann. of Math., vol. 64 (1956), pp. 20–82.
2. C. Chevalley, *Théorie des groupes de Lie*, vol. II, Hermann, Paris, 1951.
3. ———, *Théorie des groupes de Lie*, vol. III, Hermann, Paris, 1955.
4. G. Hochschild, *Algebraic Lie algebras and representative functions*, Illinois J. Math., vol. 3 (1959), pp. 499–523.
5. ———, *Algebraic Lie algebras and representative functions. Supplement*, Illinois J. Math., vol. 4 (1960), pp. 609–618.

6. ———, *Cohomology of affine algebraic homogeneous spaces*, Illinois J. Math., vol. 11 (1967), pp. 635–643.
7. ———, *The structure of Lie groups*, Holden-Day, San Francisco, 1965.
8. Calvin C. Moore, *Group extensions of p-adic and adelic linear groups*, Acta Math., to appear.
9. G. D. Mostow, *Fully reducible subgroups of algebraic groups*, Amer. J. Math., vol. 78 (1956), pp. 200–221.

University of California
Berkeley, California