COVERINGS OF PRO-AFFINE ALGEBRAIC GROUPS

G. Hochschild

The author has shown [Illinois J. Math. (1969)] that a connected affine algebraic group over an algebraically closed field of characteristic 0 has a universal affine covering if and only if its radical is unipotent. The attempt to construct universal coverings of arbitrary connected affine algebraic groups forces the acceptance of pro-affine algebraic groups, whose Hopf algebras of polynomial functions are not necessarily finitely generated. This is a motivation for extending the covering theory over the larger category of pro-affine algebraic groups.

As we shall see here, the basic methods and results from the theory of affine algebraic groups extend easily and smoothly so as to yield the appropriate results concerning coverings of pro-affine algebraic groups over an algebraically closed field of characteristic 0. In particular, the Lie algebras of these groups can be used for obtaining a simple and natural construction of universal coverings.

Our reconsideration of the covering theory also fills a gap in the theory for affine groups. One of our main results gives a characterization, in algebraic-geometric terms, of those 'space coverings' which arise from group coverings. The simplicity of this characterization is undoubtedly due to the assumption that the base field be of characteristic 0.

For the basic elementary notions and results concerning proaffine algebraic groups and their Hopf algebras of polynomial functions, we refer the reader to [2]. A few general features of this context that are not covered in [2] are dealt with in §2. The initial results concerning coverings, valid also for base fields of nonzero characteristic, are contained in §3. The main results, most of which require that the base field be of characteristic 0, are contained in §'s 4 and 5.

2. Some basic generalities. The structure of a pro-affine algebraic group over a field F consists of a group G, together with a Hopf algebra $A = \mathcal{N}(G)$ of F-valued functions on G, which are called the polynomial functions. These polynomial functions are representative functions, in the sense that, for each polynomial function f, all the translates $x \cdot f \cdot y$, with x and y in G, lie in some finite-dimensional F-space of functions. Here, $x \cdot f \cdot y$ is defined by $(x \cdot f \cdot y)(z) = f(yzx)$. It is assumed that A separates the elements of G, so that we may view the elements of G as F-algebra homo-

morphisms $A \to F$. When we regard an element x of G as a function on A in this way, we write x(f) for f(x). It is assumed also that every F-algebra homomorphism $A \to F$ is the evaluation at an element of G. If $\gamma: A \to A \otimes A$ is the comultiplication of A, then its connection with the group multiplication of G is given by $f(xy) = (x \otimes y)(\gamma(f))$; $xy = (x \otimes y) \circ \gamma$, where x and y denote elements of G, and f denotes an element of A. The antipode $\eta: A \to A$ of the Hopf algebra A corresponds to the inversion map on $G: \eta(f)(x) = f(x^{-1})$.

If the base field F is algebraically closed, and if A is any commutative Hopf algebra with antipode over F having no nilpotent elements other than 0, then the F-algebra homomorphisms $A \to F$ separate the elements of A (see [2]), so that A may be viewed as a Hopf algebra of functions on the group $\mathcal{G}(A)$ of all F-algebra homomorphisms $A \to F$; the group multiplication of $\mathcal{G}(A)$ is obtained from the comultiplication of A, as indicated above. Thus $(\mathcal{G}(A), A)$ is the structure of a pro-affine algebraic group.

It is important to note the fact that every commutative Hopf algebra coincides with the union of the family of its finitely generated (as algebras) Hopf subalgebras. We give a brief indication of the proof. Let A be a commutative Hopf algebra, and let A° be the space dual to A. To every element σ of A° , there correspond two linear endomorphisms σ^* and σ' of A, where $\sigma^* = (\sigma \otimes i) \circ \gamma$, and $\sigma' = (i \otimes \sigma) \circ \gamma$, with γ the comultiplication of A, and i the identity map on A. If U is any subspace of A then $\gamma(U) \subset U \otimes U$ if and only if U is stable under each σ^* and under each σ' . One sees immediately that, for every element u of A, the space spanned by u, the $\sigma^*(u)$'s, the $\sigma'(u)$'s, and the $\sigma^*\tau'(u)$'s, where σ and τ range over A° , is finite-dimensional. One has $\sigma^*\tau^* = ((\tau \otimes \sigma) \circ \gamma)^*$, $\sigma'\tau' = ((\sigma \otimes \tau) \circ \gamma)'$, and $\sigma^*\tau' = \tau'\sigma^*$. Hence the space obtained from u as just described is stable under each σ^* and under each σ' . Moreover, if η is the antipode of A, we have $\sigma^* \circ \eta = \eta \circ (\sigma \circ \eta)'$, and $\sigma' \circ \eta = \eta \circ (\sigma \circ \eta)^*$. Hence the sum of the space described above and its image under η is stable under each σ^* and σ' as well as under η (which is an involution). It follows that the subalgebra of A that is generated by this space is a Hopf subalgebra of A. Since this is finitely generated as an algebra, and since it contains the given element u of A, our above assertion is now established.

We say that the pro-affine algebraic group G is connected if $\mathcal{N}(G)$ is an integral domain. The opposite extreme is the notion of a profinite pro-affine algebraic group. We say that the pro-affine algebraic group G is profinite if $\mathcal{N}(G)$ coincides with the union of the family of its finite-dimensional (as vector spaces over the base field) Hopf subalgebras, so that G appears as a projective limit of a

system of finite groups, namely the groups $\mathcal{G}(S)$, for the finite-dimensional Hopf subalgebras S of A.

The following proposition is the straightforward generalization of the standard result concerning the connected component of the identity in an affine algebraic group.

PROPOSITION 2.1. Let (G, A) be the structure of a pro-affine algebraic group over an algebraically closed field F. There is a normal connected algebraic subgroup G_1 of G such that G/G_1 is profinite. For every finitely generated Hopf subalgebra S of A, the restriction image $(G_1)_S$ is the connected component of the identity in $\mathcal{G}(S)$, and G_1 is the only connected algebraic subgroup H of G with the property that each H_S is of finite index in $\mathcal{G}(S)$. The annihilating ideal of G_1 in A consists of all those elements a of A for which there is an element a' in A such that aa' = 0, while $a'(1) \neq 0$.

Proof. For every pair (S,T) of finitely generated Hopf subalgebras S and T of A such that $S \subset T$, we have the corresponding affine algebraic groups $\mathscr{C}(S)$ and $\mathscr{C}(T)$, and the restriction map $\mathscr{C}(T) \to \mathscr{C}(S)$, which is surjective, because F is algebraically closed. Moreover, this restriction map is surjective from the connected component $\mathscr{C}(T)_1$ of the identity in $\mathscr{C}(T)$ to the connected component $\mathscr{C}(S)_1$ of the identity in $\mathscr{C}(S)$. The general projective limit theorem, as stated and used extensively in [2], is applicable to this system of morphisms of affine algebraic groups, yielding the result that, if G_1 is the projective limit of the $\mathscr{C}(S)_1$'s then the restriction image $(G_1)_S$ of G_1 in $\mathscr{C}(S)$ coincides with $\mathscr{C}(S)_1$, for every finitely generated Hopf subalgebra S of A (incidentally, the same projective limit theorem was used in [2] in order to establish the basic fact that $G_T = \mathscr{C}(T)$ for every Hopf subalgebra T of A, finitely generated or not).

Let S_1 denote the annihilator of $\mathscr{G}(S)_1$ in S. Since each $(G_1)_S$ coincides with $\mathscr{G}(S)_1$, it is clear that an element of G belongs to G_1 if and only if it annihilates each S_1 . Thus, if A_1 is the union of the family of the S_1 's, then G_1 is the annihilator of A_1 in G. Conversely, let a be any element of A that annihilates G_1 . There is a finitely generated Hopf subalgebra S of A that contains a. Now a belongs to $S_1 \subset A_1$. Thus A_1 coincides with the annihilator of G_1 in A, and we have $A_1 \cap S = S_1$ for every finitely generated Hopf subalgebra S of A. It is clear from this that the factor Hopf algebra A/A_1 is the union of a family of Hopf subalgebras each of which is isomorphic with an S/S_1 . Since S/S_1 is an integral domain, namely the Hopf algebra of the connected affine algebraic group $\mathscr{G}(S)_1$, it follows that A/A_1 is an integral domain. Since A/A_1 is the Hopf

algebra of polynomial functions on G_1 , this means that G_1 is connected.

From the fact that each $(G_1)_S$ is normal in $\mathcal{G}(S)$, it follows that G_1 is normal in G. The Hopf algebra of polynomial functions on G/G_1 is the (translation-) G_1 -fixed part A^{G_1} of A (see [2]). This is evidently the union of the family of $S^{G_1,s}$, each of which is finite-dimensional, because $\mathcal{G}(S)/\mathcal{G}(S)_1$ is finite. Hence G/G_1 is profinite.

If H is any connected algebraic subgroup of G with the property of our statement of Proposition 2.1, then H_S , which, in any case, is a connected algebraic subgroup of $\mathcal{G}(S)$, must coincide with $\mathcal{G}(S)_1$, because $\mathcal{G}(S)_1$ is the only connected algebraic subgroup of finite index in $\mathcal{G}(S)$. Hence $H_S = (G_1)_S$ for every finitely generated Hopf subalgebra S of A. Since both H and G_1 are algebraic subgroups of G, this implies that $H = G_1$.

Finally, the description of A_1 given as the last part of Proposition 2.1 follows from the well-known validity of this description for each S_1 as an ideal in S, together with the fact that $A_1 \cap S = S_1$.

3. Coverings. Let G and H be connected pro-affine algebraic groups over an algebraically closed field F. Let $\pi\colon G\to H$ be a surjective morphism of pro-affine algebraic groups. We say that such a surjective morphism π is a covering of G if the kernel G of G is profinite, and the bijective morphism $G/G\to H$ induced by G is an isomorphism of pro-affine algebraic groups. If G is of characteristic 0, then the last condition is automatically satisfied, so that a covering is then simply a surjective morphism with profinite kernel.

In preparation for what follows, we must recall a few notions and facts concerning derivations of rings into modules. Let R be a commutative ring, and let S be a subring of R. If M is an R-module, then an S-derivation of R into M is an S-module homomorphism $\delta \colon R \to M$ such that $\delta(xy) = x \cdot \delta(y) + y \cdot \delta(x)$ for all elements x and y of R. Closely associated with this notion is the R-module $D_s(R)$ of the Kaehler differentials of R relative to S, together with a canonical S-derivation $d: R \to D_s(R)$, having the following universal property: for every S-derivation δ of R into an R-module M, there is one and only one R-module homomorphism $\delta^*: D_s(R) \to M$ such that $\delta^* \circ d = \delta$. One may construct $D_s(R)$ and d as follows: let J be the R-submodule of $R \otimes_{S} R$ that is generated by the elements of the form $1 \otimes xy - x \otimes y - y \otimes x$, put $D_s(R) = (R \otimes_s R)/J$, and let d(x) = $1 \otimes x + J$. We say that R is unramified over S if, for every R-module M, the only S-derivation of R into M is the 0-map. Clearly, R is unramified over S if and only if $D_s(R) = (0)$.

Proposition 3.1. Let $\pi: G \to H$ be a covering of connected pro-

affine algebraic groups over an algebraically closed field F. Then $\mathscr{A}(G)$ is integral and unramified over the image $\mathscr{A}(H) \circ \pi$ of $\mathscr{A}(H)$ in $\mathscr{A}(G)$, and its field of fractions is a Galois extension of the field of fractions of $\mathscr{A}(H) \circ \pi$, the Galois group being isomorphic with the kernel P of π via the translation action of P on $\mathscr{A}(G)$. The differential of π is an isomorphism of the Lie algebra of G onto the Lie algebra of G.

Proof. Write A for $\mathscr{M}(G)$, and B for $\mathscr{M}(H) \circ \pi$. The Hopf algebra of polynomial functions on the pro-affine algebraic group G/P may be identified with the (translation) P-fixed part A^P of A (see [2]). Since the bijection $G/P \to H$ that is induced by π is assumed to be an isomorphism of pro-affine algebraic groups, we have $B = A^P$. Let S be any finitely generated Hopf subalgebra of A. From the assumption that P is profinite, it follows that the restriction image P_S of P in $\mathscr{G}(S)$ is finite. Hence also the isomorphic group of the (left) translations effected by the elements of P on S is finite, whence it is clear that S is integral over S^P . Since S is finitely generated as an F-algebra, this implies that S is finitely generated also as an S^P -module.

The translation action of P on S extends uniquely to an action by field automorphisms of P on the field of fractions [S] of S. Using that the group of these translations is finite, one sees readily that the P-fixed part of [S] coincides with the field of fractions $[S^P]$ of S^P . Thus [S] is a finite Galois extension of $[S^P]$. In particular, it is therefore separable over $[S^P]$.

Next, we show that S is unramified over S^{P} . For this purpose, let us choose a system (s_1, \dots, s_n) of S^P -module generators of S. Let p_i denote the monic minimum polynomial of s_i with respect to $[S^p]$, and let p'_i be the formal derivative of p_i . Since s_i is separable over $[S^P]$, we have $p_i'(s_i) \neq 0$. Now S is the Hopf algebra of the connected affine algebraic group $\mathcal{G}(S)$. As is well known, it is therefore integrally closed in [S], whence S^P is integrally closed [S^P]. It follows that the coefficients of p_i lie in S^P , so that $p_i'(s_i)$ is a nonzero element of S. Put $t = p_1'(s_1) \cdots p_n'(s_n)$. Applying the canonical derivation $d: S \to D_{SP}(S)$, we see immediately that $t \cdot D_{SP}(S) = (0)$. Let T denote the annihilator of $D_{SP}(S)$ in S. The translation action of G on S stabilizes S^{P} , and therefore induces an action of G by (S, G)-semilinear automorphisms of $D_{SP}(S)$ in the natural fashion. It follows that T is stable under the translation action of G. Hence all the G-translates of the nonzero element tobtained above belong to T, so that T has no zero in G_s . Since G_s coincides with $\mathcal{G}(S)$, it follows (on applying the Hilbert Nullstellensatz) that T = S, which means that $D_{SP}(S) = (0)$. Thus S is unramified over S^{P} .

Since $\mathscr{M}(G)$ is the union of the family of its finitely generated Hopf subalgebras S, it follows immediately from the above results concerning S and S^P that $\mathscr{M}(G)$ is integral and unramified over $\mathscr{M}(G)^P = \mathscr{M}(H) \circ \pi$. Moreover, since the P-fixed part of [S] coincides with $[S^P]$ for every finitely generated Hopf subalgebra S, it is clear that the P-fixed part of $[\mathscr{M}(G)]$ coincides with the field of fractions of $\mathscr{M}(H) \circ \pi$. Since P is profinite, it follows (from Galois theory) that $[\mathscr{M}(G)]$ is a Galois extension of $[\mathscr{M}(H) \circ \pi]$, and that the Galois group coincides with the canonical image of P.

The Lie algebra $\mathcal{L}(G)$ of G consists of the differentiations $A \rightarrow F$ at the neutral element of G. The map that sends each element σ of $\mathscr{L}(G)$ onto the linear endomorphism $\sigma' = (i \otimes \sigma) \circ \gamma$ of A is a Lie algebra isomorphism of $\mathcal{L}(G)$ onto the Lie algebra of all proper F-algebra derivations of A, where an F-linear endomorphism of A is called proper if it commutes with every right translation effected on A by an element of G. Hence the last part of Proposition 3.1 will be established as soon as we have proved that every proper derivation δ of A^P is the restriction to A^P of one and only one proper derivation of A. As is well-known, the separability of [A] over [A^P] implies that δ is the restriction to A^P of one and only one derivation δ° of A into [A]. Hence it suffices to show that $\delta^{\circ}(A) \subset A$, and that δ° is proper. In order to prove the first of these facts, consider the map of A into the A-module A/A that is obtained by following up δ° with the canonical A-module homomorphism $[A] \to [A]/A$. Since δ° sends A^{P} into $A^{P} \subset A$, this map is an A^{P} -derivation. Since A is unramified over A^{P} , this map must therefore be the 0-map, which means that $\delta^{\circ}(A) \subset A$. In order to show that δ° is proper, let ρ_x denote the right translation effected on A by an arbitrary element x of G $(\rho_x(f)(y) = f(xy))$. Then δ° and $\rho_x^{-1} \circ \delta^{\circ} \circ \rho_x$ are both extensions of δ . Hence they must coincide. Thus δ° is proper. This completes the proof of Proposition 3.1.

Note that the kernel P of a covering $\pi\colon G\to H$ is necessarily contained in the center of G. The proof is as follows: since P is profinite, $\mathscr{L}(P)$ is the union of the family of its finite-dimensional Hopf subalgebras. If T is any one of these, then the conjugation action of G on P yields a polynomial representation of G by F-algebra automorphisms of G, i.e., a morphism of pro-affine algebraic groups of G into the affine algebraic group of all G-algebra automorphisms of G. From the fact that G(G) is finite and separates the elements of G, one deduces easily that the group of all G-algebra automorphisms of G is finite (or else note that G is the direct sum of a

finite family of copies of F). On the other hand, the image of G under our polynomial representation is a *connected* algebraic linear group, because G is connected. Therefore, our representation of G must be trivial. This shows that, for every t in $\mathscr{A}(P)$, every z in P, and every x in G, we have $t(x^{-1}zx) = t(z)$, whence it is clear that P is central in G.

4. Lie algebra constructions. Let L be a Lie algebra over a field F, and let $\mathscr{U}(L)$ denote the universal enveloping algebra of L. We recall that $\mathscr{U}(L)$ is a Hopf algebra: the comultiplication $\mathscr{U}(L) \to \mathscr{U}(L) \otimes \mathscr{U}(L)$ is the unique F-algebra homomorphism sending each element x of L onto $x \otimes 1 + 1 \otimes x$, and the antipode is the unique F-algebra antihomomorphism $\mathscr{U}(L) \to \mathscr{U}(L)$ extending the multiplication by -1 on L.

Let $\mathscr{U}(L)$ denote the 'continuous dual' of $\mathscr{U}(L)$. Its elements are those F-linear maps $\mathscr{U}(L) \to F$ which annihilate some two-sided ideal of finite codimension in $\mathscr{U}(L)$. The cocommutative Hopf algebra structure of $\mathscr{U}(L)$ dualizes into a commutative Hopf algebra structure of $\mathscr{U}(L)$.

Now suppose that L is the Lie algebra of a connected pro-affine algebraic group G. Then we have a canonical Hopf algebra homomorphism $\alpha\colon \mathscr{A}(G)\to \mathscr{H}(L)$ whose definition is as follows. The representation of L by proper F-algebra derivations of $\mathscr{A}(G)$ defines a $\mathscr{U}(L)$ -module structure of $\mathscr{A}(G)$, for which $\mathscr{A}(G)$ is a locally finite $\mathscr{U}(L)$ -module. For u in $\mathscr{U}(L)$, and a in $\mathscr{A}(G)$, let $u \cdot a$ denote the transform of a by a. Then the element a(a) of $\mathscr{H}(L)$ is defined by a(a)(a) = ($a \cdot a$)(1), where 1 stands for the neutral element of G. It is easy to verify, directly from the definitions, that a is indeed a homomorphism of Hopf algebras.

The full dual of $\mathscr{U}(L)$ is still a commutative F-algebra, the multiplication being induced from the comultiplication of $\mathscr{U}(L)$. In the case where the base field F is of characteristic 0, this F-algebra is easily shown to be isomorphic with the F-algebra of formal integral power series in a set of variables that is in bijective correspondence with a basis of the F-space L. In particular, the F-subalgebra $\mathscr{U}(L)$ of the full dual is therefore an integral domain whenever the base field F is of characteristic 0.

PROPOSITION 4.1. Let (G, A) be the structure of a connected pro-affine algebraic group over a field F of characteristic 0. Let L denote the Lie algebra of G. Then the canonical Hopf algebra homomorphism $\alpha: A \to \mathcal{H}(L)$ is injective.

Proof. Let a be an element of the kernel of α . This means

that, for every element u of $\mathcal{U}(L)$, the transform $u \cdot a$ takes the value 0 at the neutral element of G. There is a finitely generated Hopf subalgebra S of A that contains a. Since F is of characteristic 0, we have from standard affine algebraic group theory that the space spanned by the translates $x \cdot a$, with x ranging over the connected affine algebraic group $\mathcal{G}(S)$, is contained in $\mathcal{U}(\mathcal{L}(\mathcal{G}(S)) \cdot a)$. If we prove that each element of this last space takes the value 0 at the neutral element of G, we shall therefore have a(x) = 0 for every x in $\mathcal{G}(S)$, and a fortiori for every x in G, so that a = 0. Hence it suffices to show that the restriction of L to S coincides with the full Lie algebra $\mathcal{L}(\mathcal{G}(S))$ of $\mathcal{G}(S)$.

Clearly, L is the projective limit of the system of the Lie algebras $\mathscr{L}(\mathscr{G}(S))$ and the restriction maps $\mathscr{L}(\mathscr{G}(S_1)) \to \mathscr{L}(\mathscr{G}(S_2))$ for the pairs (S_1, S_2) of finitely generated Hopf subalgebras with $S_2 \subset S_1$. Now the restriction image $\mathscr{G}(S_1)_{S_2}$ is algebraically dense in $\mathscr{G}(S_2)$ (it need not coincide with $\mathscr{G}(S_2)$, because we have not assumed here that F is algebraically closed). Since F is of characteristic 0, this implies, as is well-known, that the restriction map $\mathscr{L}(\mathscr{G}(S_1)) \to \mathscr{L}(\mathscr{G}(S_2))$ is surjective. Thus L is the projective limit of a system of finite-dimensional F-spaces with surjective linear maps. To such a system, the general projective limit theorem is applicable, and it yields the result that the restriction map $L \to \mathscr{L}(\mathscr{G}(S))$ is surjective, which completes the proof of Proposition 4.1.

We note in passing that a slightly more elaborate application of the same case of the projective limit theorem yields the result that, even if S is not finitely generated, the restriction map $L \to \mathcal{L}(\mathcal{G}(S))$ is surjective.

We wish to establish a partial converse to Proposition 3.1. The result we shall obtain requires the assumption that the base field be of characteristic 0. Therefore, we shall assume from now on that our base field F is algebraically closed and of characteristic 0.

Let (G,A) be the structure of a connected pro-affine algebraic group over F. Suppose that B is an integral domain F-algebra containing A as an F-subalgebra, and that B is integral and unramified over A. We shall call such a B an integral unramified extension of A. Our proof of the last part of Proposition 3.1 applies to the present situation, and shows that the canonical $\mathcal{U}(L)$ -module structure of A extends to one and only one $\mathcal{U}(L)$ -module structure of B for which the elements of B act as B-algebra derivations. If B is locally finite as a $\mathcal{U}(L)$ -module, then we shall call B a profinite extension of A.

Theorem 4.2. Let (G, A) be the structure of a connected pro-

affine algebraic group over the algebraically closed field F of characteristic 0, and let L denote the Lie algebra of G. Let B be a profinite extension of A. Then the canonical Hopf algebra homomorphism $\alpha: A \to \mathcal{H}(L)$ can be extended to an F-algebra isomorphism of B onto a Hopf subalgebra of $\mathcal{H}(L)$. In particular, the Hopf algebra structure of A, together with the F-algebra structure of B, extends to a Hopf algebra structure of B, and B may thus be identified with the Hopf algebra of a covering of G.

Proof. Let $c: A \to F$ denote the co-unit of A, i.e., the evaluation at the neutral element of G. Since B is integral over A, this homomorphism can be extended to an F-algebra homomorphism $B \rightarrow F$, which we shall still denote by c (although it is not uniquely determined by its restriction to A). Using c and the locally finite $\mathcal{U}(L)$ -module structure of B in exactly the same way as in the definition of the canonical map α of A into $\mathcal{H}(L)$, we obtain an extension of α to an F-algebra homomorphism $\beta: B \to \mathcal{H}(L)$. If b is any element of B, we have a relation $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, with each a_i in A. If $b \neq 0$, and if we take such a relation with the smallest possible n, then we have $a_n \neq 0$. Applying β to this relation, and noting that $\beta(a_n) = \alpha(a_n) \neq 0$ (by Proposition 4.1), we see that $\beta(b) \neq 0$. Thus β is injective. Moreover, it is evident from the definition of β , and from the unicity of the $\mathcal{U}(L)$ -module structure of B, that $\beta(B)$ is a $\mathcal{U}(L)$ -submodule of $\mathcal{H}(L)$, and that β is a homomorphism of $\mathcal{U}(L)$ -modules.

Now let us consider the right L-module structure of A that is obtained by associating, with each element σ of L, the derivation $\sigma^* = (\sigma \otimes i) \circ \gamma$ of A. Just like the left L-module structure of A, this extends to one and only one right L-module structure of B such that L acts by F-algebra derivations. Let us write $b \cdot \sigma$ for the transform of an element b of B under the derivation corresponding to the element σ of L, and let us indicate the canonical right L-module structure of $\mathcal{H}(L)$ in the same fashion. Now consider the map $\beta_{\sigma}: B \to \mathscr{H}(L)$ defined by $\beta_{\sigma}(b) = \beta(b \cdot \sigma) - \beta(b) \cdot \sigma$. restriction of β_{σ} to A is evidently the 0-map. Hence, if we regard $\mathscr{H}(L)$ as an A-module, with A acting via α , then β_{σ} is an A-linear derivation of B into $\mathcal{H}(L)$. Since B is unramified over A, it follows that β_{σ} is the 0-map. In particular, $\beta(B)$ is therefore stable, not only under the left action of L, but also under the right action. In terms of the Hopf algebra structure of $\mathcal{H}(L)$, this means that the image of $\beta(B)$ under the comultiplication of $\mathcal{H}(L)$ lies in $\beta(B) \otimes \beta(B)$.

Now let P denote the smallest Hopf subalgebra of $\mathcal{H}(L)$ that contains $\beta(B)$. Let us view $\mathcal{H}(L)$ as the Hopf algebra of polynomial

functions on the pro-affine algebraic group $\mathcal{G}(\mathcal{H}(L))$. It is known that the stability property of $\beta(B)$ we have just established implies that P is generated as an F-algebra by the elements of $\beta(B)$ and the reciprocals of those elements of $\beta(B)$ which are group homomorphisms of $\mathcal{G}(\mathcal{H}(L))$ into the multiplicative group of F (see [2, §2]). In order to simplify the notation, let us now identify B with $\beta(B)$. Let b be an element of B that is a group homomorphism, and let p(x) be the monic minimum polynomial of b with respect to the field of fractions [A] of A. We know from our proof of Proposition 3.1 that the coefficients of p(x) actually belong to A. Since A is stable under the antipode η of $\mathcal{H}(L)$, the element $\eta(b)$, which is equal to the reciprocal b^{-1} of b, is still integral over A. Hence the monic minimum polynomial, q(x) say, of b^{-1} with respect to [A] also belongs to A[x]. If a is the constant term of p(x), then the constant term of q(x) is a^{-1} . Hence a^{-1} lies in A, whence we see that b^{-1} lies in $A[b] \subset B$. In our original notation, the result is that $\beta(B) = P$, i.e., that $\beta(B)$ is a Hopf subalgebra of H(L). The remaining assertions of Theorem 4.2 are immediate consequences: the injection $A \rightarrow B$ yields a surjective morphism of the pro-affine algebraic group $\mathcal{G}(B)$ onto $\mathcal{G}(A) = G$. From the fact that B is integral over A, it follows that the kernel of this morphism is profinite.

The embedding $B \to \mathcal{H}(L)$ of Theorem 4.2 has a unicity property, as follows. Suppose that ρ is an A-algebra isomorphism of B onto another profinite extension B' of A. Let us identify B with its image $\beta(B)$ in $\mathcal{H}(L)$, and let $\beta': B' \to \mathcal{H}(L)$ be the F-algebra homomorphism constructed from the $\mathcal{U}(L)$ -module structure of B'and an F-algebra homomorphism $c': B' \to F$ extending the co-unit of A, as in the proof of Theorem 4.2. Because of the unicity of the $\mathcal{U}(L)$ -module structure of B', our A-algebra isomorphism ρ is necessarily also an isomorphism of $\mathcal{U}(L)$ -modules. Hence, for every element b of B, and every element u of $\mathcal{U}(L)$, we have $\beta'(\rho(b))(u) =$ $c'(u \cdot \rho(b)) = (c' \circ \rho)(u \cdot b)$. Now $c' \circ \rho$ is an F-algebra homomorphism $B \to F$, which we view as an element p of $\mathcal{G}(B)$. If c denotes the co-unit of $\mathcal{H}(L)$, and if the right translation action of p on B is indicated by $f \rightarrow f \cdot p$, the above gives $\beta'(\rho(b))(u) = p(u \cdot b) = c((u \cdot b) \cdot p) = c(u \cdot b) \cdot p$ $c(u \cdot (b \cdot p)) = (b \cdot p)(u)$, so that $\beta'(\rho(b)) = b \cdot p$. Thus we have B = $\beta'(B')$. Moreover, the restriction of p to A is the neutral element of $\mathcal{G}(A) = G$, so that p lies in the kernel of our covering $\mathcal{G}(B) \to G$ $\mathcal{G}(A)$. In particular, p is therefore central in $\mathcal{G}(B)$. If we endow B' with the Hopf algebra structure obtained from β' , our result may be expressed by saying that the transpose $\rho^{\circ}: \mathcal{G}(B') \to \mathcal{G}(B)$ is an isomorphism of pro-affine algebraic varieties such that $\rho^{\circ}(x)\rho^{\circ}(y)=$

 $p\rho^{\circ}(xy)$ for all elements x and y of $\mathscr{G}(B')$. For the case B=B', we see that a change of the embedding $\beta\colon B\to\mathscr{H}(L)$ is reflected in the group $\mathscr{G}(B)$ as a change of the multiplication $(x,y)\to xy$ to a new multiplication $(x,y)\to pxy$, where p is as above.

The significance of Theorem 4.2 is strengthened considerably by the following characterization of profinite extensions.

THEOREM 4.3 Let (G, A) be as in Theorem 4.2, and let B be an F-algebra containing A as an F-subalgebra. Then B is a profinite extension of A if and only if it is the union of a family of finitely generated F-subalgebras each of which is an integral unramified extension of a finitely generated Hopf subalgebra of A.

Proof. The necessity of the condition is clear from Theorem 4.2 and Proposition 3.1. In proving the sufficiency, we may evidently assume that A and B are finitely generated, i.e., it suffices to prove that if A is finitely generated, and if B is a finitely generated integral unramified extension of A, then B is locally finite as a $\mathcal{U}(L)$ -module, where L is the Lie algebra of the connected affine algebraic group G.

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 can apply complex analysis and the theory of complex analytic groups. The transfer to the field C of complex numbers is exactly the same as the one we made in proving [1, Th. 4.1]: there is a subfield F_0 of F such that the following obtains.

- (1) F_0 is the algebraic closure in F of a finitely generated extension field of the field of rational numbers.
- (2) We have $A = A_0 \bigotimes_{F_0} F$, and $B = B_0 \bigotimes_{F_0} F$, where A_0 is a finitely generated Hopf algebra over F_0 , and B_0 is a finitely generated integral unramified extension of A_0 .

Now observe that, because of (1), F_0 may be identified with a subfield of the field C of complex numbers, so that we can form the Hopf algebra $A_1 = A_0 \bigotimes_{F_0} C$, and the integral unramified extension $B_1 = B_0 \bigotimes_{F_0} C$ of A_1 . Now A_1 is a finitely generated integral domain, so that $\mathscr{C}(A_1)$ is a connected affine algebraic group over C. We may regard $\mathscr{C}(A_1)$ also as a complex analytic group, and as a complex analytic manifold (it is well-known that a connected complex affine algebraic variety is topologically connected). Although we have, as yet, no group structure on $\mathscr{C}(B_1)$, we may view it as an affine algebraic variety. The injection $A_1 \to B_1$ transposes into a morphism of affine algebraic varieties $\mathscr{C}(B_1) \to \mathscr{C}(A_1)$. From the fact that B_1 is integral over A_1 , we have that this morphism is surjective, and

the inverse image of each point of $\mathcal{G}(A_1)$ is finite. From the fact that B_1 is unramified over A_1 , one deduces easily that the differential of our morphism maps the tangent space at each point of $\mathcal{G}(B_1)$ bijectively onto the tangent space at the image of that point in $\mathcal{G}(A_1)$. It follows that $\mathcal{G}(B_1)$ can be endowed with the structure of a complex analytic manifold such that our morphism is a covering of analytic manifolds, and such that each element of B_1 is a holomorphic function on $\mathcal{G}(B_1)$.

It is clear from the elementary theory of analytic group coverings that we can endow the covering manifold $\mathcal{G}(B_1)$ of $\mathcal{G}(A_1)$ with the structure of a complex analytic group such that our analytic manifold covering becomes a covering of complex analytic groups. denote the C-algebra of all holomorphic functions on $\mathcal{G}(B_1)$. complex analytic group $\mathcal{G}(B_i)$ acts by translation on S. We consider the differential of this representation, i.e., the corresponding action, by derivations, of the Lie algebra, L_1 say, of $\mathcal{G}(B_1)$ on S. Let σ be any element of L_1 , and let σ' denote the corresponding derivation of B_1 into S. If we follow up σ' with the canonical B_1 module homomorphism $S \to S/B_1$, we obtain a derivation $\sigma^{\circ} : B_1 \to S/B_1$. Since σ' stabilizes A_1 (because it coincides on A_1 with the derivation corresponding to σ when σ is viewed as an element of the Lie algebra of the affine algebraic group $\mathcal{G}(A_1)$, this derivation σ° is A_1 -linear. But B_1 is unramified over A_1 , so that σ° must therefore be the 0-map. This means that σ' sends B_1 into B_1 . It follows that B_1 is stable also under the translation action of the complex analytic group $\mathcal{G}(B_1)$.

Now note that B_1 is a finitely generated C-algebra. In particular, B_1 is therefore of countable dimension as a C-space. Let b be any element of B_1 . Since all the $\mathcal{G}(B_1)$ -translates of b lie in B_1 , they lie in a C-space of countable dimension. It is known (see [3, Lemma 1.2]) that if a holomorphic function on a complex analytic group has the property that its translates span a space of functions of countable dimension then its translates actually span a space of finite dimension. Hence we conclude that B_1 is locally finite as a $\mathcal{G}(B_1)$ -module, and therefore also as an L_1 -module. Identifying L_1 with the Lie algebra of the affine algebraic group $\mathcal{G}(A_1)$, we see that this means that B_1 is locally finite with respect to the canonical extension of the $\mathcal{U}(L_1)$ -module structure of A_1 . It is clear from the relation of B_1 to the original B, that this implies that B is locally finite as a $\mathcal{U}(L)$ -module. Hence B is indeed a profinite extension of A, and Theorem 4.3 is proved.

5. Universal coverings and simply connected groups. A covering $\pi: G^* \to G$ is said to be a universal covering of G if, for

every covering $\tau \colon T \to G$, there is one and only one covering $\pi^{\tau} \colon G^* \to T$ such that $\tau \circ \pi^{\tau} = \pi$.

THEOREM 5.1 Let (G,A) be the structure of a connected proaffine algebraic group over an algebraically closed field F of characteristic 0. Let L denote the Lie algebra of G, and let $\alpha: A \to \mathcal{H}(L)$ be the canonical Hopf algebra embedding. Let $\alpha(A)^*$ denote the integral closure of $\alpha(A)$ in $\mathcal{H}(L)$. Then $\alpha(A)^*$ is a Hopf subalgebra of $\mathcal{H}(L)$, and the restriction map $\mathcal{G}(\alpha(A)^*) \to \mathcal{G}(\alpha(A))$, followed by the transpose $\mathcal{G}(\alpha(A)) \to G$ of α , is a universal covering of G.

Proof. Let us identify A with its isomorphic image $\alpha(A)$ in $\mathscr{H}(L)$. One sees immediately that if an element f of $\mathscr{H}(L)$ is integral over A, then the same is true for its image under the antipode η , and for all its translates $x \cdot f$ and $f \cdot x$, with x in $\mathscr{G}(\mathscr{H}(L))$. Thus A^* is a Hopf subalgebra of $\mathscr{H}(L)$. The restriction map $\mathscr{G}(A^*) \to \mathscr{G}(A) = G$ is a covering, owing to the fact that A^* is integral over A. Let us denote this covering by π .

Now let $\tau\colon T\to G$ be any covering of G. By Proposition 3.1, $\mathscr{M}(T)$ is integral over $A\circ\tau$, and the differential τ° of τ is a Lie algebra isomorphism of the Lie algebra $\mathscr{L}(T)$ of T onto the Lie algebra L of G. The inverse of τ° extends to a Hopf algebra isomorphism $\mathscr{U}(L)\to\mathscr{U}(\mathscr{L}(T))$, which dualizes into a Hopf algebra isomorphism $\tau^*\colon \mathscr{H}(\mathscr{L}(T))\to\mathscr{H}(L)$. Let σ be the canonical Hopf algebra imbedding $\mathscr{M}(T)\to\mathscr{H}(\mathscr{L}(T))$. Now $\tau^*\circ\sigma$ is an injective Hopf algebra homomorphism of $\mathscr{M}(T)$ into $\mathscr{H}(L)$, and its composite with the transpose $A\to\mathscr{M}(T)$ of τ is the injection map $A\to\mathscr{H}(L)$. It follows that the image of $\mathscr{M}(T)$ must lie in A^* , so that $\tau^*\circ\sigma$ is an injective Hopf algebra homomorphism $\mathscr{M}(T)\to A^*$. The transpose of this is clearly a covering $\pi^\tau\colon \mathscr{G}(A^*)\to T$ such that $\tau\circ\pi^\tau=\pi$.

Finally, if $\rho: \mathscr{G}(A^*) \to T$ is any covering such that $\tau \circ \rho = \pi$, then the differential of ρ is equal to $(\tau^{\circ})^{-1} \circ \pi^{\circ}$. Since a morphism of connected pro-affine algebraic groups over a field of characteristic 0 is determined by its differential, ρ must therefore coincide with the above π° . This completes the proof of Theorem 5.1.

Note that if G is defined over a subfield F_1 of F, then the universal covering obtained in Theorem 5.1 is also defined over F_1 .

We shall say the connected pro-affine algebraic group G is $simply \ connected$ if every covering of G is an isomorphism.

Theorem 5.2. Let G be a connected pro-affine algebraic group over an algebraically closed field F, and let K be a connected normal algebraic subgroup of G. If both G/K and K are simply connected,

then G is simply connected. Conversely, if G is simply connected, then G/K is simply connected and, if F is of characteristic 0, then K is also simply connected.

Proof. Suppose that both G/K and K are simply connected, and let $\pi\colon G'\to G$ be a covering of G. Let P denote the kernel of π , and let K' be the connected component of the neutral element in $\pi^{-1}(K)$. Let $\pi'\colon G'/K'\to G/K$ be the morphism induced by π . Evidently, π' is surjective, and the kernel of π' is (PK')/K'. Since P is profinite, so is therefore the kernel of π' . From the fact that π induces an isomorphism of pro-affine algebraic groups $G'/P\to G$, one sees readily that the bijective morphism $(G'/K')/((PK')/K')\to G/K$ that is induced by π' is also an isomorphism of pro-affine algebraic groups. Thus π' is a covering of G/K. Since G/K is simply connected, we must therefore have $P\subset K'$. The restriction of π to K' is now seen to be a covering with kernel P. Since K is simply connected, it follows that P must be trivial. Thus we have shown that G is simply connected whenever both G/K and K are simply connected.

Now suppose that G is simply connected. Exactly the same proof as that of Lemma 2.1 in [1] shows that G/K is simply connected: given a covering $\tau\colon H{\to}G/K$, one considers the fibered product of H and G, with respect to τ and the canonical map $G{\to}G/K$. One sees easily that the projection of this fibered product onto G is a covering whose kernel is isomorphic with the kernel of τ . Hence τ must be an isomorphism.

It remains to be shown that if G is simply connected, and if Fis of characteristic 0, then K is simply connected. If H is any pro-affine algebraic group, we denote by H_u the unipotent radical of H, i.e., the unique maximum unipotent normal algebraic subgroup of H. It is easy to see that a unipotent pro-affine algebraic group over an algebraically closed field of characteristic 0 is simply connected; otherwise we could at once infer from Proposition 3.1 that some affine homomorphic image of it has a nontrivial covering with finite kernel, and this is well-known to be impossible for a unipotent affine algebraic group over a field of characteristic 0. Thus the unipotent radicals G_u and K_u are simply connected. Since K is normal in G, we have $K_u \subset G_u$, and hence $K_u = G_u \cap K$. Since K_u is simply connected, we have from the part of Theorem 5.2 already proved that K is simply connected if and only if K/K_u is simply connected. Since $K_u = G_u \cap K$, we may identify K/K_u with its canonical image in G/G_u , i.e., with a normal connected algebraic subgroup of G/G_u . Since F is of characteristic 0, G/G_u and K/K_u are reductive pro-affine algebraic groups, which means that all their

polynomial representations are semisimple (cf. [2]). Therefore, without loss of generality, we shall now assume that G and K are reductive.

Let C(K) denote the connected component of the neutral element in the center of K, and define C(G) in the same way. We claim that $C(K) \subset C(G)$. In order to see this, let S be any finitely generated Hopf subalgebra of $\mathcal{N}(G)$. Then the restriction image $C(K)_{S}$ is a toroid. The conjugation action of G induces an action of G by Hopf algebra automorphisms on S, with respect to which S is a locally finite G-module. Since C(K) is normal in G, this G-module structure of S induces a G-module structure on the restriction image $S_{C(K)}$. Since $C(K)_S$ is a toroid, we have $S_{C(K)}$ $F[t_1, \dots, t_n, t_1^{-1}, \dots, t_n^{-1}]$, where the t_i 's are algebraically independent homomorphisms of $C(K)_S$ into the multiplicative group of F. Let x be an element of G, and let x' denote the corresponding Hopf algebra automorphism of $S_{C(K)}$. Then each $x'(t_i)$ is a monomial formed with the t_s and their reciprocals. Since $S_{C(K)}$ is locally finite as a G-module, it is clear that the set of all monomials so obtained from elements of G must be finite. Hence the image of G in the automorphism group of $S_{C(K)}$ is finite. On the other hand, this image must be a connected affine algebraic group, because it is the image of G under a morphism of pro-affine algebraic groups. Hence this image must be trivial. Since this holds for every finitely generated Hopf subalgebra of $\mathcal{M}(G)$, we conclude that G centralizes C(K), so that $C(K) \subset C(G)$.

Now let us consider the algebraic hull in G of the commutator subgroup of G. Let us denote this algebraic hull by [G,G], and define [K,K] in the same way. For every finitely generated Hopf subalgebra S of $\mathscr{M}(G)$, the restriction image G_S is a connected reductive affine algebraic group. Hence G_S is the product of its commutator subgroup and $C(G_S)$. The commutator subgroup of G_S is an algebraic subgroup, and it coincides with the restriction image $[G,G]_S$. Also, $C(G_S)=C(G)_S$ (by the projective limit theorem and Proposition 2.1). Thus we have $G_S=[G,G]_SC(G)_S$. Since [G,G] and C(G) are algebraic subgroups of G, the multiplication map $[G,G]\times C(G)\to G$, which is evidently a group homomorphism, is a morphism of pro-affine algebraic groups. It is known from [2] that its image [G,G]C(G) in G is therefore an algebraic subgroup of G. Since $([G,G]C(G))_S=G_S$ for every finitely generated Hopf subalgebra S of $\mathscr{M}(G)$, it follows that [G,G]C(G)=G. Similarly, K=[K,K]C(K).

For each S as above, $[G, G]_S$ is semisimple, and its intersection with $C(G)_S$ is finite. It is clear from this that the surjective morphism $[G, G] \times C(G) \to G$ is a covering. Since G is simply con-

nected, it follows that G is actually the *direct* product of its algebraic subgroups [G, G] and C(G). This implies that $[K, K] \cap C(K)$ is also trivial, because $C(K) \subset C(G)$. Therefore, K is the direct product $[K, K] \times C(K)$. Evidently, the direct factors [G, G] and C(G) of the simply connected group G must be simply connected.

By the part of Theorem 5.2 already proved, it suffices to show that both C(K) and [K, K] are simply connected. Therefore, our problem is reduced to the following two cases:

- (1) G is semisimple (in the sense that G_s is semisimple for every finitely generated Hopf subalgebra S of $\mathscr{A}(G)$);
 - (2) G is abelian (and reductive).

Consider case (1). In this case, we have, for each S as above, $G_S = P(S)K_S$, where P(S) is the connected component of the neutral element in the centralizer of K_S in G_S . If T is another finitely generated Hopf subalgebra of $\mathscr{M}(G)$ such that $S \subset T$, then we have $P(S) \subset P(T)_S K_S$ and $P(T)_S \subset P(S)$, so that $P(S) \subset P(T)_S (P(S) \cap K_S)$. Since $P(S) \cap K_S$ is finite, this shows that $P(T)_S$ is of finite index in P(S). But this forces $P(T)_S = P(S)$, because P(S) is connected. Now it follows from the projective limit theorem that each P(S) is actually the restriction image P_S , where P is the connected component of the neutral element in the centralizer of K in G, and hence that G = PK (by an argument we have already used above). Clearly, $P \cap K$ is profinite, whence we see that the multiplication map $P \times K \to G$ is a covering. Since G is simply connected, we have therefore $G = P \times K$, whence K is simply connected.

Now consider case (2). Let $\tau\colon K'\to K$ be a covering, and let P denote the kernel of τ . From the fact that K is abelian and P profinite, it follows that K' is abelian. It has been proved by J-P. Serre that, in the category of commutative pro-algebraic groups over an algebraically closed field of characteristic 0, the group extension functor Ext is right exact (see Th. 1, § 10.1 of [4]). In particular, the map $\operatorname{Ext}(G/K,K')\to\operatorname{Ext}(G/K,K)$ that is induced by τ is therefore surjective. Hence there is a group extension $K'\to G'\to G/K$ and a morphism $\sigma\colon G'\to G$ such that the following diagram is exact and commutative

Here, G' is a projective limit of factor groups that are algebraic groups. From the diagram, we see at once that σ is surjective, and that the kernel of σ coincides with the kernel P of τ . It

follows that each factor group of G' that is an algebraic group is an extension of a finite group (a factor group of P) by an affine algebraic group (a factor group of G), whence it must be an affine algebraic group. Thus G' is actually a pro-affine algebraic group, and σ is a covering in our sense. Hence the kernel P of σ must be trivial, and we have shown that K is simply connected. The proof of Theorem 5.2 is now complete.

REFERENCES

- 1. G. Hochschild, Algebraic groups and Hopf algebras, Illinois J. Math. 14 (1970), 52-65.
- 2. G. Hochschild and G. D. Mostow, *Pro-affine algebraic groups*, Amer. J. Math. XCI (1969), 1127-1140.
- 3. G. Hochschild and G. D. Mostow, Affine embeddings of complex analytic homogeneous spaces, Amer. J. Math. 97 (1965), 807-839.
- 4. J-P. Serre, Groupes Proalgébriques, IHES, 1960, No. 7, 341-403.

Received December 19, 1969.

UNIVERSITY OF CALIFORNIA, BERKELEY