JOURNAL OF ALGEBRA 79, 375–392 (1982)

Commutative Hopf Algebras and Cocommutative Hopf Algebras in Positive Characteristic

MITSUHIRO TAKEUCHI*

Department of Mathematics, University of Tsukuba, Ibaraki 305, Japan

Communicated by N. Jacobson

Received January 1, 1981

Let A be a commutative Hopf algebra over a field k of characteristic $p > 0$. Let $\varphi: C \to B$ be a surjective map of commutative algebras such that $x^p = 0$ for any x in $\mathrm{Ker}(\varphi)$, so that the map $F_C: k^{1/p} \otimes C \to C$, $\lambda \otimes a \mapsto \lambda^p a^p$ factors through $k^{1/p} \otimes \varphi$, yielding a map $F_C^B: k^{1/p} \otimes B \to C$. A map of algebras $f: A \to B$ can be lifted to an algebra map $\bar{f}: A \to C$ such that $f = \varphi \circ \bar{f}$ if and only if $\mathrm{Ker}(F_A) \subset \mathrm{Ker}(F_C^B \circ (k^{1/p} \otimes f))$. In particular, if F_A is injective, any algebra map $A \to B$ can be lifted to $A \to C$. The dual results will be given for cocommutative Hopf algebras and coalgebra maps.

INTRODUCTION

It is known that every reduced algebraic group over a perfect field is *smooth* [1, p. 239]. This means that if A is a finitely generated commutative Hopf algebra over a field k such that $\bar{k} \otimes A$ is reduced, then for any surjective map of commutative algebras $\varphi: C \to B$ whose kernel $\mathrm{Ker}(\varphi)$ is nilpotent, any algebra map $f: A \to B$ can be lifted to an algebra map $\bar{f}: A \to C$ such that $\varphi \circ \bar{f} = f$ [1, Corollary 4.6, p. 111; 4, (28.C), p. 198, (28.D), p. 200]. If k is of characteristic 0, $\bar{k} \otimes A$ is always reduced, and if k is of characteristic $p > 0$, $\bar{k} \otimes A$ is reduced, if and only if $k^{1/p} \otimes A$ is reduced. In this paper, we assume k is a field of characteristic $p > 0$ and give a direct and rather easy proof of the above lifting property. Reducedness of $k^{1/p} \otimes A$ is equivalent to the injectivity of the map $F_A: k^{1/p} \otimes A \to A$, $\lambda \otimes a \mapsto \lambda^p a^p$. Unless F_A is injective, not every algebra map $A \to B$ can be lifted to $A \to C$. The following result will give a criterion for it be lifted:

* This article was written while the author was a member of The Institute for Advanced Study, and partially supported by NSF Grant MCS77–18723 A03.

0021-8693/82/120375–18$02.00/0

THEOREM 1.1. *Let A be a commutative Hopf algebra and let $\varphi: C \to B$ be a surjective map of commutative algebras such that $x^p = 0$ for any x in* $\operatorname{Ker}(\varphi)$. *The map F_C factors as*

$$F_C: k^{1/p} \otimes C \xrightarrow{k^{1/p} \otimes \varphi} k^{1/p} \otimes B \xrightarrow{F_C^B} C.$$

Let $f: A \to B$ be an algebra map. There is an algebra map $\bar{f}: A \to C$ such that $\varphi \circ \bar{f} = f$ if and only if $\operatorname{Ker}(F_A) \subset \operatorname{Ker}\,(F_C^B \circ (k^{1/p} \otimes f))$.

As a corollary, if F_A is injective, it follows that every algebra map $A \to B$ can be lifted to an algebra map $A \to C$. This fact is true, if only φ is surjective with *bounded nil* kernel.

The geometric meaning of the above result is as follows. Let G be an affine (not necessarily algebraic) group scheme over k. Let $F_G: G \to G^{(p)}$ denote the Frobenius map for G. Let $X \hookrightarrow Y$ be a closed immersion of affine schemes such that $F_Y: Y \to Y^{(p)}$ has image in $X^{(p)}$. *A scheme map $f: X \to G$ can be extended to a scheme map $\bar{f}: Y \to G$ if and only if $f^{(p)}: X^{(p)} \to G^{(p)}$ maps* $\operatorname{Im}(F_Y)$ *into* $\operatorname{Im}(F_G)$.

The above results can be dualized. The V-map $V_C: C \to k^{1/p} \otimes C$ of a cocommutative coalgebra C was introduced by Heyneman and Sweedler [2, 4.1] as the dual concept to the F-map of commutative algebras. The following is dual to Theorem 1.1.

THEOREM 3.4. *Let H be a cocommutative Hopf algebra, let C be a cocommutative coalgebra, and $D \subset C$ a subcoalgebra such that* $\operatorname{Im}(V_C) \subset k^{1/p} \otimes D$. *A coalgebra map $f: D \to H$ can be extended to a coalgebra map $\bar{f}: C \to H$ if and only if $k^{1/p} \otimes f$ maps* $\operatorname{Im}(V_C)$ *into* $\operatorname{Im}(V_H)$.

The structure theorem of irreducible cocommutative Hopf algebras whose V-map is surjective [2, 4.2.7] follows immediately from the above. There is also an intimate relation between the above theorem and the extension theorem of sequences of divided powers [10].

Both Theorems (1.1) and (3.4) are proved similarly. We use the splitting property of subgroup schemes of affine group schemes killed by the Frobenius map and the corresponding property for cocommutative Hopf algebras killed by the V-map.

We work over a fixed field k of characteristic $p > 0$. All schemes, algebras, coalgebras, and so on are over k. We shall use the terminology of [6] for Hopf algebras.

1. COMMUTATIVE HOPF ALGEBRAS

If A is a commutative algebra, the $k^{1/p}$-algebra $k^{1/p} \otimes A$ can be viewed as a k-algebra via

$$k \to k^{1/p} \otimes A, \qquad \lambda \mapsto \lambda^{1/p} \otimes 1.$$

This k-algebra will be denoted by $A^{(p)}$. We have an algebra map

$$F_A : A^{(p)} \to A, \qquad \lambda \otimes a \longmapsto \lambda^p a^p.$$

If $X = \mathrm{Spec}(A)$ the affine scheme of A, then $X^{(p)}$ will mean $\mathrm{Spec}(A^{(p)})$. The algebra map F_A induces a scheme map

$$F_X = \mathrm{Spec}(F_A) : X \to X^{(p)}$$

which is called the *Frobenius map* of X [1, pp. 270, 271]. We denote by $\mathrm{Im}(F_X)$ or $F(X)$ the closed subscheme $\mathrm{Spec}(kA^p)$ of $X^{(p)}$, where $kA^p = \mathrm{Im}(F_A)$.

If $\phi: A \to B$ is a map of commutative algebras, $\phi^{(p)}: A^{(p)} \to B^{(p)}$ denotes the induced algebra map $k^{1/p} \otimes \phi$. If $f: Y \to X$ is the corresponding map of affine schemes, $f^{(p)}: Y^{(p)} \to X^{(p)}$ denotes the scheme map corresponding to $\phi^{(p)}$.

The main theorem of this section is formulated as follows:

1.1 THEOREM. *Let A be a commutative Hopf algebra.*

(a) *Let D be a commutative algebra and $\phi: D \to A$ a surjective algebra map. If $\mathrm{Ker}(\phi) \cap kD^p = 0$, then ϕ has a section which is an algebra map.*

(b) *Let B, C be commutative algebras and $\varphi: C \to B$ a surjective algebra map such that $\varphi(x) = 0$ implies $x^p = 0$ for x in C. Then F_C factors as*

$$F_C : C^{(p)} \xrightarrow{\varphi^{(p)}} B^{(p)} \xrightarrow{F_C^B} C.$$

Let $f: A \to B$ be an algebra map. There is an algebra map $\bar{f}: A \to C$ such that $\varphi \circ \bar{f} = f$ if and only if

$$\mathrm{Ker}(F_A) \subset \mathrm{Ker}(F_C^B \circ f^{(p)}). \tag{1.1.1}$$

Before going into the proof, we will state how (1.1) will be proved, so that the logical structure of Section 1 is transparent at the onset.

First, we give the geometric meaning of (1.1) in (1.2), so (1.2) is equivalent to (1.1). Part (b) of (1.1) will follow from part (a) of (1.1) plus (1.3). Part (a) of (1.1) will follow from (1.4) plus (2.9), while (2.9) will follow from the main theorem of Section 2. Finally (1.6) to (1.9) are consequences of (1.1).

1.2. COROLLARY. *Let G be an affine group scheme.*

(a) *Let Z be an affine scheme containing G as a closed subscheme. If $F(G) = F(Z)$ as subschemes of $Z^{(p)}$, then there is a scheme map $Z \to G$ which is the identity on G.*

(b) *Let X be an affine scheme and $Y \subset X$ a closed subscheme. Assume $F(X) \subset Y^{(p)}$. A scheme map $h\colon Y \to G$ can be extended to a scheme map $\bar{h}\colon X \to G$ if and only if $h^{(p)}$ maps $F(X)$ into $F(G)$.*

Proof. Assume G, Z, X, Y correspond to A, D, C, B in (1.1). It is enough to check that the conditions in (1.1) are fulfilled. (a) $\mathrm{Ker}(\phi) \cap kD^p = 0$ if and only if $\phi\colon kD^p \simeq kA^p$ if and only if $F(G) = F(Z)$. (b) $x^p = 0$ for all $x \in \mathrm{Ker}(\varphi)$ if and only F_C factors through $\varphi^{(p)}$. Condition (1.1.1) implies that $f^{(p)}\colon A^{(p)} \to B^{(p)}$ induces a map of quotient algebras $kA^p \to F_C^B(B^{(p)}) = kC^p$. If h corresponds to f, this is equivalent to that $h^{(p)}$ maps $F(X)$ into $F(G)$. Q.E.D.

We begin the proof of (1.1). The "only if" part of (b) is clear, since $f = \varphi \circ \bar{f}$ will imply $F_C^B \circ f^{(p)} = F_C^B \circ \varphi^{(p)} \circ \bar{f}^{(p)} = F_C \circ \bar{f}^{(p)} = \bar{f} \circ F_A$. The "if" part will follow from (a) in view of the following proposition.

1.3. Proposition. *Let*

$$\begin{array}{ccc} A & \xleftarrow{\ \omega\ } & E \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ B & \xleftarrow{\ \varphi\ } & C \end{array}$$

be a pullback diagram of commutative algebras. Assume φ is surjective and $x^p = 0$ for all x in $\mathrm{Ker}(\varphi)$. *Condition* (1.1.1) *implies that ω is surjective and* $\mathrm{Ker}(\omega) \cap kE^p = 0$.

Proof. If φ is surjective, so is ω. Let

$$u\colon A^{(p)} \to E$$

be the algebra map defined by

$$g \circ u = F_C^B \circ f^{(p)}, \qquad \omega \circ u = F_A.$$

Then $\mathrm{Ker}(u) = \mathrm{Ker}(F_A) \cap \mathrm{Ker}(F_C^B \circ f^{(p)}) = \mathrm{Ker}(F_A)$ by (1.1.1). Since $u \circ \omega^{(p)} = F_E$, we have $\mathrm{Im}(F_E) \subset \mathrm{Im}(u)$. Hence $\mathrm{Im}(F_E) \cap \mathrm{Ker}(\omega) \subset \mathrm{Im}(u) \cap \mathrm{Ker}(\omega) = u(\mathrm{Ker}(F_A)) = 0$. Q.E.D.

To prove the "if" part of (1.1)(b), make a pullback diagram as above, where ω has an algebra section s by (1.1)(a). It is enough to put $\bar{f} = g \circ s$. We can reduce the proof of (1.1)(a) to the case when D is also a Hopf algebra and ϕ is a Hopf algebra map, in view of the following proposition.

1.4. Proposition. *With the assumption of* (1.1)(a), *there is a commutative Hopf algebra $\tilde{D}$, together with a surjective algebra map*

$\chi: \tilde{D} \to D$ *such that* (i) $\phi \circ \chi: \tilde{D} \to A$ *is a Hopf algebra map and* (ii) $\mathrm{Ker}(\phi \circ \chi) \cap k\tilde{D}^p = 0$.

Proof. There is a vector space V, together with a linear surjection $\pi: D \to V$ such that

$$(\phi, \pi): D \simeq A \times V.$$

Let $C(V)$ be the cofree coalgebra on V [6, p. 125], and let $\tilde{D} = A \sqcap C(V)$ be the direct product of coalgebras with canonical projections

$$A \xleftarrow{\Phi} \tilde{D} \xrightarrow{\Pi} V.$$

It satisfies the following universal mapping property: For any coalgebra C and any pair (h_1, h_2), where $h_1: C \to A$ is a coalgebra map and $h_2: C \to V$ a linear map, there is a unique coalgebra map $h: C \to \tilde{D}$ such that $h_1 = \Phi \circ h$, $h_2 = \Pi \circ h$. Define a linear map $\chi: \tilde{D} \to D$ by the condition $\phi \circ \chi = \Phi$, $\pi \circ \chi = \Pi$. Let (m_A, u_A) and (m_D, u_D) denote the algebra structures of A and D. Using the above universal mapping property, we can define coalgebra maps

$$\tilde{m}: \tilde{D} \otimes \tilde{D} \to \tilde{D}, \qquad \tilde{u}: k \to \tilde{D}$$

by the condition

$$\Phi \circ \tilde{m} = m_A \circ (\Phi \otimes \Phi), \qquad \Pi \circ \tilde{m} = \pi \circ m_D \circ (\chi \otimes \chi),$$
$$\Phi \circ \tilde{u} = u_A, \qquad \Pi \circ \tilde{u} = \pi \circ u_D.$$

It follows that $\chi: \tilde{D} \to D$ commutes with the algebra structures. Using this, one can easily check the associativity and the unit condition for $(\tilde{m}, \tilde{u})$. Thus, $\tilde{D}$ becomes a bialgebra which is obviously commutative, and $\phi \circ \chi$ $(= \Phi)$: $\tilde{D} \to A$ is a bialgebra map. All we have to prove is (1) surjectivity of χ, (2) $\mathrm{Ker}(\Phi) \cap k\tilde{D}^p = 0$, and (3) the existence of an antipode of $\tilde{D}$. (1) Let $A \oplus V$ be the coalgebra extension of A obtained by adjoining V as primitive elements. There is a coalgebra map $h: A \oplus V \to \tilde{D}$ such that $\chi \circ h$ is the identity map. Hence χ is surjective. (2) Since Φ is a coalgebra map, $I = \mathrm{Ker}(\Phi) \cap k\tilde{D}^p$ is a coideal of $\tilde{D}$ and we have $\chi(I) \subset \mathrm{Ker}(\phi) \cap kD^p = 0$. $\mathrm{Ker}(\chi)$ contains no non-zero coideal by the universal mapping property for $\tilde{D}$. Hence $I = 0$. (3) $k\tilde{D}^p$ has an antipode, since it is isomorphic to kA^p. Thus $\tilde{D}^{(p)}$ modulo a nil biideal has an antipode. Hence $\tilde{D}^{(p)}$ has an antipode by the following Lemma 1.5. It follows that $\tilde{D}$ has an antipode. Q.E.D.

1.5. LEMMA. *Let A be a commutative bialgebra and $I \subset A$ a nil biideal. If A/I has an antipode, then A has an antipode.*

Proof. By [7, Corollary 69, p. 582], it is enough to prove that any group-like element $g \in A$ is invertible. By assumption g is invertible modulo I. Since I is nil, g itself is invertible. Q.E.D.

The proof of (1.1)(a) in case when D is a Hopf algebra and ϕ is a Hopf algebra map will be done in Section 2. We will need the splitting property of subgroup schemes of affine group schemes killed by the Frobenius map.

We give several consequences of Theorem 1.1.

A commutative algebra A is called *smooth* [4, (28.D), p. 200] if for any surjective map of commutative algebras $\varphi: C \to B$ with nilpotent kernel and for any algebra map $f: A \to B$, there is an algebra map $\bar{f}: A \to C$ such that $\varphi \circ \bar{f} = f$. We say A is *strongly smooth* if for any surjective map of commutative algebras $\varphi: C \to B$ with *bounded nil* kernel (which means that there is an integer $n > 0$ such that $x^n = 0$ for all $x \in \mathrm{Ker}(\varphi)$) the above lifting property is fulfilled.

1.6. COROLLARY. *Let A be a commutative Hopf algebra. If F_A is injective, A is a strongly smooth algebra.*

Proof. It is enough to check the above lifting property with a surjective map of commutative algebras $\varphi: C \to B$ such that $x^p = 0$ for any $x \in \mathrm{Ker}(\varphi)$. Since condition (1.1.1) is empty, the claim follows by (1.1)(b). Q.E.D.

The restriction saying that $\mathrm{Ker}(\varphi)$ is *bounded* nil is indispensable, as the following example shows.

1.7. EXAMPLE. Let A be the commutative algebra generated by elements $x_1, x_2, \ldots$, with defining relations $x_i = x_{i+1}^p$, $i = 1, 2, \ldots$, and let $\tilde{A}$ be the commutative algebra generated by elements $y_1, y_2, \ldots$, with defining relation $y_1^p = y_2^{p^2} = \cdots = y_i^{p^i} = \cdots$. A has a Hopf algebra structure, F_A is injective, and the algebra map $\phi: \tilde{A} \to A$, $\phi(y_i) = x_i$ is surjective with nil kernel. However, there is no algebra section of ϕ.

Proof. One of the possible Hopf algebra structures on A is given by letting all x_i primitive elements. F_A is clearly injective. $\mathrm{Ker}(\phi)$ is generated by nilpotent elements $y_i - y_{i+1}^p$, $i = 1, 2, \ldots$. Let $R = k[y_1]$ which is a polynomial ring. The set of all monomials $\prod_{i=2}^{\infty} y_i^{e_i}$, where $\{e_i\}$ is a sequence of integers of finite support with $0 \leqslant e_i < p^i$, forms a free basis of the R-module $\tilde{A}$. It follows that for $j = 1, 2, \ldots$, the subalgebra $R\tilde{A}^{p^j}$ is generated over R by those monomials $\prod_{i=2}^{\infty} y_i^{e_i}$ such that $p^j \mid e_i$ and $0 \leqslant e_i < p^i$. This means

$$\bigcap_{j=1}^{\infty} R\tilde{A}^{p^j} = R.$$

Therefore, if $s: A \to \tilde{A}$ is an algebra map, all elements $s(x_i)$ must be in R; hence $s(A) \subset R$. Since $\phi(R) \neq A$, it follows that there is no section of ϕ.

Q.E.D.

Let A be a commutative algebra with augmentation $\varepsilon: A \to k$ and let $M = \mathrm{Ker}(\varepsilon)$. The multiplication in the symmetric A-algebra $S_A M$ will be denoted by

$$m_1 * \cdots * m_r \qquad \text{for} \quad m_1, \ldots, m_r \in M$$

in order to distinguish from the multiplication in M. The F-map for the non-unital algebra M, which is defined similarly as unital algebras, factors as follows,

$$F_M : M^{(p)} \xrightarrow{f_M} S_A^p M \xrightarrow{\mu_{p,2}} S_A^2 M \xrightarrow{\mu_{2,1}} M,$$

where

$$f_M(\lambda \otimes m) = \lambda^p m * \cdots * m \qquad (p \text{ times}),$$

$$\mu_{p,2}(m_1 * \cdots * m_p) = m_1 \cdots m_{p-1} * m_p,$$

$$\mu_{2,1}(m_1 * m_2) = m_1 m_2$$

for $\lambda \in k^{1/p}$, $m, m_1, \ldots, m_p \in M$. We have a complex

$$\mathrm{Ker}(F_M) \xrightarrow{\mu_{p,2} \circ f_M} S_A^2 M \xrightarrow{\mu_{2,1}} M. \tag{1.8.1}$$

1.8. Proposition. *Let A be a commutative Hopf algebra. Let $M = \mathrm{Ker}(\varepsilon)$ where $\varepsilon: A \to k$ is the counit. Complex* (1.8.1) *is exact. If F_A is injective, $\mu_{2,1}$ is injective.*

Proof. Let $q: S_A^2 M \to k$ be a linear map. Define the product on $A \oplus k$

$$(a, x)(b, y) = (ab, \varepsilon(a)y + \varepsilon(b)x + q(a^+ * b^+)), \qquad a, b \in A,\ x, y \in k,$$

where $a^+ = a - \varepsilon(a)$, and get a commutative associative algebra $A \oplus_q k$ with identity $(1, 0)$. This is a special case of Hochschild ring extensions [4, (25.C), p. 178]. There is the algebra projection $\pi: A \oplus_q k \to A$, $\pi(a, x) = a$, with $\mathrm{Ker}(\pi)^2 = 0$. We have $\mathrm{Ker}(\pi) \cap k(A \oplus_q k)^p = 0$ if and only if $q = 0$ on $\mu_{p,2} \circ f_M(\mathrm{Ker}(F_M))$. If this is the case, π has an algebra section $s: A \to A \oplus_q k$ by (1.1)(a). Write $s(a) = (a, l(a))$ for $a \in A$. Then $l(1) = 0$ and $l(m_1 m_2) = q(m_1 * m_2)$ for $m_1, m_2 \in M$. Thus $q = l \circ \mu_{2,1}$. This means the dual complex of (1.8.1) is exact. Hence it is exact. The last statement is clear.

Q.E.D.

As the above proof shows, the injectivity of $\mu_{2,1}$ is a consequence of smoothness of A, rather than of the injectivity of F_A. More precisely, $\mu_{2,1}$ is injective if and only if the Hochschild extension $A \oplus_q k$ of A splits (i.e., there is an algebra section $A \to A \oplus_q k$ of A splits (i.e., there is an algebra section $A \to A \oplus_q k$) for any linear map $q: S_A^2 M \to k$. We claim that *A is formally smooth with respect to the M-adic topology* [4, (28.C), p. 198] *if $\mu_{2,1}$ is injective.* Let $\varphi: C \to B$ be a surjective map of commutative algebras with $\mathrm{Ker}(\varphi)^2 = 0$. Let $f: A \to B$ be an algebra map such that $f(M^i) = 0$ for some $i > 0$. We must show that f can be lifted to an algebra map $A \to C$. Let $I = \mathrm{Ker}(\varphi)$ which is a B-module, and hence an A-module. In order to lift f to $A \to C$, it is enough to lift it successively to $A \to C/MI$, $A \to C/M^2I$, and so on. Hence we can assume $MI = 0$. There is a linear lifting $f': A \to C$ with $f'(1) = 1$. The map $(m_1, m_2) \mapsto f'(m_1) f'(m_2) - f'(m_1 m_2)$, for $m_1, m_2 \in M$ induces a linear map $q: S_A^2 M \to I$. If we write $q = h \circ \mu_{2,1}$ with a linear map $h: M \to I$, then

$$\bar{f}: A \to C, \qquad \bar{f}(a) = f'(a) + h(a - \varepsilon(a))$$

will become a lifted algebra map. This proves the claim.

Assume A is finitely generated, or more generally A_M (localization at M) is notherian. It follows from [1, 4.2, p. 109; 4, (28.M), p. 207] that A is M-adically smooth if and only if $\mathrm{Spec}(A)$ is smooth at M (in the sense of [1, 4.1, p. 108]). If A is a Hopf algebra and ε is the counit, then the smoothness at M (or at e) implies the whole smoothness of A [1, 2.1, p. 238] and the injectivity of F_A.

Summarizing the above, we get the following.

1.9. Proposition. *Let A be a commutative algebra with augmentation $\varepsilon: A \to k$, and let $M = \mathrm{Ker}(\varepsilon)$.*

(i) *F_A is injective.*

(ii) *A is smooth.*

(iii) *$\mu_{2,1}$ is injective.*

(iv) *A is M-adically smooth.*

We have (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv). *If A is a Hopf algebra,* (i) $\Rightarrow$ (ii). *If A is a finitely generated Hopf algebra with counit ε, then* (i) *through* (iv) *are equivalent with one another.*

The last statement is false, unless A is finitely generated. Take the algebra A of (1.7) for instance. Since we have $M = M^2$, where $M = (x_1, x_2, \ldots)$, every quotient algebra of A is M-adically smooth. In particular $A/(x_1^p)$, which has a Hopf algebra structure, is M-adically smooth. Nevertheless, the projection $A/(x_1^{p^2}) \to A/(x_1^p)$ has no algebra section.

2. Affine Group Schemes Killed by the Frobenius Map

There is a categorical correspondence between affine algebraic groups G whose Frobenius map F_G is trivial, and finite dimensional p-Lie algebras L given as follows [1, 4.1, p. 282]: Let $U^{[p]}(L)$ be the restricted universal enveloping algebra of L. It has the Hopf algebra structure with L as the set of primitive elements. Let $U^{[p]}(L)^*$ be the dual Hopf algebra which is commutative. The equivalence is given by $L \mapsto \mathrm{Spec}(U^{[p]}(L)^*)$ and $G \mapsto \mathrm{Lie}(G)$ (the Lie algebra of G).

Let L be a finite dimensional p-Lie algebra and let $L' \subset L$ be a p-Lie subalgebra. If $\{x_1,..., x_n\}$ is a basis of L modulo L', then the set of elements $x_1^{e_1} \cdots x_n^{e_n}$ with $0 \leqslant e_i < p$ spans a subcoalgebra C of $U^{[p]}(L)$. The restricted Poincaré–Birkhoff–Witt theorem [1, 3.6, p. 277] implies that the multiplication of $U^{[p]}(L)$ induces an isomorphism of coalgebras

$$C \otimes U^{[p]}(L') \simeq U^{[p]}(L).$$

This has the following geometric meaning:

2.1. Proposition. *Let G be an affine algebraic group such that F_G is trivial, and let $H \subset G$ be a closed subgroup scheme. There is a closed subscheme $X \subset G$ such that the multiplication of G induces an isomorphism of affine schemes*

$$X \times H \simeq G.$$

The purpose of this section is to generalize (2.1) to those G which are not necessarily algebraic. Using it, we can finish the proof of (1.1)(a).

For an affine group G and a closed subgroup scheme $H \subset G$, we denote by G/H the cokernel in the category of "dur" sheaves $\underset{\approx}{M}_k E$ of the diagram

$$G \times H \underset{\text{projection}}{\overset{\text{product}}{\rightrightarrows}} G$$

which is denoted by $\overset{\approx}{G/H}$ in [1, 7.2, p. 353]. As a consequence of [1, 1.5, p. 362] we have the following:

2.2. Lemma. *There is a closed subscheme $X \subset G$ such that $X \times H \simeq G$ if and only if G/H is affine and the projection $G \to G/H$ has a section.*

More precisely we have the following:

2.3. Lemma. *Assume G/H is affine. There is a 1–1 correspondence between closed subschemes $X \subset G$ such that $X \times H \simeq G$ and sections*

$s\colon G/H \to G$ given by $X \mapsto s_X$ and $s \mapsto \mathrm{Im}(s)$, where the section s_X associated with X is induced by the composite

$$G \simeq X \times H \xrightarrow{\text{proj.}} X \hookrightarrow G.$$

The proof is easy and omitted.

We have given in [9, Theorem 10, p. 465] the following criterion to know when G/H is affine.

2.4. PROPOSITION. *G/H is affine if and only if the affine ring $O(G)$ is a faithfully coflat left (or equivalently right) $O(H)$-comodule.*

An affine group scheme is called *pro-finite* if all of its algebraic quotients are finite. For example, those affine groups which are killed by the Frobenius map are pro-finite in view of the categorical correspondence described in the beginning of this section.

2.5. LEMMA. *Let G be a pro-finite group scheme. For any closed subgroup scheme $H \subset G$, G/H is affine.*

Proof. We use (2.4). If G is finite, $O(G)^*$ is a left (or right) faithfully flat $O(H)^*$-module by [8, Theorem 3.1, p. 253]. This means $O(G)$ is a faithfully coflat $O(H)$-comodule. In general, let $A = O(G)$ and $A/I = O(H)$, where I is a Hopf ideal of A. A is the union of finite dimensional Hopf subalgebras A_λ, and A_λ is a faithfully coflat A_λ/I_λ-comodule, where $I_\lambda = A_\lambda \cap I$. Since $A/I = \varinjlim_\lambda A_\lambda/I_\lambda$, it follows easily that A is a faithfully coflat A/I-comodule.
Q.E.D.

2.6. THEOREM. *Let G be an affine group scheme such that F_G is trivial. For any closed subgroup scheme $H \subset G$, G/H is affine and the projection $G \to G/H$ has a section.*

Proof. Since G is pro-finite, we have only to prove the existence of a section.

We begin with the case when H is algebraic. There is a closed normal subgroup scheme $N \lhd G$ such that $N \cap H = (e)$ and G/N is algebraic. Apply (2.1) to G/N which contains H as a closed subgroup, and get a closed subscheme $Y \subset G/N$ such that

$$Y \times H \simeq G/N$$

Let $X \subset G$ be the inverse image of Y. Then we have

$$X \times H \simeq G.$$

Let H be arbitrary. Let Λ be the set of all pairs (N, X), where $N \lhd G$ is a closed normal subgroup scheme and $X \subset G/N$ is a closed subscheme such that

$$X \times HN/N \simeq G/N.$$

In view of (2.3), we can also define Λ to be the set of all pairs (N, s) where $N \lhd G$ closed and

$$s\colon G/HN \to G/N$$

is a section to the projection $G/N \to G/HN$. We give the following ordering on Λ: Let (N, X) and (N', X') be two elements in Λ. $(N, X) \leqslant (N', X')$ if $N \supset N'$ and the projection $G/N' \to G/N$ maps X' into X. This is equivalent to saying that

$$\begin{array}{ccc} G/HN' & \xrightarrow{s_{X'}} & G/N' \\ \downarrow & & \downarrow \\ G/HN & \xrightarrow{s_X} & G/N \end{array}$$

commutes, where the vertical maps denote the projections.

The ordered set Λ is inductive. Let (N_α, X_α), $\alpha \in I$ be a chain in Λ. Take the projective limit $\varprojlim_\alpha$ of

$$X_\alpha \times HN_\alpha/N_\alpha \simeq G/N_\alpha$$

and get

$$X \times HN/N \simeq G/N,$$

where $N = \bigcap_\alpha N_\alpha$. ($G/N = \varprojlim_\alpha G/N_\alpha$ will follow from [1, 7.5, p. 355], and $H/H \cap N = \varprojlim_\alpha H/H \cap N_\alpha$ similarly. The latter means $HN/N = \varprojlim_\alpha HN_\alpha/N_\alpha$, since $HN/N = H/H \cap N$ [1, 3.7(c), p. 332].) Thus (N, X) is an element in Λ which is larger than every (N_α, X_α).

Let (N, X) be a maximal element in Λ. We derive a contradiction by assuming $N \neq (e)$. There is a closed normal subgroup scheme $K \lhd G$ such that G/K is algebraic and $N \not\subset K$. Let $N_0 = N \cap K$ which is normal in G and properly contained in N. N/N_0 is algebraic. Look at the following diagram,

$$\begin{array}{ccc} G/N & \underset{p}{\overset{s_X}{\rightleftarrows}} & G/HN \\ {\scriptstyle f}\downarrow\uparrow{\scriptstyle q} & & \uparrow{\scriptstyle q'} \\ G/N_0 & \xrightarrow[p_0]{} & G/HN_0 \end{array}$$

where p, q, p_0, q' are the canonical projections. q has a section f, since N/N_0 is an algebraic subgroup of G/N_0. Let $l = f \circ s_X \circ q' : G/HN_0 \to G/N_0$. Then $q' \circ p_0 \circ l = q'$. Using the canonical left action of G/N_0 on G/HN_0, we have

$$q'(l(x)^{-1} \cdot x) = q'(e) \qquad \text{for all} \quad x \in (G/HN_0)(R)$$

with commutative algebra R. This means

$$l(x)^{-1} \cdot x \in (HN/HN_0)(R).$$

Since N/N_0 is algebraic, the projection

$$N/N_0 \to HN/HN_0$$

has a section. Hence, there is a scheme map

$$t: G/HN_0 \to N/N_0$$

such that

$$p_0 \circ t(x) = l(x)^{-1} \cdot x, \qquad x \in (G/HN_0)(R).$$

Define a scheme map

$$s: G/HN_0 \to G/N_0$$

by $s(x) = l(x)\, t(x)$ for $x \in (G/HN_0)(R)$ with commutative algebra R, then we have

$$p_0 \circ s(x) = l(x) \cdot (p_0 \circ t(x)) = x,$$
$$q \circ s = q \circ l = s_X \circ q'.$$

Hence s is a section of p_0, and the pair (N_0, s) is strictly larger than (N, s_X), a contradiction.

Therefore $N = (e)$, and we have $X \times H \simeq G$. Q.E.D.

2.7. COROLLARY. *Let G be an affine group scheme and let $H \subset G$ be a closed subgroup scheme. If $F(G) = F(H)$ as subgroup schemes of $G^{(p)}$, then there exists a closed subscheme $X \subset G$ such that $X \times H \simeq G$.*

Proof. Let G^1 be the kernel of $F_G : G \to G^{(p)}$, and let $H^1 = H \cap G^1$. The hypothesis implies $G = G^1 \cdot H$. We know there is a closed subscheme $X \subset G^1$ with $X \times H^1 \simeq G^1$. It follows immediately that

$$X \times H \simeq G. \qquad \text{Q.E.D.}$$

2.8. COROLLARY. *With the assumption of* (2.7), *there is a scheme map* $r: G \to H$ *which is the identity on* H.

Proof. We can take X containing the identity element. We have only to compose the projection $X \times H \to H$ with the isomorphism $G \simeq X \times H$.

Q.E.D.

The last corollary has the following algebraic meaning (see (1.2)):

2.9. COROLLARY. *Let* A, D *be commutative Hopf algebras and let* $\phi: D \to A$ *be a surjective Hopf algebra map such that* $\operatorname{Ker}(\phi) \cap kD^p = 0$. *Then* ϕ *has a section which is an algebra map.*

This will finish the proof of (1.1)(a).

3. COCOMMUTATIVE HOPF ALGEBRAS

The V-map for a cocommutative coalgebra C

$$V_C : C \to k^{1/p} \otimes C$$

was introduced by Heyneman and Sweedler [2, 4.1] as the dual concept to the F-map of commutative algebras. It is a $1/p$-linear coalgebra map. We denote by $V(C)$ the image of V_C. If H is a cocommutative Hopf algebra, V_H is a $1/p$-linear Hopf algebra map. We give the dual results of Section 1, using the V-map instead of the Frobenius map.

3.1. LEMMA. *Let* H *be a cocommutative Hopf algebra with* $L = P(H)$ *the primitive elements.* $\operatorname{Ket}(V_H) = LH = HL$.

Proof. Since the V-map of $\bar{k} \otimes H$ is obtained from V_H by extending the scalars and $P_{\bar{k}}(\bar{k} \otimes H) = \bar{k} \otimes P(H)$, we can assume k is algebraically closed. Let G be the set of group-like elements in H and let H^1 be the irreducible component at 1. We know that $H \simeq k[G] \otimes H^1$. Since the V-map of $k[G]$ is an isomorphism, we can reduce to the case H is irreducible. That case is precisely [5, Theorem 1, p. 521]. Q.E.D.

3.2. PROPOSITION. *Let* H *be a cocommutative Hopf algebra and let* $H' \subset H$ *be a Hopf subalgebra. Let* $L = P(H)$ *and* $L' = P(H')$ *be the p-Lie algebras of primitive elements, and let* $U = U^{[p]}(L)$, $U' = U^{[p]}(L')$ *be the restricted universal enveloping algebras. If* $V(H) = V(H')$ *in* $k^{1/p} \otimes H$, *then the multiplication in* H *induces an isomorphism*

$$U \otimes_{U'} H' \simeq H.$$

Proof. This has been proved during the proof of [10, Theorem A] in case H is irreducible. But what we used there is the fact that $\mathrm{Ker}(V_H) = LH$. Hence, we can drop the irreducibility hypothesis in view of (3.1). Q.E.D.

We have the following splitting theorem for cocommutative Hopf algebras which is analogous to (2.7).

3.3. THEOREM. *Let H be a cocommutative Hopf algebra and let $H' \subset H$ be a Hopf subalgebra. If $V(H) = V(H')$, there is a subcoalgebra $C \subset H$ containing 1 such that the multiplication in H induces a coalgebra isomorphism*

$$C \otimes H' \simeq H.$$

In particular, there is a coalgebra projection $r: H \to H'$ which is the identity on H'.

Proof. With the notation of (3.2), let X be a basis of L modulo L'. Give an arbitrary total ordering on X and let C be the linear span of all elements $x_1^{e_1} \cdots x_n^{e_n}$, where $x_1 < \cdots < x_n$ in X and $0 \leqslant e_i < p$. Then C is a subcoalgebra of U and we have $C \otimes U' \simeq U$ by the restricted Poincaré–Birkhoff–Witt theorem. Applying the functor $(-) \otimes_{U'} H'$ to both sides, we get $C \otimes H' \simeq H$ in view of (3.2). Q.E.D.

We have the following analogue of (1.1) or (1.2).

3.4. THEOREM. *Let H be a cocommutative Hopf algebra.*

(a) *Let C be a cocommutative coalgebra containing H as a subcoalgebra. If $V(C) = V(H)$, there is a coalgebra projection $r: C \to H$ which is the identity on H.*

(b) *Let C be a cocommutative coalgebra and let $D \subset C$ be a subcoalgebra such that $V(C) \subset k^{1/p} \otimes D$. A coalgebra map $f: D \to H$ can be extended to a coalgebra map $\bar{f}: C \to H$ if and only if $k^{1/p} \otimes f$ maps $V(C)$ into $V(H)$.*

Proof. (a) Let $W \subset C$ be a linear subspace such that $C = H \oplus W$. Let $\tilde{H} = H \sqcup T(W)$ be the coproduct of algebras, where $T(W)$ denotes the tensor algebra of W, with canonical injections $i: H \to \tilde{H}$ and $j: W \to \tilde{H}$. Define a linear injection

$$\chi: C \hookrightarrow \tilde{H}$$

by $\chi \mid H = i$, $\chi \mid W = j$. With the coalgebra structures $(\Delta_H, \varepsilon_H)$ and $(\Delta_C, \varepsilon_C)$ of H and C, we define algebra maps

$$\tilde{\Delta}: \tilde{H} \to \tilde{H} \otimes \tilde{H}, \qquad \tilde{\varepsilon}: \tilde{H} \to k$$

as follows:

$$\tilde{\Delta} \circ i = (i \otimes i) \circ \Delta_H, \qquad \tilde{\Delta} \circ j = (\chi \otimes \chi) \circ \Delta_C \mid W,$$
$$\tilde{\varepsilon} \circ i = \varepsilon_H, \qquad \tilde{\varepsilon} \circ j = \varepsilon_C \mid W.$$

One sees that $\chi: C \hookrightarrow \tilde{H}$ is a coalgebra embedding, and it follows from this that $\tilde{H}$ becomes a cocommutative bialgebra. This construction is dual to (1.4). Since $\chi(C)$ generates $\tilde{H}$ as an algebra, $V(C) = V(H)$ implies $V(\tilde{H}) = V \circ \chi(H)$. In particular, there is no non-zero subcoalgebra $D \subset \tilde{H}$ such that $D \cap \chi(H) = 0$. Hence, all simple subcoalgebras of $\tilde{H}$ are contained in $\chi(H)$. Therefore $\tilde{H}$ becomes a Hopf algebra. There is a coalgebra projection $r: \tilde{H} \to H$ which is χ^{-1} on $\chi(H)$, by (3.3). Then, $r \circ \chi: C \to H$ is the required coalgebra projection.

(b) If f can be extended to $\bar{f}$, $k^{1/p} \otimes \bar{f}$ maps $V(C)$ into $V(H)$ and $k^{1/p} \otimes f$ equals $k^{1/p} \otimes \bar{f}$ on $V(C)$. This proves the "only if" part. To prove the "if" part, make the following pushout diagram of coalgebras (or linear spaces):

$$\begin{array}{ccc} D & \hookrightarrow & C \\ {\scriptstyle f}\big\downarrow & & \big\downarrow{\scriptstyle f'} \\ H & \hookrightarrow & E. \end{array}$$

By assumption, we have $V_C: C \to k^{1/p} \otimes D$. Define a $1/p$-linear coalgebra map

$$v: E \to k^{1/p} \otimes H$$

by the conditions: $v \mid H = V_H$, $v \circ f' = (k^{1/p} \otimes f) \circ V_C$. Then, V_E factors as

$$V_E: E \xrightarrow{v} k^{1/p} \otimes H \hookrightarrow k^{1/p} \otimes E$$

since we have $V_E \mid H = v \mid H$ and $V_E \circ f' = v \circ f'$ by the definition of v. Since $E = H + f'(C)$, we have

$$V(E) = v(E) = V(H) + v \circ f'(C) = V(H) + (k^{1/p} \otimes f) \circ V(C) \quad \text{in } k^{1/p} \otimes H.$$

Hence $V(E) = V(H)$ if and only if $k^{1/p} \otimes f$ maps $V(C)$ into $V(H)$. If $V(E) = V(H)$, there is a coalgebra map $r: E \to H$ which is the identity on H, by (a). We have only to put $\bar{f} = r \circ f'$. Q.E.D.

We give several consequences of the above theorem.

For a real number α, let $[\alpha]$ denote the largest integer $\leqslant \alpha$.

3.5. LEMMA. *Let C be a cocommutative coalgebra with coradical filtration $\{C_n\}$. We have*

$$V(C_n) \subset k^{1/p} \otimes C_{[n/p]}$$

Proof. Since C is the union of finite dimensional subcoalgebras, we can asuume C is finite dimensional. Let A be the dual algebra with radical M. F_A induces a map of quotient algebras

$$F_A : (A/M^i)^{(p)} \to A/M^{ip}$$

for any $i > 0$. Since C_n is the dual of A/M^{n+1}, this means that

$$V(C_{ip-1}) \subset k^{1/p} \otimes C_{i-1} \qquad \text{for} \quad i > 0.$$

Since $n < (e+1)p$ with $e = [n/p]$, we have $n \leqslant (e+1)p - 1$. Hence

$$V(C_n) \subset V(C_{(e+1)p-1}) \subset k^{1/p} \otimes C_e. \qquad \text{Q.E.D.}$$

3.6. THEOREM. *Let H be a cocommutative Hopf algebra such that $V_H : H \to k^{1/p} \otimes H$ is surjective.*

(a) *If C is a cocommutative coalgebra containing H as a subcoalgebra, there is a coalgebra projection $r: C \to H$ which is the identity on H.*

(b) *Let C be a cocommutative coalgebra and let $D \subset C$ be a subcoalgebra. Any coalgebra map $f: D \to H$ can be extended to a coalgebra map $\bar{f}: C \to H$.*

Proof. Part (b) follows directly from (a). To prove (a), write C as a direct sum of subcoalgebras $C = C' \oplus C''$, where $C' = H^{(\infty)}$ [3, p. 223]. Since there is at least one coalgebra map, $C'' \to H$ (e.g., $c \mapsto \varepsilon(c)1$), we may assume $C = C'$, or H contains the coradical C_0. Let $\{C_n\}$ be the coradical filtration of C. We define coalgebra maps $f_n : C_n + H \to H$ inductively. Begin with $f_0 =$ the identity. Assume f_n is defined. Since

$$V(C_{n+1} + H) \subset k^{1/p} \otimes (C_n + H)$$

by (3.5), we can extend f_n to a coalgebra map $f_{n+1} : C_{n+1} + H \to H$ by (3.4)(b). (Use the fact $V(H) = k^{1/p} \otimes H$.) Taking the inductive limit of $\{f_n\}$, we get the required coalgebra projection: $C \to H$. Q.E.D.

The above theorem may be viewed as the coalgebraic analogue of (1.6), but it is much stronger than that.

The following characterization of irreducible cocommutative Hopf algebras whose V-map is surjective is a direct consequence of the above.

3.7 COROLLARY [2, 4.2.7, p. 289]. *Let H be a cocommutative irreducible Hopf algebra with $U = P(H)$ and $H^+ = \mathrm{Ker}(\varepsilon)$. Let $\pi: H^+ \to U$ be a linear projection. $V_H: H \to k^{1/p} \otimes H$ is surjective if and only if (H, π) is the cofree cocommutative pointed irredicible coalgebra on U.*

Proof. Let $B(U)$ be the cofree cocommutative pointed irreducible coalgebra on U [6, 12.2.5, p. 263]. The projection π induces a coalgebra imbedding

$$\phi: H \hookrightarrow B(U)$$

which is the identity on U. If ϕ is an isomorphism, V_H is obviously surjective. If V_H is surjective, there is a coalgebra map $r: B(U) \to H$ such that $r \circ \phi$ is the identity map of H, by (3.6). Since $r \mid U$ must be the identity map, r is injective by [6, 11.0.1, p. 217]. It follows that ϕ and r are isomorphisms of coalgebras. Q.E.D.

The coalgebraic counterpart of (1.8) is as follows: For a cocommutative coalgebra C with one specified group-like element 1, let $C^+ = \mathrm{Ker}(\varepsilon)$,

$$\delta: C^+ \to C^+ \otimes C^+, \qquad \delta(c) = \Delta(c) - c \otimes 1 - 1 \otimes c$$

and iterate δ n-times to get

$$\delta_n: C^+ \to \bigotimes^{n+1} C^+.$$

The V-map for C restricted on C^+ factors as follows: For each integer $n > 0$, let $\Box_s^n C^+$ be the set of all symmetric tensors $\sum_i c_{i1} \otimes \cdots \otimes c_{in}$ in $\bigotimes^n C^+$ such that

$$\sum_i c_{i1} \otimes \cdots \otimes \delta(c_{ij}) \otimes \cdots \otimes c_{in}$$

are the same for $j = 1, \ldots, n$. (This is the dual concept of $S_A^n M$.) Then we have

$$V_C: C^+ \xrightarrow{\delta} \Box_s^2 C^+ \xrightarrow{\delta_{p-2} \otimes I} \Box_s^p C^+ \xrightarrow{v} k^{1/p} \otimes C^+,$$

where the $1/p$-linear map v is defined in [2, 4.1.1(a), p. 273] (where denoted by V) as the dual map of

$$f_M: M^{(p)} \to S_A^p M.$$

We put

$$\bar{v} = v \circ (\delta_{p-2} \otimes I): \Box_s^2 C^+ \to k^{1/p} \otimes C^+.$$

3.8. COROLLARY (to (3.4)) [10, Theorem C]. *Let H be a cocommutative Hopf algebra. With respect to the identity* 1 *as the specified group-like element, we have*

$$\delta(H^+) = \{u \in \square_s^2 C^+ \mid \bar{v}(u) \in V(H)\}.$$

Proof. $\delta(C^+)$ is obviously contained in the right-hand side. If u is in the right-hand side, make a coalgebra $C = H \oplus kz$ with condition

$$\Delta(z) = z \otimes 1 + 1 \otimes z + u, \qquad \varepsilon(z) = 0.$$

Then C is cocommutative and

$$V(z) = \bar{v}(u) \in V(H).$$

Hence there is a coalgebra retract $r: C \to H$. We have $u = \delta(r(z)) \in \delta(H^+)$.

Q.E.D.

We have shown in the previous paper [10] that the above result leads to a very simple proof of the extension theorem of sequences of divided powers.

REFERENCES

1. M. DEMAZURE AND P. GABRIEL, Groupes algébriques, Tome I, Masson & Cie, Paris; North-Holland, Amsterdam, 1970.
2. R. G. HEYNEMAN AND M. E. SWEEDLER, Affine Hopf algebras, II, *J. Algebra* **16** (1970), 271–297.
3. R. G. HEYNEMAN AND D. E. RADFORD, Reflexity and coalgebras of finite type, *J. Algebra* **28** (1974), 215–246.
4. H. MATSUMURA, "Commutative Algebra," Second ed., Benjamin-Cummings, Reading, Mass., 1980.
5. M. E. SWEEDLER, Hopf algebras with one group-like element, *Trans. Amer. Mat. Soc.* **127** (1967), 515–526.
6. M. E. SWEEDLER, "Hopf Algebras," Benjamin, NewYork, 1969.
7. M. TAKEUCHI, Free Hopf algebras generated by coalgebras, *J. Math. Soc. Japan* **23** (1971), 561–582.
8. M. TAKEUCHI, A correspondence between Hopf ideals and sub-Hopf algebras, *Manuscripta Math.* **7** (1972), 251–270.
9. M. TAKEUCHI, Relative Hopf modules, *J. Algebra* **60** (1979), 452–471.
10. M. TAKEUCHI, A simple proof of the extension theorem of sequences of divided powers in characteristic *p*, *Proc. Amer. Math. Soc.* **84** (1982), 125–128.