HOPF ALGEBRAS WITH ONE GROUPLIKE ELEMENT

BY

MOSS EISENBERG SWEEDLER[1]

Introduction. We are interested in the coalgebra structure of cocommutative Hopf algebras. Over an algebraically closed field a cocommutative Hopf algebra K with antipode is of the form $H \otimes \Gamma(G)$ (as a coalgebra) where $\Gamma(G)$ is the group algebra of G the group of grouplike elements—elements of K where $dg = g \otimes g$—and H is the unique maximal sub-Hopf algebra of K containing one grouplike element, namely 1. If the characteristic of the field is zero then H is isomorphic to the universal enveloping algebra of its primitive elements—elements where $dx = 1 \otimes x + x \otimes 1$—which form a Lie algebra. These results of Kostant prompt the present study of H when the characteristic is not zero.

We do not insist the field be algebraically closed but merely that the unique simple subcoalgebra of our Hopf algebra is the 1-dimensional space spanned by the unit. In this case the subalgebra generated by the primitive elements is a restricted universal enveloping algebra but not necessarily the entire Hopf algebra. A necessary and sufficient condition for H to be primitively generated is that for all $a' \in H'$ (the dual to H which has a natural algebra structure) where $\langle a', 1\rangle = 0$ then $a'^p = 0$, p the characteristic of the field. When the field is perfect H modulo the left ideal generated by the primitives (the ideal is actually two-sided) with its vector space structure altered is isomorphic to a sub-Hopf algebra of H.

The main results come from the study of divided powers. ${}^0x, {}^1x, \ldots, {}^tx$ is a sequence of divided powers if for $n = 0, \ldots, t$, $d({}^nx) = \sum_{i=0}^{n} {}^ix \otimes {}^{n-i}x$; in characteristic zero if x is primitive, letting ${}^ix = x^i/i!$ gives an infinite sequence of divided powers. We prove a generalization of the Birkhoff-Witt theorem in which divided powers replace ordinary powers.

The results obtained here on Hopf algebras and divided powers are used in an extension of Galois theory to include all finite normal field extensions. A Hopf algebra replaces the Galois group. The Hopf algebra is the group algebra of the Galois group in case the field extension is separable. If the extension is purely inseparable the Hopf algebra has only one grouplike element. These results will appear in a subsequent paper.

In the area of algebraic groups divided powers are of interest since certain infinite sequences of divided powers correspond to oneparameter subgroups.

Received by the editors April 13, 1966.

[1] The research for the first four sections was done while the author held an NSF Graduate Fellowship.

When C is a cocommutative coalgebra C' is a commutative algebra which determines a scheme $X = \operatorname{Spec} C'$. The requirement that C have one grouplike element is equivalent to C' being a local augmented algebra or X being a local scheme with a unique section $\operatorname{Spec} k \to X$, where k is the ground field. We have not chosen to follow the geometric approach since our techniques are fundamentally coalgebraic and since in the last section we study coanticommutative graded Hopf algebras with one grouplike element which arise in algebraic topology.

Over an algebraically closed field a coanticommutative graded Hopf algebra K which has an antipode is of the form $F \otimes \Gamma(G)$ (as a coalgebra) where G is the group of grouplike elements and F is a unique maximal sub-Hopf algebra with one grouplike element; thus we are studying F. F contains a unique maximal evenly graded sub-Hopf algebra H. If E is the exterior algebra on the space spanned by the odd primitive elements then F is isomorphic to $H \otimes E$ as a coalgebra. This last section with the previous section implies $F = \otimes_\gamma C_\gamma$ as a coalgebra (where each C_γ is a coalgebra) when the even primitives of F satisfy the nested basis condition of Theorem 3. This is always the case if F is of finite type. Moreover, each C_γ can be given an algebra structure by which it is a Hopf algebra and the result $F = \otimes_\gamma C_\gamma$ as a coalgebra does not depend upon the algebra structure of F being associative. Thus we have a generalization of the dual to Borel's theorem.

1. By Hopf algebra we mean a vector space H over the field k of characteristic p; where $\mu: k \to H$, $m: H \otimes H \to H$ give H an algebra structure; $\varepsilon: H \to k$, $d: H \to H \otimes H$ give H a coalgebra structure and ε, d are algebra (homo)morphisms.

If C is a coalgebra and $c \in C$ we will write $\sum_{(c)} c_{(1)} \otimes c_{(2)}$ to denote $d_C(c)$, $\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}$ denotes $(I \otimes d_C)d_C(c)$, etc. Let $f: C \oplus \cdots \oplus C \to V$ be an n-linear map which induces the linear map $\bar{f}: C \otimes \cdots \otimes C \to V$. We write $\sum_{(c)} f(c_{(1)}, \ldots, c_{(n)})$ to denote $\bar{f}(\sum_{(c)} c_{(1)} \otimes \cdots \otimes c_{(n)})$.

If C is a coalgebra, A an algebra then $\operatorname{Hom}(C, A)$ has a natural algebra structure; if $f, g \in \operatorname{Hom}(C, A)$, $f * g = m_A \circ (f \otimes g) \circ d_C$, the unit is $\mu_A \varepsilon_C$. Often we identify k with its image under μ_A in which case $\varepsilon = \varepsilon_C$ is the identity of $\operatorname{Hom}(C, A)$. In particular $C' = \operatorname{Hom}(C, k)$ is an algebra. C is a left C'-module where

$$a' \cdot c = \sum_{(c)} c_{(1)} \langle a', c_{(2)} \rangle,$$

for $a' \in C'$, $c \in C$. This action satisfies $\langle a'b', c \rangle = \langle a', b' \cdot c \rangle$ and

$$d(a' \cdot c) = \sum_{(c)} c_{(1)} \otimes a' \cdot c_{(2)}. \tag{1}$$

Until §5 we assume all coalgebras and Hopf algebras under discussion are cocommutative, i.e., $\sum_{(c)} c_{(1)} \otimes c_{(2)} = \sum_{(c)} c_{(2)} \otimes c_{(1)}$ for all $c \in C$. In this case C' is a commutative algebra.

C is called *split* if all nonzero minimal subcoalgebras are 1-dimensional. The subcoalgebras of C are precisely the C' submodules. Cyclic submodules are finite dimensional; thus, when k is algebraically closed the simple submodules are 1-dimensional and C is split.

C is called *coconnected* if it is split and has a unique 1-dimensional subcoalgebra. In this case we can uniquely identify the 1-dimensional coalgebra with k as follows: let c be a nonzero element of the 1-dimensional coalgebra, then $\varepsilon(c)\neq 0$ and we identify 1 with $c/\varepsilon(c)$. $d(1)=1 \otimes 1$ in C so this identification preserves the coalgebra structure of k.

Assume C is coconnected, in C' let $\mathcal{M}=1^0$ (the subspace of elements orthogonal to 1). Filter C by $C_i=(\mathcal{M}^{i+1})^0$, $i=0, 1, \ldots$. Note $C_0=k$.

$$(2) \qquad d(C_n) \subset \sum_{0}^{n} C_i \otimes C_{n-i},$$

and if C is a Hopf algebra $C_iC_j\subset C_{i+j}$. By induction on the rank of the tensor $d(c)$ it follows $C=\bigcup C_i$. If $0\neq d(c)$ is of rank 1 then $c/\varepsilon(c)$ is grouplike; hence, $c\in k=C_0$. Suppose we have shown that if $d(c)$ is of rank n then $c\in C_{n-1}$; let $c\in C$ where $d(c)$ is of rank $n+1$. $c=\sum_{(c)} c_{(1)}\varepsilon(c_{(2)})$ implies $d(c)-c \otimes 1$ is of rank n. For $a'\in\mathcal{M}$ we have $a'\cdot 1=0$ and with (1) this implies $d(a'\cdot c)$ is of rank less than $n+1$; hence, $a'\cdot c\in C_{n-1}$. Thus for $a_1',\ldots,a_{n+1}'\in\mathcal{M}$, $\langle a_1'\cdots a_{n+1}', c\rangle=\langle a_1'\cdots a_n', a_{n+1}'\cdot c\rangle=0$ and $c\in C_n$.

$x\in C$ is called *primitive* if $d(x)=x \otimes 1+1 \otimes x$. In this case $x\in C_1$ and $\varepsilon(x)=0$. Letting L denote the space of primitive elements and $C^+=\operatorname{Ker}\varepsilon$, then

$$(3) \qquad L = C_1\cap C^+ \qquad \text{and} \qquad C_1 = k\oplus L.$$

If C is a Hopf algebra L is a Lie algebra under $[x, y]=xy-yx$ and if $p>0$, L is a restricted Lie algebra.

Let H be a coconnected Hopf algebra. Note $\mu\colon k\to H$, the unit, is the unique coalgebra morphism of k to H. If $p=0$ let U denote the universal enveloping algebra (u.e.a.) of L. If $p>0$ let U denote the restricted u.e.a. (r.u.e.a.) of L. U has a natural Hopf algebra structure induced by the (restricted) Lie algebra morphisms $L\to L\oplus L$, $x\to(x, x)$; $L\to k$, $x\to 0$. U is a split cocommutative coconnected Hopf algebra where $L(U)=L$. By the universal property of U there is an algebra morphism $\gamma\colon U\to H$ which is a Hopf algebra morphism. That γ is injective follows from:

LEMMA 1. *Let C be a coconnected coalgebra, D a coalgebra and $\phi\colon C\to D$ a coalgebra morphism. ϕ is injective if and only if $\phi|L$ is injective.*

Proof. Assume $\phi|L$ is injective. Being a coalgebra morphism $\varepsilon\phi(L)=0$, $\varepsilon\phi(1)=1$, hence by (3) $\phi|C_1$ is injective. By induction we assume $\phi|C_n$ is injective and so $(\phi \otimes \phi) \mid (C_n \otimes C_n)$ is injective. Suppose $c\in C_{n+1}\cap\operatorname{Ker}\phi$, then since

$$d(c) = 1 \otimes c+c \otimes 1+Y, \qquad Y\in C_n \otimes C_n,$$

it follows $0=d\phi(c)=(\phi \otimes \phi)d(c)=(\phi \otimes \phi)(Y)$. This implies $Y=0$, hence $c=0$. The converse is clear. Q.E.D.

We identify U with its image in H so we have that the subalgebra of H generated by L is the (r.)u.e.a. of L. We shall show $U=H$ when $p=0$; it follows from Theorem 3. When $p>0$ we shall show that $U=(H'F(\mathscr{M}))^0$ where $F\colon H'\to H'$, $a'\to a'^p$ is the Frobenius morphism and $H'F(\mathscr{M})$ is the ideal generated by $F(\mathscr{M})$. Proofs of the above utilize the following technique which "picks-out" subspaces of a coconnected coalgebra.

Let C be a coconnected coalgebra, for $0<n\in Z$ let

$$d^n\colon C\to C^{[n+1]},\qquad c\to\sum_{(c)} c_{(1)}\otimes\cdots\otimes c_{(n+1)}$$

(where $X^{[m]}$ signifies $X\otimes\cdots\otimes X$, m copies of X). Let $d^0\equiv I$. Also, if we let $E=I-\varepsilon$ and $\delta^n=E^{[n+1]}d^n$ then

$$\langle a_1', c\rangle = \langle a_1', E(c)\rangle, \tag{4}$$

$$\langle a_1'\cdots a_n', c\rangle = \langle a_1'\otimes\cdots\otimes a_n', \delta^{n-1}(c)\rangle, \tag{5}$$

where $a_1',\dots,a_n'\in\mathscr{M}$, $c\in C$. The equation $C_n=\operatorname{Ker}\delta^n$ follows from (5) and $C_n=(\mathscr{M}^{n+1})^0$. Moreover, $\delta^{n-1}(C_n)\subset L^{[n]}$ follows from (2) and (3).

If V is a subspace of C let $V_n=V\cap C_n$. Let TL denote the tensor algebra on L, V_0 is $\{0\}$ or k so we can consider $V_0\subset TL$; also, we can consider $\delta^{i-1}(V_i)\subset TL$. With V we associate $TL_V=V_0\oplus(\oplus_1^\infty\delta^{i-1}(V_i))\subset TL$.

LEMMA 2. *Let C be a coconnected coalgebra and $V\subset W$ subspaces of C, then $V=W$ if and only if $TL_V=TL_W$.*

Proof. Suppose $TL_V=TL_W$ then $V_0=W_0$. Say by induction we have $V_n=W_n$, let $w\in W_{n+1}$. Choose $v\in V_{n+1}$ where $\delta^n(v)=\delta^n(w)$. $0=\delta^n(w-v)$ implies $(w-v)\in W_n=V_n$; hence, $w\in V_{n+1}$. The converse is clear. Q.E.D.

We introduce notation to simplify discussion of symmetric tensors in TL. Let W be a vector space, TW the tensor algebra of W and Sn the symmetric group on n letters. For $n>0$, $W^{[n]}$ is an Sn module where $s\cdot(w_1\otimes\cdots\otimes w_n)=(w_{1s}\otimes\cdots\otimes w_{ns})$, $s\in Sn$, $w_1,\dots,w_n\in W$. Let $S(w_1\otimes\cdots\otimes w_n)\in W^{[n]}\subset TW$ denote the sum of the elements in the orbit of $w_1\otimes\cdots\otimes w_n$.

Let G be an ordered set and for each $\gamma\in G$ let $0\leqq e_\gamma\in Z$. The vector $(e_\gamma)_{\gamma\in G}$ will be denoted e. Let $|e|\equiv\sum e_\gamma$; this is a well defined nonnegative integer or infinity. Let $e!\equiv\prod e_\gamma!$ and if f is another vector let $e+f$ be the vector with the γ component $e_\gamma+f_\gamma$. Let

$$\binom{e+f}{e}$$

be $(e+f)!/e!f!$. We write $e<f$ if each $e_\gamma<f_\gamma$, $e|f$ if each e_γ divides f_γ and $e\nmid f$ if it is not true that $e|f$. For $0\leqq n\in Z$ let $\boldsymbol{n}$ be the vector with each component equal to n. For $\{w_\gamma\}_{\gamma\in G}\subset W$ and e where $|e|=n>0$, let Sw^e denote $S(\cdots\otimes w_\gamma^{[e_\gamma]}\otimes\cdots)$, if $|e|=0$ let $Sw^e=1$. Finally, if W is an algebra let w^e be the ordered product $\prod w_\gamma^{e_\gamma}$. Note that if $\{w_\gamma\}_{\gamma\in G}$ is a basis for W then $\{Sw^e\mid n=|e|\}$ is a basis for the symmetric tensors of degree n in TW.

2. Unless otherwise stated all Hopf algebras under consideration will be assumed to be coconnected.

LEMMA 3. *If $p>0$, then $U=(H'F(\mathscr{M}))^0$. If $\{l_\gamma\}_{\gamma\in G}$ is a basis for L, then TL_U has a basis*

$$\{Sl^e \mid e < \mathbf{p}\}. \tag{6}$$

Proof. First we show $U\subset(H'F(\mathscr{M}))^0$. Consider H' as an H module by $\langle a'\cdot b, c\rangle\equiv\langle a', bc\rangle$, $a'\in H'$, $b, c\in H$. The elements of L act as derivations of H'; thus if $l_1,\dots,l_n\in L$, $a'\in H'$, $b'\in\mathscr{M}$, then

$$\langle a'(b'^p), l_1\cdots l_n\rangle = \langle (a'\cdot l_1)(b'^p), l_2\cdots l_n\rangle$$

and by induction on n this is zero.

The elements of (6) are linearly independent, let V be the space they span. By Lemma 2 we are done if we show $TL_{(H'F(\mathscr{M}))^0}\subset V\subset TL_U$. Let $x\in(H'F(\mathscr{M}))^0_n$. By cocommutativity and coassociativity $\delta^{n-1}(x)$ is a symmetric tensor of degree n, so $\delta^{n-1}(x)=\sum\lambda_i Sl^{e_i}$, $\lambda_i\in k$, $|e_i|=n$. Suppose we do not have $e_i<\mathbf{p}$. Let $\{d_\gamma\}_{\gamma\in G}\subset\mathscr{M}$ be dual to $\{l_\gamma\}$, then $d^{e_i}\in H'F(\mathscr{M})$ and by (5), $\langle d^{e_i}, x\rangle=\lambda_i$; which shows $\lambda_i=0$ and $TL_{(H'F(\mathscr{M}))^0}\subset V$.

For any $e<\mathbf{p}$ where $|e|=n$, we have $l^e/e!\in U_n$ and $\delta^{n-1}(l^e/e!)=Sl^e$, so $V\subset TL_U$. Q.E.D.

As a corollary we see $U=H$ if and only if $F(\mathscr{M})=0$.

The last formula in the proof of Lemma 3 follows from the combinatoric result:

LEMMA 4. *Using the above notation let $x\in H_n$ and $y\in H_m$ where $\delta^{n-1}(x)=\sum\lambda_i Sl^{e_i}$ and $\delta^{m-1}(y)=\sum\tau_j Sl^{f_j}$, λ_i, $\tau_j\in k$; then*

$$\delta^{n+m-1}(xy) = \sum_{i,j}\lambda_i\tau_j\binom{e_i+f_j}{e_i}Sl^{e_i+f_j}.$$

We include no proof.

Since H is not necessarily primitively generated the ideal generated by L is not necessarily H^+. The two-sided ideal generated by the primitives is characterized in the following.

LEMMA 5. *We assume $p>0$.*

(1) *$LH=HL=F(H')^0$.*

(2) *Let $\{l_\gamma\}_{\gamma\in G}$ be a basis for L, V the space with basis $\{Sl^e \mid \mathbf{p}\nmid e\}$ and W the space with basis $\{Sl^e\mid \mathbf{p}\mid e\}$; then, $TL_H=(TL_H\cap V)\oplus(TL_H\cap W)$.*

(3) *$TL_{LH}=TL_H\cap V$.*

Proof. First we prove (2) and show $TL_H\cap V\subset TL_{LH}$ by proving for any $x\in H_n$ there is a $v\in(LH)_n$ where $\delta^{n-1}(v)\in V$ and $\delta^{n-1}(x-v)\in W$. We proceed by induction on t where $\delta^{n-1}(x)=\sum_1^t\lambda_i Sl^{e_i}$. If $t=0$, then $\delta^{n-1}(x)=0\in W$. Say $t\geqq 1$, if $\delta^{n-1}(x)\notin W$ then for some i—say $i=t$—$\mathbf{p}\nmid e_t$. We identify $L^{[n-1]}$ with $L^{[n-1]}\otimes k$ so that by (1) and (4)

$$\delta^{n-2}(a'\cdot y) = (I^{[n-1]}\otimes a')\delta^{n-1}(y), \tag{7}$$

where $a' \in \mathcal{M}$ and $y \in H_n$. Let $e_{i,\gamma}$ denote the γ-component of e_i. Since $p \nmid e_t$ there is $\pi \in G$ where $p \nmid e_{t,\pi}$; *let n_γ denote the vector whose γ-component is n and all other components are zero.* By (7) $\delta^{n-2}(d_\pi \cdot x) = \sum_1^t \lambda_i' Sl^{e_i - 1_\pi}$, where $\{d_\gamma\} \subset \mathcal{M}$ is dual to $\{l_\gamma\}$ and λ_i' is zero if $e_{i,\pi} = 0$ and λ_i otherwise. By Lemma 4, $\delta^{n-1}(l_\pi(d_\pi \cdot x)) = \sum_1^t \lambda_i e_{i,\pi} Sl^{e_i}$, so if $l_\pi(d_\pi \cdot x)/e_{t,\pi} = v \in LH$, then

$$\delta^{n-1}(x-v) = \sum_1^{t-1} \lambda_i \left(\frac{1-e_{i,\pi}}{e_{t,\pi}} \right) Sl^{e_i}$$

and we have completed the induction. (Note $\delta^{n-1}(v) \in V$.)

Second we show $LH \subset F(H')^0$. Let H' be an H module as in the proof of Lemma 3. $\langle a'^p, lh \rangle = \langle (a'^p) \cdot l, h \rangle = 0$, where $a' \in H'$, $l \in L$, $h \in H$, since the elements of L act as derivations.

To conclude, by Lemma 2 it suffices to show $TL_{F(H')^0} \subset TL_H \cap V \subset TL_{LH}$. The right hand containment has already been verified, we show $TL_{F(H')^0} \subset V$. Let $x \in F(H')^0_n$ where $\delta^{n-1}(x) = \sum \lambda_i Sl^{e_i}$ and suppose for some j, $p \mid e_j$. Then $d^{e_j} \in F(H')$ and $0 = \langle d^{e_j}, x \rangle = \lambda_j$, which implies $\delta^{n-1}(x) \in V$.

The "mirror" proof shows $HL = F(H')^0$. Q.E.D.

LH is a Hopf ideal, i.e., LH is a two-sided ideal and $d(LH) \subset LH \otimes H + H \otimes LH$; hence, H/LH has the structure of a Hopf algebra. In the next section we demonstrate H/LH is isomorphic to a sub-Hopf algebra of H with its vector space structure altered, when k is perfect.

3. In this section we assume $p > 0$ and k is perfect. F is p-linear by which we mean $F(a'+b') = F(a') + F(b')$ and $F(\lambda a') = \lambda^p F(a')$ for $a', b' \in H'$, $\lambda \in k$. The transpose map $F' : H'' \to H''$ is defined by $\langle a', F'(b'') \rangle \equiv \langle F(a'), b'' \rangle^{1/p}$. F' is $1/p$-linear. Considering $H \subset H''$ we shall show $F'(H) \subset H$ by explicitly describing $F'|H$. Let V denote $F'|H$ and let $\{h_\gamma\}_{\gamma \in G}$ be a basis for H. For $h \in H$, $d^{p-1}(h)$ is a symmetric tensor in $H^{[p]}$, so $d^{p-1}(h) = \sum \lambda_i Sh^{e_i}$ where $|e_i| = p$. For any $a' \in H'$, $\langle F(a'), h \rangle^{1/p} = \sum \lambda_i^{1/p} \langle a'^{[p]}, Sh^{e_i} \rangle^{1/p} = \sum_J \lambda_i^{1/p} \langle a'^{[p]}, Sh^{p_{\gamma(i)}} \rangle^{1/p} = \sum_J \lambda_i^{1/p} \langle a', h_{\gamma(i)} \rangle$, where

$$J = \{ i \mid e_i = p_{\gamma(i)} \}.$$

Thus

$$V(h) = \sum_J \lambda_i^{1/p} h_{\gamma(i)}. \tag{8}$$

$dV = (V \otimes V)d$ since F is a ring homomorphism. V is a ring homomorphism because the following diagram is commutative:

$$\begin{tikzcd} H' \arrow[r, "m_H'"] \arrow[d, "V' = F"'] & (H \otimes H)' \arrow[d, "(V \otimes V)'"] \\ H' \arrow[r, "m_H'"] & (H \otimes H)', \end{tikzcd}$$

$(V \otimes V)'$ is the Frobenius morphism in $(H \otimes H)'$.

THEOREM 1. *There is a unique $1/p$-linear Hopf algebra morphism $V\colon H \to H$ where $V'=F$,* Ker $V=LH$ *and* Im $V=(\{a' \in H' \mid a'^p=0\})^0$.

Proof. We have already proved the first statement. Clearly, Ker $V=(\text{Im } F)^0$ which is LH by Lemma 5; the last statement is merely that Im $V=(\text{Ker } F)^0$. Q.E.D.

Let V^n denote $V \cdots V$ (n times), the $1/p^n$-linear Hopf algebra morphism from H to H and let F^n denote the map $F \cdots F$ (n times), the transpose map to V^n. If $x \in V^n(H)$ we say x has coheight n (the elements of Ker F^n are said to have (Frobenius) height n). We let $V^\infty(H)$ denote $\bigcap_1^\infty V^n(H)$. Elements of $V^\infty(H)$ are said to have infinite coheight. These elements form a subalgebra and also a subcoalgebra since $V^\infty(H)=(\bigcup_1^\infty \text{Ker } F^n)^0$ and $\bigcup_1^\infty \text{Ker } F^n$ is a two-sided ideal in H'. Thus $V^\infty(H)$ is a sub-Hopf algebra of H. Let $L_i=L \cap V^i(H)$, $i=0, 1, \dots, \infty$; each L_i is a restricted Lie algebra.

LEMMA 6. *Let $\{l_\gamma\}_{\gamma\in G_0}$ be a basis for L_0 and let $G_0 \supset G_1 \supset \cdots \supset G_n$ where $\{l_\gamma\}_{\gamma \in G_i}$ is a basis for L_i, $i=0, 1, \dots, n$. For $\gamma \in G_0$ let $(\gamma) \in Z$ be maximal such that $\gamma \in G_{(\gamma)}$. Suppose $h \in H_m$ and $\delta^{m-1}(h)=\sum \lambda_i Sl^{e_i}$, $0 \neq \lambda_i \in k$; then $(\pi)<n$ implies $e_{i,\pi}<p^{(\pi)+1}$, for all i.*

Proof. Let $\{d_\gamma\}_{\gamma\in G_0} \subset \mathscr{M}$ be dual to $\{l_\gamma\}$ where we have chosen d_π to lie in Ker $F^{(\pi)+1}$. Then $0=(d_\pi)^{p^{(\pi)+1}}$ and $\lambda_i=\langle d^{e_i}, h\rangle$ imply $e_{i,\pi}<p^{(\pi)+1}$. Q.E.D.

4. Divided powers.

EXAMPLE. Suppose H is a Hopf algebra and $p=0$. Let $x \in L$ and let ${}^n x$ denote $x^n/n!$, $n=0, 1, \dots$. We have $d({}^n x)=\sum_0^n {}^i x \otimes {}^{n-i}x$.

For arbitrary p a finite or infinite sequence of elements ${}^0x, {}^1x, \dots \in H$ is called a *sequence of divided powers of* ${}^1x$ if for each n, $d({}^n x)=\sum_0^n {}^i x \otimes {}^{n-i}x$. An element ${}^n x$ lying in such a sequence is called an nth *divided power of* ${}^1x$. Since H is coconnected ${}^0x=1$ and ${}^1x \in L$. A simple induction shows $\varepsilon({}^i x)=0$ for $i \geqq 1$. Also, ${}^i x \in H_i$ for all i. If $p>0$ then $V({}^n x)={}^{n/p}x$ if $p|n$ and zero otherwise. For $0<e\in Z$, let $\|e\| \in Z$ be defined by $p^{\|e\|} \leqq e < p^{\|e\|+1}$. If we have a sequence of divided powers ${}^0x, \dots, {}^e x$, it follows that ${}^1x=V^{\|e\|}({}^{p^{\|e\|}}x)$ and so ${}^1x$ has coheight $\|e\|$.

THEOREM 2. *Assume $p>0$, k is perfect and ${}^1x$ is primitive. ${}^1x$ has coheight n if and only if there is a sequence of divided powers ${}^0x, {}^1x, \dots {}^{p^{n+1}-1}x$, for $n=0, 1, \dots, \infty$.*

THEOREM 3. *If k is arbitrary assume L has a basis of the form $\{l_\gamma\}_{\gamma \in G_\infty}$ where G_∞ is ordered and ${}^0l_\gamma$, $l_\gamma={}^1l_\gamma, \dots$ is an infinite sequence of divided powers; or if $p>0$ and k is perfect assume L has a basis of the form $\{l_\gamma\}_{\gamma\in G_0}$ where $G_0 \supset G_1 \supset \cdots \supset G_\infty$, G_0 is ordered, $\{l_\gamma\}_{\gamma \in G_i}$ is a basis for L_i ($i=0, 1, \dots, \infty$) and ${}^0l_\gamma$, $l_\gamma={}^1l_\gamma, \cdots {}^{p^{(\gamma)+1}-1}l_\gamma$ is a sequence of divided powers. Then the monomials ${}^{e_1}l_{\gamma_1} \cdots {}^{e_m}l_{\gamma_m}$ where $\gamma_1 < \cdots < \gamma_m$, $0 \leqq e_i < p^{(\gamma_i)+1}$ and $0<m\in Z$, form a basis for H.*

In Theorems 2 and 3 ${}^0x, \dots, {}^{p^{n+1}-1}x$ denotes an infinite sequence if $n=\infty$. The symbol (γ) denotes ∞ if $\gamma \in G_\infty$, otherwise $(\gamma) \in Z$ is maximal where $\gamma \in G_{(\gamma)}$;

if $(\gamma)=\infty$ then $p^{(\gamma)+1}$ denotes ∞. Theorem 2 will be proved by means of the following *Extension Lemma* whose proof is complicated.

LEMMA 7. *Assume $p>0$, k is perfect and we are given a sequence of divided powers ${}^0x,\ldots,{}^{t-1}x$ satisfying: ${}^ex$ has coheight $n-\|e\|$ for $1\leqq e<t$ and $t<p^{n+1}$; then there is a ${}^tx$ of coheight $n-\|t\|$ such that ${}^0x,\ldots,{}^tx$ is a sequence of divided powers.*

Proof. We proceed by induction on n and on t. Note by the induction hypotheses if ${}^1y\in L_m$ and $m<n$ then ${}^0y$, ${}^1y$ can be extended to a sequence of divided powers ${}^0y,{}^1y,\ldots,{}^{p^{m+1}-1}y$. If $m=n$ we can extend to ${}^0y,{}^1y,\ldots,{}^{t-1}y$. *The first step of the proof is to show there is an element ${}^tx'$ of coheight $n-\|t\|$ where $\delta^{t-1}({}^tx')={}^1x^{[t]}$.* (When $n=0$ let ${}^tx'=x^t/t!$.) When $n\geqq 1$ this step is difficult and we must first find ${}^{p^n}x'$ where $\delta^{p^n-1}({}^{p^n}x')={}^1x^{[p^n]}$.

Let $z\in H_m$ where $V^n(z)={}^1x$. Choose a basis $\{l_\gamma\}_{\gamma\in G_0}$ for L as in Lemma 6. We can write $\delta^{m-1}(z)=\sum_1^M\lambda_iSl^{e_i}$ where $|e_i|=m$ for each i. If $p^n\nmid m$, then $p^n\nmid e_i$ for any i. If $p^n|m$ then $\delta^{(m/p^n)-1}(V^n(z))=\sum_J\lambda_i^{1/p^n}Sl^{e_i/p^n}$, where $J=\{i\mid p^n|e_i\}$ and since $V^n(z)={}^1x$ it follows we can assume $p^n\nmid e_i$ if $m>p^n$. (Note that $F^n(\mathscr{M})\subset\mathscr{M}^{p^n}$ implies $V^n(H_{p^n-1})\subset k$ and so $m\geqq p^n$.) Say $m>p^n$, then $p^n\nmid e_M$. So for some ϕ, $p^n\nmid e_{M,\phi}$; if $(\phi)<n$, then by Lemma 6, $b=e_{M,\phi}<p^{(\phi)+1}$ and by induction on n there is a b divided power, ${}^bl_\phi$, of l_ϕ. If $(\phi)=n$ then $e_{M,\phi}=ap^n+b$, $0<b<p^n$; $l_\phi\in L_{n-1}$ $(L_n\subset L_{n-1})$ so by the induction on n there is ${}^bl_\phi$, a b divided power of l_ϕ.

By (7) iterated and Lemma 4,

$$\delta^{m-1}({}^bl_\phi(d_\phi^b\cdot z)) = \sum_1^M\lambda_i\binom{e_{i,\phi}}{b}Sl^{e_i}.$$

(See the lines following (7) for greater detail on this point.)

$$\binom{e_{M,\phi}}{b}\not\equiv 0 \pmod p,$$

so if

$$y = {}^bl_\phi(d_\phi^b\cdot z)\bigg/\binom{e_{M,\phi}}{b},$$

then

$$\delta^{m-1}(z-y) = \sum_1^{M-1}\lambda_i\left[1-\binom{e_{i,\phi}}{b}\bigg/\binom{e_{M,\phi}}{b}\right]Sl^{e_i}$$

and $V^n(z-y)={}^1x$, since $V^n({}^bl_\phi)=0$. Thus by descending induction on M we can assume $m=p^n$.

We can write $\delta^{p^n-1}(z)={}^1x^{[p^n]}+\sum_1^N\lambda_iSl^{f_i}$, where for each i, $|f_i|=p^n$. Since

$$^1x = V^n(z) = {}^1x+\sum_J\lambda_il_{\gamma(i)},$$

where $J=\{i\mid f_i=p^n_{\gamma(i)}\}$, we can assume that $f_{i,\gamma}<p^n$, for all i and γ. Moreover, by a slight modification of Lemma 6, if $(\gamma)<n$ then $f_{i,\gamma}<p^{(\gamma)+1}$. By the induction on n

we have ${}^{f_{i,\gamma}}l_\gamma$, an $f_{i,\gamma}$ divided power of l_γ. If $w=\sum_1^N \lambda_i \prod_G {}^{f_{i,\gamma}}l_\gamma$, then by Lemma 4, $\delta^{p^n-1}(z-w)={}^1x^{[p^n]}$. Let ${}^{p^n}x'=z-w$.

Let ${}^{p^j}x'=V^{n-j}({}^{p^n}x')$, then $\delta^{p^j-1}({}^{p^j}x')={}^1x^{[p^j]}$ and ${}^{p^j}x'$ has coheight $n-j$, for $j=0,1,\dots,n$. Write t in the form $t=a_np^n+a_{n-1}p^{n-1}+\cdots+a_1p+a_0$, where $0\leqq a_i<p$. Note, $\|t\|$ is the maximal i where $a_i\neq 0$. $t!/(p^n!)^{a_n}\cdots(p^0!)^{a_0}\not\equiv 0 \pmod p$, so that if we set

$$ {}^tx' = ((p^n!)^{a_n}\cdots(p^0!)^{a_0}/t!)\prod_0^n ({}^{p^i}x')^{a_i}, $$

then by Lemma 4, $\delta^{t-1}({}^tx')={}^1x^{[t]}$; also, ${}^tx'$ has coheight $n-\|t\|$. This concludes the first step.

For the vector $a=(a_1,a_2,\dots)$ let $n(a)$ be the maximal n where $a_n\neq 0$ and ∞ if no such n exists. Let ${}^{[a]}x$ denote ${}^{a_1}x\otimes{}^{a_2}x\otimes\cdots\otimes{}^{a_n}x$ if $n(a)=n$ is finite and each $a_i<t$. *The second step of the proof is to use ${}^tx'$ to begin a descending induction proving there is ${}^sx'$ of coheight $n-\|t\|$ where $\delta^{s-1}({}^sx')=\sum_{a\in A}{}^{[a]}x$, $A=\{a \mid n(a)=s,\ |a|=t,\ a>0\}$, $s=t,t-1,\dots,2$.*

Suppose we have such ${}^sx'$, $2<s\leqq t$, we shall construct ${}^{s-1}x'$. Consider $\delta^{s-2}({}^sx')=\sum_{a\in B}{}^{[a]}x+Y$, $Y\in H^{+[s-1]}$ and $B=\{a \mid n(a)=s-1,\ |a|=t,\ a>0\}$. We now show $Y\in L\otimes H^{+[s-2]}$. Since Ker $\delta^1=H_1$ it suffices to show that

$$ (E\otimes E\otimes I^{[s-2]})(d\otimes I^{[s-2]})(Y) = 0, $$

or that

$$ (E\otimes E\otimes I^{[s-2]})(d\otimes I^{[s-2]})(\delta^{s-2}({}^sx')) = (E\otimes E\otimes I^{[s-2]})(d\otimes I^{[s-2]})\Big(\sum_{a\in B}{}^{[a]}x\Big). $$

The left hand side is

$$ (E\otimes E\otimes I^{[s-2]})(d\otimes I^{[s-2]})(E^{[s-1]})(d^{s-2}({}^sx')) = E^{[s]}d^{s-1}({}^sx') = \delta^{s-1}({}^sx') $$

which is equal to the right hand side. (In the preceding calculation we used the identity $(E\otimes E)\,dE=(E\otimes E)d$.) Thus $Y\in L\otimes H^{+[s-2]}$ and by symmetry $Y\in L^{[s-1]}$, which means Y can be written $\sum_1^M \lambda_j S l^{e_j}$, where $|e_j|=s-1$. Note $e_{j,\gamma}\neq 0$ implies $(\gamma)\geqq n-\|t\|$ since ${}^sx'$ and ${}^1x,\dots,{}^{t-1}x$ have coheight $n-\|t\|$.

We now show that when $(\phi)<n$ and $e_{j,\phi}\neq 0$ then $e_{j,\phi}<p^{(\phi)-n+\|t\|+1}$. Suppose not, so that for some ϕ and some j—say $j=1$—$0\neq e_{1,\phi}\geqq p^{(\phi)-n+\|t\|+1}$ $(\geqq p)$. Since l_ϕ has coheight less than $(\phi)+1$ we can choose $\{d_\gamma\}_{\gamma\in G_0}\subset\mathscr{M}$ dual to $\{l_\gamma\}$ where $d_\phi\in \operatorname{Ker} F^{(\phi)+1}$. Then $F^{n-\|t\|}(d_\phi^{p^{(\phi)-n+\|t\|+1}})=0$. Choose $z\in H$ where $V^{n-\|t\|}(z)={}^sx'$ and let

$$ a' = \Big(\prod_{\gamma\in G}^{\gamma\neq\phi} d_\gamma^{e_{1,\gamma}}\Big)\big(d_\phi^{e_{1,\phi}-p^{(\phi)-n+\|t\|+1}}\big). $$

$$ \begin{aligned} 0 &= \langle F^{n-\|t\|}(d_\phi^{p^{(\phi)-n+\|t\|+1}}),\ F^{n-\|t\|}(a')\cdot z\rangle^{1/p} \\ (*)\qquad &= \langle F^{n-\|t\|}(d^{e_1}),\ z\rangle^{1/p} = \langle d^{e_1},\ {}^sx'\rangle \\ &= \lambda_1+\Big\langle \cdots\otimes d_\phi^{[e_{1,\phi}]}\otimes\cdots,\ \sum_{a\in B}{}^{[a]}x\Big\rangle \\ &= \lambda_1+\sum_{a\in C}\lambda_a\langle d_\phi,\ {}^{a_1}x\rangle\cdots\langle d_\phi,\ {}^{a_{n(a)}}x\rangle, \end{aligned} $$

for appropriate $\lambda_a \in k$ and where $C=\{a \mid n(a)=e_{1,\phi},\ |a| \leqq t-((s-1)-e_{1,\phi}),\ a>\mathbf{0}\}$. However, $p^{\|t\|+1}>t$ implies $(p^{(\phi)-n+\|t\|+1})(p^{n-(\phi)})+(e_{1,\phi}-e_{1,\phi})>t$; we are assuming $e_{1,\phi} \geqq p^{(\phi)-n+\|t\|+1}$ and clearly $s-1 \geqq e_{1,\phi}$; thus, $(e_{1,\phi})p^{n-(\phi)}+((s-1)-e_{1,\phi})>t$ or $(e_{1,\phi})p^{n-(\phi)}>t-((s-1)-e_{1,\phi})$. This implies for each term in the right hand summation at (*) at least one a_i is less than $p^{n-(\phi)}$. For such a_i, ${}^{a_i}x$ has coheight $(\phi)+1$ since ${}^{a_i}x$ has coheight $n-\|a_i\|$ and $\|a_i\| \leqq n-(\phi)-1$. Thus $\langle d_\phi, {}^{a_i}x\rangle=0$; all the terms in the right hand summation vanish; it follows $\lambda_1=0$ and we can assume that if $(\phi)<n$ and $0 \neq e_{j,\phi}$ then $(e_{j,\phi})p^{n-\|t\|}<p^{(\phi)+1}$. By the induction on n there is an element u which is an $(e_{j,\phi})p^{n-\|t\|}$ divided power of l_ϕ, then $v_\phi^j \equiv V^{n-\|t\|}(u)$ has coheight $n-\|t\|$ and is an $e_{j,\phi}$ divided power of l_ϕ.

If $(\phi)=n$ there is v_ϕ^j an $e_{j,\phi}$ divided power of l_ϕ which has coheight $n-\|e_{j,\phi}\|$. Such a v_ϕ^j exists since $e_{j,\phi} \leqq s-1<t$ so we can apply the induction hypotheses. v_ϕ^j has coheight $n-\|t\|$ since $e_{j,\phi}<t$.

When $e_{j,\phi}=0$ let $v_\phi^j \equiv 1$. Define $y_j \equiv \prod_{\gamma \in G} v_\gamma^j$, $y \equiv \sum_1^M \lambda_j y_j$ and ${}^{s-1}x'={}^{s}x'-y$. Then ${}^{s-1}x'$ has coheight $n-\|t\|$ and by Lemma 4, $\delta^{s-2}({}^{s-1}x')=\sum_{a \in B} {}^{[a]}x$.

We have completed the descending induction step on s which leads to ${}^2x'$ of coheight $n-\|t\|$ where $\delta({}^2x')=\sum_1^{t-1} {}^{i}x \otimes {}^{t-i}x$. Defining ${}^tx$ to be ${}^2x'-\varepsilon({}^2x')$ gives the desired element. Q.E.D.

Proof of Theorem 2. Clearly the existence of the sequence of divided powers implies ${}^1x$ has the desired coheight.

Conversely when ${}^1x$ has coheight $n \in Z$, Lemma 7 guarantees ${}^0x$, ${}^1x$ can be extended to a sequence of divided powers ${}^0x, {}^1x, \ldots, {}^{p^{n+1}-1}x$.

The infinite case is proved as follows: Let K denote $V^\infty(H)$. K' is naturally isomorphic to $H'/(\bigcup \operatorname{Ker} F^i)$. Thus the Frobenius morphism on K' is injective which implies its transpose, the V map of K, is surjective and all elements of K have infinite coheight in K. Thus for ${}^1x$ a primitive element in K the sequence ${}^0x$, ${}^1x$ can be extended to an infinite sequence of divided powers lying in K by Lemma 7. Q.E.D.

Proof of Theorem 3. First we show the monomials span H^+. Let $h \in H_m^+$, then $\delta^{m-1}(h)=\sum \lambda_i Sl^{e_i}$. For k perfect, $e_{i,\phi}<p^{(\phi)+1}$, by Lemma 6. Let x_i be the ordered product $\prod_{G_0} {}^{e_{i,\gamma}}l_\gamma$ and $y \equiv \sum \lambda_i x_i$. By Lemma 4 $\delta^{m-1}(y)=\delta^{m-1}(h)$ and by Lemma 2 the space spanned by the monomials is H^+.

We now show independence. For $\gamma \in G_0$ let C_γ be the subcoalgebra of H spanned by the sequence of divided powers of l_γ. Given $\gamma_1<\cdots<\gamma_n$ we have the coconnected coalgebra $C=C_{\gamma_1} \otimes \cdots \otimes C_{\gamma_n}$ and $L(C)$ has a basis

$$\{1 \otimes \cdots \otimes 1 \otimes l_{\gamma_i} \otimes 1 \otimes \cdots \otimes 1 \mid l_{\gamma_i} \text{ is in the } i\text{-place, } i=1,\ldots,n\}.$$

The map $C \to H$, $x_1 \otimes \cdots \otimes x_n \to x_1 \cdots x_n$ is a coalgebra morphism which is injective on $L(C)$; hence, by Lemma 1 is injective. Q.E.D.

Theorem 3 should be interpreted as a coalgebra structure theorem; it says $H \cong \otimes_{G_0} C_\gamma$. There are Hopf algebras over a perfect field where L does not have a basis of the form assumed in Theorem 3.

5. **Graded Hopf algebras.**

Throughout this section we assume $p \neq 2$.

We shall now consider coanticommutative coconnected Hopf algebras. An exterior algebra is such a Hopf algebra. In an exterior algebra on the vector space V, V corresponds to the primitive elements and V lies in the odd-graded part. Note that an evenly graded Hopf algebra will be a Hopf algebra in the sense of the previous sections. Theorem 4 of this section implies that a coanticommutative coconnected Hopf algebra has the coalgebra structure of the tensor product of an exterior Hopf algebra with an evenly graded Hopf algebra.

Z_2 is the field of two elements. We shall consider vector spaces graded with respect to the additive group of Z_2. If X and Y are two such spaces then $X \otimes Y$ is graded over Z_2 in the usual fashion. Let $T\colon X \otimes Y \to Y \otimes X$, be the map $x \otimes y \to (-1)^{ij} y \otimes x$, where $x \in X^i$, $y \in Y^j$. T is the graded twist map. If X and Y are graded (co) algebras then $(X \otimes Y)$ is a graded (co) algebra, we use the graded twist map in defining the structure on $X \otimes Y$. F is a graded Hopf algebra if it is simultaneously a graded algebra and a graded coalgebra and d and ε are graded algebra morphisms. A graded coalgebra is coanticommutative if $Td = d$. It is split if it is coanticommutative and all simple subcoalgebras are 1-dimensional. Let C be a graded split coalgebra, C' is the graded algebra where $C'^0 = (C^0)'$ and $C'^1 = (C^1)'$. C' is an anticommutative algebra, i.e., $mT = m$.

C is coconnected if it contains a unique 1-dimensional subcoalgebra. As before we identify this coalgebra with k. $k \subset C^0$ by coanticommutativity. When C is coconnected it is filtered as before, and the same results hold for the filtration. Also, $C_n = (C_n \cap C^0) \oplus (C_n \cap C^1)$. The definition of primitive elements remains unchanged; $L = L^0 \oplus L^1$, where $L^i = L \cap C^i$. If C is a Hopf algebra L is a graded Lie algebra; L^0 is a Lie ideal which is a restricted Lie algebra if $p > 0$. Lemmas 1 and 2 hold for graded coalgebras.

If W is Z_2-graded and $s \in Sn$ is the transposition $(i, i+1)$, as an operator on $W^{[n]}$ let s be the map $I^{[i-1]} \otimes T \otimes I^{[n-i-1]}$. This extends to give $W^{[n]}$ the structure of an Sn module. The elements fixed under the action of Sn are called the symmetric tensors of degree n. For an ordered set G and $\{w_\gamma\}_{\gamma \in G} \subset W$, Sw^e is defined in the same manner as before, the only difference being the new action of Sn on $W^{[n]}$. By coanticommutativity and coassociativity, $\delta^{n-1}(C_n)$ consists of symmetric tensors of degree n.

Let F be a graded coconnected Hopf algebra, within F^0 lies a unique maximal coalgebra which is an algebra by maximality; hence, F^0 contains a unique maximal Hopf algebra H.

THEOREM 4. *Let $\{l_\gamma\}_{\gamma \in G_1}$ be a basis for L^1, let C_γ be the coalgebra spanned by* 1 *and l_γ, order G_1. F is isomorphic to $H \otimes (\otimes_{G_1} C_\gamma)$ as a coalgebra; an isomorphism is given by the map $h \otimes l_{\gamma_1} \otimes \cdots \otimes l_{\gamma_n} \to hl_{\gamma_1} \cdots l_{\gamma_n}$, where $h \in H$ and $\gamma_1 < \cdots < \gamma_n$. (Recall the coalgebra structure of $(\otimes_{G_1} C_\gamma)$ is the coalgebra structure on the tensor product of graded coalgebras; hence, is isomorphic to the coalgebra structure of the exterior algebra on L^1.)*

Proof. The above map is a coalgebra morphism and by Lemma 1 is injective. Let M be the image of the map, the space spanned by the monomials $hl_{\gamma_1}\cdots l_{\gamma_n}$, *we shall show $TL_M=TL_F$ which by Lemma 2 implies $M=F$. First we must show* $TL_H=TL_F\cap T(L^0)$. (We are considering $T(L^0)\subset TL\subset TF$.) Clearly, $TL_H\subset TL_F \cap T(L^0)$, suppose $x\in F_n$ where $\delta^{n-1}(x)\in T(L^0)$. We show by descending induction on s that there is $y_s\in F$ where $\delta^{n-1}(y_s)=\delta^{n-1}(x)$ and $\delta^s(y_s)\in H^{[s+1]}$. Let $y_{n-1}=x$, it has the desired properties. Suppose we have y_s, $s>0$, we consider $\delta^{s-1}(y_s)\in F^{[s]}$. Since $(\delta\otimes I^{[s-1]})\delta^{s-1}(y_s)=\delta^s(y_s)\in H^{[s+1]}$, it follows $\delta^{s-1}(y_s)\in(\operatorname{Ker}\delta)\otimes F^{[s-1]}+\delta^{-1}(H\otimes H)\otimes H^{[s-1]}$. We have $\delta^{-1}(H\otimes H)=H\oplus L^1$, $\operatorname{Ker}\delta=L\oplus k$ and $\operatorname{Im}\delta^{s-1}\subset F^{+[s]}$ so $\delta^{s-1}(y_s)\in L\otimes F^{+[s-1]}+H^{+[s]}$. By symmetry we have $\delta^{s-1}(y_s)\in L^{[s]}+H^{+[s]}$.

Let $\{l_\gamma\}_{\gamma\in G_0}$ be an ordered basis for L^0. Let $G=G_0\cup G_1$, G has ordering induced by the ordering of G_0 and G_1 and $G_0<G_1$. For the vector $e=(e_\gamma)_{\gamma\in G}$, let e^i be the vector $(e_\gamma)_{\gamma\in G_i}$, $i=0, 1$.

Write $\delta^{s-1}(y_s)=\sum_1^t\lambda_iSl^{e_i}+Y$, where $Y\in H^{+[s]}$ and t is minimal. If $t=0$, $\delta^{s-1}(y_s)\in H^{+[s]}$ and we can let $y_{s-1}=y_s$. Otherwise if $t\neq 0$, for some maximal $\phi\in G_1$, $e_{j,\phi}\neq 0$, say $j=t$, by coanticommutativity $e_{i,\gamma}=0$ or 1 for $\gamma\in G_1$, so $e_{t,\phi}=1$. Let $a'\in F'^1$ where $\langle a', l_\gamma\rangle=\delta_{\phi,\gamma}$, then by (7), $\delta^{s-2}(a'\cdot y_s)=\sum\lambda_ie_{i,\phi}Sl^{(e_i-1_\phi)}$. So $\delta^{s-1}((a'\cdot y_s)l_\phi)=\sum_1^t\lambda_ie_{i,\phi}Sl^{e_i}$ and $\delta^{s-1}(y_s-(a'\cdot y_s)l_\phi)=\sum_1^{t-1}\lambda_i(1-e_{i,\phi})Sl^{e_i}+Y$, this contradicts the minimality of t; hence, $t=0$. The induction step on s completed, we arrive at y_0 where $\delta^{n-1}(y_0)=\delta^{n-1}(x)$ and $\delta^0(y_0)\in H$; the latter implies $y_0\in H$. We have $TL_H=TL_F\cap T(L^0)$.

Now we show $TL_M=TL_F$. Let $x\in F_n$ and $\delta^{n-1}(x)=\sum_1^t\lambda_iSl^{e_i}$. We induct on t. If $t=0$ then $0\in M$ and $\delta^{n-1}(0)=\delta^{n-1}(x)$. Assume $t\geqq 1$. In the expression for $\delta^{n-1}(x)$ choose j where $r=|(e_j)^1|$ is maximal—say $j=t$. Let $\{d_\gamma\}_{\gamma\in G_1}\subset F'^1$ be dual to $\{l_\gamma\}_{\gamma\in G_1}$ and let $a'=d^{(e_t)^1}$. By (7), $\delta^{n-r-1}(a'\cdot x)=\sum_J\lambda_iSl^{(e_i)^0}$, where $J=\{i\mid(e_i)^1=(e_t)^1\}$. By the preceding paragraph there is $h\in H$ where $\delta^{n-r-1}(h)=\delta^{n-r-1}(a'\cdot x)$. Let $w\equiv hl^{(e_t)^1}\in M$. Then $\delta^{n-1}(w)=\sum_J\lambda_iSl^{e_i}$ and $\delta^{n-1}(x-w)=\sum_1^{t-1}\tau_iSl^{e_i}$ for appropriate $\tau_i\in k$. Thus we are done by the induction on t. Q.E.D.

Bibliography

1. P. Cartier, *Hyperalgebres et groupes de Lie formels*, Seminaire "Sophus Lie", 2e annee, 1955/1956.

2. E. Halpern, *Twistedpolynomial hyperalgebras*, Mem. Amer. Math. Soc. No. 29 (1958), 61 pp.

3. J. Milnor and J. Moore, *On the structure of Hopf algebras*, Ann. of Math. (2) **81** (1965), 211–264.

Massachusetts Institute of Technology,
Cambridge, Massachusetts