POLYNOMIAL-DUAL COALGEBRA STRUCTURE IN HOPF ALGEBRAS

by

P. BRIAN SHAY

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

1972

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

May 16, 1972

Alphonse T. Vasquez, Chairman
Examining Committee

Alex Heller, Executive Officer

Professor Eldon Dyer
Professor Alex Heller
Professor John C. Moore

Supervisory Committee

To

JOHN C. MOORE

for his influential work

and a train ride to New York.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I thank Professor Alphonse Vasquez, my advisor, for his extraordinary teaching, his patient insistence on clarity, and primarily, for the ever-narrowing focus which led me to this work. I thank Professor Alex Heller for his unmodified enthusiasm and an overview which has had an important influence on the organization of my computational results. I thank Professor Eldon Dyer for a bold approach to difficult calculations which I owe directly to him. For hundreds of generous hours of discussion and lectures, I am grateful to each of them.

I thank Professors Dale Husemoller and Raymond Hoobler for references which saved me much blind effort, and Steve Althoen for his invaluable curiosity about symmetric functions.

I thank my dear wife, Karla, for our years of uninterrupted laughter, which made this work so easy.

I thank the National Science Foundation, the disbursers of N.D.E.A. funds, and the Personnel and Budget Committee of the Mathematics Department at Hunter College for generous support.

I thank Ms. Ione Hutson, who patiently dealt with a first draft which I thought was a final manuscript, for her excellent typing.

INTRODUCTION

We provide a method of exposing polynomial-dual coalgebra structure in Hopf algebras which are torsion-free over rings of characteristic zero. If sufficiently many sequences dual to the powers of polynomial generators are available, one can apply a structure theorem due to Borel and Sweedler (Chapter I). Over fields of characteristic zero, such sequences can easily be constructed. We have devised a method for detecting such sequences over arbitrary ground rings of characteristic zero in torsion-free situations. This is organized as an obstruction theory (Chapter II).

The central idea is that primitives are related to indecomposables by Newton's formula far more generally than has been supposed. This is familiar in $H^*(BU;Z)$, but the commutativity, associativity, and the traditional description of this Hopf algebra in symmetric function terminology seem to have combined to give this relationship an accidental appearance.

A thorough account of the effect of choices involved in constructing such sequences is given in Chapter II. The hypothesis of associativity is added at this point to make a rather difficult proof legible (Proposition 2). If challenged, we can do without this assumption and retain in non-associative cases the power of Proposition 3 for proving Hopf algebras haven't polynomial dual coalgebra structure.

As trivial consequences of Chapter II, one can show, e.g., if $\mathcal{A}$ is a connected, commutative, associative, co-commutative, co-associative torsion-free Hopf algebra over Z, whose primitives, $P(\mathcal{A})$, form a free abelian group, then

(i) $\mathcal{A}$ <u>has</u> polynomial-dual coalgebra structure if $\mathcal{A}$ is filtered, is a λ-ring, and $P(\mathcal{A})$ is a ψ-module.

(ii) $\mathcal{H}$ hasn't polynomial-dual coalgebra structure if $\mathcal{H}$ is graded, lies in even degrees, $\exists\, x \in (P(\mathcal{H}))_i$, $(P(\mathcal{H}))_{p^n i} = 0$, where p does not "divide" x^{p^n} for some $i,n,p \in Z^+$, p prime.

Studying $H^*(BU;Z)$ from the coalgebraic point of view developed in Chapter I and II, in Chapter III we find a basis which is better behaved under Whitney sum than the standard basis consisting of monomials in the Chern classes. A start is made on the computation of the mod p Steenrod algebra action on $H^*(BU;Z_p)$ in Chapter V. The results are flattering to the basis of Chapter III.

An argument is given in Chapter IV that the group of Hopf algebra automorphisms of $H^*(BU;Z)$ is isomorphic to $Z_2 \times Z_2$.

Chapters VII and VIII provide a standard algebra presentation for the algebra structure of associative Hopf algebras enjoying polynomial-dual coalgebra structure. (Associativity can probably be dropped as a hypothesis, with slight additional complication in the presentation.)

By truncation of sequences at powers of primes (see the curious result of Chapter VI), it is quite possible that this presentation will do for a very wide class of associative, co-associative, co-commutative, connected Hopf algebras.

In Chapters IX and X we adapt the scheme of Chapters I and II to an important universal construction. An application is provided which is sufficiently remote from Newton's formula in the symmetric function setting to indicate a possible wide range of use of these methods as a computing tool.

Note on Terminology

a) Rings will always be commutative and associative with unit.

b) Algebras and coalgebras will always be provided with units and augmentations, respectively.

c) A connected algebra is an algebra provided with a splitting (an augmentation) for its unit. A connected coalgebra is provided with a map from the ground ring (a unit) which is split by its augmentation. In either case, the ring is a direct summand in a canonical way. A connected Hopf algebra is connected as an algebra, via its augmentation, or equivalently, as a coalgebra, via its unit.

d) We do not require Hopf algebras to be associative (important) or coassociative, filtered, or graded (unimportant).

e) A tower in a connected coalgebra, $(C, \Delta, \epsilon, \eta)$, is a sequence of elements $\{P_i\}_{i=0,1,\ldots,n}$ satisfying: $\forall\, i\ , \Delta(P_i) = \sum_{i=j+k} P_j \otimes P_k$ and $\epsilon(P_i) = \delta_{i,0}$; $\eta(1) = P_0$. Clearly a tower is a subcoalgebra. n may be ∞ . We are aware of departing from the standard terminology, "divided power sequence," in making this definition. We reason as follows: "divided power" is an algebraic notion, "divided power sequence" is a coalgebraic notion. Furthermore, we show below (p.7) that to each divided power sequence in a Hopf algebra there corresponds a family of primitives. It is exactly when each of these primitives is zero that the divided power sequence is a sequence of divided powers in torsion-free situations. It seems unreasonable that this rare situation should be patronymic. (When limiting discussion to fields, as is the tradition, this distinction must be regarded as essentially rude.) If "tower" is not sufficiently evocative, perhaps "diagonal tower" is an alternative.

CHAPTER I

A CLASSICAL THEOREM OF BOREL

We generalize in part a theorem first given in dual form by Borel (see Milnor & Moore [1]). For a generalization of this formulation, when R is a field, see Sweedler [2].

Theorem 1. Let $\{\mathcal{H};(\circ,\nabla);(\Delta,\varepsilon)\}$ be a filtered (graded and lying in even degrees), connected, cocommutative, coassociative Hopf algebra over commutative ring R. Suppose $P(\mathcal{H})$ has an ordered basis $\{P_{\alpha,1}\}\ \alpha \in \mathcal{A}$, each element supporting an infinite tower $\{P_{\alpha,j}\}\ j \in Z^+$. Then $\mathcal{H}$ is free as an R-module with basis $\{1,(\ldots((P_{\alpha_1,i_1} P_{\alpha_2,i_2}) P_{\alpha_3,i_3}) \ldots P_{\alpha_k,i_k}) \mid i_1,i_2,\ldots,i_k \in Z^+-\{0\},\ \alpha_1 < \alpha_2 < \ldots < \alpha_k \in \mathcal{A}\}$.

Proof: As $\mathcal{H}$ is not necessarily associative, we have chosen the convention - parentheses accumulate on the left. It is trivial to prove via induction and the formulas $P_{\alpha,i} \to \sum_{i+j=k} P_{\alpha,j} \otimes P_{\alpha,k}$ that, if $\alpha_1,\alpha_2,\ldots,\alpha_k \in \mathcal{A}$, $(\ldots(P_{\alpha_1,i_1},P_{\alpha_2,i_2}) \ldots P_{\alpha_k,i_k}) \xrightarrow{\Delta} \sum_{j=1}^{k} \sum_{i_j'+i_j''=i_j}$ $(\ldots(P_{\alpha_1,i_1'} P_{\alpha_2,i_2'}) \ldots P_{\alpha_k,i_k'}) \otimes (\ldots(P_{\alpha_1,i_1''} P_{\alpha_2,i_2''}) \ldots P_{\alpha_k,i_k''})$. As this formula is the only coalgebraic computation which figures in the proof, we shall feel free to eliminate parentheses. Moreover, we shall abbreviate $P_{\alpha_1,i_1} \ldots P_{\alpha_k,i_k}$ by $P_{A,I}$ and say, with less confusion, that $P_{A,I} \xrightarrow{\Delta} \sum_{J+K=I} P_{A,J} \otimes P_{A,K}$. Notice that any tensor of type $P_{A',I'} \otimes P_{A'',J'}$ may be written as $P_{A,I} \otimes P_{A,J}$, where A is the ordered set $A' \cup A''$, and $i_r = i_{r'}$ if $\alpha_r \in A'$, $i_r = 0$ if $\alpha_r \in A - A'$, and $j_s = j_{s'}$ if $\alpha_s \in A''$, $j_s = 0$ if $\alpha_s \in A - A''$.

We refer to $P_{A,I}$ as a tower monomial. We say the width of $P_{A,I}$ is j if $I = (i_1, i_2, \ldots, i_k)$ and exactly j of the i's are not zero. We write $I+J$ for $(i_1+g_1, \ldots, i_k+j_k)$. The width of $P_{A,I} \otimes P_{A,J}$ is defined to be the width of $P_{A,I+J}$. Let $\ell(I) = i_1+i_2+\ldots+i_k$, if $I = (i_1, i_2, \ldots, i_k)$. The length of $P_{A,I}$ $(P_{A,I} \otimes P_{A,J})$ is $\ell(I)$ $(\ell(I+J))$.

We first show that the elements we claim are a basis are at least independent. Let $\sum_{A,I} C_{A,I} P_{A,I} = 0$ where $C_{A,I} = 0$ unless $i_1>0, i_2>0 \ldots i_k>0$ where $I = (i_1, i_2, \ldots, i_k)$. The maximum length of the terms $P_{A,I}$ such that $C_{A,I}$ is non-zero must be greater than 1 or we are describing an impossible linear combination in our basis of primitives.

Let us suppose that coefficients $C_{A,I}$ of all tower monomials $P_{A,I}$ of length greater than n are zero in our relation, and that no relations exist among tower monomials of length less than n. We need only show that the coefficients of the tower monomials of length n are zero. Let us apply $(I-\eta\epsilon)^{\otimes n} \circ \Delta \otimes I^{n-2} \circ \ldots \circ \Delta = (I-\eta\epsilon)^{\otimes n} \circ \Delta_n$ to the relation, where $I: \mathcal{A} \to \mathcal{A}$ is the identity. One easily computes the image to be

$$\sum_{\ell(I)=n} C(\alpha_1, \alpha_2, \ldots, \alpha_k),\ (i_1, i_2, \ldots, i_k) \sum_{\sigma \in \Sigma_n / \Sigma_{i_1} \times \Sigma_{i_2} \times \ldots \times \Sigma_{i_k}} \sigma \circ \underbrace{P_{\alpha_1,1} \otimes P_{\alpha_1,1} \otimes \ldots \otimes P_{\alpha_1,1}}_{i_1 \text{ factors}} \otimes \underbrace{P_{\alpha_2,1} \otimes \ldots \otimes P_{\alpha_2,1}}_{i_2 \text{ factors}} \ldots \otimes \underbrace{P_{\alpha_k,1} \otimes \ldots \otimes P_{\alpha_k,1}}_{i_k \text{ factors}}$$

for the $C_{A,I}$ with $\ell(I) > n$ are zero, and $\Delta_n P_{A,I}$ is a sum of tensors with at least one factor 1 if $\ell(I) < n$. Such tensors project to zero under $(I-\eta\epsilon)^{\otimes n}$. But the tensors $\{P_{\beta_1,1} \otimes P_{\beta_2,1} \otimes \ldots \otimes P_{\beta_n,1}\}(\beta_1, \ldots, \beta_n) \in \mathcal{A}^n$ of $P(\mathcal{A})^{\otimes n} \subseteq \mathcal{A}^{\otimes n}$ are independent, so that $C_{A,I} = 0$ if $|I| = n$. This completes a proof of independence.

We are now faced with showing that $\mathcal{H}_i$ is spanned by tower monomials, $\forall\ i \in Z^+-\{0\}$. We assume this is true for $i_0 \leq i < n$ where $\mathcal{H}_{i_0}$ is the first filtrand of $\mathcal{H}$ which is strictly bigger than $\mathcal{H}_0$. $\mathcal{H}_{i_0}$ is, of course, spanned by a subset of the primitives. Let $x \in \mathcal{H}_n$, with zero R component. Then $x \xrightarrow{\Delta} x \otimes 1 + 1 \otimes x + \sum_A \sum_{I,J} C^A_{I,J} P_{A,I} \otimes P_{A,J}$ by inductive assumption. Notice that no I or $J = (0,0,\ldots,0)$ if $C^A_{I,J} \neq 0$. Suppose that we can show $C^A_{I,J} = C^A_{I',J'}$ whenever $I+J = I' + J'$. Denote the common value by C^A_K , where $K = I+J$. Let us compute Δ on $x - \sum_{A,K} C^A_K P_{A,K}$. We get

$$(x - \sum_{A,K} C^A_K P_{A,K}) \otimes 1 + 1 \otimes (x - \sum_{A,K} C^A_K P_{A,K})$$

$$+ \sum_A \sum_K \sum_{I+J=K} (C^A_{I,J} - C^A_K) P_{A,I} \otimes P_{A,J}$$

$$= (x - \sum_{A,K} C^A_K P_{A,K}) \otimes 1 + 1 \otimes (x - \sum_{A,K} C^A_K P_{A,K}) .$$

Hence,

$$x - \sum_{A,K} C^A_K P_{A,K} \in P(\mathcal{H}) \quad \text{and} \quad x = \sum_{A,K} C^A_K P_{A,K} + \sum_{\alpha \in \mathcal{A}} d_\alpha P_{\alpha,1} ,$$

and x is in the span of the tower monomials, as required. It suffices to prove the following

Lemma: If $I+J = I'+J'$, then $C^A_{I,J} = C^A_{I',J'}$.

Proof: We have both cocommutativity and coassociativity to help us. Cocommutativity is used only in the following very special case: Suppose $P^A_I \otimes P^A_J = P_{\alpha,1}P_{\beta,0} \otimes P_{\alpha,0}P_{\beta,1} = P_{\alpha,1} \otimes P_{\beta,1}$. Clearly $P_{A,I'} \otimes P_{A,J'} = P_{\beta,1} \otimes P_{\alpha,1}$ if $I'+J' = I+J$, excluding I' or $J' = (0,0)$. By cocommutativity, and the independence of tower elements in filtrands

below $\mathcal{H}_n$, we have $C^{(\alpha,\beta)}_{(0,1),(1,0)} = C^{(\alpha,\beta)}_{(1,0),(0,1)}$. This shallow use of cocommutativity is not very surprising. One should recall that iff generators of an algebra commute, the algebra is commutative.

Coassociativity will provide the remaining equations. Let us apply both $(\Delta\otimes I)\circ\Delta$ and its equal $(I\otimes\Delta)\circ\Delta$ to x and project away from $\mathcal{H}_0\otimes\mathcal{H}\otimes\mathcal{H}\cup\mathcal{H}\otimes\mathcal{H}_0\otimes\mathcal{H}\cup\mathcal{H}\otimes\mathcal{H}\otimes\mathcal{H}_0$. $(I-\eta\epsilon)^{\otimes 3}\circ(\Delta\otimes I)\circ\Delta x =$

$$\sum_A \sum_{\substack{I\neq 0\\ J\neq 0}} \sum_{\substack{I'+I''=I\\ I'\neq 0, I''\neq 0}} C^A_{I,J}\, P^A_{I'}\otimes P^A_{I''}\otimes P^A_J \ .$$

$$(I-\eta\epsilon)^{\otimes 3}(I\otimes\Delta)\circ\Delta x = \sum_A \sum_{\substack{I\neq 0\\ J\neq 0}} \sum_{\substack{J'+J''=J\\ J'\neq 0, J''\neq 0}} C^A_{I,J}\, P^A_I\otimes P^A_{J'}\otimes P^A_{J''} \ .$$

From these two expressions and the independence of the monomials in filtrands below $\mathcal{H}_n$, the coefficient of $P^A_R\otimes P^A_S\otimes P^A_T$, $R\neq 0$, $S\neq 0$, $T\neq 0$ is $C^A_{R+S,T} = C^A_{R,S+T}$. (Notice $\ell(R)+\ell(S)+\ell(T)\geq 3$). As an illustration, let us assume the width of $P_{A,I}\otimes P_{A,J}$ is 1 , its length is $\ell\geq 3$. By the formula $C^A_{R+S,T} = C^A_{R,S+T}$, we have

$$C^{(\alpha)}_{(2),(\ell-2)} = C^{(\alpha)}_{(1)+(1),(\ell-2)} = C^{(\alpha)}_{(1),(1)+(\ell-2)} = C^{(\alpha)}_{(1),(\ell-1)}$$

$$C^{(\alpha)}_{(3),(\ell-3)} = C^{(\alpha)}_{(2)+(1),(\ell-3)} = C^{(\alpha)}_{(2),(1)+(\ell-3)} = C^{(\alpha)}_{(2),(\ell-2)}$$

$$\vdots$$

$$C^{(\alpha)}_{(\ell-1),(1)} = C^{(\alpha)}_{(\ell-2)+(1),(1)} = C^{(\alpha)}_{(\ell-2),(1)+(1)} = C^{(\alpha)}_{(\ell-2),(2)}$$

so that

$$C^{(\alpha)}_{I,J} = C^{(\alpha)}_{I',J'} \quad \text{whenever} \quad I+J = I'+J' = (\ell) \ .$$

We say (I,J) and (I',J') are adjacent if $i_r = i_{r'}$ except when $r = s$, $j_r = j_{r'}$ except when $r = s$ and $i_s + j_s = i_{s'} + j_{s'}$.

Clearly, as in the illustration, $C^A_{I,J} = C^A_{I',J'}$ if (I,J) and (I',J') are adjacent.

For the general case, we merely observe that if $I+J = I'+J' = K$, $I' \neq 0$, $J' \neq 0$, $I \neq 0$, $J \neq 0$, and $\ell(K) \geq 3$, then there is obviously a sequence of pairs $(I_1,J_1), (I_2,J_2),\ldots,(I_p,J_p)$ satisfying

i) (I_q,J_q) is adjacent to (I_{q+1},J_{q+1}), $q = 1,2,\ldots,p-1$.

ii) $I_q \neq 0$, $J_q \neq 0$, $q = 1,2,\ldots,p$.

iii) $(I_1,J_1) = (I,J)$

iv) $(I_p,J_p) = (I',J')$.

It follows that $C^A_{I,J} = C^A_{I',J'}$, and we are done.

CHAPTER II

AN OBSTRUCTION THEORY FOR TOWER CONSTRUCTION

Let $\{\mathcal{H}; (\circ, \eta); (\Delta, \epsilon)\}$ be a connected Hopf algebra over a commutative ring with unit, R . A sequence of elements $\{P_i\}_{i = 0,\ldots,n(\ldots)}$ is said to be a (diagonal) tower of height n (of infinite height) over P_1 if $P_i \xrightarrow{\Delta} \sum_{j+k=i} P_j \otimes P_k$, $i = 0,1,\ldots,n(\ldots)$ and $\epsilon(P_i) = \delta_{i,0}$. P_i may be referred to as the i^{th} story of the tower. If $\mathcal{H}$ is to be graded, we restrict P_1 to the even dimensions. Evidently, P_1 belongs to the submodule of primitive elements, denoted $P(\mathcal{H})$.

We wish to state and discuss criteria for the construction of towers over primitive elements. If $P \in P(\mathcal{H})$, $n > 1$, P_n may clearly be replaced by $P_n + P$ without violating the coalgebraic conditions. Hence, any stepwise procedure for raising towers is subject to choices at each step. We attempt to describe accurately the effect of such choices.

We do not insist on graded Hopf algebras, but we mention as necessary any peculiarities which would be caused by grading. Generally, there will be no sign troubles, as our towers will lie in even dimensions.

Suppose now that P_1 is a primitive element of $\mathcal{H}$. We construct two sequences, $\{P_i\}$ and $\{K_i\}$ in alternate recursion as follows: We let $K_1 = 0$. Suppose $\forall i < n$ that K_i and P_i are defined, that $iP_i - K_i$ is primitive, and that $P_i \xrightarrow{\Delta} \sum_{j+k=i} P_j \otimes P_k$. (Note that P_1 and K_1 satisfy these requirements.) Let $K_n \equiv \sum_{\ell+m=n} P_\ell (mP_m - K_m)$ (no

zero subscripts). We have

Proposition 1: (a) $\exists\, P_n$ s.t. $P_n \xrightarrow{\Delta} \sum_{i+j=n} P_i \otimes P_j$ implies

$nP_n - K_n$ is primitive.

(b) If $\mathcal{H} \otimes \mathcal{H}$ is n-torsion free, $\exists\, P_n$ s.t. $nP_n - K_n$

is primitive implies $P_n \to \sum_{i+j=n} P_i \otimes P_j$.

Proof: We simply demonstrate that $K_n \xrightarrow{\Delta} K_n \otimes 1 + 1 \otimes K_n + n(\sum_{i+j=n} P_i \otimes P_j)$.

(a) and (b) follow immediately.

Computing:

$$\Delta K_n = \sum_{\ell+m=n} \Delta P_\ell \cdot \Delta(mP_m - K_m) =$$

$$\sum_{\ell+m=n} P_\ell(mP_m - K_m) \otimes 1 + 1 \otimes P_\ell(mP_m - K_m) +$$

$$\sum_{\ell+m=n} P_\ell \otimes (mP_m - K_m) + \sum_{\ell+m=n} (\ell P_\ell - K_\ell) \otimes P_m +$$

$$\sum_{i+j+k=n} P_i(jP_j - K_j) \otimes P_k + P_k \otimes P_i(jP_j - K_j) =$$

$$K_n \otimes 1 + 1 \otimes K_n + n \sum_{\ell+m=n} P_\ell \otimes P_m - \sum_{\ell+m=n} P_\ell \otimes K_m$$

$$- \sum_{\ell+m=n} K_\ell \otimes P_m + \sum_{h+k=n} K_h \otimes P_k + P_k \otimes K_h$$

$$= K_n \otimes 1 + 1 \otimes K_n + n \cdot \sum_{\ell+m=n} P_\ell \otimes P_m .$$

Notice - we are not using any commutativity or associativity relations. We have provided essentially algebraic criteria for the extension of towers, a coalgebraic feature of the Hopf algebra; i.e., if we wish to extend a tower, we multiply and add certain elements associated with the tower, and test for divisibility in the quotient module $\mathcal{H}/P(\mathcal{H})$.

These criteria fail only with the existence of Z-torsion, and then only at certain stages.

For example, suppose R is a field of characteristic p. If n is not divisible by p, we can divide any element by n in $\mathcal{H}$, let alone in $\mathcal{H}/P(\mathcal{H})$. So a canonical process for constructing towers over primitives is available except at multiples of p. At each multiple of p, there may or may not be an extension. However, if there is, we can push upwards to the next multiple of p without obstruction.

In the notation above, for $i = 2,\ldots,p-1$, $K_i = P_1^i/(i-1)!$ and P_i is the familiar $P_1^i/i! = K_i/i$. P_p is not algebraically related to P_1, if it exists. $K_{p+1} = P_p P_1 - P_1^{p+1}/(p-1)!$, $P_{p+1} = K_{p+1}$. $K_{p+2} = P_p P_1^2 - 3 \cdot P_1^{p+2}/(p-1)!\,2!$, $P_{p+2} = K_{p+2}/2$, etc. (For an improvement, when R is perfect, see Sweedler [2], Lemma 7).

Suppose P_i is chosen for $i < n$, $\mathcal{H} \otimes \mathcal{H}$ has no n-torsion, and K_n is <u>not</u> divisible by n modulo primitives; i.e., K_n is not in $\mathrm{Ker}(\mathcal{H} \approx \mathcal{H} \otimes Z \to \mathcal{H}/P(\mathcal{H}) \otimes Z \to \mathcal{H}/P(\mathcal{H}) \otimes Z_n)$. There cannot be a tower of height n which extends $\{P_i\}$ $i < n$. Is there an inherent obstruction to raising any tower of height n over P_1, or have we merely made unfortunate choices relative to our freedom within $P(\mathcal{H})$ in constructing the lower stories? We are anxious to state algebraic relations between towers over the same primitive which will illuminate this problem. Until we develop adequate notation, however, suffice it to say that only the choices at the stories numbered by the divisors of n are relevant to this question.

As we are not restricting ourselves to commutative Hopf algebras, we need some technical information about the way primitives fail to

commute with towers.

It is a triviality that $[Q,P] \equiv QP - PQ$ is primitive if P and Q are. Suppose that $\{P_i\}_{i=1,\ldots,n}$ is a tower over the primitive P_1, and that Q is primitive. We shall assign to each pair (Q,P_i) a primitive, denoted $p(Q,P_i)$. In particular $p(Q,P_1)$ will be $[Q,P_1]$. Let us suppose that $p(Q,P_i)$ have been defined for $i < n$. Let

$$p(Q,P_n) \equiv [Q,P_n] - \sum_{j+k=n} P_k\, p(Q,P_j) \qquad \text{(no zero subscripts)}.$$

We show that $p(Q,P_n)$ is primitive.

$$\Delta p(Q,P_n) = \Delta Q \Delta P_n - \Delta P_n \Delta Q - \sum_{j+k=n} \Delta P_k \cdot \Delta p(Q,P_j)$$

$$= p(Q,P_n)\otimes 1 + 1\otimes p(Q,P_n) + \sum_{j+k=n} \{QP_j\otimes P_k + P_k\otimes QP_j$$

$$- P_jQ\otimes P_k - P_k\otimes P_jQ\} - \sum_{j+k=n} \{P_k\otimes p(Q,P_j) + p(Q,P_j)\otimes P_k\}$$

$$- \sum_{h+i+k=n} \{P_k\otimes P_i p(Q,P_h) + P_i p(Q,P_h)\otimes P_k\} = p(Q,P_n)\otimes 1$$

$$+ 1\otimes p(Q,P_n) + \sum_{j+k=n} \{[Q,P_j]\otimes P_k + P_k\otimes [Q,P_j]\}$$

$$- \sum_{j+k=n} \{P_k\otimes p(Q,P_j) + p(Q,P_j)\otimes P_k\} - \sum_{j+k=n} \{P_k\otimes \sum_{h+i=j} P_i p(Q,P_h)$$

$$+ \sum_{h+i=j} P_i p(Q,P_h)\otimes P_k\} = p(Q,P_n)\otimes 1 + 1\otimes p(Q,P_n)\ .$$

This process can be iterated, of course. Since $p(Q,P_i)$ is primitive, $p(p(Q,P_i),P_j)$ is defined, and is primitive. Hence $p(p(p(Q,P_i),P_j),P_k)$ is, etc. One can easily convince oneself of the efficiency of the notation if one tries to write these primitives non-recursively.

We introduce double positive integer notation for elements in $\mathcal{V}$ — $P_{i,j}, K_{i,j}, V_{i,j}$ — with the following conventions.

(a) $\forall i$ $P_{i,1}$ is primitive.

(b) $\forall i$ $\{P_{i,j}\}_{j=1,\ldots,n_i}$ is a tower of height n_i over $P_{i,1}$.

(c) $\forall i$ $K_{i,j}$ is, of course, $\sum_{k+\ell=j} P_{i,k}(\ell P_{i,\ell}-K_{i,\ell})$ $\forall j$ and $(\ell P_{i,\ell}-K_{i,\ell})$ is primitive $\forall \ell$.

(d) $\forall i$, $V_{i,j} = i(jP_{i,j}-K_{i,j})$ $\forall j$.

(e) if $\mathscr{X}$ is graded, P_{i_1,j_1} and P_{i_2,j_2} have the same degree if and only if $i_1 j_1 = i_2 j_2$.

We now state a lemma which essentially says: If a modification by a primitive element is made at the i^{th} story of a tower of height n, i.e., P_i is replaced by P_i+P, the modified tower of height i can be extended to a tower of height n, if a sufficiently high tower can be constructed over P.

Lemma: Let $\{P_{i,j}\}_{j=1,\ldots,n_i}$ and $\{P_{k,\ell}\}_{\ell=1,\ldots,n_k}$ be towers of heights n_i and n_k respectively. Let $k = g \cdot i$, $g \geq 2$. Then both $\{\sum_{j+g\ell=m} P_{i,j} P_{k,\ell}\}_{m=1,\ldots}$ and $\{\sum_{j+g\ell=m} P_{k,\ell} P_{i,j}\}_{m=1,\ldots}$ are towers of height $\min\{n_i, gn_j + (g-1)\}$ over $P_{i,1}$.

Proof: Trivial. Apply Δ and organize indices.

Corollary: Let $\{P_{h,j}\}_{j=1,\ldots}$ be towers of height n_h, $h = 1,\ldots,k$. Then $\{\sum_{\Sigma i_\ell j_\ell = m} (\ldots(P_{i_1,j_1} P_{i_2,j_2}) \ldots P_{i_k,j_k})\}_{m=1,2,\ldots}$ is a tower over $P_{1,1}$ of height $\min\{hn_h+(h-1)\}$ for any permutation i of $(1,2,\ldots,k)$,

and is said to be the i-amalgamation (or canonical amalgamation if i = identity) of the towers $\{P_{h,j}\}$.

We now graph the construction of a tower, displaying the effect of choice, page 12. We use the notation $P \to K$ since K is determined by lower P's, and $K \dashrightarrow P$ since P is not uniquely determined by K , but represents a choice. We use the canonical amalgamation described in the corollary, abbreviated as $\{\overline{P}_j\}$.

We call the towers $\{P_{h,j}\}$ $h > 1$, branch towers, and the primitives $\{P_{h,1}\}$ $h > 1$, modifying primitives. We are clearly portraying only "first-order effects", i.e., we make full use of choices at each story, but each modifying primitive comes equipped with a tower. We are not describing the effect of choices on these branch towers. Our fundamental result is:

Proposition 2: If $\mathscr{V}$ is associative,

$$\overline{K_m} = \sum_{i|m} i\, K_{i,m/i} + \sum_{k>1} \{ m\, P_{i_1,j_1} P_{i_2,j_2} \cdots P_{i_k,j_k} - p(p(\ldots(p(V_{i_1,j_1}, P_{i_2,j_2}),\ldots), P_{i_k,j_k})\} \,.$$

$$\sum i_\ell j_\ell = m \qquad i_1 < i_2 < \ldots < i_k$$

Proof: We proceed by induction. This is trivial for $m = 2$. Assume it is true for $j < m$. Then clearly in this range $j\,\overline{P_j} - \overline{K_j}$

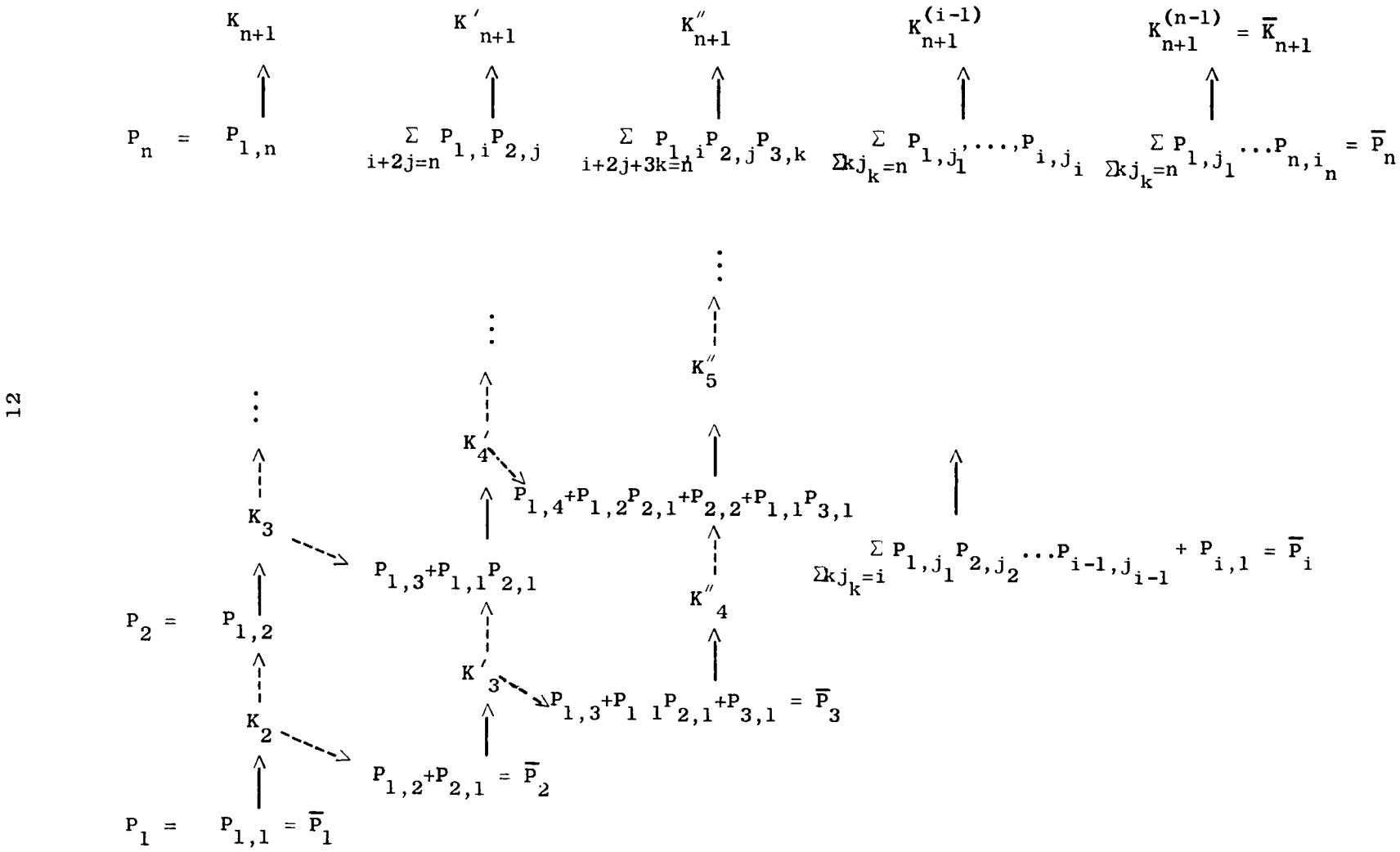
$$= \sum_{j=k\ell} V_{k,\ell} + \sum_{\Sigma i_\ell j_\ell = j} p(p(\ldots(p(V_{i_1,j_1}, P_{i_2,j_2})\ldots), P_{i_k,j_k}) \,.$$

$$i_1 < i_2 < \ldots < i_k$$

Of course $\overline{P_j} = \sum_{\Sigma i_\ell j_\ell = j} P_{i_1,j_1},\ldots,P_{i_k,j_k}$ and $\overline{K_m} = \sum_{r+s=m} \overline{P_r}(s\overline{P_s} - \overline{K_s})$.

$$i_1 < i_2 < \ldots < i_k$$

FIGURE 1


K_{n+1}
K'_{n+1}
K''_{n+1}
$K^{(i-1)}_{n+1}$
$K^{(n-1)}_{n+1} = \overline{K}_{n+1}$
$P_n = P_{1,n}$
$\sum_{i+2j=n} P_{1,i}P_{2,j}$
$\sum_{i+2j+3k=n} P_{1,i}P_{2,j}P_{3,k}$
$\sum_{\Sigma kj_k=n} P_{1,j_1},\ldots,P_{i,j_i}$
$\sum_{\Sigma kj_k=n} P_{1,j_1}\ldots P_{n,i_n} = \overline{P}_n$
K''_5
K'_4
K_3
$P_{1,4}+P_{1,2}P_{2,1}+P_{2,2}+P_{1,1}P_{3,1}$
$P_{1,3}+P_{1,1}P_{2,1}$
K''_4
$\sum_{\Sigma kj_k=i} P_{1,j_1}P_{2,j_2}\ldots P_{i-1,j_{i-1}} + P_{i,1} = \overline{P}_i$
$P_2 = P_{1,2}$
K'_3
K_2
$P_{1,3}+P_{1,1}P_{2,1}+P_{3,1} = \overline{P}_3$
$P_{1,2}+P_{2,1} = \overline{P}_2$
$P_1 = P_{1,1} = \overline{P}_1$

We now organize the "monomials" in this expression for $\overline{K_m}$. A first step is to group the monomials by the ordered subsets of "i" subscripts — i.e., we isolate monomials of the sorts

(*) $P_{g_1,j_1} P_{g_2,j_2} \cdots P_{g_{k-1},j_{k-1}} V_{g_k,j_k}$ where $\Sigma_{g_f j_f} = m$ and

(**) $P_{h_1,j_1} P_{h_2,k_2} \cdots P_{h_\ell,k_\ell} p(p\ldots(p(V_{h_{\ell+1},k_{\ell+1}},P_{h_{\ell+2},k_{\ell+2}}),\ldots),P_{h_m,k_m}$

where $\Sigma_{h_f k_f} = m$ and $\{g_1,g_2,\ldots,g_k\} = \{h_1,h_2,\ldots,h_m\}$.

If $i_1 < i_2 < \ldots < i_n$ are the distinct entries of these equal sets, we say the monomials are of type $\{i_1,i_2,\ldots,i_n\}$ and of width n . For example, $P_{1,2} P_{2,3} p(p(V_{2,4},P_{5,6}),P_{6,2})$ is of type $\{1,2,5,6\}$ and of width 4 . For a given i_r , let the i_r height of (*) be $\Sigma_{g_s=i_r} j_s$. and the i_r height of (**) be $\Sigma_{h_t=i_r} j_t$. Clearly these sums have only one or two summands. In the example, the 2 height is 7 , the 1,5, and 6 heights are 2,6, and 2 respectively.

We say a monomial is of type $\{(i_1,j_1),(i_2,j_2),\ldots,(i_k,j_k)\}_{\Sigma i_\ell j_\ell = m}$ if it is a monomial of type $\{i_1,i_2,\ldots,i_k\}$ and its i_r height is j_r . We now add monomials of the same type.

(i) type $\{(i,m/i)\}_{i\cdot m/i=m}$

$$\Sigma_{j'+j''=j} P_{i,j'} V_{i,j''} = \Sigma_{j'+j''=j} P_{i,j'} i(j'' P_{i,j''} - K_{i,j''})$$

$$= i K_{i,m/i} .$$

(ii) type $\{(i_1,j_1),(i_2,j_2)\}_{i_1j_1+i_2j_2=m}$.

$$P_{i_1,j_1}V_{i_2,j_2} + P_{i_2,j_2}V_{i_1,j_1} + \sum_{j_2'+j_2''=j_2} P_{i_1,j_1}P_{i_2,j_2'}V_{i_2,j_2''}$$

$$+ \sum_{j_1'+j_1''=j_1} P_{i_1,j_1'}P_{i_2,j_2}V_{i_1,j_1''} + \sum_{j_1'+j_1''=j_1} P_{i_1,j_1'}\,p(V_{i_1,j_1''},P_{i_2j_2})$$

$$+ \sum_{\substack{j_1'+j_1''=j_1\\ j_2'+j_2''=j_2}} P_{i_1,j_1'}P_{i_2,j_2'}\,p(V_{i_1,j_1''},P_{i_2,j_2''})$$

$$+ \sum_{j_2'+j_2''=j_2} P_{i_2,j_2'}\,p(V_{i_1,j_1},P_{i_2,j_2''})$$

$$= (i_2j_2\,P_{i_1,j_1}P_{i_2,j_2} - i_2\,P_{i_1,j_1}K_{i_2,j_2} + ([P_{i_2,j_2},V_{i_1,j_1}]$$

$$+ i_1j_1\,P_{i_1,j_1}P_{i_2,j_2'} - i_1\,K_{i_1,j_1}P_{i_2,j_2}) + (i_2\,P_{i_1,j_1}K_{i_2,j_2})$$

$$+ \Big(\sum_{j_1'+j_1''=j_1} P_{i_1,j_1'}[P_{i_2,j_2},V_{i_1,j_1''}] + i_1\,K_{i_1,j_1}P_{i_2,j_2}\Big)$$

$$+ \sum_{j_1'+j_1''=j_1} P_{i_1,j_1'}\{p(V_{i_1,j_1''},P_{i_2,j_2}) + \sum_{j_2'+j_2''=j_2} P_{i_2,j_2'}\,p(V_{i_1,j_1''},P_{i_2,j_2''})\}$$

$$+ \sum_{j_2'+j_2''=j_2} P_{i_2,j_2'}\,p(V_{i_1,j_1},P_{i_2,j_2''}) = m\,P_{i_1,j_1}P_{i_2,j_2}$$

$$+ \{[P_{i_2,j_2},V_{i_1,j_1}] + \sum_{j_2'+j_2''=j_2} P_{i_2,j_2'}\,p(V_{i_1,j_1},P_{i_2,j_2''})\}$$

$$+ \sum_{j_1'+j_1''=j_1} P_{i_1,j_1'}\cdot\{[P_{i_2,j_2},V_{i_1,j_1''}] + \sum_{j_2'+j_2''=j_2} P_{i_2,j_2'}\,p(V_{i_1,j_1''},P_{i_2,j_2''})$$

$$+ p(V_{i_1,j_1''},P_{i_2,j_2})\} = m\cdot P_{i_1,j_1}P_{i_2,j_2} - p(V_{i_1,j_1},P_{i_2,j_2}) .$$

(Recall the inductive definition of the pairing $p(\ ,\ )$. One should note the usefulness of writing AB as $[A,B] + BA$. This is the essential trick.)

(iii) type $\{(i_1,j_1),(i_2,j_2),\ldots,(i_k,j_k)\}_{\Sigma i_\ell j_\ell = m}$ $2 \le k < n$.

$$m \cdot P_{i_1,j_1} P_{i_2,j_2} \cdots P_{i_k,j_k} - p(\ldots(p(V_{i_1,j_1},P_{i_2,j_2}),\ldots,),P_{i_k,j_k})$$

by inductive assumption.

(iv) type $\{(i_1,j_1),(i_2,j_2),\ldots,(i_n,j_n)\}$.

We shall use the inductive assumption (iv), not for $\overline{K_m}$, but for $\overline{K}_{i_1 j_1 + \ldots + i_{n-1} j_{n-1} = m - i_n j_n}$. We look at some partial summands in the form of lemmas and consolidate in the form of remarks.

Lemma 1. $P_{i_n,j_n}\, p(\ldots(p(V_{i_1,j_1},P_{i_2,j_2}),\ldots),P_{i_{n-1},j_{n-1}})$

$$+ \sum_{j_n' + j_n'' = j_n} P_{i_n,j_n'}\, p(\ldots(p(V_{i_1,j_1},\ldots),P_{i_{n-1},j_{n-1}}),P_{i_n,j_n''})$$

$$= -p(\ldots\, p(V_{i_1,j_1},P_{i_2,j_2})\ldots),P_{i_{n-1},j_{n-1}}),P_{i_n,j_n})$$

$$+ p(\ldots p(V_{i_1,j_1},P_{i_2,j_2})\ldots),P_{i_{n-1},j_{n-1}}) \cdot P_{i_n,j_n} .$$

(This is more or less the definition of $p(\ ,\ )$ again).

Remark 1. We now use the inductive assumption (iv) for $\overline{K}_{m-i_n j_n}$ to see that $p(\ldots p(V_{i_1,j_1},P_{i_2,j_2})\ldots)P_{i_{n-1},j_{n-1}}) \cdot P_{i_n,j_n}$

$$= (m - i_n j_n) \cdot P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} \cdot P_{i_n,j_n}$$

$$- \Sigma \text{ types } \{(i_1,j_1),\ldots,(i_{n-1},j_{n-1})\}_{\Sigma i_\ell j_\ell = m - i_n j_n} \cdot P_{i_n,j_n} .$$

Lemma 2. $\sum_{j_n' + j_n'' = j_n} P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} P_{i_n,j_n'} V_{i_n,j_n''}$

$$+ P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} \cdot V_{i_n,j_n}$$

$$= i_n \cdot P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} K_{i_n,j_n}$$

$$+ i_n j_n P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} P_{i_n,j_n} - i_n P_{i_1,j_1} \cdots P_{i_{n-1},j_{n-1}} K_{i_n,j_n}$$

$$= i_n j_n \cdot P_{i_1,j_1} \cdots P_{i_n,j_n} .$$

Remark 2: We consolidate. Our partial sum is now

$$m \cdot P_{i_1,j_1} \cdots P_{i_n,j_n} - p(\ldots p(V_{i_1,j_1}, P_{i_2,j_2}) \ldots), P_{i_n,j_n})$$

$$- \Sigma \text{ types } \{(i_1,j_1),\ldots,(i_{n-1},j_{n-1})\}_{\Sigma i_\ell j_\ell = m - i_n j_n} \cdot P_{i_n,j_n} .$$

The trick we use to dissolve the unwanted term is the following.

Lemma 3. P arbitrary, Q primitive implies $Pp(Q,P_{i_n,j_n})$

$$+ \sum_{j_n' + j_n'' = j_n} P P_{i_n,j_n'} p(Q,P_{i_n,j_n''}) + P P_{i_n,j_n} Q = P[Q,P_{i_n,j_n}]$$

$+ P P_{i_n,j_n} Q = PQP_{i_n,j_n}$. This is, of course, a direct consequence of the definition of $p(\ ,\ )$.

Remark 3: Replacing P by terms of the sort $P_{g_1,k_1} P_{g_2,k_2} \cdots P_{g_f,k_f}$ and Q by terms of the sorts V_{h_1,k_1} and $p(\ldots(p(V_{h_1,k_1}, P_{h_2,k_2}) \ldots P_{h_f,k_f})$ with g's and h's selected from $\{i_1,i_2,\ldots,i_{n-1}\}$, the left hand side of the equation in Lemma 3 provides the remaining monomials for our sum of monomials of type $\{(i_1,j_1) \ldots (i_n,j_n)\}_{\Sigma i_f j_f = m}$. The right hand side provides the monomials of type $\{(i_1,j_1) \ldots (i_{n-1},j_{n-1})\}_{\Sigma i_f j_f = m - i_n j_n}$ right multiplied by P_{i_n,j_n}. By Remark 2 we are done.

Clearly (i) and (ii)-(iii)-(iv) provide a proof of the proposition.

We mention two technical points:

(i) The proof of Proposition 2 does not depend on the use of the canonical amalgamation. Any σ-amalgamation should have done as well, merely by replacing the summation ranges $i_1 < i_2 < \ldots < i_k$ by $\sigma(i_1) < \sigma(i_2) < \ldots < \sigma(i_k)$.

(ii) One should not hesitate to replace any tower $\{P_{h,j}\}_{j=1,\ldots,m_n}$ by zeros, if $h > 1$.

We focus again on the key problem. If a primitive supports two towers of height $m-1$, and one cannot be extended to height m , can the other? Proposition 2 partially answers this question. If the two towers are related as the extremes in Figure 1, the answer is dependent on the extendibility of the branch towers over the primitives modifying at stories dividing m . In detail, in order for the figure to apply with $n+1 = m$, for each $i \mid m$, the height of $\{P_{i,j}\}$ must be $\geq m/i - 1$. If $\forall\, i \mid m$, $i \neq 1$, these towers can be extended to, or are taller than, height m/i , then $K_{i,m/i}$ is divisible by m/i , modulo primitives. Hence $i\,K_{i,m/i}$ is divisible by m , modulo primitives. By Proposition 2, $\overline{K_m}$ and K_m have the same image in $\mathcal{X}/P(\mathcal{X}) \otimes Z_m$. If it is zero, both $\{P_i\}$ and $\{\overline{P_i}\}$ can be extended to height m ; if not, neither can.

On the other hand, suppose there is exactly one i_0 s.t. $i_0 \mid m$, $i_0 \neq 1$ and $K_{i_0,m/i_0}$ does not got to zero in $\mathcal{X}/P(\mathcal{X}) \otimes Z_{m/i_0}$. Then at most one of the towers $(\{P_i\},\{\overline{P_i}\})$ can be extended, possibly neither.

We describe two special situations. We assume $\mathcal{X}$ is torsion-free as an abelian group.

Proposition 3. If $\{P_i\}$ and $\{\overline{P_i}\}$ are towers of height $m-1$ over P_1 and all primitives of $\mathcal{X}$ support towers of height $[m/2]$, then both towers can be extended to height m , or neither can.

Proposition 3′. Suppose $\mathcal{N}$ is graded, $P_1 \in P_h$, and $\{P_i\}$ and $\{\overline{P_i}\}$ are towers of height $m-1$ over P_1. Suppose that whenever $P \in P(\mathcal{N})_{\ell k}$, $\ell=2,3,\ldots,$ P supports a tower of height $[m/\ell]$. Then both $\{P_i\}$ and $\{\overline{P_i}\}$ can be extended to height m, or neither can.

Proof: (same for both propositions) Denote P_i by $P_{1,i}$. By computing Δ, we see that $\overline{P_2} - P_{1,2}$ is primitive. Call it $P_{2,1}$. Choose a tower $\{P_{2,i}\}$ of height $[m/2]$ for $P_{2,1}$. By computing Δ, $\overline{P_3} - (P_{1,3} + P_{1,1} P_{2,1})$ is primitive. Call it $P_{3,1}$. Choose a tower of height $[m/3]$ for $P_{3,1}$. By computing Δ, $\overline{P_4} - P_{i,4} - P_{1,2} P_{2,1} - P_{2,2}$ is primitive, etc. We reconstruct Figure 1, and now have available Proposition 2, from which 3 and 3′ follow.

We summarize. To each primitive P of $\mathcal{N}$, for each $n \in Z^+$, we assign a set $\mathcal{O}^n(P) \subset \mathcal{N}/P(\mathcal{N}) \otimes Z_n$ as follows: for each tower over P of height $n-1$, we compute $K_n \in \mathcal{N}$, and take its image under the canonical module morphism $\mathcal{N} \to \mathcal{N}/P(\mathcal{N}) \approx \mathcal{N}/P(\mathcal{N}) \otimes Z \to \mathcal{N}/P(\mathcal{N}) \otimes Z_n$. If there are no towers over P of height $n-1$, $\mathcal{O}^n(P)$ is empty. There exists a tower of height n over P only if $\mathcal{O}^n(P)$ contains zero. When $\mathcal{N}$ is n-torsion-free, there exists a tower of height n over P if and only if $\mathcal{O}^n(P)$ contains zero.

In this language we have, for $\mathcal{N}$ torsion-free as a Z-module,

Proposition 3. If $\mathcal{O}^m(Q)$ contains zero for all $Q \in P(\mathcal{N})$, $\forall\, m \le n/2$ then $\mathcal{O}^n(P)$ contains exactly one element, $\forall\, P \in P(\mathcal{N})$.

Proposition 3′. If $\mathcal{N}$ is graded, $P \in P(\mathcal{N})_k$, and $\forall\, Q \in P(\mathcal{N})_{k\ell, \ell=2,3,\ldots}$, $m < n/\ell$ implies $\mathcal{O}^m(Q)$ contains zero, then $\mathcal{O}^n(P)$ contains exactly one element.

We look at an example in which one of these sets has more than one

element. Let $_Z\mathcal{H} = \{x_i,\ i = 1,\ldots,n,\ldots\ ,\ y\ ;\ x_iy = yx_i\ ,\ x_ix_j = x_jx_i = \binom{i+j}{i} x_{i+j}\ ;\ y \to y\otimes 1 + 1\otimes y\ ,\ x_i \to \sum_{j+k=i} x_j\otimes x_k\}$. Consider the following two towers over x_1 : $\{x_1,x_2,x_3\}$ and $\{x_1,x_2+y,x_3+x_1y\}$. By Proposition 2, $\overline{K_4} \equiv K_4 + 2y^2 \equiv x_1^4/3! + 2y^2 \pmod 4$. But $x_1^4/3!$ is $0 \mod 4$, $2y^2$ is not, nor is it primitive. So $\overline{K_4}$ and K_4 have different images in $\mathcal{H}/P(\mathcal{H}) \otimes Z_4$, and $\mathcal{O}^4(x_1)$ contains two distinct elements.

We consider the question of how general a situation is described by Figure 1. Let $\mathcal{H} = \{P_i,Q_i\ ,\ i = 1,2,\ldots : P_i \xrightarrow{\Delta} \sum_{j+k=i} P_j \otimes P_k$

$$Q_i \xrightarrow{\Delta} \Sigma Q_j \otimes Q_k\ ;\ P_1 = Q_1\} .$$

($\mathcal{H}$ is neither associative nor commutative.) Suppose we could "solve the obstruction problem" in this Hopf algebra, i.e., suppose we could list all the primitives and establish the height of the highest tower over each primitive. Then we would be in a position to know whether or not Figure 1 is the norm. If two towers are the same height over a primitive in any connected Hopf algebra, is one the amalgamation of the other with branch towers? This seems to be a very difficult problem.

In the associative quotient, it can be shown that $P_2 - Q_2$ has a tower of height two:

$$3P_4 + P_1^2P_2 - P_1^4 - P_2^2 - 3P_1P_3 + 2P_1P_2P_1$$

$$+ Q_4 + P_1^2Q_2 - P_1Q_3 - P_2Q_2 .$$

It follows readily that in every associative connected Hopf algebra any two towers of height 4 over the same primitive are amalgamations of one another with branch towers.

CHAPTER III

THE COALGEBRA, $H^*(BU;Z)$

We describe the coalgebra structure of the Hopf algebra familiar to topologists as $H^*(BU;Z)$. This is well-known to be a "self-dual" Hopf algebra, (see, e.g., Dyer [3]), and our argument is a new proof of this fact. The innovation is that duality is not used. A more inspired defense of this repetition is better deferred until we make important use of some of the details of the argument.

Let ${}_R\mathcal{J}_{A,C}$ be the Hopf algebra over R, a commutative ring, described by "generators and relations" as follows:

$$\left\{{}_R\mathcal{J}_{A,C},\ (\circ,\eta),\ (\Delta,\epsilon)\right\} = \left\{P_i, i \in Z^+ \ ;\ (P_iP_j)P_k\right.$$

$$= P_i(P_jP_k), (i,j,k) \in (Z^+)^3\ ,\ P_iP_j = P_jP_i\ (i,j) \in (Z^+)^2\ ,$$

$$P_iP_0 = P_i,\ i \in Z^+\ ,\ \eta(1) = P_0\ ;\ P_k \to \sum_{i+j=k} P_i \otimes P_j\ ,$$

$$\left. k \in Z^+,\ \epsilon(P_i) = \delta_{i,0}\right\}.$$

As an algebra, clearly ${}_R\mathcal{J}_{A,C} \cong R[P_1,P_2,\ldots,P_n,\ldots]$, and ${}_R\mathcal{J}_{A,C}$ may be filtered by the submodules of polynomials of degree less than $n+1$ for all $n \in Z^+$. We shall give a basis for the primitive submodule of ${}_R\mathcal{J}_{A,C}$, and for each element of this basis, construct an infinite tower. In preparation, we make the (expected) definitions of a sequence of elements, $\{K_i\}_{i\in Z^+-\{0\}}$, of ${}_R\mathcal{J}_{A,C}$.

$$K_1 \equiv 0\ .\qquad K_i \equiv \sum_{j+k=i} P_j(kP_k - K_k)$$

Theorem 1. For each strictly positive integer n, the submodule of $P({}_R\mathcal{J}_{A,C})$ spanned by homogeneous polynomials of degree n is free on one generator, $nP_n - K_n$. Hence, a basis for $P({}_R\mathcal{J}_{A,C})$ is $\{iP_i - K_i\}_{i\in Z^+} - \{0\}$.

Proof: Let us suppose first that $R = Z$. We write P^I for $P_1^{i_1}P_2^{i_2}\ldots P_n^{i_n}$ and $\omega(I)$ for $i_1 + 2i_2 + \ldots + ni_n$, if $I = \{i_1, i_2, \ldots, i_n\}$.

$\Delta P^I = \sum_{\omega(J)+\omega(K)=\omega(I)} a_I^{J,K} P^J \otimes P^K$ defines for each I a family of elements, $\{a_I^{J,K}\}_{J,K}$, of Z.

Let $P = \sum_{\omega(I)=n} b_I P^I$ be primitive and homogeneous of degree n.

$$\Delta P = \sum_{\omega(I)=n} b_I P^I \otimes 1 + 1 \otimes \sum_{\omega(I)=n} b_I P^I$$

$$+ \sum_{\omega(J)+\omega(K)=n} \sum_{\omega(I)=n} (a_I^{J,K} b_I) P^J \otimes P^K$$

$$= P \otimes 1 + 1 \otimes P .$$

$\{b_I\}_{\omega(I)=n}$ is a solution to the system of equations with integer coefficients, $\{\sum_{\omega(I)=n} a_I^{J,K} X_I\}_{\substack{\omega(J)+\omega(K)=n \\ J\neq 0,\ K\neq 0}} = 0$.

This system of equations is highly redundant. It is easy to see, for example, that $a_I^{J,K} = a_I^{K,J}$, for all I,J,K by virtue of the cocommutativity of ${}_R\mathcal{J}_{A,C}$.

We propose to describe a subfamily of equations which must be irredundant. There will be one equation for each I such that $\omega(I) = n$, save one. This subsystem of equations cannot have two rationally independent solutions.

On the other hand, $nP_n - K_n$ is primitive, and so provides a solution. Let us suppose that if $n' < n$, $n'P_{n'} - K_{n'}$ is a homogeneous polynomial in $\{P_1, P_2, \ldots, P_{n'}\}$ whose $P_1^{n'}$ coefficient is ± 1. Since $nP_n - K_n = nP_n - \sum_{i+j=n} P_i(jP_j - K_j)$, clearly $nP_n - K_n$ is a homogeneous polynomial in $\{P_1, P_2, \ldots, P_n\}$ whose P_1^n coefficient is ± 1 (only $P_1((n-1)P_{n-1} - K_{n-1})$ can contribute to P_1^n). Hence $nP_n - K_n$ is indivisible, and generates the homogeneous primitives of degree n. Clearly every primitive can be written as a sum of homogeneous primitives. Except for our deferred linear algebraic argument, this completes the proof of Theorem 1 if R is Z.

Suppose R is an arbitrary commutative ring. Then

i) $$R\mathcal{J}_{A,C} \overset{\delta}{\cong} Z\mathcal{J}_{A,C} \underset{Z}{\otimes} R$$

ii) $$R\mathcal{J}_{A,C} \underset{R}{\otimes} R\mathcal{J}_{X,C} \overset{\alpha}{\cong} (Z\mathcal{J}_{A,C} \underset{Z}{\otimes} R) \underset{R}{\otimes} (Z\mathcal{J}_{A,C} \otimes R)$$

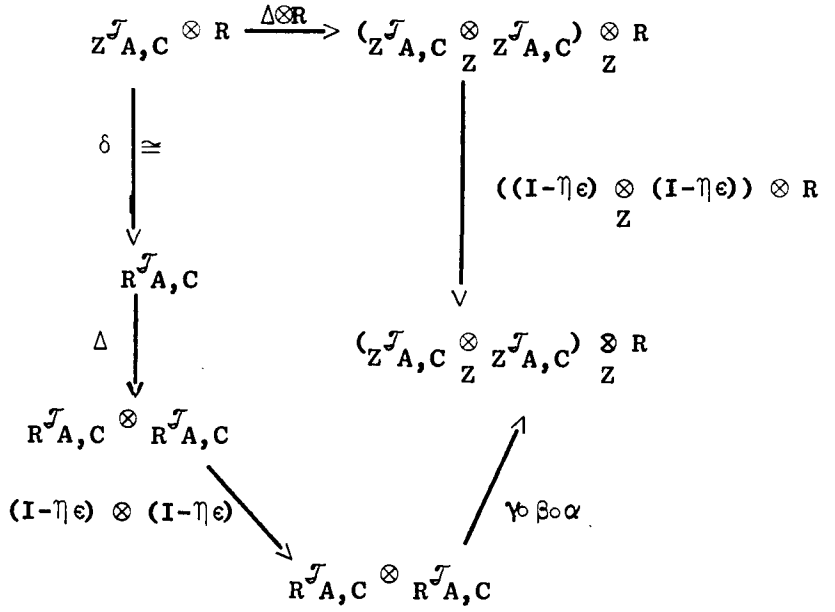
$$\overset{\beta}{\cong} (Z\mathcal{J}_{A,C} \underset{Z}{\otimes} Z\mathcal{J}_{A,C}) \otimes (R \underset{R}{\otimes} R)$$

$$\overset{\gamma}{\cong} (Z\mathcal{J}_{X,C} \underset{Z}{\otimes} Z\mathcal{J}_{A,C}) \underset{Z}{\otimes} R$$

iii) $$P(Z\mathcal{J}_{A,C}) = \text{Ker } (((I - \eta\epsilon) \underset{Z}{\otimes} (I - \eta\epsilon))\circ\Delta)$$

iv) $$P(R\mathcal{J}_{A,C}) = \text{Ker } ((I - \eta\epsilon) \underset{R}{\otimes} (I - \eta\epsilon))\circ\Delta)$$

v) The following diagram commutes.



vi) Image $(((I - \eta\epsilon) \otimes_Z (I - \eta\epsilon))\circ\Delta) \otimes_Z R \overset{\text{"}\alpha^{-1}\beta^{-1}\gamma^{-1}\text{"}}{\cong}$

Image $((I - \eta\epsilon) \otimes_R (I - \eta\epsilon)\circ\Delta)$

vii) Image $((I - \eta\epsilon) \otimes_Z (I - \eta\epsilon)\circ\Delta)$ is a free abelian group

since it is a subgroup of $Z^{\mathcal{J}_{A,C}} \otimes Z^{\mathcal{J}_{A,C}}$

viii) From vii), Tor_Z (Image $(I - \eta\epsilon \otimes_Z I - \eta\epsilon)\circ\Delta$, R) is zero.

i - viii imply $P(_R\mathcal{J}_{A,C}) \overset{\text{"}\delta\text{"}}{\cong} P(_Z\mathcal{J}_{A,C}) \otimes_Z R$.

Theorem 1 follows immediately for arbitrary commutative rings.

We return now to the linear algebra left undone. We order the monomials P^I with $\omega(I) = n$, lexicographically. $\Delta P_1^{i_1}P_2^{i_2}\ldots P_n^{i_n}$ clearly has a non zero $P_1^{i_1+i_2+\ldots+i_n} \otimes P_1^{i_2}P_2^{i_3}\ldots P_{n-1}^{i_n}$ coefficient, as each P_j contributes a $P_1 \otimes P_{j-1}$ factor. On the other hand, no

monomial higher in the ordering has a non-zero coefficient for this tensor, for only summands of ΔP_j of type $P_1 \otimes P_{j-1}$ and $P_0 \otimes P_j$ can contribute factors.

Let $E_{J,K}$ be the equation $\sum_{\omega(I)=n} a_I^{J,K} X_I = 0 \Big|_{\substack{\omega(J)+\omega(K)=n \\ J\neq 0,\ K\neq 0}}$.

Consider the subfamily of equations, $E_{J,K}$, where J and K are related as: $J_I = (i_1+i_2+\ldots+i_n,0,0,\ldots,0)$, $K_I = (i_2,i_3,\ldots,0)$. Clearly $\omega(J) + \omega(K) = (1\cdot(i_1+i_2+\ldots,i_n) + 0) + (1\cdot i_2+\ldots+(k-1)i_k+\ldots+(n-1)i_n)$ $= \Sigma\, k_{i_k} = n$, so that there is exactly one such equation for each I such that $\omega(I) = n$, except for $I = (n,0,0,\ldots,0)$ — J_I would be I and K_I would be zero, which is not admissible.

Order this subfamily by the lexicographic ordering on the I's. Then X_{I_0} makes its first appearance in $E_{J_{I_0},K_{I_0}}$ with non-zero coefficient, by the above discussion. Such a system of homogeneous equations cannot be redundant, and there is one more variable than the number of equations.

We would like to demonstrate that $iP_i - K_i \in {}_Z\mathcal{J}_{A,C}$ supports an infinite tower, for $i \in Z^+ - \{0\}$. Let us suppose this is possible. Define $iP_i - K_i \equiv P_{i,1}$, and let $\{P_{i,j}\}_{j=1,2,\ldots}$ be an infinite tower over $P_{i,1}$. Theorem 1 of this Chapter and Borel's theorem of Chapter I imply that ${}_Z\mathcal{J}_{A,C}$ is a free abelian group on generators $\{P_{i_1,j_1}P_{i_2,j_2}\ldots P_{i_k,j_k}\}_{\substack{i_1\leq i_2\ldots \\ j_s\in Z^+-\{0\}}}$ and 1. But ${}_Z\mathcal{J}_{A,C} \underset{Z}{\otimes} R \cong {}_R\mathcal{J}_{A,C}$, and ${}_R\mathcal{J}_{A,C}$ is a free R-module on the same generators. Hence, for any R, the coalgebra ${}_R\mathcal{J}_{A,C}$ is isomorphic to a tensor product of a

countable family of tower coalgebras, $\bigotimes_{i\in Z^+-\{0\}} \{P_{i,j}\}_{j\in Z^+}$.

We turn now to the construction of the towers when $R = Z$.

Notation: If $n \geq 1$, ${}_Z\mathcal{T}^n_{A,C} \equiv$ the sub Hopf algebra of ${}_Z\mathcal{T}_{A,C}$ generated by $P_1, P_2, \ldots, P_n$.

$i_n: {}_Z\mathcal{T}^n_{A,C} \to {}_Z\mathcal{T}_{A,C}$ and $i^{n'}_n\ {}_Z\mathcal{T}^n_{A,C} \to {}_Z\mathcal{T}^{n'}_{A,C}$, $n' > n$ are inclusion maps.

If $i \geq 1$, $Z[X^i] \equiv Z[X^i_1, X^i_2, \ldots, X^i_n] \subseteq Z[X_1, X_2, \ldots, X_n]$, the polynomial algebra in $X = \{X_1, X_2, \ldots, X_n\}$.

$\sigma_i(X^j) \equiv i^{th}$ elementary symmetric polynomial in $Z[X^j]$.

There is a unique algebra map $\iota_n: {}_Z\mathcal{T}^n_{A,C} \to Z[X]$ extending $P_i \to \sigma_i(X) = \sigma_i(X^1)$, $i = 1,2,\ldots,n$. The fundamental theorem of symmetric polynomials (see, e.g., Jacobson [4]) ensures that ι_n is a monomorphism whose image is precisely the symmetric polynomials in $Z[X]$.

There are algebra maps $\psi_n: {}_Z\mathcal{T}^n_{A,C} \to {}_Z\mathcal{T}^{n-1}_{A,C}$ defined by $P_i \to P_i$, $i=1,2,\ldots,n-1$, $P_n \to 0$, and $\varphi_n: Z[X_1,\ldots,X_n] \to Z[X_1,\ldots,X_{n-1}]$ defined by $X_i \to X_i$, $i=1,2,\ldots,n-1$ and $X_n \to 0$. The following diagrams commute, for all n , by the definition of the elementary symmetric polynomials.

$$\begin{array}{ccc} {}_Z\mathcal{T}^n_{A,C} & \xrightarrow{\psi_n} & {}_Z\mathcal{T}^{n-1}_{A,C} \\ & \xleftarrow{i^n_{n-1}} & \\ \downarrow \iota_n & & \downarrow \iota_{n-1} \\ Z[X_1,X_2,\ldots,X_n] & \xrightarrow{\varphi_n} & Z[X_1,X_2,\ldots,X_{n-1}] \end{array}$$

It suffices to show that the algebraic criteria for building towers of height j over $iP_i - K_i$ in $Z\mathcal{T}_{A,C}$ are satisfied in $Z\mathcal{T}^n_{A,C}$, where $ij \leq n$. We shall, in fact, compute in $\operatorname{Im} \tau_n$.

We write $P_{1,j}$ for P_j, $P_{j,1}$ for $jP_j - K_j$. For $i < n$, we wish to define sequences $\{P_{i,j}\}_{j=1,\ldots,[n/i]}$, $\{K_{i,j}\}_{j=1,\ldots,[n/i]}$ in such a way that $K_{i,j} = \sum_{j=k+\ell} P_{i,k}(\ell P_{i,\ell} - K_{i,\ell})$ and

$$jP_{i,j} - K_{i,j} = ij\, P_{1,ij} - K_{1,ij}$$

$$\equiv ij\, P_{ij} - K_{ij} .$$

Let us recall Newton's formula (see, e.g., Jacobson [4]). If

$$S_j(Y) \equiv S_j(Y_1, Y_2, \ldots, Y_n) \equiv Y_1^j + Y_2^j + \ldots + Y_n^j \in Z[Y_1, \ldots, Y_n]$$

for all $j \in Z^+$, then

$$j\sigma_j(Y) - \sigma_{j-1}(Y)\, S_1(Y) + \ldots + (-1)^{j-1}\, \sigma_1(Y)\, S_{j-1}(Y) + (-1)^j\, S_j(Y) = 0 .$$

Let us suppose that $\{P_{i,j'}\}$ and $\{K_{i,j'}\}$ are defined for fixed i, for $j' < j \leq [n/i]$ and

i) $\tau_n(P_{i,j'}) = (-1)^{(i-1)j'}\, \sigma_{j'}(X^i) \in Z[X^i] \subseteq Z[X]$.

ii) $\tau_n(iP_{i,j'} - K_{i,j'}) = (-1)^{ij'-1}\, S_{j'}(X^i) \in Z[X^i] \subseteq Z[X]$.

Then

$$\tau_n(K_{i,j}) = \tau_n\Big(\sum_{k+\ell=j} P_{i,k}(\ell P_{i,\ell} - K_{i,\ell})\Big)$$

$$= \sum_{k+\ell=j} (-1)^{(i-1)k}\, \sigma_k(X^i) \cdot (-1)^{i\ell-1}\, S_\ell(X^i)$$

$$= (-1)^{(i-1)j-1} \sum_{k+\ell=j} (-1)^\ell\, \sigma_k(X^i)\, S_\ell(X^i) .$$

Newton's formula, replacing Y by X^i, gives

$$j((-1)^{(i-1)j}\ \sigma_j(X^i)) - \varepsilon_n(K_{i,j}) + (-1)^{ij}\ S_j(X^i) = 0\ .$$

Since $\sigma_j(X^i)$ is symmetric, it is in the image of ε_n. Let $P_{i,j}$ be the unique pre-image of $(-1)^{(i-1)j}\ \sigma_j(X^i)$ under ε_n. Then $\varepsilon_n(jP_{i,j} - K_{i,j}) = (-1)^{ij-1}\ S_j(X^i)$. But $S_j(X^i) \equiv (X_1^i)^j + \ldots + (X_n^i)^j \equiv S_{ij}(X)$, and $(-1)^{ij-1}\ S_{ij}(X) = \varepsilon_n(ijP_{1,ij} - K_{1,ij})$ $= \varepsilon_n(ijP_{ij} - K_{ij})$ by the Newton formula, replacing Y by X. Since ε_n is a monomorphism, $jP_{i,j} - K_{i,j} = ijP_{ij} - K_{ij}$, which is primitive. Hence, by Proposition I of Chapter II, $P_{i,j}$ is an extension of the tower $\{P_{i,j'}\}_{j'<j}$ over $P_{i,1} = iP_i - K_i$.

We must be certain that we are not altering the towers as we increase n. Such a procedure would not provide infinite towers, but merely finite towers of arbitrary height. But the commutativity of the above diagrams (p.25) is our assurance. Since $\sigma_i(X^j)$ in $Z[X_1,\ldots,X_n]$ restricts to $\sigma_i(X^j)$ in $Z[X_1,\ldots,X_{n-1}]$ if $ij \leq n-1$, $P_{i,j}$, as defined in ${}_z\mathcal{J}^n_{A,C}$, restricts to $P_{i,j}$, as defined in ${}_z\mathcal{J}^{n-1}_{A,C}$.

We summarize, and paraphrase

<u>Theorem 2</u>. ${}_R\mathcal{J}_{A,C}$ is a free R-module on generators 1 and $\{P_{i_1,j_1}P_{i_2,j_2}\ldots P_{i_k,j_k}\}_{i_1\leq i_2\leq\ldots\leq i_k\ ;\ j_s \in Z^+-\{0\}}$. As a coalgebra,

${}_R\mathcal{J}_{A,C} \xleftarrow{\cong} \bigotimes_{i\in Z^+-\{0\}} \{P_{i,j}\}_{j\in Z^+}$.

<u>Theorem 2'</u>. In $R[X_1,X_2,\ldots,X_n]$, a basis for the symmetric polynomials of degree $\leq n$ is

$$S = \{\sigma_{i_1}(X^1)\ \sigma_{i_2}(X^2)\ \ldots\ \sigma_{i_n}(X^n)\ |\ i_1+2i_2+\ldots+ni_n \leq n\}\ .$$

Theorem 2′ follows immediately from Theorem 2, by our representation of $R\mathcal{J}^n_{A,C}$ as a subalgebra of $R[X_1,\ldots,X_n]$. The basis elements of Theorem 2 pass, under ι_n, to the basis elements of Theorem 2′, up to sign.

Caution: The restriction on degree is not entirely removable. In degree $3n$, $\sigma_n(X) \cdot \sigma_n(X^2)$ and $\sigma_n(X^3)$ are equal. We do not know whether or not $3n$ is the first degree in which the analogue of S fails to be a basis. If $n = 2$, this is so.

CHAPTER IV

THE HOPF ALGEBRA AUTOMORPHISMS OF $H^*(BU;Z)$

We demonstrate that the group of Hopf algebra automorphisms of $Z^{\mathcal{J}_{A,C}}$ is isomorphic to $Z_2 \times Z_2$.

Theorem 1. If φ is an automorphism of $Z^{\mathcal{J}_{A,C}}$ which fixes P_1, and $\varphi \neq I$, then $\varphi(P_2) = P_1^2 - P_2$.

Proof: Let us suppose $\varphi(P_i) = P_i$ for $i < n$, and $\varphi(P_n) \neq P_n$. Since φ is a coalgebra map, $\varphi(P_n)$ extends the tower $\{P_1, P_2, \ldots, P_{n-1}\}$, as does P_n, so $\varphi(P_n) - P_n$ is primitive. By Theorem 1 of Chapter III, $\varphi(P_n) - P_n = \lambda_n(nP_n - K_n)$ for some $\lambda_n \in Z$ (it is readily shown by induction on degree that φ is homogeneous). On the other hand, $\varphi(P_n)$ is an algebra automorphism, so $\varphi(P_n) = \pm P_n$ + decomposables. Equating coefficients of P_n, $\pm 1 - 1 = \lambda_n \cdot n$. $\lambda_n \neq 0$ since $\varphi(P_n) \neq P_n$, so $n = 2$, $\lambda_2 = -1$, and $\varphi(P_2) = (-1)(2P_2 - K_2) + P_2 = P_1^2 - P_2$.

*Theorem 2. There is an automorphism φ of $Z^{\mathcal{J}_{A,C}}$ such that $\varphi(P_1) = P_1$, $\varphi(P_2) = P_1^2 - P_2$.

Proof: By Proposition 3, Chapter II, there is an infinite tower $\{P_i'\}_{i=1,2,\ldots}$ extending $\{P_1, P_1^2 - P_2\}$. Suppose there exists such a tower in which P_i', when written as a polynomial in $\{P_i\}_{i=1,2,\ldots}$ has P_i coefficient ± 1. Then $\varphi(P_i) \equiv P_i'$ extends uniquely to an algebra map which is clearly a compatible coalgebra map, and onto by induction on degree. Furthermore, if M is any monomial in $\{P_i\}_{i=1,2,\ldots}$, then $\varphi(M) = \pm M$ + lower monomials in the lexicographic ordering. If P is any polynomial $\neq 0$, $\varphi(P) \neq 0$, since $\varphi(P) = \pm M$ + lower monomials where

*See addendum, page 32.

M is the largest monomial of P.

Let us suppose then, that there is a tower $\{P_i'\}_{i=1,2,\ldots,n-1}$ such that

(i) $P_i' = (-1)^{i-1} P_i + P_1^i$ + monomials in Ideal$(P_2, P_3, \ldots, P_{i-1})$

$n > i > 2, P_1' = P_1$, $P_2' = -P_2 + P_1^2$, and

(ii) $iP_i' - K_i' = (-1)^{i-1} (iP_i - K_i)$, where

$$K_i' = \sum_{i=j+k} P_j'(kP_k' - K_k') .$$

We show that (i) and (ii) are satisfied for some choice of P_n'.

Let us compute.

$$K_n' = \sum_{\ell+m=n} P_\ell'(mP_m' - K_m') .$$

By Proposition 3, Chapter II, there is an extension of $\{P_i\}_{i=1,2,\ldots,n}$, since every primitive in $Z\mathcal{T}_{A,C}$ supports an infinite tower. Furthermore, if P_n' extends, by Theorem 1 of Chapter III, $nP_n' - K_n' = \lambda_n(nP_n - K_n)$ for some $\lambda_n \in Z$, or $nP_n' = K_n' + \lambda_n(nP_n - K_n)$. The coefficient of P_1^n in $nP_n - K_n$ is $(-1)^{n-1}$ by induction. In K_n', each summand $P_\ell'(mP_m' - K_m') = P_\ell'((-1)^{m-1}(mP_m - K_m))$ contributes coefficient 1 to $P_1^\ell \cdot P_1^m = P_1^{\ell+m} = P_1^n$, and there are $n-1$ summands. Let μ_n be the coefficient of P_1^n in the polynomial expression for P_n'. Equating coefficients,

$$n\mu_n = (n-1) + \lambda_n \cdot (-1)^{n-1}, \text{ or } \lambda_n \equiv (-1)^{n-1} \bmod n .$$

Without loss of generality, $\lambda_n = (-1)^{n-1}$, for any multiple of $(nP_n - K_n)$ which is divisible by n may be absorbed in nP_n'.

So we may choose P_n' in such a way that

$$nP_n' - K_n' = (-1)^{n-1}(nP_n - K_n) .$$

Since $n\mu_n = (n-1) + \lambda_n(-1)^{n-1}$ and $\lambda_n = (-1)^{n-1}$, $n\mu_n = n$, and $1 = \mu_n \equiv$ the P_1^n coefficient of P_n'. Since K_n and K_n' are decomposable, the P_n coefficient of P_n' is $(-1)^{n-1}$. Thus, (i) and (ii) are satisfied, and Theorem 2 is proved.

Theorem 3. There is exactly one automorphism φ of ${}_Z\mathcal{J}_{A,C}$ such that $\varphi(P_1) = P_1$ and $\varphi(P_2) = P_1^2 - P_2$.

Proof: Suppose φ_1 and φ_2 satisfy the restrictions given. Then

$$\varphi_1^{-1}\varphi_2(P_1) = P_1 , \quad \varphi_1^{-1}\varphi_2(P_2) = P_2 .$$

Theorem 1 implies $\varphi_1^{-1}\varphi_2 = I$, so $\varphi_1 = \varphi_2$. Theorem 2 provides the unique automorphism.

Theorem 4. $\varphi^2 = I$ if φ is the automorphism of Theorem 2.

Proof: $\varphi^2(P_1) = P_1$, $\varphi^2(P_2) = \varphi(P_1^2 - P_2) = \varphi(P_1^2) - \varphi(P_2)$

$$= P_1^2 - (P_1^2 - P_2) = P_2 .$$

Hence, by Theorem 1, $\varphi^2 = I$.

Let $\psi: P_i \to (-1)^i P_i$ determine $\psi: {}_Z\mathcal{J}_{A,C} \to {}_Z\mathcal{J}_{A,C}$. ψ is clearly an automorphism of order 2 which commutes with φ.

Theorem 5. The inclusion $Z_2 \times Z_2 \cong gp(\varphi, \psi) \subseteq Aut({}_Z\mathcal{J}_{A,C})$ is an isomorphism of groups.

Proof: Any automorphism γ fixes P_1 or sends P_1 to $-P_1$. If γ fixes P_1, it is φ or I. If γ sends P_1 to $-P_1$, then $\psi\gamma$ fixes P_1 and is φ or I.

In $H^*(BU;Z)$, which is isomorphic to $_Z\mathcal{J}_{A,C}$ by the identification of the i^{th} Chern class c_i with P_i , ψ and $\psi \circ \varphi$ are familiar as conjugation and the "power series inverse" of the total Chern class $c = 1 + c_1 + c_2 + \ldots$, respectively.

Addendum: We seem to have suffered from an excess of zeal in the proof of Theorem 2. An argument can be constructed rather easily making use of the canonical anti-automorphism described in Milnor & Moore [1], §8.

CHAPTER V

A COMPUTATION OF $\wp^{i-1}(c_i) \in H^*(BU;Z_p)$

We shall exploit our knowledge of the coalgebra structure of $H^*(BU;Z_p)$ and the well-known fact that the Steenrod mod p reduced powers, $\{\wp^i\}_{i\in Z^+}$, preserve primitives to make the title computations. We shall write $\wp^{i-1}(c_i)$as a linear combination of the basis we described in Chapter III, and then translate, rather awkwardly, into the standard basis, the monomials in the Chern classes. We suspect that successive computations of $\wp^{i-2}(c_i),\wp^{i-3}(c_i),\ldots,$ and $\wp^1(c_i)$ can be gotten, and moreover, that the "right" basis is the new one. Our result is purely Hopf algebraic, and makes no use of prime number arithmetic, except in changing bases.

Let us recall, from Chapter III, that ${}_Z\mathcal{J}_{A,C}$ contains a family of elements $\{P_{i,j}\}_{i\in Z^+-\{0\},j\in Z^+}$, such that

$$
\begin{aligned}
&\text{(i)} && P_{i,0} = 1 \quad \text{for all } i\,.\\
&\text{(ii)} && P_{1,j} = P_j \quad \text{for all } j\,.\\
&\text{(iii)} && P_{i,1} = iP_i - K_i\,, \text{ for all } i\,.\\
&\text{(iv)} && jP_{i,j} - K_{i,j} = ijP_{1,ij} - K_{1,ij} = ijP_{ij} - K_{ij} = P_{ij,1}\\
& && \qquad \text{for all } i \text{ and } j\,.\\
&\text{(v)} && 1 \text{ and the elements } P_{i_1,j_1}P_{i_2,j_2}\ldots P_{i_k,j_k}\,, \text{ with } k = 1,2,\ldots,\\
& && i_1 < i_2 < \ldots < i_k,\ j_t \neq 0 \text{ make up a basis of } {}_Z\mathcal{J}_{A,C}\,.\\
&\text{(vi)} && \text{If } n \text{ is sufficiently large, in } Z[X] = Z[X_1,X_2,\ldots,X_n]\,,\\
& && P_{i,j} \text{ may be identified with } (-1)^{(i-1)j}\,\sigma_j(X^i)\,, \text{ in}
\end{aligned}
\tag{V.1}
$$

particular, if j is 1, $P_{i,1}$ with $(-1)^{i-1}\sigma_1(X^i) = (-1)^{i-1}s_i(X)$, where the σ's and s's are the elementary symmetric polynomials and the symmetric powers, respectively.

(vii) $H^*(BU;Z_p)$ may be identified with ${}_{Z_p}\mathcal{T}_{A,C} \cong {}_{Z}\mathcal{T}_{A,C} \otimes Z_p$ by identifying c_i with $P_i = P_{1,i}$, where c_i is the i^{th} universal Chern class $\in H^{2i}(BU;Z_p)$.

Our result is:

$$\wp^{i-1}(P_{1,i}) = \sum_{\substack{r+s=i \\ r\geq 0 \ s\geq 1}} P_{(s-1)p+1,1}\, P_{p,r}\,. \tag{V.2}$$

Notice, since $(s-1)p+1 \neq p$ for all s, this is a linear combination of basis elements. Before proving this result, let us rewrite the formula as a polynomial in the Chern classes. We shall need Waring's formula, the non-recursive version of Newton's formula (see Mac Mahon [5])

$$(-1)^i s_i(X) = \sum_{\substack{\omega(J)=i \\ \#(J)=j}} \frac{(-1)^{j_i}}{j}\binom{j}{j_1,j_2,\ldots,j_n}\sigma_1(X)^{j_1}\ldots\sigma_n(X)^{j_n}$$

where $\omega(J) = j_1+j_2+\ldots+j_n$. $\#(J) = j_1+j_2+\ldots+j_n$, and

$$\binom{j}{j_1,j_2,\ldots,j_n} = \frac{j!}{j_1!j_2!\ldots j_n!} \quad \text{(or 0 if any } j_i \text{ is negative).}$$

Let us rewrite $\sum_{\substack{r+s=i \\ r\geq 0 \ s\geq 1}} P_{(s-1)p+1,1}\, P_{p,r}$ as

$$\sum_{\substack{r+s=i \\ r\geq 0 \ s\geq 1}} (-1)^{(s-1)p}\sigma_1(X^{(s-1)p+1})\cdot(-1)^{(p-1)r}\sigma_r(X^p)$$

$$\equiv (-1)^i \sum_{\substack{r+s=i \\ r\geq 0 \ s\geq 1}} (-1)^{r-1} s_{(s-1)p+1}(X)\,\sigma_r(X)^p$$

(by Fermat's theorem and $\sigma_1(X^i) = s_i(X)$)

$$\equiv (-1)^i \sum_{\substack{r+s=i \\ r\geq 0\ s\geq 1}} (-1)^{r+(s-1)p} \sum_{\substack{\omega(K)=(s-1)p+1 \\ \#(K)=k}} (-1)^k \frac{(s-1)p+1}{k} \binom{k}{k_1 k_2 \ldots k_n} \sigma_1(X)^{k_1} \ldots \sigma_r(X)^{k_r+p} \ldots \sigma_n(X)^{k_n}$$

(by Waring's formula)

$$\equiv (-1) \sum_{\substack{\omega(J)=(i-1)p+1 \\ \#(J)=j}} (-1)^j \frac{(i-1)p+1}{j} \binom{j}{j_1 j_2 \ldots j_n} \sigma_1(X)^{j_1} \ldots \sigma_n(X)^{j_n}$$

$$+ (-1) \sum_{r=1}^{i-1} \sum_{\substack{\omega(J)=(i-1)p+1 \\ \#(J)=j}} (-1)^{j-p} \frac{(i-r-1)p+1}{j-p} \binom{j-p}{j_1 \ldots j_r - p \ldots j_n}$$

$$\times \sigma_1(X)^{j_1} \ldots \sigma_r(X)^{j_r} \ldots \sigma_n(X)^{j_n}$$

$$\equiv -\sum_{\substack{\omega(J)=(i-1)p+1 \\ \#(J)=j}} (-1)^j \left\{ \frac{1}{j} \binom{j}{j_1 j_2 \ldots j_n} - \sum_{r=1}^{n} \frac{1}{j-p} \binom{j-p}{j_1 \ldots j_r - p \ldots j_n} \right\}$$

$$\times \sigma_1(X)^{j_1} \ldots \sigma_n(X)^{j_n} \pmod{p} .$$

($(i-r-1)p+1 \equiv 1 \pmod{p}$ for all r ; the range of r is now different, $r=1,\ldots,n$, instead of $r=1,\ldots,i-1$, but this is harmless, since if $r > (i-1)$, $j_r - p < 0$ since $\omega(J) = (i-1)p+1 = j_1+\ldots+(rj_r)+\ldots+nj_n$.)

So, identifying c_i with $\sigma_i(X) \approx P_i$, we have

$$\rho^{i-1}(c_i) = - \sum_{\substack{\omega(J)=(i-1)p+1 \\ \#(J)=j}} (-1)^j \left\{ \frac{1}{j} \binom{j}{j_1 j_2 \ldots j_n} - \frac{1}{j-p} \sum_{r=1}^{n} \binom{j-p}{j_1 \ldots j_r - p \ldots j_n} \right\} \tag{V.3}$$

$$c_1^{j_1} c_2^{j_2} \ldots c_n^{j_n}$$

It is conceivable that this expression simplifies, via mod p arithmetic.

For example, if $p = 2$, which is inadmissible, the coefficients vanish except when $J = (0,0,\ldots,0,1)_{(i-1)p+1}$ and $(0,0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)_{r\quad s}$ with $r+s = (i-1)p+1$. We give an argument in an appendix to this chapter. In spite of the trouble, this is worth doing, as it verifies the compatability of our result with Wu's formula for the value of the Steenrod squares on the Stiefel Whitney classes, in the special case, $Sq^{i-1}(w_i)$. We notice immediately that if J has all entries less than p, the coefficient is $\frac{(-1)^{l+j}}{j}\binom{j}{j_1\ldots j_n}$. There are examples when J fails to have entries less than p in which the "correction terms" are not trivial. e.g., if $p=3$, $j=5$, $j_1=3$, $j_2=1$, $j_3=1$, $i=4$, $(i-1)p+1=10$, the coefficient of $c_1^3c_2c_5$ in $\mathcal{P}^3(c_4) \equiv 2 \pmod 3$, but $\frac{(-1)^{l+j}}{j}\binom{j}{j_1j_2j_3} \equiv 1 \pmod 3$.

We now secure our result. Throughout, p is a fixed strictly positive integer, not necessarily a prime.

On $Z[X_1,X_2,\ldots,X_n]$, let us define operators $\{\mathcal{P}^i\}_{i\in Z^+}$ as follows:

$$
\begin{aligned}
&\text{i)} \quad \mathcal{P}^i(1) = 0,\ i \in Z^+-\{0\},\ \mathcal{P}^0(1) = 1. \\
&\text{ii)} \quad \mathcal{P}^0(X_j) = X_j,\ j \in \{1,2,\ldots,n\} \\
&\text{iii)} \quad \mathcal{P}^1(X_j) = X_j^p,\ j \in \{1,2,\ldots,n\}. \\
&\text{iv)} \quad \mathcal{P}^i(X_j) = 0 \ \text{ if } \ i > 1,\ j \in \{1,2,\ldots,n\}. \\
&\text{v)} \quad \text{If } P,P',P'' \text{ are polynomials in } Z[X], \text{ and } P = P' + P'', \\
&\qquad \text{then } \mathcal{P}^i(P) = \mathcal{P}^i(P') + \mathcal{P}^i(P''). \\
&\text{vi)} \quad \text{If } P,P',P'' \text{ are polynomials in } Z[X], \text{ and } P = P'P'', \\
&\qquad \text{then } \mathcal{P}^i(P'P'') = \sum_{i'+i''=i} \mathcal{P}^{i'}(P')\,\mathcal{P}^{i''}(P'').
\end{aligned}
\tag{V.4}
$$

$$\wp^i(M) = \sum_{i'+i''=i} \wp^{i'}(X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n-1})\cdot\wp^{i''}(X_n)$$

$$= \wp^{i-1}(X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n-1})\cdot\wp^1(X_n) \qquad \text{(by Lemma 2)}$$

$$= (X_1^{i_1}\ldots X_n^{i_n-1})^p\ X_n^p \qquad \text{(by inductive assumption)}$$

$$= M^p\ .$$

Lemma 4. $\wp^\ell(X_j^k) = \binom{k}{\ell} X_j^{k+\ell(p-1)}$ for all j, k, and ℓ.

Proof: Assume this is true for $k' < k$, for all j and ℓ.

$$\wp^\ell(X_j^k) = \sum_{\ell'+\ell''=\ell} \wp^{\ell'}(X_j^{k-1})\ \wp^{\ell''}(X_j)$$

$$= \wp^\ell(X_j^{k-1})\ X_j + \wp^{\ell-1}(X_j^{k-1})\cdot X_j^p$$

$$= \binom{k-1}{\ell} X_j^{k-1+\ell(p-1)}\cdot X_j + \binom{k-1}{\ell} X_j^{(k-1)+(\ell-1)(p-1)}\ X_j^p$$

$$= \left[\binom{k-1}{\ell} + \binom{k-1}{\ell-1}\right]\cdot X_j^{k+\ell(p-1)} = \binom{k}{\ell} X_j^{k+\ell(p-1)}\ .$$

Lemma 5. $\wp^\ell(s_k(X)) = \binom{k}{\ell} s_{k+\ell(p-1)}(X)$ for all k and ℓ.

Proof: This follows immediately from the definitions of the symmetric powers, Lemma 4, and the additivity of the operators.

Lemma 6. $\wp^{jk}(\sigma_k(X^j)) = \sigma_k(X^{jp})$ for all j and k.

Proof: This follows immediately from the definitions of the elementary symmetric functions, Lemma 3, and the additivity of the operators.

We now identify the sub-(Hopf) algebra $Z\mathcal{T}^n_{A,C} \subseteq Z\mathcal{T}_{A,C}$ with the symmetric polynomials in $Z[X]$, via the identification of $P_{i,j}$ with $(-1)^{i-1}\ \sigma_j(X^i)$, when $ij < n$. It is clear from (V.4) v) and vi), Lemma 5, and the well known facts that the symmetric powers generate the symmetric polynomials rationally, and the symmetric polynomials are a direct summand of $Z[X]$, that the family of generators $\{\wp^i\}_{i\in Z^+}$

Of course, v) and vi) must be shown to be consistent with i)-iv) and to be well defined. These are trivial exercises and we leave them undone. e.g., vi) must be applied first to monomials, whose distinct factorizations are easily written down, and the operator values determined by these factorizations can be readily compared.

There are some easy consequences of the definitions:

Lemma 1. If P is a polynomial in $Z[X]$, $\wp^0(P) = P$.

Proof: It suffices to prove this for monomials $X_1^{j_1}X_2^{j_2}\ldots X_n^{j_n}$. Suppose it is true for monomials of degree less than or equal to $j_1 + j_2 + \ldots + j_n - 1$. Then $\wp^0(X_1^{j_1}X_2^{j_2}\ldots X_n^{j_n}) = \wp^0(X_1^{j_1}X_2^{j_2}\ldots X_n^{j_n-1}) \times \wp^0(X_n) = X_1^{j_1}\ldots X_n^{j_n-1} \cdot X_n$. (We assume without loss of generality that $j_n \geq 1$.)

Lemma 2. If P is a polynomial of degree k, then $\wp^i(P) = 0$ if $i > k$.

Proof: It suffices to prove this for monomials $X_1^{j_1}X_2^{j_2}\ldots X_n^{j_n}$

$$\wp^i(X_1^{j_1}\ldots X_n^{j_n}) = \sum_{i'+i''=i} \wp^{i'}(X_1^{j_1}\ldots X_n^{j_n-1})\ \wp^{i''}(X_n)$$

$$= \wp^i(X_1^{j_1}\ldots X_n^{j_n-1})\ \wp^0(X_n) + \wp^{i-1}(X_1^{j_1}\ldots X_n^{j_n-1}) \cdot \wp^1(X_n)$$

$$= 0 \cdot X_n + 0 \cdot X_n^p$$

by the induction assumption. (We assume without loss of generality that $j_n \geq 1$.)

Lemma 3. If M is a monomial of degree i, then $\wp^i(M) = M^p$.

Proof: Let $M = X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n}$. (We assume without loss of generality that $i_n \geq 1$.)

$$\wp^i(M) = \sum_{i'+i''=i} \wp^{i'}(X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n-1})\cdot\wp^{i''}(X_n)$$

$$= \wp^{i-1}(X_1^{i_1}X_2^{i_2}\ldots X_n^{i_n-1})\cdot\wp^1(X_n) \qquad \text{(by Lemma 2)}$$

$$= (X_1^{i_1}\ldots X_n^{i_n-1})^p\, X_n^p \qquad \text{(by inductive assumption)}$$

$$= M^p .$$

Lemma 4. $\wp^\ell(X_j^k) = \binom{k}{\ell} X_j^{k+\ell(p-1)}$ for all j, k, and ℓ.

Proof: Assume this is true for $k' < k$, for all j and ℓ.

$$\wp^\ell(X_j^k) = \sum_{\ell'+\ell''=\ell} \wp^{\ell'}(X_j^{k-1})\,\wp^{\ell''}(X_j)$$

$$= \wp^\ell(X_j^{k-1})\,X_j + \wp^{\ell-1}(X_j^{k-1})\cdot X_j^p$$

$$= \binom{k-1}{\ell} X_j^{k-1+\ell(p-1)}\cdot X_j + \binom{k-1}{\ell} X_j^{(k-1)+(\ell-1)(p-1)}\, X_j^p$$

$$= \left[\binom{k-1}{\ell} + \binom{k-1}{\ell-1}\right]\cdot X_j^{k+\ell(p-1)} = \binom{k}{\ell} X_j^{k+\ell(p-1)} .$$

Lemma 5. $\wp^\ell(s_k(X)) = \binom{k}{\ell} s_{k+\ell(p-1)}(X)$ for all k and ℓ.

Proof: This follows immediately from the definitions of the symmetric powers, Lemma 4, and the additivity of the operators.

Lemma 6. $\wp^{jk}(\sigma_k(X^j)) = \sigma_k(X^{jp})$ for all j and k.

Proof: This follows immediately from the definitions of the elementary symmetric functions, Lemma 3, and the additivity of the operators.

We now identify the sub-(Hopf) algebra $Z\mathcal{T}^n_{A,C} \subseteq Z\mathcal{T}_{A,C}$ with the symmetric polynomials in $Z[X]$, via the identification of $P_{i,j}$ with $(-1)^{i-1}\,\sigma_j(X^i)$, when $ij < n$. It is clear from (V.4) v) and vi), Lemma 5, and the well known facts that the symmetric powers generate the symmetric polynomials rationally, and the symmetric polynomials are a direct summand of $Z[X]$, that the family of generators $\{\wp^i\}_{i\in Z^+}$

map symmetric polynomials into symmetric polynomials. A compatibility argument, such as that offered in Chapter III, page 25, would assure us that the operators extend uniquely to $_{Z}\mathcal{T}_{A,C}$. We leave this to the reader. In an obvious way, operators are induced in $H^*(BU;Z_p)$ $\cong {}_{Z}\mathcal{T}_{A,C} \underset{Z}{\otimes} Z_p$.

Theorem 1. If p is an odd prime, $\{\wp^i\}_{i\in Z^+}$ are the Steenrod reduced powers.

Proof: Let us verify the axioms for the Steenrod reduced p-powers. (See Steenrod and Epstein [6], p. 76)

1) $\wp^i: H^q(BU;Z_p) \to H^{q+2i(p-1)}(BU;Z_p)$ is a homomorphism of abelian groups. The correctness of dimensions follows from (V.4) by an easy induction. (V.4) v) implies the group homomorphism property.

2) $\wp^0 = 1$. This is Lemma 1.

3) If X is homogeneous of degree $2k$, then $\wp^k(X) = X^p$. This is Lemma 3, coupled with Fermat's theorem.

4) If $2k >$ degree X, then $\wp^k(X) = 0$. This is Lemma 2.

5) Cartan formula: $\wp^k(XY) = \sum_i \wp^i(X)\,\wp^{k-i}(Y)$. This is (V.4),vi). This is still insufficient, for we have not invoked naturality. Up to degree $2n$, we may identify $H^*(BU;Z_p)$ as the sub-algebra of $H^*(BU(1)^{Xn};Z_p)$, which is a Z_p polynomial algebra in generators $\{X_1,X_2,\ldots,X_n\}$ of degree 2, fixed under the action of the symmetric group, with Chern classes restricting to elementary symmetric polynomials. The Steenrod operations must extend to operators on $Z[X_1,\ldots,X_n]$ satisfying axioms 1).- 5). It is clear from our development that this can be done uniquely, and that our operators and the Steenrod operations agree.

This is essentially a well-worn argument. However, a crucial

difference is that we exchanged the axiom " $\mathcal{P}^k(X) = X^p$ if X is of degree $2k$ " to the weaker analogue for monomials only in order to define integral lifts of the operations.

Let us now perform the computation, in a more general form, returning to the notation of (V.1):

$$\mathcal{P}^{ij-1}(P_{i,j}) = (-1)^{(ij-1)(p-1)} \cdot i \cdot \sum_{\substack{r+s=j \\ r\geq i, s\geq 0}} P_{(ir-1)p+1,1}\, P_{ip,s} \,. \qquad (V.5)$$

If $i = 1$ and p is an odd prime, this clearly reduces to (V.2).

First, let us rewrite Lemmas 6 and 5 as

$$\begin{aligned} \mathcal{P}^{jk}(P_{j,k}) &= (-1)^{(j-1)k}\,(-1)^{(jp-1)k} \cdot P_{jp,k} \\ &= (-1)^{jk(p-1)}\, P_{jp,k} \end{aligned} \qquad (V.6)$$

and

$$\begin{aligned} \mathcal{P}^{\ell}(P_{k,1}) &= (-1)^{k-1} \cdot (-1)^{k+\ell(p-1)-1} \binom{k}{i} P_{k+\ell(p-1),1} \\ &= (-1)^{\ell(p-1)} \binom{k}{\ell} P_{k+\ell(p-1),1} \end{aligned} \qquad (V.7)$$

Let us suppose now that (V.5) holds for fixed i, $j' < j$. We start the induction by (V.7), with $j = 1$.

$j\,\mathcal{P}^{ij-1}(P_{i,j}) =$ (by linearity)

$\mathcal{P}^{ij-1}(j\,P_{i,j} - K_{i,j}) + \mathcal{P}^{ij-1}(K_{i,j}) =$ (by (V.1)iv) and the definition of $K_{i,j}$)

$\mathcal{P}^{ij-1}(P_{ij,1}) + \mathcal{P}^{ij-1} \sum_{\substack{r+s=j \\ r>0\ s>0}} P_{i,r}\, P_{is,1} =$ (by Lemma 2, Cartan's formula (V.4)v), and (V.7))

$$j\{(-1)^{(ij-1)(p-1)}\, i\, P_{(ij-1)p+1,1}\} + \sum_{\substack{r+s=j \\ r>0\ s>0}} \mathcal{P}^{ir}(P_{i,r})\, \mathcal{P}^{is-1}(P_{is,1})$$

$$+ \sum_{r+s=j} \rho^{ir-1}(P_{i,r}) \cdot \rho^{is}(P_{is,1}) = \qquad \text{(by inductive assumption, (V.6) and (V.7))}$$

$$j\{(-1)^{(ij-1)(p-1)}\, i\, P_{(ij-1)p+1,1}\}$$

$$+ \sum_{\substack{r+s=j \\ r>0,\, s>0}} (-1)^{ir(p-1)} P_{ip,r} \cdot (-1)^{(is-1)(p-1)} \cdot is \cdot P_{(is-1)p+1,1}$$

$$+ \sum_{\substack{r+s=j \\ r>0\ s>0}} ((-1)^{(ir-1)(p-1)}\, i \cdot \sum_{\substack{t+u=r \\ t\geq 1\ u\geq 1}} P_{(it-1)p+1,1}\, P_{ip,u}) \cdot (-1)^{(is)(p-1)} P_{isp,1}$$

$$+ \sum_{\substack{r+s-j \\ r>0\ j>0}} (-1)^{(ir-1)(p-1)}\, i \cdot P_{(ir-1)p+1,1} \cdot (-1)^{(is)(p-1)} P_{isp,1} =$$

(by $P_{isp,1} = s\, P_{ip,s} - K_{ip,s}$, from (V.1) iv))

$$= j\{(-1)^{(ij-1)(p-1)}\, i\, P_{(ij-1)p+1,1}\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\{\sum_{\substack{r+s=j \\ r>0\ s>0}} s\, P_{(is-1)p+1,1}\, P_{ip,r}\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\{\sum_{\substack{t+v=j \\ t>0\ v>0}} P_{(it-1)p+1,1} \sum_{\substack{u+s=v \\ u>0\ s>0}} P_{ip,n}(sP_{ip,s} - K_{ip,s})\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\{\sum_{\substack{r+s=j \\ r>0\ j>0}} P_{(ir-1)p+1,1}(s\, P_{ip,s} - K_{ip,s})\} =$$

(by definition of $K_{ip,v}$)

$$= j\{(-1)^{(ij-1)(p-1)}\, i\, P_{(ij-1)p+1,1}\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\{\sum_{\substack{r+s=j \\ r>0\ s>0}} s\, P_{(is-1)p+1,1}\, P_{ip,r}\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\{\sum_{\substack{t+v=j \\ t>0\ v>0}} P_{(it-1)p+1,1}\, K_{ip,v}\}$$

$$+ (-1)^{(ij-1)(p-1)}\, i\Big\{ \sum_{\substack{r+s=j \\ r>0\ j>0}} s\, P_{(ir-1)p+1,1}\, P_{ip,s} \Big\}$$

$$- (-1)^{(ij-1)(p-1)}\, i\Big\{ \sum_{\substack{r+s=j \\ r>0\ j>0}} P_{(ir-1)p+1,1}\, K_{ip,s} \Big\} = \text{(by cancellation and reindexing)}$$

$$j\{(-1)^{(ij-1)(p-1)}\, i\, P_{(ij-1)p+1,1}\}$$

$$+ (-1)^{(ij-1)(p-1)} \sum_{\substack{r+s=j \\ r>0,s>0}} (r+s)\, P_{(ir-1)p+1,1}\, P_{ip,s}$$

$$= j\{(-1)^{(ij-1)(p-1)}\, i \sum_{\substack{r+s=j \\ r\geq 1,s>0}} P_{(ir-1)p+1,1}\, P_{ip,s}\}.$$

Since there is no j torsion, we "divide by j" and get (V.5), as required.

Appendix: A note on Wu's Formula.

Wu Wen-Tsun has computed the action of the Steenrod squares $\{Sq^k\}_{k\in Z^+}$ on the Stiefel Whitney classes $\{w_i\}_{i\in Z^+}$ as follows: (see Hsiang [7]).

$$Sq^k w_i = \sum_{0\leq r\leq k} \binom{i+r-k-1}{r} w_{k-r}\, w_{i+r}\,.$$

In particular,

$$Sq^{i-1}(w_i) = \sum_{\substack{r+s=i \\ r\geq 1\ s\geq 0}} w_{(r-1)2+1}\, w_s\,.$$

We show that we get an analogous formula when $p = 2$ in (V.3), i.e.,

$$(-1)^{1+j}\Big\{ \frac{1}{j} \binom{j}{j_1 \ldots j_n} - \sum_{r=1}^{n} \frac{1}{j-2} \binom{j-2}{j_1 \ldots j_{r-2} \ldots j_n} \Big\} \equiv 0 \pmod 2 \qquad \text{(V.8)}$$

when $\omega(J) = (i-1)2+1$ unless $J = (0,\ldots,0,1,0,\ldots,0)$ or

$(0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)$.

We first notice that not all of $j_1 j_2 \ldots j_n$ can be even, since $\omega(J)$ is odd. Since we make no further use of $j_1 + 2j_2 + \ldots + nj_n = (i-1)2+1$, we may assume that j_1 is odd, and $j_1, j_2, \ldots, j_n$ are not zero. Since j_1 is odd, we have $1 \equiv j_1 \pmod 2$ and (V.8) becomes

$$\frac{j_1}{j}\binom{j}{j_1 \ldots j_n} + \frac{j_1}{j-2}\sum_{r=1}^{n}\binom{j-2}{j_1 \ldots j_r - 2 \ldots j_n} \equiv 0$$

or

$$\binom{j-1}{j_1-1\ j_2 \ldots j_n} + \binom{j-3}{j_1-3\ j_2 \ldots j_n} + \sum_{r=2}^{n}\binom{j-3}{j_1-1\ j_2 \ldots j_r-2 \ldots j_n} \equiv 0 \pmod 2. \qquad \text{(V.9)}$$

Suppose that j-1 is odd. If $j-1 = 1$, clearly $\binom{j}{j_1 \ldots j_n} = \binom{2}{1\ 1}$, $\frac{1}{j}\binom{j}{j_1 \ldots j_n} \equiv 1 \bmod 2$, and the "correction terms" don't exist. This is the special case $J = (0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)$.

If $j-1 \neq 1$, then j_s is odd for some $s \neq 1$. Multiplying (V.9) by $\frac{j_s-1}{j-1} \equiv 1 \pmod 2$ we get

$$\binom{j-2}{j_1-1\ j_2 \ldots j_{s-1} \ldots j_n} + \binom{j-4}{j_1-3\ j_2 \ldots j_s-1 \ldots j_n}$$

$$+ \sum_{r=2}^{n}\binom{j-4}{j_1-1\ j_2 \ldots j_s-1 \ldots j_r-2 \ldots j_n} \equiv 0 \pmod 2$$

where $j-2$ is even.

If j-1 is even, and zero, we had $\binom{j}{j_1\ j_2 \ldots j_n} = \binom{1}{1}$ and $\frac{1}{j}\binom{j_1}{j_1\ j_2 \ldots j_n} \equiv 1 \pmod 2$, and the "correction terms" don't exist.

This is the special case $J = (0,\ldots,0,1,0,\ldots,0)$.

When $j-1$ is even, $\neq 0$, or $j-1$ is odd, $\neq 1$, we have reduced (V.8) to the following:

Lemma: If $k \neq 0$ is even, and $k = k_1+k_2+\ldots+k_n$, then

$$\binom{k}{k_1k_2\ldots k_n} + \sum_{r=1}^{n} \binom{k-2}{k_1k_2\ldots k_r-2\ldots k_n} \equiv 0 \pmod 2 .$$

We divide the proof into sublemmas.

Sublemma 1. (Dickson) $\binom{\ell}{\ell_1\ell_2\ldots\ell_n} \not\equiv 0 \bmod p$ if and only if $\ell_1+\ell_2+\ldots+\ell_n = \ell$ is an addition which can be performed "without carrying" when written in base p .

Proof: We give an alternative to Dickson's argument (see Dickson [8], p.76). We start with the familiar formula

$$\binom{a}{b} \equiv \prod_i \binom{a_i}{b_i} \pmod p$$

where $\{a_i\}$ and $\{b_i\}$ are the p-adic expansions of b and a . (See Steenrod and Epstein [6], p. 5). This implies the sublemma in the case $\binom{\ell}{\ell_1\ell_2}$. But $\binom{\ell}{\ell_1\ell_2\ldots\ell_n} = \binom{\ell}{\ell_1}\binom{\ell-\ell_1}{\ell_2\ldots\ell_n}$, and the sublemma follows by induction.

Sublemma 2. $\binom{k}{k_1k_2\ldots k_n} \equiv 0 \pmod 2$ if k is even and any k_i is odd.

Proof: This follows immediately from Sublemma 1.

Sublemma 3. If all k_i are even, and $k_1+k_2+\ldots+k_n = k$ is an addition which can be performed without carrying when written base 2 , then

$k_1+k_2+\ldots+(k_r-2)+\ldots+k_n = k-2$ is an addition which can be performed without carrying when written base 2 for exactly one r in $\{1,2,\ldots,n\}$. Furthermore, $\binom{k}{k_1\ldots k_n} \equiv \binom{k-2}{k_1k_2\ldots k_r-2\ldots k_n} \equiv 1$ under these circumstances.

Proof: Let $\{{}^ik_t\}$ be the p-adic expansion of k_t, $\{{}^ik\}$ that of k. Clearly, if ${}^{i_0}k = 1$ and ${}^ik = 0$ if $i < i_0$, then ${}^{i_0}k_r$ must be 1, no ${}^{i_0}k_t$ is 1 if $t \neq r$, and ${}^ik_t = 0$ for $i < i_0$. The equality of multinomial coefficients comes from Sublemma 1.

Sublemma 4. If all k_i are even, and $k_1+k_2+\ldots+k_n = k$ is an addition which cannot be performed without carrying then if $k_1+k_2+\ldots+(k_r-2)+\ldots+k_n = k-2$ can be performed without carrying, there is exactly one $s \neq r$ such that $k_1+\ldots+(k_s-2)+\ldots+k_n = k-2$ can be performed without carrying, when written base 2. Under these circumstances,

$$\binom{k}{k_1\ldots k_n} \equiv 0 \equiv \binom{k-2}{k_1k_2\ldots k_t-2\ldots k_t} \pmod 2$$

if $t \neq r, s$, and

$$\binom{k-2}{k_1k_2\ldots k_r-2\ldots k_n} \equiv 1 \equiv \binom{k-2}{k_1k_2\ldots k_s-2\ldots k_n} \bmod 2 .$$

Proof: Let $\{{}^ik\}$ and $\{{}^ik_t\}$ be as in Sublemma 3. If

$${}^{j_0}k_r = 1 \quad \text{and} \quad {}^jk_r = 0 \quad \text{for} \quad 1 \le j \le j_0 ,$$

then

$${}^{j_0}(k_r-2) = 0 \quad \text{and} \quad {}^j(k_r-2) = 1 \quad \text{for} \quad 1 \le j \le j_0 .$$

Since $k_1+\ldots+(k_r-2)+\ldots+k_n = k-2$ involves no carrying, there is no

t such that ${}^{j}k_{t} = 1$ for $j < j_0$ and there is at most one $t \neq r$ such that ${}^{j}k_{t} = 1$ for $j \geq j_0$. Since $k_1+k_2+\ldots+k_n = k$ did involve carrying, this must have occurred at 2^{j_0}, i.e., there is exactly one s such that $s \neq r$ and ${}^{j_0}k_{s} = 1$. Clearly, $k_1+\ldots+(k_s-2)+\ldots+k_n = k-2$ involves no carrying, and there are no other such sums. The equality of multinomial coefficients comes from Sublemma 1.

Sublemma 4 completes the proof of the Lemma, and consequently, (V.8).

CHAPTER VI

FINITE TOWERS IN COMMUTATIVE ASSOCIATIVE HOPF ALGEBRAS

We prove that in commutative, associative Hopf algebras, if a primitive supports a tower of height $n-1$, but not a tower of height n, then n is a power of a prime.

At first glance, this is upsetting, for the following reason. In $Z\mathcal{J}^{n-1}_{A,C}$ (see page 25), there is a natural tower $\{P_i\}_{i\leq n-1}$ over P_1 which cannot be extended to a tower of height n. Argument: The inclusion $Z\mathcal{J}^{n-1}_{A,C} \xrightarrow{i_{n-1}} Z\mathcal{J}_{A,C}$ is a Hopf algebra monomorphism. Any homogeneous primitive of degree n in $Z\mathcal{J}^{n-1}_{A,C}$ must map into $\lambda(nP_n - K_n)$ for some $\lambda \in Z$, by Theorem 1 of Chapter III. Clearly $K_n = \sum_{i+j=n} P_i(jP_j - K_j)$ is in the image of i_{n-1}, but no multiple of P_n is, so λ must be zero. By Proposition 1 of Chapter II, if P'_n extends $\{P_i\}_{i<n}$, then $nP'_n - K_n$ is primitive and homogeneous of degree n, and is zero. Hence K_n is divisible by n. But the P_1^n coefficient of K_n is ± 1 (see page 22), so K_n cannot be divisible by n. P'_n cannot exist.

We shall make use of Proposition 2 of Chapter II in a constructive way — but, we prove the existence of towers in $Z\mathcal{J}^{n-1}_{A,C}$ of height $n, n+1, \ldots$ up to the smallest prime power exceeding $n-1$ without exhibiting them as families of polynomials in $\{P_i\}_{i\leq n}$, the algebra generators of the Hopf algebra, an exercise with Waring's formula (p. 34).

We use Theorem 1 of Chapter III and the inclusion $Z\mathcal{J}^{n-1}_{A,C} \xrightarrow{i_{n-1}} Z\mathcal{J}_{A,C}$ to justify the following:

Lemma: A basis for $P({}_Z\mathcal{T}^{n-1}_{A,C})$ is $\{iP_i - K_i\}_{i\in\{1,2,\ldots,n-1\}}$. We have canonical towers over these primitives (see p. 27) — if $iP_i - K_i = P_{i,1}$, $\{P_{i,j}\}_{j\in\{1,2,\ldots,[n-1/i]\}}$ is a tower over $P_{i,1}$ of height $[n-1/i]$. Furthermore $jP_{i,j} - K_{i,j} = ijP_{ij} - K_{ij} = P_{ij,1}$ in allowable ranges.

Preparatory to the use of Proposition 2 of Chapter II, we must modify each story of $\{P_i\}_{i\in\{1,2,\ldots,n\}}$ whose height $i \neq 1$ divides n by a primitive, $Q_{i,1} = x_i(iP_i - K_i)$, equipped with a fixed tower $\{Q_{i,j}\}_{\substack{j\in\{1,2,\ldots,n/i\}\\ i\neq 1}}$. A trivial computation ensures that $Q_{i,j} \equiv x_i^j P_{i,j}$ will do. If $H_{i,j} = \sum_{\substack{r+s=j\\ i\neq 1}} Q_{i,r}(sQ_{i,s} - H_{i,s})$, then one shows by induction that $H_{i,j} = x_i^j K_{i,j}$. If $\{\overline{P_{1,j}}\}_{j\in\{1,2,\ldots,n-1\}}$ is the amalgamation of these towers, and $\overline{K_{1,j}}$ is defined as usual, Proposition 2 implies, in the absence of primitives in degree n,

$$(*) \qquad \overline{K_{1,n}} = \sum_{\substack{ij=n\\ i\neq 1\ j\neq 1}} i\, H_{i,j} + K_n \quad \text{in} \quad {}_Z\mathcal{T}^{n-1}_{A,C} \otimes Z_n .$$

Furthermore, $\overline{K_{1,n}} = 0$ in ${}_Z\mathcal{T}^{n-1}_{A,C} \otimes Z_n$ if and only if the tower $\{\overline{P_{1,j}}\}_{j=1,2,\ldots,n-1}$ can be extended by $\overline{P_{1,n}}$ by Proposition 1 of Chapter II.

Let us apply i_{n-1} to (*). We find ourselves in ${}_Z\mathcal{T}_{A,C} \otimes Z_n$ where $\{P_{i,j}\}_{ij=n}$ exist, and clearly, recalling that $H_{i,j} = x_i^j K_{i,j}$,

$$i_{n-1}(\overline{K_{1,n}}) = \sum_{\substack{ij=n\\ i\neq 1, j\neq 1}} i\, x_1^j (K_{i,j} - jP_{i,j}) + (K_n - nP_n)$$

$$= \Big(\sum_{\substack{ij=n\\ i\neq 1, j\neq 1}} i\, x_i^j + 1\Big)(K_n - nP_n) .$$

Since i_{n-1} is a monomorphism onto a direct summand, (obvious from the usual basis of monomials), $\overline{K_{1,n}}$ is divisible by n in $Z\mathcal{J}^{n-1}_{A,C}$ if and only if $\sum_{\substack{ij=n \\ i\neq 1, j\neq 1}} i\, x_i^j + 1 \equiv 0 \bmod n$.

Let us remember that each modifying primitive is equipped with a fixed tower. We must modify these towers as well for the most general amalgamated tower $\{\overline{P_i}\}$. But by the argument of Proposition 3 of Chapter II, any two towers of height $n-1$ over P_1 must be amalgamations of one another.

Let us modify the towers $\{Q_{i,j}\}_{j\in\{1,2,\ldots,n/i\}}$ over $Q_{i,1} = x_i P_{i,1}$. As a "first order" modification, we amalgamate towers

$\{Q_{i,j,k} \equiv x_{i,j}^k P_{ij,k}\}_{\substack{k\in\{1,2,\ldots,n/ij\} \\ j\neq 1}}$ over $Q_{i,j,1} = x_{i,j} P_{ij,1}$ with $\{Q_{i,j}\}_{j\in\{1,2,\ldots,n/i\}}$.

Define $H_{i,j,k}$ by $H_{i,j,k} = \sum_{k=\ell+m} Q_{i,j,\ell}(mQ_{i,j,m} - H_{i,j,m})$ and find by induction $H_{i,j,k} = (x_{i,j})^k K_{ij,k}$. The amalgamated tower is

$\{\overline{Q_{i,j}}\}_{\substack{j\in\{1,2,\ldots,n/i\} \\ i\neq 1}}$.

By Proposition 2, we have in $Z\mathcal{J}^{n-1}_{A,C} \otimes Z_{n/i}$

$$\overline{H_{i,n/i}} = \sum_{\substack{jk=n/i \\ j\neq 1\ k\neq 1}} j\, H_{i,j,k} + H_{i,n/i}$$

$$= \sum_{\substack{jk=n/i \\ j\neq 1\ k\neq 1}} j(x_{i,j})^k K_{ij,k} + x_i^{n/i} K_{i,n/i}.$$

Applying i_{n-1}, in $Z\mathcal{J}_{A,C} \otimes Z_{n/i}$ we have

$$i_{n-1}(\overline{H_{i,n/i}}) = \sum_{\substack{jk=n/i \\ j\neq 1 \ k\neq 1}} j(x_{i,j})^k \ (K_{ij,k} - kP_{ij,k})$$

$$+ x_i^{n/i}(K_{i,n/i} - n/iP_{i,n/i})$$

$$= \Big(\sum_{\substack{jk=n/i \\ j\neq 1 \ k\neq 1}} j(x_{i,j})^k + x_i^{n/i} \Big) \ (K_n - nP_n) \ .$$

We now return to modify the original tower $\{P_j\}_{j\in\{1,2,\ldots,n-1\}}$ by the towers $\{\overline{Q_{i,j}}\}_{\substack{j\in\{1,2,\ldots,n/i\} \\ i\neq 1}}$, rather than $\{Q_{i,j}\}_{\substack{j\in\{1,2,\ldots,n/i\} \\ i\neq 1}}$, thus incorporating "second order" modifications. The amalgamated tower will be called $\{\overline{\overline{P_{1,j}}}\}_{j\in\{1,2,\ldots,n-1\}}$. $\{\overline{\overline{K_{i,j}}}\}_{j\in\{1,2,\ldots,n-1\}}$ is defined as usual.

In $Z\mathcal{J}_{A,C}^{n-1} \otimes Z_n$, we have, by Proposition 2, if we write $r|s$ for "r is a proper divisor of s",

$$(**) \qquad \overline{\overline{K_{1,n}}} = \sum_{i|n} i \, \overline{\overline{H_{i,n/i}}} + K_n \ .$$

Applying i_{n-1}, in $Z\mathcal{J}_{A,C} \otimes Z_n$ we have, by our computation of $\overline{H_{i,n/i}}$,

$$i_{n-1}(\overline{\overline{K_{1,n}}}) = \Big\{ \sum_{i|n} i \Big\{ \sum_{j|n/i} j(x_{i,j})^{n/ij} + x_i^{n/i} \Big\}$$

$$+ 1 \Big\} \ (K_n - nP_n) \ .$$

Hence, $\{\overline{\overline{P_{1,j}}}\}_{j\in\{1,2,\ldots,n-1\}}$ extends by $\overline{\overline{P_{1,n}}}$ if and only if

$$\Big\{ \sum_{i|n} i \Big\{ \sum_{j|n/i} j(x_{i,j})^{n/ij} + (x_i)^{n/i} \Big\} + 1 \Big\} \equiv 0 \pmod{n} \ .$$

Reorganizing indices, this is equivalent to

$$\sum_{\substack{k\ell=n \\ k\neq 1,\ell\neq 1}} \ \sum_{\substack{ij=k \\ i\neq 1,j\neq 1}} k \, x_{i,j}^{\ell} + \sum_{\substack{ij=n \\ i\neq 1,j\neq 1}} i \, x_i^j + 1 \equiv 0 \pmod{n} \ .$$

The following theorem is the end product of systematically taking into account higher order modifications of the branch towers. The proof is a straightforward induction, the first two steps of which we have exhibited.

Theorem 1. There is a tower of height n over P_1 in $Z\mathcal{T}^{n-1}_{A,C}$ if and only if there is a solution to the following diophantine equation.

$$\sum_{\substack{d|n \\ d\neq 1}} d \sum_{j=1}^{\infty} \sum_{\substack{i_1 i_2 \ldots i_j = d \\ i_k > 1}} Y_{i_1, i_2, \ldots, i_j}^{n/d} \equiv -1 \pmod{n} . \qquad \text{(VI.1)}$$

By exhibiting solutions to this equation, when n is not a power of a prime, and arguing for the non-existence of such solutions when n is a power of a prime, we shall demonstrate

Theorem 2. There exists a tower of height n over P_1 in $Z\mathcal{T}^{n-1}_{A,C}$ if and only if n is not a power of a prime.

Proof. If $n = p^e$ is a power of a prime, there is clearly no solution to (VI.1), for each proper divisor, d, of n must be a multiple of p, and $pk \equiv -1 \bmod p^e$ has no solution if $e > 0$.

If n is not a power of a prime, we solve the following equation, which implies, of course, a solution of (VI.1).

$$-1 = \sum_{\substack{d|n \\ d\neq 1}} d\, x_d^{n/d} \qquad \text{(VI.2)}$$

For if n is not a power of a prime, let $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, with p_i distinct primes, $e_i > 0$, $i=1,2,\ldots,k, k\geq 2$ and let $n_i = n/p_i^{e_i}$.

The greatest common divisor of $\{n_i\}_{i\in\{1,2,\ldots,k\}}$ is clearly 1. Choose a sequence of integers $\{U_{i,0}\}_{i\in\{1,2,\ldots,k\}}$ such that

$\sum_{i=1}^{k} n_i U_{i,0} = -1$. By Fermat's theorem, $X^p \equiv X \pmod{p}$ if p is prime, $U_{i,0} = U_{i,0}^{p_i^{e_i}} + p_i U_{i,1}$ for some $U_{i,1}$, $i \in \{1,2,\ldots,k\}$. Hence,

$$\sum_{i=1}^{k} n_i p_i U_{i,1} + n_i U_{i,0}^{p_i^{e_i}} = -1 .$$

Suppose that $U_{i,j}$ are defined, $j = 1,2,\ldots,g_i - 1 < e_i$, $i = 1,2,\ldots,k$ satisfying $\sum_{i=1}^{k} n_i \sum_{j=1}^{g_i-1} p_i^j U_{i,j}^{p_i^{e_i-j}} = -1$. Define U_{i,g_i} by

$U_{i,g_i-1} = U_{i,g_i-1}^{p_i^{e_i-g_i+1}} + U_{i,g_i} p_i$. Terminating at $g_i = e_i, i \in \{1,2,\ldots,k\}$, we have $\sum_{i=1}^{k} \sum_{j=1}^{e_i} n_i p_i^j U_{i,j}^{p_i^{e_i-j}} = -1$. Since the coefficient, $n_i p_i^j$, and power, $p_i^{e_i-j}$, in each summand multiply to give n , we may solve (VI.2) by $x_{n_i p_i^j} = U_{i,j}$ and $x_d = 0$ if $d \neq n_i p_i^j$ for some i and j .

Corollary 1. Let $m \in Z^+, p^e$ be the minimal prime power greater than m . Then there is a tower of height $p^e - 1$ in ${}_Z\mathcal{J}^m_{A,C}$ over P_1 .

Proof: Clearly the existence of such a tower in ${}_Z\mathcal{J}^m_{A,C}$ is equivalent to the following: There exists a Hopf algebra map $\lambda_m^{p^{e-1}} : {}_Z\mathcal{J}^{p^e-1}_{A,C} \to {}_Z\mathcal{J}^m_{A,C}$ extending $P_1 \to P_1$. But by Theorem 2, $\lambda_m^{m+1} : {}_Z\mathcal{J}^{m+1}_{A,C} \to {}_Z\mathcal{J}^m_{A,C}$ exists, (the algebra structure is free, so the coalgebra map, which exists by virtue of the tower extension, is a Hopf algebra map as well). Similarly,

λ^{m+2}_{m+1}: $Z\mathcal{J}^{m+2}_{A,C} \longrightarrow Z\mathcal{J}^{m+1}_{A,C}$ exists ... and finally $\lambda^{p^e-1}_{p^e-2}$: $Z\mathcal{J}^{p^e-1}_{A,C} \to Z\mathcal{J}^{p^e-2}_{A,C}$

exists. We simply compose these morphisms.

Caution: There will, in general, be many solutions to (IV.1). We have exhibited only one. Thus, there is nothing unique about the maps in the corollary.

Since $R\mathcal{J}^m_{A,C} \approx Z\mathcal{J}^m_{A,C} \otimes R$, Theorems 1 and 2 and the corollary have analogues for any commutative ring, R .

Corollary 2. Let $\mathcal{K}$ be a connected, commutative, associative Hopf algebra over commutative ring R . Suppose P is primitive, supporting a tower of height m , and p^e is the minimal prime power greater than m . Then there is a tower of height p^e-1 in $\mathcal{K}$ over P .

Proof: Let $\{Q_i\}_{i=1,2,\ldots,m}$ be a tower of height m over $P = Q_1$. Map $R\mathcal{J}^m_{A,C} \to \mathcal{K}$ by sending $P_i \to Q_i$. Compose with a map $R\mathcal{J}^{p^e-1}_{A,C} \to R\mathcal{J}^m_{A,C}$ sending P_1 to P_1 .

We do not know if this result is a special circumstance due to the associativity and/or commutativity. Corollary 2 is the best result we could have expected, since any algebraic means of pulling towers up to powers of primes from below would, by dualizing, make truncated polynomial Hopf algebras impossible. These are well-known to exist.

Let $Z\mathcal{K} = \{x_1, x_2, \ldots, x_5 \; ; \; x_i x_j = \binom{i+j}{i} x_{i+j}, \; i+j=1,2,3,4,5$

$x_i \longrightarrow \sum_{i=j+k} x_j \otimes x_k\}$ be the divided power graded Z-algebra of height 5 over a primitive x_1 , in degree 2 . The tower $\{x_1, x_2, x_3, x_4, x_5\}$ may be extended by $x_1x_5 + x_2x_4 - x_3x_3$, as may be proved by tedious, but

straightforward calculation.

$\mathcal{K}_Z$ is the quotient of ${}_Z\mathcal{I}^5_{A,C}$ obtained by setting $iP_i - K_i = 0\big|_{i=1,\ldots,5}$. It is readily seen that there can be no primitives of degree 4, 6, 8, or 10, since x_2, x_3, x_4, and x_5 are actually module generators in their degrees. On the other hand, in degree 12, there is the primitive attached to this extended tower — $6(x_1x_5 + x_2x_4 - x_3x_3) - x_1x_5 = 5x_1x_5 + 6x_2x_4 - 6x_3x_3$, but there can be no primitive in ${}_Z\mathcal{I}^5_{A,C}$ in the corresponding degree, as we have observed above.

CHAPTER VII

OBSTRUCTIONS TO COMMUTATIVITY AND ASSOCIATIVITY

Let $\mathcal{H}$ be a Hopf algebra satisfying the hypotheses of Borel's theorem (Chapter I). We shall measure the deviation of the algebra structure of $\mathcal{H}$ from commutativity and associativity by the non-vanishing of families of primitives. This provides a meticulous extension (in even dimensional cocommutative coassociative cases) of the result that, in Hopf algebras over fields of characteristic zero, commutativity and associativity follow from indecomposability of primitives. (See Milnor and Moore [1], Theorem 4.17.)

In the notation of Chapter I, we shall "compute" $P_{A,I}\, P_{B,J} - P_{B,J}\, P_{A,I}$ and $(P_{A,I}\, P_{B,J})P_{C,K} - P_{A,I}(P_{B,J}\, P_{C,K})$, where $P_{A,I}$, $P_{B,J}$ and $P_{C,K}$ are elements of the basis for $\mathcal{H}$ provided by Borel's theorem. We shall identify certain elements as primitives in the discussion below, and we shall require that they support infinite towers. This can be ensured in the following way: If

$$P = \sum_{\gamma \in \mathcal{A}} C_\gamma P_{\gamma,1} \in P(\mathcal{H}) ,$$

let

$$P_n \equiv \sum_{\substack{\gamma_1 < \gamma_2 < \ldots < \gamma_k \\ i_1+i_2+\ldots+i_k=n}} C_{\gamma_1}^{i_1} C_{\gamma_2}^{i_2} \ldots C_{\gamma_k}^{i_k} (\ldots (P_{\gamma_1,i_1}, P_{\gamma_2,i_2}) \ldots P_{\gamma_k,i_k}) .$$

Then $\{P_n\}_{n \in Z^+}$ is an infinite tower over $P_1 \equiv P$.

Let us order $Z^+ \times Z^+$ by $(x,y) < (x',y')$ if $x+y \leq x'+y'$ and $x < x'$ if $x+y = x'+y'$. Let α and $\beta \in A$. Suppose that there

are primitives $p(P_{\alpha,g},P_{\beta,h})$ defined for $(0,0) \le (g,h) < (i,j)$ satisfying:

$$p(P_{\alpha,g},P_{\beta,h}) = \sum_{(0,0)\le(g_0,h_0)<(g,h)} P_{\alpha,g_0}\, P_{\beta,h_0} \sum_{k=1}^{\infty} \sum_{\substack{\Sigma g_r n_r = g-g_0 \\ \Sigma h_r n_r = h-h_0 \\ (g_1,h_1)<\ldots<(g_k,h_k)}} \prod_{r=1}^{k} (-1)^{n_r} p(P_{\alpha,g_r},P_{\beta,h_r})^{n_r} + (P_{\alpha,g}\, P_{\beta,h} - P_{\beta,h}\, P_{\alpha,g}) \,. \tag{VII.1}$$

(all multiplications are carried out from left to right.)

In particular, $p(P_{\alpha,1},P_{\beta,1}) = P_{\alpha,1}\, P_{\beta,1} - P_{\beta,1}\, P_{\alpha,1}$ and

$$0 = p(P_{\alpha,0},P_{\beta,1}) = p(P_{\alpha,1},P_{\beta,0}) = p(P_{\alpha,0},P_{\beta,0}) \,.$$

We define $p(P_{\alpha,i},P_{\beta,j})$ by (VII.1) and show that it is primitive, by the equivalent computation

$$(I-\eta\epsilon)^{\otimes 2}\circ\Delta\Big\{ \sum_{(0,0)\le(i_0,j_0)<(i,j)} P_{\alpha,i_0}\, P_{\beta,j_0} \sum_{k=1}^{\infty} \sum_{\substack{\Sigma i_r n_r = i-i_0 \\ \Sigma j_r n_r = j-j_0 \\ (i_1,j_1)<\ldots<(i_k,j_k)}} \prod_{r=1}^{k} (-1)^{n_r} p(P_{\alpha,i_r},P_{\beta,j_r})^{n_r} \Big\}$$
$$= (I-\eta\epsilon)^{\otimes 2}\circ\Delta\Big\{P_{\beta,j}\, P_{\alpha,i} - P_{\alpha,i}\, P_{\beta,j}\Big\} \,. \tag{VII.2}$$

Apply Δ to $P_{\alpha,i_0}\, P_{\beta,j_0}\, \pi$

$$\equiv P_{\alpha,i_0}\, P_{\beta,j_0}\, p(P_{\alpha,i_1},P_{\beta,j_1})^{n_1} \ldots p(P_{\alpha,i_k},P_{\beta,j_k})^{n_k} \,.$$

(Because $\mathbin{\%}$ is not necessarily associative, this does <u>not</u> define π, but only the abbreviation $P_{\alpha,i_0}\, P_{\beta,j_0}\, \pi$, as multiplication is carried out from the left.)

The image is spanned by tensors of the following types.

i) $P_{\alpha,i_0} P_{\beta,j_0} \pi \otimes 1$ and $1 \otimes P_{\alpha,i_0} P_{\beta,j_0} \pi$, which vanish upon the application of $(I-\eta\epsilon)^{\otimes 2}$.

ii) $P_{\alpha,i_0'} P_{\beta,j_0'} \otimes P_{\alpha,i_0''} P_{\beta,j_0''} p(P_{\alpha,i_1},P_{\beta,j_1})^{n_1} \ldots p(P_{\alpha,i_k},P_{\beta,j_k})^{n_k}$ with i_0' or $j_0' \neq 0$, denoted $P_{\alpha,i_0'} P_{\beta,j_0'} \otimes P_{\alpha,i_0''} P_{\beta,j_0''} \pi$, and analogously, $P_{\alpha,i_0'} P_{\beta,j_0'} \pi \otimes P_{\alpha,i_0''} P_{\beta,j_0''}$ with i_0'' or $j_0'' \neq 0$, where in each case $i_0' + i_0'' = i_0$ and $j_0' + j_0'' = j_0$. These are fixed under $(I-\eta\epsilon)^{\otimes 2}$.

iii) $P_{\alpha,i_0'} P_{\beta,j_0'} p(P_{\alpha,i_1},P_{\beta,j_1})^{n_1'} \ldots p(P_{\alpha,i_k},P_{\beta,j_k})^{n_k'} \otimes P_{\alpha,i_0''} P_{\beta,j_0''} p(P_{\alpha,i_1},P_{\beta,j_1})^{n_1''} \ldots p(P_{\alpha,i_k},P_{\beta,j_k})^{n_k''}$ with $i_0' + i_0'' = i_0$, $j_0' + j_0'' = j_0$, $n_t' + n_t'' = n_t$ for $t \in \{1,2,\ldots,k\}$, $n_r' \neq 0$ and $n_s'' \neq 0$ for some r and $s \in \{1,2,\ldots,k\}$. We abbreviate by $P_{\alpha,i_0'} P_{\beta,j_0'} \otimes P_{\alpha,i_0''} P_{\beta,j_0''} \pi''$. These are fixed under $(I-\eta\epsilon)^{\otimes 2}$.

With $P_{\alpha,i_0} P_{\beta,j_0} \pi$ as above, we define $\#(\pi)$ to be $n_1+n_2+\ldots+n_k$, $\omega_\alpha(\pi)$ to be $\sum_{s=1}^{k} i_s n_s$, and $\omega_\beta(\pi)$ to be $\sum_{t=1}^{k} j_t n_t$.

As a direct consequence of the definitions of $p(P_{\alpha,g},P_{\beta,h})$, $(g,h) < (i,j)$ and manipulation of indices,

$$(I-\eta\epsilon)^{\otimes 2}\circ\Delta \sum_{(0,0)\leq(i_0,j_0)<(i,j)} \sum_{\substack{\omega_\alpha(\pi)=i-i_0 \\ \omega_\beta(\pi)=j-j_0}} (-1)^{\#(\pi)} P_{\alpha,i_0} P_{\beta,j_0} \pi$$

are primitives $p(P_{\alpha,g},P_{\varepsilon,h})$ defined for $(0,0) \le (g,h) < (i,j)$ satisfying:

$$p(P_{\alpha,g},P_{\varepsilon,h}) = \sum_{(0,0)\le(g_0,h_0)\le(g,h)} P_{\alpha,g_0} P_{\varepsilon,h_0} \sum_{k=1}^{\infty} \sum_{\substack{\Sigma g_r n_r = g-g_0 \\ \Sigma h_r n_r = h-h_0 \\ (g_1,h_1)<\ldots<(g_k,h_k)}} \prod_{r=1}^{k} (-1)^{n_r} p(P_{\alpha,g_r},P_{\beta,h_r})^{n_r} + (P_{\alpha,g} P_{\varepsilon,h} - P_{\varepsilon,h} P_{\alpha,g}) . \qquad \text{(VII.1)}$$

(all multiplications are carried out from left to right.)

In particular, $p(P_{\alpha,1},P_{\beta,1}) = P_{\alpha,1} P_{\beta,1} - P_{\beta,1} P_{\alpha,1}$ and

$$0 = p(P_{\alpha,0},P_{\varepsilon,1}) = p(P_{\alpha,1},P_{\beta,0}) = p(P_{\alpha,0},P_{\beta,0}) .$$

We define $p(P_{\alpha,1},P_{\varepsilon,j})$ by (VII.1) and show that it is primitive, by the equivalent computation

$$(I-\eta\epsilon)^{\mathfrak{A}} \Big\{ \sum_{(0,0)\le(i_0,j_0)\le(i,j)} P_{\alpha,i_0} P_{\beta,j_0} \sum_{k=1}^{\infty} \sum_{\substack{\Sigma i_r n_r = i-i_0 \\ \Sigma j_r n_r = j-j_0 \\ (i_1,j_1)<\ldots<(i_k,j_k)}} \prod_{r=1}^{k} (-1)^{n_r} p(P_{\alpha,i_r},P_{\varepsilon,j_r})^{n_r} \Big\} \qquad \text{(VII.2)}$$

$$= (I-\eta\epsilon)^{\mathfrak{A}^2} \Big\{ P_{\varepsilon,j} P_{\alpha,i} - P_{\alpha,i} P_{\beta,j} \Big\} .$$

Apply $\mathfrak{A}$ to $P_{\alpha,i_0} P_{\varepsilon,j_0}$

$$= P_{\alpha,i_0} P_{\varepsilon,j_0} p(P_{\alpha,i_1},P_{\beta,j_1})^{n_1} \ldots p(P_{\alpha,i_k},P_{\beta,j_k})^{n_k} .$$

(Because $\mathfrak{A}$ is not necessarily associative, this does <u>not</u> define π, but only the abbreviation $P_{\alpha,i_0} P_{\varepsilon,j_0} \pi$, as multiplication is carried out from the left.)

$$= 0 \qquad \text{(adding tensors of type i)).}$$

$$+ \sum_{\substack{i'+i''=i \\ j'+j''=j \\ i'j'\neq 0 \\ i''j''\neq 0}} \{P_{\alpha,i'} P_{\beta,j'} \otimes -(P_{\alpha,i''} P_{\beta,j''} - P_{\beta,j''} P_{\alpha,i''})$$

$$+ -(P_{\alpha,i'} P_{\beta,j'} - P_{\beta,j'} P_{\alpha,i'}) \otimes P_{\alpha,i''} P_{\beta,j''}\}$$

(adding tensors of type ii))

$$+ \sum_{\substack{i'+i''=i \\ j'+j''=j \\ i'j'\neq 0 \\ i''j''\neq 0}} - (P_{\alpha,i'} P_{\beta,i'} - P_{\beta,j'} P_{\alpha,i'}) \otimes -(P_{\alpha,i''} P_{\beta,j''} - P_{\beta,j''} P_{\alpha,i''})$$

(adding tensors of type iii)).

$$= \sum_{\substack{i'+i''=i \\ j'+j''=j \\ i'j'\neq 0 \\ i''j''\neq 0}} - (P_{\alpha,i'} P_{\beta,j'} \otimes P_{\alpha,i''} P_{\beta,j''}) + (P_{\beta,j'} P_{\alpha,i'} \otimes P_{\beta,j''} P_{\alpha,i''})$$

which is clearly equal to $(I-\eta\epsilon)^{\otimes 2}\, \Delta(P_{\beta,j} P_{\alpha,i} - P_{\alpha,i} P_{\beta,j})$. This completes the argument for (VII.2). (See the computation on page 9 for the case $i=1, j$ arbitrary.)

We have unnecessarily restricted ourselves in the preceding computations for such clarity as this restriction affords. Let us consider now

$$(P_{\alpha_i,i_1} \ldots P_{\alpha_k,i_k})(P_{\beta_1,j_1} \ldots P_{\beta_\ell,j_\ell}) - (P_{\beta_1,j_1} \ldots P_{\beta_\ell,j_\ell})(P_{\alpha_1,i_1} \ldots P_{\alpha_k,i_k})$$

$= P_{A,I} P_{B,J} - P_{B,J} P_{A,I}$. In the interesting cases, of course, $\alpha_1 < \alpha_2 < \ldots < \alpha_k$ and $\beta_1 < \beta_2 < \ldots < \beta_\ell$. (Within parentheses, multiplication proceeds from the left.) We order $(Z^+)^{\times(k+\ell)}$ by the obvious analogue of the ordering on $Z^+ \times Z^+$ described above. We may then inductively define

$$p(P_{A,I},P_{B,J}) \equiv \sum_{(0,0)\le(I_0,J_0)<(I,J)} P_{A,I_0}\, P_{B,J_0}$$

$$\cdot \sum_{k=1}^{\infty} \sum_{\substack{\Sigma I_r n_r = I-I_0 \\ \Sigma J_r n_r = J-J_0}} \prod_{r=1}^{k} (-1)^{n_r}\, p(P_{A,I_r},P_{B,J_r})^{n_r} \qquad \text{(VII.3)}$$

$$+ (P_{A,I}\, P_{B,J} - P_{B,J}\, P_{A,I}) .$$

The proof that $p(P_{A,I},P_{B,J})$ is primitive is exactly parallel to the proof that $p(P_{\alpha,i},P_{\beta,j})$ is primitive.

Oddly enough, the scheme above is general enough to encompass the differences related to lack of associativity as well. For we may define

$$p(P_{A,I},P_{B,J},P_{C,K})$$

$$\equiv \sum_{(0,0,0)\le(I_0,J_0,K_0)<(I,J,K)} P_{A,I_0}\, P_{B,J_0}\, P_{C,K_0} \sum_{k=1}^{\infty} \sum_{\substack{\Sigma I_r n_r = I-I_0 \\ \Sigma J_r n_r = J-J_0 \\ \Sigma K_r n_r = K-K_0}} \prod_{r=1}^{k}$$

$$(-1)^{n_r}\, p(P_{A,I_r},P_{B,J_r},P_{C,K_r})^{n_r} \qquad \text{(VII.4)}$$

$$+ (P_{A,I}\, P_{B,J})\, P_{C,K} - P_{A,I}\, (P_{B,J}\, P_{C,K}) .$$

The proof that $p(P_{A,I},P_{B,J},P_{C,K})$ is primitive is exactly as above. The induction starts with $(P_{\alpha,1}\, P_{\beta,1})P_{\gamma,1} - P_{\alpha,1}(P_{\beta,1}\, P_{\gamma,1})$, which is clearly primitive.

We have concentrated on defining primitives in (VII.3) and (VII.4), but by an obvious inversion, these equations exhibit $(P_{A,I}P_{B,J} - P_{B,J}P_{A,I})$ and $(P_{A,I}\, P_{B,J})P_{C,K} - P_{A,I}(P_{B,J}\, P_{C,K})$ as elements in the ideal generated by towers over these primitives. An easy induction argument

will show now that, if the primitives of $\mathcal{N}$ are indecomposable, these differences are zero. It follows immediately that $\mathcal{N}$ is commutative and associative. We shall address ourselves to the converse in the next chapter.

CHAPTER VIII

A STANDARD ALGEBRA PRESENTATION FOR HOPF ALGEBRAS WITH POLYNOMIAL DUAL COALGEBRA STRUCTURE

Let $\mathcal{H}$ be an associative Hopf algebra satisfying the hypotheses of Borel's theorem. We may describe the algebra structure of $\mathcal{H}$ as follows if the ground ring has characteristic zero: $\mathcal{H} \underset{\text{algebra}}{\cong}$

$$\left\{P_{\alpha,i}, K_{\beta,j}, p(P_{\gamma,k}, P_{\delta,\ell})_m \Big|_{\substack{\alpha,\beta,\gamma<\delta \in \mathcal{A} \\ j,k,\ell,m \in Z^+-\{0\}}} : P_{\alpha,0} = 1 \ \forall\, \alpha \in \mathcal{A} \right.$$

$$iP_{\alpha,i} - K_{\alpha,i} = \sum_{\nu \in \mathcal{A}} C^{\nu}_{\alpha,i}\, P_{\nu,1} \quad \forall\, \alpha \in \mathcal{A},\ \forall\, i \in Z^+-\{0\}\ .$$

$$p(P_{\gamma,k}, P_{\delta,\ell})_1 = \sum_{\nu \in \mathcal{A}} C^{\nu}_{\gamma,k;\delta,\ell}\, P_{\nu,1} \quad \forall\, \gamma<\delta \in \mathcal{A},\ \forall\, k,\ell \in Z^+-\{0\}$$

$$p(P_{\gamma,k}, P_{\delta,\ell})_m = \sum_{s=1}^{\infty} \sum_{\substack{\nu_1<\nu_2<\ldots<\nu_s \\ i_1+i_2+\ldots+i_s=m}} \prod_{r=1}^{s} \left(C^{\nu_r}_{\gamma,k;\delta,\ell}\right)^{i_r} \qquad \text{(VIII.1)}$$

$$P_{\nu_1,i_1} \ldots P_{\nu_s,i_s} \quad \forall\, \gamma<\delta \in \mathcal{A},\ \forall\, k,\ell,m \in Z^+-\{0\}$$

$$K_{\beta,j} = \sum_{k+\ell=j} P_{\beta,k}(\ell P_{\beta,\ell} - K_{\beta,\ell}) \quad \begin{matrix} \forall\, \beta \in \mathcal{A} \\ \forall\quad j \in Z^+-\{0,1\} \end{matrix} \qquad K_{\beta,1} = 0 \quad \forall\, \beta \in \mathcal{A}$$

$$p(P_{\gamma,k}, P_{\delta,\ell})_1 = \sum_{(0,0)\le(k_0,\ell_0)<(k,\ell)} P_{\gamma,k_0}\, P_{\delta,\ell_0}\ .$$

$$\sum_{s=1}^{\infty} \sum_{\substack{\Sigma k_r n_r = k-k_0 \\ \Sigma \ell_r n_r = \ell-\ell_0}} \prod_{r=1}^{s} (-1)^{n_r}\, p(P_{\gamma,k_r}, P_{\delta,\ell_r})_{n_r}$$

$$\left. + P_{\gamma,k}\, P_{\delta,\ell} - P_{\delta,\ell}\, P_{\gamma,k} \quad \begin{matrix} \forall\, \gamma<\delta \in \mathcal{A} \\ \forall\, k,\ell \in Z^+-\{0\} \end{matrix} \right\} /Z\text{-Torsion}$$

If $\mathcal{K}$ is commutative, as well as associative, the "structure constants" $C^{\nu}_{\gamma,k;\delta,\ell}$ are clearly zero, and we may simplify to: $\mathcal{K} \cong$ algebra

$$R\Big[\Big\{P_{\alpha,i}, K_{\beta,j} \Big|_{\substack{\alpha,\beta \in \mathcal{A} \\ i,j \in Z^+-\{0\}}}\Big\}\Big] /$$

$$\Big\{ iP_{\alpha,i} - K_{\alpha,i} = \sum_{\nu \in \mathcal{A}} C^{\nu}_{\alpha,i}\, P_{\nu,1} \quad \forall\, \alpha \in \mathcal{A},\ \forall\, i \in Z^+-\{0\}, \tag{VIII.2}$$

$$K_{\beta,1} = 0 \quad \forall\, \beta \in \mathcal{A}, \text{ and } \forall\, \beta \in \mathcal{A},\ \forall\, j \in Z^+-\{0\}$$

$$K_{\beta,j} = \sum_{k+\ell=j} P_{\beta,k}(\ell P_{\beta,\ell} - K_{\beta,\ell})\Big\} \text{ /Z-Torsion.}$$

Before verifying (VIII.1), let us show that if $\mathcal{K}$ is commutative and associative, and satisfies the hypotheses of Borel's theorem, the primitives of $\mathcal{K}$ are indecomposable in the characteristic zero cases.

Proof: Suppose $P = \Sigma\, C_\lambda\, P_{\lambda,1}$ is a decomposable primitive of $\mathcal{K}$. Using the basis provided by Borel's theorem, this clearly means

$$0 = \Sigma\, C_\lambda\, P_{\lambda,1} - \Sigma\, C_J\, P_{A_{j_1},I_{j_1}}\, P_{A_{j_2},I_{j_2}} \cdots P_{A_{j_k},I_{j_k}}$$

where $C_J = 0$ if fewer than two I_j's are non-zero.

By (VIII.2), there is an integer n such that

$$n\Big(\Sigma\, C_\lambda\, P_{\lambda,1} - \Sigma\, C_J\, P_{A_{j_1},I_{j_1}}\, P_{A_{j_2},I_{j_2}} \cdots P_{A_{j_k},I_{j_k}}\Big)$$

$$= \Sigma\, R_{\alpha,i}(iP_{\alpha,i} - K_{\alpha,i} - \Sigma\, C^{\nu}_{\alpha,i}\, P_{\gamma,1})$$

$$+ \Sigma\, S_{\beta,j}(K_{\beta,j} - \Sigma\, P_{\beta,k}(\ell P_{\beta,\ell} - K_{\beta,\ell}))$$

$$+ \Sigma\, T_\beta\,(K_{\beta,1})$$

in the polynomial algebra generated by the K's and P's, where the R's, S's, and T's are elements of that polynomial algebra.

If $i \neq 1$, clearly $R_{\alpha,i} = 0$, as $R_{\alpha,i}$ is the coefficient of $P_{\alpha,i}$ on the right hand side, and zero is on the left. It follows immediately that $C_\lambda = 0 \quad \forall\, \lambda \in \mathcal{A}$, as the coefficient of $P_{\lambda,1}$ on the left hand side is C_λ, and on the right hand side is zero, in the absence of R's.

We return now to the proof of (VIII.1). We write $R \equiv S$ if $R - S$ belongs to the two-sided ideal in $\overline{\mathcal{N}} = \left\{P_{\alpha,i}\, K_{\beta,j}, p(P_{\gamma,k}, P_{\delta,\ell})_m\right\}_{\substack{\alpha,\beta,\gamma<\delta \in \mathcal{A} \\ i,j,k,\ell,m \in Z^+-\{0\}}}$ generated by the relations of (VIII.1). We shall be careless about indexing summation and product signs, but one can refer to (VIII.1) for instructions. We use the term "basis element" to describe those elements in $\overline{\mathcal{N}}$ depicting canonical basis elements in $\mathcal{N}$.

Consider $P_{\delta,\ell}\, P_{\gamma,k} \in \overline{\mathcal{N}}$, where $\gamma<\delta \in \mathcal{A}$. This is not a basis element. Let us attempt to write it as a linear combination of basis elements, up to the congruence, $\equiv$. By (VII.1), the primitivity of $p(\ ,\ )$, and the canonical method of constructing towers in $\mathcal{N}$ described in Chapter VII, we would compute as follows if we were in $\mathcal{N}$. Since we are in $\overline{\mathcal{N}}$, we must write $\equiv$ rather than $=$.

$$\begin{aligned} P_{\delta,\ell}\, P_{\gamma,k} &= P_{\gamma,k}\, P_{\delta,\ell} + \{P_{\delta,\ell}\, P_{\gamma,k} - P_{\gamma,k}\, P_{\delta,\ell}\} \\ &\equiv P_{\gamma,k}\, P_{\delta,\ell} - p(P_{\gamma,k}, P_{\delta,\ell}) + \\ &\qquad \Sigma\, P_{\gamma,k_0}\, P_{\delta,\ell_0} \Sigma\, \pi^{\pm}\, p(P_{\gamma,k_r}, P_{\delta,\ell_r})_{n_r} \qquad \text{(VIII.3)} \\ &\equiv P_{\gamma,k}\, P_{\delta,\ell} - \Sigma\, C^{\nu}_{\gamma,k;\delta,\ell}\, P_{\nu,1} \end{aligned}$$

$$+ \Sigma P_{\gamma,k_0} P_{\delta,\ell_0} \sum_r \pi$$

$$\pm \left\{ \sum_{i_1+i_2+\dots+i_s=n_r} \prod_{t=1}^{s} \left(C_{\gamma,k_r;\delta,\ell_r}\right)^{r^{\nu_t}} {}^{i_t} P_{r^{\nu_1},i_1} \cdots P_{r^{\nu_s},i_s} \right\} .$$

How far have we succeeded? $P_{\gamma,k} P_{\delta,\ell}$ and $P_{\nu,1}$ are basis elements. The other summands may involve products of tower elements which are "out of order" - e.g., it might be that ${}_{r+1}\nu_1 < {}_r\nu_s$ for some allowable choice of ${}_rN = \{{}_r\nu_1 < \dots < {}_r\nu_s\}$ and ${}_{r+1}N = \{{}_{r+1}\nu_1 < \dots < {}_{r+1}\nu_{s'}\} \subseteq \mathcal{Q}$. However, it is easily seen that the height of such a pair of tower elements is less than $k+\ell$. We merely observe that (i) $k = k_0 + \sum_r n_r k_r$ and $\ell = \Sigma \ell_0 + \Sigma n_r \ell_r$, with k_r and ℓ_r strictly positive, and (ii) the sum of the heights of the factors of the summands of (VIII.2) we are concerned with is $k_0 + \ell_0 + \sum_r n_r < k+\ell$. An induction procedure is now available for the following:

<u>Theorem 1</u>. Let $\{P_{A_j,I_j}\}_{j=1,2,\dots,t}$ be basis elements of $\bar{\mathcal{N}}$. Then

$$P_{A_1,I_1} P_{A_2,I_2} \cdots P_{A_s,I_s} \equiv \sum_{\beta_1 \le \beta_2 \le \dots \le \beta_k} C_{B,J} P_{\beta_1,j_1} P_{\beta_2,j_2} \cdots P_{\beta_k,j_k} .$$

Furthermore, the sum of the heights on the left is greater than the sum of the heights in any non-zero summand on the right, unless $\{\beta_1,\beta_2,\dots,\beta_k\} = A_1 \cup A_2 \cup \dots \cup A_s$, in which case they are equal.

N.B. We do <u>not</u> have basis elements on the right, because the inequalities relating β's are not strict.

<u>Proof:</u> We induct on the maximal sum of the heights of two adjacent, out of order, tower elements. The induction begins with the special case:

$$P_{\delta,1}\,P_{\gamma,1} = P_{\gamma,1}\,P_{\delta,1} + \{P_{\delta,1}\,P_{\gamma,1} - P_{\gamma,1}\,P_{\delta,1}\}$$

$$= P_{\gamma,1}\,P_{\delta,1} + \left\{(P_{\delta,1}\,P_{\gamma,1} - P_{\gamma,1}\,P_{\delta,1}) + p(P_{\gamma,1}\,P_{\delta,1})\right\}$$

$$- \left\{p(P_{\gamma,1}\,P_{\delta,1}) - \sum_{\nu} C^{\nu}_{\gamma,1;\delta,1}\,P_{\nu,1}\right\} \qquad \text{(VIII.3')}$$

$$- \sum_{\nu} C^{\nu}_{\gamma,1;\delta,1}\,P_{\nu,1} \equiv P_{\gamma,1}\,P_{\delta,1} - \sum C^{\nu}_{\gamma,1;\delta,1}\,P_{\nu,1}\,.$$

We refer to (VIII.3) and the discussion following to complete the argument. We may concern ourselves with one adjacent pair of tower elements at a time because the congruence is with respect to a two-sided ideal.

We must now consider computing products of type $P_{\beta,i}\,P_{\beta,j}$ up to congruence. Nothing occurs to us. However, $jP_{\beta,i}\,P_{\beta,j}$ <u>is</u> "computable", for:

$$jP_{\beta,i}\,P_{\beta,j} = P_{\beta,i}(jP_{\beta,j} - K_{\beta,j}) + P_{\beta,i}\,K_{\beta,j}$$

$$= P_{\beta,i}\left\{jP_{\beta,j} - K_{\beta,j} - \sum_{\nu} C^{\nu}_{\beta,j}\,P_{\nu,1}\right\} + \qquad \text{(VIII.4)}$$

$$\sum C^{\nu}_{\beta,j}\,P_{\beta,i}\,P_{\nu,1} + P_{\beta,i}\left\{K_{\beta,j} - \sum_{j=k+\ell} P_{\beta,k}(\ell P_{\beta,\ell} - K_{\beta,\ell})\right\}$$

$$+ \sum_{j+k=\ell} P_{\beta,i}\,P_{\beta,k}\left\{(\ell P_{\beta,\ell} - K_{\beta,\ell}) - \sum C^{\nu}_{\beta,\ell}\,P_{\nu,1}\right\}$$

$$+ \sum_{j=k+\ell} \sum_{\nu} C^{\nu}_{\beta,\ell}\,P_{\beta,i}\,P_{\beta,k}\,P_{\nu,1}$$

$$\equiv \sum_{\nu} C^{\nu}_{\beta,j}\,P_{\beta,i}\,P_{\nu,1} + \sum_{j=k+\ell} \sum_{\nu} C^{\nu}_{\beta,\ell}\,P_{\beta,i}\,P_{\beta,k}\,P_{\nu,1}\,.$$

We iterate, multiplying both sides of the congruence by k to reduce $C^{\nu}_{\beta,\ell}\,P_{\beta,i}\,P_{\beta,k}\,P_{\nu,1}$ to sums of type $\Sigma\, C^{\nu}_{\beta,\ell}\,C^{\mu}_{\beta,k}\,P_{\beta,i}\,P_{\mu,1}\,P_{\nu,1}$ and

$\Sigma\, C^{\nu}_{\beta,\ell}\, C^{\mu}_{\beta,\ell'}\, P_{\beta,i}\, P_{\beta,k'}\, P_{\mu,1}\, P_{\nu,1}$ with $k < k'$, $k'+\ell' = k$. "Primitives" will pile up on the right - some may be $P_{\beta,1}$, as ν or $\mu = \beta$ in the above formulas is allowed in the filtered (but not graded) case.

Let us reexamine our procedure when $j = 1$. Since $K_{\beta,1} \equiv 0$, the procedure is vacuous. However,

$$
\begin{aligned}
P_{\beta,i}\, P_{\beta,1} &= P_{\beta,i}(P_{\beta,1} - K_{\beta,1}) + P_{\beta,i}(K_{\beta,1} - 0) \\
&\equiv \Big\{P_{\beta,i}(P_{\beta,1} - K_{\beta,1}) + \sum_{\substack{k+\ell=i+1 \\ k\neq i}} P_{\beta,k}(\ell P_{\beta,\ell} - K_{\beta,\ell}) - K_{\beta,i}\Big\} \\
&\quad + \Big(K_{\beta,i+1} - (i+1)P_{\beta,i+1}\Big) + (i+1)P_{\beta,i+1} \\
&\quad - \sum_{\substack{k+\ell=i+1 \\ k\neq i}} P_{\beta,k}\Big\{(\ell P_{\beta,\ell} - K_{\beta,\ell}) - \sum_{\nu} C^{\nu}_{\beta,\ell}\, P_{\nu,1}\Big\} \\
&\quad - \sum_{\substack{k+\ell=i+1 \\ k\neq i}} C^{\nu}_{\beta,\ell}\, P_{\beta,k}\, P_{\nu,1} \qquad \text{(VIII.5)} \\
&\equiv -\sum C^{\nu}_{\beta,i+1}\, P_{\nu,1} + (i+1)P_{\beta,i+1} \\
&\quad - \sum_{\substack{k+\ell=i+1 \\ k\neq i}} C^{\nu}_{\beta,\ell}\, P_{\beta,k}\, P_{\nu,1}\,.
\end{aligned}
$$

Combining (VIII.4) and (VIII.5), we find:

<u>Theorem 2.</u> $j!\, P_{\beta,i}\, P_{\beta,j} \equiv$ a linear combination of basis elements

$$
+ \sum_{\substack{r,N \\ s+r=i+j \\ \nu_1\neq\beta}} C_{r,N}\, P_{\beta,r}\, P_{\nu_1,1}\, P_{\nu_2,1} \cdots P_{\nu_s,1}\,.
$$

We are now in a position to apply Theorem 1 to the right hand side. It is clear from the statement of Theorem 1 that we cannot

encounter any adjacent factors in a summand of the right hand side which come from the same tower and the sum of whose heights is greater than or equal to $i+j$.

Successive applications of Theorem 1 and Theorem 2 leave us with

Theorem 3. Let $\{P_{A_j,I_j}\}_{j=1,\ldots,t}$ be basis elements of $\bar{\mathcal{A}}$. There is an integer n such that

$$n\, P_{A_1,I_1} P_{A_2,I_2} \cdots P_{A_s,I_s}$$

$$\equiv \sum_{\beta_1<\beta_2<\ldots<\beta_k} C_{B,J}\, P_{\beta_1,j_1} \cdots P_{\beta_k,j_k} .$$

Suppose now that $R = \Sigma\, C_J\, P_{A_{j_1},I_{j_1}} \cdots P_{A_{j_s},I_{j_s}} = 0$ is a relation in $\mathcal{A}$ (clearly every relation in $\mathcal{A}$ can be written this way). Choose $N \in Z$ large enough to apply Theorem 3 to each non-zero summand of the relation multiplied by N . Theorem 3 implies that NR is a linear combination of elements in the ideal generated by relations of (VIII.1) + a linear combination of basis elements. The latter must be trivial. Since $\mathcal{A}$ is Z-torsion free, the presentation (VIII.1) follows.

CHAPTER IX

SOME UNIVERSAL CONSTRUCTIONS

§0. Introduction.

In this section, all modules, algebras, coalgebras, and Hopf algebras are filtered or graded by the positive integers, and connected (a module is connected if its 0 filtrand or submodule of degree 0 is 0). The symbol I will be used throughout for identity maps. The ground ring R is commutative with unit.

We shall, for each algebra A , construct Hopf algebras T(A) and S(A) with the following properties:

(i) T(A) is a coassociative Hopf algebra, associative if A is, commutative if A is.

S(A) is a coassociative, cocommutative Hopf algebra, associative if A is, commutative if A is.

(ii) T(A) is provided with an algebra map into A, $p:T(A) \to A$, with the following property: if $F:H \to A$ is an algebra map, H is a coassociative Hopf algebra, then there is a unique Hopf algebra map $f^*:H \to T(A)$ such that $pf^* = f$.

S(A) is provided with an algebra map into A, $p:S(A) \to A$, with the following property: if $f:H \to A$ is an algebra map, H is a coassociative, cocommutative Hopf algebra, then there is a unique Hopf algebra map $f^*:H \to S(A)$ such that $pf^* = f$.

(iii) T is a functor from the category of algebras to the category of coassociative Hopf algebras. p is a natural transformation from UT to the Identity, where U is the forgetful functor

from coassociative Hopf algebras to algebras.

S is a functor from the category of algebras to the category of coassociative cocommutative Hopf algebras. p is a natural transformation from US to the Identity, where U is the forgetful functor from the category oı coassociative cocommutative Hopf algebras to the category of algebras. (i.e. T and S are adjoints to appropriate forgetful functors.)

In slightly weaker form, these constructions may be found in Moore [9]. The version we give closely follows, except in Section 4, the directions of Husemoller [10], (which omits proofs). Husemoller promises details in Husemoller and Moore [11]. As this is unavailable, and we must provide the groundwork for computational use of the construction, we proceed.

1. An intermediary.

Let N be an R-module, not necessarily connected. $T_n(N)$ is the R-module $N \otimes N \otimes N \ldots \otimes N$ (n factors, $\otimes$ means tensor product over R). We adopt the conventions that $T_0(N)$ is R and $T_1(N)$ is N . T(N) is $\sum_{n\geq 0} T_n(N)$. T_i is said to be the i^{th} component of T , and $\iota_i : T_i(M) \to T(M)$ is the structure map.

Suppose M is a connected R module. It is clear that $T(M) \xrightarrow{p_k} \prod_{k\geq n\geq 0} T_n(M) \xleftarrow{\approx} \sum_{k\geq n\geq 0} T_n(M)$ is an isomorphism in filtrands or degrees $\leq k$, where p_k is given by component maps $\delta_{ij} : T_i(M) \to T_j(M)$, and the inverse is given by $\sum_{k\geq n\geq 0} T_n(M) \xrightarrow{\Sigma \iota_n} T(M)$. (We shall be irritatingly precise when using product and sum constructions, as it is the difference between these which makes the coalgebra construction

below impossible in the ungraded, unfiltered situations.)

We wish to make $T(M)$ a coalgebra. $1 \in R$ is to be a group-like element, i.e., $1 \xrightarrow{\Delta} 1 \otimes 1$. Let us suppose $\Delta: T(M) \to T(M) \otimes T(M)$ is defined for filtrands or degrees less than k. $\Delta|_{T(M)_k}$ is defined to be the following composition:

$$T(M)_k \xrightarrow{p_k} \Big(\prod_{k \geq n \geq 0} T_n(M)\Big)_k \xleftarrow{\approx} \Big(\sum_{k \geq n \geq 0} T_n(M)\Big)_k$$

$$\xrightarrow{\Sigma D_n} \Big(\sum_{k \geq n \geq 0} \prod_{i+j=n} T_i(M) \otimes T_j(M)\Big)_k \xleftarrow{\approx} \Big(\sum_{k \geq n \geq 0} \sum_{i+j=n} T_i(M) \otimes T_j(M)\Big)_k$$

$$\xrightarrow{E_k} \Big(\sum_{k \geq i \geq 0} T_i(M) \otimes \sum_{k \geq j \geq 0} T_j(M)\Big)_k \xrightarrow{\Sigma \tau_i \otimes \Sigma \tau_j} (T(M) \otimes T(M))_k ,$$

where D_n is defined via the natural isomorphisms $D_{i,j}: T_{i+j} \to T_i \otimes T_j$, and E_k by virtue of the natural commutativity of sums and tensor products. In the graded case, we are done. In the filtered case, we must check for coherence of definitions, but this is a trivial matter.

Let $m_1, m_2, \ldots, m_k$ be a finite sequence of elements of M. Let us identify $m_1 \otimes m_2 \otimes \ldots \otimes m_k$ with its image under $\tau_k: T_k \to T$. As can be readily seen from the definition above,

$$\begin{aligned}\Delta: m_1 \otimes m_2 \otimes \ldots \otimes m_k &\to (m_1 \otimes m_2 \otimes \ldots \otimes m_k) \otimes (1) \\ &+ (m_1 \otimes m_2 \otimes \ldots \otimes m_{k-1}) \otimes (m_k) + \ldots \\ &+ (m_1 \otimes \ldots \otimes m_i) \otimes (m_{i+1} \otimes \ldots \otimes m_k) + \ldots \\ &+ (1) \otimes (m_1 \otimes \ldots \otimes m_k) ,\end{aligned}$$

which we abbreviate

$$\sum_{i=0}^{k} (m_1 \otimes \ldots \otimes m_i) \otimes (m_{i+1} \otimes \ldots \otimes m_k) .$$

With this notation, we show that $(T(M), \Delta)$ is coassociative:

$$(I\otimes\Delta)\circ\Delta\colon m_1\otimes m_2\otimes\ldots\otimes m_k\to$$

$$(I\otimes\Delta)\sum_{i=0}^{k}(m_1\otimes\ldots\otimes m_i)\otimes(m_{i+1}\otimes\ldots\otimes m_k)$$

$$=\sum_{i=0}^{k}(m_1\otimes\ldots\otimes m_i)\otimes\Big(\sum_{j=0}^{k-1}(m_{i+1}\otimes\ldots\otimes m_{i+j})\otimes(m_{i+j+1}\otimes\ldots\otimes m_k)\Big)$$

$$=\sum_{i=0}^{k}\sum_{j=0}^{k-1}(m_1\otimes\ldots\otimes m_i)\otimes(m_{i+1}\otimes\ldots\otimes m_{i+j})\otimes(m_{i+j+1}\otimes\ldots\otimes m_k)\ .$$

On the other hand,

$$(\Delta\otimes I)\circ\Delta\colon m_1\otimes\ldots\otimes m_k\to$$

$$\sum_{s=0}^{k}\sum_{r=0}^{s}(m_1\otimes\ldots\otimes m_r)\otimes(m_{r+1}\otimes\ldots\otimes m_s)\otimes(m_{s+1}\otimes\ldots\otimes m_k)\ .$$

By an elementary change of summation variables, these are equal. Two maps out of a direct sum are equal if they are equal on generators of components, so we are done.

A diagrammatic argument for coassociativity can be built around the following commutative diagrams:

$$\begin{array}{ccc} T_{i+j+k} & \xrightarrow{\ D_{i,j+k}\ } & T_i\otimes T_{j+k} \\ {\scriptstyle D_{i+j,k}}\downarrow & & \downarrow{\scriptstyle I\otimes D_{j,k}} \\ T_{i+j}\otimes T_k & \xrightarrow{\ D_{i,j}\otimes I\ } & T_i\otimes T_j\otimes T_k \end{array}$$

Let $\epsilon\colon T(M)\to R$ be defined by $\delta_{i,0}\colon T_i\to T_0$. ϵ is split by $\iota_0\colon R\to T_0(M)$. It is clear that $(I\otimes\epsilon)\circ\Delta=(\epsilon\otimes I)\circ\Delta=I\colon T(M)\to T(M)$. This completes the argument that $(T(M),\Delta,\epsilon)$ is a coassociative coalgebra. Warning: The filtration or grading on $T(M)$ is that induced by the filtration or grading on M. However, the components,

or partial sums of components, can be used to artificially grade or filter $T(M)$, and we shall find use for this below.

$M = T_1(M)$ is precisely the primitive submodule of $T(M)$, $P(T(M))$. This is clear from the fact that $T_n \xrightarrow{D_n} \pi_{i+j=n} T_i \otimes T_j$ is a product of isomorphisms.

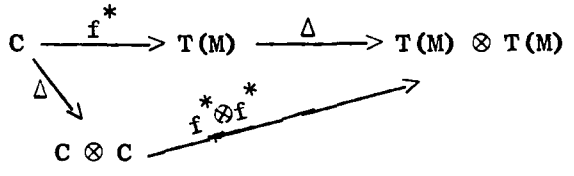
§2. The Universal Property of $T(M)$.

Let (C,Δ,ϵ) be a coassociative coalgebra, and $f:C \to M$ a map of modules. (C_0 is, of course, in the kernel.) We shall show that there is a unique map of coalgebras, $f^*:C \to T(M)$, such that $pf^* = f$, where $p:T(M) \to M$ is defined by $\delta_{i,1}:T_i \to T_1$. We define f^* as follows. On C_k, $k \geq 0$, f^* is the composition

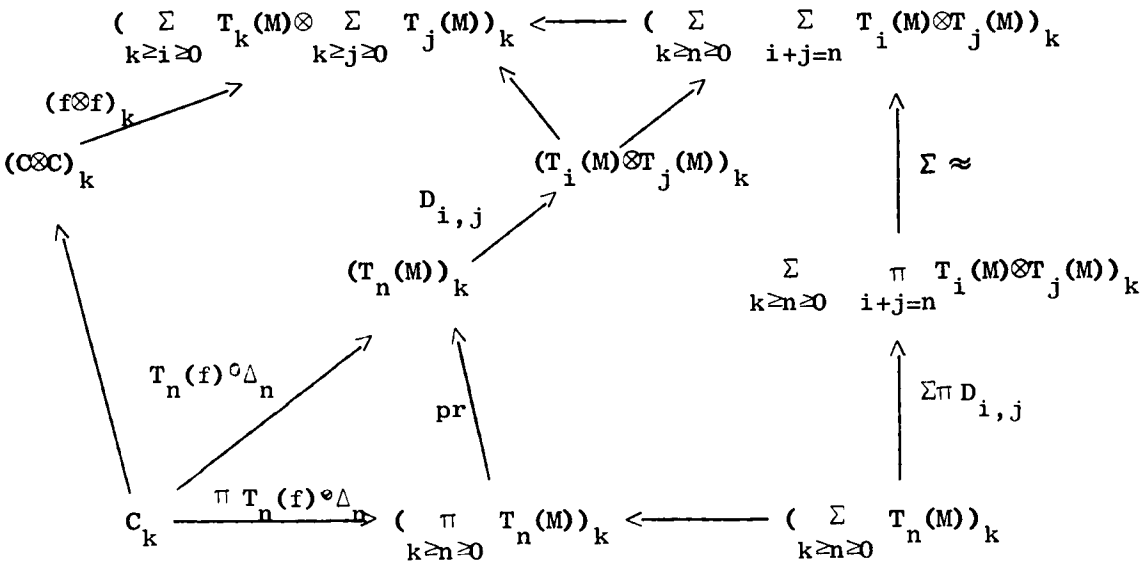
$$p_k^{-1} \circ \left(\pi_{k \geq n \geq 0} (T_n(f) \circ \Delta_n)\,|_{C_k} \right) : C_k \longrightarrow \pi_{k \geq n \geq 0} T_n(M)) \longleftarrow T(M)_k ,$$

where Δ_n is $(\Delta \otimes T_{n-2}(I)) \circ (\Delta \otimes T_{n-3}(I)) \circ \ldots \circ \Delta : C \to T_n(C)$, if $n \geq 2$, I if $n = 1$, ϵ if $n = 0$. Coherence is easily checked in the filtered case.

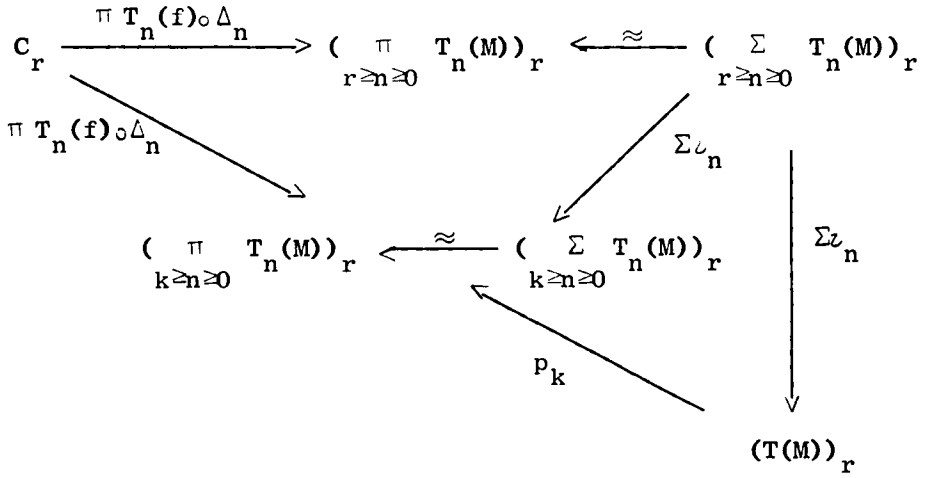
We must show that the following diagram commutes:



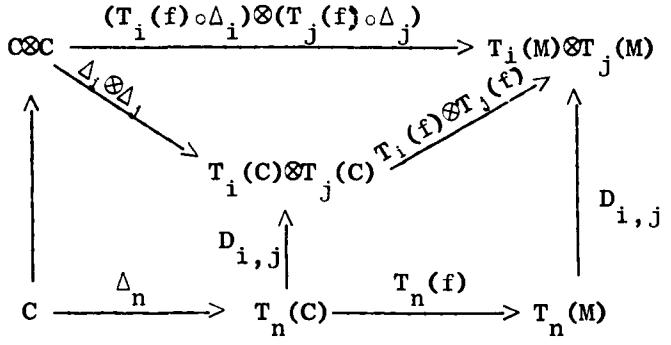
It suffices to check, for each k, n, i and j with $k \geq n = i+j$, the commutativity of the left hand pentagon below:



Recall that $(C\otimes C)_k = \sum_{r+s=k} C_r \otimes C_s$ or $\bigcup_{r+s=k} C_r \otimes C_s$ in the graded or filtered cases. If $r < i$, then $T_i(f)\circ\Delta_i$ is zero on C_r (an easy consequence of the diagonal map for C being a map of graded or filtered modules and the connected property of M). Therefore, the following diagram commutes:

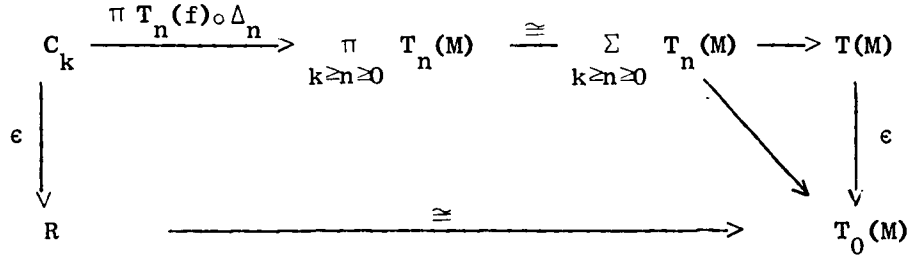


This enables us to check the commutativity of the component diagrams of the pentagons above; i.e., the restrictions to suitable degrees or filtrands of the outer diagrams below, for $i + j = n$.



The inner diagrams commute by generalized coassociativity of (C,Δ) and the naturality of $D_{i,j}$.

Finally, by definition of f^* ,



commutes, so that f^* is a map of coalgebras.

Suppose that $g:C \to T(M)$ is a coalgebra map such that $pg = f$. f^* and g must agree on C_0 and C_1 , as both are given by the augmentation and f . Suppose that f^* and g agree in degrees or filtrands less than n . Let $c \in C_n, \Delta c = c \otimes 1 + 1 \otimes c + \Sigma\, c' \otimes c''$. $g(c) = g(c) \otimes 1 + 1 \otimes g(c) + \Sigma\, g(c') \otimes g(c'') = g(c) \otimes 1 + 1 \otimes g(c) + \Sigma\, f^*(c') \otimes f^*(c'')$, by the inductive assumption. Clearly, $g(c) - f^*(c)$

is primitive, and consequently has zero components except in $T_1(M)$ $= P(T(M))$. But $pg = pf^* = f$ is precisely the condition that the 1 components agree. So $g(c) = f^*(c)$. Notice, we use connectedness of C in this proof of uniqueness, but not in the definition of f^* .

§3. The Hopf Algebra, T(A) .

Suppose now that (A,m,η,ϵ) is a connected R algebra. Then we may regard $A^+ = \text{Ker } \epsilon$ as a connected R module, and construct $T(A^+)$, which we harmlessly designate $T(A)$. We show that $T(A)$ can be made into an algebra, commutative if A is, associative if A is. Happily, the compatibility of this algebra structure with the coalgebra structure of $T(A)$, required to make $T(A)$ a Hopf algebra, is an immediate consequence of the definition.

Consider the following module map:

$$\bar{m}: T(A) \otimes T(A) \xrightarrow{p_1 \otimes p_1} (R \oplus A^+) \otimes (R \oplus A^+) \approx A \otimes A \xrightarrow{m} A \xrightarrow{I - \eta\epsilon} A^+ .$$

Since $T(A)$ is a coalgebra, $T(A) \otimes T(A)$ is a coalgebra in the canonical way, and $\bar{m}$ can be extended uniquely to a coalgebra map $m^*: T(A) \otimes T(A) \to T(A)$. $\iota_0: R \to T_0(A) \to T(A)$ is easily seen to be a unit. $(T(A), m^*, \Delta, \iota_0, p_0)$ is thus a Hopf algebra.

Suppose A is commutative. Then the following diagram commutes:

$$\begin{array}{ccccccc} T(A)\otimes T(A) & \xrightarrow{p_1\otimes p_1} & A \otimes A & \xrightarrow{m} & A & \xrightarrow{I-\eta\epsilon} & A^+ \\ \downarrow{\scriptstyle tw} & & \downarrow{\scriptstyle tw} & & \nearrow{\scriptstyle m} & & \\ T(A)\otimes T(A) & \xrightarrow{p_1\otimes p_1} & A \otimes A & & & & \end{array}$$

where tw is the twist map, signed in the graded case. By the universal property of the construction $p: T(A) \to A^+$, it follows that

the unique "lift" of the above diagram commutes, which is the commutativity of $(T(A),m^*)$.

Similarly, associativity of $(T(A),m^*)$ follows from the commutativity of

$$\begin{array}{ccccc} T(A)\otimes T(A)\otimes T(A) & \longrightarrow & A\otimes A\otimes A & \xrightarrow{m\otimes I} & A\otimes A \\ & & \downarrow{\scriptstyle I\otimes m} & & \downarrow{\scriptstyle m} \\ & & A\otimes A & \xrightarrow{m} & A \xrightarrow{I-\eta\epsilon} A^+ \end{array}$$

if A is associative.

§4. A Computational View of the Multiplication on $T(A)$.

The universal property of our construction has made the algebra structure easy to impose on $T(A)$, but we need some computational skill. Specifically, for our applications, we must be able to multiply elements of A^+ by arbitrary elements of $T(A)$. To give a description of the product of elements, it suffices to start inside components, and within components, to start with generators. We shall be happy, then, to compute products of the sort $m^*(a\otimes b)$, where $a = a_1\otimes a_2\otimes\ldots\otimes a_k \in T_k(A^+)$, $b \in T_1(A^+) = A^+$. We shall feel free to represent the multiplication in A by juxtaposition.

If $a \in T_0(A^+) = R$, the multiplication $m^*(a\otimes b)$ is defined by the module structure on A .

If $a \in T_1(A^+) = A^+$, the 0 component of $m^*(a\otimes b)$, defined by the augmentation of $T(A) \otimes T(A)$, will be 0 . The 1 component is $\bar{m}(a\otimes b) = ab$. The 2 component is $T_2(\bar{m})\circ\Delta(a\otimes b) = \bar{m}\otimes\bar{m}\circ tw\circ\Delta\otimes\Delta(a\otimes b)$ $= \bar{m}\otimes\bar{m}\circ tw\ ((a\otimes 1 + 1\otimes a)\otimes(b\otimes 1 + 1\otimes b)) = a\otimes b + (-1)^{\deg a\cdot\deg b}\, b\otimes a$, (dispensing with sign in the filtered case). All higher components

are zero, as a consequence of Lemma 4 below. In short, if a and b are in A^+, $m^*(a\otimes b) = (0, ab, a\otimes b \pm b\otimes a, 0, \ldots)$.

We give some rough information in the form of lemmas:

Lemma 1: $T_n(A^+) \subseteq \operatorname{Ker} T_{n+m}(I-\iota_0 p_0)\ \Delta_{n+m}:T(A) \to T_{n+m}(T(A))$, if $m \geq 1$. More specifically, $\Delta_{n+m}(T_n(A^+))$ is spanned by tensors $a_1\otimes a_2\otimes\ldots\otimes a_{n+m}$, with $a_{i_1} = 1$, $a_{i_2} = 1$, ..., $a_{i_m} = 1$, for some sub-collection of $a_1, a_2, \ldots, a_{n+m}$, with $a_i \in T_{\ell_i}(A^+) \subseteq T(A)$, $\Sigma \ell_i = n$.

Proof: These are general and easily demonstrable facts about graded connected coalgebras. Since $\Delta:T_n(A^+) \to \sum_{j+k=n} T_j(A^+) \otimes T_k(A^+)$, $T(A)$ may be graded as a coalgebra by the submodules $T_n(A^+)$, and $R = T_0(A^+)$ is clearly a direct summand.

Lemma 2: $T_n(A^+) \subseteq \operatorname{Ker}(T(A) \xrightarrow{\Delta_i} T_i(T(A)) \xrightarrow{T_i(p)} T_i(A))$, if $i < n$.

Proof: This is a direct consequence of the fact that

$$\Delta_i:T_n(A^+) \subseteq \sum_{\alpha_1+\alpha_2+\ldots+\alpha_i=n} T_{\alpha_1}(A^+) \otimes T_{\alpha_2}(A^+) \otimes \ldots \otimes T_{\alpha_i}(A^+) .$$

Lemma 3: If $a \in T_k(A^+)$, $b \in T_\ell(A^+)$, then $m^*(a\otimes b)$ is 0 in components i less than $\max(k,\ell)$.

Proof: From the definition, it is readily seen that

$$\Delta_i(T(A)\otimes T(A)) = tw_i(\Delta_i T(A)\otimes \Delta_i T(A))$$

where

$$tw_i:T_i\otimes T_i \xrightarrow{\cong} T_{2i} \xrightarrow{\sigma} T_{2i} \xrightarrow{\simeq} T_i \circ T_2 ,$$

where σ is the (signed) permutation of factors induced by

$$k \to \begin{cases} 2k-1 & k = 1,2,\ldots,i \\ 2k-2i & k = i+1,\ldots,2i \end{cases} .$$

Let us break the definition of the i component of $m^*(a\otimes b)$ into stages.

1) $\Delta_i\otimes\Delta_i\colon T_2(T(A)) \to T_2(T_i(T(A)))$.

2) $tw_i\colon T_2(T_i(T(A))) \to T_i(T_2(T(A)))$.

3) $T_i(T_2(p)\colon T_i(T_2(T(A))) \to T_i(T_2(A))$.

4) $T_i(\bar{m})\colon T_i(T_2(A)) \to T_i(A)$.

5) $T_i(I-\eta\epsilon)\colon T_i(A) \to T_i(A^+)$.

Since tw_i is natural, stages 2 and 3 may be interchanged. By Lemma 2, if $a\otimes b \in T_k(A) \otimes T_\ell(A)$ and k or ℓ is greater than i, $a\otimes b$ will go to zero after applying stages 1 and 3 in succession.

Lemma 4: If $a \in T_k(A^+)$, $b \in T_\ell(A^+)$, $m^*(a\otimes b)$ is 0 in components $i > k+\ell$.

Proof: By Lemma 1, each tensor of $(tw_i\circ \Delta_i\otimes\Delta_i)(a\otimes b)$ has at least one factor of type $r_1 \otimes r_2$ $r_1, r_2 \in R$. Applying $\bar{m}$, such a factor goes to $r_1 r_2 \in R$, which projects to 0 in A^+ . By multilinearity, such a tensor goes to zero at stage 5.

Suppose now that $a \in T_k(A^+)$, $b \in T_\ell(A^+)$. By Lemmas 3 and 4, all non-trivial components of $m^*(a\otimes b)$ lie between $\max(k,\ell)$ and $k+\ell$. In particular, if $\ell = 1$, we must compute only the k and $k+1$ components. We shall do this, and hope to leave the impression that the general case is more difficult by notation only.

Apply $\Delta_k\otimes\Delta_k$ to $a\otimes b$. $\Delta_k b$ is clearly $b\otimes 1\otimes\ldots\otimes 1 + 1\otimes b\otimes 1\otimes\ldots\otimes 1 + \ldots + 1\otimes 1\otimes\ldots\otimes 1\otimes b$. We argue now that we may discard most of the tensors of $\Delta_k a$.

Suppose one has a factor $r \in R$. As $a \in T_k(A^+)$ and $r \in T_0(A^+)$,

some other factor of the tensor will belong to $T_j(A^+)$, $j \geq 2$. Since tw_i is natural, apply $T_2(T_k(p))$ before tw_k. The tensor will go to 0 under this projection. It suffices to compute

$$a\otimes b \xrightarrow{T_k(I-\tau_0 p_0)\circ\Delta_k\otimes\Delta_k} (a_1\otimes a_2\otimes\ldots\otimes a_k)\otimes \sum_{j=1}^{k} 1\otimes\ldots\otimes\overset{j}{b}\otimes 1\otimes\ldots\otimes 1$$

$$\xrightarrow{tw_k} \sum_{j=1} (-1)^{(\alpha_{j+1}+\ldots+\alpha_k)\beta}(a_1\otimes 1)\otimes(a_2\otimes 1)\otimes\ldots\otimes(a_j\otimes b)\otimes\ldots\otimes(a_k\otimes 1)$$

$$\xrightarrow{T_k(I-\eta\epsilon)\circ T_k(m)\circ T_k(p)} \sum_{j=1}^{k} (-1)^{(\alpha_{j+1}+\ldots+\alpha_k)\beta}(a_1\otimes a_2\otimes\ldots\otimes a_j b\otimes\ldots\otimes a_k)\ ,$$

where α_i and β are the degrees of a_i and b. We now have the k component.

For the $k+1$ component, begin by applying $\Delta_{k+1}\otimes\Delta_{k+1}$ to $a\otimes b$. $\Delta_{k+1}\, b$ is clearly $\sum_{j=1}^{k+1} 1\otimes\ldots\otimes\overset{j}{b}\otimes\ldots\otimes 1$. We argue again that we may discard most of the tensors of $\Delta_{k+1}\, a$. Suppose such a tensor has two factors in $T_0(A^+)$. Then, as $a\in T_k(A^+)$, some other factor of this tensor will belong in $T_j(A^+), j\geq 2$. As above, we may project before twisting, and such a tensor projects to zero.

In our computation, we may thus replace $\Delta_k\, a$ by

$\sum_{j=1}^{k+1} a_1\otimes\ldots\otimes a_{j-1}\otimes 1\otimes a_j\otimes\ldots\otimes a_k$. At Stage 3, (see proof of Lemma 3) we have $\sum_{j=1}^{k+1}(-1)^{(\alpha_{j+1}+\ldots+\alpha_k)\beta}(a_1\otimes 1)\otimes\ldots\otimes(a_{j-1}\otimes 1)\otimes(1\otimes b)\otimes(a_j\otimes 1)\otimes\ldots\otimes(a_k\otimes 1)$

+ tensors with factors $(1\otimes 1)$. Under $T_k(I-\eta\epsilon)\circ T_k(m)\circ T_k(p)$, only the first type of summands survive, to give

$$\sum_{j=1}^{k+1}(-1)^{(\alpha_{j+1}+\ldots+\alpha_k)\beta}\, a_1\otimes a_2\otimes\ldots\otimes a_{j-1}\otimes b\otimes a_j\otimes\ldots\otimes a_k\ .$$

We have completed our computation. Summarizing,

$$m^*((a_1\otimes a_2\otimes\ldots\otimes a_k)\otimes b) = \sum_{j=1}^{k} \pm\, a_1\otimes a_2\otimes\ldots\otimes a_{j-1}\otimes a_j b\otimes\ldots\otimes a_k$$

$$+ \sum_{j=1}^{k+1} \pm\, a_1\otimes\ldots\otimes a_{j-1}\otimes b\otimes a_j\otimes\ldots\otimes a_k \in T_k(A^+) \oplus T_{k+1}(A^+)$$

$$\subseteq T(A) ,$$

where $a_i, b \in A^+$.

§5. S(M) , A Subcoalgebra of T(M) .

Let Σ_n be the symmetric group. Burnside's presentation of Σ_n is

$\{(i,i+1),\ i=1,2,\ldots,n-1:\ e = (i,i+1)^2 ,\ i=1,2,\ldots,n-1 .$

$e = ((i,i+1)(i+1,i+2))^3 \qquad i=1,2,\ldots,n-2 ,$

$e = ((i,i+1)k,k+1))^2 \qquad i \le k-2,\ k=3,4,\ldots,n-1\}$

(See Coxeter and Moser [12])

We define an action of Σ_n on $T_n(M)$ by extension of

$$(i,i+1)\circ m_1\otimes m_2\otimes\ldots\otimes m_n = (-1)^{\mu_i\mu_{i+1}}\, m_1\otimes\ldots\otimes_{i-1}\otimes m_{i+1}\otimes m_i\otimes\ldots\otimes m_n ,$$

where μ_j is the degree of m_j . In the filtered case, leave signs out. The action is well-defined, as relations in the presentation correspond to

$$(-1)^{\mu_i\mu_{i+1}}\cdot(-1)^{\mu_{i+1}\mu_i} = 1 ,$$

$$(-1)^{\mu_{i+1}\mu_{i+2}}\cdot(-1)^{\mu_i\mu_{i+2}}\cdot(-1)^{\mu_{i+1}\mu_i}\cdot(-1)^{\mu_{i+1}\mu_{i+2}}\cdot(-1)^{\mu_i\mu_{i+2}}\cdot(-1)^{\mu_i\mu_{i+1}} = 1 .$$

$$(-1)^{\mu_k\mu_{k+1}}\cdot(-1)^{\mu_i\mu_{i+1}}\cdot(-1)^{\mu_k\mu_{k+1}}\cdot(-1)^{\mu_i\mu_{i+1}} = 1 .$$

Let $S_n(M)$ be the submodule of $T_n(M)$ fixed under this action. Let

S(M) be $\sum_{n\ge 0} S_n(M)$.

Claim: S(M) is a co-commutative subcoalgebra of T(M) .

Proof: To show S(M) is a subcoalgebra, it suffices to show that

$$\text{image } (S_k(M) \xrightarrow{\subseteq} T_k(M) \xrightarrow{\iota_k} T(M) \xrightarrow{\Delta} T(M) \otimes T(M))$$

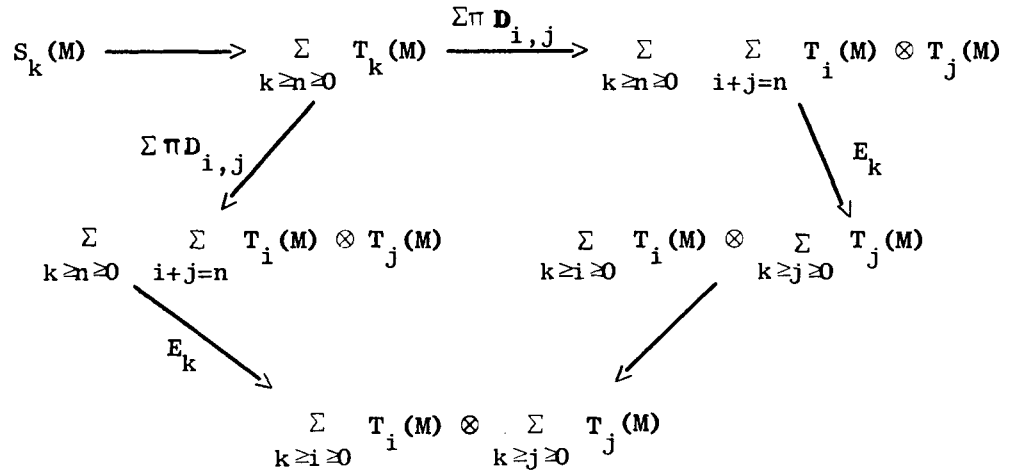
lies in $S(M) \otimes S(M)$ for each $k \geq 0$. Unsurprisingly, this can be reduced to locating the image of

$$S_k(M) \subseteq T_k(M) \to \sum_{k \geq n \geq 0} T_n(M) \to$$

$$\sum_{k \geq n \geq 0} T_n(M) \otimes \sum_{k \geq n \geq 0} T_n(M) \quad \text{inside} \quad \sum_{k \geq n \geq 0} S_k(M) \otimes \sum_{k \geq n \geq 0} S_n(M) .$$

The identification of $\sum_{k \geq n \geq 0} \sum_{i+j=n} T_i(M) \otimes T_j(M)$ with a subset of $\sum_{k \geq n \geq 0} T_i(M) \otimes \sum_{k \geq j \geq 0} T_j(M)$ is equivariant with respect to the obvious map of groups: $\sum_{k \geq n \geq 0} \sum_{i+j=n} \Sigma_i \times \Sigma_j \to \sum_{k \geq i \geq 0} \Sigma_i \times \sum_{k \geq j \geq 0} \Sigma_j$. From this observation and further untangling of the definition of the diagonal map, it suffices to check that $S_k(M) \subseteq T_k(M)$ is mapped into $S_i(M) \otimes S_j(M)$ by $D_{i,j}(M)\colon T_k(M) \to T_i(M) \otimes T_j(M)$ for $i+j = k$. Identifying Σ_j as the subset of Σ_k which fixes $\{i+1, i+2, \ldots, k\}$ and Σ_i as the subset of Σ_k which fixes $\{1,2,\ldots,i\}$, we merely observe that the submodule of $T_k(M)$ fixed under Σ_k is necessarily fixed under the subgroup $\Sigma_i \times \Sigma_j$. This completes the argument that $S(M)$ is a subcoalgebra.

We may reformulate the question of co-commutativity of $S(M)$ as: Is the following a commutative diagram?



The map tw , restricted to the subset $\sum_{k\geq n\geq 0} \sum_{i+j=n} T_i(M)\otimes T_j(M)$

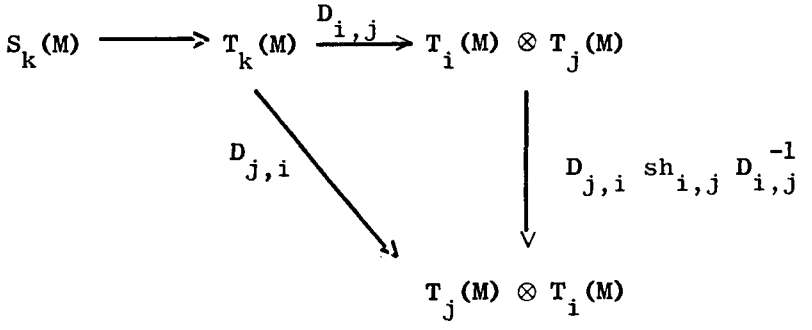
of $\sum_{k\geq i\geq 0} T_i(M)\otimes \sum_{k\geq j\geq 0} T_j(M)$ is the sum of the maps

$$\sum_{i+j=n} T_i(M)\otimes T_j(M) \xrightarrow{(sh^D)_n} \pi_{i+j=n} T_i(M)\otimes T_j(M) \approx \sum_{i+j=n} T_i(M)\otimes T_j(M)$$

with $(sh^D)_n$ induced by $T_i(M)\otimes T_j(M) \xrightarrow{D_{j,i}\ sh_{i,j}\ D_{i,j}^{-1}} T_j(M)\otimes T_i(M)$

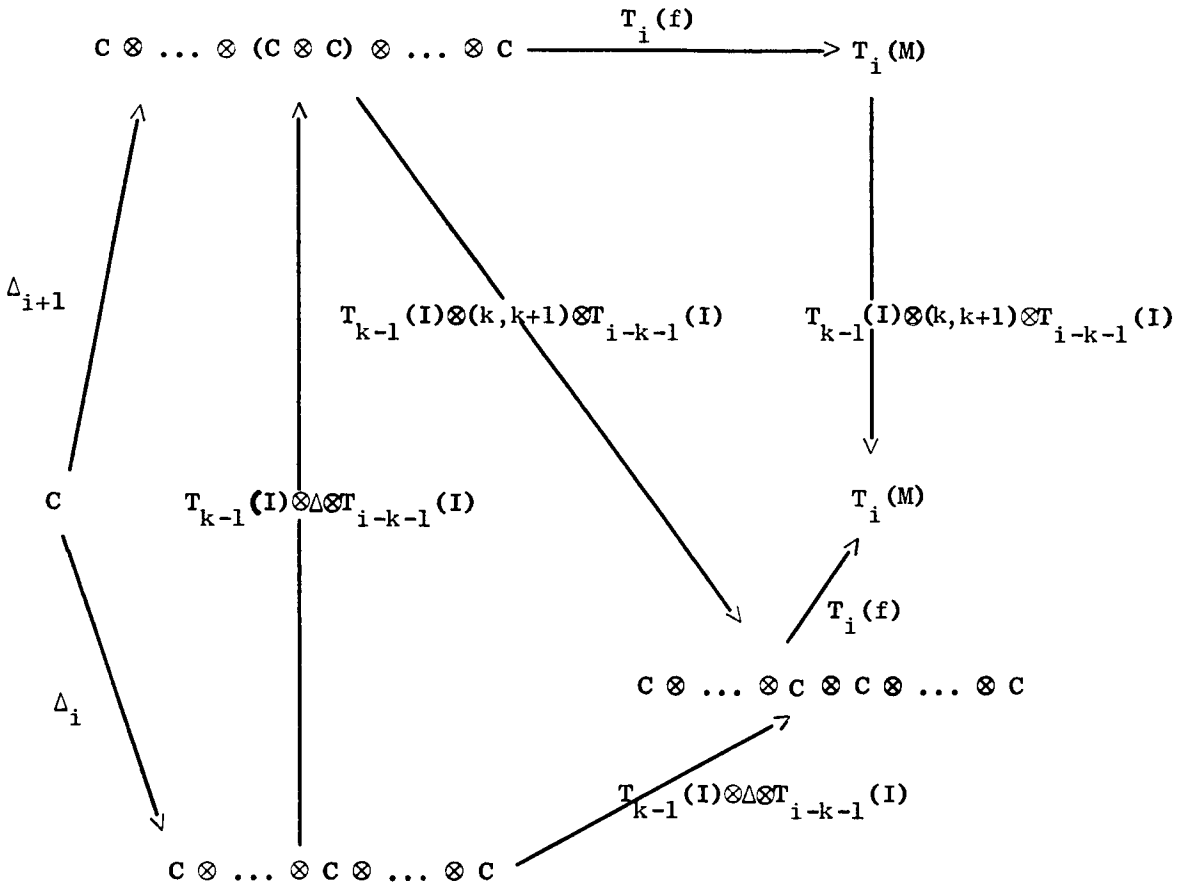
and zero maps, where $sh_{i,j}$ is induced by $\ell \to \begin{cases} \ell+j & \ell = 1,2,\ldots,i \\ \ell-i & \ell = i+1,i+2,\ldots,n \end{cases}$.

We may now verify the commutativity of



directly from the definition of $S_k(M)$.

Suppose now that C is a co-commutative, coassociative coalgebra, $f: C \to M$ a map of modules. Then the unique $f^*: C \to T(M)$ extending f factors through $S(M) \subseteq T(M)$. This is a direct consequence of the genralized coassociativity and cocommutativity of C and the definition of f^*; i.e., the commutativity of the following diagram suffices for an argument.



§6. S(A), a Sub-Hopf Algebra of T(A).

Suppose now that A is an algebra. We let $S(A^+)$ be written $S(A)$. $S(A) \otimes S(A)$ is a co-commutative coalgebra. Since $S(A)$ is and the module map

$$S(A) \otimes S(A) \longrightarrow T(A) \otimes T(A) \xrightarrow{\bar{m}} A^+$$

extends uniquely to a map of coalgebras $S(A) \otimes S(A) \to S(A)$. This is clearly the restriction of the multiplication m^* on $T(A)$, and we may appropriate the computations of Section 4 for use in $S(A)$. $S(A)$ is, of course, commutative or associative when $T(A)$ is, being a sub-algebra.

We have said nothing about the naturality of the constructions, but this is trivially verified.

CHAPTER X

POLYNOMIAL DUAL SUBCOALGEBRAS OF S(A)

1. Introduction.

We are interested in the following question. Suppose M is an R-submodule of an R-algebra A, which is torsion free as an abelian group. Is there a sub-Hopf algebra, $\mathcal{K}_M$, of S(A) which has polynomial dual coalgebra structure, and whose primitive submodule is M? If M is free abelian and a pure subgroup of A, we adapt the scheme of Chapter II to answer this question. We demonstrate that the tests we have devised for the existence of towers in S(A) may be administered in A. This is cheerful news, for in Chapter IX, § 4, we observed that computing in S(A) is awesome. We get less satisfactory results when A is not commutative or associative, but we indicate a plan for improving these cases.

All modules, algebras, etc. are required to be filtered or graded and connected. Graded objects are presumed to lie in even degrees. Rings are of characteristic zero.

2. Towers over Submodules of Algebras.

Theorem 1. Suppose M is a free R-submodule of A^+, where A is an algebra over R. Let M be a pure sub-abelian group of A. Let $\{P_{\alpha,1}\}_{\alpha\in\mathcal{A}}$ be a basis for M. Suppose for each $\alpha \in \mathcal{A}$ there are sequences in A^+, $\{P_{\alpha,j}\}_{j\in Z^+-\{0\}}$ and $\{K_{\alpha,j}\}_{j\in Z^+-\{0\}}$, extending $P_{\alpha,1}$ and 0 satisfying

i) $jP_{\alpha,j} - K_{\alpha,j} \in M$ and

ii) $K_{\alpha,j} = \sum_{j=k+\ell} P_{\alpha,k}(\ell P_{\alpha,\ell} - K_{\alpha,\ell})$ $\forall\, j \in Z^+-\{0\}$.

Then there are infinite towers $\{\overline{P_{\alpha,j}}\}_{j\in Z^+-\{0\}}$ in $S(A)$ extending $\overline{P_{\alpha,1}} = P_{\alpha,1}$, $\forall\, \alpha \in \mathcal{A}$, such that the sub-Hopf algebra, $\mathcal{K}_M$, of $S(A)$ generated by $\{\overline{P_{\alpha,j}}\}_{\substack{\alpha\in\mathcal{A}\\ j\in Z^+-\{0\}}}$ has polynomial dual coalgebra structure whenever $P(\mathcal{K}_M) \cap m^*((\mathcal{K}_M \otimes \mathcal{K}_M)^+) \subseteq M$.

Remarks:

i) We are committing ourselves to constructing the towers $\{\overline{P_{\alpha,j}}\}_{j\in Z^+}$ and demonstrating that the indecomposable primitives of $\mathcal{K}_M$ lie in M . The coalgebra structure will be a consequence of Borel's theorem.

ii) It is possible that $P_{\alpha,j} = 0$ for some $j > 1$. It, of course, is impossible that $\overline{P_{\alpha,j}} = 0$ for any indices.

iii) If $M = A^+$, Theorem 1 says $S(A)$ has polynomial dual coalgebra structure, for we may let $P_{\alpha,j} = P_{\alpha,1}^{\,j}$ and $K_{\alpha,j} = (j-1)P_{\alpha,1}^{\,j}$. This is well known, and is, in fact, the point of the construction.

iv) If A is commutative and associative, $S(A)$ is, by Chapter IX, p.84. By iii) above, and Chapter VIII, the primitives are indecomposable in $S(A)$. We may drop the condition $P(\mathcal{K}_M) \cap m^*((\mathcal{K}_M \otimes \mathcal{K}_M)^+) \subseteq M$ as it is trivially satisfied.

v) There are counter-examples. Let $A = Z[X]$, $M = ZX$. $m^*(X \otimes X) = X^2 + 2(X \otimes X)$ by Chapter IX, p. 77. But $nX + X^2 + 2(X \otimes X)$ is not divisible by 2 for any $n \in Z$. Hence (Proposition 1, Chapter II), no tower of height 2 can be built over X in any sub-Hopf algebra of $S(Z[X])$ whose primitives lie in M .

Proof of Theorem 1. We define

$$\overline{P_{\alpha,j}} \equiv \sum_{k=1}^{\infty} \sum_{j_1+j_2+\ldots+j_k=j} P_{\alpha,j_1} \otimes P_{\alpha,j_2} \otimes \ldots \otimes P_{\alpha,j_k} .$$

Clearly $\overline{P_{\alpha,j}} \in S(A) \subseteq T(A)$ and $\overline{P_{\alpha,j}} \xrightarrow{\Delta} \sum_{k+\ell=j} \overline{P_{\alpha,k}} \otimes \overline{P_{\alpha,\ell}}$ so that $\{\overline{P_{\alpha,j}}\}_{j\in Z^+-\{0\}}$ is an infinite tower over $\overline{P_{\alpha,1}} \equiv P_{\alpha,1} \in M$.

We now define $\overline{K_{\alpha,j}} \equiv \sum_{k+\ell=j} m^*(\overline{P_{\alpha,k}} \otimes (\ell\overline{P_{\alpha,\ell}} - \overline{K_{\alpha,\ell}}))$ recursively. We show that $j\overline{P_{\alpha,j}} - \overline{K_{\alpha,j}} = jP_{\alpha,j} - K_{\alpha,j} \in M$. We shall drop the subscripts $\alpha \in \mathcal{A}$, as the argument is independent of α.

$\overline{P_n} - \overline{K_1} = \overline{P_1} - 0 = P_1 \in M$, so we may assume for $j < n$ that $j\overline{P_j} - \overline{K_j} = jP_j - K_j \in M$.

$$n\overline{P_n} - \overline{K_n} = n\overline{P_n} - \sum_{k+\ell=n} m^*(\overline{P_k} \otimes \ell\overline{P_\ell} - \overline{K_\ell})$$

$$= n\overline{P_n} - \sum_{k+\ell=n} m^*(\overline{P_k} \otimes (\ell P_\ell - K_\ell))$$

$$= n\overline{P_n} - \sum_{k+\ell=n} \sum_{g=1}^{\infty} \sum_{k_1+k_2+\ldots+k_g=k} m^*(P_{k_1} \otimes P_{k_2} \otimes \ldots \otimes P_{k_g}) \otimes (\ell P_\ell - K_\ell)$$

(by (Chapter IX, p.80))

$$= n\overline{P_n} - \sum_{k+\ell=n} \sum_{g=1}^{\infty} \sum_{k_1+k_2+\ldots+k_g=k}$$

$$\left\{ \sum_{i=1}^{g} P_{k_1} \otimes \ldots \otimes P_{k_i} (\ell P_\ell - K_\ell) \otimes \ldots \otimes P_{k_g} \right.$$

$$\left. + \sum_{i=0}^{g} P_{k_1} \otimes \ldots \otimes P_{k_i} \otimes (\ell P_\ell - K_\ell) \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g} \right\} .$$

We now change the order of summation so that terms of type

$P_{k_1} \otimes \ldots \otimes P_{k_{i-1}} \otimes P_{k_i}(\ell P_\ell - K_\ell) \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g}$ with $k_i + \ell = n - k_1 - \ldots - \hat{k}_i - \ldots - k_g$ for fixed $\{k_1, \ldots, \hat{k}_i, \ldots, k_g\}$, are added first, with sum

(*) $\quad P_{k_1} \otimes \ldots \otimes P_{k_{i-1}} \otimes K_{k_i+\ell} \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g}$.

Next, split tensors $P_{k_1} \otimes \ldots \otimes P_{k_i} \otimes (\ell P_\ell - K_\ell) \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g}$ into

(**) $\quad \ell P_{k_1} \otimes \ldots \otimes P_{k_i} \otimes P_\ell \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g}$

(***) $\quad P_{k_1} \otimes \ldots \otimes P_{k_i} \otimes K_\ell \otimes P_{k_{i+1}} \otimes \ldots \otimes P_{k_g}$.

Tensors of type (*) are canceled by tensors of type (***), except the special case K_n .

Tensors of type (**) have coefficient n after summation.

With these observations, we find

$$n\overline{P_n} - \overline{K_n} = n\overline{P_n} - K_n - n \sum_{k=2}^{\infty} \sum_{j_1+j_2+\ldots+j_k=n} P_{j_1} \otimes \ldots \otimes P_{j_k}$$

$$= nP_n - K_n \ .$$

Suppose now that P is primitive in $\mathcal{A}_M$. Project P to $\mathcal{A}_M/m^*(\mathcal{A}_M \otimes \mathcal{A}_M)^+ \equiv Q(\mathcal{A}_M)$. The images of $\overline{P_{\alpha,i}}$ are module generators for $Q(\mathcal{A}_M)$. In $Q(\mathcal{A}_M)$, $P = \Sigma\, n'_{\alpha,i}\, \overline{P_{\alpha,i}}$. Choose $N \in Z$ so that $i \mid N$ if $n_{\alpha,i} \neq 0$. Then $NP = \Sigma\, n'_{\alpha,i} \cdot i\overline{P_{\alpha,i}}$ in $Q(\mathcal{A}_M)$. Clearly, $\overline{K_{\alpha,i}}$ projects to zero in $Q(\mathcal{A}_M)$ $\forall\ \alpha \in \mathcal{A}$, $\forall\ i \in Z^+$. Hence $NP - \Sigma\, n_{\alpha,i}(i\overline{P_{\alpha,i}} - \overline{K_{\alpha,i}})$ projects to 0 in $Q(\mathcal{A}_M)$. Since $P(\mathcal{A}_M) \cap m^*((\mathcal{A}_M \otimes \mathcal{A}_M)^+) \subseteq M$, $NP - \Sigma\, n_{\alpha,i}(i\overline{P_{\alpha,i}} - \overline{K_{\alpha,i}}) \in M$ and NP

does, as well. But M is pure, so $P \in M$.

Example. Suppose A is a Hopf algebra, satisfying the hypotheses of Borel's theorem, and M is the primitive submodule. Clearly M is a pure sub-abelian group of A^+. Theorem 1 says there is a sub-Hopf algebra of $S(A)$ isomorphic (under $p: S(A) \to A$) to A as a Hopf algebra, if A is commutative and associative.

We discuss now a scheme for improving Theorem 1 in the non-commutative, non-associative cases, using the apparatus of Chapter VII and VIII. Notice that $P_{\alpha,i} \in A$ has been treated as an analogue of a tower element, $\overline{P_{\alpha,i}} \in S(A)$, and M as the analogue of the primitive submodule of a Hopf algebra; we develop this point of view.

Let $P_{A,I} \equiv P_{\alpha_1,i_1} P_{\alpha_2,i_2} \dots P_{\alpha_k,i_k} \in A$, just as $\overline{P_{A,I}} = \overline{P_{\alpha_1,i_1}}\ \overline{P_{\alpha_2,i_2}} \dots \overline{P_{\alpha_k,i_k}} \in S(A)$. We may use the definitions (VII.3) and (VII.4) to define inductively elements $p(P_{A,I},P_{B,J}) \in A$ and $p(P_{A,I},P_{B,J},P_{C,K}) \in A$. These definitions and the requirement that these elements are actually in M should be hypothesis in an improved version of Theorem 1. We should be able to demonstrate that

$$(*)\quad p(P_{A,I},P_{B,J}) = p(\overline{P_{A,I}},\overline{P_{B,J}}) \in A \cap S(A)$$

$$(**)\quad p(P_{A,I},P_{B,J},P_{C,K}) = p(\overline{P_{A,I}},\overline{P_{B,J}},\overline{P_{C,K}}) \in A \cap S(A)$$

just as $i\overline{P_{\alpha,i}} - \overline{K_{\alpha,i}}$ was demonstrably equal to $IP_{\alpha,i} - K_{\alpha,i}$.

We should then proceed as follows: (i) showing that $\mathcal{N}_M$, defined as above, has as a rational basis $B = \left\{\overline{P_{\alpha_1,i_1}}\ \overline{P_{\alpha_2,i_2}} \dots \overline{P_{\alpha_k,i_k}}\right\}_{\substack{\alpha_1<\dots<\alpha_k \\ i_1,\dots i_k \in Z^+-\{0\}}}$. This would involve (*) and (**), as well as the techniques of Chapter VIII, extended to the non-associative case; (ii) noticing with little

effort that the primitives in the span of B are in M ; and (iii) invoking the purity of M . This puts all of the primitives of $\mathcal{K}_M$ in M , and we may apply Borel's theorem.

A lack of interest might impede filling in the details of this sketch, (and has), but we don't imagine anything else could. Unless applications become available, it seems punishing to do it.

3. Examples of Towers over Submodules in Commutative, Associative Algebras.

We propogandize the computability of sequences required for the application of Theorem 1 in non-trivial examples.

Let W be a finite group acting on a commutative, associative algebra A over R , a ring of characteristic zero. Let $\varphi: A \to R$ be an algebra homomorphism. Let A^W be the subalgebra of A fixed under the action of W , and suppose A^W is generated by a family $\{B_\alpha\}_{\alpha \in \mathcal{A}}$. Let $\bar{A} \equiv A/\{B_\alpha - \varphi(B_\alpha)\}$ be the quotient algebra, with projection map $p: A \to \bar{A}$. Let $D: A \to A$ be a derivation, and M be the submodule of $\bar{A}$ spanned by $\{pDB_\alpha\}_{\alpha \in \mathcal{A}}$.

Theorem 2. Suppose, for each α , there is a finite family of elements of A , $\{A_{\alpha,i}\}_{i \in I_\alpha}$, such that $B_\alpha = \sum_{i \in I_\alpha} A_{\alpha,i}$, satisfying

(i) if $w \in W$, $A_{\alpha,i}^{w} = A_{\alpha,j}$ for some $j \in I_\alpha$, for all $i \in I_\alpha$.

(ii) $DA_{\alpha,i} = n_{\alpha,i} A_{\alpha,i}$, for some $n_{\alpha,i} \in Z \subseteq R$, for all $\alpha \in A$, for all $i \in I_\alpha$.

In addition, assume M is a pure sub-abelian group of $\bar{A}$. Then for each $\alpha \in \mathcal{A}$ there are sequences $\{P_{\alpha,n}\}_{n \in Z^+ - \{0\}}$ and $\{K_{\alpha,n}\}_{n \in Z^+ - \{0\}}$ satisfying:

(iii) $nP_{\alpha,n} - K_{\alpha,n} \in M$ for all $\alpha \in \mathcal{A}$, for all $n \in Z^+ - \{0\}$.

(iv) $\sum_{i+j=n} P_{\alpha,i}(jP_{\alpha,j} - K_{\alpha,j}) = K_{\alpha,n}$ for all $\alpha \in \mathcal{A}$, for all $n \in Z^+ - \{0\}$.

(v) $K_{\alpha,1} = 0$ and $P_{\alpha,1} = p(DB_\alpha)$, for all $\alpha \in \mathcal{A}$.

Proof: If $n \in Z$, $k \in Z^+$, we define

$$\binom{n}{k} \equiv \begin{cases} \dfrac{n(n-1)\ldots n(n-k+1)}{k(k-1)\ldots 1} & \text{if } k > 0 \\ 1 & \text{if } k = 0 \end{cases}$$

If $\alpha \in \mathcal{A}$, $j \in Z^+ - \{0\}$, we define

$$P_{\alpha,j} \equiv \sum_{k=1}^{\infty} \sum_{i_1,i_2,\ldots,i_k \in I_\alpha} \sum_{\substack{j_1+j_2+j_k=j \\ j_1,j_2,\ldots,j_k \in Z^+ - \{0\}}} p\left\{ \binom{n_{\alpha,i_1}}{j_1}\binom{n_{\alpha,i_2}}{j_2}\ldots\binom{n_{\alpha,i_k}}{j_k} A_{\alpha,i_1}^{j_1} A_{\alpha,i_2}^{j_2} \cdots A_{\alpha,i_k}^{j_k} \right\}$$

$$K_{\alpha,j} = jP_{\alpha,j} + p\left\{(-1)^j \sum_{i \in I_\alpha} n_{\alpha,i} A_{\alpha,i}^j\right\}.$$

We must verify (iii), (iv), and (v). Since D is linear, $DB_\alpha = \sum_{i \in I_\alpha} n_{\alpha,i} A_{\alpha,i}$ follows from (ii). (v) follows immediately. (iv) is straightforward if one is in possession of the following combinatorial identity, which we prove: Let $n \in Z^+$, $m \in Z$, then

$$(-1)^n n \cdot \binom{m}{n} + m \sum_{j=0}^{n-1} (-1)^j \binom{m}{j} = 0.$$

Proof: By induction,

$$(-1)^{n-1}(n-1)\binom{m}{n-1} + m\sum_{j=0}^{n-2}(-1)^j\binom{m}{j} = 0 \ , \text{ so}$$

$$(-1)^n n\binom{m}{n} + m\cdot(-1)^{n-1}\binom{m}{n-1} + m\sum_{j=0}^{n-2}(-1)^j\binom{m}{j}$$

$$= (-1)^n\cdot n\binom{m}{n} + m(-1)^{n-1}\binom{m}{n-1} + (-1)^n(n-1)\binom{m}{n-1}$$

$$= (-1)^n\left\{n\binom{m}{n} - (m-(n-1))\binom{m}{n-1}\right\} .$$

The last expression is trivially zero.

Consider (iii). We must show $p\left\{\sum_{i\in I_\alpha} n_{\alpha,i} A_{\alpha,i}^j\right\}$ is in the span of $\{pDB_\beta\}_{\beta\in\mathcal{A}}$, for all $\alpha\in\mathcal{A}$, $j\in Z^+-\{0\}$. Since D is a derivation, (ii) implies $D\left(\sum_{i\in I_\alpha} A_{\alpha,i}^j\right) = j\sum_{i\in I_\alpha} n_{\alpha,i} A_{\alpha,i}^j$. It suffices to show that $p\left(D\left(\sum_{i\in I_\alpha} A_{\alpha,i}^j\right)\right)$ is in M, since M is pure. By (i), W permutes the $A_{\alpha,i}$'s, so that $\Sigma A_{\alpha,i}^j \in A^W$ which is generated by $\{B_\alpha\}_{\alpha\in\mathcal{A}}$. Thus $\Sigma A_{\alpha,i}^j = \sum_A r_A B_{\alpha_1} B_{\alpha_2}\cdots B_{\alpha_k}$. But

$$p\left(D\left(\sum_A r_A B_{\alpha_1},B_{\alpha_2},\ldots,B_{\alpha_k}\right)\right) = p\left(\sum_A r_A \sum_{j=1}^k (B_{\alpha_n}\cdots D(B_{\alpha_j})\cdots B_{\alpha_k}\right)$$

$$= \sum_A r_A \sum_{j=1}^k \varphi(B_{\alpha_1})\ldots p(D(B_{\alpha_j}))\ldots\varphi(B_{\alpha_k}) \text{ which is clearly in } M .$$

This completes the proof of Theorem 2.

Consider the Weyl group W acting on the complex representation ring, $R(T)$, of a maximal torus, T, in a simply connected compact simple Lie group, G. Polynomial generators for $R(G)$ are the fundamental representations $\{\rho_i\}$. Under the inclusion $i:T\to G$, $R(G)$

may be identified with $R(T)^W$, and $i^*(\rho_i)$ may be expressed as a sum of weights which are permuted by W . Any derivation of $R(T)$ is uniquely determined by its values on fundamental weights $\{w_i\}$. For derivation D sending $w_i \to n_i w_i$, $n_i \in Z$, the hypotheses of Theorem 2 will be satisfied, with the exception of the condition on M , which depends on φ and D , and is, of course, very difficult to check. If $\varphi: R(T) \to Z$ is the augmentation, assigning to an element of $R(T)$ its virtual dimension, $R(T)/\{i^*(\rho_i)-\varphi i^*(\rho_i)\}$ may be identified with $K(G/T)$, which is a free abelian group of rank $|W|$. (See Vasquez [13].)

It should occur to the reader familiar with Bott [14] that this specialization of Theorem 2, or a subtle variant, might find its place in a proof that $K_*(\Omega G)$ is a polynomial algebra for such Lie groups.

Roughly speaking (let us ignore the difference between simply connected and centerless groups), Bott was able to show that to each circle $s: S^1 \to G$ satisfying certain technical conditions, a map $f_s: G/G_s \to \Omega G$ could be assigned (where G_s is the centralizer of s in G) , whose image in ordinary homology generated $H_*(\Omega G)$ as an algebra. Dualized, this fact is interpreted as: $(f_s^*)^*: H^*(\Omega G) \to S(H^*(G/G_s))$ is a Hopf algebra inclusion onto a (module) direct summand. Under certain torsion free assumptions, general descriptions of $H^*(G/G_s)$ and $f_s^*(P(H^*(\Omega G)) \subseteq H^*(G/G_s)$ were given by Bott, with well-known models for specific groups and circles. In this setting, the existence of such infinite sequences as described in Theorem 1 is equivalent to $H_*(\Omega G)$ being a polynomial algebra. Bott always found other means to get this result in his examples. We consider one class of his examples, the symplectic groups, and construct the sequences.

Following Bott ([14],p. 59), we let $G = Sp(n)$, $G_s = U(n)$, and identify $H^*(Sp(n)/U(n))$ with $Z[X_1,X_2,\ldots,X_n]^{\Sigma n}/Z[X_1^2,X_2^2,\ldots,X_n^2]^{\Sigma n} = A$. Let $\rho: Z[X_1,X_2,\ldots,X_n]^{\Sigma n} \to A$ be the projection. Let D be the derivation in $Z[X_1,X_2,\ldots,X_n]^{\Sigma n}$ described by $\sum_{i=1}^{n} \partial/\partial X_i$. Divide the image of $Z[X_1^2,X_2^2,\ldots,X_n^2]^{\Sigma n}$ under this derivation by 2, and project into A. This submodule, M, is shown to be the image of the primitives of $H^*(\Omega Sp(n))$ in $H^*(Sp(m)/U(n))$ under a suitable map. Let $\sigma_j(X_1,X_2,\ldots,X_n)$ be the j^{th} elementary symmetric polynomial. Let $S_i(X_1,X_2,\ldots,X_n) = S_i$ be the i^{th} symmetric power, $\sum_{j=1}^{n} X_j^i$. We first demonstrate, as Bott states, that $\{\rho S_{2i-1}\}_{i=1,2,\ldots,n}$ is a basis for M. By Newton's formula, with $\sigma_j(X^2) = \sigma_j(X_1^2,X_2^2,\ldots,X_n^2)$, $S_j(X^2) = S_j(X_1^2,X_2^2,\ldots,X_n^2)$,

$$0 = p(1/2\ D(i\sigma_i(X^2) - \ldots \pm \sigma_j(X^2)\ S_{i-j}(X^2) \mp \ldots \pm S_i(X^2))$$

$$= p\ 1/2\ D\ i\sigma_i(X^2) + p\ 1/2\ D(-1)^i\ S_i(X^2)$$

(since D is a derivation, and symmetric polynomials in $\{X_1^2,X_2^2,\ldots,X_n^2\}$ go to zero under p) =

$$= i\ p\ 1/2\ D\ \sigma_i(X^2) + (-1)^i\ \rho\ S_{2i-1}(X)$$

(since D is defined by $\sum_{i=1}^{n} \partial/\partial X_i$)

"Dividing by i", $p\ 1/2\ D\ \sigma_i(X^2) = (-1)^{i-1}\ \rho\ S_{2i-1}(X)$.

This makes $\{\rho\ S_{2i-1}\}_{i=1,2,\ldots,n}$ a spanning set. There is no need to agonize over the purity of M or whether or not $\{\rho\ S_{2i-1}\}_{i=1,2,\ldots,n}$

is independent in A. Bott's geometrical arguments provide an indirect proof that M is a direct summand of appropriate rank.

We define $P_{2i-1,j}$ to be $\rho\,\sigma_j(X^{2i-1})$, $i = 1,2,\ldots,n$. Note that $P_{2i-1,1} = \rho\,\sigma_1(X^{2i-1}) = \rho\,S_{2i-1}(X)$. If $K_{2i-1,j} = j\,\rho\,\sigma_j(X^{2i-1}) + (-1)^j\,\rho\,S_j(X^{2i-1})$, Newton's formula in $Z[X_1^{2i-1},X_2^{2i-1},\ldots,X_n^{2i-1}]$ guarantees that $K_{2i-1,j} = \sum_{j=k+\ell} P_{2i-1,k}(\ell P_{2i-1,\ell} - K_{2i-1,\ell})$. We must verify that $\rho(S_j(X^{2i-1}))$ is in M for $j \in Z^+ - \{0\}$, $i = 1,2,\ldots,n$. This is trivial if j is even, for $S_j(X^{2i-1}) \in Z[X_1^2,X_2^2,\ldots,X_n^2]^{\Sigma n}$ if j is even. We may suppose $j = 2k+1$. $S_j(X^{2i-1}) = S_1(X^{(2i-1)(2k+1)}) = S_1(X^{4ik+2(i-k)-1})$. But $\rho(1/2\ D\ S_1(X^{4ik+2(i-k)}) = (2ik+(i-k))\,\rho\,S_1(X^{4ik+2(i-k)-1})$. Since $S_1(X^{4ik+2(i-k)}) \in Z[X_1^2,X_2^2,\ldots,X_n^2]^{\Sigma n}$ and M is pure, we are done.

Let us recall that we have yet to apply Theorem 2, and have merely developed an analogy.

Let $A = Z[X_1,X_2,\ldots,X_n]$, $W = \Sigma n$. $\{\sigma_i\}_{i=1,2,\ldots,n}$ are generators for A^W. Let φ be the trivial splitting of $\eta: Z \to A$, so that $\overline{A} = Z[X_1,X_2,\ldots,X_n]/Z[X_1,X_2,\ldots,X_n]^{\Sigma n}$. Let D be the unique extension of $X_i \to iX_i$. $D\,\sigma_i = \sum_{j_1<j_2<\ldots<j_i} (j_1+j_2+\ldots+j_i)\,X_{j_1}\,X_{j_2}\ldots X_{j_i}$ and may be designated the i^{th} elementary weighted polynomial. We let M be the span of the elementary weighted polynomials in $\overline{A}$. Clearly, hypotheses (i) and (ii) of Theorem 2 are satisfied. It remains to verify that M is a pure sub-group of $\overline{A}$. Deferring this for the

moment, we have the following result, by combining Theorem 1 and Theorem 2: If

$$\bar{A} = Z[X_1, X_2, \ldots, X_n]/Z[X_1, X_2, \ldots, X_n]^{\Sigma n} \quad ,$$

and M is the submodule of $\bar{A}$ spanned by the elementary weighted polynomials, then there is a sub-Hopf algebra of $S(\bar{A})$ which has polynomial dual coalgebra structure, and has M as its primitive submodule.

We show now that M is pure in $\bar{A}$. By a homogeneity argument, we quickly reduce the problem to the following:

Lemma: If $X \in Z[X_1, X_2, \ldots, X_n]$ is homogeneous of degree r, and

$$\begin{aligned} iX = \mu \sum_{j_1 < j_2 < \ldots < j_r} (j_1 + j_2 + \ldots + j_r)\, X_{j_1} X_{j_2} \cdots X_{j_r} \\ + \lambda \sigma_r + \Big(\sum_{1 \le i_1 \le n} a_{i_1} X_{i_1} \Big) \sigma_{r-1} + \cdots \qquad (X.1) \\ + \Big(\sum_{1 \le i_1 \le i_2 \le \ldots \le i_s \le n} a_{i_1, i_2, \ldots, i_s} X_{i_1} X_{i_2} \cdots X_{i_s} \Big) \sigma_{r-s} \\ + \ldots + \Big(\sum_{i \le i_1 \le i_2 \le \ldots \le i_{r-1} \le n} a_{i_1, i_2, \ldots, i_{r-1}} X_{i_1} X_{i_2} \cdots X_{i_{r-1}} \Big) \sigma_1 \, , \end{aligned}$$

where i, μ, λ, and $a_I \in Z$, then i divides μ.

Proof: We designate the coefficient of X_I on the right hand side of (X.1) by $C(X_I)$. Clearly i divides $C(X_I)$ for all I, as the monomials are a basis in $Z[X_1, X_2, \ldots, X_n]$.

Let us compute $C(X_{j_1} X_{j_2} \cdots X_{j_r})$ where $j_1 < j_2 < \ldots < j_r$. This is easily seen to be

$$\mu(j_1 + j_2 + \ldots + j_r) + \lambda + \sum_{s_1=1}^{r} a_{j_{s_1}} + \cdots \qquad (X.2)$$

$$+ \sum_{1 \le s_1 < s_2 < \ldots < s_t \le r} a_{j_{s_1}, j_{s_2}, \ldots, j_{s_t}} + \ldots$$

$$+ \sum_{1 \le s_1 < s_2 < \ldots < s_{r-1} \le r} a_{j_{s_1}, j_{s_2}, \ldots, j_{s_{r-1}}} ,$$

and must be divisible by i . We would like to know that $\mu(j_1+j_2+\ldots+j_r) + \lambda$ is divisible by i , for

Sublemma: If $\mu(j_1+j_2+\ldots+j_r) + \lambda$ is a multiple of i for every $J = \{j_1<j_2<\ldots<j_r\}$, then i divides μ .

Proof of Sublemma: We simply choose $J_1 = \{1,2,\ldots,r\}$ and $J_2 = \{1,2,\ldots,r-1,r+1\}$. (Notice, we are disinterested when $r = n$, for $D\sigma_n$ is clearly zero in $\overline{A}$). $\{\mu(1+2+\ldots+r) + \lambda\}$ $- \{\mu(1+2+\ldots+(r-1)+(r+1) + \lambda\} \equiv 0 \pmod{i}$. But this difference is μ . So i divides μ .

We return now to (X.2). We can put ourselves in a position to apply the sublemma if we can add to (X.2) a linear combination of coefficients (each of which is $\equiv 0 \pmod{i}$) of other monomials in the right hand side of (X.1) in such a way as to absorb the summands of (X.2) other than $\mu(j_1+j_2+\ldots+j_r)$ and λ . This can be done as follows. If $\{t_1 < t_2 < \ldots < t_k\} \subseteq \{j_1 < j_2 < \ldots < j_r\}$, we let $s(t_i) = q$ if $t_i = j_q$.

Sublemma:

$$\sum_{\substack{\{t_1<t_2<\ldots<t_k\} \subseteq \{j_1<j_2<\ldots<j_r\} \\ s(t_{\ell+1}) - s(t_\ell) = i_\ell \\ i_1+i_2+\ldots+i_k=r}} (-1)^{r-k} \; C(X_{t_1}^{i_1} X_{t_2}^{i_2} \ldots X_{t_k}^{i_k}) \qquad (X.3)$$

$$= \mu(j_1+j_2+\ldots+j_r) + \lambda .$$

(Notice, we are including (X.2) as a summand in (X.3) in the special case

$$t_\ell = j_\ell,\ i_\ell = 1,\ \ell = 1,2,\ldots,r\ .\ \ ).$$

We forego a proof, as it is quite straightforward. The difficulty of deciding what the appropriate sum of coefficients is has been overcome in the statement of the sublemma.

BIBLIOGRAPHY

[1] J.W. Milnor and J.C. Moore, "On the structure of Hopf algebras," Ann. of Math., 81 (1965), 211-264.

[2] M.E. Sweedler, "Hopf algebras with one grouplike element," Trans. Amer. Math. Soc., 127 (1967), 515-526.

[3] E. Dyer, Cohomology Theories, W.A. Benjamin, New York, 1969.

[4] N. Jacobson, Lectures in Abstract Algebra, V. I., D. Van Nostrand, Princeton, 1951.

[5] P.A. Mac Mahon, Combinatory Analysis, V. II, Chelsea, New York.

[6] N.E. Steenrod, (lectures, written and revised by D.B.A. Epstein) Cohomology Operations, Ann. of Math. Studies, 50, Princeton University Press, Princeton, 1962.

[7] W.-C. Hsiang, "On Wu's formula of Steenrod squares on Stiefel-Whitney classes," Bol. Soc. Mat. Mex., (2), 8, (1963).

[8] L.E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, II," Ann. of Math., (1), 11, (1896-1897), 65-120.

[9] J.C. Moore, "Algèbres de Hopf universelles," Séminaire Henri Cartan, 1959/1960, exposé 10.

[10] D. Husemoller, "The structure of the Hopf algebra $H^*(BU)$ over a $Z_{(p)}$-algebra," Am. J. Math., 93, (1971), 329-349.

[11] D. Husemoller and J.C. Moore, "Algebras, coalgebras, and Hopf algebras," (to appear).

[12] H.S.M. Coxeter and W.O.J . Moser, Generators and Relations for Discrete Groups, Springer, Berlin, 1957.

[13] A. Vasquez, (to appear).

[14] R. Bott, "The space of loops on a Lie group," Mich. Math. J., 5, (1958), 35-61.

AUTOBIOGRAPHY

P. Brian Shay was born in New York City in 1943. He entered Fordham College in New York City in 1960, lured by an invitation to dispense with his last year of school. In 1961 he was awarded a National Merit Scholarship; in 1964, a B.S. in Physics from Fordham College. He was a schoolmaster at Portsmouth Priory School, Portsmouth, R.I., from 1964 to 1966. In 1967, he was awarded an M.A. in Mathematics by Fordham University, at which time he came to The City University to study algebraic topology.

He has published a result, "Discoherently Associative Bifunctors on Groups," in Reports of the Midwest Category Theory Seminar V, edited by J.W. Gray and S. Mac Lane, Springer-Verlag, New York, (1971), at the kind invitation of Professor Saunders Mac Lane. He is on the faculty of Hunter College, The City University of New York.

In December of 1968 he married Karla Neil, an artist. They live in New York City.