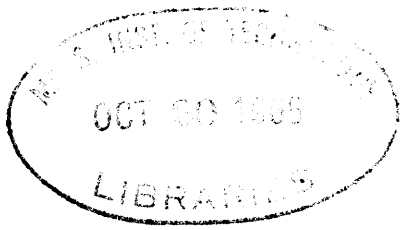


Cocommutative Hopf Algebras with Antipode

by

Moss Eisenberg Sweedler

B.S., Massachusetts Institute of Technology
(1963)

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF
PHILOSOPHY

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

August, 1965

Signature of Author .....
Department of Mathematics, August 31, 1965

Certified by .....
Thesis Supervisor

Accepted by .....
Chairman, Departmental Committee on
Graduate Students

038

Cocommutative Hopf Algebras with Antipode

by

Moss Eisenberg Sweedler

Submitted to the Department of Mathematics on August 31, 1965, in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

Abstract

In the first chapter the preliminaries of the theory of Hopf algebras are presented. The notion and properties of the antipode are developed. An important filtration is induced in the Hopf algebra by its dual when the Hopf algebra is split. It is shown conilpotence and an algebraically closed field insure a Hopf algebra is split. The monoid of grouplike elements is studied.

In the second chapter conditions for an algebra A -- which is a comodule for a Hopf algebra H --to be of the form $A \cong B \otimes H$ (linear isomorphism) are given. The dual situation is studied. The graded Hopf algebra associated with a split Hopf algebra decomposes in the above manner.

Chapter III contains the cohomology theory of a commutative algebra which is a module for a cocommutative Hopf algebra. There is extension theory and specialization to the situation the Hopf algebra is a group algebra.

Chapter IV is dual to chapter III.

Chapter V is devoted to coconnected cocommutative Hopf algebras, mostly in characteristic $p > 0$. There, the notion of divided powers is developed and shown to characterize the coalgebra structure of a class of Hopf algebras. The Hopf algebras are shown to be extensions of certain sub Hopf algebras by their primitive elements.

Thesis Supervisor: Bertram Kostant
Title: Professor of Mathematics

Contents

Introduction 4

Chapter I. Preliminaries 7

Chapter II. Decompositions 36

Chapter III. Cohomology 47

Chapter IV. Cohomology 87

Chapter V. Cocommutative Coconnected Hopf Algebras.. 93

Bibliography 161

Index 162

Biography 166

Introduction

A Hopf algebra as considered herein is simultaneously an algebra and a coalgebra where the algebra structure morphisms are morphisms of the coalgebra structure, (or vice versa). This differs from the graded Hopf algebras of [2] Milnor and Moore, except in characteristic 2. The problem is to determine the structure of cocommutative Hopf algebras.

Our first approach lies in a cohomology theory. We have constructed abelian cohomology groups

$$H^i(H,A) \ , \quad H(C,H)^i \ , \quad 0 \leq i \in Z \ ,$$

where H is a Hopf algebra, A an algebra which is a left "C.H.A." H-module, C a coalgebra which is a right "C.H.A." H-comodule. We then determine the structures of algebras (coalgebras) which are extensions of H (C) by B (H). This theory applies to the algebra structure and the coalgebra structure--separately--of coconnected cocommutative Hopf algebras. We hope to develop an extension theory where the extension is a Hopf algebra and is an extension of one Hopf algebra by another.

Our cohomology theory gives the familiar group cohomology in case $H = \Gamma(G)$ the group algebra of the group G. If A^r is the group of regular (invertible) elements

of A then

$$H^i(H,A) = H^i(G,A^r) .$$

Furthermore, if A is a finite Galois extension of the underlying field k and G is the Galois group of A/k, then the isomorphism classes of extensions of $H = \Gamma(G)$ by A form a subgroup of the Brauer Group.

Kostant has shown--the results are unpublished--that a split cocommutative Hopf algebra with antipode is a smash product of a group algebra and a coconnected cocommutative Hopf algebra; and that in characteristic zero a coconnected cocommutative Hopf algebra is a universal enveloping algebra of the Lie algebra of primitive elements. We present proofs of these results and study coconnected cocommutative Hopf algebras in characteristic $p > 0$. For a certain class (including all where the restricted Lie algebra of primitive elements is finite dimensional) of coconnected cocommutative Hopf algebras we are able to determine the coalgebra structure. The coalgebra structure is described in a generalization of the Poincaré-Birkhoff-Witt theorem. We now outline the generalization.

In characteristic zero let $\{x^\alpha\}$ be an ordered basis for the Lie algebra L, $L \subset U$ its universal enveloping algebra, a Hopf algebra. If

$$x^\alpha_n = \frac{(x^\alpha)^n}{n!} \qquad i = 0,1,2,...$$

then

$$dx_n^{\alpha} = \sum_{i=0}^{n} x_i^{\alpha} \otimes x_{n-i}^{\alpha} \quad .$$

The Poincaré-Birkhoff-Witt theorem is equivalent to:

$$\text{i)} \quad \left\{ x_{e_1}^{\alpha_1} \cdots x_{e_m}^{\alpha_m} \;\middle|\; \begin{array}{l} \alpha_1 < \cdots < \alpha_m \\ m = 0,1,\ldots \\ 0 < e_i \in Z \end{array} \right\}$$

forms a basis for U .

In any characteristic we say

$$x_0, x_1, x_2, \ldots\ldots x_n, \ldots$$

is a sequence of divided powers if

$$dx_n = \sum_{i=0}^{n} x_i \otimes x_{n-i} \quad .$$

We show how ordered products of divided powers--as in i)--form a basis for the certain class of coconnected cocommutative Hopf algebras.

For all coconnected cocommutative Hopf algebras in characteristic $p > 0$, we show the Hopf algebra obtained by factoring out the ideal generated by the primitive elements is isomorphic to a sub Hopf algebra of the original Hopf algebra, when the vector space structure on the quotient is altered. We also show the original Hopf algebra is an extension--as an algebra and coalgebra--of the quotient by the primitively generated sub Hopf algebra.

Chapter I

The study of Hopf algebras is a self-dual theory. For this reason diagram notation is useful, as it makes dual definitions and proofs evident.

For all time we fix the field k which is the base for all vector spaces. If $X_1,\ldots,X_n$ are vector spaces over k, $\mathfrak{S}_n$ the permutation group on n-letters $\sigma \in \mathfrak{S}_n$, we consider

$$\sigma: X_1 \otimes \cdots \otimes X_n \to X_{1\sigma} \otimes \cdots \otimes X_{n\sigma}$$

$$x_1 \otimes \cdots \otimes x_n \to x_{1\sigma} \otimes \cdots \otimes x_{n\sigma} \quad .$$

Often σ will be written $(i_1,\ldots i_n)$ where $\{i_1,\ldots i_n\} = \{1,2,\ldots n\}$; in this case

$$X_1 \otimes \cdots \otimes X_n \xrightarrow{(i_1,\ldots i_n)} X_{i_1} \otimes \cdots \otimes X_{i_n} \quad .$$

If $X_1 = X_2 = \cdots = X_n$, $X_1 \otimes \cdots \otimes X_n$ is a left $\mathfrak{S}_n$-module.

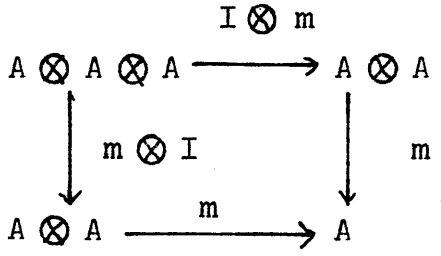
If X, Y are vector spaces "$f: X \to Y$" means f is a linear map from X to Y.

Once we define a "right" object such as module or co-module, we consider the "left" object to be defined with the mirror definition. Similarly for "left" objects.

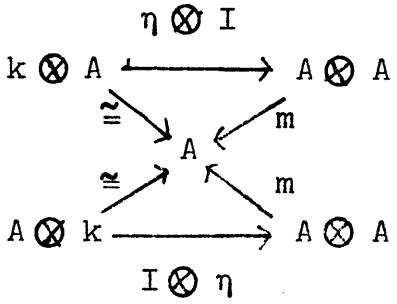
Algebras

(A,m,η) is an algebra (over k) where A is a vector space over k, $m: A \otimes A \to A$, $\eta: k \to A$, if the following diagrams are commutative.

I)



II)



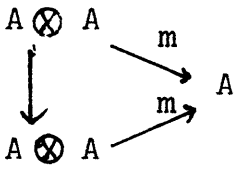
I) is equivalent to associativity.

II) is equivalent to $\eta(1)$, (η) is a <u>unit</u>.

k is an algebra where η is the identity, m is the usual multiplication.

An algebra A is <u>commutative</u> if

(2,1)



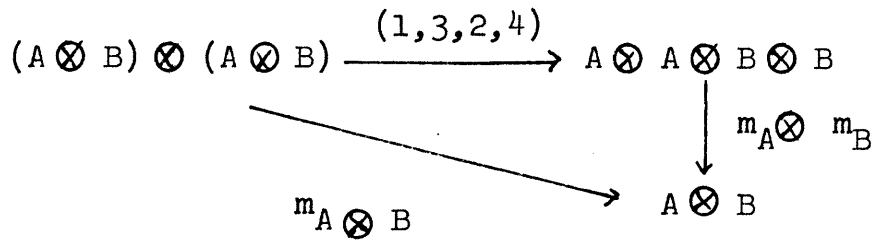
is commutative.

If A is an algebra, X, Y vector spaces $f: X \to Y$ then $k \otimes f: X \to A \otimes Y$

$$x \to 1 \otimes f(x) ,$$

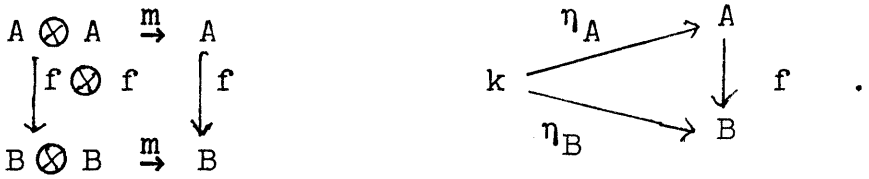
where for an algebra A, $1 \in A$ always denotes $\eta_A(1)$.

If A and B are algebras $A \otimes B$ is an algebra where



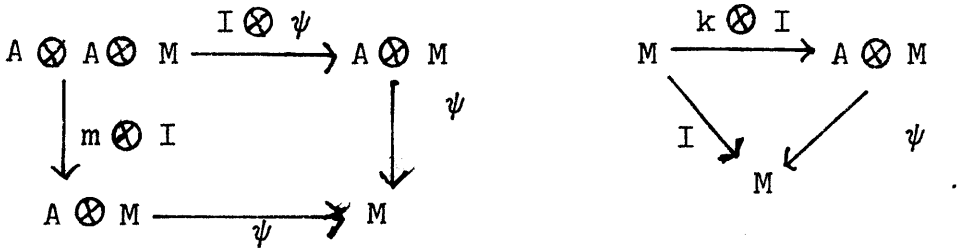
and $\eta_{A \otimes B} = k \otimes \eta_B = \eta_A \otimes k$.

$f: A \to B$ is a <u>morphism of algebras</u> if the following diagrams are commutative:



$k \xrightarrow{\eta_A} A$ will often be written $k \xrightarrow{k} A$.

If A is an algebra a <u>left A-module</u> is a vector space M with a map $\psi: A \otimes M \to M$ satisfying:



If M, N are left A-modules $f: M \to N$ is a <u>morphism of left A-modules</u> if

$$\begin{array}{ccc} A \otimes M & \xrightarrow{\psi_M} & M \\ \downarrow{\scriptstyle I \otimes f} & & \downarrow{\scriptstyle f} \\ A \otimes N & \xrightarrow{\psi_N} & N \end{array}$$

is commutative .

An augmentation ε_A of an algebra A is an algebra morphism $\varepsilon_A : A \to k$. An augmented algebra is an algebra with a fixed augmentation.

If A is an augmented algebra k is a left (or right) A-module by:

$$A \otimes k \xrightarrow{\varepsilon \otimes I} k \otimes k \xrightarrow{m} k \ .$$

If M is a left A-module and N a right A-module $N \otimes_A M$ is a vector space such that

$$N \otimes A \otimes M \xrightarrow{\psi_N \otimes I \,-\, I \otimes \psi_M} N \otimes M \to N \otimes_A M \to 0$$

is an exact sequence of vector spaces.

If A is an augmented algebra, $A^+ = \operatorname{Ker} \varepsilon_A$, M a left A-module, then $k \otimes_A M = \operatorname{Coker} (A^+ \otimes M \xrightarrow[i \otimes I]{} A \otimes M \xrightarrow[\psi]{} M)$, or if $A^+ \cdot M$ denotes $\operatorname{Im}(A^+ \otimes M \xrightarrow[i \otimes I]{} A \otimes M \xrightarrow[\psi]{} M)$

$k \otimes_A M = M/(A^+ \cdot M)$.

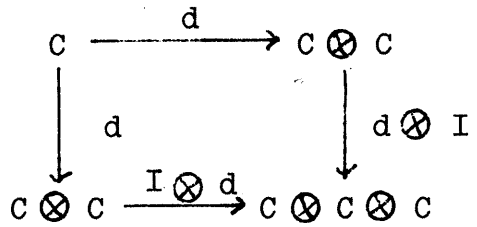
Coalgebras

(C, d, ε) is a coalgebra over k where C is a vector space over k ,

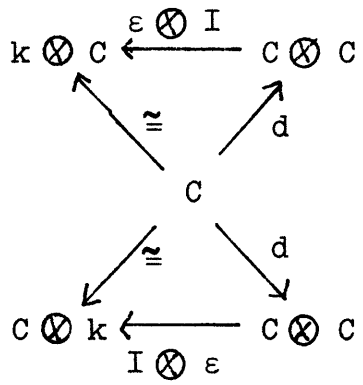
$$d: C \to C \otimes C \qquad \varepsilon: C \to k$$

if the following diagrams are commutative:

I)



II)

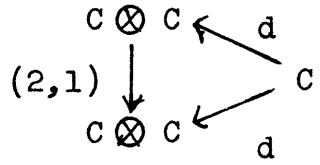


I) is equivalent to coassociativity

II) is equivalent to ε is an <u>augmentation of a coalgebra</u>.

k is a coalgebra where $d = k \otimes I$ and ε = the identity.

A coalgebra is <u>cocommutative</u> if



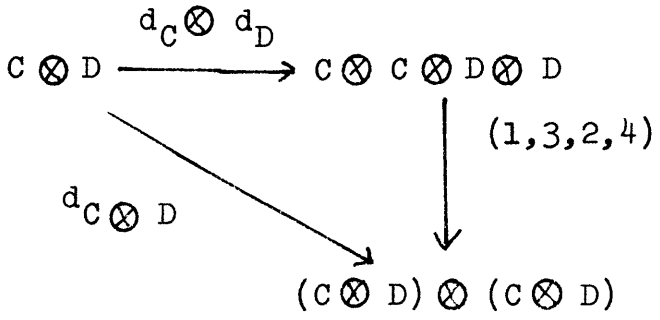
is commutative.

If C is a coalgebra and X, Y are vector spaces $f: X \to Y$, then

$$\varepsilon \otimes f: C \otimes X \to Y$$

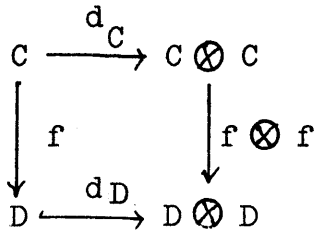
$$C \otimes X \xrightarrow{\varepsilon \otimes f} k \otimes Y \xrightarrow{\cong} Y \quad .$$

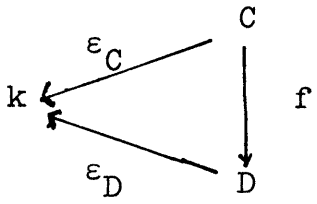
If C, D are coalgebras $C \otimes D$ is a coalgebra where



$$\varepsilon_{C \otimes D} = \varepsilon_C \otimes \varepsilon_D \ .$$

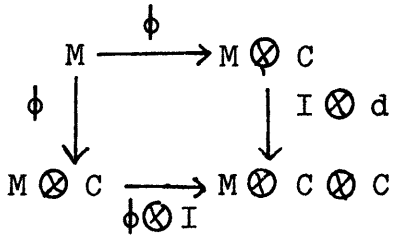
$f: C \to D$ is a <u>morphism of coalgebras</u> if the diagrams,

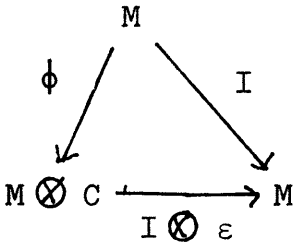




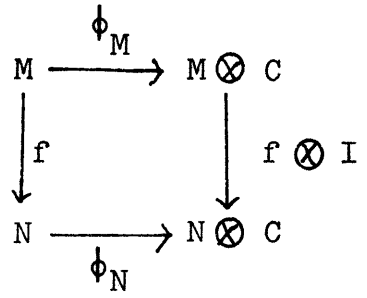
are commutative.

If C is a coalgebra, a <u>right C-comodule</u> is a vector space M with a map $\phi: M \to M \otimes C$ satisfying:





If M, N are right C-comodules $f: M \to N$ is a <u>morphism of right C-comodules</u> if



is commutative.

A unit of a coalgebra C is a coalgebra morphism $\eta_C: k \to C$.

A coalgebra with unit is a coalgebra with a fixed unit.

If C is a coalgebra with unit k is a right (or left) C-comodule where

$$k \underset{d}{\to} k \otimes k \xrightarrow[I \otimes \eta_C]{} k \otimes C \quad .$$

If N is a left C-comodule M a right C-comodule, $M \,\square^C\, N$ is a vector space such that

$$0 \to M \,\square^C\, N \to M \otimes N \xrightarrow{\phi_M \otimes I - I \otimes \phi_N} M \otimes A \otimes N$$

is an exact sequence of vector spaces.

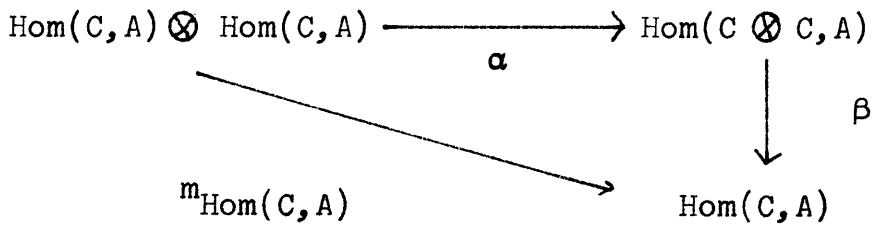
If C is a coalgebra with unit $J_C = \text{Coker } \eta_C$, $\pi: C \to J_C$ then $M \,\square^C\, k = \text{Ker } (M \underset{\phi}{\to} M \otimes C \xrightarrow[I \otimes \pi]{} M \otimes J_C)$.

We shall freely use facts such as kernels and cokernels of comodule morphisms are subcomodules or quotient comodules, when the "dual" fact is well known.

If X, Y are vector spaces

$$\text{Hom}(X,Y) = \{f: X \to Y\} .$$

$\mathrm{Hom}(X,Y)$ is a vector space. Often $\mathrm{Hom}(X,Y)$ carries additional structure, for example if C is a coalgebra and A an algebra then $\mathrm{Hom}(C,A)$ has a natural algebra structure as follows



where $\alpha(f \otimes g) = m_A \circ f \otimes g$ and β is induced by $d: C \to C \otimes C$. Multiplication in $\mathrm{Hom}(C,A)$ will often be denoted by $*$, thus $f * g = m_A \circ f \otimes g \circ d_C$. The unit in $\mathrm{Hom}(C,A)$ is

$$k \to \mathrm{Hom}(C,A)$$
$$\lambda \to \lambda(\eta_A \circ \varepsilon_C) .$$

We let X^* denote $\mathrm{Hom}(X,k)$, as usual we consider $X \subset X^{**}$. We have just shown if X is a coalgebra X^* is an algebra. Consider

$$X^* \otimes X^* \xrightarrow{\alpha} (X \otimes X)^*$$

α as above. α is injective for if $\sum_{i=1}^{n} \lambda_i x_i^* \otimes y_i^* \in X^* \otimes X^*$, we can assume $\{x_i^*\}$ is linearly independent. Then there exists $\{x_i\} \subset X$ where $\langle x_i^*, x_j \rangle = \delta_{i,j}$ and $\{y_i\} \subset X$ where $\langle y_i^*, y_i \rangle = 1$. Thus

$$\langle \alpha(\sum_{i=1}^{n} \lambda_i x_i^* \otimes y_i^*) , x_j \otimes y_j \rangle = \lambda_j$$

which shows α is injective. If X is finite dimensional $\dim(X^* \otimes X^*) = (\dim X)^2 = \dim(X \otimes X)^*$ which shows in this case α is an isomorphism. We identify $X^* \otimes X^*$ with its image under α in $(X \otimes X)^*$. If X is finite dimensional $(X \otimes X)^* = X^* \otimes X^*$.

Suppose A is a finite dimensional algebra; then $\eta: k \to A$ $m: A \otimes A \to A$ induce transpose mappings:

$$\varepsilon = {}^t\eta: A^* \to k^* = k , \quad d = {}^t m: A^* \to (A \otimes A)^* = A^* \otimes A^* .$$

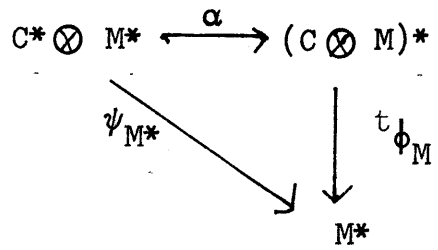
With these maps A^* is a coalgebra. Similarly if A is a finite dimensional coalgebra A^* is an algebra; however, this is the same algebra structure as deduced above.

If X, Y are vector spaces

$$\alpha: X^* \otimes Y^* \to (X \otimes Y)^*$$

$$\langle \alpha(x^* \otimes y^*), x \otimes y \rangle = \langle x^*, x \rangle \langle y^*, y \rangle \qquad \begin{matrix} x \in X, \ y \in Y \\ x^* \in X^*, \ y^* \in Y^* . \end{matrix}$$

α is injective. (We proved this, above, for $Y = X$, the same proof works.) Identify $X^* \otimes Y^*$ with its image under α in $(X \otimes Y)^*$. If M is a left C-comodule, C a coalgebra then



defines ψ_{M^*} , and this gives M^* the structure of a left C^*-module. Similarly if, A is a finite dimensional algebra, M a left A-module by

$$A \otimes M \xrightarrow{\psi_M} M$$

then ${}^t\psi_M\colon M^* \to (A \otimes M)^* = A^* \otimes M^*$ defines a left A^*-comodule structure on M^* .

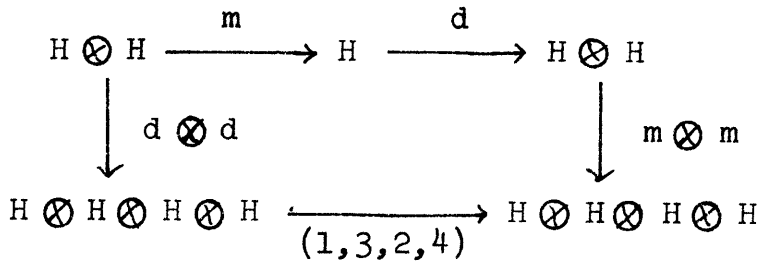
Hopf Algebras

(H,m,η,d,ε) is a Hopf algebra when

1) (H,m,η) is an algebra with augmentation ε ,

2) (H,d,ε) is a coalgebra with unit η ,

3) the diagram



is commutative.

3) and "η is a unit for the coalgebra (H,d,ε)" is equivalent to "$d:H \to H \otimes H$ is an algebra morphism".

3) and "ε is an augmentation for the algebra (H,m,η)" is equivalent to "$m: H \otimes H \to H$ is a coalgebra morphism".

Since a Hopf algebra H is a coalgebra and algebra $\mathrm{Hom}(H,H)$ has the structure of an algebra. H^* has an algebra structure and if H is finite dimensional H^* has a coalgebra structure, as well. In this case H^* is a Hopf algebra.

In $\mathrm{Hom}(H,H)$ $\eta \circ \varepsilon$ is the unit. We shall often consider $k = k \cdot 1 \subset H$ so ε will denote the unit in $\mathrm{Hom}(H,H)$. The identity $I: H \to H$ is an element of $\mathrm{Hom}(H,H)$. $S \in \mathrm{Hom}(H,H)$ is an <u>antipode</u> for H if $I * S = \varepsilon = S * I$, that is S is the inverse to I.

<u>Example:</u>

Let G be a monoid (group without inverses). $\Gamma(G)$ = the "monoid" algebra = $\bigoplus_{g \in G} k \cdot g$ where

$$\left(\sum_{i=1}^{n} \lambda_i g_i\right)\left(\sum_{j=1}^{m} \lambda_j g_j\right) = \sum_{i,j=1}^{n,m} \lambda_i \lambda_j g_i g_j .$$

$\Gamma(G)$ is an algebra where

$$\eta: k \to \Gamma(G)$$

$$\lambda \to \lambda \cdot e \ .$$

$\Gamma(G)$ is a Hopf algebra where

$$d: \Gamma(G) \to \Gamma(G) \otimes \Gamma(G)$$

$$g \to g \otimes g$$

$$\varepsilon: \Gamma(G) \to k$$

$$g \to 1 \ .$$

$\Gamma(G)$ has an antipode if and only if G is a group. Suppose G is a group define $S: \Gamma(G) \to \Gamma(G)$

$$g \to g^{-1}$$

then S is an antipode. If S is an antipode,

$e = 1 = I * S(g) = gS(g)$, where $S(g) = \sum_{i=1}^{n} \lambda_i g_i$ which implies $S(g) = g^{-1}$, hence G has inverses and is a group.

We now show that if H has an antipode, S , then

(1)

1) $d \circ S = (2,1) \circ S \otimes S \circ d$

2) $S \circ m = m \circ S \otimes S \circ (2,1)$

3) $\varepsilon \circ S = S \circ \varepsilon = \varepsilon$

4) If H is commutative (as an algebra) or cocommutative (as a coalgebra) then $S^2 = S \circ S = I$.

We prove 1) as follows:

$d \circ S$, $(2,1) \circ S \otimes S \circ d \in \mathrm{Hom}(H, H \otimes H)$ which is an algebra. $d \in \mathrm{Hom}(H, H \otimes H)$ we show $d \circ S$ is a left inverse to d and $(2,1) \circ S \otimes S \circ d$ is a right inverse

to d . This proves they are equal. We shall use the following: If C, D are coalgebras, A, B are algebras, $f: C \to D$ a coalgebra morphism, $h: A \to B$ an algebra morphism and $g_1, g_2 \in \mathrm{Hom}(D,A)$ then

$$(h \circ g_1 \circ f) * (h \circ g_2 \circ f) = h \circ (g_1 * g_2) \circ f \ .$$

The proof is clear from the definitions.

Consider

$$(d \circ S) * d = d \circ (S * I) = d \circ \varepsilon = k \otimes \varepsilon$$

$(d \circ \varepsilon = d$ because $d(1) = 1 \otimes 1)$.

We let $m^n = m \circ m \otimes I \circ \cdots \circ m \otimes \underbrace{I \otimes \cdots \otimes I}_{n-1}$,

by associativity m^n is independent of the order of the m's . Similarly we let $d^n = d \otimes \underbrace{I \otimes \cdots \otimes I}_{n-1} \circ \cdots \circ d \otimes I \circ d$,

d^n is independent of the order of the d's by coassociativity. If $h \in H$ we often let

$$\sum_i h_i' \otimes h_i'' \otimes \cdots \otimes h_i^{(n+1)} = d^n h \ .$$

Then

$$d * [(2,1) \circ S \otimes S \circ d](h) = \sum_i h_i' S(h_i^{(4)}) \otimes h_i'' S(h_i''')$$

$$\uparrow \quad I * S = \varepsilon$$

$$= \sum_i h_i' S(h_i''') \otimes \varepsilon(h_i'')$$

$$\uparrow \quad f * \varepsilon = f$$

$$= \sum_i h_i' S(h_i'') \otimes 1 = \varepsilon(h) \otimes 1 \ ,$$

$$\uparrow$$

$$I * S = \varepsilon$$

which verifies 1) .

For 2) we show $S \circ m$ is left inverse to m and $m \circ S \otimes S \circ (2,1)$ is right inverse.

$$(S \circ m) * m = (S * I) \circ m = \varepsilon \circ m = \varepsilon \otimes \varepsilon \ .$$

$$m * [m \circ S \otimes S \circ (2,1)](h \otimes g) = \sum_{i,j} h_i' g_j' \, S(g_j'') S(h_i'')$$

$$= \sum_i h_i' \varepsilon(g) S(h_i'') = \sum_i \varepsilon(g) h_i' \, S(h_i'') = \varepsilon(g)\varepsilon(h) \ .$$

For 3) $\varepsilon = \varepsilon \circ I * S = (\varepsilon \circ I) * (\varepsilon \circ S) = \varepsilon * \varepsilon \circ S$

$$= \varepsilon \circ S$$

and $\varepsilon = I * S \circ \varepsilon = (I \circ \varepsilon) * (S \circ \varepsilon) = \varepsilon * S \circ \varepsilon = S \circ \varepsilon \ .$

For 4) suppose H is commutative so

$$m \circ S \otimes S = m \circ S \otimes S \circ (2,1) = S \circ m \ .$$

Then $S * S^2(h) = \sum_i S(h_i') S^2(h_i'') = \sum_i S(h_i' \, S(h_i''))$

$$= S \circ \varepsilon(h) = \varepsilon(h)$$

which shows S^2 is right inverse to S , so $S^2 = I$. If H is cocommutative $S \otimes S \circ d = (2,1) \circ S \otimes S \circ d = d \circ S \ .$

$$S * S^2(h) = \sum_i S(h_i') S^2(h_i'') = m \circ I \otimes S(\sum_i S(h_i') \otimes S(h_i''))$$

$$= m \circ I \otimes S \, (\sum_j [S(h)]_j' \otimes [S(h)]_j'')$$

$$= I * S \circ S(h) = \varepsilon \circ S(h) = \varepsilon(h) ,$$

which shows S^2 is right inverse to S hence $S^2 = I$.

H as an H*-module

We have H , H^* , $H^{**} \supset H$, we define a left action of H^* on H^{**} ; under this action H is a submodule. We then concern ourselves with the action of H^* on H .

Consider H^{**} a left H^*-module by

$$\langle a^*, b^* \cdot h^{**} \rangle = \langle a^* * b^*, h^{**} \rangle .$$

Then if $h^{**} = h \in H$, $dh = \sum_i h_i' \otimes h_i''$

$$b^* \cdot h = \sum_i h_i' \langle b^*, h_i'' \rangle \in H \subset H^{**} .$$

This shows H is a submodule of H^{**} and explicitly gives the action of H^* on H . We consider H as a left H^*-module. (We could have begun with H^{**} as a right H^*-module by $\langle b^*, h^{**} \cdot a^* \rangle = \langle a^* * b^*, h^{**} \rangle$. Again H would be a submodule where

$$h \cdot a^* = \sum_i \langle a^*, h_i' \rangle h_i'' \in H .$$

Then properties of the left representation of H^* on H have corresponding "mirror" properties to the right representation.)

H is called <u>split</u> if as a left and right H^*-module all simple submodules are 1-dimensional. We give a

criterion for H to be split. Let $g: H \to H \otimes H$

$$g = [(1,2) - (2,1)] \circ d \ .$$

Define subspaces $X_i \subset H$, $X_1 = \operatorname{Ker} g$.

$$g_i = (H \xrightarrow[1]{g} H \otimes H \xrightarrow[2]{\varepsilon \otimes g} H \otimes H \xrightarrow[3]{\varepsilon \otimes g} \cdots \xrightarrow[i]{\varepsilon \otimes g} H \otimes H) \ ;$$

$$X_i = \operatorname{Ker} g_i \ .$$

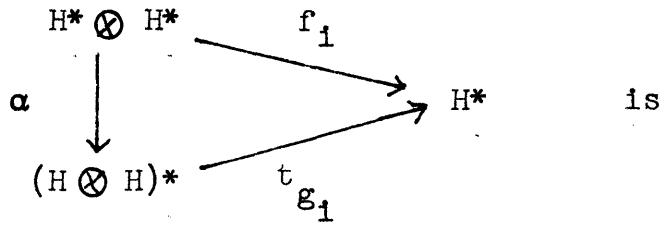
Then $X_1 \subset X_2 \subset \cdots$. We call H <u>conilpotent</u> if $\bigcup_{i=1}^{\infty} X_i = H$.

Observe if H is cocommutative $X_1 = H$. Let

$$f = m \circ [(1,2) - (2,1)]: H^* \otimes H^* \to H^*$$

$$f_i = (H^* \otimes H^* \xrightarrow[i]{k \otimes f} H^* \otimes H^* \xrightarrow[i-1]{k \otimes f} \cdots \xrightarrow[2]{k \otimes f} H^* \otimes H^* \xrightarrow[1]{f} H^*)$$

then



is commutative. Thus

$$\operatorname{Im} f_i \subset \operatorname{Im}({}^t g_i) \subset (\operatorname{Ker} g_i)^{\perp} = X_i^{\perp} \ .$$

If $\cup X_i = H$ then $\cap X_i^{\perp} = \{0\}$ so $\cap \operatorname{Im} f_i = \{0\}$. We have proved: H is conilpotent implies H^* is a nilpotent Lie algebra under $[\ ,\ ]$. (Where $[x^*,y^*] = x^*y^* - y^*x^* = f(x^* \otimes y^*)$). We know if k is algebraically closed and

H^* is nilpotent as a Lie algebra then any finite dimensional simple H^*-module (left or right) is 1-dimensional. (Proved in Lie Algebras, [2] , Corollary page 41.) If $M \subset H$ is a simple submodule then M is cyclic; i.e., $M = H^* \cdot h$ where $0 \neq h \in M$. If $dh = \sum_{i=1}^{n} h_i' \otimes h_i''$ $a^* \cdot h = \sum_{i=1}^{n} h_i' \langle a^*, h_i'' \rangle$ which shows $M \subset$ the space spanned by $\{h_i'\}_{i=1}^{n}$ and any cyclic--hence simple--submodule of H, is finite dimensional. Thus if k is algebraically closed and H is conilpotent H is split.

Suppose H is conilpotent, we do not assume k is algebraically closed, then since H is the union of its cyclic submodules--hence of finite dimensional submodules--it follows, from [2] theorem 5 page 40, as a left H^*-module

$$H = \bigoplus_{\alpha \in \mathcal{A}} H^\alpha \quad , \qquad H^\alpha \text{ submodules;}$$

and for $a^* \in H^*$ as a transformation on any finite dimensional submodule of H^α, the minimal polynomial is the prime polynomial $P(\alpha, a^*)$ to some power. If H is also split any of the prime polynomials must be of the form $P(\alpha, a^*) = X - \lambda(\alpha, a^*)$ where $\lambda(\alpha, a^*) \in k$. We shall show that within H^α there is precisely one simple submodule, and a unique element g_α in this simple submodule where $dg_\alpha = g_\alpha \otimes g_\alpha$ and $\lambda(\alpha, a^*) = \langle a^*, g_\alpha \rangle$.

Assume only that H is a split Hopf algebra. If $y \in H$ where $dy = y \otimes y$ then $H^* \cdot y = k \cdot y$ is a simple submodule. Note $\varepsilon(y) = 1$ because $y = \varepsilon * I(y) = \varepsilon(y)y$. Suppose $M \subset H$ is a simple submodule, $0 \neq y \in M$. $dy = \sum_{i=1}^{n} y_i' \otimes y_i''$ we can assume $\{y_i''\}$ is linearly independent; M is one dimensional and $\{y_i'\} \subset M$ implies $dy = y' \otimes y''$; $I = I * \varepsilon$ implies $y' \varepsilon (y'') = y$ and $\varepsilon(y'') \neq 0$. Similarly $\varepsilon(y')y'' = y$ and $\varepsilon(y') \neq 0$. $\varepsilon * \varepsilon = \varepsilon$ implies $\varepsilon(y) = \varepsilon(y')\varepsilon(y'') \neq 0$. Thus

$$dy = \frac{y}{\varepsilon(y'')} \otimes \frac{y}{\varepsilon(y')} = \frac{y}{\varepsilon(y)} \otimes y \quad \text{and}$$

$$d\,\frac{y}{\varepsilon(y)} = \frac{y}{\varepsilon(y)} \otimes \frac{y}{\varepsilon(y)} .$$ An element $g \in H$ is <u>grouplike</u> if $dg = g \otimes g$. We have just shown a simple submodule M of a split Hopf algebra contains a unique grouplike element which is $\frac{y}{\varepsilon(y)}$ for any $0 \neq y \in M$. Conversely if g is grouplike $\varepsilon(g) = 1$ and $H^* \cdot g$ is simple.

Let $G(H) = G = \{\text{grouplike elements of } H\}$. Then we have shown there is a bijective correspondence between G and the simple submodules of H. We observe the homological interpretation of G is as the set of coalgebra morphisms from k to H, since $g \in G$ corresponds to $\gamma_g(1)$ where

$$\gamma_g : k \to H \quad \text{is a coalgebra morphism.}$$

Note for $g \varepsilon G$ the minimal polynomial for $a^* \varepsilon H^*$ as an operator on $H^* \cdot g$ is $X - \langle a^*, g\rangle$. Thus when H is conilpotent as well as split (so $H = \bigoplus_{\alpha \varepsilon \mathcal{A}} H^\alpha$) if $M^\alpha \subset H^\alpha$ is simple and g_α the unique grouplike element in M^α then $dg_\alpha = g_\alpha \otimes g_\alpha$ and the minimal polynomial of a^* restricted to M^α is $X - \langle a^*, g_\alpha\rangle$.

This shows $\lambda(\alpha, a^*) = \langle a^*, g_\alpha\rangle$ because the minimal polynomial of a^* restricted to M^α is also $X - \lambda(\alpha, a^*)$. If $\tilde{M}^\alpha$ were a second simple submodule of H^α and $\tilde{g}_\alpha$ the grouplike element of $\tilde{M}^\alpha$ then similarly:

$$\langle a^*, \tilde{g}_\alpha\rangle = \lambda(\alpha, a^*) \quad (= \langle a^*, g_\alpha\rangle)$$

which implies $\tilde{g}_\alpha = g_\alpha$ and $\tilde{M}^\alpha = M^\alpha$. Thus for a conilpotent split Hopf algebra H

$$H = \bigoplus_{g \varepsilon G} H^g$$

and the minimal polynomial of a^* acting on a finite dimensional submodule of H^g is a power of $X - \langle a^*, g\rangle$.

Again we just assume H is split. We show G is a linearly independent set. If G is not linearly independent there is a minimal relation $\sum_{i=1}^{n} \lambda_i g_i = 0$, $(n \geq 2)$ where $g_i \varepsilon G$ are distinct $\lambda_i \varepsilon k$. By the minimality of n $g_2, g_3, \ldots g_n$ are linearly independent. Choose $a^* \varepsilon H^*$ where $\langle a^*, g_2\rangle = 1$, $\langle a^*, g_i\rangle = 0$ $i=3,\ldots n$.

Then $\lambda_1\langle a^*, g_1\rangle = -\sum_{i=2}^{n} \lambda_i\langle a^*, g_i\rangle = -\lambda_2$

$$0 = a^* \cdot 0 = a^* \cdot \left(\sum_{i=1}^{n} \lambda_i g_i\right) = \sum_{i=1}^{n} \lambda_i g_i\langle a^*, g_i\rangle$$

$$= -\lambda_2 g_1 + \lambda_2 g_2 = \lambda_2(g_2 - g_1) \ .$$

This implies $\lambda_2 = 0$ or $g_1 = g_2$ which contradicts the minimality of n . Observe if $g, h \in G$ $d(gh) = (dg)(dh) = (g \otimes g)(h \otimes h) = gh \otimes gh$. Thus G is a monoid and since it is a linearly independent set in H , the space spanned by $G \cong \Gamma(G)$, as an algebra. We consider $\Gamma(G) \subset H$.

If H has an antipode S , $g \in G$ then $dS(g) = (2,1) \circ S \otimes S \circ dg = S(g) \otimes S(g)$ so that $S(g) \in G$.

$$gS(g) = I * S(g) = \varepsilon(g) = 1 \ ;$$

so $S(g)$ is the inverse to g in G and G is a group.

Filtration of H

We exhibit a natural filtration on H which is exhaustive when H is split. The multiplication and diagonal map respect the filtration as does an antipode when present. The filtration leads to a graded Hopf algebra. It is also an invaluable basis for induction.

Within H^* let $J = \Gamma(G)^{\perp}$. It is a straight forward verification that for any subcoalgebra $C \subset H$

$(dC \subset C \otimes C \subset H \otimes H)$ $C^{\perp}$ is a 2-sided ideal in H^*. Thus J is a 2-sided ideal in H^*. Define

$$H_i = (J^{i+1})^{\perp} \qquad i=0,1,\ldots .$$

We assume H is split and wish to verify:

1) $H = \cup H_i$

2) $H_i H_j \subset H_{i+j}$

3) $dH_i \subset \sum_{m+n=i} H_m \otimes H_n$.

(2) We show $H_i = \{h \in H \mid J^{i+1} \cdot h = 0\}$.

$\subset$: let $x \in H_i$, $b^* \in J^{i+1}$ a 2-sided ideal, thus for any $a^* \in H^*$ $a^* * b^* \in J^{i+1}$ and

$$\langle a^* * b^*, x\rangle = 0 \ . \qquad \text{But}$$

$$\langle a^* * b^*, x\rangle = \langle a^*, b^* \cdot x\rangle ,$$

implies $b^* \cdot x = 0$.

$\supset$: let $x \in \{h \in H \mid J^{i+1} \cdot h = 0\}$ $b^* \in J^{i+1}$, then $\langle b^*, x\rangle = \langle \varepsilon * b^*, x\rangle = \langle \varepsilon, b^* \cdot x\rangle = 0$; and we are done.

$H^* \otimes H^*$ is "dense" in $(H \otimes H)^*$ in that if $0 \neq z \in H \otimes H$ there is $z^* \in H^* \otimes H^*$ where $\langle z^*, z\rangle \neq 0$. In fact there is $a^* \otimes b^* \in H^* \otimes H^*$, $a^*, b^* \in H^*$ where $\langle a^* \otimes b^*, z\rangle \neq 0$. Thus to

(3) prove $\underline{d(a^* \cdot h) = \Sigma\, h_i' \otimes a^* \cdot h_i''}$ we need

only show $\langle b^* \otimes c^*, d(a^* \cdot h)\rangle = \langle b^* \otimes c^*, \Sigma\, h_i' \otimes a^* \cdot h_i''\rangle$. The left hand side is

$$\langle b^* * c^*, a^* \cdot h\rangle = \langle (b^* * c^*) * a^*, h\rangle$$

$$= \langle b^* * (c^* * a^*), h\rangle = \sum_i \langle b^*, h_i'\rangle\langle c^* * a^*, h_i''\rangle$$

$$= \sum_i \langle b^*, h_i'\rangle\langle c^*, a^* \cdot h_i''\rangle$$

which is the right hand side.

Thus if $\psi\colon H^* \otimes H \to H$ is the left action we have proved

$$\begin{array}{ccc} H^* \otimes H & \xrightarrow{\psi} & H \\ \downarrow{\scriptstyle I \otimes d} & & \\ H^* \otimes H \otimes H & & \downarrow{\scriptstyle d} \\ \downarrow{\scriptstyle (2,1,3)} & & \\ H \otimes H^* \otimes H & \xrightarrow[I \otimes \psi]{} & H \otimes H \end{array}$$

commutative.

To prove $H = \cup H_i$ we proceed by induction on $n = \dim(h \cdot H^*)$ showing $h \in H_{n-1}$. If $n = 1$ then $h = \lambda g$ $g \in G$ $\lambda \in k$, whence $h \in \Gamma(G) = H_0$. Suppose $\dim(h \cdot H^*) = n > 1$, choose a basis for $h \cdot H^*$ as follows: H is split so there is $g \in G$, $g \in h \cdot H^*$, let $x_1 = g$ extend to a basis $x_1, \ldots x_n$ for $h \cdot H^*$. Then

$$dh = \sum_{i=1}^{n} h_i' \otimes x_i \quad ;$$

for suitable $\{h_i'\} \subset H$. If $a^* \in J$,

$da^* \cdot h = \sum_{i=1}^{n} h_i' \otimes a^* \cdot x_i = \sum_{i=2}^{n} h_i' \otimes a^* \cdot x_i$. Thus

$\dim((a^* \cdot h) \cdot H^*) \leq n - 1$ and by induction $a^* \cdot h \in H_{n-2}$.

By (2) this shows $h \in H_{n-1}$.

To prove $dH_i \subset \sum_{n+m=i} H_n \otimes H_m$ we deduce from:

$$\begin{cases} H^* \otimes H^* \xrightarrow{m} H^* \quad m = {}^t d \mid H^* \otimes H^* \\ H_i = (J^{i+1})^{\perp} \\ m\Big(\sum_{n+m=i+1} J^n \otimes J^m\Big) \subset J^{i+1} \\ (\text{where } J^0 = H^*) \end{cases}$$

that

$$d(H_i) \subset \Big(\sum_{n=0}^{i+1} J^n \otimes J^{i+1-n}\Big)^{\perp}$$

$$= \bigcap_{n=0}^{i+1} (J^n \otimes J^{i+1-n})^{\perp}$$

$$= (H \otimes H_i) \cap (H \otimes H_{i-1} + H_0 \otimes H) \cap (H \otimes H_{i-2} + H_1 \otimes H) \cap \cdots$$

$$\cdots \cap (H \otimes H_0 + H_{i-1} \otimes H) \cap H_i \otimes H$$

$$= \sum_{n=0}^{i} H_n \otimes H_{i-n} .$$

Thus $d: H \to H \otimes H$ is a morphism of filtered algebras since the natural filtration on $H \otimes H$ induced by H is $(H \otimes H)_i = \sum_{n=0}^{i} H_n \otimes H_{i-n}$.

We show $H_iH_j \subset H_{i+j}$ by induction on $i + j$. When $i + j = 0$, $H_0 = i(G)$ which is closed under multiplication. Suppose the result is true for smaller $i + j$.

$$dH_i \subset H_0 \otimes H_i + H_1 \otimes H_{i-1} + \cdots + H_i \otimes H_0$$

$$dH_j \subset H_0 \otimes H_j + \cdots\cdots\cdots + H_j \otimes H_0$$

d is an algebra morphism

thus

$$dH_iH_j \subset H_0 \otimes H + H \otimes H_0 + H_{i+j-1} \otimes H_{i+j-1} \cdot$$

This implies $J \cdot H_iH_j \subset H_{i+j-1}$ and by

(2) $H_iH_j \subset H_{i+j}$. Thus $m: H \otimes H \to H$ respects the filtration.

If S is an antipode for H $S(G) \subset G$ so $S(H_0) \subset H_0$. By induction suppose for $n < i$

$$S(H_n) \subset H_n$$

$$dH_i \subset H_i \otimes H_0 + H_{i-1} \otimes H_1 + \cdots + H_0 \otimes H_i$$

by $(2,1) \circ S \otimes S \circ d = d \circ S$ and induction

$$dS(H_i) \subset H_0 \otimes H + H \otimes H_0 + H_{i-1} \otimes H_{i-1} \cdot$$

This implies $J \cdot S(H_i) \subset H_{i-1}$ and by

(2) $S(H_i) \subset H_i$.

If k is filtered by $k = k_0$, then $\eta: k \to H$, $\varepsilon: H \to k$ respect filtration. Thus we can pass to

$$\overline{H} = gr(H) = \bigoplus_{i=0}^{\infty} \overline{H}_i \quad \text{where} \quad \overline{H}_0 = H_0$$

$\overline{H}_i = H_i/H_{i-1}$ $i=1,2,\ldots$ which is a Hopf algebra over $\overline{k} = k_0 = k$. If H has an antipode then so does $\overline{H}$.

When H is conilpotent as well as split $H = \bigoplus_{g \in G} H^g$, H^g submodules of H under the left action of H^* . The minimal polynomial of any $a^* \in H^*$ acting on a finite dimensional submodule of H^g is a power of $X - \langle a^*, g\rangle$. H^g is a submodule implies $dH^g \subset H^g \otimes H$. We wish to show $dH^g \subset H^g \otimes H^g$, this follows from when we show $dH^g \subset H \otimes H^g$.

If $\psi: H^* \otimes H \to H$ is the left action consider $H \otimes H$ as a left H^*-module by

$$H^* \otimes H \otimes H \xrightarrow{(1,3,2)} H \otimes H^* \otimes H \xrightarrow{I \otimes \psi} H .$$

$H \otimes H$ decomposes as $H \otimes H = \bigoplus_{g \in G} H \otimes H^g$ where $H \otimes H^g$ is a submodule and the minimal polynomial of $a^* \in H^*$ acting on a finite dimensional submodule of $H \otimes H^g$ is a power of $X - \langle a^*, g\rangle$. To show $dH^g \subset H \otimes H^g$ it suffices to show for any $x \in H^g$, $a^* \in H^*$ the minimal polynomial of a^* acting on $H^* \cdot dx$ is a power of $X - \langle a^*, g\rangle$.

$$H^* \cdot dx = \sum_i x_i' \otimes H^* \cdot x_i'' = dH^* \cdot x \quad \text{by} \qquad (3).$$

If $b^* = a^* - \langle a^*, g\rangle$

$$b^{*n} \cdot H^* \cdot dx = b^{*n} dH^* \cdot x = db^{*n} \cdot H^* \cdot x = 0$$

for suitably large n ; since $x \in H^g$ implies

$b^{*n} \cdot H^* \cdot x = 0$ for large n .

Thus $dH^g \subset H^g \otimes H \cap H \otimes H^g = H^g \otimes H^g$ and H^g is a subcoalgebra of H .

For any subset $X \subset H$ let

$$X_n = X \cap H_n .$$

We show by induction on $n + m$, $H_n{}^g H_m{}^h \subset H^{gh}$. Clear for $n + m = 0$ because $H_0{}^g = k \cdot g$, $H_0{}^h = k \cdot h$. Suppose the result is true for smaller values of $n + m$.

$$dH_n{}^g \subset H_0{}^g \otimes H_n{}^g + \cdots + H_n{}^g \otimes H_0{}^g$$

$$dH_m{}^h \subset H_0{}^h \otimes H_m{}^h + \cdots + H_m{}^h \otimes H_0{}^h$$

by induction

$$dH_n{}^g H_m{}^h \subset H_0{}^{gh} \otimes H + H \otimes H_0{}^{gh} + H_{n+m-1}^{gh} \otimes H_{n+m-1}^{gh} .$$

Thus if $x \in H_n{}^g H_m{}^h$, $a^* \in H^*$

$$(a^* - \langle a^*, gh \rangle) \cdot x \in H^{gh}$$

and the minimal polynomial of a^* acting on $H^* \cdot x$ is a power of $X - \langle a^*, gh \rangle$. Hence $H^g H^h \subset H^{gh}$. In particular $H^1 = H^e$ is a subalgebra as well as subcoalgebra, thus H^e is a sub Hopf algebra. If H has an antipode S , a similar induction to that showing $H_n{}^g H_m{}^h \subset H^{gh}$ shows $S(H^g) \subset H^{S(g)} = H^{g^{-1}}$, thus $S(H^e) \subset H^e$ and $S|H^e$ is the antipode for H^e .

As another application of the filtration we characterize

when elements of the algebra $\mathrm{Hom}(H,B)$ are regular (invertible); where H is a split Hopf algebra and B an algebra. If B^r is the group of regular elements of B then $f \in \mathrm{Hom}(H,B)$ is regular if and only if $f(G) \subset B^r$.

(4) Suppose f is regular with inverse f^{-1}, then $1 = \varepsilon(g) = f(g)\, f^{-1}(g) = f * f^{-1}(g)$ for any $g \in G$ and hence $f(G) \subset B^r$. Conversely suppose $f(G) \subset B^r$ we construct f^{-1} by defining it on H_0 and extending it to H by induction. For $g \in H_0 = \Gamma(G)$ let $f^{-1}(g) = (f(g))^{-1}$, thus f^{-1} is defined on H_0. Suppose by induction f^{-1} is defined on H_{n-1}; we wish to extend it to H_n. Let $a \in H_n$

$$da = \sum_{i_0=1}^{m} g_{i_0}' \otimes a_{i_0}'' + \sum_{i_1} a_{i_1}' \otimes a_{i_1}'' + \cdots + \sum_{i_n} a_{i_n}' \otimes a_{i_n}''$$

$$\varepsilon \qquad\qquad \varepsilon \qquad\qquad\qquad \varepsilon$$

$$H_0 \otimes H_n \qquad H_1 \otimes H_{n-1} \qquad\qquad H_n \otimes H_0$$

where $g_{i_0}' \in G$. $\varepsilon * I(a) = a$ implies

$$\sum_{i_0=1}^{m} a_{i_0}'' \equiv a \pmod{H_{n-1}};$$

thus it suffices to define $f^{-1}(a_{i_0}'')$ $i_0 = 1, \ldots m$.

If $\{a^*_j\} \subset H^*$ where $\langle a^*_j, g_{i_0}' \rangle = \delta_{j,i_0}$ then under the right action of H^* on H

$$a \cdot a^*_j \equiv a_{i_0}'' \pmod{H_{n-1}}$$

and it suffices to define $f^{-1}(a \cdot a^*_j)$ $\quad j=1,\dots m$.

$$d(a \cdot a^*_j) = \sum_{i_0=1}^{m} g_{i_0}' \cdot a^*_j \otimes a_{i_0}'' + \cdots + \sum_{i_n} a_{i_n}' \cdot a^*_j \otimes a_{i_n}''$$

$$= g_j' \otimes a_j'' + X \ , \quad X \in H_n \otimes H_{n-1} \ .$$

$$\varepsilon * I(a \cdot a^*_j) = a \cdot a^*_j \qquad \text{implies}$$

$$a_j'' \equiv a \cdot a^*_j \pmod{H_{n-1}} .$$

Thus we have shown it suffices to define $f^{-1}(a)$ where

$$da = g \otimes a + X \ , \ g \in G \ , \ X \in H_n \otimes H_{n-1} \ .$$

For such $\underline{a}$ define

$$f^{-1}(a) = f^{-1}(g)[\varepsilon(a) - m \circ f \otimes f^{-1} \circ (d(a) - g \otimes a)]$$

$$= f^{-1}(g)[\varepsilon(a) - \sum_i f(x_i')f^{-1}(x_i'')] \ ,$$

where $X = \sum_i x_i' \otimes x_i''$.

$$f * f^{-1}(a) = f(g)[f^{-1}(g)[\varepsilon(a) - \sum_i f(x_i')f^{-1}(x_i'')]]$$

$$+ \sum_i f(x_i')f^{-1}(x_i'')$$

$$= \varepsilon(a) \ .$$

Thus f has a right inverse. Similarly it has a left inverse and is regular.

We know that $G(H)$ is a group when H has an antipode. The above result shows that when H is split it has

an antipode if and only if $G(H)$ is a group. In particular if $G(H) = \{1\}$ then H has an antipode.

Chapter II

In this chapter we prove two decomposition theorems for modules and comodules of a Hopf algebra with antipode. The theorems are dual. We apply the theorems to a split Hopf algebra with antipode by means of the grading. For a split conilpotent Hopf algebra with antipode we find

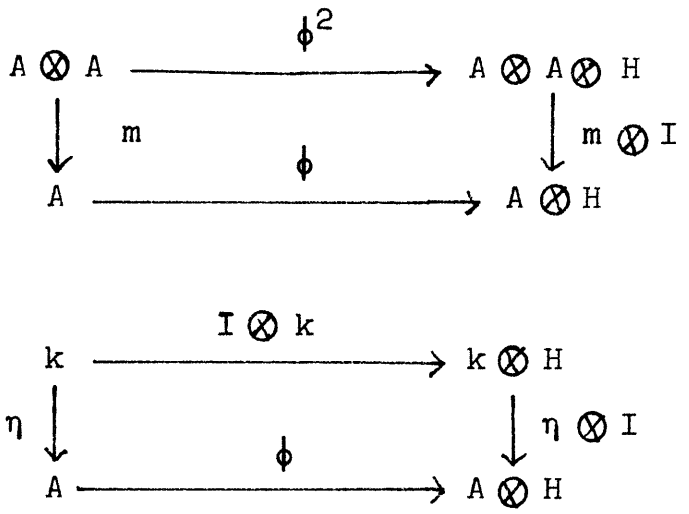
$$H^e \otimes \Gamma(G) \xrightarrow{\quad m \quad} H$$

is a linear isomorphism.

Suppose X is a vector space which is a right H-comodule, (H considered as a coalgebra). We use the multiplicative structure of H to make $X \otimes X$ a right H-comodule. Let $\phi\colon X \to X \otimes H$ be the comodule structure, then the comodule structure on $X \otimes X$ is denoted ϕ^2.

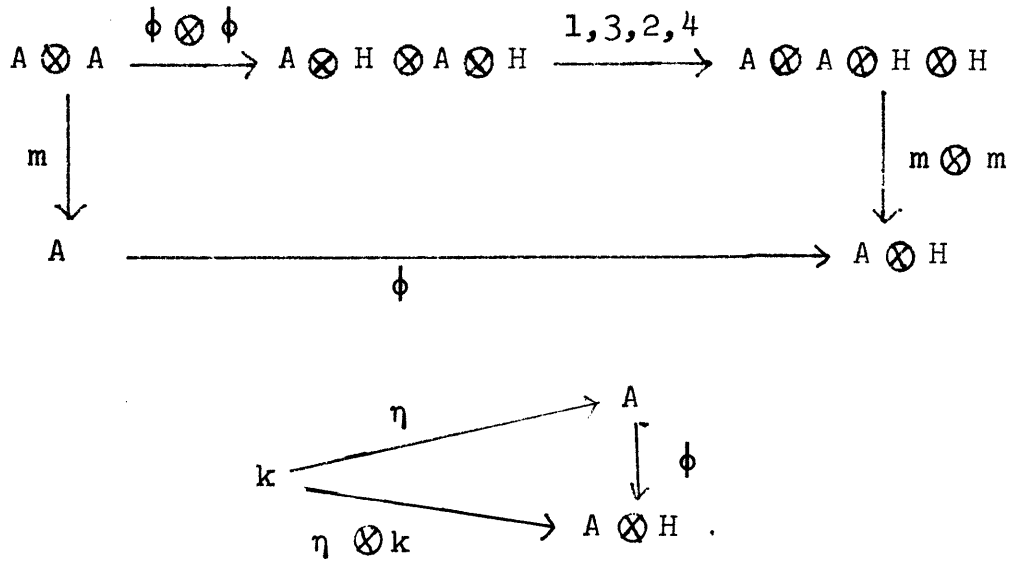
$$\phi^2\colon X \otimes X \xrightarrow{\phi\otimes\phi} X \otimes H \otimes X \otimes H \xrightarrow{(1,3,2,4)} X \otimes X \otimes H \otimes H \xrightarrow{I \otimes I \otimes m} X \otimes X \otimes H \ .$$

For an algebra A to be a right H-comodule <u>as an algebra</u> we require $m\colon A \otimes A \to A$, $k \xrightarrow{\eta} A$ are morphisms of comodules. That means



are commutative.

The diagrams can be rewritten:



Hence an equivalent condition for A to be a right H-comodule as an algebra is that $\phi: A \to A \otimes H$ is an algebra morphism. Unless otherwise specified when an algebra is a right H-comodule it is as an algebra. H is a right H-comodule

under $d: H \to H \otimes H$ (as an algebra).

Let $B = A \,\square^H k$ where the algebra A is a right H-comodule. Since we consider $k \subset H$, $B = \phi^{-1}(A \otimes k)$ and B is a subalgebra of A.

Theorem 1: H is a Hopf algebra with antipode S; A an algebra which is a right H-comodule; $B = A \,\square^H k$.

Suppose $\sigma: H \to A$ where

i) σ is a morphism of right H-comodules ($d: H \to H \otimes H$ is the comodule structure),

ii) $\sigma \in \mathrm{Hom}(H,A)$ is regular, i.e., there is $\sigma^{-1} \in \mathrm{Hom}(H,A)$ where $\sigma * \sigma^{-1} = \eta \circ \varepsilon = \sigma^{-1} * \sigma$;

then $\alpha: B \otimes H \xrightarrow{i \otimes \sigma} A \otimes A \xrightarrow{m} A$ is a linear isomorphism.

In fact $\mathrm{Im}(A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1}} A \otimes A \xrightarrow{m} A) \subset B$.

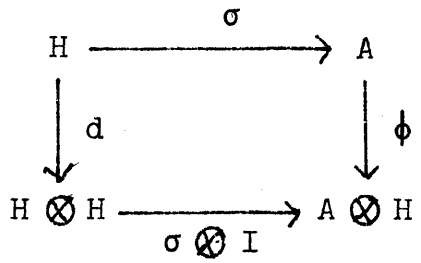
If $P = m \circ I \otimes \sigma^{-1} \circ \phi: A \to B$ then

$$\beta: A \xrightarrow{\phi} A \otimes H \xrightarrow{P \otimes I} B \otimes H$$

is the inverse isomorphism to α.

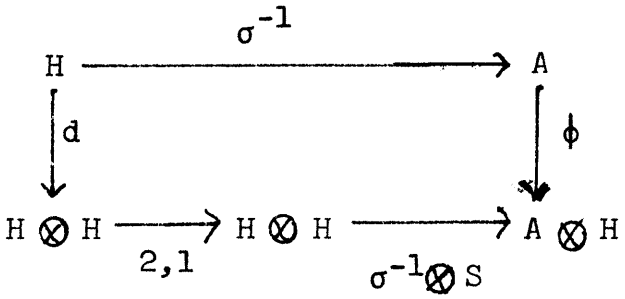
Observe α, P, β are morphisms of left B-modules; α, β are morphisms of right H-comodules.

Proof. We shall show α and β are inverse to each other set theoretically. By i)

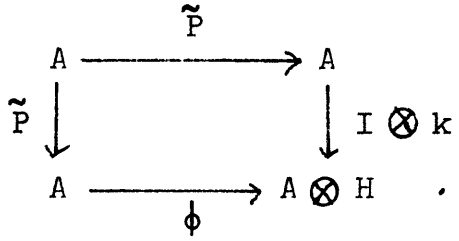


is commutative.

We wish to show



is commutative. In $\mathrm{Hom}(H, A \otimes H)$ $\phi \circ \sigma$ has right inverse $\phi \circ \sigma^{-1}$ and $\sigma \otimes I \circ d$ has left inverse $\sigma^{-1} \otimes S \circ (2,1) \circ d$, which establishes the commutative diagram. Define $\tilde{P}: A \to A$ $\tilde{P} = m \circ I \otimes \sigma^{-1} \circ \phi$. $\mathrm{Im}(\tilde{P}) \subset B$ is equivalent to commutivity of



$$A \xrightarrow{\tilde{P}} A \xrightarrow{\phi} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1}} A \otimes A \xrightarrow{m} A \xrightarrow{\phi} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1}} A \otimes A \xrightarrow{\phi \otimes \phi} A \otimes H \otimes A \otimes H$$

$$\xrightarrow{(1,3,2,4)} A \otimes A \otimes H \otimes H \xrightarrow{m \otimes m} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes d} A \otimes H \otimes H \xrightarrow{I \otimes (2,1)} A \otimes H \otimes H$$

$$\xrightarrow{\phi \otimes \sigma^{-1} \otimes S} A \otimes H \otimes A \otimes H \xrightarrow{(1,3,2,4)} A \otimes A \otimes H \otimes H$$

$$\xrightarrow{m \otimes m} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{\phi \otimes d} A \otimes H \otimes H \otimes H \xrightarrow{(1,2,4,3)} A \otimes H \otimes H \otimes H$$

$$\xrightarrow{I \otimes I \otimes \sigma^{-1} \otimes S} A \otimes H \otimes A \otimes H$$

$$\xrightarrow{(1,3,4,2)} A \otimes A \otimes H \otimes H \xrightarrow{m \otimes m} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes d^2} A \otimes H \otimes H \otimes H \xrightarrow{I \otimes I \otimes S \otimes \sigma^{-1}} A \otimes H \otimes H \otimes A$$

$$\xrightarrow{(1,4,2,3)} A \otimes A \otimes H \otimes H \xrightarrow{m \otimes m} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes d} A \otimes H \otimes H \xrightarrow{I \otimes I * S \otimes \sigma^{-1}} A \otimes H \otimes A$$

$$\xrightarrow{(1,3,2)} A \otimes A \otimes H \xrightarrow{m \otimes I} A \otimes H$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1}} A \otimes A \xrightarrow{m \otimes k} A \otimes H$$

$$= A \xrightarrow{\tilde{P} \otimes k} A \otimes H \quad .$$

Thus we can define $P: A \to B$. P is $\tilde{P}$ with its image restricted to B .

Now consider $\alpha\beta$ =

$$A \xrightarrow{\phi} A \otimes H \xrightarrow{\phi \otimes I} A \otimes H \otimes H \xrightarrow{I \otimes \sigma^{-1} \otimes I} A \otimes A \otimes H$$

$$\xrightarrow{m \otimes I} B \otimes H \xrightarrow{i \otimes \sigma} A \otimes A \xrightarrow{m} A$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes d} A \otimes H \otimes H \xrightarrow{I \otimes \sigma^{-1} \otimes \sigma} A \otimes A \otimes A$$

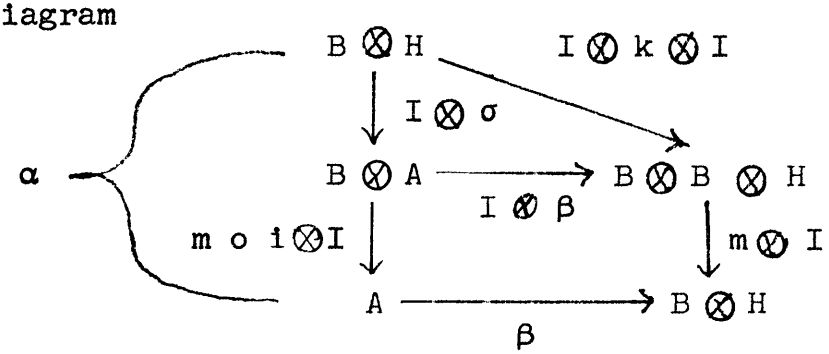
$$\xrightarrow{I \otimes m} A \otimes A \xrightarrow{m} A$$

$$= A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1} * \sigma} A \otimes A \xrightarrow{m} A$$

$$= A \xrightarrow{I} A \quad .$$

Consider $\beta\alpha$:

In the diagram



the square commutes because β is a left B-module morphism. The triangle commutes because

$$\begin{aligned}\beta \circ \sigma &= m \otimes I \circ I \otimes \sigma^{-1} \otimes I \circ \phi \otimes I \circ \phi \circ \sigma \\ &= m \otimes I \circ I \otimes \sigma^{-1} \otimes I \circ I \otimes d \circ \phi \circ \sigma \\ &= m \otimes I \circ I \otimes \sigma^{-1} \otimes I \circ I \otimes d \circ \sigma \otimes I \circ d \\ &= \sigma * \sigma^{-1} \otimes I \circ d \\ &= k \otimes I \ .\end{aligned}$$

Hence $\beta\alpha = I_{B \otimes H}$

Q.E.D.

Now we consider the dual situation. If X is a left H-module (H considered as an algebra) where $\psi: H \otimes X \to X$ is the structure morphism then $X \otimes X$ is a left H-module under ψ^2 where

$$\psi^2: H \otimes X \otimes X \xrightarrow{d \otimes I \otimes I} H \otimes H \otimes X \otimes X$$

$$\xrightarrow{(1,3,2,4)} H \otimes X \otimes H \otimes X \xrightarrow{\psi \otimes \psi} X \otimes X \ .$$

If the coalgebra A is a left H-module the conditions:

$d: A \to A \otimes A$ is a morphism of H-modules

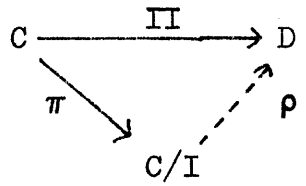
$\varepsilon: A \to k$ is a morphism of H-modules

are equivalent to:

$\psi: H \otimes A \to A$ is a coalgebra morphism.

They both imply the same commutative diagrams. The coalgebra A is a left H-module <u>as a coalgebra</u> if either of the conditions is satisfied. Whenever we speak of a coalgebra as a left H-module it is always as a coalgebra. H is a left H-module under $m: H \otimes H \to H$.

Within a coalgebra C a 2-sided coideal I is a subspace where $I \subset \operatorname{Ker} \varepsilon$, $dI \subset I \otimes C + C \otimes I$. If $\pi: C \to C/I$ is the canonical map then if I is a 2-sided coideal C/I has a natural coalgebra structure where $\pi: C \to C/I$ is a morphism of coalgebras. Conversely if $\Pi: C \to D$ is a surjective morphism of coalgebras then $I = \operatorname{Ker} \Pi$ is a 2-sided coideal and the factor map ρ



is a morphism of coalgebras.

Within H let H^+ denote $\operatorname{Ker} \varepsilon$. ε is a coalgebra morphism so H^+ is a 2-sided coideal. Then $H^+ \otimes A$ is a 2-sided coideal in $H \otimes A$, where the coalgebra A is a left H-module; and $\psi(H^+ \otimes A) = H^+ \cdot A$ is a 2-sided coideal in A since ψ is a coalgebra morphism. Thus $B = k \otimes_H A = A/H^+ \cdot A$ has a quotient coalgebra structure. If $\pi: A \to B$ A is naturally a right B-comodule where

$$A \xrightarrow{d} A \otimes A \xrightarrow{I \otimes \pi} A \otimes B .$$

Theorem 2. H is a Hopf algebra with antipode S; A a coalgebra which is a left H-module; $B = k \otimes_H A$.

Suppose $P: A \to H$ where

i) P is a morphism of left H-modules

ii) P is a regular element of $\mathrm{Hom}(A,H)$

then $\beta: A \xrightarrow{d} A \otimes A \xrightarrow{P \otimes \pi} H \otimes B$ is a linear isomorphism.

In fact $\mathrm{Ker}(A \xrightarrow{d} A \otimes A \xrightarrow{P^{-1} \otimes I} H \otimes A \xrightarrow{\psi} A) \supset H^+ \cdot A$.

So if σ is the factoring

$$\begin{array}{ccccccc} A & \xrightarrow{d} & A \otimes A & \xrightarrow{P^{-1} \otimes I} & H \otimes A & \xrightarrow{\psi} & A \\ & \searrow^{\pi} & & & & \nearrow_{\sigma} & \\ & & & B & & & \end{array}$$

then $\alpha: H \otimes B \xrightarrow{I \otimes \sigma} H \otimes A \xrightarrow{\psi} A$ is the inverse isomorphism to β.

Observe β, σ, α are morphisms of right B-comodules, β, α are morphisms of left H-modules.

The proof is dual to that of theorem 1.

We now present applications of theorem 1. Suppose H is a graded Hopf algebra with antipode S. That is,

$$H = \bigoplus_{i=0}^{\infty} H_i$$

$$H_i H_j \subset H_{i+j} \qquad dH_i \subset \bigoplus_{n=0}^{i} H_n \otimes H_{i-n}$$

$$S(H_i) \subset H_i$$

$$\eta: k \to H \ , \quad \varepsilon: H \to k$$

are morphisms of graded vector spaces where $k = k_0$. Then H_0 is a sub Hopf algebra with antipode and the natural projection $\pi: H \to H_0$ is a morphism of Hopf algebras, namely an algebra and coalgebra morphism. H is a right H_0-comodule under

$$\phi: H \xrightarrow{d} H \otimes H \xrightarrow{I \otimes \pi} H \otimes H_0 \ .$$

$\sigma: H_0 \to H$ the natural imbedding is an H_0-comodule morphism with inverse $S \circ \sigma$. If $B \subset H$, $B = H \ \square^{H_0} k$ then by theorem 1

$$B \otimes H_0 \xrightarrow{i \otimes \sigma} H \otimes H \xrightarrow{m} H$$

is a linear isomorphism.

In case H is a split Hopf algebra with antipode we obtained a graded Hopf algebra with antipode, $\overline{H}$.

$\overline{H}_0 = H_0 = \Gamma(G)$. Let $\overline{B}$ denote the subalgebra $\overline{H} \ \square^{\overline{H}_0} \ k$. Then

$$\overline{B} \otimes \Gamma(G) \xrightarrow{m} \overline{H}$$

is a linear isomorphism.

In case H is a split conilpotent Hopf algebra with antipode

$$H = \bigoplus_{g \in G} H^g .$$

We put a $\Gamma(G)$-comodule structure on H by

$$\phi: H \to H \otimes \Gamma(G)$$
$$H^g \to H^g \otimes g ,$$
$$h \in H^g , \ \phi(h) = h \otimes g .$$

H is a $\Gamma(G)$-comodule <u>as an algebra</u> since

$$H^g H^h \subset H^{gh} .$$

$H \square^{\Gamma(G)_k} = H^e$. The natural injection σ of $\Gamma(G) \xrightarrow{\sigma} H$ is a $\Gamma(G)$-comodule morphism with inverse $S \circ \sigma$. Hence by theorem 1 $H^e \otimes \Gamma(G) \xrightarrow{m} H$ is a linear isomorphism.

Chapter III

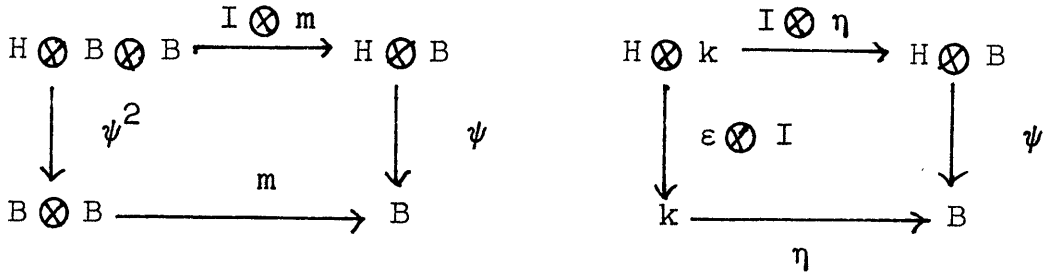
Cohomology

We define abelian cohomology groups $H^i(H,B)$ $i=0,1,2...$ where H is a cocommutative Hopf algebra, B is a commutative algebra which is an H-module satisfying certain conditions. In case H is a group Hopf algebra $H^i(H,B)$ is the familiar group cohomology $H^i(G,B^r)$ where B^r is the subgroup of regular elements of B. We define the notion of an algebra which is an extension of H by B and show the isomorphism classes of extensions correspond to $H^2(H,B)$. When B is a Galois field extension of k and H the group algebra of the Galois group of B over k, then the extensions of H by B correspond to elements of the Brauer Group. We show how to multiply extensions so that the correspondence between extensions and $H^2(H,B)$ is a group isomorphism.

In the next chapter we define cohomology groups $H(B,H)^i$ when B is a cocommutative coalgebra H a commutative Hopf algebra and B is an H-comodule satisfying certain conditions, we outline a dual extension theory to the previous case and outline how $H(B,H)^2$ corresponds to isomorphism classes of extensions.

With H a Hopf algebra B an algebra which is a

left H-module under $\psi: H \otimes B \to B$ then B is called a left Hopf algebra H-module if the following diagrams are commutative:



The left diagram means $m: B \otimes B \to B$ is a left H-module morphism; the right diagram means $\eta: k \to B$ is a left H-module morphism. B is called commutative Hopf algebra H-module (C.H.A. H-module) if B is a commutative algebra and H a cocommutative Hopf algebra. For a coalgebra C and algebra A $0 < n \in Z$, let $\mathrm{Hom}^n(C,A) = \mathrm{Hom}(\overbrace{C \otimes \cdots \otimes C}^{n}, A)$. Let $\mathrm{Reg}^n(C,A) = \{\text{regular (invertible) elements of } \mathrm{Hom}^n(C,A)\}$. $\mathrm{Reg}^n(C,A)$ is a multiplicative subgroup of $\mathrm{Hom}^n(C,A)$. If B is a left C.H.A. H-module $\mathrm{Reg}^n(H,B)$ is an abelian group. We let $\mathrm{Hom}^0(C,A) = \mathrm{Hom}(k,A) = A$ and $\mathrm{Reg}^0(C,A) = \{\text{regular elements of } A\} = A^r$.

Now we assume B is a left C.H.A. H-module where $\psi: H \otimes B \to B$ is the module action. $\mathrm{Reg}^n(H,B)$ $0 \leq n \in Z$ is an abelian group. Define

$$\delta^n: \mathrm{Reg}^n(H,B) \to \mathrm{Hom}^{n+1}(H,B)$$

$$\delta^n f = (\psi \circ I \otimes f) * \prod_{i=1}^{n} f^{(-1)^i} \circ (\underbrace{I \otimes \cdots \otimes I}_{i-1} \otimes m \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i})$$

$$* f^{(-1)^{n+1}} \otimes \varepsilon$$

where $f \in \mathrm{Reg}^n(H,B)$ $n > 0$; for $n = 0$ $\delta^0 b(h) = (h \cdot b)b^{-1}$ $b \in B^r$, $h \in H$. We shall let $F^{[a]}$ denote $\overbrace{F \otimes \cdots \otimes F}^{a}$. In $\mathrm{Reg}^n(H,B)$ $n > 0$, $\eta \circ \varepsilon^{[n]}$ is the unit. This is often denoted ε . We shall show $\delta^n(\varepsilon) = \varepsilon$, and given $f,g \in \mathrm{Reg}^n(H,B)$ $\delta^n(f * g) = \delta^n(f) * \delta^n(g)$. These imply that we can consider δ^n as a map from $\mathrm{Reg}^n(H,B)$ to $\mathrm{Reg}^{n+1}(H,B)$ and that δ^n is a group homomorphism. $\delta^0 1(h) = (h \cdot 1)1 = \varepsilon(h)$ so $\delta^0 1 = \varepsilon$. Note $h \cdot 1 = \varepsilon(h)$ is one of the conditions for B to be an H.A. H-module, we now use the other:

$$\delta^0(bc)(h) = (h \cdot (bc))c^{-1}b^{-1} = \sum_i (h_i' \cdot b)(h_i'' \cdot c)(c^{-1}b^{-1})$$

$$= \sum_i (h_i' \cdot b)b^{-1}(h_i'' \cdot c)c^{-1}$$

$$= [\delta^0(b) * \delta^0(c)](h) .$$

For the case $n > 0$

$$\delta^n(\varepsilon) = \psi \circ I \otimes \varepsilon * \prod_{i=1}^{n} \varepsilon^{(-1)^i} \circ I^{[i-1]} \otimes m \otimes I^{[n-i]} * \varepsilon^{(-1)^i} \otimes \varepsilon$$

$$= \varepsilon * \prod_{i=1}^{n} \varepsilon * \varepsilon = \varepsilon .$$

Note $\psi \circ I \otimes \varepsilon = \varepsilon$ because B is an H.A. H-module. This also guarantees $\psi \circ I \otimes (f * g) = (\psi \circ I \otimes f) * (\psi \circ I \otimes g)$. $(f * g)^{(-1)^i} = f^{(-1)^i} * g^{(-1)^i}$ because the group is abelian and $(f * g)^{(-1)^i} \circ I^{[i-1]} \otimes m \otimes I^{[n-i]} =$

$$[f^{(-1)^i} \circ I^{[i-1]} \otimes m \otimes I^{[n-i]}] * [g^{(-1)^i} \circ I^{[i-1]} \otimes m \otimes I^{[n-i]}]$$

because $I^{[i-1]} \otimes m \otimes I^{[n-i]}$ is a coalgebra morphism. It is clear $(f * g)^{(-1)^{n+1}} \otimes \varepsilon = (f^{(-1)^{n+1}} \otimes \varepsilon) * (g^{(-1)^{n+1}} \otimes \varepsilon)$; and thus $\delta^n(f * g) = \delta^n(f) * \delta^n(g)$.

We have the sequence of abelian groups and homomorphisms

$$\mathrm{Reg}^0(H,B) \xrightarrow{\delta^0} \mathrm{Reg}^1(H,B) \xrightarrow{\delta^1} \mathrm{Reg}^2(H,B) \xrightarrow{\delta^2} \cdots .$$

We shall now show

$$\delta^{n+1}\delta^n = \varepsilon\colon \mathrm{Reg}^n(H,B) \to \mathrm{Reg}^{n+2}(H,B) .$$

We do this by expanding $\delta^{n+1}\delta^n f$. In our notation

$$\cdots * \overbrace{\text{term}}^{4} * \cdots \quad \text{expands to}$$

$$\cdots * \overbrace{\text{term}}^{41} * \overbrace{\text{term}}^{42} * \overbrace{\text{term}}^{43} * \cdots .$$

The explanations of the expansions follow the computation and a typical note is of the form: $4 \to 41 * 42 * 43$: "explanation".

$$\delta^{n+1}\delta^{n} f = \qquad \text{(where } n > 0\text{)}$$

$$\overbrace{\psi \circ I \otimes (\psi \circ I \otimes f * \pi_{i=1}^{n} f^{(-1)^i} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]})}^{1} * f^{(-1)^{n+1}} \otimes \varepsilon) *$$

$$\overbrace{\pi_{j=1}^{n+1} (\psi \circ I \otimes f * \pi_{i=1}^{n} f^{(-1)^i} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]})}^{2} * f^{(-1)^{n+1}} \otimes \varepsilon)^{(-1)^j} \circ (I^{[j-1]} \otimes m \otimes I^{[n+1-j]})$$

$$\overbrace{* (\psi \circ I \otimes f * \pi_{i=1}^{n} f^{(-1)^i} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]})}^{3} * f^{(-1)^{n+1}})^{(-1)^{n+2}} \otimes \varepsilon$$

$$= \overbrace{\psi \circ I \otimes (\psi \circ I \otimes f)}^{11} * \overbrace{\pi_{i=1}^{n} \psi \circ I \otimes (f^{(-1)^i} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]}))}^{12}$$

$$* \overbrace{\psi \circ I \otimes f^{(-1)^{n+1}} \otimes \varepsilon}^{13} *$$

21

$$\overbrace{\prod_{j=1}^{n+1} (\psi \circ I \otimes f^{(-1)^j}) \circ (I^{[j-1]} \otimes m \otimes I^{[n+1-j]})}$$

22

$$* \overbrace{\prod_{\substack{1\leq i\leq n \\ 1\leq j\leq n+1}} f^{(-1)^{i+j}} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]}) \circ (I^{[j-1]} \otimes m \otimes I^{[n+1-j]})}$$

23

$$* \overbrace{\prod_{j=1}^{n+1} ((f^{(-1)^{n+1+j}} \otimes \varepsilon) \circ (I^{[j-1]} \otimes m \otimes I^{[n+1-j]})} *$$

31

$$\overbrace{(\psi \circ I \otimes f^{(-1)^{n+2}}) \otimes \varepsilon * \prod_{i=1}^{n} [(f^{(-1)^{i+n+2}} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]})) \otimes \varepsilon]}$$

32

$$* \overbrace{f^{(-1)^{n+1+n+2}} \otimes \varepsilon \otimes \varepsilon}$$

111 121

$$= \overbrace{\psi \circ m \otimes f}^{111} * \overbrace{\prod_{i=1}^{n} \psi \circ I \otimes (f^{(-1)^i} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]}))}^{121} *$$

131

$$\overbrace{\psi \circ I \otimes f^{(-1)^{n+1}} \otimes \varepsilon}^{131} *$$

211 212

$$\overbrace{\psi \circ m \otimes f^{-1}}^{211} * \overbrace{\prod_{j=2}^{n+1} \psi \circ I \otimes (f^{(-1)^j} \circ (I^{[j-2]} \otimes m \otimes I^{[n+1-j]}))}^{212} *$$

221

$$\overbrace{\prod_{1 \le i \le j-2 \le n-1} f^{(-1)^{i+j}} \circ (I^{[i-1]} \otimes m \otimes I^{[j-i-2]} \otimes m \otimes I^{[n+1-j]})}^{221} *$$

222

$$\overbrace{\prod_{1 \le j < i \le n} f^{(-1)^{i+j}} \circ (I^{[j-1]} \otimes m \otimes I^{[i-j-1]} \otimes m \otimes I^{[n-i]})}^{222} *$$

223

$$\overbrace{\prod_{1 \le i = j-1 \le n} f^{(-1)^{i+j}} \circ (I^{[j-2]} \otimes m^2 \otimes I^{[n+1-j]})}^{223} *$$

224

$$\overbrace{\pi_{1\leq i=j\leq n} f^{(-1)^{i+j}} \circ (I^{[j-1]} \otimes m^2 \otimes I^{[n-j]})}$$

231

$$\overbrace{* \pi_{j=1}^{n} [(f^{(-1)^{n+1+j}} \circ (I^{[j-1]} \otimes m \otimes I^{[n-j]})) \otimes \varepsilon] *}$$

232

$$\overbrace{f^{(-1)^{n+1+n+1}} \otimes \varepsilon \circ m *}$$

311

$$\overbrace{\psi \circ I \otimes f^{(-1)^{n+2}} \otimes \varepsilon}$$

312

$$* \overbrace{\pi_{i=1}^{n} [(f^{(-1)^{i+n+2}} \circ (I^{[i-1]} \otimes m \otimes I^{[n-i]})) \otimes \varepsilon]}$$

321

$$\overbrace{* f^{-1} \otimes \varepsilon \circ m}$$,

which cancels to ε as follows:

111 —— 211 221 —— 222

121 —— 212 223 —— 224

131 —— 311 231 —— 312 232 —— 321 .

In the expansion:

$1 \longrightarrow 11*12*13$: $\psi \circ I \otimes f * g = (\psi \circ I \otimes f) * (\psi \circ I \otimes g)$

$2 \longrightarrow 21*22*23$:

$$f * g \circ (I^{[a]} \otimes m \otimes I^{[b]}) = (f \circ I^{[a]} \otimes m \otimes I^{[b]}) * (g \circ I^{[a]} \otimes m \otimes I^{[b]})$$

$$(f * g)^{-1} = f^{-1} * g^{-1}$$

$$(\psi \circ I \otimes f)^{-1} = \psi \circ I \otimes f^{-1}$$

$$(f \circ (I^{[a]} \otimes m \otimes I^{[b]}))^{-1} = f^{-1} \circ (I^{[a]} \otimes m \otimes I^{[b]})$$

$3 \longrightarrow 31*32$: $(f * g) \otimes \varepsilon = (f \otimes \varepsilon) * (g \otimes \varepsilon)$, $(f * g)^{-1} = f^{-1} * g^{-1}$

$$(\psi \circ I \otimes f)^{-1} = \psi \circ I \otimes f^{-1}$$

$$(f \circ I^{[a]} \otimes m \otimes I^{[b]}))^{-1} = f^{-1} \circ (I^{[a]} \otimes m \otimes I^{[b]}) .$$

The rest of the expansion is clear.

In the cancellation $221 \text{——} 222$ because

$$221) = \pi_{a+b+c=n-2} f^{(-1)^{a-c+n+2}} \circ (I^{[a]} \otimes m \otimes I^{[b]} \otimes m \otimes I^{[c]})$$

$$222) = \pi_{a+b+c=n-2} f^{(-1)^{a-c+n+1}} \circ (I^{[a]} \otimes m \otimes I^{[b]} \otimes m \otimes I^{[c]}) .$$

The rest of the cancellation is clear. In the above calculation we assumed $n > 0$; however, it is true $\delta^1\delta^0 = \varepsilon$. We omit the straightforward verification.

We have a complex

$$\mathrm{Reg}^0(H,B) \xrightarrow{\delta^0} \mathrm{Reg}^1(H,B) \xrightarrow{\delta^1} \mathrm{Reg}^2(H,B) \xrightarrow{\delta^2} \cdots ,$$

which depends upon H, B and $\psi: H \otimes B \to B$. We define the cohomology

$$H^n(H,B) = \mathrm{Ker}\ \delta^n/\mathrm{Im}\ \delta^{n-1} \qquad n > 0 .$$

$$H^0(H,B) = \mathrm{Ker}\ \delta^0 .$$

Example

B is a commutative algebra and G is a group of automorphisms of B . For example B may be a Galois extension of k and G the Galois group. Let $H = \Gamma(G)$, B is a left C.H.A. H-module under the induced representation. Thus we have the cohomology groups $H^i(H,B)$. Recall $B^r = \{\text{regular elements of } B\}$. B^r is an abelian group and is a G-module in the usual group theoretic sense. We show

$$H^n(G,B^r) = H^n(H,B)$$

where the left term refers to cohomology of groups and the right term to Hopf algebra cohomology. We do this by showing the "standard complex" in computing the group

cohomology is isomorphic to

$$\mathrm{Reg}^0(H,B) \xrightarrow{\delta^0} \mathrm{Reg}^1(H,B) \xrightarrow{\delta^1} \cdots .$$

In the standard complex for group cohomology:

$$C^n = \{ f \mid f: G \times \cdots \times G \to B^r \}$$

$f, g \in C^n \quad fg(g_1,\ldots g_n) = f(g_1,\ldots g_n)g(g_1,\ldots g_n)$

$(g_1,\ldots g_n) \in G \times \cdots \times G$.

$$\delta^n: C^n \to C^{n+1} \qquad \delta^n f(g_1,\ldots g_{n+1}) =$$

$$g_1 \cdot f(g_2,\ldots g_{n+1}) \prod_{i=1}^{n} [f(g_1,\ldots g_{i-1}, g_i g_{i+1}, g_{i+2},\ldots g_{n+1})]^{(-1)^i}$$

$$[f(g_1,\ldots g_n)]^{(-1)^{n+1}} .$$

We consider $\overbrace{G \times \cdots \times G}^{n}$ as a basis for $H^{[n]}$ so that $f \in C^n$ extends uniquely to an element $\overline{f} \in \mathrm{Hom}^n(H,B)$.
Clearly the map

$$C^n \to \mathrm{Hom}^n(H,B)$$

$$f \to \overline{f}$$

is injective. Since $G(H \otimes \cdots \otimes H) = G \times \cdots \times G$

by (4) $\overline{f} \in \mathrm{Reg}^n(H,B)$ and

$$C^n \to \mathrm{Reg}^n(H,B)$$
$$f \to \overline{f}$$

is surjective hence bijective. It is a straightforward verification that $C^n \to \mathrm{Reg}^n(H,B)$ is a group homomorphism, hence, isomorphism and

$$\begin{array}{ccccccc} C^0 & \xrightarrow{\delta^0} & C^1 & \xrightarrow{\delta^1} & C^2 & \xrightarrow{\delta^2} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \\ \mathrm{Reg}^0(H,B) & \xrightarrow[\delta^0]{} & \mathrm{Reg}^1(H,B) & \xrightarrow[\delta^1]{} & \mathrm{Reg}^2(H,B) & \xrightarrow[\delta^2]{} & \cdots \end{array}$$

is an isomorphism of complexes. Hence $H^n(H,B) = H^n(G,B^r)$.

A Normal Complex

Within $\mathrm{Reg}^n(H,B)$ we define for $n > 0$

$$\mathrm{Reg}_1^n(H,B) = \left\{ f \in \mathrm{Reg}^n(H,B) \;\middle|\; \begin{array}{ccc} H \otimes \cdots \otimes H & \xrightarrow{f} & B \\ & \nwarrow \quad \nearrow & \\ & k & \end{array} \text{ is commutative} \right\}$$

$$= \left\{ f \in \mathrm{Reg}^n(H,B) \;\middle|\; f(1 \otimes \cdots \otimes 1) = 1 \right\} .$$

Let $\delta_1^n = \delta^n | \mathrm{Reg}_1^n(H,B) : \mathrm{Reg}_1^n(H,B) \to \mathrm{Reg}^{n+1}(H,B)$.

$\delta_1{}^n f(1^{[n]}) = 1$ so

$$\delta_1{}^n : \mathrm{Reg}_1{}^n(H,B) \rightarrow \mathrm{Reg}_1{}^{n+1}(H,B) \quad .$$

We define $\mathrm{Reg}_1{}^0(H,B) = B^r$ and $\delta_1{}^0 = \delta^0$.

$\delta^0 b(1) = (1 \cdot b)b^{-1} = 1$, $b \in B^r$ so

$$\delta_1{}^0 : \mathrm{Reg}_1{}^0(H,B) \rightarrow \mathrm{Reg}_1{}^1(H,B) \quad .$$

To show the cohomology obtained from the normal complex is the same as the previous cohomology we define maps between the two complexes where the compositions are chain homotopic to the identities.

$$\dot{\iota}_n : \mathrm{Reg}_1{}^n(H,B) \rightarrow \mathrm{Reg}^n(H,B)$$

the natural inclusion is a morphism of complexes, i.e., $\delta^n \circ \dot{\iota}_n = \dot{\iota}_{n+1} \circ \delta_1{}^n$.

Given $f \in \mathrm{Reg}(H,B)$ by (4) chapter I

$\lambda_f = f(1 \otimes \cdots \otimes 1) \in B^r$. Note $\lambda_{f*g} = \lambda_f \lambda_g$. Let $\wedge_f$ denote the map

$$H^{[n]} \longrightarrow B$$

$$h_1 \otimes \cdots \otimes h_n \longrightarrow \lambda_f \, \varepsilon(h_1) \cdots \varepsilon(h_n)$$

Then

$$\mathrm{Reg}^n(H,B) \rightarrow \mathrm{Reg}^n(H,B)$$

$$f \rightarrow \wedge_f$$

is a homomorphism; as is

$$\pi_n : \mathrm{Reg}^n(H,B) \to \mathrm{Reg}_1{}^n(H,B)$$
$$f \to f * \Lambda_f^{-1} = f * \Lambda_{f^{-1}} .$$

$$\lambda_{\delta^n f} = \begin{cases} 1 & n \text{ is even} \\ \lambda_f & n \text{ is odd} , \end{cases}$$

so

$$\Lambda_{\delta^n f} = \begin{cases} \varepsilon & n \text{ even} \\ \Lambda_f \otimes \varepsilon & n \text{ odd} , \end{cases}$$

$$\delta^n \Lambda_f = \begin{cases} \varepsilon & n \text{ even} \\ \Lambda_f \otimes \varepsilon & n \text{ odd} . \end{cases}$$

This implies $\pi_{n+1}\delta^n f = \begin{cases} \delta^n f & n \text{ even} \\ \delta^n f * (\Lambda_f^{-1} \otimes \varepsilon) & n \text{ odd}, \end{cases}$

and that $\delta_1{}^n \pi_n f = \begin{cases} \delta^n f & n \text{ even} \\ \delta^n f * (\Lambda_f^{-1} \otimes \varepsilon) & n \text{ odd} . \end{cases}$

Hence, $\{\pi_i\}$ is a morphism of complexes. Clearly

$\pi_n \circ \dot{\iota}_n : \mathrm{Reg}_1{}^n(H,B) \to \mathrm{Reg}_1{}^n(H,B)$ is the identity.

$\dot{\iota} \circ \pi$ is chain homotopic to the identity as follows:

$$\nu_n : \mathrm{Reg}^n(H,B) \to \mathrm{Reg}^{n-1}(H,B)$$

$$\nu_n(f)(h_1 \otimes \cdots \otimes h_{n-1}) = \Lambda_f(h_1 \otimes \cdots \otimes h_{n-1} \otimes 1) .$$

$$f * (\dot{\zeta}_n \pi_n(f))^{-1} = f * \Lambda_f * f^{-1} = \Lambda_f .$$

$$\delta^{n-1}\nu_n(f) * \nu_{n+1}\delta^n(f) = \Lambda_f .$$

Thus $\delta \circ \nu * \nu \circ \delta = I * (\dot{\zeta}\, \pi)^{-1}$ and $\dot{\zeta}\, \pi$ is chain homotopic to the identity, and the two complexes give the same cohomology.

Extensions

H is a Hopf algebra B an algebra and A an algebra which is an H-comodule as an algebra, $\phi : A \to A \otimes H$ being the structure. The sequence $B \xrightarrow{\eta} A \xrightarrow{\phi} A \otimes H$ is called left exact if

1) η is an injective algebra morphism,

2) $\mathrm{Im}\, \eta = A \,\square^H k$.

The sequence is called split exact if: H has an antipode, the sequence is left exact, and there is $\sigma : H \to A$ satisfying

1) σ is a morphism of right H-comodules

2) $\sigma \in \mathrm{Reg}^1(H,A)$.

If the sequence is split exact, by theorem 1,

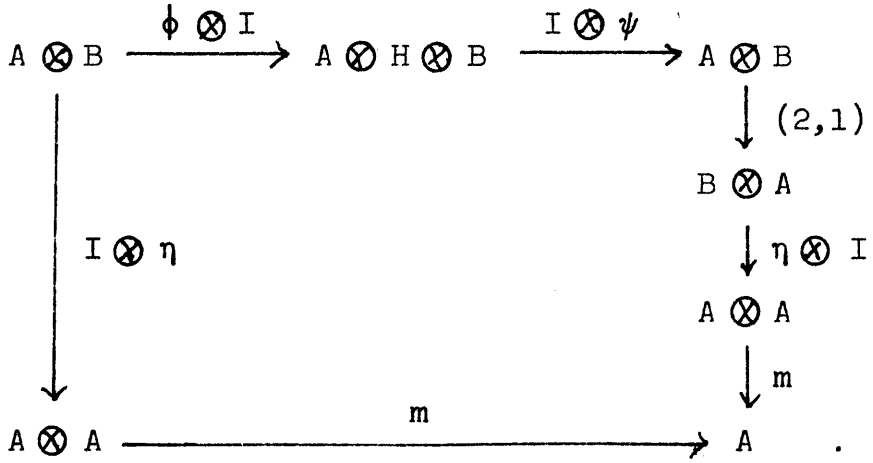
$$B \otimes H \xrightarrow{\eta \otimes \sigma} A \otimes A \xrightarrow{m} A$$

is an isomorphism of left B-modules and right H-comodules.

We further suppose $\psi: H \otimes B \to B$ gives B the structure of a C.H.A. H-module. A is called an <u>extension of H by B</u> when

1) $B \xrightarrow{\eta} A \xrightarrow{\phi} A \otimes H$ is a split exact sequence,

2) The following diagram is commutative,

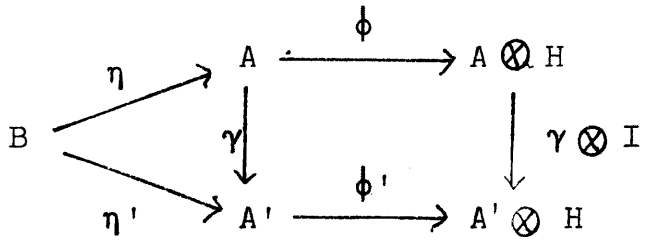


Given extensions A, A' of H by B, where the split exact sequences are

$$B \xrightarrow{\eta} A \xrightarrow{\phi} A \otimes H$$

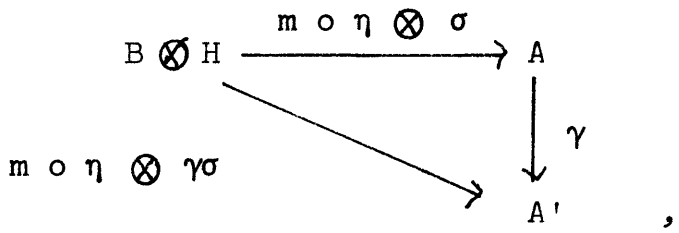
$$B \xrightarrow{\eta'} A' \xrightarrow{\phi'} A' \otimes H ,$$

we say they are <u>isomorphic</u> if there is an algebra morphism $\gamma: A \to A'$, such that



is commutative.

In this case γ is a left B-module morphism and right H-comodule morphism. If $\sigma: H \to A$ is a morphism of right H-comodules and is regular then $\gamma\sigma: H \to A'$ has the same properties. Then the diagram



is commutative; the horizontal and diagonal maps are isomorphisms; hence, γ is an algebra isomorphism. Extensions being isomorphic is an equivalence relation and we can form the isomorphism classes of extensions.

Examples of Extensions, the Smash Product

We now define the smash product for an algebra which is a left H.A. H-module. When the algebra is a left C.H.A. H-module the smash product is an extension whose isomorphism class corresponds to the identity. In a sense all other

extensions are isomorphic to a smash product "altered" by a 2-cocycle.

ψ: $H \otimes B \to B$ gives B the structure of a left H.A. H-module. Map $B \otimes H \xrightarrow{\rho} \mathrm{Hom}(B \otimes H, B \otimes H)$, we define the map by showing how $B \otimes H$ acts--from the left--on $B \otimes H$:

$$(B \otimes H) \otimes (B \otimes H) \xrightarrow{I \otimes d \otimes I \otimes I} B \otimes H \otimes H \otimes B \otimes H$$

$$\xrightarrow{(1,2,4,3,5)} B \otimes H \otimes B \otimes H \otimes H$$

$$\xrightarrow{I \otimes \psi \otimes m} B \otimes B \otimes H \xrightarrow{m \otimes I} B \otimes H \quad .$$

If $b, \beta \in B \qquad h, \xi \in H$

$$\rho(b \otimes h)(\beta \otimes \xi) = \sum_i b(h_i' \cdot \beta) \otimes h_i''\xi \quad .$$

ρ is injective since $\rho(b \otimes h)(1 \otimes 1) = b \otimes h$. $\mathrm{End}(B \otimes H) = \mathrm{Hom}(B \otimes H, B \otimes H)$ has a usual algebra structure by means of composition, Im ρ is a subalgebra of $\mathrm{End}(B \otimes H)$ since $\rho(b \otimes h)\rho(\beta \otimes \xi) = \rho(\sum_i bh_i' \cdot \beta \otimes h_i''\xi)$. We define an associative algebra structure on $B \otimes H$ by insisting ρ be an algebra morphism. $B \otimes H$ with this structure will be denoted $B \overset{\varepsilon}{\otimes} H$. The above formula shows:

$$b \overset{\varepsilon}{\otimes} h, \quad \beta \overset{\varepsilon}{\otimes} \xi \in B \overset{\varepsilon}{\otimes} H$$

$$(b \overset{\varepsilon}{\otimes} h)(\beta \overset{\varepsilon}{\otimes} \xi) = \sum_i bh_i' \cdot \beta \overset{\varepsilon}{\otimes} h_i''\xi \quad .$$

If B is a C.H.A. H-module and H has an antipode, $B \overset{\varepsilon}{\otimes} H$ is an extension of H by B. Since H is a right H-comodule $B \overset{\varepsilon}{\otimes} H$ is a right H-comodule where

$$b \overset{\varepsilon}{\otimes} h \xrightarrow{\phi} \sum_i b \overset{\varepsilon}{\otimes} h_i' \otimes h_i''$$

ϕ is an algebra morphism so $B \overset{\varepsilon}{\otimes} H$ is a right H-comodule --as an algebra.

$$\eta: B \xrightarrow{I \otimes k} B \overset{\varepsilon}{\otimes} H$$

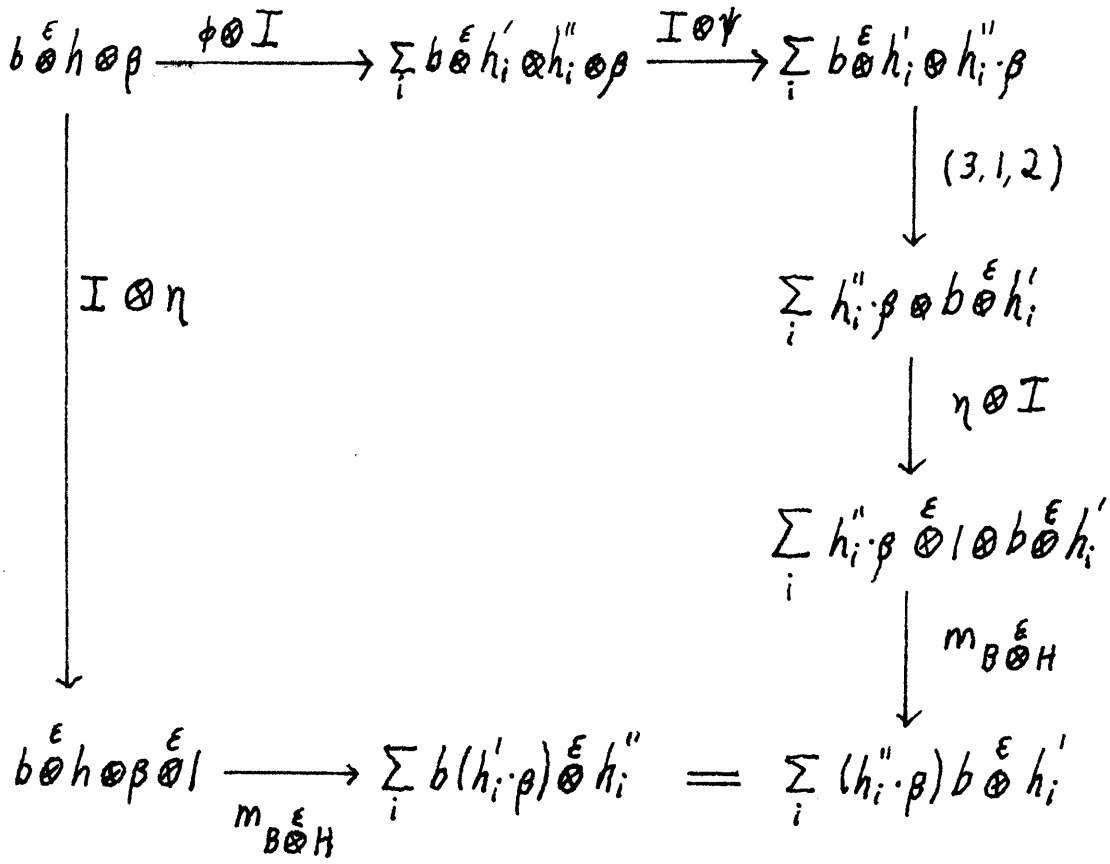
is an injective algebra morphism and $\operatorname{Im} \eta = (B \overset{\varepsilon}{\otimes} H)\square^{H} k$, so

$$B \xrightarrow{\eta} B \overset{\varepsilon}{\otimes} H \xrightarrow{\phi} B \overset{\varepsilon}{\otimes} H \otimes H$$

is a left exact sequence which is split exact because

$$\sigma = k \otimes I: H \to B \overset{\varepsilon}{\otimes} H$$

is a morphism of right H-comodules and has inverse $k \otimes S$, S the antipode of H. With $b, \beta \in B$, $h \in H$



Equality holds because B is commutative and H is co-commutative. This is the second condition required of extensions.

We have really proved a theorem of Kostant's about the smash product when at the end of chapter II we showed if H were a split conilpotent Hopf algebra with antipode then

$$H^e \otimes \Gamma(G) \xrightarrow{m} H$$

is a linear isomorphism. $\Gamma(G)$ is a group algebra Hopf algebra, if $\Gamma(G)$ acts on H^e by $g \cdot h = ghg^{-1}$, $g \in G$

$h \in H^e$ then H^e is a left H.A. $\Gamma(G)$-module. We can now say

$$H^e \overset{\varepsilon}{\otimes} \Gamma(G) \xrightarrow{m} H$$

is an algebra isomorphism. In this case the smash product has further structure. H^e is a Hopf algebra as is $\Gamma(G)$, $H^e \overset{\varepsilon}{\otimes} 1$, $1 \overset{\varepsilon}{\otimes} \Gamma(G)$ generate $H^e \overset{\varepsilon}{\otimes} \Gamma(G)$ so that $H^e \overset{\varepsilon}{\otimes} \Gamma(G)$ is a coalgebra. That it is a Hopf algebra follows because $m: H^e \overset{\varepsilon}{\otimes} \Gamma(G) \to H$ is a coalgebra isomorphism as well as algebra isomorphism. Thus

$$H^e \overset{\varepsilon}{\otimes} \Gamma(G) \xrightarrow{m} H$$

is an isomorphism of Hopf algebras.

We generalize the smash product as follows; suppose B is a C.H.A. H-module $\psi: H \otimes B \to B$, $f \in \mathrm{Hom}(H \otimes H, B)$, and H has an antipode. $B \overset{f}{\otimes} H$ is the vector space with multiplication

$$1)\quad (B \overset{f}{\otimes} H) \otimes (B \overset{f}{\otimes} H) \xrightarrow{I \otimes d^2 \otimes I \otimes d}$$

$$B \otimes H \otimes H \otimes H \otimes B \otimes H \otimes H \xrightarrow{1,2,5,3,6,4,7}$$

$$B \otimes H \otimes B \otimes H \otimes H \otimes H \otimes H \xrightarrow{I \otimes \psi \otimes f \otimes m} B \otimes B \otimes B \otimes H$$

$$\xrightarrow{m^2 \otimes I} B \overset{f}{\otimes} H, \text{ or}$$

$$(b \overset{f}{\otimes} h)(\beta \overset{f}{\otimes} \xi) = \sum_{i,j} bh_i' \cdot \beta f(h_i'' \otimes \xi_j') \otimes h_i''' \xi_j'' .$$

Lemma 1): $B \overset{f}{\otimes} H$ is an extension of H by B with $\eta: B \xrightarrow{I \otimes k} B \overset{f}{\otimes} H$, $\sigma: H \xrightarrow{k \otimes I} B \overset{f}{\otimes} H$ a regular morphism of right H-comodules ($B \overset{f}{\otimes} H$, H have the usual right H-comodule structures) if and only if $f \in \mathrm{Reg}_1^{\,2}(H,B)$ and f is a 2-cocycle.

Proof: Suppose $f \in \mathrm{Reg}_1^{\,2}(H,B)$ is a 2-cocycle then

$$2)\quad \psi \circ I \otimes f * f^{-1} \circ m \otimes I * f \circ I \otimes m * f^{-1} \otimes \varepsilon = \varepsilon \otimes \varepsilon \otimes \varepsilon \quad \text{or}$$

$$3)\quad \psi \circ I \otimes f * f \circ I \otimes m = f \otimes \varepsilon * f \circ m \otimes I .$$

$f^{-1} \circ m \otimes I \,|\, H \otimes k \otimes k$, $f \circ I \otimes m \,|\, H \otimes k \otimes k$ can be considered as maps of H to B, and as such they are inverse maps. Thus applying both sides of the formula 2) to $h \otimes 1 \otimes 1$, gives $f^{-1}(h \otimes 1) = \varepsilon(h)$ thus $f(h \otimes 1) = \varepsilon(h)$. Similarly $f(1 \otimes h) = \varepsilon(h)$.

Let $\rho: B \otimes H \to \mathrm{End}(B \otimes H)$ be defined by the left action of $B \otimes H$ on $B \otimes H$ given in 1) (with the f's removed). ρ is injective since

$$\rho(b \otimes h)(1 \otimes 1) = b \otimes h .$$

$$\rho(b\otimes h)\rho(\beta\otimes\xi)(c\otimes g) = \rho(b\otimes h)\Big(\sum_{j,k}\beta(\xi_j'\cdot c)f(\xi_j''\otimes g_k')\otimes\xi_j'''\ g_k''\Big)$$

$$= \sum_{i,j,k} b(h_i'\cdot[\beta(\xi_j'\cdot c)f(\xi_j''\otimes g_k')])f(h_i''\otimes\xi_j'''\ g_k'')\otimes h_i'''\ \xi_j^{(4)}g_k'''$$

$$= \sum_{i,j,k} b(h_i'\cdot\beta)(h_i''\xi_j'\cdot c)\underbrace{(h_i'''\cdot f(\xi_j''\otimes g_k'))f(h_i^{(4)}\otimes\xi_j'''g_k'')}\otimes h_i^{(5)}\xi_j^{(4)}g_k'''$$

(by formula 3))

$$= \sum_{i,j,k} b(h_i'\cdot\beta)(h_i''\xi_j'\cdot c)\underbrace{f(h_i'''\otimes\xi_j'')f(h_i^{(4)}\xi_j'''\otimes g_k')}\otimes h_i^{(5)}\xi_j^{(4)}g_k''$$

$$= \sum_{i,j,k} b(h_i'\cdot\beta)f(h_i''\otimes\xi_j')(h_i'''\xi_j''\cdot c)f(h_i^{(4)}\xi_j'''\otimes g_k')\otimes h_i^{(5)}\xi_j^{(4)}g_k''$$

$$= \rho\Big(\sum_{i,j} b(h_i'\cdot\beta)f(h_i''\otimes\xi_j')\otimes h_i''\xi_j''\Big)(c\otimes g)\ .$$

This shows Im ρ is a subalgebra of End$(B\otimes H)$ and if we transport the structure of Im ρ to $B\otimes H$ we have

$B \overset{f}{\otimes} H$, thus $B \overset{f}{\otimes} H$ is associative. $\varepsilon(h) = f(h \otimes 1) = f(1 \otimes h)$ implies $1 \overset{f}{\otimes} 1$ is the unit for $B \overset{f}{\otimes} H$ and $B \overset{f}{\otimes} H$ is an algebra.

$\eta: B \xrightarrow{I \otimes k} B \overset{f}{\otimes} H$ is an injective algebra morphism. $B \overset{f}{\otimes} H$ is a right H-comodule as an algebra. $\eta(B) = (B \overset{f}{\otimes} H) \square^H k$.

$$B \xrightarrow{\eta} B \overset{f}{\otimes} H \xrightarrow{\phi} B \overset{f}{\otimes} H \otimes H$$

is a left exact sequence. $\sigma: H \xrightarrow{k \otimes I} B \overset{f}{\otimes} H$ is a right H-comodule morphism with inverse $\sigma^{-1} = [\eta \circ f^{-1} \circ (S \otimes I) \circ d] * \sigma \circ S$,

$$= \sigma \circ S * [\eta \circ f^{-1} \circ (I \otimes S) \circ d], \text{ because}$$

$$\sigma^{-1} * \sigma = [\eta \circ f^{-1} \circ (S \otimes I) \circ d] * [\sigma \circ S * \sigma],$$

$$\sigma \circ S * \sigma(h) = \sum_i [(1 \overset{f}{\otimes} S(h_i'))][(1 \overset{f}{\otimes} h_i'')] \quad (dS = S \otimes S \circ d,$$

H cocommutative)

$$= \sum_i f(S(h_i') \otimes h_i'') \overset{f}{\otimes} S(h_i''')h_i \quad (4)$$

$$= \sum_i f(S(h_i') \otimes h_i'') \overset{f}{\otimes} 1$$

$$= \eta \circ f \circ (S \otimes I) \circ d\,(h).$$

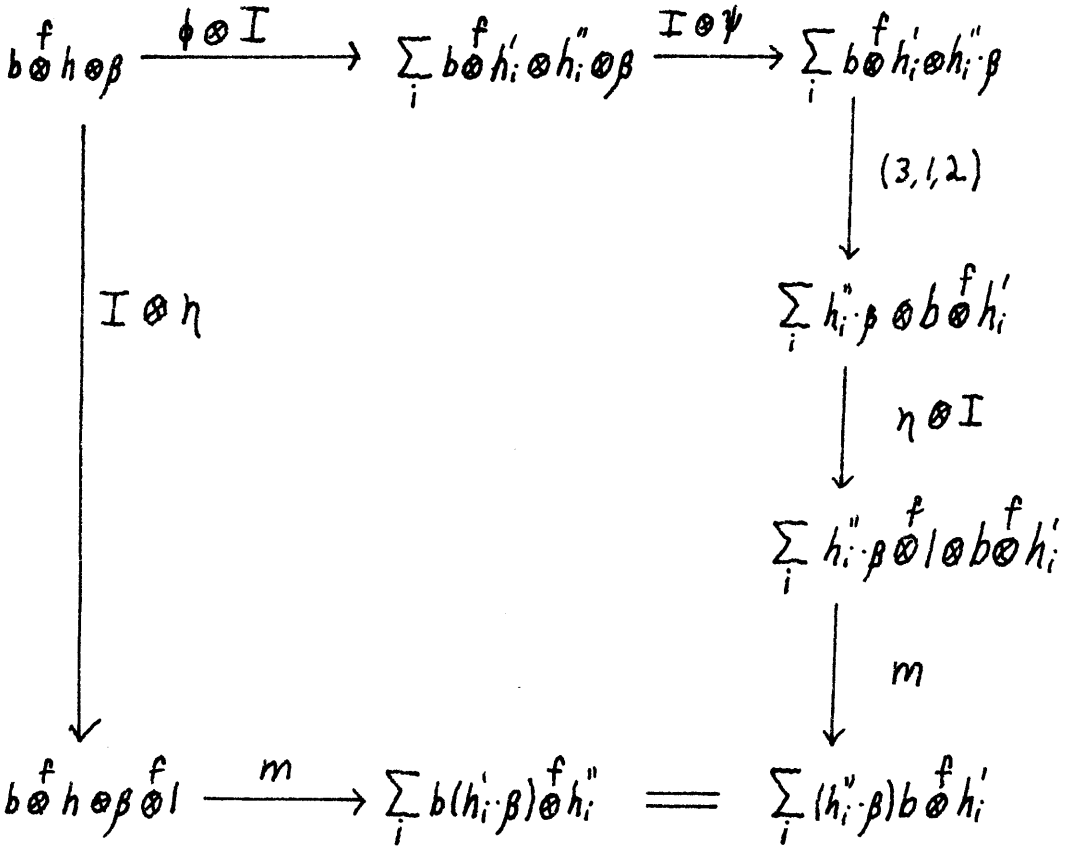
Thus $\sigma \circ S * \sigma = \eta \circ f \circ (S \otimes I) \circ d$ which is inverse to $\eta \circ f^{-1} \circ (S \otimes I) \circ d$ and $\sigma^{-1} * \sigma = \varepsilon$. Similarly σ has right inverse

$$\sigma \circ S * [\eta \circ f^{-1} \circ (I \otimes^f S) \circ d]$$

which shows σ is regular and the two inverses equal. Thus

$$B \xrightarrow{\eta} B \otimes^f H \xrightarrow{\phi} B \otimes^f H \otimes H$$

is a split exact sequence and σ is a regular right H-comodule morphism.



Thus $B \otimes^f H$ is an extension of H by B.

Conversely, suppose $B \otimes^f H$ is an extension of H by B with $\eta: B \xrightarrow{I \otimes k} B \otimes^f H$ an algebra morphism $\sigma: H \xrightarrow{k \otimes I} B \otimes^f H$ a regular morphism of right H-comodules.

Observe $m_{B \overset{f}{\otimes} H} \circ \sigma \otimes \sigma = \eta \circ f * \sigma \circ m$ as morphisms from $H \otimes H$ to $B \overset{f}{\otimes} H$, (in fact $B \overset{f}{\otimes} H$ is $B \overset{\varepsilon}{\otimes} H$ "altered" by this formula). Since m is a coalgebra morphism and σ invertible we obtain

$$m \circ \sigma \otimes \sigma * \sigma^{-1} \circ m = \eta \circ f .$$

This shows f is invertible where

$$\sigma \circ m * m \circ (2,1) \circ \sigma^{-1} \otimes \sigma^{-1} = \eta \circ f^{-1} .$$

Hence, $f \in \mathrm{Reg}^2(H,B)$. η is an algebra morphism implies $1 \overset{f}{\otimes} 1$ is the unit of $B \overset{f}{\otimes} H$ which implies $f(1 \otimes 1) = 1$ so $f \in \mathrm{Reg}_1^{\,2}(H,B)$. Finally by associativity

$$((1 \overset{f}{\otimes} h)(1 \overset{f}{\otimes} \xi))(1 \overset{f}{\otimes} g) = (1 \overset{f}{\otimes} h)((1 \overset{f}{\otimes} \xi)(1 \overset{f}{\otimes} g))$$

implies

$$\sum_{i,j,k} f(h_i' \otimes \xi_j')f(h_i''\xi_j'' \otimes g_k') \overset{f}{\otimes} h_i''' \xi_j''' g_k''$$

$$= \sum_{i,j,k} (h_i' \cdot f(\xi_j' \otimes g_k'))f(h_i'' \otimes \xi_j''g_k'') \overset{f}{\otimes} h_i''' \xi_j''' g_k''' .$$

Taking $\mathrm{I} \otimes \varepsilon$ of both sides gives

$$(f \otimes \varepsilon) * (f \circ m \otimes I) = (\psi \circ I \otimes f) * (f \circ I \otimes m) ,$$

since f is regular this says f is a 2-cocycle.

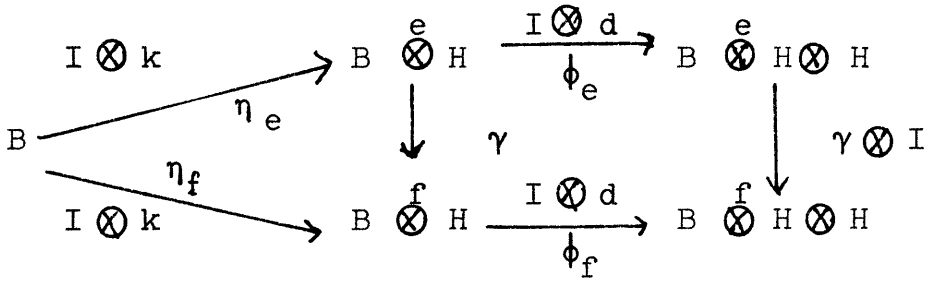
Q.E.D.

When $f = \varepsilon \otimes \varepsilon = \varepsilon_{H \otimes H}$, then $B \overset{f}{\otimes} H$ is $B \overset{\varepsilon}{\otimes} H$

the smash product.

Lemma 2): Suppose $e, f \in \mathrm{Reg}_1^2(H,B)$ are cocycles, then the extensions $B \overset{e}{\otimes} H$, $B \overset{f}{\otimes} H$ are isomorphic if and only if e, f are homologous in $\mathrm{Reg}_1^2(H,B)$.

Proof: Suppose $\gamma: B \overset{e}{\otimes} H \to B \overset{f}{\otimes} H$ is an isomorphism of extensions. Then



is commutative and γ is an algebra morphism. By theorem 1 chapter II

$$\mathrm{Im}(B \overset{f}{\otimes} H \xrightarrow{\phi_f} B \overset{f}{\otimes} H \otimes H \xrightarrow{I \otimes \sigma_f^{-1}} B \overset{f}{\otimes} H \otimes B \overset{f}{\otimes} H \xrightarrow{m} B \overset{f}{\otimes} H)$$

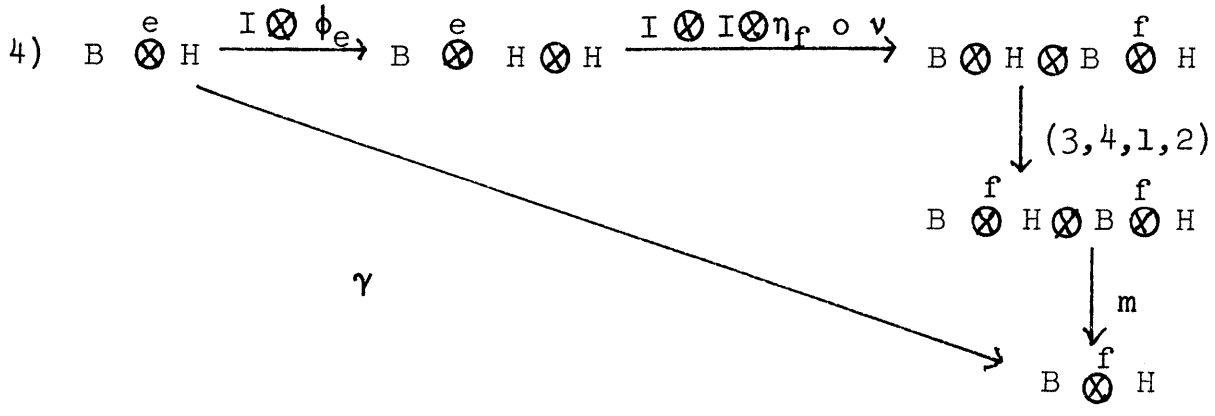
$\subset \eta(B)$ so we consider

$P: B \overset{f}{\otimes} H \to B$ where

$$\eta_f \circ P = m_{B \overset{f}{\otimes} H} \circ I \otimes \sigma_f^{-1} \circ \phi_f .$$

We define $\nu: H \xrightarrow{\sigma_e} B \overset{e}{\otimes} H \xrightarrow{\gamma} B \overset{f}{\otimes} H \xrightarrow{P} B$

and wish to show commutivity of:



5) that is $\gamma(b \overset{e}{\otimes} h) = \sum_i (\eta_f \circ \nu(h_i''))(b \overset{f}{\otimes} h_i')$.

By definition $\eta_f \circ \nu = m_{B \overset{\circ}{\otimes} H} \circ I \otimes \sigma_f^{-1} \circ \phi_f \circ \gamma \circ \sigma_e$

(γ , σ_e comodule morphisms)

$= m_{B \overset{f}{\otimes} H} \circ I \otimes \sigma_f^{-1} \circ [(\gamma \circ \sigma_e) \otimes I] \circ d$ so

$\eta_f \circ \nu(h) = \sum_i \gamma(1 \overset{e}{\otimes} h_i')\sigma_f^{-1}(h_i'')$. Inserting this in the right side of 5) and using cocommutivity gives

6) $\sum_i \gamma(1 \overset{e}{\otimes} h_i')\sigma_f^{-1}(h_i'')(b \overset{f}{\otimes} h_i''')$

$= \sum_i \gamma(1 \overset{e}{\otimes} h_i')\sigma_f^{-1}(h_i'')(b \overset{f}{\otimes} 1)\sigma_f(h_i''')$.

In theorem 1 we showed

$$\phi_f \circ \sigma_f^{-1} = \sigma_f^{-1} \otimes S \circ (2,1) \circ d$$

applying this and the second condition for extensions, (and cocommutivity):

$$\sigma_f^{-1}(h)(b \overset{f}{\otimes} 1) = \sum_i (S(h_i') \cdot b \overset{f}{\otimes} 1)\sigma_f^{-1}(h_i'') \ .$$

Inserting this in the right side of 6) yields

$$\sum_i \gamma(1 \overset{e}{\otimes} h_i')(S(h_i'') \cdot b \overset{f}{\otimes} 1)\sigma_f^{-1}(h_i''')\sigma_f(h_i^{(4)})$$

$$= \sum_i \gamma(1 \overset{e}{\otimes} h_i')(S(h_i'') \cdot b \overset{f}{\otimes} 1)\ \varepsilon(h_i''')$$

$$7) \qquad = \sum_i \gamma(1 \overset{e}{\otimes} h_i')(S(h_i'') \cdot b \overset{f}{\otimes} 1) \ .$$

Again using the second condition for extensions and that γ is a comodule morphism,

$$7) \quad = \sum_i ([h_i' \cdot (S(h_i'') \cdot b)] \overset{f}{\otimes} 1)\gamma(1 \overset{e}{\otimes} h_i''')$$

$$= \sum_i ((h_i' S(h_i'')) \cdot b \overset{f}{\otimes} 1)\gamma(1 \overset{e}{\otimes} h_i''')$$

$$= \sum_i (\varepsilon(h_i') \cdot b \overset{f}{\otimes} 1)\gamma(1 \overset{e}{\otimes} h_i'')$$

$$= (b \overset{f}{\otimes} 1)\gamma(1 \overset{e}{\otimes} h) = \gamma(b \overset{e}{\otimes} h) \ .$$

The last equality, because γ is a left B-module morphism. Thus we have established 4) and 5) .

Applying 5) to the fact "γ is an algebra morphism":

$$\gamma(1 \overset{e}{\otimes} h)\gamma(1 \overset{e}{\otimes} \xi) = \gamma((1 \overset{e}{\otimes} h)(1 \overset{e}{\otimes} \xi)) \ .$$

$$\text{Left side} = \sum_{i,j} (\nu(h_i') \overset{f}{\otimes} h_i'')(\nu(\xi_j') \overset{f}{\otimes} \xi_j'')$$

$$8) \quad = \sum_{i,j} \nu(h_i')(h_i'' \cdot \nu(\xi_j'))f(h_i''' \otimes \xi_j'') \otimes h_i^{(4)}\xi_j''' \ .$$

$$\text{Right side} = \gamma(\sum_{i,j} e(h_i' \otimes \xi_j') \otimes h_i''\xi_j'')$$

$$9) \quad = \sum_{i,j} \nu(h_i'\xi_j') \ e \ (h_i'' \otimes \xi_j'') \otimes h_i'''\xi_j''' \ .$$

Taking $I \otimes \varepsilon$ of 8), 9) and equating gives:

$$10) \quad (\nu \otimes \varepsilon) * (\psi \circ I \otimes \nu) * f = (\nu \circ m) * e \ .$$

Since $\eta_f \circ \nu = m_{B \overset{f}{\otimes} H} \circ I \otimes \sigma_f^{-1} \circ [(\gamma \circ \sigma_e) \otimes I] \circ d$

$$= (\gamma \circ \sigma_e) * \sigma_f^{-1}$$

it follows ν is regular where

$$\eta_f \circ \nu^{-1} = \sigma_f * (\gamma \circ \sigma_e^{-1}) \ .$$

Moreover $\sigma_e(1) = 1 \overset{e}{\otimes} 1$; and $\sigma_f(1) = 1 \overset{f}{\otimes} 1$ implies $\sigma_f^{-1}(1) = 1 \overset{f}{\otimes} 1$ thus $\nu(1) = 1$ and

$$\nu \in \mathrm{Reg}_1^{\,1}(H,B) \ .$$

By 10) $\delta^1\nu = e * f^{-1}$ so e and f are homologous.

Conversely suppose e and f are homologous let $\delta^1\nu = \varepsilon * f^{-1}$, $\nu \in \mathrm{Reg}_1^{\,1}(H,B)$. Define γ: $B \overset{e}{\otimes} H \to B \overset{f}{\otimes} H$ in terms of ν by 4) .

$$\gamma(1 \overset{e}{\otimes} 1) = \nu(1) \ 1 \overset{f}{\otimes} 1 = 1 \overset{f}{\otimes} 1 \ .$$

$$\gamma(b \overset{e}{\otimes} h)\gamma(\beta \overset{e}{\otimes} \xi) = \sum_{i,j} (\nu(h_i')b \overset{f}{\otimes} h_i'')(\nu(\xi_j')\beta \overset{f}{\otimes} \xi_j'')$$

$$= \sum_{i,j} \nu(h_i')b(h_i'' \cdot (\nu(\xi_j')\beta))f(h_i''' \otimes \xi_j'') \overset{f}{\otimes} h_i^{(4)}{}_{\xi_j}{}^{(3)}$$

$$= \sum_{i,j} b(h_i' \cdot \beta)\nu(h_i'')(h_i''' \cdot \nu(\xi_j'))f(h_i^{(4)} \otimes \xi_j'') \overset{f}{\otimes} h_i^{(5)}{}_{\xi_j}{}^{(3)} .$$

(since $\delta^1\nu = e * f^{-1}$ 10) is satisfied)

$$= \sum_{i,j} b(h_i' \cdot \beta)\nu(h_i''\xi_j') \, e \, (h_i''' \otimes \xi_j'') \overset{f}{\otimes} h_i^{(4)}{}_{\xi_j}{}^{(3)}$$

$$= \sum_{i,j} \gamma(b(h_i' \cdot \beta) \, e \, (h_i'' \otimes \xi_j') \overset{e}{\otimes} h_i''' \xi_j'')$$

$$= \gamma([b \overset{e}{\otimes} h][\beta \overset{e}{\otimes} \xi]) .$$

So γ is an algebra morphism. From the definition of γ it is a left B-module morphism and right H-comodule morphism; hence, γ is an isomorphism of extensions.

Q.E.D.

Lemma 3): Each extension is isomorphic to an extension of the form $B \overset{f}{\otimes} H$.

Proof: Let the extension be A , the split exact sequence be

$$B \xrightarrow{\eta} A \xrightarrow{\phi} A \otimes H ,$$

$\sigma: H \to A$ be a regular morphism of right H-comodules. Consider

$$(m \circ \sigma \otimes \sigma) * (\sigma^{-1} \circ m): H \otimes H \to A .$$

The diagram

$$\begin{array}{ccc} H \otimes H & \xrightarrow{(m \circ \sigma \otimes \sigma) * (\sigma^{-1} \circ m)} & A \\ \downarrow & & \downarrow \phi \\ A & \xrightarrow[I \otimes k]{} & A \otimes H \end{array}$$

is commutative; hence,

$$\mathrm{Im}((m \circ \sigma \otimes \sigma) * (\sigma^{-1} \circ m)) \subset \eta(B)$$

and there is $f: H \otimes H \to B$ where

$$\eta \circ f = (m \circ \sigma \otimes \sigma) * (\sigma^{-1} \circ m) .$$

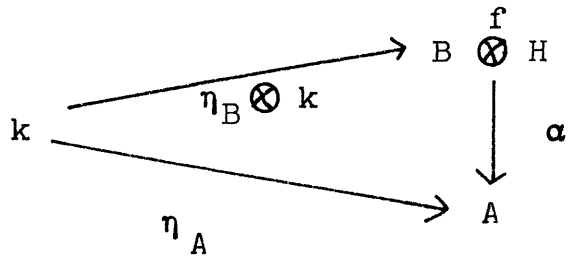
By theorem 1

$$\alpha: B \overset{f}{\otimes} H \xrightarrow{\eta \otimes \sigma} A \otimes A \xrightarrow{m} A$$

is an isomorphism of left B-modules and right H-comodules so the diagram

$$\begin{array}{ccccc} & & B \overset{f}{\otimes} H & \xrightarrow[\phi_f]{} & B \overset{f}{\otimes} H \otimes H \\ B & \overset{I \otimes k}{\nearrow} & \downarrow \alpha & & \downarrow \alpha \otimes I \\ & \underset{\eta}{\searrow} & A & \xrightarrow{\phi} & A \otimes H \end{array} ,$$

is commutative. In particular



is commutative. Since α is bijective if we show it is multiplicative, it implies $B \overset{f}{\otimes} H$ is an algebra and an extension; and it implies α is an isomorphism of extensions.

$$\alpha(b \overset{f}{\otimes} h)\alpha(\beta \overset{f}{\otimes} \xi) = \eta(b)\sigma(h)\eta(\beta)\sigma(\xi)$$

(by second extension condition and σ a comodule morphism)

$$= \sum_i \eta(b(h_i' \cdot \beta))\sigma(h_i'')\sigma(\xi)$$

(by definition of f, η o f * σ o m = m o $\sigma \otimes \sigma$

$$= \sum_{i,j} \eta(b(h_i' \cdot \beta)f(h_i'' \otimes \xi_j')\sigma(h_i''' \xi_j'')$$

$$= \sum_{i,j} \alpha(b(h_i' \cdot \beta)f(h_i'' \otimes \xi_j') \overset{f}{\otimes} h_i''' \xi_j'')$$

$$= \alpha[(b \overset{f}{\otimes} h)(\beta \overset{f}{\otimes} \xi)] .$$

Q.E.D.

Theorem 3: When H has an antipode there is a natural correspondence between the isomorphism classes of extensions and $H^2(H,B)$. Under this correspondence $e \in H^2(H,B)$ corresponds to the smash product $B \overset{\varepsilon}{\otimes} H$.

Proof: By lemmas 1, 2 there is a natural bijective correspondence between $H^2(H,B)$ and those isomorphism classes containing an extension of the form $B \overset{f}{\otimes} H$, by lemma 3 all isomorphism classes are included.

Since the smash product is $B \overset{\varepsilon}{\underset{\varepsilon}{\otimes}} H$ the last statement holds.

Q.E.D.

Suppose B is a finite Galois extension of k and $H = \Gamma(G)$ where G is the Galois group. B is an H.A. H-module where the structure is induced by G. Then extensions of the form $B \overset{f}{\otimes} H$ are central simple algebras over k. This is treated in [1], Rings with Minimum Condition, under the name "crossed products". Their notion of "factor set" is precisely our 2-cocycle. Since $B \overset{f}{\otimes} H$ is central simple, and since the extensions equivalent to $B \overset{f}{\otimes} H$ are isomorphic as algebras; they are algebras in the same class--element--in the Brauer Group. That distinct classes of extensions correspond to distinct elements of the Brauer Group follows from their Corollary 8.5C which says the classes of extensions correspond to those elements of the Brauer Group with splitting field B. The smash product $B \overset{\varepsilon}{\otimes} H$ is a total matrix algebra (over k), this is their Corollary 8.4G.

In the Brauer Group the multiplication corresponds to the tensor product of algebras, we give a method for

forming the product of two extensions so the correspondence of theorem 3 is a group isomorphism.

Let A, $\tilde{A}$ be extensions of H by B where the split exact sequences are:

$$B \xrightarrow{\eta} A \xrightarrow{\phi} A \otimes H$$

$$B \xrightarrow{\tilde{\eta}} \tilde{A} \xrightarrow{\tilde{\phi}} \tilde{A} \otimes H \ .$$

In $A \otimes \tilde{A}$ let $T = \mathrm{Ker}(((1,3,2) \circ \phi \otimes I) - I \otimes \tilde{\phi})$, T is a subalgebra of $A \otimes \tilde{A}$ since it is the kernel of the difference of two algebra morphisms. The defining property of T is expressed in the commutivity of:

$$\begin{array}{ccc} T & \longrightarrow & A \otimes \tilde{A} \\ \downarrow & & \downarrow I \otimes \tilde{\phi} \\ A \otimes \tilde{A} & & \\ \downarrow \phi \otimes I & & \\ A \otimes H \otimes \tilde{A} & \xrightarrow[(1,3,2)]{} & A \otimes \tilde{A} \otimes H \end{array} ,$$

let $\phi_T = (T \to A \otimes \tilde{A} \xrightarrow{I \otimes \tilde{\phi}} A \otimes \tilde{A} \otimes H)$. Next we show $\mathrm{Im}\ \phi_T \subset T \otimes H$ so that we consider $\phi_T \colon T \to T \otimes H$.

$$T \otimes H = \mathrm{Ker}([((1,3,2) \circ \phi \otimes I) - I \otimes \tilde{\phi}] \otimes I),$$

$$[(1,3,2) \circ \phi \otimes I - I \otimes \tilde{\phi}] \otimes I \circ \phi_T =$$

$$(1,3,2,4) \circ \phi \otimes I \otimes I \circ \phi_T - I \otimes \tilde{\phi} \otimes I \circ \phi_T =$$

$$(1,3,2,4) \circ \phi \otimes I \otimes I \circ (1,3,2) \circ \phi \otimes I - I \otimes \tilde{\phi} \otimes I \circ I \otimes \tilde{\phi} =$$

$$I \otimes I \otimes d \circ (1,3,2) \circ \phi \otimes I - I \otimes I \otimes d \circ I \otimes \tilde{\phi} =$$

$$(I \otimes I \otimes d)[(1,3,2) \circ \phi \otimes I - I \otimes \tilde{\phi}]$$

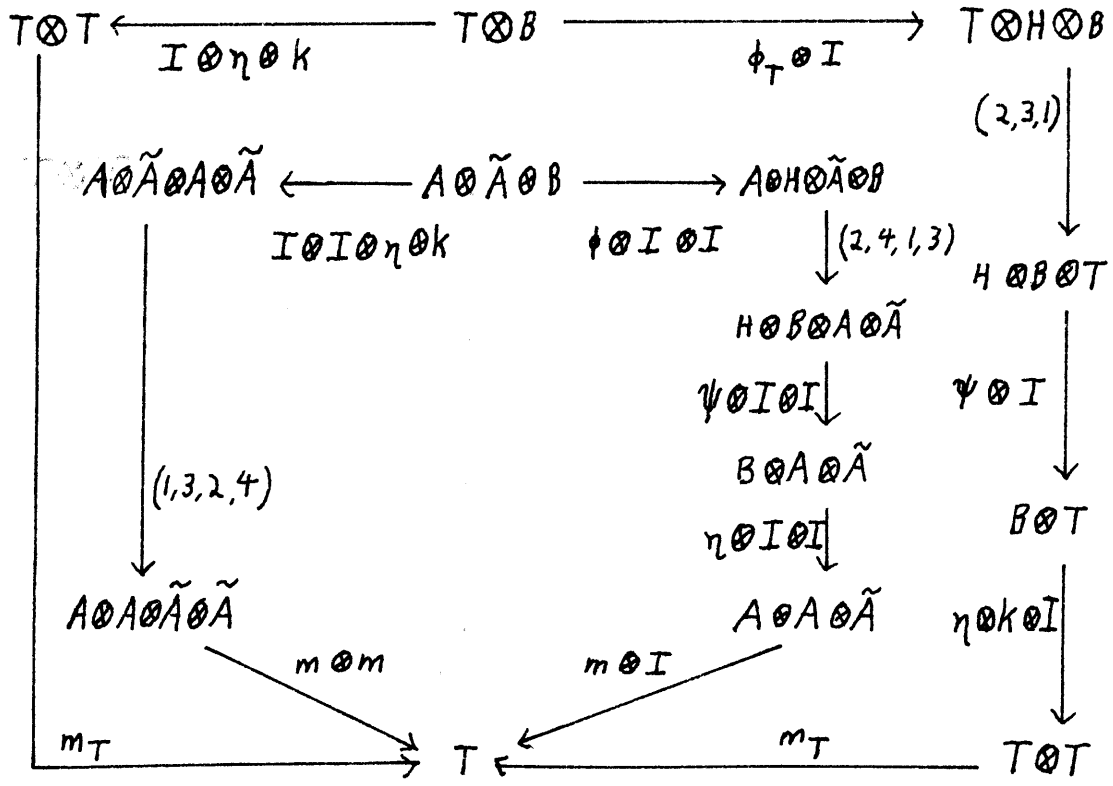
which is zero applied to T, thus

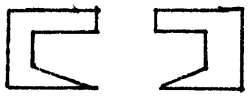
$$\phi_T : T \to T \otimes H$$

and it is clear T is an H-comodule (as an algebra).

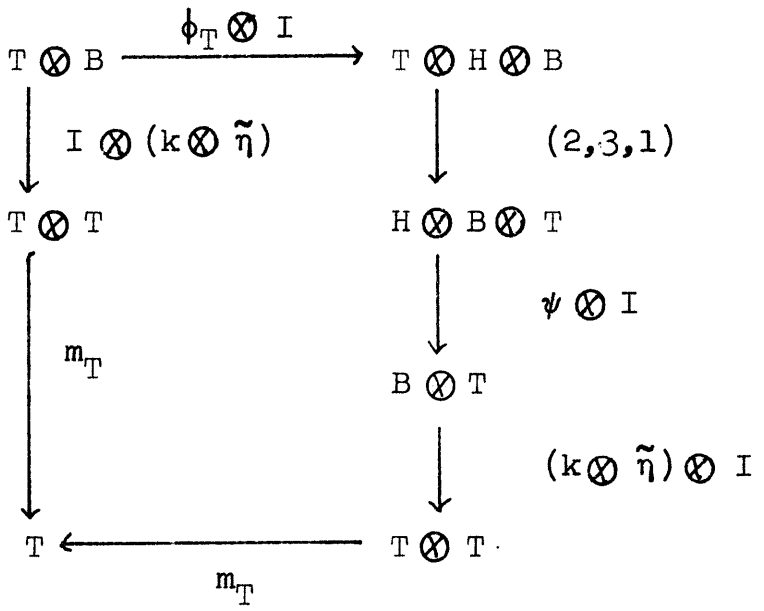
$$\eta \otimes k - k \otimes \tilde{\eta} : B \to A \otimes \tilde{A}$$

If $I = \mathrm{Im}(\eta \otimes k - k \otimes \tilde{\eta})$ it is clear $I \subset T$. We propose to show the right ideal generated by I in T is a 2-sided ideal. Note $\mathrm{Im}(\eta \otimes k) \subset T \supset \mathrm{Im}(k \otimes \tilde{\eta})$ we consider these as maps to T. The diagram

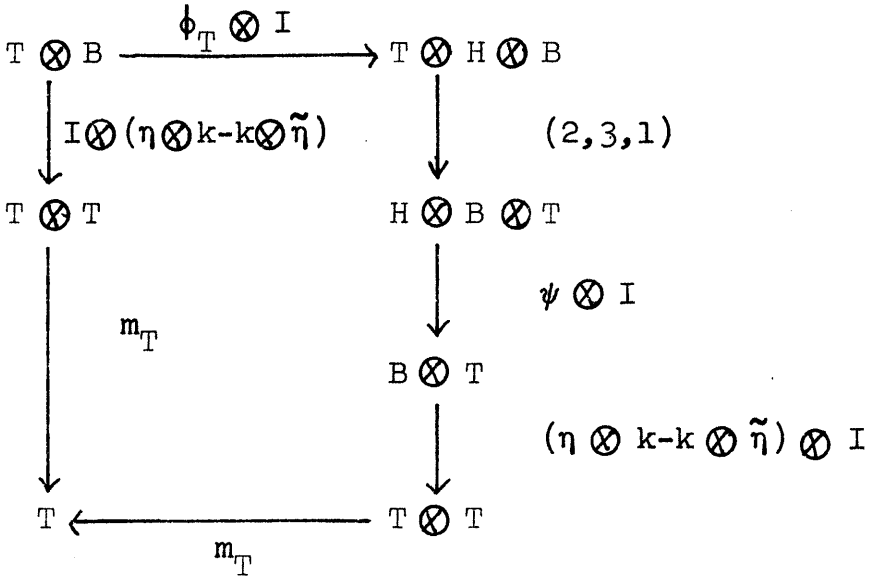


is commutative where the inner pentagon commutes by the second extension condition, and the  commute from the definitions.

Similarly the diagram:



is commutative. Thus



is commutative which shows $TI \subset IT$ and the right ideal

is 2-sided. I is a sub comodule and ϕ_T is an algebra morphism so IT is a sub comodule and the algebra $D = T/IT$ is an H-comodule (as an algebra). Let $\phi_D: D \to D \otimes H$ be the comodule structure. From the definition of I ,

$$\begin{array}{ccc} B & \xrightarrow{\eta \otimes k} & T \\ \downarrow & & \downarrow \\ T & \xrightarrow{\quad} & D \end{array} \qquad k \otimes \tilde{\eta}$$

is commutative, let $\eta_D = (B \xrightarrow{\eta \otimes k} T \to D)$. $\eta_D: B \to D$ is an algebra morphism, and $\operatorname{Im} \eta_D \subset D \ \square^H k$.

Since A is an extension we have $\sigma: H \to A$ a regular morphism of right H-comodules and $P: A \to B$ where $\eta \circ P = A \xrightarrow{\phi} A \otimes H \xrightarrow{I \otimes \sigma^{-1}} A \otimes A \xrightarrow{m} A$. (See theorem 1.) For $\tilde{A}$ we have $\tilde{\sigma}$, $\tilde{P}$. P, $\tilde{P}$ are morphisms of left B-modules.

Consider $H \xrightarrow{\sigma \otimes \tilde{\sigma} \circ d} A \otimes \tilde{A}$, the image of this map lies in T , let

$$\sigma_D: H \xrightarrow{d} H \otimes H \xrightarrow{\sigma \otimes \tilde{\sigma}} T \to D .$$

σ_D is an invertible morphism of right H-comodules where the inverse is

$$\sigma_D{}^{-1}: H \xrightarrow{d} H \otimes H \xrightarrow{\sigma^{-1} \otimes \tilde{\sigma}^{-1}} T \to D .$$

Then we have $P_D: D \to D \ \square^H k$ where

$$P_D = D \xrightarrow[\phi_D]{} D \otimes H \xrightarrow[I \otimes \sigma_D^{-1}]{} D \otimes D \xrightarrow{m} D \,\square^H k \,.$$

The diagram:

$$\begin{array}{ccccc} B \otimes B & \xleftarrow{P \otimes \tilde{P}} & T & \longrightarrow & D \\ \downarrow{\scriptstyle \eta \otimes \tilde{\eta}} & & & & \downarrow{\scriptstyle P_D} \\ T & & \longrightarrow & & D \,\square^H k \end{array}$$

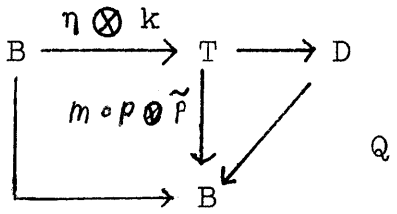
is commutative. It can be rewritten

$$\begin{array}{ccc} T & \longrightarrow & D \\ \downarrow{\scriptstyle m \circ P \otimes \tilde{P}} & & \downarrow{\scriptstyle P_D} \\ B & \xrightarrow[\eta_D]{} & D \,\square^H k \,. \end{array}$$

Since $\operatorname{Im} P_D = D \,\square^H k$, $T \to D$ is surjective, it follows $\operatorname{Im} \eta_D = D \,\square^H k$. Clearly $I \subset \operatorname{Ker} m \circ P \otimes \tilde{P}$, since P, $\tilde{P}$ are left B-module morphisms $IT \subset \operatorname{Ker} m \circ P \otimes \tilde{P}$, or there is a factoring Q,

$$\begin{array}{ccc} T & \longrightarrow & D \\ \downarrow{\scriptstyle m \circ P \otimes \tilde{P}} & \swarrow_{Q} & \\ B & & . \end{array}$$

Thus



is commutative. The horizontal composite is η_D hence we have shown η_D is injective. Thus

$$B \xrightarrow{\eta_D} D \xrightarrow{\phi_D} D \otimes H$$

is a split exact sequence.

The second condition for extensions is satisfied. Thus D is an extension of H by B.

If $\gamma\colon A \to A_1$, $\tilde{\gamma}\colon \tilde{A} \to \tilde{A}_1$ are equivalences of extensions then:

$$\gamma \otimes \tilde{\gamma}\colon A \otimes \tilde{A} \to A_1 \otimes \tilde{A}_1$$

$$\gamma \otimes \tilde{\gamma}|T\colon T \to T_1$$

$\gamma \otimes \tilde{\gamma}|T$ factors to $\gamma_D\colon D \to D_1$ and γ_D is an equivalence of extensions. Thus the method of producting extensions gives the isomorphism classes of extensions a product structure. Direct calculation shows the product of $B \overset{f}{\otimes} H$, $B \overset{\tilde{f}}{\otimes} H$ is extension isomorphic to $B \overset{f * \tilde{f}}{\otimes} H$, so that under the correspondence of theorem 3, the multiplicative structures correspond. This shows the isomorphism classes form a group and the correspondence is a group isomorphism.

Chapter IV

Cohomology

We treat the dual situation to the previous chapter. We outline the definition of abelian cohomology groups $H(B,H)^i$ $i=0,1,2\ldots$, when H is a commutative Hopf algebra, B a cocommutative coalgebra which is a right H-comodule satisfying certain conditions. We also outline the dual extension theory, defining when a coalgebra is an extension of B by H and when extensions are isomorphic. The isomorphism classes of extension again correspond to $H(B,H)^2$, we define the dual extension to $B \overset{f}{\otimes} H$ of the previous chapter; this indicates the correspondence between $H(B,H)^2$ and the isomorphism classes of extensions.

B is a coalgebra, H a Hopf algebra $\phi: B \to B \otimes H$ is a right H-comodule structure for B . $B \otimes B$ is an H-comodule under ϕ^2 . B is a right H.A. H-comodule if

$$d: B \to B \otimes B$$
$$\varepsilon: B \to k ,$$

are comodule morphisms. B is a right C.H.A. H-comodule if B is a right H.A. H-comodule, B is cocommutative and H is commutative.

For a coalgebra C and an algebra $0 < n \in Z$ let

$\mathrm{Hom}(C,A)^n = \mathrm{Hom}(C,A^{[n]})$. Let $\mathrm{Reg}(C,A)^n = (\mathrm{Hom}(C,A)^n)^r$.

Then $\mathrm{Reg}(B,H)^n$ is an abelian group when B is a C.H.A. H-comodule. Let $\mathrm{Reg}(B,H)^0 = \mathrm{Reg}(B,k)^1$.

Let B be a right C.H.A. H-comodule. For $f \in \mathrm{Reg}(B,H)^0$ consider

$$B \xrightarrow{\phi} B \otimes H \xrightarrow{f^{-1} \otimes I} k \otimes H = H .$$

Define

$$\delta_0 : \mathrm{Reg}(B,H)^0 \to \mathrm{Reg}(B,H)^1$$

$$\delta_0 f = f * f^{-1} \otimes I \circ \phi ,$$

we are considering $f: B \to k \subset H$. When $n > 0$ define

$$\delta_n : \mathrm{Reg}(B,H)^n \to \mathrm{Reg}(B,H)^{n+1}$$

$$\delta_n f = k \otimes f * \pi_{i=1}^{n} I^{[i-1]} \otimes d \otimes I^{[n-i]} \circ f^{(-1)^i} * f^{(-1)^{n+1}} \otimes I \circ \phi .$$

Then $\delta_{n+1}\delta_n = \varepsilon$, δ_n is a group homomorphism so we have a complex

$$\mathrm{Reg}(B,H)^0 \xrightarrow{\delta_0} \mathrm{Reg}(B,H)^1 \xrightarrow{\delta_1} \cdots$$

and define the cohomology groups

$$H(B,H)^n = \mathrm{Ker}\ \delta_n / \mathrm{Im}\ \delta_{n-1} \qquad n \geq 1$$

$$H(B,H)^0 = \mathrm{Ker}\ \delta_0 .$$

As in the previous theory we have a normal complex:

$$n > 0 \qquad \mathrm{Reg}(B,H)_+^n = \left\{ f \in \mathrm{Reg}(B,H)^n \;\middle|\; \begin{array}{ccc} B & \xrightarrow{f} & H^{[n]} \\ & {\scriptstyle\varepsilon}\searrow \quad \swarrow{\scriptstyle\varepsilon} & \\ & k & \end{array} \text{ is commutative } . \right\}$$

$$\delta_n^+ = \delta_n | \mathrm{Reg}(B,H)_+^n : \mathrm{Reg}(B,H)_+^n \to \mathrm{Reg}(B,H)_+^{n+1} \quad .$$

$$\mathrm{Reg}(B,H)_+^0 = \mathrm{Reg}(B,H)^0$$

$$\delta_0^+ = \delta_0 : \mathrm{Reg}(B,H)_+^0 \to \mathrm{Reg}(B,H)_+^1 \quad .$$

The cohomology computed by this complex is the same.

Extension Theory

H is a Hopf algebra A, B coalgebras, A a left H-module (as a coalgebra), $\psi : H \otimes A \to A$, being the module structure. The sequence

$$H \otimes A \xrightarrow{\psi} A \xrightarrow{\pi} B \ ,$$

is called *right exact* if

1) π is a surjective coalgebra morphism

2) $\mathrm{Coim}\ \pi = k \otimes_H A$, i.e.

$$\mathrm{Ker}\ \pi = H^+ \cdot A \quad .$$

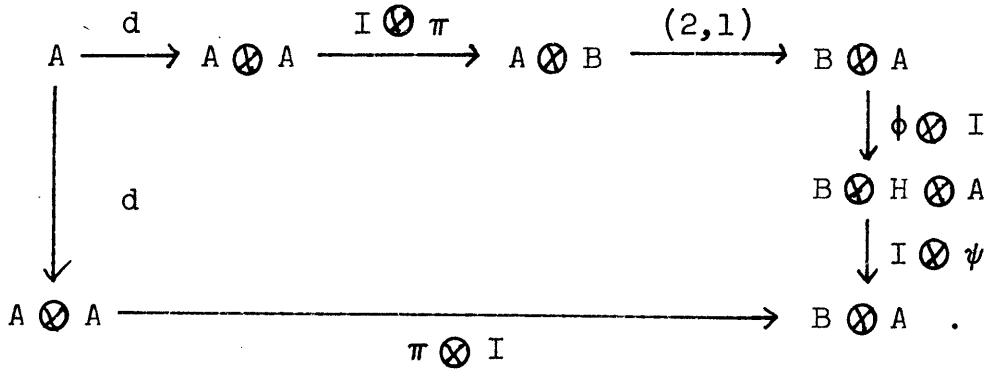
The sequence is called *split exact* when: H has an antipode,

the sequence is right exact, and there is a regular left H-module morphism $P: A \to H$. In this case

$A \xrightarrow{d} A \otimes A \xrightarrow{P \otimes \pi} H \otimes B$ is an isomorphism of right B-comodules and left H-modules by theorem 2. Let $\phi: B \to B \otimes H$ give B the structure of a right C.H.A. H-comodule, then A is called an <u>extension of B by H</u> when:

1) $H \otimes A \xrightarrow{\psi} A \xrightarrow{\pi} B$ is a split exact sequence,

2) the following diagram is commutative,

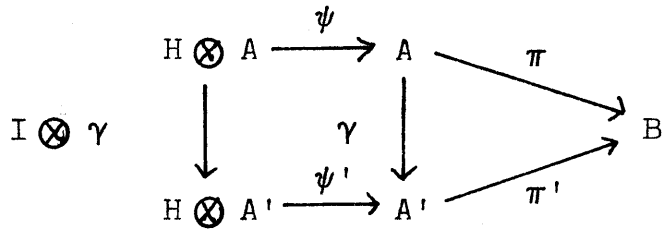


Given two extensions A, A' of B by H where the split exact sequences are

$$H \otimes A \xrightarrow{\psi} A \xrightarrow{\pi} B$$

$$H \otimes A' \xrightarrow{\psi'} A' \xrightarrow{\pi'} B \ ,$$

we say they are <u>isomorphic</u> if there is a coalgebra morphism $\gamma: A \to A'$, such that,



is commutative. Being isomorphic is an equivalence relation and we can form isomorphism classes of extensions.

An example:

Given $g \in \mathrm{Reg}(B,H)^2_+$ a 2-cocycle, form $H \underset{g}{\otimes} B$ which is $H \otimes B$ as a left H-module.

$$\pi: H \underset{g}{\otimes} B \xrightarrow{\varepsilon \otimes I} B$$

$$P: H \underset{g}{\otimes} B \xrightarrow{I \otimes \varepsilon} H \ .$$

$$H \underset{g}{\otimes} B \xrightarrow{I \otimes d^2} H \otimes B \otimes B \otimes B \xrightarrow{d \otimes g \otimes \phi \otimes I}$$

$$H \otimes H \otimes H \otimes H \otimes B \otimes H \otimes B \xrightarrow{(1,3,5,2,4,6,7)}$$

$$H \otimes H \otimes B \otimes H \otimes H \otimes H \otimes B \xrightarrow{m \otimes I \otimes m^2 \otimes I} (H \underset{g}{\otimes} B) \otimes (H \underset{g}{\otimes} B)$$

defines the coalgebra structure on $H \underset{g}{\otimes} B$. Then

$$H \otimes H \underset{g}{\otimes} B \to H \underset{g}{\otimes} B \xrightarrow{\pi} B$$

is split exact, the second condition for extensions is satisfied so $H \otimes_g B$ is an extension of B by H. Two such extensions are isomorphic if and only if the 2-cocycles are homologous. There is such an extension in each isomorphism class of extensions. This yields the natural bijective correspondence between $H(B,H)^2$ and the isomorphism classes of extensions.

Chapter V

Cocommutative, Coconnected Hopf Algebras

We have shown a split conilpotent Hopf algebra with antipode is a smash product $B \overset{\varepsilon}{\otimes} H$ where H is a group Hopf algebra acting as automorphisms of B. B is a split Hopf algebra where $G(B) = \{1\}$. We shall study such Hopf algebras which are cocommutative. In characteristic zero we prove such a Hopf algebra is a universal enveloping algebra--u.e.a.--of a Lie algebra, in characteristic $p > 0$ it contains a restricted u.e.a.--r.u.e.a.--of a restricted Lie algebra. (We assume familiarity with universal enveloping algebras and restricted universal enveloping algebras as can be found in [2] Lie Algebras.)

We define divided powers as sequences of elements

$$1 = \ell_0, \ell_1, \ldots \ell_N$$

where for $n \leq N$ $d\ell_n = \sum_{i=0}^{n} \ell_i \otimes \ell_{n-i}$ and show that in a class of cocommutative split Hopf algebras H, where $G(H) = \{1\}$ the coalgebra structure of H is characterized by divided powers.

A Hopf algebra H is coconnected if it is split and $G(H) = \{1\}$. Since $G(H)$ corresponds to the coalgebra morphisms of k to H, coconnectivity is equivalent to:

being split, and $\eta: k \to H$ is the unique coalgebra morphism of k to H.

By (4) all coconnected Hopf algebras have antipodes.

All Hopf Algebras Henceforth Are Assumed To Be Coconnected Unless Otherwise Specified.

A <u>primitive element</u> x in a Hopf algebra H is one where

$$dx = x \otimes 1 + 1 \otimes x .$$

Then $x \in H_1$ and $\varepsilon(x) = 0$. Let $L(H)$ $(=L)$ denote the space of primitive elements in H. L forms a Lie algebra under $[\ ,\ ]$; if characteristic $p > 0$

$$dx^p = 1 \otimes x^p + x^p \otimes 1 ,$$

(binomially expand $(dx)^p$), so L forms a restricted Lie algebra.

Suppose $x \in H_1$, $\varepsilon(x) = 0$.

$$dx \in H_0 \otimes H_1 + H_1 \otimes H_0 , \qquad H_0 = \{k\} \text{ so}$$

$$dx = 1 \otimes y + z \otimes 1 .$$

$$\left.\begin{aligned} I * \varepsilon &= I \\ \varepsilon * I &= I \\ \varepsilon * \varepsilon &= \varepsilon \end{aligned}\right\} \quad \text{imply} \quad \left\{\begin{aligned} \varepsilon(y) + z &= x \\ y + \varepsilon(z) &= x \\ \varepsilon(y) + \varepsilon(z) &= \varepsilon(x) = 0 . \end{aligned}\right.$$

Thus $dx = 1 \otimes (y + \varepsilon(z)) + (z + \varepsilon(y)) \otimes 1 - 1 \otimes \varepsilon(z) - \varepsilon(y) \otimes 1$

$= 1 \otimes x + x \otimes 1$,

and x is primitive. This shows

$$\text{Ker } \varepsilon \cap H_1 = L \qquad \text{and} \qquad H_1 = L \oplus H_0 = L \oplus k \ .$$

Let U denote the u.e.a. of L in char $p = 0$; and the r.u.e.a. of L in char $p > 0$. We consider $L \subset U$. U is a (coconnected) Hopf algebra where the coalgebra structure is induced by specifying the elements of L are primitive. Then $L(U) = L$.

By the defining property of U there is an algebra morphism

$$\gamma: U \to H$$

which is induced by the identification of $L \subset U$ with $L \subset H$. γ is also a coalgebra morphism; hence, is a morphism of Hopf algebras.

That γ is injective follows from the next lemma.

Lemma 4:) $\nu: A \to C$, A a Hopf algebra C a coalgebra, ν a coalgebra morphism. ν is injective if and only if $\nu|L(A)$ is injective.

Proof: Suppose $\nu|L(A)$ is injective. Since ν is a coalgebra morphism

$$\varepsilon_C(\nu(L(A))) = 0 \quad , \quad \varepsilon_C(\nu(1)) = 1$$

thus $\nu|A_1$ is injective. By induction we can assume $\nu|A_n$ is injective $n \geq 1$; hence, $\nu \otimes \nu|A_n \otimes A_n$ is injective. Suppose $a \varepsilon A_{n+1}$ then

$$da = 1 \otimes a + a \otimes 1 + Y \ , \quad Y \varepsilon A_n \otimes A_n \ .$$

Suppose $\nu(a) = 0$ then

$$0 = d\nu(a) = \nu \otimes \nu o da = \nu(1) \otimes \nu(a) + \nu(a) \otimes \nu(1) + (\nu \otimes \nu)(Y)$$

$$= (\nu \otimes \nu)(Y) \ .$$

Since $\nu \otimes \nu|A_n \otimes A_n$ is injective it follows $Y = 0$, $a \varepsilon L(A)$; which contradicts $\nu|L$ is injective.

The converse is obvious. Q.E.D.

This implies $\gamma: U \to H$ is injective. We identify U with its image which is the subalgebra of H generated by L . (Thus U is the subalgebra of H generated by L both as algebra and coalgebra.)

We shall show if H is cocommutative and

$$\begin{cases} \text{char } p = 0 & U = H \ , \\ \text{char } p > 0 & U = (H^* \rho(J))^{\perp} \end{cases}$$

where $J = k^{\perp} \subset H^*$, $\rho(J) = \{a^{*p} | a^* \varepsilon J\}$ and $(H^*\rho(J))$ is the ideal generated by $\rho(J)$. We do this by developing

a technique which "picks-out" subspaces of H. We associate with subspaces of H, subspaces of $k[\{x^\alpha\}]$ the polynomial algebra on $\{x^\alpha\}$ a basis for $L(H)$. (Note: since the method of associating subspaces with subspaces depends upon the basis $\{x^\alpha\}$, we have chosen to work with $k[\{x^\alpha\}]$--which makes the basis clear--rather than the symmetric algebra on L.)

Given a vector space X, $\overbrace{X \otimes \cdots \otimes X}^{n} = X^{[n]}$ is a left $\mathfrak{S}_n$-module. The symmetric tensors of degree n are:

$$n > 0 \qquad S_nX = \left\{ Y \in X^{[n]} \mid \sigma \cdot Y = Y \text{ all } \sigma \in \mathfrak{S}_n \right\},$$

$$n = 0 \qquad S_0X = k .$$

Let $\{x^\alpha\}$ be an ordered basis for X,

$k[\{x^\alpha\}]$ is a graded algebra.

$k[\{x^\alpha\}]$ is isomorphic to $SX = \bigoplus_{n=0}^{\infty} S_nX$ as follows:

Let $(x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m}$ be a monomial of $k[\{x^\alpha\}]_n$.

(i.e. $e_1 + \cdots + e_m = n$, $0 < e_i \in Z$, $\alpha_1 < \cdots < \alpha_m$).

Let $Y = x^{\alpha_1[e_1]} \otimes x^{\alpha_2[e_2]} \otimes \cdots \otimes x^{\alpha_m[e_m]}$.

Let $\mathfrak{S}_n(\alpha_1^{e_1}, \ldots \alpha_m^{e_m}) = \{\sigma \in \mathfrak{S}_n \mid \sigma \cdot Y = Y\}$

= the isotropy group of Y.

$\mathfrak{S}_n/\mathfrak{S}_n(\alpha_1^{e_1}, \cdots \alpha_m^{e_m})$--left cosets--corresponds to the

orbit of Y, let

$$\alpha((x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m}) = \sum_{\bar{\sigma} \in \mathfrak{S}_n/\mathfrak{S}_n(\alpha_1^{e_1}, \cdots \alpha_m^{e_m})} \bar{\sigma} \cdot Y \quad .$$

By linearity $\alpha: k[\{x^\alpha\}] \to SX$. α is an isomorphism, $\beta: SX \to k[\{x^\alpha\}]$ denotes the inverse isomorphism.

All Hopf Algebras Henceforth Are Assumed To Be Cocommutative (as well as coconnected) Unless Otherwise Specified.

Let H be a Hopf algebra, $L = L(H)$, $\{x^\alpha\}$ a basis for L and $K = k[\{x^\alpha\}]$. We shall now define an element

$$K(h) \in K \quad \text{for each } h \in H .$$

This is not a linear map.

For $h \in H_0 \ (=k)$ let

$$K(h) = \beta(h) \in K_0 .$$

For $n > 0$ (d^0 denotes I) $h \in H_n$

$$dh \in H_n \otimes H_0 + \cdots + H_0 \otimes H_n \quad \text{so}$$

1) $$d^{n-1}h \in \sum_{e_1 + \cdots + e_n = n} H_{e_1} \otimes \cdots \otimes H_{e_n} .$$

If E denotes $I - \varepsilon$, $H_0 = \operatorname{Ker} E$ and $E|H_1: H_1 \to L$ a projection. $E^{[n]} \circ d^{n-1}h \in L^{[n]}$ since in

1) any summand except $H_1 \otimes \cdots \otimes H_1$ lies in $\mathrm{Ker}(E^{[n]})$ and

$$E^{[n]}(H_1 \otimes \cdots \otimes H_1) \subset L^{[n]} .$$

By cocommutivity and coassociativity

$$E^{[n]} \circ d^{n-1}h \in S_nL .$$

If $a_1^*,\ldots,a_n^* \in J$ then $a_1^* \otimes \cdots \otimes a_n^*$ vanishes on each summand of 1) except $H_1^{[n]}$ and on this summand

$a_1^* \otimes \cdots \otimes a_n^*$ takes the same value as

$a_1^* \otimes \cdots \otimes a_n^* \circ E^{[n]}$.

Thus $\langle a_1^* * \cdots * a_n^*, h\rangle = \langle a_1^* \otimes \cdots \otimes a_n^*, d^{n-1}h\rangle$

$$= \langle a_1^* \otimes \cdots \otimes a_n^*, E^{[n]} \circ d^{n-1}h\rangle .$$

This proves:

(5) $h \in H_n - H_{n-1}$ if and only if $0 \neq E^{[n]} \circ d^{n-1}h \in S_nL$.

For $h \in H_n - H_{n-1}$ let

$$K(h) = \beta \circ E^{[n]} \circ d^{n-1}(h) \in K_n .$$

Then we have $H \rightsquigarrow K$

$h \rightarrow K(h)$

which is <u>not</u> linear. But by (5) and since β is an isomorphism we have,

⑥ if $h \varepsilon H_n$, $g \varepsilon H$ and

$K(h) - K(g) = 0$ then $g \varepsilon H_n$ and

$h - g \varepsilon H_{n-1}$.

For a subspace $X \subset H$ let

$K(X)$ = the subspace of K spanned by

$$\{K(x) | x \varepsilon X\} .$$

In general $K(H) \neq K$.

Recall for a subspace $X_n = X \cap H_n$ then it is clear

$$K(X_n) = K(X) \cap (K_n \oplus K_{n-1} \oplus \cdots \oplus K_0) .$$

Lemma 5:) Given subspaces X, Y of H where $X \subset Y$, $X_0 = Y_0$; then $K(X) = K(Y)$ implies $X = Y$.

Proof: We show by induction $X \supset Y_n$. True for $n = 0$, suppose true for $n - 1$. Let $h \varepsilon Y_n - Y_{n-1}$, then $0 \neq K(h) = \lambda_1 K(h_1) + \cdots + \lambda_m K(h_m)$, where $\lambda_i \varepsilon k$, $\{h_i\} \subset X_n - X_{n-1}$. Thus

$$0 \neq \lambda_1(\beta \circ E^{[n]} \circ d^{n-1}(h_1)) + \cdots + \lambda_m(\beta \circ E^{[n]} \circ d^{n-1}(h_m))$$

$$= \beta \circ E^{[n]} \circ d^{n-1}(\lambda_1 h_1 + \cdots + \lambda_m h_m)$$

which implies $g = \lambda_1 h_1 + \cdots + \lambda_m h_m \varepsilon X_n - X_{n-1}$ and

$K(g) = K(h)$. By (6)

$x = h - g \in Y_{n-1} \subset X$ so that

$h = x + g \in X$. Q.E.D.

Observe if X, Y are both subalgebras, subcoalgebras, ideals or coideals the condition $X_0 = Y_0$ is automatically satisfied.

(7) If $x \in H_n$ $y \in H_q$ where

$$\beta \circ E^{[n]} \circ d^{n-1}(x) = (x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m}$$

$$\beta \circ E^{[q]} \circ d^{q-1}(y) = (x^{\alpha_1})^{f_1} \cdots (x^{\alpha_m})^{f_m}$$

$$\left[\alpha_1 < \cdots < \alpha_m \quad 0 \leq e_i, f_i \in Z \right.$$

then

$$\beta \circ E^{[n+q]} \circ d^{n+q-1}(xy) = \binom{e_1 + f_1}{e_1} \cdots \binom{e_m + f_m}{e_m} (x^{\alpha_1})^{e_1 + f_1} \cdots (x^{\alpha_m})^{e_m + f_m} .$$

This is a purely combinatoric result and the proof is combinatoric. Q denotes the rational numbers. Let the Hopf algebra B be $Q[x^{\alpha_1}, \ldots x^{\alpha_m}]$ as an algebra, and the diagonal and augmentation are induced by making $\{x^{\alpha_i}\}$ primitive. $L(B)$ has basis $\{x^{\alpha_i}\}$, we let β_B denote the isomorphism β_B: $SL(B) \to Q[x^{\alpha_1}, \ldots x^{\alpha_m}]$. We prove by induction an $e_1 + \cdots + e_m = n$ that

2) $$\beta_B \circ E^{[n]} \circ d^{n-1}\left(\frac{(x^{\alpha_1})^{e_1}}{e_1!} \cdots \frac{(x^{\alpha_m})^{e_m}}{e_m!}\right) = (x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m} .$$

True for $n = 1$, say true for $n - 1$, then if

$e_1 + \cdots + e_m = n$ (we suppose without loss that $e_1 > 0$)

$$\beta_B \circ E^{[n-1]} \circ d^{n-2}\left(\frac{(x^{\alpha_1})^{e_1-1}}{(e_1-1)!}\frac{(x^{\alpha_2})^{e_2}}{e_2!}\cdots\frac{(x^{\alpha_m})^{e_m}}{e_m!}\right) = (x^{\alpha_1})^{e_1-1}(x^{\alpha_2})^{e_2}\cdots(x^{\alpha_m})^{e_m}.$$

B^* is a right B-module where

$$\langle b^* \cdot a, b\rangle = \langle b^*, ab\rangle \quad b^* \in B^* , \ a, b \in B .$$

If $x \in L(B)$ then x acts as a derivation of B^* . B has a basis of monomials in $\{x^{\alpha_i}\}$, within B^* choose a dual basis (not necessarily a basis for B^*) to the monomial basis for B . Let $\{a_i^*\}_{i=1}^m$ be the dual elements to $\{x^{\alpha_i}\}_{i=1}^m$ so $\langle a_i^*, x^{\alpha_j}\rangle = \delta_{i,j}$.

$a_i^* \cdot x^{\alpha_j} = \delta_{ij}\,\varepsilon$. ε the unit of B^* . To verify 2) it suffices to show

$$\langle a_1^{*g_1} * \cdots * a_m^{*g_m}, \frac{(x^{\alpha_1})^{e_1}}{e_1!}\cdots\frac{(x^{\alpha_m})^{e_m}}{e_m!}\rangle \quad \text{where} \quad g_1 + \cdots + g_m = n$$

$$= \begin{cases} 1 & \text{if } g_1 = e_1, \ldots g_m = e_m \\ 0 & \text{otherwise.} \end{cases}$$

$$\langle a_1^{*g_1} * \cdots * a_m^{*g_m}, \frac{(x^{\alpha_1})^{e_1}}{e_1!}\cdots\frac{(x^{\alpha_m})^{e_m}}{e_m!}\rangle =$$

$$\frac{\langle (a_1^{*g_1} * \cdots * a_m^{*g_m}) \cdot x^{\alpha_1}, \frac{(x^{\alpha_1})^{e_1-1}}{(e_1-1)!}\frac{(x^{\alpha_2})^{e_2}}{e_2!}\cdots\frac{(x^{\alpha_m})^{e_m}}{e_m!}\rangle}{e_1}$$

$$= \frac{g_1}{e_1}\langle a_1^{*g_1-1} * a_2^{*g_2} * \cdots a_m^{*g_m}, \frac{(x^{\alpha_1})^{e_1-1}}{(e_1-1)!} \frac{(x^{\alpha_2})^{e_2}}{e_2!} \cdots \frac{(x^{\alpha_m})^{e_m}}{e_m!} \rangle$$

by induction

$$= \begin{cases} 1 & \text{if } g_1-1 = e_1-1 \text{ , } g_2 = e_2 \cdots g_m = e_m \\ 0 & \text{otherwise .} \end{cases}$$

Thus 2) is established. Also that

$$\beta_B \circ E^{[q]} \circ d^{q-1}\left(\frac{(x^{\alpha_1})^{f_1}}{f_1!} \cdots \frac{(x^{\alpha_m})^{f_m}}{f_m!}\right) = (x^{\alpha_1})^{f_1} \cdots (x^{\alpha_m})^{f_m} .$$

Then

$$\beta_B \circ E^{[n+q]} \circ d^{n+q-1}\left(\left[\frac{(x^{\alpha_1})^{e_1}}{e_1!} \cdots \frac{(x^{\alpha_m})^{e_m}}{e_m!}\right]\left[\frac{(x^{\alpha_1})^{f_1}}{f_1!} \cdots \frac{(x^{\alpha_m})^{f_m}}{f_m!}\right]\right)$$

$$= \binom{e_1+f_1}{e_1} \cdots \binom{e_m+f_m}{e_m} \beta_B \circ E^{[n+q]} \circ d^{n+q-1}\left(\frac{(x^{\alpha_1})^{e_1+f_1}}{(e_1+f_1)!} \cdots \frac{(x^{\alpha_m})^{e_m+f_m}}{(e_m+f_m)!}\right)$$

$$\underline{\underline{\text{by 2)}}} \quad \binom{e_1+f_1}{e_1} \cdots \binom{e_m+f_m}{e_m} (x^{\alpha_1})^{e_1+f_1} \cdots (x^{\alpha_m})^{e_m+f_m} .$$

This establishes (7) . The following theorem is a specialization of a theorem of Kostant.

Theorem 4. In characteristic 0 a coconnected

cocommutative Hopf algebra H is U, U the u.e.a. of $L(H)$.

Proof: If $K = k[\{x^\alpha\}]$, $\{x^\alpha\}$ a basis for L, then by (7) if

$$x = \frac{(x^{\alpha_1})^{e_1}}{e_1!} \cdots \frac{(x^{\alpha_m})^{e_m}}{e_m!} \in U .$$

$K(x) = (x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m}$, which shows $K(U) = K$. By lemma 5 $U = H$. Q.E.D.

We now study the case when characteristic $p > 0$.

(8) $$U = (H^*\rho(J))^{\perp} .$$

$U \subset (H^*\rho(J))^{\perp}$: Let H act on H^* from the right by: $\langle a^* \cdot h, g\rangle = \langle a^*, hg\rangle$. If $h \in L$ h acts as a derivation of H^*. U is spanned by 1 and monomials of elements from L, $1 \in (H^*\rho(J))^{\perp}$. Let $\ell_1 \cdots \ell_m$ be a monomial $\ell_i \in L$. $H^*\rho(J)$ is spanned by elements of the form $b^* * a^{*p}$ $b^* \in H$ $a^* \in J$.

$$\langle b^* * a^{*p}, \ell_1 \cdots \ell_m\rangle = \langle (b^* * a^{*p}) \cdot \ell_1, \ell_2 \cdots \ell_m\rangle$$

$$= \langle (b^* \cdot \ell_1) * a^{*p}, \ell_2 \cdots \ell_m\rangle$$

$$+ \langle b^* * (a^{*p} \cdot \ell_1), \ell_2 \cdots \ell_m\rangle$$

$$= \langle (b^* \cdot \ell_1) * a^{*p}, \ell_2 \cdots \ell_m\rangle$$

$= 0$ by induction on the length of the monomial; hence, $U \subset (H^*\rho(J))^{\perp}$.

$$U_0 = (H^*\rho(J))^{\perp}_0 = H_0 = k .$$

Letting $\{x^{\alpha}\}$ be an ordered basis for L $K = k[\{x^{\alpha}\}]$ then by (7)

$$K(U) \supset \left\{ x^{\alpha_1 e_1} \cdots x^{\alpha_m e_m} \;\middle|\; \begin{array}{l} m = 0,1,\ldots \\ \alpha_1 < \cdots < \alpha_m \\ 0 \leq e_i < p \end{array} \right\} .$$

Let V be the subspace of K spanned by the right side. We show

$$K((H^*\rho(J))^{\perp}) \subset V .$$

Since $U \subset (H^*\rho(J))^{\perp}$ it follows from

$$V \subset K(U) \subset K((H^*\rho(J))^{\perp}) \subset V ,$$

that

$$V = K(U) = K((H^*\rho(J))^{\perp}) .$$

Let $h \in (H^*\rho(J))^{\perp}$

$$K(h) = \sum_i \lambda_i x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}} \qquad \lambda_i \in k .$$

Suppose for some t, j $e_{t_j} \geq p$. Let $\{a_i^*\} \subset J$ be a dual basis to $\{x^{\alpha_i}\}_{i=1}^{m}$. Then

$$a^* = a_1^{*e_{t_1}} * \cdots * a_m^{*e_{t_m}} \in H^*\rho(J) , \text{ and } \langle a^*, h\rangle = \lambda_t$$

which implies $\lambda_t = 0$ and $K(h) \varepsilon V$. Thus we are done by lemma 5.

We can draw the corollary that in characteristic $p > 0$ if H is cocommutative and coconnected then $U = H$ if and only if for each $a^* \varepsilon J$ $a^{*p} = 0$. This follows because $H^*\rho(J) = 0$ if and only if $\rho(J) = 0$.

Since U may not equal H we examine the ideal generated by the primitives in H.

$$\text{(9)} \qquad LH = HL = \rho(H^*)^{\perp} = \left\{ a^{*p} \mid a^* \varepsilon H^* \right\}^{\perp}$$

We shall show $LH = \rho(H^*)^{\perp}$ the proof $HL = \rho(H^*)$ is the same (up to reflection).

$HL \subset \rho(H^*)^{\perp}$: Let H act on H^* from the right by $\langle a^* \cdot h, g\rangle = \langle a^*, hg\rangle$. Then for $a^* \varepsilon H^*$, $\ell \varepsilon L$, $h \varepsilon H$,

$$\langle a^{*p}, \ell h\rangle = \langle a^{*p} \cdot \ell, h\rangle = 0$$

since ℓ acts as a derivation.

If $\{x^{\alpha}\}$ is an ordered basis for L $K = k[\{x^{\alpha}\}]$, $K \supset W$ = the space spanned by

$$\left\{ (x^{\alpha_1})^{e_1} \cdots (x^{\alpha_m})^{e_m} \;\middle|\; \begin{array}{l} m = 1,2,\ldots \\ \alpha_1 < \cdots < \alpha_m \\ \text{for some } e_i \;\; p \nmid e_i \end{array} \right\},$$

then $K(\rho(H^*)^{\perp}) \subset W$. Since if $h \varepsilon \rho(H^*)^{\perp}$

$$K(h) = \sum_i \lambda_i (x^{\alpha_1})^{e_{i_1}} \cdots (x^{\alpha_m})^{e_{i_m}} .$$

Suppose for $i = t$ $p|e_{t_1}, \ldots p|e_{t_m}$, then letting

$\{a_i^*\}_{i=1}^m \subset J$ be a dual basis to $\{x^{\alpha_i}\}_{i=1}^m$;

$a^* = a_1^{*e_{t_1}} * \cdots * a_m^{*e_{t_m}} \varepsilon \rho(H^*)$ and $\langle a^*, h\rangle = \lambda_t$ which implies $\lambda_t = 0$ and $K(\rho(H^*)^{\perp}) \subset W$.

Next we show $K(LH) \supset W \cap K(H)$. Suppose $h \varepsilon H_n - H_{n-1}$ where $K(h) \varepsilon W$, we shall show there is $g \varepsilon LH$ where $K(g) = K(h)$. Let

$$K(h) = \sum_{i=1}^{M} \lambda_i (x^{\alpha_1})^{e_{i_1}} \cdots (x^{\alpha_m})^{e_{i_m}}, \quad \alpha_1 < \cdots < \alpha_m ,$$

$$0 \neq \lambda_i \varepsilon k .$$

(For the present the elements of H^* shall act as functions i.e. $a^*(x) = \langle a^*, x\rangle$.) For each $i=1,\ldots M$ there is $1 \leq n(i) \leq m$ where

$$p \nmid e_{i_{n(i)}} .$$ By (3)

$$da^* \cdot h = \sum_i h_i' \otimes a^* \cdot h_i''$$

$$= I \otimes I \otimes a^* \circ d^2 h \varepsilon H \otimes H \otimes k = H \otimes H .$$

By cocommutivity $d^{n-2}(a^* \cdot h) = a^* \otimes I^{[n-1]} \circ d^{n-1}(h)$.

If $a^* \in J$ then

$$a^* \otimes I^{[n-1]} \circ \Big(\sum_{\substack{f_1+\cdots+f_n = n \\ \text{some } f_i = 0}} H_{f_1} \otimes \cdots \otimes H_{f_n}\Big) \subset \sum_{\substack{f_1+\cdots+f_{n-1} = n-1 \\ \text{some } f_i = 0}} H_{f_1} \otimes \cdots \otimes H_{f_{n-1}}$$

and hence

$$E^{[n-1]} \circ d^{n-2}(a^* \cdot h) = E^{[n-1]} \circ a^* \otimes I^{[n-1]} \circ \alpha \quad (K(h))$$
$$= a^* \otimes I^{[n-1]} \circ \alpha(K(h)) .$$

Thus if $a^* \cdot h \in H_{n-1} - H_{n-2}$, $a^* \in J$

(10) $$K(a^* \cdot h) = \beta \circ a^* \otimes I^{[n-1]} \circ \alpha(K(h)) .$$

With $\{a_i^*\}_{i=1}^{m} \subset J$ dual to $\{x^{\alpha_i}\}$

$$K(a^*_{n(i)} \cdot h) = \sum_{j=1}^{M} \bar{\lambda}_j (x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_{n(i)}})^{e_{j_{n(i)}}-1} \cdots (x^{\alpha_m})^{e_{j_m}}$$

where $$\bar{\lambda}_j = \begin{cases} 0 & \text{if } e_{j_{n(i)}} = 0 \\ \lambda_j & \text{if } e_{j_{n(i)}} > 0 ; \end{cases}$$

$p \nmid e_{i_{n(i)}}$ so $\bar{\lambda}_i = \lambda_i \neq 0$. By (7) and $(p \nmid e_{i_{n(i)}})$

$$K(x^{\alpha_{n(i)}}(a^*_{n(i)} \cdot h)) = \sum_{j=1}^{M} \bar{\lambda}_j \, e_{j_{n(i)}} (x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_m})^{e_{j_m}}$$

$$= \sum_{j=1}^{M} \lambda_j \, e_{j_{n(i)}} (x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_m})^{e_{j_m}} .$$

Thus if $M = 1$

$$K(x^{\alpha_{n(1)}}(a^*_{n(1)} \cdot h)) = \lambda_1 e_{1_{n(1)}} (x^{\alpha_1})^{e_{1_1}} \cdots (x^{\alpha_m})^{e_{1_m}}$$

$p \nmid e_{1_{n(1)}}$ so $g = \dfrac{x^{\alpha_{n(1)}}(a^*_{n(1)} \cdot h)}{e_{1_{n(1)}}} \in LH$ and

$K(g) = K(h)$. By induction on M we can assume for values smaller than M there is $g \in LH$ where $K(g) = K(h)$. Let

$$\tilde{g} = \frac{x^{\alpha_{n(M)}}(a^*_{n(M)} \cdot h)}{e_{M_{n(M)}}} \in LH \quad .$$

$$K(\tilde{g}) = \sum_{j=1}^{M} \lambda_j \frac{e_{j_{n(M)}}}{e_{M_{n(M)}}} (x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_m})^{e_{j_m}} \quad .$$

This may equal $K(h)$ in which case we have exhibited $\tilde{g} \in LH$ where $K(\tilde{g}) = K(h)$ otherwise

$$K(h-\tilde{g}) = \sum_{j=1}^{M-1} \lambda_j (1 - \frac{e_{j_{n(M)}}}{e_{M_{n(M)}}})(x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_m})^{e_{j_m}}$$

and by induction there is $g \in LH$ where $K(g) = K(h - \tilde{g})$. Then $g + \tilde{g} \in LH$ and $K(g + \tilde{g}) = K(h)$.

So we have shown:

$$K(LH) \supset W \cap K(H) \supset K(\rho(H^*)^{\perp}) \ ,$$

and $LH \subset K(\rho(H^*)^{\perp})$.

(11) Thus $W \cap K(H) = K(LH) = K(\rho(H^*)^{\perp})$.

$(LH)_0 = \{0\} = (\rho(H^*)^{\perp})_0$ so by lemma 5 we are done.

Observe in (8) we showed $K(U) = V$ and in (9) $K(LH) = W$; but $V \cap (K_1 \oplus \cdots \oplus K_p) = W \cap (K_1 \oplus \cdots \oplus K_p)$. Thus if $U^+ = U \cap \operatorname{Ker} \varepsilon$, then

$$U_p^+ \subset (LH)_p \ , \ (U^+_p)_0 = ((LH)_p)_0 = \{0\} \quad \text{and}$$

$K(U^+_p) = V \cap (K_1 \oplus \cdots \oplus K_p) = W \cap (K_1 \oplus \cdots \oplus K_p) = K((LH)_p)$ so by lemma 5 $U^+_p = (LH)_p$.

Since the elements of L are primitive and d is an algebra morphism the 2-sided ideal LH is a 2-sided coideal; that is $dLH \subset H \otimes LH + LH \otimes H$. Hence, H/LH has a natural algebra and coalgebra structure by which it is a Hopf algebra. We shall now show H/LH with its vector space structure altered is naturally isomorphic to a sub Hopf algebra of H . This is the first major step toward obtaining the coalgebra structure of H .

We assume now that k is perfect. If X is a vector space over k let $\underline{X}$ denote the vector space which group theoretically is X and for $\lambda \in k$ $\underline{x} \in \underline{X}$

$$\lambda \cdot \underline{x} = \underline{\lambda^p x} \ .$$

For vector spaces X, Y where $f: X \to Y$ then $\underline{f}: \underline{X} \to \underline{Y}$ is linear where $\underline{f} = f$ set theoretically.

If A is an algebra (over k) then $\underline{A}$ has multiplicative structure

$$\underline{m}: \underline{A \otimes A} = \underline{A} \otimes \underline{A} \to \underline{A}$$

and we define the unit

$$\eta_{\underline{A}}: k \to \underline{A}$$

$$\lambda \to \underline{[\eta_A(\lambda)]^p} \quad .$$

With this structure $\underline{A}$ is an algebra over k. If C is a coalgebra over k then $\underline{C}$ is a coalgebra where the diagonal map is $\underline{d}$ and

$$\varepsilon_{\underline{C}}: \underline{C} \to k$$

$$\varepsilon_{\underline{C}}(\underline{c}) = [\varepsilon_C(c)]^{\frac{1}{p}} ,$$

since k is perfect this makes sense. If H is a Hopf algebra then $\underline{H}$ is a Hopf algebra where the algebra and coalgebra structure are as indicated above. We shall freely make obvious identifications such as if X, Y are vector spaces $X \supset Y$ then

$$\underline{X/Y} = \underline{X}/\underline{Y} \quad .$$

There is a natural map $i_X: (\underline{X})^* \to \underline{(X^*)}$ where if $a^* \in (\underline{X})^*$, $x \in X$

$$\langle i_x(a^*),\ x\rangle = \langle a^*, \underline{x}\rangle^p \quad .$$

i_x is injective and surjective since k is perfect. (i_x is linear.) If C is a coalgebra so that $\underline{C}$ is a coalgebra and $\underline{(C^*)}$, $(\underline{C})^*$ are algebras then

$$i_c : (\underline{C})^* \to \underline{(C^*)}$$

is an algebra isomorphism.

If A is an algebra

$$A \otimes A \xrightarrow{m} A$$

$$\underline{A \otimes A} = \underline{A} \otimes \underline{A} \xrightarrow{m} \underline{A}$$

induce

$$A^* \xrightarrow{t_m} (A \otimes A)^*$$

$$(\underline{A})^* \xrightarrow{t_{\underline{m}}} (\underline{A \otimes A})^*$$

then

$$\begin{array}{ccc} \underline{(A^*)} & \xrightarrow{(t_m)} & \underline{[(A \otimes A)^*]} \\ \uparrow{\scriptstyle i_A} & & \uparrow{\scriptstyle i_{A \otimes A}} \\ (\underline{A})^* & \xrightarrow{t_{\underline{m}}} & (\underline{A \otimes A})^* \end{array}$$

is commutative. If A is finite dimensional so that $(\underline{A \otimes A})^* = (\underline{A} \otimes \underline{A})^* = (\underline{A})^* \otimes (\underline{A})^*$ then $i_{A \otimes A} = i_A \otimes i_A$ which shows i_A is a coalgebra morphism (the augmentation is preserved).

We identify $(\underline{X})^*$ with $\underline{(X^*)}$ through i_x ; by the

foregoing if X is an algebra, coalgebra or Hopf algebra the structure morphisms of $(\underline{X})^*$ and $\underline{(X^*)}$ are preserved.

For a Hopf algebra H we have H, $\underline{H}$, H^*, $\underline{(H^*)} = (\underline{H})^*$. Let ρ be the algebra morphism,

$$\rho: H^* \to \underline{(H^*)} = (\underline{H})^*$$
$$a^* \to \underline{a^{*p}}$$

it is an algebra morphism because H^* is commutative. Then ${}^t\rho: (\underline{H})^{**} \to H^{**}$. We shall show $\mathrm{Im}({}^t\rho|\underline{H}) \subset H$.

Choose an ordered basis $\{h_\alpha\}$ for H, then by cocommutivity and coassociativity $d^{n-1}(h) \subset S_n H$ for all $h \in H$ and we have

$$\beta \circ d^{n-1}(h) \in k[\{h_\alpha\}]_n$$

or $$d^{n-1}(h) = \sum_{i=1}^{M} \lambda_i \, \alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}}) , \quad \lambda_i \in k ,$$

where $$e_{i_1} + \cdots + e_{i_m} = n , \quad \alpha_1 < \cdots < \alpha_m .$$

For $x \in H$ let $\#(x)$ be the minimal integer t where $x \in H_t$. By choosing the basis for H as follows:

choose a basis for H_0

extend to a basis for H_1

extend to a basis for H_2

- - - - - - - - - - - - - - ;

and then ordering it we have

$$d^{n-1}(h) = \sum_{i=1}^{M} \lambda_i \, \alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}}) \ , \ \lambda_i \in k \ ,$$

where $e_{i_1} + \cdots + e_{i_m} = n \quad \alpha_1 < \cdots < \alpha_m$ and

$$\#(h) \geq e_{i_1} \#(h_{\alpha_1}) + \cdots + e_{i_m} \#(h_{\alpha_m}) \ .$$

For $a^* \in H^*$

$$\langle \rho(a^*), h \rangle = \langle a^{*[p]}, \, d^{p-1}(h) \rangle$$

$$= \langle a^{*[p]}, \, \sum_{i=1}^{M} \lambda_i \, \alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}}) \rangle \ .$$

As a symmetric tensor in $\{ h_{\alpha_i} \}$, the number of terms involved in

$$\alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}}) \quad \text{is}$$

divisible by p unless

$$h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}} \qquad \text{is of the form} \quad h_{\alpha_t}^{p}$$

for $1 \leq t \leq m$. Let

$$I = \left\{ i=1,\ldots M \,\middle|\, h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}} = h_{\alpha_t}^{p} \quad 1 \leq t \leq m \right\} ,$$

then for $i \in I$ let $n(i)$ be such that

$$h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}} = h_{\alpha_{n(i)}}^{p} \ .$$

If $i \notin I$

$$\langle a^{*[p]}, \alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}}) \rangle = 0$$

(consider the number of terms in $\alpha(h_{\alpha_1}^{e_{i_1}} \cdots h_{\alpha_m}^{e_{i_m}})$.)

Thus

$$\langle \rho(a^*), h \rangle = \langle a^{*[p]}, \sum_{i \in I} \lambda_i \alpha(h^p_{\alpha_{n(i)}}) \rangle$$

$$= \sum_{i \in I} \lambda_i \langle a^*, h_{\alpha_{n(i)}} \rangle^p .$$

3) This shows ${}^t\rho(\underline{h}) = \sum_{i \in I} \lambda_i^{\frac{1}{p}} h_{\alpha_{n(i)}} \in H$,

or $\mathrm{Im}({}^t\rho(\underline{H}) \subset H$.

Let $V = {}^t\rho|\underline{H}: \underline{H} \to H$.

Observe $\#(\underline{h}) = \#(h)$ (or $\underline{H}_n = (\underline{H})_n$). Since we choose the "extending" basis for H, for $i \in I$

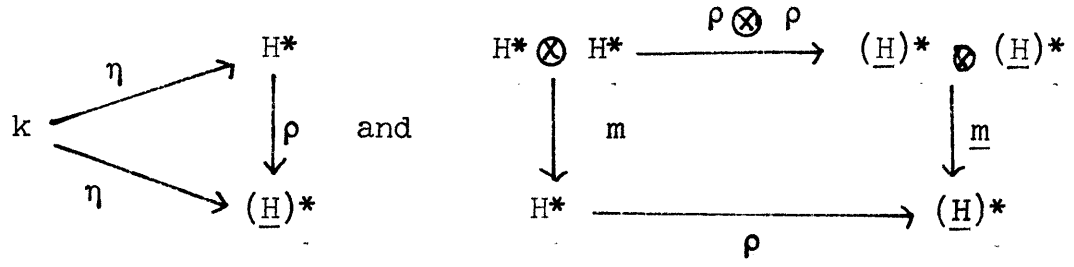
$$\#(h) \geq p \, \#(h_{\alpha_{n(i)}})$$

and so

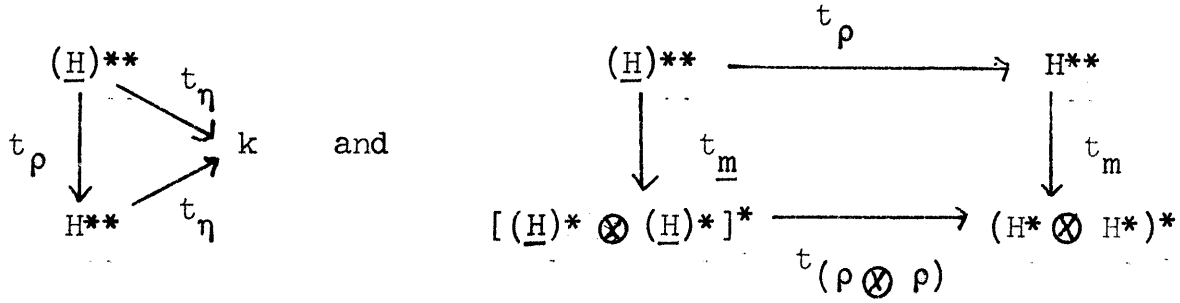
$$p \, \#(V(\underline{h})) \leq \#(\underline{h}) .$$

We wish to show V is a morphism of Hopf algebras, first we show it is a coalgebra morphism.

Being an algebra morphism



are commutative. Dualizing gives commutative diagrams,

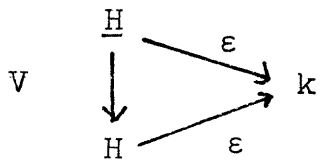


In the left diagram $\underline{H} \subset (\underline{H})^{**}$,

$$t_\rho|\underline{H}: \underline{H} \xrightarrow{V} H \subset H^{**} ,$$

$$t_\eta|\underline{H}: \underline{H} \xrightarrow{\varepsilon} k , \quad t_\eta|H: H \xrightarrow{\varepsilon} k$$

which implies commutivity of



.

In the right diagram

$$\underline{H} \otimes \underline{H} \subset [(\underline{H})^* \otimes (\underline{H})^*]^* \qquad \text{where}$$

$$\langle (\underline{a})^* \otimes (\underline{b})^* , \underline{h} \otimes \underline{g} \rangle = \langle (\underline{a})^*, \underline{h} \rangle \langle (\underline{b})^*, \underline{g} \rangle ,$$

similarly $H \otimes H \subset (H^* \otimes H^*)^*$.

Then ${}^t\rho|\underline{H} = V$, ${}^t\underline{m}|\underline{H} = d_{\underline{H}}$

$${}^t(\rho \otimes \rho)|\underline{H} \otimes \underline{H} = V \otimes V \ , \ {}^t m|H = d_H \ ,$$

and

$$\begin{array}{ccc} \underline{H} & \xrightarrow{V} & H \\ \downarrow{\scriptstyle d_{\underline{H}}} & & \downarrow{\scriptstyle d_H} \\ \underline{H} \otimes \underline{H} & \xrightarrow[V \otimes V]{} & H \otimes H \end{array}$$ so

V is a morphism of coalgebras.

Now to show V is a morphism of algebras. At 3) we have

$$t_\rho(\underline{h}) = \sum_{i \in I} \lambda_i^{\frac{1}{p}} h_{\alpha_{n(i)}} \ .$$

In choosing our "extending" basis for H we can choose $\{1\}$ as a basis for H_0 thus by 3) ,

$$\begin{array}{ccccc} & & \underline{H} & & \\ & \overset{\eta}{\nearrow} & \downarrow{\scriptstyle V} & & \\ k & & & & \text{is commutative.} \\ & \underset{\eta}{\searrow} & & & \\ & & H & & \end{array}$$

$H \otimes H$ is a coalgebra and one main property of a Hopf algebra is that $m_H : H \otimes H \to H$ is a coalgebra morphism. Since $H \otimes H$ is a coalgebra $(H \otimes H)^*$ is an algebra, $m_H : H \otimes H \to H$ being a coalgebra morphism implies

$$H^* \xrightarrow{{}^t m_H} (H \otimes H)^*$$

is an algebra morphism.

If $r: (H \otimes H)^* \to \underline{((H \otimes H)^*)} = (\underline{H \otimes H})^*$

$$Y^* \to \underline{(Y^*)}^{\rho} ,$$

then r is an algebra morphism and

$$\begin{array}{ccc} H^* & \xrightarrow{{}^t m_H} & (H \otimes H)^* \\ \downarrow \rho & & \downarrow r \\ (\underline{H})^* & \xrightarrow[{}^t m_{\underline{H}}]{} & (\underline{H \otimes H})^* \end{array}$$

is commutative, (since ${}^t m_H$ an algebra morphism and ${}^t m_{\underline{H}} = \underline{{}^t m_H}$). Then passing to the duals and transpose maps and restricting to H, $\underline{H}$, $H \otimes H$, $\underline{H} \otimes \underline{H}$ gives commutivity of

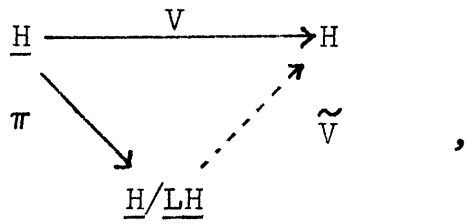
$$\begin{array}{ccc} \underline{H} \otimes \underline{H} & \xrightarrow{m} & \underline{H} \\ \downarrow V \otimes V & & \downarrow V \\ H \otimes H & \xrightarrow{m} & H \end{array}$$

so that V is an algebra morphism. Thus $V: \underline{H} \to H$ is a Hopf algebra morphism.

Since $\rho = {}^t V$ it follows

$$\text{Ker } V = (\text{Im } \rho)^{\perp}.$$

Thus by (9) Ker V = $\underline{LH}$, and there is a factoring



where $\tilde{V}$ is an injective Hopf algebra morphism.

$\underline{H/LH} = \underline{H/LH}$ so

$$\tilde{V}: \underline{H/LH} \to H$$

is an injective Hopf algebra morphism.

Within H we have the sub Hopf algebra Im V . We define inductively a nested sequence of sub Hopf algebras:

$$V_0 = H , \qquad \text{if } V_i \text{ is formed}$$

$\underline{V_i} \subset \underline{H}$, $V_{i+1} = V(\underline{V_i})$.

We have $V_0 \supset V_1 \supset \ldots$, let

$$V_\infty = \bigcap_{i=0}^{\infty} V_i .$$

Being the intersection of subalgebras V_∞ is a subalgebra. We show it is a subcoalgebra as follows:

each V_i is a subcoalgebra

hence $(V_i)^\perp \subset H^*$ is a 2-sided ideal,

$$(V_0)^{\perp} \subset (V_1)^{\perp} \subset (V_2)^{\perp} \cdots$$

and $X = \bigcup_{i=0}^{\infty} (V_i)^{\perp}$ $(\subset H^*)$ is a 2-sided ideal.

$$V_\infty = X^{\perp} .$$

This implies V_∞ is a subcoalgebra, we present a simple proof.

$(V_\infty)^*$ is naturally isomorphic to H^*/X as a vector space where

$$H^* \xrightarrow{\pi} H^*/X$$

$$H \xleftarrow[i]{} V_\infty$$

are transpose maps.

$$(H \otimes H)^* \xrightarrow{{}^t d} H^* \xrightarrow{\pi} H^*/X$$

$$H \otimes H \xleftarrow{d} H \xleftarrow{i} V_\infty$$

are transpose maps so

$$\mathrm{Im}(d \circ i) = \mathrm{Ker}(\pi \circ {}^t d)^{\perp}$$

$\mathrm{Ker}(\pi \circ {}^t d) \supset H^* \otimes X + X \otimes H^*$ which implies

$$\mathrm{Im}(d \circ i) \subset (H^* \otimes X + X \otimes H^*)^{\perp} = V_\infty \otimes V_\infty .$$

Thus V_∞ is also a sub Hopf algebra of H.

$$V_n = \mathrm{Im}\left(\begin{matrix} H \\ \vdots \\ H \end{matrix} \xrightarrow{\begin{matrix} n \\ V \\ \vdots \end{matrix}} \begin{matrix} H \\ \vdots \\ H \end{matrix} \xrightarrow{\begin{matrix} n-1 \\ V \\ \vdots \end{matrix}} \cdots \xrightarrow{3} \begin{matrix} H \\ H \end{matrix} \xrightarrow[V]{2} \begin{matrix} H \\ V \end{matrix} \xrightarrow{1} H\right) ,$$

we have the transpose map

$$\begin{pmatrix} \underline{H} \\ \vdots \\ \underline{H} \end{pmatrix}^* \xleftarrow{\begin{pmatrix} \underline{\rho} \\ \vdots \\ \underline{\rho} \end{pmatrix}} \cdots \xleftarrow{\underline{\rho}} (\underline{H})^* \xleftarrow{\rho} H^*$$

so $V_n = [\mathrm{Ker}(\underline{\rho} \circ \cdots \circ \rho)]^{\perp}$. We shall for simplicity let ρ^n denote

$$\underbrace{\begin{pmatrix} \underline{\rho} \\ \vdots \\ \underline{\rho} \end{pmatrix} \circ \cdots \circ \rho}_{n} ,$$

V^n denote $\underbrace{V \circ \cdots \circ \underline{V}}_{n}$ and $\underset{\sim}{x}$ denote $\begin{pmatrix} \underline{x} \\ \vdots \\ \underline{x} \end{pmatrix}$. As a map

$$\rho^n : H^* \to \underset{\sim}{(H^*)} = (\underset{\sim}{H})^*$$

$$a^* \to \underset{\sim}{(a^*)^{p^n}} .$$

Then $(V_n)^{\perp} = \mathrm{Ker}(\rho^n)$. We define

$$L_i = L \cap V_i \qquad i=0,1,\ldots$$

$$L_\infty = L \cap V_\infty ,$$

so we have a decreasing sequence of restricted Lie algebras

$$L = L_0 \supset L_1 \supset \cdots\cdots ,$$

$$\bigcap_{i=0}^{\infty} L_i = L_\infty .$$

Divided Powers

In any characteristic suppose we have a (possibly infinite) sequence of elements

$$x_0, x_1, x_2, \ldots$$

where for any n

$$dx_n = \sum_{i=0}^{n} x_i \otimes x_{n-i} .$$

Then $dx_0 = x_0 \otimes x_0$ so x_0 is grouplike and by coconnectivity $x_0 = 1$.

$$dx_1 = x_0 \otimes x_1 + x_1 \otimes x_0$$

$$= 1 \otimes x_1 + x_1 \otimes 1$$

so that x_1 is primitive. Such a sequence is called a sequence of divided powers of x_1 . x_n is called an n^{th} divided power of x_1 .

Example

In characteristic 0 if x is a primitive element and $x_i = \frac{x^i}{i!}$ then $x_0, x_1, x_2, \ldots$ is an infinite sequence of divided powers of x .

Given a sequence $x_0, x_1, \ldots$ of divided powers of x_1 , $\varepsilon(x_n) = 0$ $n > 0$. This follows by induction: $\varepsilon(x_1) = 0$ because x_1 is primitive, for $n > 1$

$$\varepsilon(x_n) = \varepsilon * \varepsilon(x_n) = \sum_{i=0}^{n} \varepsilon(x_i) \otimes \varepsilon(x_{n-i})$$

(by induction) $$= 2\, \varepsilon(x_n) .$$

Suppose characteristic $p > 0$, since

$$d^{p-1}(x_n) = \sum_{e_1+\cdots+e_p = p} x_{e_1} \otimes \cdots \otimes x_{e_p}$$

$$V(\underline{x_n}) = \begin{cases} 0 & p \nmid n \\ x_{\frac{n}{p}} & p|n . \end{cases}$$

For $e \in Z^+$ let $|e| \in Z$ satisfy

$$p^{|e|} \leq e < p^{|e|+1} .$$

Then if we have a finite sequence of divided powers of x_1

$$x_0, x_1, \cdots x_e$$

$x_1 \in V_{|e|}$ and if $e = p^{n+1} - 1$, $i \leq e$,

$x_i \in V_{n-|i|}$.

If we have an infinite sequence of divided powers of x_1 then $x_1 \in V_\infty$.

Theorem 5. If $x \in L_n$ there is a sequence of divided powers of x

$$x_0, x = x_1, \ldots x_{p^{n+1}-1} .$$

Proof: We shall use an induction within an induction in this proof. The "outer" or first induction is on n. The theorem is true for $n = 0$ since for $x \in L_0$

$$x_i = \frac{x^i}{i!} \qquad i=0,1,\ldots p-1$$

is the desired sequence of divided powers of x. Suppose by induction the result is true for $n - 1$.

Include x in a basis for L_n. Extend the basis to a basis for L_{n-1}, then extend to a basis for L_{n-2}, ..., obtaining finally a basis $\{x^\alpha\}$ for $L_0 = L$. Order the basis $\{x^\alpha\}$.

Let $n(\alpha) = \begin{cases} n & \text{if } x^\alpha \text{ part of the basis for } L_n \\ & \text{otherwise} \\ \text{maximal } t \in Z & \text{where } x^\alpha \in L_t . \end{cases}$

By the induction assumption we know that if $n(\alpha) < n$ there is a sequence of divided powers of x^α

$$x^\alpha_0, x^\alpha_1, \ldots \; x^\alpha_{p^{n(\alpha)+1}-1} .$$

We shall construct sequences of divided powers for the x^α where $n(\alpha) = n$. The construction has 2 distinct parts which we separate.

I) Suppose for each α where $n(\alpha) = n$,

i) there is a sequence of divided powers for x^α

$$x^\alpha_0, \ldots x^\alpha_{t-1} \qquad 0 \leq t < p^{n+1} ,$$

ii) $x^{\alpha}_{e} \in V_{n-|e|} \qquad 0 \leq e \leq t-1$

iii) there is an element $\tilde{y}^{\alpha}_{t}$ where

$$\tilde{y}^{\alpha}_{t} \in V_{n-|t|} \text{ and } K(\tilde{y}^{\alpha}_{t}) = (x^{\alpha})^{t} ;$$

then each such sequence can be extended to a sequence of divided powers of x^{α}

$$x^{\alpha}_{0}, \cdots x^{\alpha}_{t}$$

satisfying $x^{\alpha}_{e} \in V_{n-|e|} \quad 0 \leq e \leq t$.

Proof of I). Say we are given the sequence $x^{\alpha}_{0}, \ldots x^{\alpha}_{t-1}$ to extend. Suppose we have $y^{\alpha}_{s} \quad 2 < s \leq t$ satisfying:

$$E^{[s]} \circ d^{s-1}(y^{\alpha}_{s}) = \sum_{\substack{0 < f_i \\ f_1+\cdots+f_s = t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_s}$$

$y^{\alpha}_{s} \in V_{n-|t|}$; for example,

let $y^{\alpha}_{t} = \tilde{y}^{\alpha}_{t}$; we shall construct y^{α}_{s-1} satisfying

$$E^{[s-1]} \circ d^{s-2}(y^{\alpha}_{s-1}) = \sum_{\substack{0 < f_i \\ f_1+\cdots+f_{s-1} = t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_{s-1}}$$

$$y^{\alpha}_{s-1} \in V_{n-|t|} \ .$$

Consider

$$E^{[s-1]} \circ d^{s-2}(y^{\alpha}_{s}) =$$

$$\sum_{\substack{f_i>0 \\ f_1+\cdots+f_{s-1}=t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_{s-1}} + Y , \quad Y \in H^{+[s-1]}$$

$(H^{+} = \operatorname{Ker} \varepsilon)$. We show $Y \in L \otimes H^{+[s-2]}$. Since $\operatorname{Ker}(E \otimes E \circ d) = H_1$ it suffices to show $E \otimes E \otimes I^{[s-2]} \circ d \otimes I^{[s-2]}(Y) = 0$ or it suffices to show

$$E \otimes E \otimes I^{[s-2]} \circ d \otimes I^{[s-2]}\Big(\sum_{\substack{f_i>0 \\ f_1+\cdots+f_{s-1}=t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_{s-1}} + Y\Big) =$$

$$E \otimes E \otimes I^{[s-2]} \circ d \otimes I^{[s-2]}\Big(\sum_{\substack{f_i>0 \\ f_1+\cdots+f_{s-1}=t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_{s-1}}\Big) .$$

The left hand side (top)

$$= E \otimes E \otimes I^{[s-2]} \circ d \otimes I^{[s-2]} \circ E^{[s-1]} \circ d^{s-2}(y^{\alpha}_{s})$$

(since $E \otimes E \circ d \circ E = E \otimes E \circ d$)

$$= E^{[s]} \circ d^{s-1}(y^{\alpha}_{s}) = \sum_{\substack{f_i>0 \\ f_1+\cdots+f_s=t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_s}$$

which is the right hand side, (bottom). By similar reasoning $Y \in H^{+} \otimes \cdots \otimes L \otimes \cdots \otimes H^{+}$ so $Y \in L^{[s-1]}$.

Thus $E^{[s-1]} \circ d^{s-2}(y^{\alpha_s}) =$

$$\sum_{\substack{f_i > 0 \\ f_1+\cdots+f_{s-1}= t}} x^{\alpha}{}_{f_1} \otimes \cdots \otimes x^{\alpha}{}_{f_{s-1}} + \sum_j \lambda_j \alpha(x^{\alpha_1 e_{j_1}} \cdots x^{\alpha_m e_{j_m}})$$

where $e_{j_1}+\cdots+ e_{j_m} = s - 1 \quad \alpha_1 <\cdots< \alpha_m$. Now we wish to show that we can assume--when $n(\alpha_r) < n$ --

$$e_{q_r} < p^{n(\alpha_r)-n+|t|+1}$$

for all q, r . Suppose not, that for some q_r $e_{q_r} \geq p^{n(\alpha_r)-n+|t|+1}$. Without loss we assume $q_r = 1_1$.

$x^{\alpha_1} \notin V_{n(\alpha_1)+1}$ by the choice of an extending basis, so we can choose a dual basis

$$\{a_i^*\}_{i=1}^m \subset J \quad \text{to} \quad \{x^{\alpha_i}\}_{i=1}^m$$

where we assume $a_1^* \in (V_{n(\alpha_1)+1})^{\perp}$.

$$(V_{n(\alpha_1)+1})^{\perp} = \operatorname{Ker} \rho^{n(\alpha_1)+1},$$

so $(a_1^*)^{p^{n(\alpha_1)+1}} = 0$ and $\rho^{n-|t|}(a_1^{*p^{n(\alpha_1)-n+|t|+1}}) = 0$.

Since $y^{\alpha_s} \in V_{n-|t|}$ let $z \in H$ where

$$V^{n-|t|}(z) = y .$$ Let

$$a^* = a_1^{*\,e_{1_1} - p^{n(\alpha_1)-n+|t|+1}} * a_2^{*\,e_{1_2}} *\cdots* a_m^{*\,e_{1_m}} .$$

Note for $c^*, b^* \in H^*$, $h \in H$

$$V^n(\rho^n(b^*) \cdot \underset{\sim}{h}) = b^* \cdot V^n(\underset{\sim}{h})$$

since

$$\begin{aligned} \langle c^*, V^n(\rho^n(b^*) \cdot \underset{\sim}{h})\rangle &= \langle \rho^n(c^*), \rho^n(b^*) \cdot \underset{\sim}{h}\rangle \\ &= \langle \rho^n(c^* * b^*), \underset{\sim}{h}\rangle = \langle c^* * b^*, V^n(\underset{\sim}{h})\rangle \\ &= \langle c^*, b^* \cdot V^n(\underset{\sim}{h})\rangle \quad . \end{aligned}$$

Consider

$$0 = \langle \rho^{n-|t|}(a_1^{*\,p^{n(\alpha_1)-n+|t|+1}}), [\rho^{n-|t|}(a^*)] \cdot \underset{\sim}{z}\rangle$$

$$= \langle a_1^{*\,p^{n(\alpha_1)-n+|t|+1}}, V^{n-|t|}(\rho^{n-|t|}(a^*) \cdot \underset{\sim}{z})\rangle$$

$$= \langle a_1^{*\,p^{n(\alpha_1)-n+|t|+1}}, a^* \cdot y^{\alpha_s}\rangle$$

$$= \langle a_1^{*\,e_{1_1}} *\cdots* a_m^{*\,e_{1_m}}, y^{\alpha_s}\rangle$$

$$= \lambda_1 + \sum_{\substack{f_i>0 \\ f_1+\cdots+f_{s-1}=t}} \langle a_1^*, x^{\alpha_{f_1}}\rangle \cdots \langle a_1^*, x^{\alpha_{f_{e_{1_1}}}}\rangle \cdots \langle a_m^*, x^{\alpha_{f_{s-1}}}\rangle$$

For a term in the right sum not to be zero we must have

$$x^{\alpha}_{f_1} \notin V_{n(\alpha_1)+1}, \ldots x^{\alpha}_{f_{e_{1_1}}} \notin V_{n(\alpha_1)+1}$$

since $a_1^* \in (V_{n(\alpha_1)+1})^{\perp}$. Since $x^{\alpha}_{f_i} \in V_{n-|f_i|}$, we must have $n - |f_i| \leq n(\alpha_1)$ $i=1,\ldots e_{1_1}$, or $n - n(\alpha_1) \leq |f_i|$ which implies

$$\rho^{n-n(\alpha_1)} \leq f_i \quad i=1,\ldots e_{1_1} .$$

Suppose this happens then since

$$f_1 + \cdots + f_{s-1} = t \qquad \text{it follows}$$

$$e_{1_1} p^{n-n(\alpha_1)} + [s - 1 - e_{1_1}] \leq t .$$

$s - 1 \geq e_{1_1}$ and we are assuming that

$$e_{1_1} \geq p^{n(\alpha_1)-n+|t|+1}$$

so the above inequality yields

$$p^{n(\alpha_1)-n+|t|+1} p^{n-n(\alpha_1)} + [e_{1_1} - e_{1_1}] \leq t$$

or $p^{|t|+1} \leq t$ a contradiction.

Thus $\langle \rho^{n-|t|}(a_1^* p^{n(\alpha_1)-n+|t|+1}), [\rho^{n-|t|}(a^*)] \cdot \underset{\sim}{z} \rangle = \lambda_1$

which implies $\lambda_1 = 0$ and hence we can assume $e_{q_r} < p^{n(\alpha_r)-n+|t|+1}$, when $n(\alpha_r) < n$. In particular $t < p^{n+1}$ implies $|t| \leq n$ so that $e_{q_r} < p^{n(\alpha_r)+1}$ when

$n(\alpha_r) < n$. Now examine a typical term in

$$\sum_j \lambda_j \alpha((x^{\alpha_1})^{e_{j_1}} \cdots (x^{\alpha_m})^{e_{j_m}}) , \quad \text{say}$$

$$\lambda_1 \alpha(x^{\alpha_1 e_{1_1}} \cdots x^{\alpha_m e_{1_m}}) .$$

Look at $x^{\alpha_i e_{1_i}}$. If $n(\alpha_i) = n$ since $e_{1_i} \leq s - 1 < s \leq t$ there is by hypothesis i) of I

$$x^{\alpha_i}_{e_{1_i}} \varepsilon V_{n-|e_{1_i}|} \ (\subset V_{n-|t|}) .$$

If $n(\alpha_i) < n$ since $e_{1_i} < p^{n(\alpha_i)+1}$ by the outer induction hypothesis of the theorem there is $x^{\alpha_i}_{e_{1_i}}$. Since there is actually a sequence

$$x^{\alpha_i}_0 , \ldots\ldots\ x^{\alpha_i}_{e_{1_i}} , \ldots\ldots\ x^{\alpha_i}_{p^{n(\alpha_i)+1} - 1} ,$$

it follows

$$x^{\alpha_i}_{e_{1_i}} \varepsilon V_{n(\alpha_i)-|e_{1_i}|} .$$

We have $e_{1_i} < p^{n(\alpha_i)-n+|t|+1}$ which implies

$$|e_{1_i}| \leq n(\alpha_i) - n + |t|$$

or

$$n - |t| \leq n(\alpha_i) - |e_{1_i}|$$

so $x^{\alpha_i}_{e_{l_i}} \in V_{n(\alpha_i)-|e_{l_i}|} \subset V_{n-|t|}$.

Then by (7)

$$K(\lambda_1 x^{\alpha_1}_{e_{l_1}} \cdots x^{\alpha_m}_{e_{l_m}}) = \lambda_1 (x^{\alpha_1^{e_{l_1}}} \cdots x^{\alpha_m^{e_{l_m}}})$$

since $K(x^{\alpha_i}_{e_{l_i}}) = (x^{\alpha_i^{e_{l_i}}})$.

If $z_1 = \lambda_1 x^{\alpha_1}_{e_{l_1}} \cdots x^{\alpha_m}_{e_{l_m}}$, then

$$z_1 \in V_{n-|t|} .$$

Similarly we form $z_j \in V_{n-|t|}$ for all j then

$$y^{\alpha}_{s-1} = y^{\alpha}_{s} - \sum_j z_j \in V_{n-|t|} \quad \text{and}$$

$$E^{[s-1]} \circ d^{s-2} y^{\alpha}_{s-1} = \sum_{\substack{0<f_i \\ f_1+\cdots+f_{s-1}=t}} x^{\alpha}_{f_1} \otimes \cdots \otimes x^{\alpha}_{f_{s-1}} .$$

So we have completed the induction step of I) and finally stop at $y^{\alpha}_2 \in V_{n-|t|}$ where

$$E \otimes E \circ d\, y^{\alpha}_2 = \sum_{i=1}^{t-1} x^{\alpha}_i \otimes x^{\alpha}_{t-i} .$$

Then let $x^{\alpha}_t = y^{\alpha}_2 - \varepsilon(y^{\alpha}_2)$.

$$x^{\alpha}{}_t \in V_{n-|t|} \quad , \qquad \varepsilon(x^{\alpha}{}_t) = 0$$

and $E \otimes E \circ dx^{\alpha}{}_t = \sum_{i=1}^{t-1} x^{\alpha}{}_i \otimes x^{\alpha}{}_{t-i}$. Since

$$dx^{\alpha}{}_t = E \otimes E \circ dx^{\alpha}{}_t + I \otimes \varepsilon \circ dx^{\alpha}{}_t + \varepsilon \otimes I \circ dx^{\alpha}{}_t - \varepsilon \otimes \varepsilon \circ dx^{\alpha}{}_t$$

$$= \sum_{i=1}^{t-1} x^{\alpha}{}_i \otimes x^{\alpha}{}_{t-i} + 1 \otimes x^{\alpha}{}_t + x^{\alpha}{}_t \otimes 1 + d\,\varepsilon\,(x^{\alpha}{}_t)$$

$$= \sum_{i=0}^{t} x^{\alpha}{}_t \otimes x^{\alpha}{}_{t-i} \quad ,$$

$x^{\alpha}{}_t$ is the desired $t^{\underline{th}}$ divided power of $x^{\alpha}{}_1$, and

$x^{\alpha}{}_t \in V_{n-|t|}$. Thus we have proved I .

Now so that I) can operate we must produce the $\tilde{y}^{\alpha}{}_t$'s .

II:

For $x^{\alpha} \in L_n$ we wish to find $\tilde{y}^{\alpha}{}_{p^n}$. It will then be simple to obtain the other $\tilde{y}^{\alpha}{}_t$'s . $x^{\alpha} \in L_n$ so there is $z \in H$ where $V^n(\underset{w}{z}) = x^{\alpha}$.

First we prove that if there is $z \in H_{p^n}$ where

$$V^n(\underset{w}{z}) = x^{\alpha}$$ then there

is $\tilde{y}^{\alpha}{}_{p^n}$. Say we are given such z , then

$$K(z) = x^{\alpha^{p^n}} + \sum_{i=1}^{M} \lambda_i \, x^{\alpha_1{}^{e_{i_1}}} \cdots x^{\alpha_m{}^{e_{i_m}}}$$

$$\alpha_1 < \cdots < \alpha_m$$

$$e_{i_1} + \cdots + e_{i_m} = p^n \quad .$$

Then for all e_{i_r} , $e_{i_r} < p^n$, because

$$V^n(\underset{w}{z}) = x^{\alpha} + \sum_i \lambda_i^{\frac{1}{p^n}} x^{\alpha_{r_i}} ,$$

where $e_{i_{r_i}} = p^n$.

For all e_{i_r}, $e_{i_r} < p^{n(\alpha_r)+1}$ i.e. $|e_{i_r}| \leq n(\alpha_r)$.

In showing this we assume $n(\alpha_r) < n$ since otherwise the result has just been shown. Suppose some $e_{i_r} \geq p^{n(\alpha_r)+1}$ say e_{1_1} . Let $\{a_i^*\}_{i=1}^m$ be a dual basis to $\{x^{\alpha_i}\}_{i=1}^m$ and $a_1^* \in (V_{n(\alpha_1)+1})^{\perp}$. Then

$a_1^{*p^{n(\alpha_1)+1}} = 0$, (note $x^{\alpha} \in V_n \subset V_{n(\alpha_1)+1}$) but

$\langle a_1^{*e_{1_1}} *\cdots* a_m^{*e_{1_m}}, z\rangle = \lambda_1$ which shows $\lambda_1 = 0$ and we can assume

$$|e_{i_r}| \leq n(\alpha_r) .$$

Thus when $n(\alpha_r) < n$ by the "outer" induction hypothesis of the theorem, we have x^{α_r} the $e_{M_r}^{\text{th}}$ divided power. When $n(\alpha_r) = n$ $e_{M_r} < p^n$; since $x^{\alpha_r} \in V_n \subset V_{n-1}$

by the outer induction hypothesis we have $x^{\alpha_r}_{e_{M_r}}$. Let

$y = \lambda_M x^{\alpha_1}_{e_{M_1}} \cdots x^{\alpha_m}_{e_{M_m}}$. Then

$K(y) = \lambda_M(x^{\alpha_1}_{e_{M_1}} \cdots x^{\alpha_M}_{e_{M_m}})$ by (7) . Since $p^n \nmid e_{M_r}$

$\underset{\sim}{y} \varepsilon$ Ker V^n . So $K(z - y) = \sum_{i=1}^{M-1} \lambda_i x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}}$ and

$V^n(\underset{\sim}{z-x}) = V^n(\underset{\sim}{z}) = x^{\alpha}$. This shows by induction on M that there is z where

$$V^n(\underset{\sim}{z}) = x^{\alpha} \quad \text{and}$$

$K(z) = (x^{\alpha^{p^n}})$. Clearly $z \varepsilon V_{n-|p^n|} = V_0$ so let $\tilde{y}^{\alpha}_{p^n} = z$.

Second we prove that for all x^{α} there is $z \varepsilon H_{p^n}$ where $V^n(\underset{\sim}{z}) = x^{\alpha}$. Suppose not; given such x^{α} choose z where $\#(z) > p^n$ is minimal and $V^n(\underset{\sim}{z}) = x^{\alpha}$. Then

$$K(z) = \sum_{i=1}^{M} \lambda_i x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}}$$

$$\alpha_1 < \cdots < \alpha_m$$

and we can assume $0 < M$ is minimal. Let $\{a_j^*\} \subset J$ be a dual basis to $\{x^{\alpha_j}\}$. We claim for some e_{M_t} ,

$$p^n \nmid e_{M_t} ,$$

because

$$K(V^n(\underset{\sim}{z})) = \sum_i \lambda_i^{1/p^n} x^{\alpha_1 \, e_{i_1}/p^n} \cdots x^{\alpha_m \, e_{i_m}/p^n}$$

where

$$p^n | e_{i_1}, \cdots \; p^n | e_{i_m} \; .$$

Thus we can assume $p^n \nmid e_{M_1}$. Then

$$e_{M_1} = ap^n + b \; , \qquad 0 < b < p^n \; .$$

Note if $n(\alpha_1) < n$ then as usual $e_{M_1} < n(\alpha_1)$ so that $e_{M_1} = 0\, p^n + b$, and since $p^n \nmid e_{M_1}$ $0 < b < p^n$.

Thus if $n(\alpha_1) < n$

$$b = e_{M_1} < n(\alpha_1)$$

and by the overall induction assumption there is $x^{\alpha_1}_{e_{M_1}}$ an $e_{M_1}^{\underline{th}}$ divided power of x^{α_1} .

If $n(\alpha_1) = n$, since $b < p^n$, by the overall induction assumption there is $x^{\alpha_1}_{b}$ a $b^{\underline{th}}$ divided power of x^{α_1} .

So in either case there is $x^{\alpha_1}_{b}$ a $b^{\underline{th}}$ divided power of x^{α_1} . Consider $K(a_1{}^{*b} \cdot z)$, by (10)

$$K(a_1{}^{*b} \cdot z) = \sum_{i=1}^{M} \overline{\lambda}_i \, x^{\alpha_1 \, e_{i_1} - b} \, x^{\alpha_2 \, e_{i_2}} \cdots x^{\alpha_m \, e_{i_m}}$$

where

$$\overline{\lambda}_i = \begin{cases} 0 & e_{i_1} < b \\ \lambda_i & \text{otherwise} \; . \end{cases}$$

If we let the usual binomial coefficient $\binom{c}{d} = 0$ when $c < d$ then by (7)

$$K(x^{\alpha_1}{}_b(a_1{}^{*b} \cdot z)) = \sum_{i=1}^{M} \lambda_i \binom{e_{i_1}}{b} x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}} .$$

Now $\binom{e_{M_1}}{b} \not\equiv 0 \pmod{p}$

$$\binom{e_{M_1}}{b} = \left(\left(\frac{ap^n+b}{b}\right)\left(\frac{ap^n+(b-1)}{(b-1)}\right) \cdots\cdots \left(\frac{ap^n+1}{1}\right)\right)$$

so if $y = \dfrac{(x^{\alpha_1}{}_b(a_1{}^{*b} \cdot z))}{\binom{e_{M_1}}{b}}$ then

$x^{\alpha_1}{}_b \in \operatorname{Ker} V^n$ so $y \in \operatorname{Ker} V^n$ and $V^n(z-y) = x^{\alpha}$.

$$K(z-y) = \sum_{i=1}^{M-1} \lambda_i \left(1 - \frac{\binom{e_{i_1}}{b}}{\binom{e_{M_1}}{b}}\right) x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_1 e_{i_m}} ,$$

which contradicts the minimality of M, hence we can assume $z \in H_{p^n}$, and hence there is $\tilde{y}^{\alpha}_{p^n}$. So for all α where $n(\alpha) = n$ we have $\tilde{y}^{\alpha}_{p^n}$. Let $\tilde{y}^{\alpha}_{p^j} = V^{n-j}(\tilde{y}^{\alpha}_{p^n})$ $j=0,1,\ldots n$. Then $K(\tilde{y}^{\alpha}_{p^j}) = (x^{\alpha})^{p^j}$ and

$$\tilde{y}^{\alpha}_{p^j} \in V_{n-|p^j|} = V_{n-j} .$$

For $\tilde{y}^{\alpha}_{t}$, $t < p^{n+1}$

$$t = a_n p^n + a_{n-1} p^{n-1} + \cdots + a_1 p + a_0$$

$$0 \leq a_i < p$$

$|t|$ = maximal i where $a_i \neq 0$.

By (7) if we let

$$\mathbf{y}^{\boldsymbol{\alpha}}{}_t = (\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_{p^n})^{a_n} \cdots\cdots (\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_{0})^{a_0}$$

then $E^{[t]} \circ d^{t-1}(\mathbf{y}^{\boldsymbol{\alpha}}{}_t) = \left(\frac{(a_n p^n + \cdots + a_0 p^0)!}{(p^n!)^{a_n} \cdots (p^0!)^{a_0}}\right) \alpha(X^{\boldsymbol{\alpha}^t})$.

The coefficient is not zero (mod p).

$$\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_t = \left(\frac{(p^n!)^{a_n} \cdots (p^0!)^{a_0}}{t!}\right) \mathbf{y}^{\boldsymbol{\alpha}}{}_t$$

then $K(\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_t) = (x^{\boldsymbol{\alpha}^t})$.

$\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_t \in V_{n-|t|}$. Thus we have $\left\{\tilde{\mathbf{y}}^{\boldsymbol{\alpha}}{}_t\right\}_{t=0}^{p^{n+1}-1}$ with desired properties and by I) (the sequences of divided powers can be started at $x^{\boldsymbol{\alpha}}{}_0 = 1$ for all $\boldsymbol{\alpha}$) we are done.

Q.E.D.

Corollary to the proof of theorem 5). If $x \varepsilon V_\infty$ there is an infinite sequence of divided powers of x

$$x_0, x_1, x_2, \ldots\ldots$$

Proof: Since $V(V_\infty) = V_\infty$ we may work within V_∞, that is assume $H = V_\infty$. Then

$$V_0 = V_1 = V_2 = \cdots = V_\infty .$$

If $\{x^\alpha\}$ is a basis for $L = L_n$ by the previous theorem there is a sequence of divided powers for each x^α

$$x^\alpha_0, \ldots x^\alpha_{p^{n+1}-1} .$$

This particular sequence satisfies the hypothesis of I) with respect to $n+1$, i.e.

ii) $x^\alpha_e \varepsilon V_{n+1-|e|}$

iii) there is $\tilde{y}^\alpha_t$ where $\tilde{y}^\alpha_t \varepsilon V_{n-|t|}$ and $K(\tilde{y}^\alpha_t) = x^{\alpha^t}$. The existence of $\tilde{y}^\alpha_t$ follows from II) of the theorem and of course all conditions such as $x^\alpha_e \varepsilon V_{n+1-|e|}$ are automatically satisfied. Moreover the "outer" induction hypothesis of the theorem is satisfied since for all α we have sequences

$$x^\alpha_0, \ldots x^\alpha_{p^{n+1}-1} .$$

Thus this particular sequence

$$x^{\alpha}_{0}, \cdots x^{\alpha}_{p^{n+1}-1}$$

can be extended to

$$x^{\alpha}_{0}, \cdots x^{\alpha}_{p^{n+2}-1} \quad .$$

Repeating this we can extend the sequence indefinitely.

Q.E.D.

Let $\{x^{\alpha}\}$ be a basis for L. Order $Z \cup \{\infty\}$ by $Z < \infty$. For α let $n(\alpha) \in Z \cup \{\infty\}$ be maximal where $x^{\alpha} \in V_{n(\alpha)}$. We shall call $\{x^{\alpha}\}$ an extending basis for L if

$\{x^{\alpha} | n(\alpha) \geq n\}$ forms a basis for L_n. In particular if the sequence

$$L_0 \supset L_1 \supset L_2 \supset \cdots\cdots \quad (\supset L_{\infty})$$

stabilizes in a finite number of steps then there is an extending basis for L. Between the theorem and corollary we have shown for x^{α} there is a sequence of divided powers

$$x^{\alpha}_{0}, x^{\alpha}_{1}, \cdots x^{\alpha}_{p^{n(\alpha)+1}-1}$$

where this denotes an infinite sequence if $n(\alpha) = \infty$. When $n(\alpha) = \infty$ let $p^{n(\alpha)+1} = \infty$.

In characteristic $p = 0$ if $\{x^\alpha\}$ is a basis for L then for each x^α there is an infinite sequence of divided powers, e.g. let $x^\alpha{}_n = \frac{x^\alpha{}_n}{n!}$. We call any basis for L an extending basis. For x^α we let

$$x^\alpha{}_0, x^\alpha{}_1, \cdots x^\alpha{}_{p^{n(\alpha)+1}-1}$$

denote any <u>infinite</u> sequence of divided powers for x^α and let $p^{n(\alpha)+1} = \infty$. The following theorem generalizes the Poincaré-Birkhoff-Witt theorem.

<u>Theorem 6)</u>: The characteristic of k is arbitrary, k is perfect. Let H be a cocommutative coconnected Hopf algebra where L has an extending basis $\{x^\alpha\}$. For each x^α fix a sequence of divided powers

$$x^\alpha{}_0, \cdots x^\alpha{}_{p^{n(\alpha)+1}-1} .$$

Order the basis $\{x^\alpha\}$. Then the monomials

$$x^{\alpha_1}_{e_1} \cdots x^{\alpha_m}_{e_m}, \quad \alpha_1 < \cdots < \alpha_m , \quad e_i < p^{n(\alpha_i)+1} ,$$

form a basis for H .

<u>Proof</u>: <u>Span:</u> Let $h \in H$

$$k[\{x^\alpha\}] = K .$$

$$K(h) = \sum_i \lambda_i \, x^{\alpha_1 \, e_{i_1}} \cdots x^{\alpha_m \, e_{i_m}} .$$

$$\alpha_1 < \cdots < \alpha_m .$$

Then $e_{q_r} < p^{n(\alpha_r)+1}$. Suppose not say $e_{l_1} \geq p^{n(\alpha_1)+1}$.

Choose $\{a_i^*\} \subset J$ a dual basis to $\{x^{\alpha_i}\}$ and $a_1^* \in (V_{n(\alpha_1)+1})^{\perp}$. Then $a_1^{*p^{n(\alpha_1)+1}} = 0$ but if $a^* = a_1^{*e_{l_1}} *\cdots* a_m^{*e_{l_m}}$ $\langle a^*, h\rangle = \lambda_1$ which implies $\lambda_1 = 0$ and we can assume $e_{q_r} < p^{n(\alpha_r)+1}$. Then let $x_i = \lambda_i x^{\alpha_1}_{e_{i_1}} \cdots x^{\alpha_m}_{e_{i_m}}$. By (7) $K(\Sigma x_i) = K(h)$,

Σx_i lies in the space spanned by the monomials so K (the space spanned by the monomials) $\supset K(H)$ and by lemma 5 H = space spanned by the monomials.

Independence:

Let A_α be the subcoalgebra of H spanned by

$$x^{\alpha}_{0}, x^{\alpha}_{1}, \ldots x^{\alpha}_{p^{n(\alpha)+1}-1} .$$

Put an algebra structure on A_α by

$$k \rightarrow A_\alpha$$

$$1 \rightarrow x^{\alpha}_{0} .$$

$$x^{\alpha}_{i}x^{\alpha}_{j} = \begin{cases} \binom{i+j}{i} x^{\alpha}_{i+j} & \text{if } i+j < p^{n(\alpha)+1} \\ 0 & \text{otherwise.} \end{cases}$$

Then A_α is a Hopf algebra. This can be checked directly, or in $Q[x]/\langle x^{p^{n(\alpha)+1}} \rangle$ (where if $p^{n(\alpha)+1} = \infty$ we mean $Q[x]$)

$$1, \frac{x}{1!}, \frac{x^2}{2!} \cdots \frac{x^{p^{n(\alpha)+1}-1}}{(p^{n(\alpha)+1}-1)!}$$

generate a sub Hopf algebra A over Z. Then $A \otimes_Z k$ is a Hopf algebra over k which is isomorphic to A_α.

Now we show any finite set of monomials is linearly independent. Given $\alpha_1, \ldots \alpha_m$, where $\alpha_1 < \cdots < \alpha_m$, form

$$A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_m}$$

which is a Hopf algebra and we have a natural morphism

$$\gamma: A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_m} \to H$$

$$x^{\alpha_1}_{e_1} \otimes \cdots \otimes x^{\alpha_m}_{e_m} \to x^{\alpha_1}_{e_1} \cdots x^{\alpha_m}_{e_m},$$

γ is a coalgebra morphism. $L(A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_m})$ has a basis

$$x_1^{\alpha_1} \otimes 1^{[m-1]}, \quad 1 \otimes x_1^{\alpha_2} \otimes 1^{[m-2]}, \quad \ldots \quad 1^{[m-1]} \otimes x_1^{\alpha_m},$$

$\gamma | L(A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_m})$ is injective, thus by lemma 4 γ is injective, which proves the linear independence. Q.E.D.

We call a Hopf algebra connected if $\varepsilon: H \to k$ is the unique algebra morphism from H to k. If H is finite dimensional then H^* is a Hopf algebra. H is connected and H^* is split if and only if H^* is coconnected. H is commutative if and only if H^* is cocommutative. Suppose H is finite dimensional, connected, commutative; H^* is split and k is perfect, then H^* is coconnected and cocommutative and has an extending basis by finite dimensionality. Thus by theorem 6: (in the notation of the theorem)

$$H^* \tilde{=} A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_m}$$

as a coalgebra. By finite dimensionality char $p > 0$ and $n(\alpha_i) < \infty$.

H^* has a basis of monomials as described in theorem 6. Let $\{a_\gamma^{**}\} \subset (H^*)^*$ be a dual basis to the monomial basis for H^*. Let $\{a_{\gamma_i}^{**}\}_{i=1}^{m} \subset \{a_\gamma^{**}\}$ be the dual basis to $\{x^{\alpha_i}\}_{i=1}^{m}$, (the extending basis for $L(H^*)$.)

Then $(H^*)^* \cong \dfrac{k[\underline{\bar{X}}_1]}{\langle \underline{\bar{X}}_1^{p^{n(\alpha_1)+1}} \rangle} \otimes \cdots \otimes \dfrac{k[\underline{\bar{X}}_m]}{\langle \underline{\bar{X}}_m^{p^{n(\alpha_m)+1}} \rangle}$

as an algebra

where an isomorphism is induced by

$$\underline{\bar{X}}_i \rightarrow a_{\gamma_i}^{**} \qquad i=1,\ldots m \ .$$

By finite dimensionality $H^{**} = H$. Thus we have proved a finite dimensional commutative, connected, Hopf algebra over a perfect field where the dual is split is of the form: (as an algebra)

$$\frac{k[\underline{\bar{X}}_1]}{\langle \underline{\bar{X}}_1^{p^{e_1}} \rangle} \otimes \cdots \otimes \frac{k[\underline{\bar{X}}_m]}{\langle \underline{\bar{X}}_m^{p^{e_m}} \rangle} \ .$$

If k is algebraically closed then by the results of the first chapter we can drop the condition that the dual is split since it is automatically satisfied, also k is automatically perfect.

We now conclude by applying results of previous chapters. We show a coconnected cocommutative Hopf algebra over a perfect field is an extension--as an algebra and a coalgebra--of H/LH by U when U is commutative. In characteristic zero $H = U$ and $LH = H^+$ so, the result is trivial. Assume k is perfect of characteristic $p > 0$.

Lemma 6: Let $\{x^{\alpha}\}$ be an ordered basis for L, and $K = k[\{x^{\alpha}\}]$. If $h \in V_1$ where

$$K(h) = \sum_i \lambda_i (x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}})$$

then there is $g \in H$ where

$$K(g) = \sum_i \lambda_i{}^p (x^{\alpha_1 pe_{i_1}} \cdots x^{\alpha_m pe_{i_m}}),$$

and

$$V(g) = h .$$

Proof: Since $h \in V_1$ there is $f \in H$ where $V(f) = h$. Say $\#(h) = n$, so $\#(f) \geq pn$. We first show we can choose f where $\#(f) = pn$. Suppose not choose f where $\#(f) > pn$ is minimal then

4) $$K(f) = \sum_j \mu_j (x^{\beta_1 f_{j_1}} \cdots x^{\beta_t f_{j_t}}) \quad \mu_j \in k$$

$\{x^{\beta_j}\} \subset$ the ordered basis,

$$\beta_1 < \cdots < \beta_t , \quad f_{j_1} + \cdots + f_{j_t} = \#(f) > pn .$$

Suppose for some j $p | f_{j_1}, \ldots p | f_{j_t}$. Let $\{a_k^*\}_{k=1}^t \subset J$ be a dual basis to $\{x^{\beta_k}\}_{k=1}^t$, $a^* = a_1^{*\, f_{j_1}/p} * \cdots * a_t^{*\, f_{j_t}/p}$.

$\mu_j^{\frac{1}{p}} = \langle \rho(a^*), \underline{f} \rangle = \langle a^*, V(\underline{f}) \rangle = \langle a^*, h \rangle$. However,

$a^* \in J^{\frac{\#(f)}{p}}$ and $\frac{\#(f)}{p} > n = \#(h)$ implies $\langle a^*, h\rangle = 0$

so $\nu_j = 0$.

Thus in 4) we can assume for each j there is r where $p \nmid f_{j_r}$. Then $K(f) \subset W$ where W is defined in the proof of (9) , by

(11) $$K(H) \cap W = K(LH) ;$$

hence, there is $x \in LH$ where $K(f) = K(x)$. By (6) $\#(f-x) < \#(f)$, since $\underline{LH} = \operatorname{Ker} V$, $V(\underline{f-x}) = V(\underline{f}) = h$. This contradicts the minimality of $\#(f)$ and shows we can choose f where $\#(f) = pn$. Then

$$K(f) = \sum_i \lambda^{p}{}_i (x^{\alpha_1^{pe_{i_1}}} \cdots x^{\alpha_m^{pe_{i_m}}}) + \sum_{j=1}^{M} \nu_j (x^{\beta_1^{f_{j_1}}} \cdots x^{\beta_t^{f_{j_t}}})$$

$\{x^{\beta_j}\}$ contained in the ordered basis, $\nu_j \in k$,

$\beta_1 < \cdots < \beta_t$ $f_{j_1} + \cdots + f_{j_t} = pn$, and we can assume M is minimal. If $M = 0$ we are done, suppose not. Suppose $p | f_{M_1} \cdots p | f_{M_t}$. As usual $\{a_\alpha^*\} \subset J$ is a dual basis to $\{x^\alpha\}$ and $a^* = a_{\beta_1}{}^{*\frac{f_{M_1}}{p}} * \cdots * a_{\beta_t}{}^{*\frac{f_{M_t}}{p}}$.

$$\nu_M^{\frac{1}{p}} + \sum_i \lambda_i \langle a_{\beta_1}{}^{*[\frac{f_{M_1}}{p}]} \otimes \cdots \otimes a_{\beta_t}{}^{*[\frac{f_{M_t}}{p}]} , \alpha(x^{\alpha_1^{e_{i_1}}} \cdots x^{\alpha_m^{e_{i_m}}}) \rangle$$

$$= \langle \rho(a^*), \underline{f} \rangle = \langle a^*, V(\underline{f}) \rangle = \langle a^*, h \rangle$$

$$= \sum_i \lambda_i \langle a_{\beta_1}^{*[\frac{f_{M_1}}{p}]} \otimes \cdots \otimes a_{\beta_t}^{*[\frac{f_{M_t}}{p}]} , \alpha(x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}}) \rangle ,$$

which implies $\mu_M = 0$ and contradicts the minimality of M. Hence, $p \nmid f_{M_r}$ for some r. It is no loss to assume $r = 1$.

Then by (10), (7)

$$K(x^{\beta_1}(a_{\beta_1}^* \cdot f)) = \sum_{j=1}^{M} \mu_j f_{j_1} x^{\beta_1 f_{j_1}} \cdots x^{\beta_t f_{j_t}}$$

and

if $x = \dfrac{x^{\beta_1}(a_{\beta_1}^* \cdot f)}{f_{M_1}} \in LH$ then

$$K(f-x) = \sum_i \lambda^{p_i}(x^{\alpha_1 pe_{i_1}} \cdots x^{\alpha_m pe_{i_m}})$$

$$+ \sum_{j=1}^{M-1} \mu_j (1 - \frac{f_{j_1}}{f_{M_1}}) x^{\beta_1 f_{j_1}} \cdots x^{\beta_t f_{j_t}}$$

$x \in LH$ so $V(\underline{f-x}) = h$, this contradicts the minimality of $M > 0$ hence $M = 0$. Q.E.D.

Theorem 7. There is a projection $P: H \to U$ which is a regular morphism of left U-modules.

Proof: Fix a basis $\{V^\gamma\}$ for V_1 obtained as follows: choose a basis--say $\{1\}$ --for $(V_1)_0$. Extend to a basis for $(V_1)_1$, extend to a basis for $(V_1)_2, \ldots$. Fix an ordered basis $\{x^\alpha\}$ for L. For each $V^\gamma \in \{V^\gamma\}$ let $K(V^\gamma) = \sum_i \lambda_i x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}}$. By lemma 6 we can find and fix

$$\sigma(V^\gamma) \in H \qquad \text{where}$$

$$K(\sigma(V^\gamma)) = \sum_i \lambda_i{}^p x^{\alpha_1 pe_{i_1}} \cdots x^{\alpha_m pe_{i_m}}.$$

Then by linearity we can extend σ to

$$\sigma: V_1 \to H$$

$$V^\gamma \to \sigma(V^\gamma).$$

We wish to show

$$U \otimes V_1 \xrightarrow{m \circ i \otimes \sigma} H$$

is a linear isomorphism.

Surjective: By induction on n we shall show $H_n \subset \text{Im } m \circ i \otimes \sigma$. Since $\sigma(1) = 1$ because we chose $\{1\}$ as a basis for $(V_1)_0$, $H_0 \subset \text{Im}(m \circ i \otimes \sigma)$. Suppose $H_{n-1} \subset \text{Im}(m \circ i \otimes \sigma)$, let $h \in H_n - H_{n-1}$.

$$K(h) = \sum_j \nu_j x^{\alpha_1 f_{j_1}} \cdots x^{\alpha_m f_{j_m}}$$

suppose for some j where $\nu_j \neq 0$ $\quad p|f_{j_1}, \ldots p|f_{j_m}$.

Then

$$K(V(\underline{h})) = \sum_j \nu_j^{\frac{1}{p}} x^{\alpha_1 \frac{f_{j_1}}{p}} \cdots x^{\alpha_m \frac{f_{j_m}}{p}}$$

j where

$$p|f_{j_1}, \ldots p|f_{j_m}$$

$V(\underline{h}) = \sum_k \nu_k V^{\gamma_k}$. Consider

$$x = \sum_k \nu_k^p \sigma(V^{\gamma_k}) .$$

$$K(x) = \sum_j \nu_j x^{\alpha_1 f_{j_1}} \cdots x^{\alpha_m f_{j_m}}$$

j where

$$p|f_{j_1}, \ldots p|f_{j_m} .$$

$x \in \mathrm{Im}(m \circ i \otimes \sigma)$ so that by considering $h - x$ we may assume

$$K(h) = \sum_j \nu_j x^{\alpha_1 f_{j_1}} \cdots x^{\alpha_m f_{j_m}}$$

where for each j there is

$$f_{j_t} \quad \text{where} \quad p \nmid f_{j_t} .$$

Then as in the proof of (9)

$$K(h) = K(\sum_i \lambda_i \ell_i (a_i^* \cdot h_i))$$

where $\lambda_i \in k$, $\ell_i \in L$ $a_i^* \in J$ $h_i \in H_n$. Since $h_i \in H_n$ $a_i^* \cdot h_i \in H_{n-1}$ so by induction there is $X_i \in U \otimes V_1$ where $m \circ i \otimes \sigma(X_i) = a_i^* \cdot h_i$.

$U \otimes V_1$ is naturally a left U-module. $m \circ i \otimes \sigma$ is a left U-module morphism so that

$$m \circ i \otimes \sigma(\ell_i \cdot X_i) = \ell_i (a_i^* \cdot h_i) .$$

Let $\Sigma \lambda_i \ell_i \cdot X_i = X \in U \otimes V_1$. Then $K(h) - K(m \circ i \otimes \sigma(X)) = 0$ so $h - m \circ i \otimes \sigma(X) \in H_{n-1} \subset \operatorname{Im} m \circ i \otimes \sigma$ by (6), which implies $h \in \operatorname{Im} m \circ i \otimes \sigma$ and $H_n \subset \operatorname{Im} m \circ i \otimes \sigma$. Thus $m \circ i \otimes \sigma$ is surjective.

Injective: Since U, V_1 are filtered, $U \otimes V_1$ is filtered by

$$(U \otimes V_1)_n = \sum_{i=0}^{n} U_i \otimes (V_1)_{n-i} .$$

Suppose $m \circ i \otimes \sigma$ is not injective, then there is $X \in (U \otimes V_1)$ where $m \circ i \otimes \sigma(X) = 0$. We choose such X where $X \in (U \otimes V_1)_n$ and n is minimal. Since U is a r.u.e.a. of L, U has a basis

$$\left\{ x^{\alpha_1 e_1} \cdots x^{\alpha_m e_m} \;\middle|\; \begin{array}{l} \alpha_1 < \cdots < \alpha_m \\ m = 0,1,\ldots \\ 0 < e_i < p \end{array} \right\}$$

and $x^{\alpha_1 e_1} \cdots x^{\alpha_m e_m} \varepsilon\ U_{e_1 + \cdots + e_m}$. Thus we can write

$$X = \sum_{i,j} \lambda_{i,j}\, x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}} \otimes V^{\gamma_j}$$

$$\alpha_1 < \cdots < \alpha_m \qquad 0 \leq e_{i_r} < p .$$

Moreover since the sum is finite we assume for V^{γ_j} (appearing in the sum)

$$K(V^{\gamma_j}) \varepsilon\ k[\ x^{\alpha_1}, \ldots x^{\alpha_m}\ ] .$$

This is a notational convenience later.

$X \varepsilon\ (U \otimes V_1)_n$ implies

$n \geq e_{i_1} + \cdots + e_{i_m} + \#(V^{\gamma_j})$ whenever $\lambda_{i,j} \neq 0$. (This uses the fact we have chosen an extending basis for V_1.) Moreover by minimality of n there is $\lambda_{q,r} \neq 0$ where $n = e_{q_1} + \cdots + e_{q_m} + \#(V^{\gamma_r})$.

Choose q,r where $\lambda_{q,r} \neq 0$

$n = e_{q_1} + \cdots + e_{q_m} + \#(V^{\gamma_r})$ and

$\#(V^{\gamma_r})$ is maximal.

Say $q,r = 1,1$ $\#(V^{\gamma_1}) = N$, $e_{1_1} + \cdots + e_{1_m} = M$. Notice $\#(\sigma(V^{\gamma})) = p\#(V^{\gamma})$ so by our choice of $1,1$ if $\lambda_{i,j} \neq 0$ $(m \circ i \otimes \sigma(x^{\alpha_1 e_{i_1}} \cdots x^{\alpha_m e_{i_m}} \otimes V^{\gamma_j})) \leq M + pN$.

If equality holds then $\#(V^{\gamma_j}) = N$ since $n \geq e_{i_1} + \cdots + e_{i_m} + \#(V^{\gamma_j})$.

Let $T = M + pN$. Since U has a basis of monomials let $\{a_\beta^*\} \subset H^*$ be a dual basis and let $\{a_k^*\}_{k=1}^{m} \subset \{a_\beta^*\}$ be the dual basis to $\{x^{\alpha_k}\}_{k=1}^{m}$. H^* is a right H-module where $\langle b^* \cdot h, g\rangle = \langle b^*, gh\rangle$ and the primitive elements of H act as derivations. By our choice of $\{a_k^*\}$, $\langle a_k^*, x^{\alpha_\ell}\rangle = \delta_{k,\ell}$. Let $I = \{j \mid \#(V^{\gamma_j}) = N\}$, $1 \in I$. $\{V^{\gamma_j} \mid j \in I\}$ is a linearly independent set and since we have chosen an extending basis for V_1,

$$\{K(V^{\gamma_j}) \mid j \in I\}$$

is a linearly independent set, as is

$$\{\alpha(K(V^{\gamma_j})) \mid j \in I\}.$$

Then $\{\alpha(K(\sigma(V^{\gamma_j})))\}_{j \in I}$

is a linearly independent set. (Because by definition of

$\sigma(V^{\gamma_j})$ if $\sum_{j\varepsilon I} \xi_j\, \alpha(K(\sigma(V^{\gamma_j}))) = 0$ then

$$\sum_{j\varepsilon I} \xi_j^{\frac{1}{p}}\, \alpha(K(V^{\gamma_j})) = 0 \quad .)$$

Thus there is a set of elements $B_j^* \varepsilon H^{*[pN]}$ $j \varepsilon I$, where

$$B_j^* = \sum_{\ell} \eta_{j,\ell}\, a_1^{*\,[f_{1,j,\ell}]} \otimes \cdots \otimes a_m^{*\,[f_{m,j,\ell}]}$$

and $\{B_j^*\}_{j\varepsilon I}$ is a dual basis to $\{\alpha(K(\sigma(V^{\gamma_j})))\}_{j\varepsilon I}$.

If $m^{pN-1}: H^* \otimes \cdots \otimes H^* \to H^*$ is usual multiplication then letting $b_j^* = m^{pN-1}(B_j^*)$ $j \varepsilon I$, $b_j^* \varepsilon J^{pN}$. $\{b_j^*\}$ is a dual basis to $\{\sigma(V^{\gamma_j})\}_{j\varepsilon I}$. Moreover by the form of $K(\sigma(V^{\gamma_j}))$ [each exponent is divisible by p] it follows for B_j^* that when $\eta_{j,\ell} \neq 0$ we can assume

$$p|f_{1,j,\ell} \ , \cdots \ p|f_{m,j,\ell}$$

so that $b_j^* \varepsilon \{a^{*p} | a^* \varepsilon J\}$. Thus any derivation vanishes on b_j^*.

$b_1^* * a_1^{*\,e_{1_1}} *\cdots* a_m^{*\,e_{1_m}} \varepsilon J^T$ so that

$$\langle b_1^* * a_1^{*\,e_{1_1}} *\cdots* a_m^{*\,e_{1_m}},\ m \circ i \otimes \sigma(X)\rangle =$$

$$\langle b_1^* * a_1^{*\,e_{1_1}} *\cdots* a_m^{*\,e_{1_m}},\ m \circ i \otimes \sigma\Big(\sum_{\substack{i \\ j\varepsilon I}} \lambda_{i,j} x_1^{\alpha_1^{e_{i_1}}} \cdots x_m^{\alpha_m^{e_{i_m}}} \otimes V^{\gamma_j}\Big)\rangle$$

$$= \sum_{\substack{i \\ j\in I}} \lambda_{i,j} \langle (b_1^* * a_1^{*e_{l_1}} *\cdots* a_m^{*e_{l_m}}) \cdot (x_{\alpha_1}^{e_{i_1}} \cdots x_{\alpha_m}^{e_{i_m}}), {}_V{}^{\gamma_j} \rangle$$

$$= e_{l_1}! \cdots e_{l_m}! \sum_{j\in I} \lambda_{i,j} \langle b_1^*, {}_V{}^{\gamma_j} \rangle =$$

$$e_{l_1}! \cdots e_{l_m}! \lambda_{1,1} \cdot$$

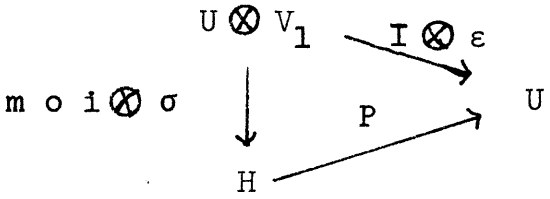
$0 \leq e_{l_k} < p \quad k = 1, \ldots m \quad \lambda_{1,1} \neq 0$ so

this contradicts $m \circ i \otimes \sigma(X) = 0$ and hence $m \circ i \otimes \sigma$ is injective.

Thus $U \otimes V_1 \xrightarrow{m \circ i \otimes \sigma} H$ is an isomorphism (of left U-modules). Then $I \otimes \varepsilon\colon U \otimes V_1 \to U$ a projection of left U-modules induces

$$P\colon H \to U$$

a projection of left U-modules. P is defined by commutivity of



$I \otimes \varepsilon(1 \otimes 1) = 1$. $m \circ i \otimes \sigma(1 \otimes 1) = 1$, hence, $P(1) = 1$ and since H is coconnected P is regular. Q.E.D.

This theorem establishes the difficult part of showing H is an extension of H/LH by U as an algebra and

coalgebra.

Coalgebra Extension

Assume U is commutative. Let $\psi: U \otimes H \to H$ $\psi = m \circ i \otimes I$. U is a Hopf algebra and H is a coalgebra, under ψ H is a left U-module as a coalgebra. Then sequence

$$U \otimes H \xrightarrow{\psi} H \xrightarrow{\pi} H/LH$$

is split exact by theorem 7.

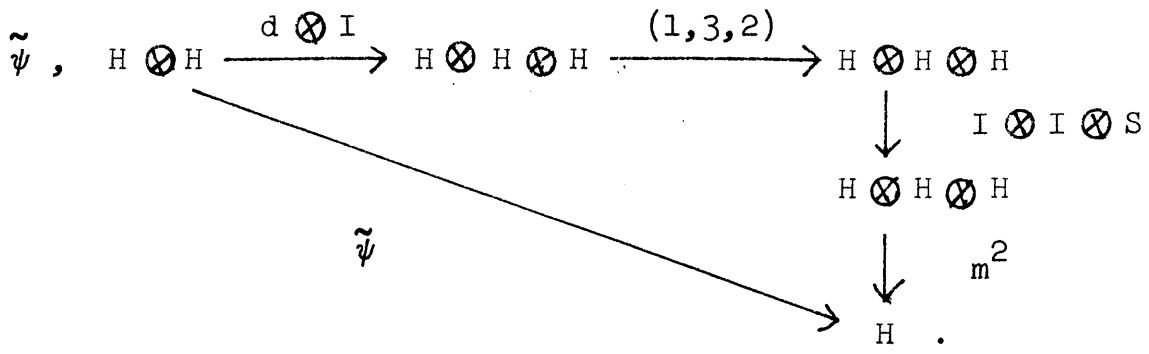
H/LH is a right C.H.A. U-comodule under $\phi: H/LH \to H/LH \otimes U$ $\phi = I \otimes k$. By cocommutivity

$$\begin{array}{ccccccc} H & \xrightarrow{d} & H \otimes H & \xrightarrow{I \otimes \pi} & H \otimes H/LH & \xrightarrow{(2,1)} & H/LH \otimes H \\ \downarrow{\scriptstyle d} & & & & & & \downarrow{\scriptstyle \phi \otimes I} \\ & & & & & & H/LH \otimes U \otimes H \\ & & & & & & \downarrow{\scriptstyle I \otimes \psi} \\ H \otimes H & & \xrightarrow[\pi \otimes I]{} & & & & H/LH \otimes H \end{array},$$

is commutative; hence, by definition H is an extension of H/LH by U as a coalgebra.

Algebra Extension

H is a left H-module under the adjoint representation



S denotes the antipode which exists because H is coconnected. We show $\tilde{\psi}$ defines a module structure.

$1, x, y, z \in H$

$$1 \cdot z = 1\ z\ S(1) = z\ .$$

$$x \cdot (y \cdot z) = \sum_i x_i'(y \cdot z)S(x_i'')$$

$$= \sum_{i,j} x_i'(y_j'(z)S(y_j''))S(x_i'')$$

$$= \sum_{i,j} x_i'y_j'\ z\ S(x_i''y_j'')$$

$$= \sum_i (xy)_i'\ z\ S(xy)_i''$$

$$= (xy) \cdot z\ .$$

We show H is a left H.A. H-module

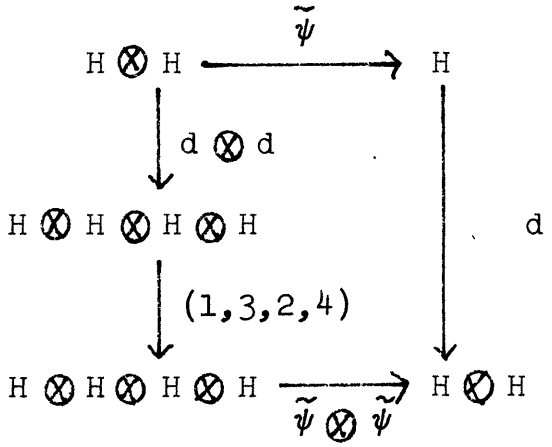
$$x \cdot 1 = \sum_i x_i'\ 1\ S(x_i'') = \varepsilon(x)\ .$$

$$x \cdot (yz) = \sum_i x_i'(yz)S(x_i'') = \sum_i x_i'\ y\ \varepsilon\ (x_i'')\ z\ S(x_i''')$$

$$= \sum_i x_i' y S(x_i'') x_i''' \; z \; S(x_i'''')$$

$$= \sum_i (x_i' \cdot y)(x_i'' \cdot z) \; .$$

$\tilde{\psi}$ also is a coalgebra morphism i.e.



is commutative.

$$d(x \cdot y) = d(\sum_i x_i' \; y \; S(x_i''))$$

$$= \sum_{i,j} x_i' y_j' \; S(x_i'''') \otimes x_i'' y_j'' \; S(x_i''')$$

$$= \sum_{i,j} x_i' y_j' \; S(x_i'') \otimes x_i''' \; y_j'' \; S(x_i'''')$$

$$= \tilde{\psi} \otimes \tilde{\psi} \circ (1,3,2,4) \circ d \otimes d(x \otimes y) \; .$$

This shows--by an easy induction-- $\#(x \cdot y) \leq \#(y)$. Hence $H \cdot L \subset H_1$. Since L generates U , $H_1 \subset U$ and H is a left H.A. H-module $H \cdot U \subset U$. Assume U is

commutative, if

$$x,y \in U \qquad x \cdot y = \sum_i x_i' \, y \, S(x_i'')$$

$$= \sum_i x_i' \, S(x_i'')y = \varepsilon(x)y \ .$$

Thus $U^+ \cdot U = 0$ and $(HU^+) \cdot U = 0$ since $HU^+ = HL = LH$, $\tilde{\psi}|H \otimes U$ factors to $\psi: H/LH \otimes U \to U$. Under ψ, U is a left H/LH-module and a left C.H.A. H/LH-module since under $\tilde{\psi}$ H is a left H.A. H-module. We show $\tilde{\psi}$ satisfies

$$\begin{array}{ccccc} H \otimes H & \xrightarrow{d \otimes I} & H \otimes H \otimes H & \xrightarrow{(1,3,2)} & H \otimes H \otimes H \\ \downarrow{\scriptstyle m} & & & & \downarrow{\scriptstyle \tilde{\psi} \otimes I} \\ H & & \xrightarrow{\qquad m \qquad} & & H \otimes H \end{array} \ .$$

$$xy = \sum_i x_i' \, y \, \varepsilon(x_i'') = \sum_i x_i' \, y \, S(x_i'')x_i'''$$

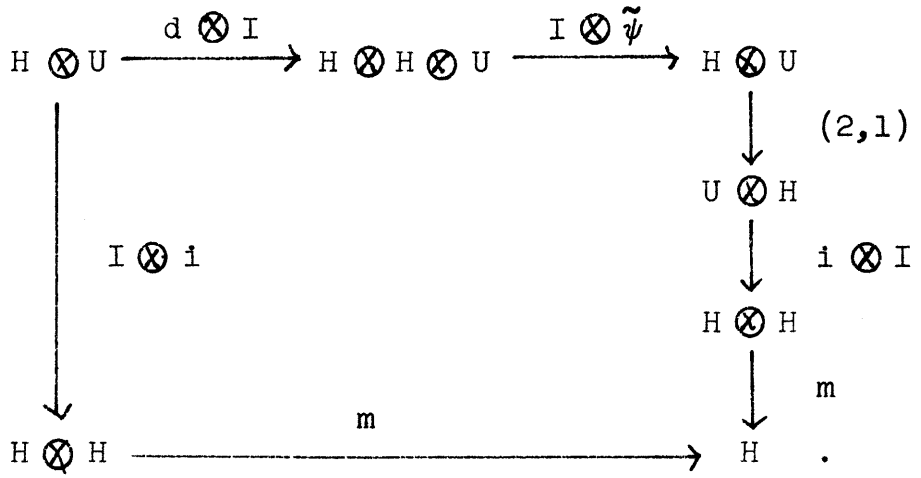
$$= \sum_i (x_i' \cdot y)x_i'' \ .$$

If H is an H/LH-comodule by

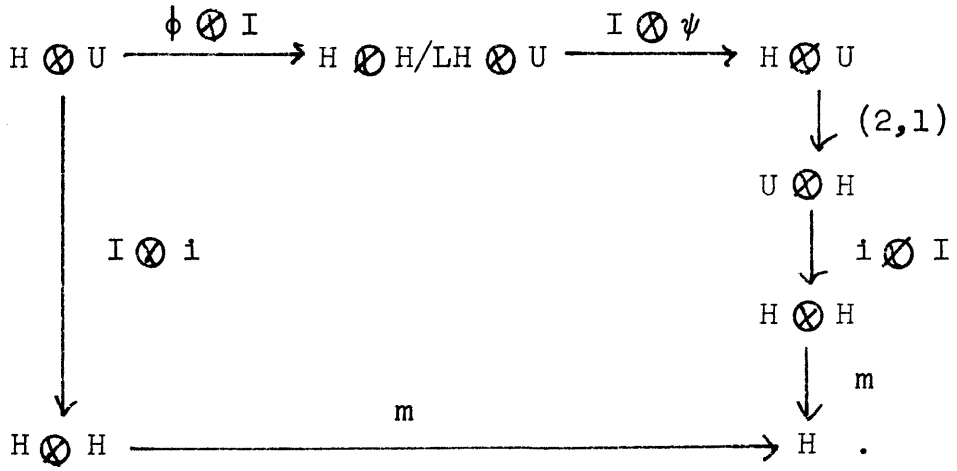
$$\phi: H \xrightarrow{d} H \otimes H \xrightarrow{I \otimes \pi} H \otimes H/LH$$

then ϕ is clearly an algebra morphism so H is a right H/LH-comodule <u>as an algebra</u>. From the above diagram and

cocommutivity we have the commutative diagram:

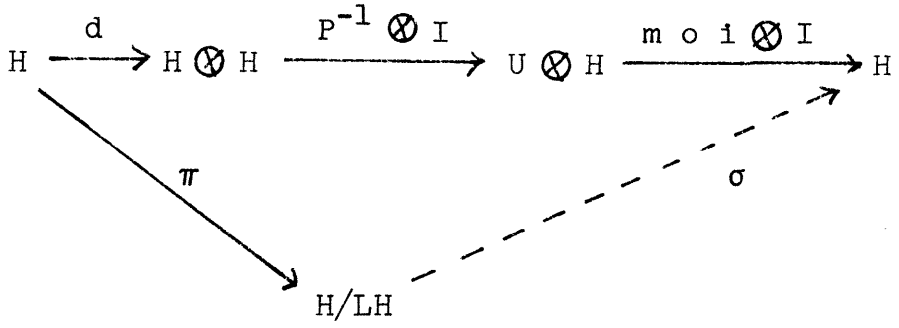


Using $\phi = I \otimes \pi \circ d$ and the definition of ψ we have the commutative diagram:



Thus the second condition for H to be an extension of H/LH by U --as an algebra--is satisfied.

By theorem 2) σ: $H/LH \to H$ defined by



is a morphism of right H/LH-comodules. (P is as in theorem 7.) It is invertible because H/LH is coconnected. ($\underline{H/LH} \tilde{=} V_1$) . Moreover by theorem 2)

$$U \otimes H/LH \xrightarrow{i \otimes \sigma} H \otimes H \xrightarrow{m} H$$

is a linear isomorphism. Observe $U \subset H \square^{H/LH} k$. By theorem 1

$$(H \square^{H/LH} k) \otimes H/LH \xrightarrow{i \otimes \sigma} H \otimes H \xrightarrow{m} H$$

is a linear isomorphism. Hence, $U = H \square^{H/LH} k$, and

$$U \xrightarrow{i} H \xrightarrow{\phi} H \otimes H/LH$$

is a split exact sequence. This verifies the first condition for H to be an extension of H/LH by U .

Bibliography

[1] E. Artin, C. Nesbitt, and R. Thrall, Rings with Minimum Condition, University of Michigan Press, 1944.

[2] N. Jacobson, Lie Algebras, Interscience, 1962.

[3] J. Milnor and J. Moore, On the Structure of Hopf Algebras, Princeton University Notes.

Index

Adjoint representation, 155

Algebra, 8

$\underline{A}$, 111

commutative, 8

Antipode, 17

Augmentation, 10, 11

Brauer Group, 80

Coalgebra, 10

$\underline{C}$, 111

cocommutative, 11

Coconnected, 93

Cohomology, 47, 87

δ^n, 48

δ_n, 88

$H(B,H)^i$, 88

$H^i(H,B)$, 56

$Hom(C,A)^n$, 88

$Hom^n(C,A)$, 48

normal complex, 58

$Reg(C,A)^n$, 88

$Reg^n(C,A)$, 48

Coideal, 43

Comodule, 12

(C.)H.A. comodule, 87

comodule as an algebra, 36

ϕ^2, structure on $X \otimes X$, 36

Connected, 143

Divided power, 122

Duality, 14

Extension, 61, 62, 89, 90, 155

$B \overset{f}{\otimes} H$, 67

Brauer Group, 80

$H \underset{g}{\otimes} B$, 91

isomorphism of extensions, 62, 90

left exact sequence, 61

product of extensions, 81

right exact sequence, 89

smash product, 63

split exact sequence, 61, 89

Filtration, 26

$\Gamma(G)$, 17

Grouplike element, 24

Hopf algebra, 16

coconnected, 93

conilpotent, 22

filtration, 26

G(H), 24

H^g, 25

L(H), 94

split, 21

U , 95

J , 26

K(x), 98

L_i, 121

Module, 9

(C.)H.A. module, 48

H as H*, 21

module as a coalgebra, 43

$\mathfrak{S}_n$-module, 7

ψ^2, structure on $X \otimes X$, 42

Poincaré-Birkhoff-Witt theorem, 140

Primitive element, 94

ρ , 113

Restricted Universal Enveloping Algebra, 93, 95

Smash product, 63

$H^e \otimes T(G) \xrightarrow{m} H$, 66

Symmetric tensor, 97

Universal Enveloping Algebra, 93, 95

Unit, 8, 13

V , 115

V_i , 119

Vector space, 7

$\underline{X}$, 110

Biography

Moss Eisenberg Sweedler was born in Brooklyn, New York, April 29, 1942. He was graduated from the Massachusetts Institute of Technology with a B.S. in June 1963. He continued study there as a graduate student.