HOPF GALOIS EXTENSIONS

by

Nursel Erey

B.S., Mathematics, Boğaziçi University, 2009

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics
Boğaziçi University
2011

To me!

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor, Müge Kanuni, for her support and encouragement during my studies.

My sincere thanks are due to Atabey Kaygun for his valuable suggestions during the finalization of this text.

I thank Arzu Boysal for participating in my thesis committee.

I acknowledge TÜBİTAK for providing me with graduate scholarship.

I am indebted to my parents for all their love and encouragement.

Finally and above all, thanks to my sister Aysel Erey. Her presence makes everything easier.

ABSTRACT

HOPF GALOIS EXTENSIONS

Let H be a Hopf algebra which coacts to the right on A and let B be the subalgebra of coinvariants. The extension $B \subset A$ is said to be Hopf Galois if the canonical map $\beta : A \otimes_B A \to A \otimes H$ is a bijection. This work investigates this kind of extension for special coactions.

ÖZET

HOPF GALOIS GENİŞLEMELERİ

Hopf Galois genişlemesi, A cebiri üzerine sağdan eşetkiyen bir Hopf cebiri H'nin olduğu durum için tanımlanır. Eğer B, bu eşetkimede A'nın eşdeğişmezlerinin oluşturduğu alt cebiri gösterirse, $B \subset A$ genişlemesinin Hopf Galois olması, doğal

$$\beta : A \otimes_B A \to A \otimes H$$

fonksiyonunun birebir ve örten olması olarak tanımlanır. Bu tezde çeşitli eşetkimeler için Hopf Galois genişlemeleri incelenmiştir.

TABLE OF CONTENTS

LIST OF SYMBOLS

$\cdot_{ad_l}$	Left adjoint action
A^{op}	The opposite algebra of A
$A\#_\sigma H$	Crossed product of A with H
$a \rightharpoonup f$	The transpose of left multiplication by a
C^{cop}	The opposite coalgebra of C
$c \leftharpoonup f$	c is hit by f from right
$f \leftharpoonup a$	The transpose of right multiplication by a
$f \rightharpoonup c$	c is hit by f from left
$f * g$	Convolution product of f and g
$[F : K]$	Degree of F over K
$Gal(E/F)$	The Galois group of the extension E/F
$Hom_R(A, B)$	The set of R linear maps from A to B
H^*	Dual space of H
$Im(f)$	Image of f
$\int_H^l$	The space of left integrals in H
$\int_H^r$	The space of right integrals in H
k	A field
$Ker(f)$	Kernel of f
${}_A\mathcal{M}$	The category of left A-modules
$\mathcal{M}_A$	The category of right A-modules
${}^C\mathcal{M}$	The category of left C-comodules
$\mathcal{M}^C$	The category of right C-comodules
M^{coH}	Coinvariant subspace of M
M^H	Invariant subspace of M
$\mathcal{M}_H^H$	The category of right H-Hopf modules
R	An associative commutative ring with identity
T^*	The map induced by T
$\delta_{i,j}$	Kronecker delta function

τ	Twist map
$\otimes$	Tensor product

1. INTRODUCTION

The definition of Hopf Galois extensions for commutative algebras is due to Chase and Sweedler [1]. The general definition was introduced by Kreimer and Takeuchi [2] in 1981. Hopf Galois extensions generalize classical Galois extensions of fields, strongly graded algebras and crossed products.

There are many examples of Hopf Galois extensions in noncommutative geometry and quantum group theory. Every quantum principal bundle with a compact structure group is a Hopf Galois extension [3]. If the Hopf algebra H has a bijective antipode then faithfully flat H-Galois extensions have a geometric interpretation [4]. In this case, it is possible to prove some results on affine quotients without using the theory of affine groups. Moreover, the study of Hopf Galois extensions enables understanding of the structure of Hopf algebras themselves. [2] and [4] give characterizations of certain extensions that give rise to the equivalence of the relative Hopf module categories.

In the first two chapters of this thesis, we give the basic concepts of the theory of Hopf algebras. Chapter 4 includes the necessary background to define (co)actions. We give key theorems on integrals and Hopf modules. Chapter 5 is devoted to examples of Hopf Galois extensions with an emphasis on crossed products.

2. ALGEBRAS AND COALGEBRAS

We refer to [5] and [6] for this chapter.

2.1. Algebras

Throughout this section, unless otherwise stated, we will assume that R is an associative commutative ring with unit.

Definition 2.1. *An R-module A with two R-linear maps μ and u is called an R-*algebra *provided that the R-linear maps $\mu : A \otimes_R A \longrightarrow A$ and $u : R \longrightarrow A$ make the following diagrams commutative.*

$$\begin{tikzcd}
R \otimes_R A \arrow[r, "u \otimes I_A"] \arrow[dr, "\simeq"'] & A \otimes_R A \arrow[d, "\mu"] & A \otimes_R R \arrow[l, "I_A \otimes u"'] \arrow[dl, "\simeq"] \\
 & A &
\end{tikzcd}$$

and

$$\begin{tikzcd}
A \otimes_R A \otimes_R A \arrow[r, "I_A \otimes \mu"] \arrow[d, "\mu \otimes I_A"'] & A \otimes_R A \arrow[d, "\mu"] \\
A \otimes_R A \arrow[r, "\mu"] & A
\end{tikzcd}$$

The R-linear maps μ and u are respectively called multiplication and unit map of the algebra. We will simply write ab instead of $\mu(a \otimes b)$. With this notation, second diagram corresponds to usual associativity. Also, first diagram implies that for any element a

$$u(1)a = \mu \circ (u \otimes I_A)(1 \otimes a) = \simeq \circ(1 \otimes a) = a \text{ and}$$
$$au(1) = \mu \circ (I_A \otimes u)(a \otimes 1) = \simeq \circ(a \otimes 1) = a$$

which means that $u(1)$ is the multiplicative identity in the algebra. Then, the unit map of an algebra with identity 1_A is determined as $u(r) = u(r \cdot 1) = r \cdot u(1) = r \cdot 1_A$ where the second equality follows from the R-linearity of u. Also, if the R-module A is endowed with an R-linear associative multiplication and it has a unit element 1_A, then there exists an R-linear map $u : R \to A$ such that the first diagram commutes. Namely, $u(r) := r \cdot 1_A$ makes the diagram commutative. Thus an equivalent definition of an R-algebra includes associative multiplication and unit element.

Remark 2.2. *When the ring R is commutative, tensor products $N \otimes_R M$ and $M \otimes_R N$ are isomorphic and the twist map, $\tau : N \otimes_R M \to M \otimes_R N$ given by $\tau(n \otimes m) = m \otimes n$ is an isomorphism.*

Definition 2.3. *An R-algebra A is* commutative *if $ab = ba$ for all $a, b \in A$. Diagrammatically, this corresponds to commutativity of the following:*

$$\begin{tikzcd}
A \otimes_R A \arrow[rr, "\tau"] \arrow[dr, "\mu"'] & & A \otimes_R A \arrow[dl, "\mu"] \\
& A &
\end{tikzcd}$$

Example 2.4. *(The Group Algebra)The group algebra kG is a k-vector space whose basis consists of the elements of a group G. Thus, every element of kG is a finite sum $\sum_{g \in G} \alpha_g g$ where α_g is a family of elements in k. The multiplication is given by $(\alpha g)(\beta h) = (\alpha\beta)gh$ for $\alpha, \beta \in k$ and $g, h \in G$ and, it is extended linearly. Hence for arbitrary elements multiplication is defined as*

$$\Big(\sum_i \alpha_i g_i\Big)\Big(\sum_i \beta_i g_i\Big) = \sum\big(\sum_{\substack{i,j \\ g_i g_j = g_k}} \alpha_i \beta_j\big) g_k$$

The multiplication is associative on basis elements hence it is associative on arbitrary elements since the extension is linear and clearly unit element is $1_k 1_G$.

Example 2.5. *Tensor product, $A \otimes_R B$, of two R-algebras A and B is again an R-algebra. The multiplication map $\mu_{A \otimes_R B}$, in this case is $(\mu_A \otimes \mu_B)(I_A \otimes tw \otimes I_B)$. In simple notation, $(a \otimes b)(c \otimes d) = ac \otimes bd$ for every $(a \otimes b), (c \otimes d) \in A \otimes_R B$. The unit element in $A \otimes_R B$ is $1_A \otimes 1_B$.*

Definition 2.6. *Let A and B be two R-algebras. An R-linear map $f : A \to B$ is called an* algebra morphism *if $f(aa^{'}) = f(a)f(a^{'})$ for every a,$a^{'} \in A$ and $f(1_A) = 1_B$. The first condition corresponds to commutativity of the following diagram*

$$\begin{tikzcd}
A \otimes_R A \arrow[r, "\mu_A"] \arrow[d, "f \otimes f"'] & A \arrow[d, "f"] \\
B \otimes_R B \arrow[r, "\mu_B"'] & B
\end{tikzcd}$$

Also, $f(1_A) = 1_B$ if and only if $f(r1_A) = rf(1_A)$ for every $r \in R$ by linearity of f. But this is equivalent to commutativity of the following

$$\begin{tikzcd}
R \arrow[r, "="] \arrow[d, "u_A"'] & R \arrow[d, "u_B"] \\
A \arrow[r, "f"'] & B
\end{tikzcd}$$

2.2. Coalgebras

Definition 2.7. *An R-*coalgebra *is an R-module C with R-linear maps $\Delta : C \to C \otimes C$ and $\varepsilon : C \to R$ called coproduct and counit respectively which satisfy the equalities $(I_C \otimes \Delta)\Delta = (\Delta \otimes I_C)\Delta$ (coassociativity) and $(I_C \otimes \varepsilon)\Delta = I_C = (\varepsilon \otimes I_C)\Delta$(counit property). These properties correspond to commutativity of*

$$\begin{tikzcd}
C \otimes_R C \otimes_R C & C \otimes_R C \arrow[l, "I_C \otimes \Delta"'] \\
C \otimes_R C \arrow[u, "\Delta \otimes I_C"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}$$

and

$$\begin{tikzcd}
R \otimes_R C & C \arrow[l, "\simeq"'] \arrow[r, "\simeq"] \arrow[d, "\Delta"'] & C \otimes_R R \\
 & C \otimes_R C \arrow[ul, "\varepsilon \otimes I_C"] \arrow[ur, "I_C \otimes \varepsilon"'] &
\end{tikzcd}$$

Example 2.8. *Any k-vector space C has a k-coalgebra structure with comultiplication and counit maps $\Delta(c) = c \otimes c$, $\varepsilon(c) = 1$ defined on the basis elements and extended linearly. In particular, k is a k-coalgebra and $\Delta(a) = a \otimes 1$ for any $a \in k$ since the extension is linear.*

Example 2.9. *The tensor product $C \otimes_R D$ of two R-coalgebras C and D has a canonical coalgebra structure. Its comultiplication map $\Delta_{C\otimes D}$ is the composition*

$$(I \otimes \tau \otimes I)(\Delta \otimes \Delta) : C \otimes_R D \to (C \otimes_R D) \otimes_R (C \otimes D)$$

given by $c \otimes d \mapsto \sum (c_1 \otimes d_1) \otimes (c_2 \otimes d_2)$. Also the counit map $\varepsilon_{C\otimes D}$ is the tensor product $\varepsilon_C \otimes \varepsilon_D$ of counit maps. From now on, we will always consider this coalgebra structure on tensor products of coalgebras unless otherwise stated.

Definition 2.10. *A coalgebra (C, Δ, ε) is said to be* cocommutative *if $\Delta = \tau \circ \Delta$, in other words if the following diagram commutes*

$$\begin{tikzcd}
C \otimes_R C \arrow[rr, "\tau"] & & C \otimes_R C \\
& C \arrow[ul, "\Delta"] \arrow[ur, "\Delta"'] &
\end{tikzcd}$$

Definition 2.11. *An R-linear map $f : C \to C'$ between two R-coalgebras C and C' is called a* coalgebra morphism *if the diagrams below commute.*

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\Delta"'] & C' \arrow[d, "\Delta'"] \\
C \otimes_R C \arrow[r, "f\otimes f"'] & C' \otimes_R C'
\end{tikzcd}$$

$$\begin{tikzcd}
C \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & C' \arrow[dl, "\varepsilon'"] \\
& R &
\end{tikzcd}$$

Remark 2.12. *If $f : A \to B, f' : B \to C, g : D \to E$ and $g' : E \to F$ are morphisms* *of modules then for the tensor product of morphisms the equality of compositions*

$$(f^{'} \otimes g^{'})(f \otimes g) = (f^{'} f \otimes g^{'} g)$$

holds.

Sweedler's Notation 2.13. *Let* (C, Δ, ε) *be a coalgebra. For every element* $c \in C$, $\Delta(c) = \sum_{i=1}^{k} c_i \otimes \overline{c_i}$ *is a finite sum of generators in* $C \otimes_R C$. *We write* $\Delta(c) = \sum c_1 \otimes c_2$, *where* c_1 *stands for the family of elements* $c_1, c_2, ..., c_k$ *and* c_2 *stands for the family of elements* $\overline{c_1}, \overline{c_2}, ..., \overline{c_k}$.

Using Sweedler's notation, counit property can be expressed by the equation $\sum \varepsilon(c_1)c_2 = c = \sum c_1 \varepsilon(c_2)$ and, coassociativity means that

$$\sum c_1 \otimes c_{21} \otimes c_{22} = \sum c_{11} \otimes c_{12} \otimes c_2.$$

Also, a coalgebra is cocommutative if $\sum c_1 \otimes c_2 = \sum c_2 \otimes c_1$ for every c in coalgebra. Now we define recurrently the function $\Delta_n = (\Delta \otimes I^{n-1})\Delta_{n-1}$ for $n \geq 2$. Let $\sum c_1 \otimes c_2 \otimes ... \otimes c_n$ denote the value of $\Delta_{n-1}(c)$. Note then that

$$\sum c_1 \otimes c_2 \otimes c_3 = \sum c_1 \otimes c_{21} \otimes c_{22} = \sum c_{11} \otimes c_{12} \otimes c_2.$$

Proposition 2.14. $Hom_R(C, A)$ *is an algebra for any* R*-coalgebra* (C, Δ, ε) *and* R*-algebra* (A, μ, u) *with unit* $u\varepsilon$ *and the convolution product given by*

$$f * g = \mu(f \otimes g)\Delta$$

Proof. To prove the associativity of convolution we take $c \in C$ and use the associativity and coassociativity of A and C respectively as follows:

$$\begin{aligned}(f*(g*h))(c) &= \sum (f(c_1))((g*h)(c_2)) \\ &= \sum (f(c_1))(g(c_{21})h(c_{22})) \\ &= \sum (f(c_{11}))(g(c_{12})h(c_2)) \\ &= \sum (f(c_{11})g(c_{12}))(h(c_2)) \\ &= \sum (f*g)(c_1)h(c_2) \\ &= ((f*g)*h)(c)\end{aligned}$$

Also unit element in $Hom_R(C, A)$ is $u\varepsilon$ since

$$\begin{aligned}(f*u\varepsilon)(c) &= \sum f(c_1)\varepsilon(c_2) \\ &= \sum f(c_1)\varepsilon(c_2)1_A \\ &= \sum f(c_1\varepsilon(c_2)) \\ &= f(c)\end{aligned}$$

Similarly $u\varepsilon * f = f$. □

Corollary 2.15. *The dual $C^* = Hom_R(C, R)$ of any coalgebra C is an algebra with convolution product and unit element ε.*

Definition 2.16. *Given an R-algebra (A, μ, u), the map $\mu\tau : A \otimes A \to A$ defines a new algebra on the R-module A. This algebra is called the* opposite algebra *of A and denoted by A^{op}. Similarly, any coalgebra (C, Δ, ε) has an* opposite coalgebra *structure with comultiplication map $\tau\Delta$ and, the same counit map ε. The opposite coalgebra is denoted by C^{cop}. It is clear then that an (co)algebra is (co)commutative if and only if its opposite (co)algebra is (co)commutative.*

Lemma 2.17. *Let (C, Δ, ε) be a coalgebra. The generalized coassociativity*

$$\Delta_n = (I^p \otimes \Delta \otimes I^{n-1-p})\Delta_{n-1}$$

holds for any $n \geq 2$ and $p \in \{0, ..., n-1\}$.

Proof. We will give a proof by induction on n. Since the basis step is clear by coassociativity , let us assume that the equality is satisfied for some $n \geq 2$ and all $p \in \{0, ..., n-1\}$. We pick $p \in \{0, ..., n\}$ and using inductive hypothesis for $p-1$, we write

$$\begin{aligned}
(I^p \otimes \Delta \otimes I^{n-p})\Delta_n &= (I^p \otimes \Delta \otimes I^{n-p})(I^{p-1} \otimes \Delta \otimes I^{n-p})\Delta_{n-1} \\
&= (I^{p-1} \otimes (I \otimes \Delta) \otimes I^{n-p})(I^{p-1} \otimes \Delta \otimes I^{n-p})\Delta_{n-1} \\
&= (I^{p-1} \otimes (I \otimes \Delta)\Delta \otimes I^{n-p})\Delta_{n-1} \\
&= (I^{p-1} \otimes (\Delta \otimes I)\Delta \otimes I^{n-p})\Delta_{n-1} \\
&= (I^{p-1} \otimes \Delta \otimes I^{n-p+1})(I^{p-1} \otimes \Delta \otimes I^{n-p})\Delta_{n-1} \\
&= (I^{p-1} \otimes \Delta \otimes I^{n-p+1})\Delta_n
\end{aligned}$$

The same argument now can be repeated by using the inductive hypothesis for $p-2$. That is, using $\Delta_n = (I^{p-2} \otimes \Delta \otimes I^{n-p+1})\Delta_{n-1}$ we get

$$(I^p \otimes \Delta \otimes I^{n-p})\Delta_n = (I^{p-2} \otimes \Delta \otimes I^{n-p+2})\Delta_n.$$

In fact, continuing this way we can obtain

$$\begin{aligned}
(I^p \otimes \Delta \otimes I^{n-p})\Delta_n &= (I^{p-1} \otimes \Delta \otimes I^{n-p+1})\Delta_n \\
&= (I^{p-2} \otimes \Delta \otimes I^{n-p+2})\Delta_n \\
&\;\vdots \\
&= (\Delta \otimes I^n)\Delta_n \\
&= \Delta_{n+1}
\end{aligned}$$

□

Lemma 2.18. *In a coalgebra (C, Δ, ε) the following rules are valid.*

(i) For $i \geq 2$, $\Delta_i = (\Delta_{i-1} \otimes I)\Delta$

(ii) For any $n \geq 2$, $i \in \{1, ..., n-1\}$ and $m \in \{0, ..., n-i\}$

$$\Delta_n = (I^m \otimes \Delta_i \otimes I^{n-i-m})\Delta_{n-i}$$

Proof. (i) We proceed by induction on i. For $i = 2$, the equality reduces to definition. Suppose that $\Delta_i = (\Delta_{i-1} \otimes I)\Delta$ for some $i \geq 2$. Then we see that

$$\begin{aligned}
\Delta_{i+1} &= (\Delta \otimes I^i)\Delta_i \\
&= (\Delta \otimes I^i)(\Delta_{i-1} \otimes I)\Delta \\
&= (\Delta \otimes I^{i-1} \otimes I)(\Delta_{i-1} \otimes I)\Delta \\
&= ((\Delta \otimes I^{i-1})\Delta_{i-1} \otimes I)\Delta \\
&= (\Delta_i \otimes I)\Delta
\end{aligned}$$

(ii) Let $n \geq 2$ be fixed. To prove the desired result by induction on i we first observe that the basis step is generalized coassociativity. We assume that the equality $\Delta_n = (I^m \otimes \Delta_{i-1} \otimes I^{n-i+1-m})\Delta_{n-i+1}$ holds for some $i-1$ where $i \geq 2$ and m is an arbitrary element in $\{0, ..., n-i+1\}$. So if we choose $m \in \{0, ..., n-i\}$ we can use inductive hypothesis since $\{0, ..., n-i\} \subseteq \{0, ..., n-i+1\}$. Hence we get

$$\begin{aligned}
\Delta_n &= (I^m \otimes \Delta_{i-1} \otimes I^{n-i+1-m})\Delta_{n-i+1} \\
&= (I^m \otimes \Delta_{i-1} \otimes I^{n-i-m+1})(I^m \otimes \Delta \otimes I^{n-i-m})\Delta_{n-i} \\
&= (I^m \otimes \Delta_{i-1} \otimes I \otimes I^{n-i-m})(I^m \otimes \Delta \otimes I^{n-i-m})\Delta_{n-i} \\
&= (I^m \otimes (\Delta_{i-1} \otimes I)\Delta \otimes I^{n-i-m})\Delta_{n-i} \\
&= (I^m \otimes \Delta_i \otimes I^{n-i-m})\Delta_{n-i}
\end{aligned}$$

where the first line is by inductive hypothesis, second line is by generalized coassociativity and the last line follows by part (i). □

Theorem 2.19 (Computation Rule)**.** *In a coalgebra (C, Δ, ε), we can replace the series $\sum c_1 \otimes c_2 \otimes ... \otimes c_{i-1} \otimes c_i \otimes c_{i+1} \otimes ... \otimes c_{i+k} \otimes c_{i+k+1} \otimes ... \otimes c_{i+k+m}$ by the series $\sum c_1 \otimes c_2 \otimes ... \otimes c_{i-1} \otimes \Delta_k(c_i) \otimes c_{i+1} \otimes ... \otimes c_{i+m}$ where $i, k, m \geq 1$.*

Proof.

$$\begin{aligned}\sum c_1 \otimes c_2 \otimes ... \otimes c_{i+k+m} &= \Delta_{i+k+m-1}(c)\\ &= (I^{i-1} \otimes \Delta_k \otimes I^m)\Delta_{i+m-1}(c)\\ &= (I^{i-1} \otimes \Delta_k \otimes I^m)(\sum c_1 \otimes c_2 \otimes ... \otimes c_{i+m})\\ &= \sum c_1 \otimes ... \otimes \Delta_k(c_i) \otimes ... \otimes c_{i+m}\end{aligned}$$

where we used part (ii) of Lemma 2.18 in the second line. $\square$

3. HOPF ALGEBRAS

Our main references for this chapter are [6], [7] and [8].

3.1. Hopf Algebras and Antipodes

Definition 3.1. *A* bialgebra B *is a* k*-vector space which has both an algebra structure* (B, μ, u) *and a coalgebra structure* (B, Δ, ε) *such that* Δ *and* ε *are algebra morphisms or equivalently* μ *and* u *are coalgebra morphisms. Note that in this case* Δ *is an algebra morphism means that the following diagrams commute.*

$$\begin{tikzcd}
B \otimes B \arrow[rr, "\mu"] \arrow[d, "\Delta\otimes\Delta"'] & & B \arrow[dd, "\Delta"] \\
(B \otimes B) \otimes (B \otimes B) \arrow[d, "I_B\otimes tw\otimes I_B"'] & & \\
(B \otimes B) \otimes (B \otimes B) \arrow[rr, "\mu\otimes\mu"] & & (B \otimes B)
\end{tikzcd}$$

$$\begin{tikzcd}
R \arrow[r, "u"] \arrow[d, "\simeq"'] & B \arrow[d, "\Delta"] \\
R \otimes R \arrow[r, "u\otimes u"'] & B \otimes B
\end{tikzcd}$$

Also ε *is an algebra morphism if*

$$\begin{tikzcd}
B \otimes B \arrow[r, "\mu"] \arrow[d, "\varepsilon\otimes\varepsilon"'] & B \arrow[d, "\varepsilon"] \\
R \otimes R \arrow[r, "\simeq"'] & R
\end{tikzcd}$$

and

$$\begin{tikzcd} & B \arrow[dr, "\varepsilon"] & \\ R \arrow[ur, "u"] \arrow[rr, "="'] & & R \end{tikzcd}$$

commute.

In any bialgebra B, the followings are now immediate from the diagrams above.

- $\Delta(1_B) = 1_B \otimes 1_B$
- $\Delta(ab) = \Delta(a)\Delta(b) = \sum a_1 b_1 \otimes a_2 b_2$
- $\varepsilon(1_B) = 1_R$
- $\varepsilon(ab) = \varepsilon(a)\varepsilon(b)$

Remark 3.2. *If B is a bialgebra, then $B^{op}, B^{cop}, B^{opcop}$ are all bialgebras.*

Definition 3.3. *Given a bialgebra H, let H^C and H^A denote the underlying coalgebra and algebra of H respectively. An* antipode *S of H is a linear map in $Hom(H^C, H^A)$ which is inverse to I_H with respect to the convolution product. In Sweedler's notation*

$$\sum S(h_1)h_2 = \sum h_1 S(h_2) = u\varepsilon(h)$$

for any $h \in H$. If the bialgebra H has an antipode, then it is called a Hopf algebra.

Definition 3.4. *A* bialgebra morphism *$f : B \to B'$ is an R-linear map which is both an algebra and coalgebra morphism. If B is a Hopf algebra, then f is said to be a* Hopf algebra morphism.

Proposition 3.5. *Let $f : H \to B$ be a Hopf algebra morphism between two Hopf algebras H and B. If S_B and S_H are antipodes of B and H, then $S_B f = f S_H$. In other words, morphisms of Hopf algebras preserve the antipodes.*

Proof. We will show that $S_B f$ is a left inverse of f and $f S_H$ is a right inverse of f with respect to the convolution product in $Hom(H^C, B^A)$. Then we will conclude that

$S_B f = f S_H$ since in any ring (in particular in any algebra), right and left inverses are the same if they exist.
Since f is morphism of coalgebras we have $(f \otimes f)\Delta_H = \Delta_B f$ and $\varepsilon_B f = \varepsilon_H$. Making use of these equalities we see that

$$\begin{aligned} S_B f * f &= \mu_B(S_B f \otimes f)\Delta_H \\ &= \mu_B(S_B \otimes I_B)(f \otimes f)\Delta_H \\ &= \mu_B(S_B \otimes I_B)\Delta_B f \\ &= (S_B * I_B)f \\ &= u_B \varepsilon_B f \\ &= u_B \varepsilon_H \\ &= I_{Hom(H^C, B^A)} \end{aligned}$$

Also, since f is a morphism of algebras we have $\mu_B(f \otimes f) = f \mu_H$ and $f u_H \varepsilon_H = u_B \varepsilon_H$. Similar to above, these lead to the equality $f * f S_H = I_{Hom(H^C, B^A)}$, completing the proof. $\square$

Some basic properties of the antipode are given in the following proposition.

Proposition 3.6. *Let H be a Hopf algebra with antipode S. Then:*

(i) S is an antimorphism of algebras, i.e.

$$S(hg) = S(g)S(h) \textit{ for any } g, h \in H \textit{ and } S(1_H) = 1_H$$

(ii) S is an antimorphism of coalgebras, i.e.

$$\Delta(S(h)) = \sum S(h_2) \otimes S(h_1) \textit{ and } \varepsilon(S(h)) = \varepsilon(h) \textit{ for any } h \in H.$$

Proof. (i) We consider the algebra structure on $Hom_k(H \otimes H, H)$ as in Proposition 2.14. We define the k-linear maps $F, G : H \otimes H \to H$ as $F(h \otimes g) = S(g)S(h)$

and $G(h \otimes g) = S(hg)$. We claim that μ is a left inverse for F and a right inverse for G with respect to convolution. Once the claim is proved, the desired equality $S(hg) = S(g)S(h)$ follows by uniqueness of inverses in algebras. To this end, let $a, b \in H$. Then we have

$$\begin{aligned}
(\mu * F)(a \otimes b) &= \sum \mu((a \otimes b)_1)F((a \otimes b)_2) \\
&= \sum \mu(a_1 \otimes b_1)F(a_2 \otimes b_2) \\
&= \sum a_1 b_1 S(b_2)S(a_2) \\
&= \sum a_1 \varepsilon(b) 1_H S(a_2) \\
&= \varepsilon(a)\varepsilon(b)1_H \\
&= u\varepsilon_{H\otimes H}(a \otimes b)
\end{aligned}$$

And similarly we have,

$$\begin{aligned}
(G * \mu)(a \otimes b) &= \sum G((a \otimes b)_1)\mu((a \otimes b)_2) \\
&= \sum G(a_1 \otimes b_1)\mu(a_2 \otimes b_2) \\
&= \sum S(a_1 b_1)a_2 b_2 \\
&= \sum S((ab)_1)(ab)_2 \\
&= \varepsilon(ab)1_H \\
&= u\varepsilon_{H\otimes H}(a \otimes b)
\end{aligned}$$

Note that we replaced above $\sum a_1 b_1 \otimes a_2 b_2$ by $\sum (ab)_1 \otimes (ab)_2$ using that H is a bialgebra. Also we have $S(1_H) = 1_H S(1_H) = (I * S)(1_H) = u\varepsilon(1_H) = 1_H$ since $\Delta(1_H) = 1_H \otimes 1_H$.

(ii) For this part, we consider the algebra $Hom_k(H, H \otimes H)$ and define the maps $F := \tau(S \otimes S)\Delta$ and $G := \Delta S$. As similar to part (i), we will show that Δ is a right inverse of G and left inverse of F. We see that,

$$\begin{aligned} G * \Delta = \Delta S * \Delta &= \mu_{H\otimes H}(\Delta S \otimes \Delta)\Delta \\ &= (\mu \otimes \mu)(I \otimes \tau \otimes I)(\Delta S \otimes \Delta)\Delta \\ &= (\mu \otimes \mu)(I \otimes \tau \otimes I)(\Delta \otimes \Delta)(S \otimes I)\Delta \\ &= \Delta\mu(S \otimes I)\Delta \\ &= \Delta u \varepsilon \\ &= (u \otimes u) \simeq \varepsilon \\ &= u_{H\otimes H}\varepsilon_H \end{aligned}$$

where $\simeq : k \to k \otimes k$ is the natural isomorphism. Mimicking this proof, it is easy to see that $\Delta * F = u_{H\otimes H}\varepsilon$ whence $G = F$ follows. Also for any $h \in H$ we have $\varepsilon S(h) = \sum \varepsilon S(\varepsilon(h_1)h_2) = \sum \varepsilon(h_1)\varepsilon(S(h_2))$ since both ε and S are linear. We make use of ε being a morphism of algebras to get

$$\sum \varepsilon(h_1)\varepsilon(S(h_2)) = \sum \varepsilon(h_1 S(h_2)) = \varepsilon(\varepsilon(h)1_H) = \varepsilon(h)\varepsilon(1_H) = \varepsilon(h).$$

Hence we obtained $\varepsilon S = \varepsilon$. □

Using Proposition 3.6 we observe that

$$\begin{aligned} (\Delta \otimes I)(S(h)_1 \otimes S(h)_2) &= (\Delta \otimes I)(S(h_2) \otimes S(h_1)) \\ &= \sum S(h_2)_1 \otimes S(h_2)_2 \otimes S(h_1) \\ &= \sum S(h_{22}) \otimes S(h_{21}) \otimes S(h_1) \\ &= \sum S(h_3) \otimes S(h_2) \otimes S(h_1) \end{aligned}$$

In fact, this argument can inductively be repeated and it leads to the following:

Corollary 3.7. *For any $n \geq 2$ the following equality holds.*

$$\sum S(h)_1 \otimes S(h)_2 \otimes ... \otimes S(h)_n = \sum S(h_n) \otimes ... \otimes S(h_2) \otimes S(h_1)$$

In the sequel, we will use these properties without explicitly mentioning.

Proposition 3.8. *Let H be a Hopf algebra with antipode S. Then the following conditions are equivalent.*

(i) *For every $h \in H$, $\sum S(h_2)h_1 = \varepsilon(h)1_H$*
(ii) *For every $h \in H$, $\sum h_2 S(h_1) = \varepsilon(h)1_H$*
(iii) $S^2 = I$

Proof. We will prove only the equivalence of (ii) and (iii) since the equivalence of (i) and (iii) follows similarly. Suppose that the condition (ii) holds. It suffices to show that S^2 is inverse to S with respect to convolution. For $h \in H$, we see that

$$(S^2 * S)(h) = \sum S^2(h_1)S(h_2) = \sum S(h_2 S(h_1)) = S(\varepsilon(h)1_H) = \varepsilon(h)S(1_H) = \varepsilon(h)1_H.$$

To prove the converse implication, we assume that $S^2 = I$. For any $h \in H$,

$$\sum h_2 S(h_1) = \sum S^2(h_2)S(h_1)$$

by assumption. But we have

$$\sum S^2(h_2)S(h_1) = \sum S(h_1 S(h_2)) = S(\varepsilon(h)1_H) = \varepsilon(h)S(1_H) = \varepsilon(h)1_H$$

completing the proof. □

Corollary 3.9. *If S is the antipode of a commutative or cocommutative Hopf algebra H, then $S^2 = I$.*

Proof. If H is (co)commutative, then the condition $((ii))(i)$ of Proposition 3.8 is satisfied. □

Remark 3.10. *Let H be a Hopf algebra with antipode S. Then H^{opcop} is another Hopf algebra with the same antipode S.*

Given a Hopf algebra H, by Remark 3.2 H^{cop} is a bialgebra. However H^{cop} need not be a Hopf algebra in general. The next lemma gives a necessary and sufficient condition for H^{cop} to be a Hopf algebra. When this is the case, the antipode of H^{cop} is denoted by S^{cop} and called the *twisted antipode* for H.

Lemma 3.11. *Let H be a Hopf algebra with antipode S. The bialgebra H^{cop} is a Hopf algebra iff S is a composition invertible function. In this case, $S^{cop} = S^{-1}$.*

Proof. Suppose first that H^{cop} is a Hopf algebra so that S^{cop} exists. Let $h \in H$, then we have

$$\begin{aligned} S^{cop}S(h) = \sum S^{cop}S(h_1\varepsilon(h_2)) &= \sum \varepsilon(h_2)1_H S^{cop}S(h_1) \\ &= \sum h_{22}S^{cop}(h_{21})S^{cop}S(h_1) \\ &= \sum h_3 S^{cop}(S(h_1)h_2) \\ &= \sum h_2 S^{cop}(\varepsilon(h_1)1_H) \\ &= \sum \varepsilon(h_1)h_2 S^{cop}(1_H) \\ &= h1_H \end{aligned}$$

And writing $SS^{cop}(h)$ as $\sum SS^{cop}(\varepsilon(h_1)h_2)$, one can similarly conclude that $SS^{cop}(h) = h$. Hence we obtain $S^{cop}S = SS^{cop} = I$ and $S^{cop} = S^{-1}$. Conversely suppose that S is invertible. Note then that S^{-1} is an antimorphism of H since

$$S(S^{-1}(hk)) = S(S^{-1}(k)S^{-1}(h))$$

implies that $S^{-1}(hk) = S^{-1}(k)S^{-1}(h)$ by injectivity of S. For any $h \in H$, we clearly have $\sum S^{-1}(h_2)h_1 = \sum S^{-1}(h_2)S^{-1}S(h_1)$. But then since S^{-1} is antimorphism we obtain

$$\sum S^{-1}(h_2)S^{-1}S(h_1) = \sum S^{-1}(S(h_1)h_2) = S^{-1}(\varepsilon(h)1_H) = \varepsilon(h)1_H.$$

Similarly it can be shown that $\sum h_2 S^{-1}(h_1) = \varepsilon(h)1_H$ whence $S^{cop} = S^{-1}$. □

3.2. (Co)Ideals and Factor Objects

In this section we will construct factor objects. These results will later be used to check that a quotient space is a Hopf algebra.

Definition 3.12. *Let (C, Δ, ε) be a coalgebra over k.*

- *(i) A k-subspace D of C is called a* subcoalgebra *if $\Delta(D) \subseteq D \otimes D$.*
- *(ii) A k-subspace I of C is called a* coideal *if $\Delta(I) \subseteq I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.*

Lemma 3.13. *If $f : V_1 \to V_2, g : W_1 \to W_2$ are morphisms of k- vector spaces then, $Ker(f \otimes g) = Ker(f) \otimes W_1 + V_1 \otimes Ker(g)$.*

Proof. We will only show that $Ker(f \otimes g) \subseteq Ker(f) \otimes W_1 + V_1 \otimes Ker(g)$ since the reverse inclusion is obvious. Suppose that $(v_\alpha)_{\alpha \in \mathcal{F}}$ is a basis for $Ker(f)$. We can then complete it to $(v_\alpha)_{\alpha \in \mathcal{I}}$, a basis for V_1, where $\mathcal{F} \subseteq \mathcal{I}$. Similarly, let $(w_\beta)_{\beta \in \mathcal{G}}$ be a basis for $Ker(g)$ and let $(w_\beta)_{\beta \in \mathcal{J}}$ be its completion. Now take an element $u \in Ker(f \otimes g)$. Since $(v_\alpha \otimes w_\beta)_{(\alpha,\beta) \in (\mathcal{I} \times \mathcal{J})}$ is a basis for $V_1 \otimes W_1$, u can be written as

$$u = \sum_{\substack{\alpha \in \mathcal{F} \\ \beta \in \mathcal{G}}} c_{\alpha\beta} v_\alpha \otimes w_\beta + \sum_{\substack{\alpha \in \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} v_\alpha \otimes w_\beta + \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{G}}} c_{\alpha\beta} v_\alpha \otimes w_\beta + \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} v_\alpha \otimes w_\beta \tag{3.1}$$

for some scalars $c_{\alpha\beta} \in k$. Applying $f \otimes g$ to both sides of this equality, we get that

$$\begin{aligned} 0 &= (f \otimes g)(u) \\ &= \sum_{\substack{\alpha \in \mathcal{F} \\ \beta \in \mathcal{G}}} c_{\alpha\beta} 0 \otimes 0 + \sum_{\substack{\alpha \in \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} 0 \otimes g(w_\beta) + \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{G}}} c_{\alpha\beta} f(v_\alpha) \otimes 0 + \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} f(v_\alpha) \otimes g(w_\beta) \\ &= 0 + 0 + 0 + \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} f(v_\alpha) \otimes g(w_\beta) \\ &= \sum_{\substack{\alpha \in \mathcal{I} \setminus \mathcal{F} \\ \beta \in \mathcal{J} \setminus \mathcal{G}}} c_{\alpha\beta} f(v_\alpha) \otimes g(w_\beta). \end{aligned}$$

Since both $(f(v_\alpha))_{\alpha \in \mathcal{I} \setminus \mathcal{F}}$ and $(g(w_\beta))_{\mathcal{J} \setminus \mathcal{G}}$ are linearly independent sets, we must have that $\big(f(v_\alpha)\otimes g(w_\beta)\big)_{\alpha\in\mathcal{I}\setminus\mathcal{F},\ \beta\in\mathcal{J}\setminus\mathcal{G}}$ is also linearly independent. This yields that $c_{\alpha\beta}=0$ for all $\alpha\in\mathcal{I}\setminus\mathcal{F}$ and $\beta\in\mathcal{J}\setminus\mathcal{G}$. Hence the last summand in equation (3.1) vanishes. In other words, we obtained that

$$u=\underbrace{\sum_{\substack{\alpha\in\mathcal{F}\\ \beta\in\mathcal{G}}} c_{\alpha\beta}v_\alpha\otimes w_\beta+\sum_{\substack{\alpha\in\mathcal{F}\\ \beta\in\mathcal{J}\setminus\mathcal{G}}} c_{\alpha\beta}v_\alpha\otimes w_\beta}_{\in Ker(f)\otimes W_1}+\underbrace{\sum_{\substack{\alpha\in\mathcal{I}\setminus\mathcal{F}\\ \beta\in\mathcal{G}}} c_{\alpha\beta}v_\alpha\otimes w_\beta}_{\in V_1\otimes Ker(g)}$$

which is the desired result.

□

Lemma 3.14. *Let $f:C\to D$ be a coalgebra morphism. Then,*

(i) $Im(f)$ is a subcoalgebra of D.
(ii) $Ker(f)$ is a coideal in C.

Proof. (*i*) $Im(f)$ is clearly a k-subspace since f is k-linear. Also we have

$$\begin{aligned}\Delta_D(Im(f))&=\Delta_D(f(C))\\&=(f\otimes f)\Delta_D(C)\text{ since } f \text{ is a coalgebra map}\\&\subseteq(f\otimes f)(C\otimes C)\\&=Im(f)\otimes Im(f)\end{aligned}$$

which proves that $Im(f)$ is a subcoalgebra of D.

(*ii*) First note that $\Delta_D f(Ker(f))=0$ since $\Delta_D(0)=0$. Then since f is a coalgebra map, we get $(f\otimes f)\Delta_C(Ker(f))=\Delta_D f(Ker(f))=0$. But this gives that

$$\Delta_C(Ker(f))\subseteq Ker(f\otimes f)$$

and the result follows by Lemma 3.13. □

Theorem 3.15. *Let C be a coalgebra, I a coideal and $p : C \to C/I$ the canonical projection of k-vector spaces. Then,*

(i) There exists a unique coalgebra structure on C/I such that p is a morphism of coalgebras.

(ii) If $f : C \to D$ is a morphism of coalgebras with $I \subseteq Ker(f)$, then there exists a unique morphism of coalgebras $\overline{f} : C/I \to D$ such that the diagram below commutes.

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "p"'] & D \\
C/I \arrow[ur, dotted, "\overline{f}"'] &
\end{tikzcd}$$

Proof. (i) Consider the map $(p \otimes p)\Delta : C \to C/I \otimes C/I$. We know that

$$(p \otimes p)\Delta(I) \subseteq (p \otimes p)(I \otimes C + C \otimes I)$$

as I is a coideal. But since p is the projection map, we have

$$\begin{aligned}
(p \otimes p)(I \otimes C + C \otimes I) &= p(I) \otimes p(C) + p(C) \otimes p(I) \\
&= 0 \otimes p(C) + p(C) \otimes 0 \\
&= 0.
\end{aligned}$$

Hence $I \subseteq Ker((p \otimes p)\Delta)$. By the universal property of the factor vector spaces there exists a unique linear map $\overline{\Delta}$ such that the diagram below commutes.

$$\begin{tikzcd}
C \arrow[r, "(p\otimes p)\Delta"] \arrow[d, "p"'] & C/I \otimes C/I \\
C/I \arrow[ur, dotted, "\overline{\Delta}"'] &
\end{tikzcd}$$

Then this map is defined by $\overline{\Delta}(\overline{c}) = \sum \overline{c_1} \otimes \overline{c_2}$ where $c = p(c)$. It is clear that $\overline{\Delta}$ is coassociative. Next, since I is a coideal, we have $\varepsilon(I) = 0$. This means that $I \subseteq Ker(\varepsilon)$.

So again by universal property of the factor vector spaces there exists a unique linear map $\overline{\varepsilon} : C/I :\to k$ such that

$$\begin{tikzcd}
C \arrow[r, "\varepsilon"] \arrow[d, "p"'] & k \\
C/I \arrow[ur, dotted, "\overline{\varepsilon}"'] &
\end{tikzcd}$$

commutes. It is clear then that $\overline{\varepsilon}(\overline{c}) = \varepsilon(c)$ for any $c \in C$ and ε satisfies the counit property. As the two diagrams above commute, p is a coalgebra map. $\overline{\Delta}$ and $\overline{\varepsilon}$ being unique, we deduce the uniqueness of coalgebra structure for which p is a morphism of coalgebras.

(ii) Similarly. □

An immediate corollary of this theorem is "the fundamental theorem for coalgebras".

Corollary 3.16. *Given a morphism $f : C \to D$ of coalgebras, $C/Ker(f) \cong Im(f)$ as coalgebras.*

Theorem 3.15 has a similar version for bialgebras and Hopf algebras. We first give a definition.

Definition 3.17. *A k-subspace I of a Hopf algebra is said to be a* Hopf ideal *provided that I is ideal, coideal and $S(I) \subseteq I$.*

Theorem 3.18. *Let B be a (Hopf) bialgebra and I be a (Hopf) ideal and coideal of B. Then B/I is a (Hopf) bialgebra and $p : B \to B/I$ is a morphism of (Hopf) bialgebras.*

3.3. Examples

Example 3.19. *(The Group Algebra) The algebra kG in Example 2.4 becomes a Hopf algebra by defining*

$$\Delta(g) = g \otimes g \quad \textit{and} \quad \varepsilon(g) = 1$$

for any $g \in G$. In this case the antipode is given by $S(g) = g^{-1}$ on basis elements.

Example 3.20. *(The Tensor Algebra) Let M be a k-vector space. The tensor algebra of M is defined as*

$$T(M) := \bigoplus_{n \geq 0} T^n(M)$$

where $T^0(M) = k,\ T^1(M) = M$ and $T^n(M) = \overbrace{M \otimes ... \otimes M}^{n\ times}$ for $n \geq 2$. The algebra structure on $T(M)$ is constructed as follows. If $x = m_1 \otimes ... \otimes m_n \in T^n(M)$ and $y = h_1 \otimes ... \otimes h_r \in T^r(M)$ then the product of the elements is given by

$$x \cdot y = m_1 \otimes ... \otimes m_n \otimes h_1 \otimes ... \otimes h_r \in T^{n+r}(M).$$

This multiplication is linearly extended to arbitrary elements in $T(M)$. Note then that $k \cdot (m \otimes m \otimes ... \otimes m) = km \otimes m \otimes ... \otimes m$. Next, the coalgebra maps are gives as

$$\Delta(m) = m \otimes 1 + 1 \otimes m \ \textit{and,} \ \varepsilon(m) = 0 \ \textit{for all} \ m \in M. \tag{3.2}$$

In this case, ε is identity on $T^0(M)$ and zero elsewhere. Moreover the antipode is given by $S(m) = -m$ for $m \in M$. Observe also that for an arbitrary element $m_1 \otimes ... \otimes m_n \in$

$T^n(M)$ we have

$$\begin{aligned} S(m_1 \otimes ... \otimes m_n) &= S(m_n) \cdot S(m_{n-1}) ... \ S(m_1) \text{ since } S \text{ is an antimorphism of algebras} \\ &= -m_n \cdot -m_{n-1} ... \ -m_1 \\ &= (-1)^n (m_n \otimes ... \otimes m_1). \end{aligned}$$

Example 3.21. *(The Symmetric Algebra) The symmetric algebra $S(M)$ is defined as the factor Hopf algebra $T(M)/I$ where I is the ideal of $T(M)$ generated by the elements of the form*

$$x \otimes y - y \otimes x$$

for $x, y \in M$. To check that $S(M)$ is a Hopf algebra, by Theorem 3.18 *one only needs to verify that I is a Hopf ideal of $T(M)$. First let us show that I is a coideal of $T(M)$. As Δ and ε are morphisms of algebras, it suffices to show that*

$$\Delta(x \otimes y - y \otimes x) \in I \otimes T(M) + T(M) \otimes I$$

and that

$$\varepsilon(x \otimes y - y \otimes x) = 0$$

for any $x, y \in M$. We have that

$$\begin{aligned} \Delta(x \otimes y - y \otimes x) &= \Delta(x \otimes y) - \Delta(y \otimes x) \\ &= \Delta(x)\Delta(y) - \Delta(y)\Delta(x) \text{ since } \Delta \text{ is an algebra morphism} \\ &= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x) \\ &= (xy \otimes 1 + x \otimes y + y \otimes x + 1 \otimes xy) \\ &\qquad - (yx \otimes 1 + y \otimes x + x \otimes y + 1 \otimes yx) \\ &= (xy - yx) \otimes 1 + 1 \otimes (xy - yx). \end{aligned}$$

But since $xy - yx \in I$ *and* $1 \in T(M)$ *it follows that* $(xy - yx) \otimes 1 + 1 \otimes (xy - yx) \in I \otimes T(M) + T(M) \otimes I$. *Moreover,*

$$\begin{aligned}\varepsilon(x \otimes y - y \otimes x) &= \varepsilon(x \otimes y) - \varepsilon(y \otimes x) \\ &= \varepsilon(xy) - \varepsilon(yx) \\ &= \varepsilon(x)\varepsilon(y) - \varepsilon(y)\varepsilon(x) \text{ since } \varepsilon \text{ is algebra map} \\ &= 0 \text{ by } (3.2).\end{aligned}$$

Now we show that $S(I) \subseteq I$. *Similarly since* S *is an antimorphism of algebras, we only verify that* $S(x \otimes -y \otimes x) \in I$. *But this is immediate since*

$$\begin{aligned}S(x \otimes y - y \otimes x) = S(x \otimes y) - S(y \otimes x) &= S(xy) - S(yx) \\ &= S(y)S(x) - S(x)S(y) \\ &= (-y)(-x) - (-x)(-y) \\ &= (-y) \otimes (-x) - (-x) \otimes (-y) \in I.\end{aligned}$$

Example 3.22. *(The Universal Enveloping Algebra of a Lie Algebra) The universal enveloping algebra* $U(\mathfrak{g})$ *of the Lie algebra* $\mathfrak{g}$, *is the factor algebra* $T(\mathfrak{g})/I$ *where* I *is the ideal generated by the elements of the form* $[x, y] - xy + yx$ *for* $x, y \in \mathfrak{g}$. *Similar to previous examples, one can verify that* I *is indeed a Hopf ideal of* $T(\mathfrak{g})$.

3.4. Duals

We have seen that the dual C^* of a coalgebra C is an algebra. A natural question is to ask whether an analogous result exists for duals of algebras. The answer to this is affirmative when the algebra is finite dimensional. Moreover the dual of a finite dimensional Hopf algebra has also a Hopf algebra structure.

Let $T : M \to N$ be a linear map between two modules. We will denote by $T^* : N^* \to M^*$ the induced map which is defined by $T^*(f) = fT$ for any $f \in N^*$.

Theorem 3.23. *If* A *is a finite dimensional algebra, then there exists a canonical coalgebra structure on* A^*.

Proof. Let μ and u be the multiplication and unit maps of A respectively. It is well known in module theory that the morphism

$$\begin{aligned}
\varphi : A^* \otimes A^* &\longrightarrow (A \otimes A)^* \\
f \otimes g &\longmapsto \varphi(f \otimes g) : A \otimes A \longrightarrow R \\
&\qquad\qquad\qquad\qquad a \otimes b \longmapsto f(a)g(b)
\end{aligned}$$

is an isomorphism of R modules when A is finite dimensional. Then since φ^{-1} exists we define $\Delta := \varphi^{-1}\mu^*$ and $\varepsilon :=\simeq u^*$. From the construction of Δ and injectivity of φ we can define $\Delta(f) = \sum g_i \otimes h_i$ for any $g_i, h_i \in A^*$ with the property that $f(ab) = \sum g_i(a)h_i(b)$ for any $a, b \in A$. Having constructed the comultiplication and counit maps we need to verify the coassociativity and counit property. To prove the coassociativity let $f \in A^*$ and $\Delta(f) = \sum_i g_i \otimes h_i$. Suppose that $\Delta(g_i) = \sum_j g^1_{i,j} \otimes g^2_{i,j}$ and $\Delta(h_i) = \sum_j h^1_{i,j} \otimes h^2_{i,j}$. Then what we have to show is

$$\sum_{i,j} g^1_{i,j} \otimes g^2_{i,j} \otimes h_i = \sum_{i,j} g_i \otimes h^1_{i,j} \otimes h^2_{i,j}.$$

We consider the map $\theta : A^* \otimes A^* \otimes A^* \to (A \otimes A \otimes A)^*$ given by $\theta(u \otimes v \otimes w)(a \otimes b \otimes c) = u(a)v(b)w(c)$ for $u, v, w \in A^*$ and $a, b, c \in A$. We see that

$$\begin{aligned}
\theta(\sum_{i,j} g^1_{i,j} \otimes g^2_{i,j} \otimes h_i)(a \otimes b \otimes c) &= \sum_{i,j} g^1_{i,j}(a) g^2_{i,j}(b) h_i(c) \\
&= \sum_i g_i(ab) h_i(c) \\
&= f(abc)
\end{aligned}$$

by definition of Δ. With a similar computation one gets

$$\theta(\sum_{i,j} g_i \otimes h^1_{i,j} \otimes h^2_{i,j})(a \otimes b \otimes c) = f(abc)$$

and the desired result is obtained by injectivity of θ. Also the counit property is satisfied since for any $a \in A$

$$(\varepsilon \otimes I)\Delta(f)(a) = (\sum \varepsilon(g_i)h_i)(a) = \sum g_i(1_A)h_i(a) = f(a)$$

and similarly $(I \otimes \varepsilon)\Delta = I$. $\square$

In what follows we shall always consider the above coalgebra structure for duals of algebras. Note that Theorem 3.23 does not give an open formula for $\Delta(f)$. In fact we can determine $\Delta(f)$ explicitly by using bases of A and A^*. Let $(e_i)_i$ be a basis of A and $(e_i^*)_i$ be its dual basis. Then $(e_j^* \otimes e_l^*)_{j,l}$ is a basis of $A^* \otimes A^*$. So for every $f \in A^*$, $\Delta(f) = \sum_{j,l} a_{j,l} e_j^* \otimes e_l^*$ for some sequence $(a_{j,l})_{j,l}$ in the base ring. Then using the definition of comultiplication for any s, t we get

$$f(e_s e_t) = \sum g_i(e_s)h_i(e_t) = \sum_{j,l} a_{j,l} e_j^* e_l^*(e_t) = a_{s,t}.$$

Hence $\Delta(f) = \sum_{j,l} f(e_j e_l) e_j^* \otimes e_l^*$.

Proposition 3.24. *If B is a finite dimensional bialgebra, then B^* is also a bialgebra. Moreover if S is the antipode of B, then S^* is an antipode for B^*.*

Proof. Let $\overline{\Delta}$ and $\overline{\varepsilon}$ be the structure maps of B^* that are dual to those in B. Let $f, g \in B^*$ and $a, b \in B$ then we get that

$$\begin{aligned}(f * g)(ab) &= \sum f((ab)_1)g((ab)_2) \\ &= \sum f(a_1b_1)g(a_2b_2) \text{ since B is a bialgebra} \\ &= \sum f_1(a_1)f_2(b_1)g_1(a_2)g_2(b_2) \\ &= \sum (f_1 * g_1)(a)(f_2 * g_2)(b)\end{aligned}$$

But this implies that $\overline{\Delta}(f * g) = \sum (f_1 * g_1) \otimes (f_2 * g_2)$. Also it is clear that $\overline{\Delta}(1_{H^*}) =$

$1_{H^*} \otimes 1_{H^*}$. Hence it follows that $\overline{\Delta}$ is an algebra morphism. Moreover we have

$$\overline{\varepsilon}(f * g) = (f * g)(1_B) = f(1_B)g(1_B) = \overline{\varepsilon}(f)\overline{\varepsilon}(g)$$

and $\overline{\varepsilon}(\varepsilon) = \varepsilon(1_B) = 1$ which gives that $\overline{\varepsilon}$ is an algebra morphism as well. Now suppose that B is a Hopf algebra with antipode S. Let us denote by U the unit map of B^*. We note then that for any $b \in B$, and $f \in B^*$ we have the equality $(U\overline{\varepsilon})(b) = \varepsilon(b)f(1_B)$. Also S^* is inverse to I with respect to convolution since

$$\begin{aligned}(S^* * I)(f)(b) &= \sum (S^*(f_1) * f_2)(b) \\ &= \sum f_1(S(b_1))f_2(b_2) \\ &= \sum f(S(b_1)b_2) \\ &= \sum f(\varepsilon(h)1_B) \\ &= \varepsilon(h)f(1_B).\end{aligned}$$

Similarly one can show that $I * S^* = U\overline{\varepsilon}$. □

Proposition 3.25. *Let H be a finite dimensional Hopf algebra. Then $H \cong H^{**}$ as Hopf algebras.*

Proof. We claim that the evaluation map

$$\begin{aligned}\theta : H &\longrightarrow H^{**} \\ h &\longmapsto \theta(h) : H^* \longrightarrow R \\ &\qquad\qquad\qquad f \longmapsto f(h)\end{aligned}$$

is the desired isomorphism. Since we know that the evaluation map is an isomorphism of vector spaces, it remains to show that it is a morphism of algebras and coalgebras. We first show that it is an algebra morphism. For this, let $h, k \in H$ and $f \in H^*$. Then we obtain

$$\begin{aligned}\theta(hk)(f) = f(hk) &= \sum f_1(h)f_2(k)\\ &= \sum \theta(h)(f_1)\theta(k)(f_2)\\ &= (\theta(h)\theta(k))(f).\end{aligned}$$

Also θ preserves the units since $\theta(1_H)(f) = f(1_H) = \varepsilon_{H^*}(f)$ and hence $\theta(1_H) = 1_{H^*}$.

Now to show that θ is a morphism of coalgebras we will first verify the commutativity of the diagram below.

$$\begin{tikzcd}
H \arrow[r, "\theta"] \arrow[d, "\Delta_H"'] & H^{**} \arrow[d, "\Delta_{H^{**}}"] \\
H \otimes H \arrow[r, "\theta\otimes\theta"'] & H^{**} \otimes H^{**}
\end{tikzcd}$$

That is, we need the equality $\Delta_{H^{**}}\theta(h) = \sum \theta(h_1) \otimes \theta(h_2)$. By the construction of comultiplication map in dual coalgebras, it suffices to show that $\theta(h)(f * g) = \sum \theta(h_1)(f)\theta(h_2)(g)$ for any $f, g \in H^*$. But this is immediate since

$$\theta(h)(f * g) = (f * g)(h) = \sum f(h_1)g(h_2) = \sum \theta(h_1)(f)\theta(h_2)(g).$$

Also we have

$$\varepsilon_{H^{**}}\theta(h) = \theta(h)(1_H^*) = \theta(h)(\varepsilon) = \varepsilon(h)$$

which gives the commutativity of

$$\begin{tikzcd}
H \arrow[r, "\theta"] \arrow[dr, "\varepsilon_H"'] & H^{**} \arrow[d, "\varepsilon_{H^{**}}"] \\
 & k
\end{tikzcd}$$

and finishes the proof. □

4. MODULES

From now on, we will consider the spaces over a field k. This will allow us to use bases.

4.1. Modules and Comodules

In this section, we will review some of the basic properties of modules over algebras and comodules over coalgebras.

Definition 4.1. *If (A, μ, u) is a k-algebra then, the k vector space M is said to be a* left A-module *provided there exists a k-linear map $\Phi : A \otimes M \to M$ such that the diagrams*

$$\begin{tikzcd}
A \otimes A \otimes M \arrow[r, "I\otimes\Phi"] \arrow[d, "\mu\otimes I"'] & A \otimes M \arrow[d, "\Phi"] \\
A \otimes M \arrow[r, "\Phi"'] & M
\end{tikzcd}$$

and

$$\begin{tikzcd}
A \otimes M \arrow[dr, "\Phi"'] & k \otimes M \arrow[l, "u\otimes I"'] \arrow[d, "\simeq"] \\
 & M
\end{tikzcd}$$

are commutative.

As long as the context is clear, we will denote $\Phi(a \otimes m)$ by usual multiplication notation. We assume a similar definition for right A-modules. By reversing the arrows in the above diagrams we define comodules:

Definition 4.2. *If (C, Δ, ε) is a k-coalgebra then, the k vector space M is said to be a* right C-comodule *provided there exists a k-linear map $\rho : M \to M \otimes C$ such that the* *diagrams*

$$\begin{tikzcd}
M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C \arrow[d, "I\otimes\Delta"] \\
M \otimes C \arrow[r, "\rho\otimes I"'] & M \otimes C \otimes C
\end{tikzcd}$$

and

$$\begin{tikzcd}
M \arrow[r, "\rho"] \arrow[d, "\simeq"'] & M \otimes C \arrow[dl, "I\otimes\varepsilon"] \\
M \otimes k &
\end{tikzcd}$$

are commutative.

Similarly one can define left C-comodules. In this case, the comodule map is defined from M to $C \otimes M$. For the right C-comodule M, we use the notation

$$\rho(m) = \sum m_0 \otimes m_1.$$

Then, the diagrams above can be rewritten in the following two equations

$$\sum m_{00} \otimes m_{01} \otimes m_1 = \sum m_0 \otimes m_{11} \otimes m_{12} \text{ and,}$$

$$\sum \varepsilon(m_1)m_0 = m.$$

Now we denote both sides of the first equation by $\sum m_0 \otimes m_1 \otimes m_2$. Then we put

$$\sum m_0 \otimes m_1 \otimes ... \otimes m_n := (\rho \otimes \overbrace{I \otimes ... \otimes I}^{n-1 \text{ times}})...(\rho \otimes I)\rho(m).$$

There exists a computation rule for comodules which is similar to that of coalgebras. We state this rule in the following theorem but omit its proof since it is similar to former one.

Theorem 4.3. *Let $n \geq 2$ and $1 \leq i \leq n-1$ be arbitrary. Then we have*

$$\sum m_0 \otimes m_1 \otimes ... \otimes m_n = \sum m_0 \otimes m_1 \otimes ... \otimes \Delta(m_i) \otimes ... \otimes m_{n-1}.$$

Remark 4.4. *In the case of left C-comodules we will use the notation*

$$\sum m_{-n} \otimes m_{-n+1} \otimes ... \otimes m_0 = (\rho \otimes \overbrace{I \otimes ... \otimes I}^{n-1 \ times})...(\rho \otimes I)\rho(m).$$

All these notations will allow us to keep in mind that the element with index 0 is in the comodule whereas the other elements are in C.

Example 4.5. *Any coalgebra (C, Δ, ε) is a left and right comodule over itself with the structure map $\rho = \Delta$.*

Example 4.6. *If C is a coalgebra and M is a k- vector space then, $M \otimes C$ becomes a right C-comodule with structure map $\rho : m \otimes c \mapsto \sum m \otimes c_1 \otimes c_2$.*

Example 4.7. *Let H be a Hopf algebra and M and N be right H-modules. Then $M \otimes N$ becomes a right H-module via $(m \otimes n)h = \sum mh_1 \otimes nh_2$.*

Definition 4.8. *(i) Let M and N be two left A-modules with structure maps Φ_M and Φ_N respectively. An A-*module morphism *$f : M \to N$ is a k-linear map which makes the following diagram commutative.*

$$\begin{tikzcd}
A \otimes M \arrow[r, "I\otimes f"] \arrow[d, "\Phi_M"'] & A \otimes N \arrow[d, "\Phi_N"] \\
M \arrow[r, "f"'] & N
\end{tikzcd}$$

(ii) Let (V, ρ_V) and (W, ρ_W) be two right C-comodules. The k-linear map $g : V \to W$ is called a morphism of C-comodules *if $\rho_W g = (g \otimes I)\rho_V$. In the sigma notation, this is $\sum g(v)_0 \otimes g(v)_1 = \sum g(v_0) \otimes g(v_1)$ for any $v \in V$.*

We will denote the category of right C-comodules by $\mathcal{M}^C$. In this category, the objects are right C-comodules and the morphisms are comodule morphisms. Likewise ${}^C\mathcal{M}$ will denote the category of left C-comodules. If A is an algebra, the category of left (resp. right) A-modules will be denoted by ${}_A\mathcal{M}$ (resp. $\mathcal{M}_A$). In what follows, we will generally use right comodules or left modules without mentioning equivalent results for left comodules and right modules. In the language of category theory, this equivalence is asserted in the following propositions.

Proposition 4.9. *Let A be an algebra. Then the categories $\mathcal{M}_A$ and ${}_{A^{op}}\mathcal{M}$ are isomorphic.*

Proof. Let M be an object in $\mathcal{M}_A$. Suppose that $\cdot$ denotes the right action of A on M. Then, $a \circ m = m \cdot a$ defines a left A^{op}-module on M since

$$\begin{aligned} a \circ (b \circ m) = (m \cdot b) \cdot a &= m \cdot (ba) \\ &= m \cdot (a \cdot_{A^{op}} b) \\ &= (a \cdot_{A^{op}} b) \circ m \end{aligned}$$

for any $a, b \in A$ and $m \in M$, where we denoted by $\cdot_{A^{op}}$ the multiplication in A^{op}. Also we have $(\lambda 1_{A^{op}}) \circ m = m \cdot (\lambda 1_{A^{op}}) = m\lambda$ for any $\lambda \in k$. It is clear that every morphism of right A- modules is a morphism of left A^{op}- modules. Hence we have defined a covariant functor $F : \mathcal{M}_A \to {}_{A^{op}}\mathcal{M}$ and similarly the inverse functor to F can be defined. ☐

Proposition 4.10. *Let C be a coalgebra. Then the categories ${}^C\mathcal{M}$ and $\mathcal{M}^{C^{cop}}$ are isomorphic.*

Proof. To every object M in ${}^C\mathcal{M}$, with structure map $\rho(m) = \sum m_{-1} \otimes m_0$, we can associate the object M in $\mathcal{M}^{C^{cop}}$ whose structure map is given by $\gamma(m) = \sum m_0 \otimes m_{-1}$. The rest is similar to previous proposition. ☐

Remark 4.11. *Let H be a Hopf algebra with antipode S. Then,* *(i) If M is a right H-module then M becomes a left H-module with $h \cdot m = mS(h)$.*

(ii) If M is a left H-module then M becomes a right H-module with $m \cdot h = S(h)m$.

(iii) If M is a right H-comodule with structure map $\rho(m) = \sum m_0 \otimes m_1$ then M becomes a left H-comodule with $\rho'(m) = \sum S(m_1) \otimes m_0$.

(iv) If M is a left H-comodule with structure map $\rho(m) = \sum m_1 \otimes m_0$ then M becomes a right H-comodule with $\rho'(m) = \sum S(m_1) \otimes m_0$.

Lemma 4.12. *If M is a right C-comodule then M is a left C^*-module.*

Proof. Suppose that M is a right C-comodule with the structure map

$$\rho : M \to M \otimes C, m \mapsto \sum m_0 \otimes m_1.$$

We claim that M becomes a left C^*-module via

$$f \cdot m = \sum < f, m_1 > m_0$$

for any $f \in C^*$ and $m \in M$. To prove it, let $g \in C^*$ then we get

$$\begin{aligned} f \cdot (g \cdot m) &= \sum < f, (g \cdot m)_1 > (g \cdot m)_0 \\ &= \sum (< f, (\sum < g, m_1 > m_0)_1 >)(\sum < g, m_1 > m_0)_0 \\ &= \sum < g, m_1 > (< f, m_{01} >) m_{00} \text{ since } f \text{ and } \rho \text{ are } k\text{-linear} \\ &= \sum < g, m_{12} >< f, m_{11} > m_0 \\ &= \sum < f * g, m_1 > m_0 \\ &= (f * g) \cdot m \end{aligned}$$

Observe that we used the fact that

$$\sum (n\lambda)_0 \otimes (n\lambda)_1 = \rho(n\lambda) = \lambda\rho(n) = \sum \lambda n_0 \otimes n_1$$

for any $n \in M$ and $\lambda \in k$. Moreover,

$$\lambda 1_{c^*} \cdot m = \sum < \lambda 1_{C^*}, m_1 > m_0 = \sum \lambda \varepsilon(m_1) m_0 = \lambda m$$

where the last equality follows by comodule property of M. □

The converse of this Lemma is not true in general. A C^*-module which becomes C-comodule in this way is called *rational*. If we denote the category of rational C^*-modules by $\mathcal{R}at({}_{C^*}\mathcal{M})$ then, there is an isomorphism between $\mathcal{R}at({}_{C^*}\mathcal{M})$ and $\mathcal{M}^C$.

Remark 4.13. *Using Lemma* 4.12*, we can put a left module structure on every right comodule. For instance, if we consider the right* C*-comodule structure of* C *as in Example* 4.5 *we see that* C *is a left* C^**-module with*

$$f \rightharpoonup c = \sum < f, c_2 > c_1$$

for $f \in C^*$ *and* $c \in C$*. This is usually called the* left hit action *of* C^* *on* C*. On the other hand, if* C *is considered with its left* C*-comodule structure then, by Proposition* 4.10 C *is a right* C^{cop}*-comodule. Applying Lemma* 4.12*,* C *becomes a left* $(C^{cop})^*$*-module. But Lemma* 4.15 *tells us that all left* $(C^{cop})^*$*-modules are in fact* C^**-modules. Thus* C *is finally a right* C^**-module with the* right hit action

$$c \leftharpoonup f = \sum < f, c_1 > c_2.$$

Remark 4.14. *Similarly, if* A *is an algebra then* A^* *is a left* A*-module via*

$$< a \rightharpoonup f, b > = < f, ba >$$

and a right A*-module via*

$$< f \leftharpoonup a, b > = < f, ab >$$

for any $a, b \in A$ *and* $f \in A^*$.

Lemma 4.15. *M is a left $(C^{cop})^*$-module iff it is a right C^*-module.*

Proof. Suppose that M is a left $(C^{cop})^*$-module with the left module action denoted by "${}_L\cdot$". We claim that for $f \in C^* = (C^{cop})^*$ and $m \in M$, $m \cdot_R f := f_L \cdot m$ defines a right C^*-module on M. Indeed for $g \in C^*$

$$\begin{aligned}(m \cdot_R f) \cdot_R g &= g_L \cdot (f_L \cdot m)\\ &= (g *_{(C^{cop})^*} f)_L \cdot m\\ &= m \cdot_R (g *_{(C^{cop})^*} f)\\ &= m \cdot_R (f *_{C^*} g)\end{aligned}$$

where $*_A$ denotes the multiplication in an algebra A. Moreover, we have

$$m \cdot_R (\lambda 1_{C^*}) = (\lambda 1_{C^*})_L \cdot m = (\lambda 1_{(C^{cop})^*})_L \cdot \lambda m = \lambda m$$

for any $\lambda \in k$. And, the converse is similar. □

Proposition 4.16. *Let C be a coalgebra and M be a k-vector space. Suppose that $\rho : M \to M \otimes C, m \mapsto \sum_i m_i \otimes c_i$ is a k-linear map. Then (M, ρ) is a right C-comodule if and only if (M, ϕ) is a left C^*-module, where $\phi : C^* \otimes M \to M$ is given by $\phi(f \otimes m) = \sum_i < f, c_i > m_i$.*

Proof. To simplify our notation let us denote $\rho(m)$ by $\sum m_0 \otimes m_1$ and, $\phi(f \otimes m)$ by $f \cdot m$. Then we shall write $f \cdot m = \sum < f, m_1 > m_0$ for any $m \in M, f \in C^*$. First we assume that M is a left C^*-module with structure map ϕ. Then since we have $\varepsilon \cdot m = m$, it follows that $\sum \varepsilon(m_1) m_0 = m$. Moreover for arbitrary $f, g \in C^*$ and

$m \in M$ we get that

$$\begin{aligned}(fg) \cdot m &= \sum < fg, m_1 > m_0 \\ &= \sum < f, m_{11} >< g, m_{12} > m_0 \\ &= \psi(I \otimes f \otimes g)(\rho \otimes I)\rho(m)\end{aligned}$$

and

$$\begin{aligned}f \cdot (g \cdot m) &= f \cdot (\sum < g, m_1 > m_0) \\ &= \sum < g, m_1 > (f \cdot m_0) \\ &= \sum < g, m_1 >< f, m_{01} > m_{00} \\ &= \psi(I \otimes f \otimes g)(\rho \otimes I)\rho(m)\end{aligned}$$

where $\psi : M \otimes k \otimes k \to M$ is the canonical isomorphism. We claim that

$$x := (I \otimes \Delta)\rho(m) - (\rho \otimes I)\rho(m)$$

is zero. To this end, we pick a basis $(e_i)_i$ of C and write $x = \sum_{i,j} m_{ij} \otimes e_i \otimes e_j$ for some $m_{ij} \in M$. For fixed i_0 and j_0 we consider the dual maps e_{i_0}, $e_{j_0} \in C^*$. Then we clearly have $m_{i_0 j_0} = (I \otimes e^*_{i_0} \otimes e^*_{j_0})(x) = 0$ which implies that $x = 0$ since i_0 and j_0 was arbitrary. Hence M is a right C-comodule. The reverse direction follows by Lemma 4.12. □

4.2. Hopf Modules

Definition 4.17. *Let H be a k-Hopf algebra. A k- space M is called a* right H-Hopf module *if it has a right H-module structure and a right H-comodule structure such that these two structures are compatible. That is,*

$$\sum (mh)_0 \otimes (mh)_1 = \sum m_0 h_1 \otimes m_1 h_2$$

for all $m \in M$ *and* $h \in H$.

Note that if ϕ and ρ are respectively module and comodule structure maps then, the compatibility condition can be expressed by the commutativity of

$$\begin{tikzcd}
M \otimes H \arrow[r, "\phi"] \arrow[d, "f"'] & M \arrow[d, "\rho"] \\
(M \otimes H) \otimes H \arrow[r, "\phi\otimes I"'] & M \otimes H
\end{tikzcd}$$

where $f : m \otimes h \mapsto \sum m_0 \otimes h_1 \otimes m_1 h_2$ gives $M \otimes H$ the right H-comodule structure. Thus compatibility condition says that ϕ is a morphism of H-comodules. On the other hand, this condition can be stated as "ρ is a right H-module map". This is equivalent to commutativity of

$$\begin{tikzcd}
M \arrow[r, "\phi"] & M \otimes H \\
M \otimes H \arrow[u, "\phi"] \arrow[r, "\rho\otimes I"'] & (M \otimes H) \otimes H \arrow[u, "\varphi"']
\end{tikzcd}$$

where φ gives $M \otimes H$ the right H-module structure as in Example 4.7. The following Lemma asserts that the compatibility condition can be generalized.

Lemma 4.18. *If* M *is a right* H*-Hopf module and* $n \geq 2$ *then the equality*

$$\sum (mh)_0 \otimes (mh)_1 \otimes ... \otimes (mh)_n = \sum m_0 h_1 \otimes m_1 h_2 \otimes ... \otimes m_n h_{n+1}$$

holds for any $m \in M$ *and* $h \in H$.

Proof. We prove the equality inductively. Suppose that the desired equality holds for some n. Then,

$$\begin{aligned}\sum(mh)_0 \otimes (mh)_1 \otimes ... \otimes (mh)_{n+1} &= \sum(mh)_{00} \otimes (mh)_{01} \otimes (mh)_1 \otimes ... \otimes (mh)_n \\ &= \sum(m_0h_1)_0 \otimes (m_0h_1)_1 \otimes m_1h_2 \otimes ... \otimes m_nh_{n+1} \\ &= \sum m_{00}h_{11} \otimes m_{01}h_{12} \otimes m_1h_2 \otimes ... \otimes m_nh_{n+1} \\ &= \sum m_{00}h_1 \otimes m_{01}h_2 \otimes m_1h_3 \otimes ... \otimes m_nh_{n+2} \\ &= \sum m_0h_1 \otimes m_1h_2 \otimes .... \otimes m_{n+1}h_{n+2}.\end{aligned}$$

Note that the second line follows by assumption. □

Definition 4.19. *A map is said to be a* right H-Hopf module morphism *if it is both a right H-comodule map and a right H-module map.*

Remark 4.20. *We denote the category of right H-Hopf modules by $\mathcal{M}_H^H$.*

Example 4.21. *Let V be a k-space and H be a Hopf algebra. Then $V \otimes H$ becomes a right H-module via right regular representation:*

$$\phi : (V \otimes H) \otimes H \to V \otimes H, (v \otimes h) \otimes g \mapsto v \otimes hg$$

Also $V \otimes H$ is a right H-comodule via

$$\rho : (V \otimes H) \to (V \otimes H) \otimes H, v \otimes h \mapsto \sum v \otimes h_1 \otimes h_2.$$

These structures are compatible since

$$\begin{aligned}\rho((v \otimes h)g) &= \rho(v \otimes hg) \\ &= \sum v \otimes (hg)_1 \otimes (hg)_2 \\ &= \sum v \otimes h_1g_1 \otimes h_2g_2 \\ &= \sum((v \otimes h_1)g_1) \otimes h_2g_2 \\ &= \sum(v \otimes h)_0g_1 \otimes (v \otimes h)_1g_2\end{aligned}$$

for any $v \in V$ and $h, g \in H$.

In fact, the next theorem says that up to Hopf module isomorphism, the only right H-Hopf module is the one in Example 4.21. Before proving the theorem we need a definition:

Definition 4.22. *Let M be a right H-comodule and N be a left H-module. Then the* coinvariant subspace *of M is the set*

$$M^{coH} = \{m \in M \mid \rho(m) = m \otimes 1\}$$

and the invariant subspace *of N is the set*

$$N^H = \{n \in N \mid hn = \varepsilon(h)n, \ \forall h \in H\}.$$

Theorem 4.23. *(Fundamental Theorem of Hopf Modules) Let M be in $\mathcal{M}_H^H$. Then $M \cong M^{coH} \otimes H$ as right H-Hopf modules where $M^{coH} \otimes H$ has the Hopf module structure of Example* 4.21.

Proof. We define the maps $\alpha : M^{coH} \otimes H \to M, m \otimes h \mapsto mh$ and $\beta : M \to M \otimes H, m \mapsto \sum m_0 S(m_1) \otimes m_2$. We claim that α is a morphism of right H-Hopf modules and β is inverse to α with respect to composition. First let us show that $\beta(M) \subseteq M^{coH} \otimes H$. We see that for any $m \in M$,

$$\begin{aligned}
(\rho \otimes I)(\sum m_0 S(m_1) \otimes m_2) &= \sum m_{00} S(m_1)_1 \otimes m_{01} S(m_1)_2 \otimes m_2 \\
&= \sum m_{00} S(m_{12}) \otimes m_{01} S(m_{11}) \otimes m_2 \\
&= \sum m_0 S(m_3) \otimes m_1 S(m_2) \otimes m_4 \\
&= \sum m_0 S(m_2) \otimes \varepsilon(m_1) 1_H \otimes m_3 \\
&= \sum m_0 S(\varepsilon(m_1) m_2) \otimes 1_H \otimes m_3 \\
&= \sum m_0 S(m_1) \otimes 1_H \otimes m_2
\end{aligned}$$

whence $\sum m_0 S(m_1) \otimes m_2 \in M^{coH} \otimes H$. Also we have

$$\begin{aligned}\alpha\beta(m) &= \alpha \sum m_0 S(m_1) \otimes m_2 \\ &= \sum m_0 S(m_1) m_2 \\ &= \sum m_0 \varepsilon(m_1) 1_H \\ &= m.\end{aligned}$$

And, conversely for any $m \in M^{coH}$

$$\begin{aligned}\beta\alpha(m \otimes h) &= \beta(mh) \\ &= \sum (mh)_0 S((mh)_1) \otimes (mh)_2 \\ &= \sum m_0 (h_1 S(m_1 h_2)) \otimes m_2 h_3, \text{ by Lemma 4.18} \\ &= \sum m(h_1 S(h_2)) \otimes h_3, \text{ since } m \in M^{coH} \text{ gives } m_0 = m \text{ and } m_1 = 1_H \\ &= \sum m\varepsilon(h_1) 1_H \otimes h_2 \\ &= \sum m \otimes \varepsilon(h_1) h_2 \\ &= \sum m \otimes h\end{aligned}$$

Now, to prove that α is a right H-comodule map we need the commutativity of the following diagram.

$$\begin{tikzcd}(M^{coH} \otimes H) \arrow[r, "\alpha"] \arrow[d, "\gamma"'] & M \arrow[d, "\rho"] \\ (M^{coH} \otimes H) \otimes H \arrow[r, "\alpha \otimes I"'] & M \otimes H\end{tikzcd}$$

In sigma notation this is equivalent to

$$\sum (mh)_0 \otimes (mh)_1 = \sum mh_1 \otimes h_2$$

for any $m \in M^{coH}$. But this is immediate since $m_0 = m$ and $m_1 = 1_H$. And, finally it is clear that α is a right H-module map since M is a right H-module. $\square$

The structure of Hopf modules was discovered in [9] and is valid for Hopf modules in braided tensor categories. We will illustrate an application of Fundamental Theorem of Hopf Modules to finite dimensional Hopf algebras in Theorem 4.26. Although Theorem 4.26 is due to [9], we give a simplified proof of [10].

Let H be a finite dimensional Hopf algebra with antipode S. We consider the left H^*-module structure on H^* which is given by left multiplication. That is, $f \cdot g = f * g$ for any $f, g \in H^*$. Suppose that $(e_i)_i$ is a basis for H and let $(e_i^*)_i$ be the dual basis. Then by Proposition 4.16, H^* is a right H-comodule with structure map

$$\rho(f) = \sum_i (e_i^* \cdot f) \otimes e_i = \sum f_0 \otimes f_1. \tag{4.1}$$

Observe that for any $g \in H^*$ we have that $g = \sum < g, e_i > e_i^*$. Hence we obtain that

$$\begin{aligned} \sum < g, h_1 >< f, h_2 > &= \sum < g, e_i >< e_i^*, h_1 >< f, h_2 > \\ &= \sum < (e_i^* \cdot f), g(e_i)h > \\ &= \sum < f_0, < g, f_1 > h > \text{ by equation (4.1)} \\ &= \sum < g, f_1 >< f_0, h > . \end{aligned} \tag{4.2}$$

Also, if H^* is considered with left H-module structure as in Remark 4.14 then it is a right H-module with

$$< f \leftharpoondown h, k > = < f, kS(h) >$$

by Remark 4.11.

Lemma 4.24. *Let H be a finite dimensional Hopf algebra. Then H^* is a right Hopf module with action $\leftharpoondown$ and coaction ρ as above.*

Proof. We show that the compatibility

$$\rho(f \leftharpoonup h) = \sum f_0 \leftharpoondown h_1 \otimes f_1 h_2$$

holds for $f \in H^*, h \in H$. Note that by (4.2) this is equivalent to show that

$$\sum < g, x_1 >< f \leftharpoonup h, x_2 > = \sum < f_0 \leftharpoondown h_1, x >< g, f_1 h_2 >$$

for any $g \in H^*, x \in H$. We see that

$$\begin{aligned}
\sum < f_0 \leftharpoondown h_1, x >< g, f_1 h_2 > &= \sum < f_0, xS(h_1) >< h_2 \rightharpoondown g, f_1 > \\
&= \sum < h_2 \rightharpoondown g, x_1 S(h_1)_1 >< f, x_2 S(h_1)_2 > \\
&= \sum < h_2 \rightharpoondown g, x_1 S(h_{12}) >< f, x_2 S(h_{11}) > \\
&= \sum < h_3 \rightharpoondown g, x_1 S(h_2) >< f, x_2 S(h_1) > \\
&= \sum < g, x_1 S(h_2) h_3 >< f, x_2 S(h_1) > \\
&= \sum < g, x_1 \varepsilon(h_2) >< f, x_2 S(h_1) > \\
&= \sum < g, x_1 >< f, x_2 S(h) > \\
&= \sum < g, x_1 >< f \leftharpoondown h, x_2 >
\end{aligned}$$

which completes the proof. ☐

Definition 4.25. *Let H be a Hopf algebra, then the space of* left integrals *in H is the set*

$$\int_H^l = \{\lambda \in H \mid h\lambda = \varepsilon(h)\lambda, \textit{for all } h \in H\}$$

and similarly the space of right integrals *in H is*

$$\int_H^r = \{\lambda \in H \mid \lambda h = \varepsilon(h)\lambda, \textit{for all } h \in H\}.$$

Theorem 4.26. *Let H be a finite dimensional Hopf algebra over k. Then,* *(i)* *Both* $\int_H^l$ *and* $\int_H^r$ *are one dimensional.*

(ii) *The antipode* S *is bijective and* $S(\int_H^l) = \int_H^r$.

(iii) *For* $0 \neq \varphi \in \int_{H^*}^l$, *the map* $H \to H^*$, *given by* $h \mapsto (h \rightharpoonup \varphi)$ *is a left linear isomorphism.*

Proof. We consider the right H-Hopf module structure on H^* as in Lemma 4.24. By Theorem 4.23 the map $\alpha : (H^*)^{coH} \otimes H \to H^*, f \otimes h \mapsto (f \leftharpoondown h)$ is an isomorphism.

(i) Since H is finite dimensional we have $dimH = dimH^*$ which gives that $dim(H^*)^{coH} = 1$ by above isomorphism. Observe that

$$\begin{aligned}(H^*)^{coH} &= (H^*)^{H^*} \text{ by Theorem 5.15}\\ &= \{f \in H^* \mid x \cdot f = \varepsilon(x)f, \text{for all } x \in H^*\}\\ &= \int_{H^*}^l\end{aligned}$$

Replacing H^* by H, we conclude that $dim \int_H^l = 1$ as well. Also $dim \int_H^r = 1$ will follow by (ii).

(ii) Let S be the antipode of H and, $h \in H$ such that $S(h) = 0$. Then we get that

$$f \leftharpoondown h = S(h) \rightharpoonup f = 0 \rightharpoonup f = 0.$$

So $f \otimes h = 0$ by injectivity of α. Hence $h = 0$ and S is injective. But since H is finite dimensional, S is also a bijection.

Now we show that $S(\int_H^l) = \int_H^r$. First to see that $S(\int_H^l) \subseteq \int_H^r$ take $h \in \int_H^l$ and $x \in H$.

We have that

$$\begin{aligned} S^{-1}(x)h &= \varepsilon(S^{-1}(x))h \text{ since } h \in \int_H^l \\ &= \varepsilon(x)hS^{-1}(1_H) \text{ since } \varepsilon = \varepsilon S^{-1} \\ &= hS^{-1}(\varepsilon(x)1_H) \\ &= S^{-1}(\varepsilon(x)S(h)). \end{aligned}$$

This means that $S(h)x = \varepsilon(x)S(h)$ proving $S(h) \in \int_H^r$. Conversely for any $y \in \int_H^r$ we claim that $S^{-1}(y) \in \int_H^l$. By assumption $yS(x) = \varepsilon(S(x))y$ for all $x \in H$. But this holds iff $yS(x) = y\varepsilon(x)$ for each $x \in H$. Applying S^{-1} to both sides gives the desired result.

(iii) Using the fact that $(H^*)^{coH} \otimes H \cong H^*$ and $dim \int_{H^*}^l = 1$, we obtain that

$$H^* = \varphi \leftharpoondown H = S(H) \rightharpoonup \varphi.$$

Finally bijectivity of S gives $H^* = H \rightharpoonup \varphi$. □

5. ACTIONS AND COACTIONS OF HOPF ALGEBRAS

5.1. Connection Between Actions and Coactions

Definition 5.1. *Let H be a k-Hopf algebra.* H acts on the k-algebra A *(or* A is a left H-module algebra*) if the following conditions are satisfied.*

(i) *A is a left H-module*
(ii) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$*, for any* $h \in H$ *and* $a, b \in A$
(iii) $h \cdot 1_A = \varepsilon(h) 1_A$*, for any* $h \in H$.

In a symmetric fashion, one can define a right H-module algebra.

Lemma 5.2. *Let A be a k-algebra which is a left H-module such that* $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$ *for all* $h \in H$ *and* $a, b \in A$*. Then,*

$$(h \cdot a) \cdot b = \sum h_1 \cdot (a(S(h_2) \cdot b))$$

holds for all $h \in H$ *and* $a, b \in A$.

Proof. We compute the right hand side of the desired equality as follows.

$$\begin{aligned}
\sum h_1 \cdot (a(S(h_2) \cdot b)) &= \sum (h_{11} \cdot a)(h_{12} \cdot (S(h_2) \cdot b)) \\
&= \sum (h_{11} \cdot a)(h_{12} S(h_2)) \cdot b, \text{ since } A \text{ is } H\text{-module} \\
&= \sum (h_1 \cdot a)(h_2 S(h_3)) \cdot b \\
&= \sum (h_1 \cdot a)(\varepsilon(h_2) 1_H) \cdot b \\
&= \sum ((h_1 \varepsilon(h_2)) \cdot a) b \\
&= \sum (h \cdot a) b
\end{aligned}$$

□

Proposition 5.3. *Let A be a k-algebra which is also a left H-module. Then A is an H-module algebra iff* $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$ *for every* $h \in H$ *and* $a, b \in A$.

Proof. Let $h \in H$ and assume that the equality holds . Then we have

$$\begin{aligned} h \cdot 1_A &= (h \cdot 1_A)1_A \\ &= \sum h_1 \cdot (1_A(S(h_2) \cdot 1_A)), \text{ by taking } a = b = 1_A \text{ in Lemma 5.2} \\ &= \sum h_1(S(h_2) \cdot 1_A) \\ &= \sum (h_1 S(h_2)) \cdot 1_A \\ &= \sum \varepsilon(h) 1_A \end{aligned}$$

proving that A is an H-module algebra. The converse is clear. ☐

Note that the above proposition tells us that we can drop the condition (*iii*) in the Definition 5.1.

Definition 5.4. *Let A be an H-module algebra. Then the* algebra of invariants *is the set*

$$A^H = \{a \in A \mid h \cdot a = \varepsilon(h)a, \forall h \in H\}.$$

Observe that A^H is indeed a k-subalgebra of A since for $a, b \in A^H$ and $h \in H$ we have

$$h \cdot (ab) = \sum (h_1 a)(h_2 b) = \sum \varepsilon(h_1) a \varepsilon(h_2) b = \sum \varepsilon(h_1 \varepsilon(h_2)) ab = \sum \varepsilon(h) ab.$$

Example 5.5. *A Hopf algebra H is a left H-module algebra via the* left adjoint action *ad_l:*

$$h \cdot_{ad_l} x = \sum h_1 x S(h_2)$$

for all $h, x \in H$. *Also, the algebra of invariants of* H *coincides with the center of* H. *To see that* H *is indeed an* H*-module algebra, let* $h, p, a \in H$ *and* $c \in k$. *Then,*

$$\begin{aligned} h \cdot_{ad_l} (p \cdot_{ad_l} a) &= h \cdot_{ad_l} (\sum p_1 a S(p_2)) \\ &= \sum h_1 p_1 a S(p_2) S(h_2) \\ &= \sum (hp)_1 a S(h_2 p_2) \\ &= (hp) \cdot_{ad_l} a. \end{aligned}$$

Moreover, since Δ *is a* k*-linear map we have* $\Delta(c1_H) = c\Delta(1_H) = c1_H \otimes 1_H$. *Hence* $(c1_H) \cdot_{ad_l} a = (c1_H) a S(1_H) = ca1_H = ca$. *Now it remains to check that* H *acts on* H. *Using the computation rule,*

$$\begin{aligned} h \cdot_{ad_l} (ap) &= \sum h_1 a p S(h_2) \\ &= \sum h_1 a p S(\varepsilon(h_2) h_3) \\ &= \sum h_1 a \varepsilon(h_2) p S(h_3) \\ &= \sum h_1 a S(h_2) h_3 p S(h_4) \\ &= \sum (h_1 \cdot_{ad_l} a)(h_2 \cdot_{ad_l} p). \end{aligned}$$

For $H^H = Z(H)$, *let* $g \in H^H$. *Then for all* $h \in H$,

$$\begin{aligned} hg = (\sum h_1 \varepsilon(h_2)) g = \sum h_1 g \varepsilon(h_2) &= \sum h_1 g S(h_2) h_3 \\ &= \sum \varepsilon(h_1) g h_2, \ \textit{since } g \in H^H \\ &= \sum g \varepsilon(h_1) h_2 \\ &= gh \end{aligned}$$

proving that $H^H \subseteq Z(H)$. *Conversely, if* $g \in Z(H)$ *then,* $hg = gh$ *for all* $h \in H$. *So for every* h, $\sum h_1 g S(h_2) = \sum h_1 S(h_2) g = \varepsilon(h) g$ *since* g *commutes with* $S(h_2)$. *Thus* $g \in H^H$, *and we get the desired result.*

Example 5.6. *A Hopf algebra* H *is a right* H*-module algebra via the* right adjoint *action ad_r:*

$$x \cdot_{ad_r} h = \sum S(h_1) x h_2$$

for all $x, h \in H$.

Proposition 5.7. *Let G be a group and A be a k-algebra. Then, A is a kG-module algebra iff G acts as automorphisms of A. In this case, A^{kG} (the subalgebra of kG-invariants) is equal to A^G (the usual subalgebra of fixed points for G).*

Proof. First suppose that G acts as automorphisms of A, that is, there exists a morphism $\phi : G \to Aut(A)$ of groups where $Aut(A)$ denotes the group of k-algebra isomorphisms of A, with composition of functions. Note that this is equivalent to say that the group G acts on the set A with action given by

$$g \cdot a = \phi(g)(a) \text{ for any } g \in G \text{ and } a \in A.$$

and the action on an arbitrary element of A can be considered as an k-algebra isomorphism of A. We express the latter by the following conditions:

(i) $g \cdot (a + b) = g \cdot a + g \cdot b$
(ii) $g \cdot (la) = l(g \cdot a)$
(iii) $g \cdot (ab) = (g \cdot a)(g \cdot b)$
(iv) $g \cdot 1_A = 1_A$
(v) $g \cdot a = g \cdot b$ implies that $a = b$, for any $g \in G, l \in k$ and $a, b \in A$
(vi) for every $f \in A$, there exists $d \in A$ such that $g \cdot d = f$.

Then it is clear that A is a left kG-module with respect to linear extension of this action. Conversely, if A is an kG-module algebra then, it is clear that the kG-module action on A is also a group action of G on A. Moreover the conditions from (i) to (iv) immediately follow. For the injectivity of $\phi(g)$, where g is an arbitrary element in G, suppose that $g \cdot a = g \cdot b$. Then, $g^{-1} \cdot (g \cdot a) = g^{-1} \cdot (g \cdot b)$. But since A is a kG-module, we get $(g^{-1}g) \cdot a = (g^{-1}g) \cdot b$ which gives $1 \cdot a = 1 \cdot b$. Consequently we have $a = b$. Now for surjectivity, let $f \in H$ and $g \in G$. Then we have $g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = 1 \cdot a = a$ completing the proof of the iff statement. If this statement is the case, we have

$$\begin{aligned} A^{kG} &= \{a \in A \mid h \cdot a = \varepsilon(h)a, \ \forall h \in kG\} \\ &= \{a \in A \mid g \cdot a = a, \ \forall g \in G\} \\ &= A^G \end{aligned}$$

since $\varepsilon(h) = 1$ if $h \in G$ and $\varepsilon(h) = 0$ if $h \in k$. □

Definition 5.8. *Let H be a k-Hopf algebra and A be a k-algebra. H* coacts to the right *on A (or A is a* right H-comodule algebra*) if the following conditions are satisfied.*

(i) *A is a right H-comodule with* $\rho : A \to A \otimes H, a \mapsto \sum a_0 \otimes a_1$

(ii) $\sum (ab)_0 \otimes (ab)_1 = \sum a_0 b_0 \otimes a_1 b_1$ *for all* $a, b \in A$

(iii) $\rho(1_A) = 1_A \otimes 1_H$

Similarly, a left H-comodule algebra can be defined.

Note that if A is a k-algebra which is a right H-comodule with structure map $\rho : A \to A \otimes H$. Then A is an H-comodule algebra iff one of the following equivalent statements holds.

(i) ρ is a morphism of algebras

(ii) The multiplication map μ of A is a morphism of comodules and the unit map $u : k \to A$ is a morphism of comodules where the right comodule structure on $A \otimes A$ is given by $\overline{\rho} : a \otimes b \mapsto \sum a_0 \otimes b_0 \otimes a_1 b_1$.

Clearly all these statements correspond to the commutativity of the diagrams below.

$$\begin{tikzcd}
A \otimes A \arrow[r, "\mu"] \arrow[d, "\overline{\rho}"'] & A \arrow[d, "\rho"] \\
A \otimes A \otimes H \arrow[r, "\mu \otimes I"'] & A \otimes H
\end{tikzcd}
\qquad
\begin{tikzcd}
k \arrow[r, "u"] \arrow[d, "\simeq"'] & A \arrow[d, "\rho"] \\
k \otimes H \arrow[r, "u \otimes I"'] & A \otimes H
\end{tikzcd}$$

Definition 5.9. *Let A be an H-comodule algebra. The* algebra of the coinvariants *of A is the set*

$$A^{coH} = \{a \in A \mid \rho(a) = a \otimes 1\}.$$

Example 5.10. *A Hopf algebra H is a right H-comodule algebra with structure map $\rho := \Delta$. In this case, if $h \in H^{coH}$ then, $\rho(h) = h \otimes 1 = \Delta(h)$. Thus $(\varepsilon \otimes I)\Delta(h) = \varepsilon(h) \otimes 1$ and $\varepsilon(h)1 = h$. This shows that $H^{coH} \subset k1$. Conversely, $\rho(k1) = k1 \otimes 1$ and $k1 \in H^{coH}$. Hence $H^{coH} = k1$.*

Proposition 5.11. *Let G be a finite group and A be an algebra. Then G acts as k-automorphisms of A iff A is a $(kG)^*$-comodule algebra.*

Proof. If G acts as k-automorphisms of A we define the map $\rho : A \to A \otimes (kG)^*$ by $\rho(a) = \sum_{i=1}^{n} (x_i \cdot a) \otimes p_i$ where $G = \{x_1, ..., x_n\}$ and $\{p_1, ..., p_n\}$ is the dual basis of $(kG)^*$. Then it is easy to check that it gives A a $(kG)^*$-comodule algebra structure. Conversely suppose that $(kG)^*$ coacts to the right on A via $\psi(a) = \sum_{h \in G} a_h \otimes p_h$. Then G acts on A via $g \cdot a = \sum_h < p_h, g > a_h$. ☐

Definition 5.12. *Let G be a group.*

*(i) A k-module M is a G-*graded module *if $M = \bigoplus_{g \in G} M_g$, where the M_g's are the k-submodules of M.*

*(ii) A k-algebra A is a G-*graded algebra *(or* graded k-algebra of type G*) if $A = \bigoplus_{g \in G} A_g$, where the A_g's are the k-subspaces of A and, $A_g A_h \subseteq A_{gh}$ for all $g, h \in G$. Moreover if $A_g A_h = A_{gh}$ for every $g, h \in G$ (or equivalently $A_g A_{g^{-1}} = A_1$ for all $g \in G$) then A is said to be* strongly graded.

Lemma 5.13. *Let G be a group and M be a k-algebra. Then, M is a right kG-comodule iff M is a G-graded module.*

Proof. Suppose that M is a right kG-comodule with structure map ρ. We can write $\rho(m)$ as $\sum m_g \otimes g$ for any $m \in M$. Then since $(I \otimes \Delta_{kG})\rho = (\rho \otimes I)\rho$, we have

$$\sum_{h,g} (m_g)_h \otimes h \otimes g = \sum_g m_g \otimes g \otimes g.$$

But we know that the set G forms a basis for kG. So every element of $M \otimes kG \otimes kG$ may be written uniquely in the form $\sum_g n \otimes s \otimes g$ by well-known poperties of tensor products. Thus it follows that $(m_g)_h = \delta_{g,h} m_g$. For fixed g, we define $M_g = \{m_g |\ m \in M\}$. Then for any $m \in M$,

$$\begin{aligned} \sum m_0 \otimes m_1 = \sum_g m_g \otimes g \Rightarrow \sum m_0 \varepsilon(m_1) &= \sum_g m_g \varepsilon(g) \\ \Rightarrow m &= \sum_g m_g. \end{aligned}$$

Moreover, if there exists $m_g = n_h \in M_g \cap M_h$ then, $m_g = (m_g)_g = (n_h)_g = 0$. Hence $\bigoplus_g M_g = M$. Conversely, if M is a G-graded module then, clearly the map $\rho(m) = m \otimes g$, defined for each $m \in M_g$, gives M its desired comodule structure. □

Proposition 5.14. *Let G be a group and A be a k-algebra. Then, A is a right kG-comodule algebra iff A is a G-graded algebra. In this case, $A^{cokG} = A_{1_G}$.*

Proof. First assume that A is a kG-comodule algebra. Then by Lemma 5.13, we know that $A = \bigoplus_g A_g$ where $A_g = \{a_g |\ a \in A\}$. For any $a_g \in A_g$, we have

$$\rho(a_g) = \sum_h (a_g)_h \otimes h = a_g \otimes g.$$

Hence if $b_h \in A_h$ we get that $\rho(a_g b_h) = a_g b_h \otimes gh$ for any $b_h \in A_h$. Thus $a_g b_h \in A_{gh}$ proving that $A_g A_h \subseteq A_{gh}$. For the converse suppose that A is a G-graded algebra. Then again by Lemma 5.13, we need only to check that ρ is an algebra map. For homogenous elements $a \in A_g$ and $b \in A_h$ we know that $ab \in A_{gh}$ since $A_gA_h \subseteq A_{gh}$. So $\rho(ab) = ab \otimes gh = \rho(a)\rho(b)$. And, clearly $\rho(1_A) = 1_A \otimes 1_G$ since $1_A \in A_{1_G}$. □

When the Hopf algebra H is finite dimensional, there is a connection between actions and coactions:

Theorem 5.15. *Let H be a finite dimensional Hopf algebra. Then H^* acts on A iff H coacts on A, and under this equivalence $A^{H^*} = A^{coH}$.*

Proof. Suppose first that A is a right H-comodule algebra. Then by Lemma 4.12 we know that A is an H^*-module via $f \cdot a = \sum < f, a_1 > a_0$ for $f \in H^*$ and $a \in A$. Now for arbitrary $a, b \in A$ and $f \in H^*$ we have

$$\begin{aligned} f \cdot (ab) &= \sum < f, (ab)_1 > (ab)_0 \\ &= \sum < f, a_1b_1 > (a_0b_0) \\ &= \sum < f_1, a_1 >< f_2, b_1 > a_0b_0 \\ &= \sum < f_1, a_1 > a_0 < f_2, b_1 > b_0 \\ &= \sum (f_1 \cdot a)(f_2 \cdot b) \end{aligned}$$

which shows that H^* acts on H. To prove the converse, let $\{e_1, ..., e_n\}$ be a basis of H and, $\{e_1^*, ..., e_n^*\}$ be its dual basis. Define the k-linear map

$$\rho : A \longrightarrow A \otimes H$$

$$a \longmapsto \sum_{i=1}^n e_i^* \cdot a \otimes e_i.$$

Then we can write $(e_i^* \cdot a) = \sum_j < e_i^*, e_j > (e_j^* \cdot a)$ for any i. By Proposition 4.16 it follows that the left H^*-module structure on A is induced from ρ. Hence A is a right

H-comodule. Now we see that

$$\begin{aligned}
\rho(1_A) &= \sum_{i=1}^{n} e_i^* \cdot 1 \otimes e_i \\
&= \sum_{i=1}^{n} < e_i^*, 1 > 1 \otimes e_i, \text{ since } H^* \text{ acts on } A \\
&= \sum_{i=1}^{n} 1 \otimes < e_i^*, 1 > e_i \\
&= 1_A \otimes 1_H.
\end{aligned}$$

To conclude that A is a right H-comodule algebra, it remains to show that $\rho(ab) = \rho(a)\rho(b)$. First note that it is easy to check that for any $g \in H^*, g = \sum_{i=1}^{n} < g, e_i > e_i^*$. Let $f \in H^*$ be arbitrary, then we obtain

$$\begin{aligned}
(I \otimes f)(\rho(ab)) &= \sum_{i=1}^{n} e_i^* \cdot (ab) \otimes < f, e_i > \\
&= \sum_{i=1}^{n} (e_i^* < f, e_i >) \cdot (ab) \otimes 1, \text{ since the action is } k\text{-linear} \\
&= f \cdot (ab) \otimes 1, \text{ by the initial observation} \\
&= \sum (f_1 \cdot a)(f_2 \cdot b) \otimes 1, \text{ by multiplication in dual Hopf algebras} \\
&= \sum_{i,j=1}^{n} (< e_i^*, < f_1, e_i >> a)(< e_j^*, < f_2, e_j >> b) \otimes 1 \\
&= \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes < f_1, e_i >< f_2, e_j > \\
&= \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes < f, e_i e_j > \\
&= (I \otimes f)(\rho(a)\rho(b))
\end{aligned}$$

which gives the desired result since f was arbitrary. Moreover we have

$$\begin{aligned} A^{H^*} &= \{a \in A \mid f \cdot a = \varepsilon_{H^*}(f)a, \text{ for all } f \in H^*\} \\ &= \{a \in A \mid \sum < f, a_1 > a_0 =< f, 1_H > a, \text{ for all } f \in H^* \\ &= \{a \in A \mid (I \otimes f)(\rho(a)) = (I \otimes f)(a \otimes 1), \text{ for all } f \in H^*\} \\ &= \{a \in A \mid \rho(a) = a \otimes 1\} \\ &= A^{coH}. \end{aligned}$$

□

5.2. Crossed Products

Hopf crossed products that are considered in this section generalize usual crossed products over groups and semidirect products. The motivation of studying these general crossed products comes from their importance in the theory of extensions of Hopf algebras. We will see later that they can be characterized as a special kind of Hopf Galois extension. Their characterization also have several applications in duality and Maschke-type theorems [11].

Moreover, in case of a cocommutative Hopf algebra H which measures a commutative algebra A, crossed products have a cohomological interpretation. In [12], Sweedler defined cohomology groups $H^\bullet(H, A)$ where the convolution invertible map σ of Definition 5.17 corresponds to a two cocycle in this cohomology.

Definition 5.16. *Let H be a Hopf algebra and A an algebra. We say that H* measures *A (or A is an H-*measured algebra*) if there exists a k-linear map $\phi : H \otimes A \to H$ such that for every $h \in H, a \in A$ we have $h \cdot 1 = \varepsilon(h)1$ and $h \cdot (ab) = \sum(h_1 \cdot a)(h_2 \cdot b)$, where $h \cdot a$ denotes $\phi(h \otimes a)$.*

Definition 5.17. *Let H be a Hopf algebra and A an H-measured algebra. Assume that σ is a convolution invertible map in $Hom_k(H \otimes H, A)$. The* crossed product *$A\#_\sigma H$ is $A \otimes H$ as a vector space. The elements $a \otimes h$ are denoted by $a\#h$ and multiplication* *is given by*

$$(a\#h)(b\#g) = \sum a(h_1 \cdot b)\sigma(h_2, g_1)\#h_3g_2 \tag{5.1}$$

for $h, g \in H, a, b \in A$.

Theorem 5.18. *$A\#_\sigma H$ is an associative algebra with $1_{A\#_\sigma H} = 1\#1$ iff the followings hold.*

(i) *A is a* twisted H-module, *that is* $1 \cdot a = a$ *and*

$$h \cdot (g \cdot a) = \sum \sigma(h_1, g_1)(h_2g_2 \cdot a)\sigma^{-1}(h_3, g_3)$$

for all $h, g \in H, a \in A$

(ii) *σ is a* 2-cocycle, *that is,* $\sigma(h, 1) = \sigma(1, h) = \varepsilon(h)1$ *and*

$$\sum h_1 \cdot \sigma(g_1, m_1)\sigma(h_2, g_2m_2) = \sum \sigma(h_1, g_1)\sigma(h_2g_2, m_2)$$

for all $h, g, m \in H$.

We will generally deal with associative crossed products with identity.

Example 5.19. *Suppose that $A\#_\sigma H$ is an associative crossed product with identity. If σ is trivial, that is $\sigma(h, k) = \varepsilon(h)\varepsilon(k)1$ then by twisted module condition we have $h \cdot (k \cdot a) = \sum \sigma(h_1, k_1)(h_2k_2 \cdot a)\sigma^{-1}(h_3, k_3)$. However it is easy to see that $\sigma^{-1}(h_n, k_n)$ is equal to $\sigma^{-1}(1, h_nk_n)$ for any $n \geq 2$ since we have that*

$$\sum \sigma(1, h_{n-1}k_{n-1})\sigma^{-1}(1, h_nk_n) = \varepsilon(hk)1 = \varepsilon(h)\varepsilon(k)1 = \sum \sigma(h_{n-1}, k_{n-1})\sigma^{-1}(h_n, k_n)$$

and $\sigma(1, h_{n-1}k_{n-1}) = \sigma(1, h_{n-1}k_{n-1})$. So, in this case A is a left H-module algebra. Moreover the multiplication reduces to

$$(a\#h)(b\#g) = \sum a(h_1 \cdot b)\#h_2k$$

for any $a, b \in A, h, g \in H$. This special case of crossed product is called smash product algebra *and denoted by $A\#H$.*

Lemma 5.20. *Let $A\#_\sigma H$ be an associative crossed product with identity. The map $\rho : A\#_\sigma H \to (A\#_\sigma H) \otimes H$, defined by $\rho(a\#h) = \sum(a\#h_1) \otimes h_2$ gives $A\#_\sigma H$ a right H-comodule algebra structure. In this case, $(A\#_\sigma H)^{coH} = A\#_\sigma 1$. Also $A\#_\sigma H$ becomes a left A-module via*

$$\phi : A \otimes (A\#_\sigma H) \longrightarrow A\#_\sigma H$$

$$a \otimes (b\#h) \longmapsto ab\#h.$$

Proof. By coassociativity and counit property in H the diagrams below commute.

$$\begin{tikzcd}
A\#_\sigma H \arrow[r, "\rho"] \arrow[d, "\rho"'] & (A\#_\sigma H) \otimes H \arrow[d, "I\otimes\Delta"] \\
(A\#_\sigma H) \otimes H \arrow[r, "\rho\otimes I"'] & (A\#_\sigma H) \otimes H \otimes H
\end{tikzcd}
\qquad
\begin{tikzcd}
A\#_\sigma H \arrow[d, "\rho"'] \arrow[dr, "\simeq"] & \\
(A\#_\sigma H) \otimes H \arrow[r, "I\otimes\varepsilon"'] & (A\#_\sigma H) \otimes k
\end{tikzcd}$$

This shows that $A\#_\sigma H$ is a right H-comodule. Moreover ρ is an algebra map since

$$\begin{aligned}
\rho(a\#h)\rho(b\#g) &= \sum a(h_{11} \cdot b)\sigma(h_{12}, g_{11})\#h_{13}g_{12} \otimes h_2 g_2 \\
&= \sum a(h_1 \cdot b)\sigma(h_2, g_1)\#h_{31}g_{21} \otimes h_{32}g_{22} \\
&= \rho((a\#h)(b\#g))
\end{aligned}$$

for any $a, b \in A$ and $h, g \in H$. The second statement is clear since $A\#_\sigma H$ is known to be a left A-module via the given map. ☐

5.2.1. A characterization

We will characterize crossed products as a certain kind of extension. For this, we first give the following definition.

Definition 5.21. *Let $A \subset B$ be k-algebras and H a Hopf algebra. $A \subset B$ is called a* right H-extension *if* B *is a right* H*-comodule algebra with* $B^{coH} = A$*. Moreover, this extension is called* H-cleft *if there exists a right* H*-comodule map* $\gamma : H \to B$ *which is convolution invertible.*

Remark 5.22. *If* $A \subset B$ *is cleft via* $\gamma : H \to B$*, then* $\gamma(1)$ *is an invertible element in* B *since* $(\gamma * \gamma^{-1})(1) = \gamma(1)\gamma^{-1}(1) = 1$ *and similarly* $\gamma^{-1}(1)$ *is left inverse to* $\gamma(1)$*. So we may always assume that* $\gamma(1) = 1$ *since otherwise we could use the convolution invertible map* $\overline{\gamma} = \gamma(1)^{-1}\gamma$*.*

Lemma 5.23. *Let* $A \subset B$ *be an* H*-cleft extension. Suppose that* $\rho(b) = \sum b_0 \otimes b_1$ *gives* B *the* H*-comodule algebra structure and,* $\gamma : H \to B$ *makes the extension cleft. Then,*

(i) $\rho\gamma^{-1} = (\gamma^{-1} \otimes S)\tau\Delta$

(ii) for any $b \in B$*,* $\sum b_0\gamma^{-1}(b_1) \in A$*.*

Proof. (i) We first note that $\rho\gamma$ and $\rho\gamma^{-1}$ are inverse to each other in $Hom(H, B \otimes H)$ since for $h \in H$,

$$\begin{aligned}(\rho\gamma^{-1} * \rho\gamma)(h) &= \sum \rho(\gamma^{-1}(h_1))\rho(\gamma(h_2))\\ &= \sum \rho(\gamma^{-1}(h_1)\gamma(h_2))\\ &= \varepsilon(h)(1 \otimes 1).\end{aligned}$$

Also since γ is an H-comodule map, the diagram

$$\begin{tikzcd} H \arrow[r, "\gamma"] \arrow[d, "\Delta"'] & B \arrow[d, "\rho"] \\ H \otimes H \arrow[r, "\gamma\otimes I"'] & B \otimes H \end{tikzcd}$$

commutes. Now we will show that $\theta = (\gamma^{-1} \otimes S)\tau\Delta$ is inverse to $\rho\gamma$. Then $\theta = \rho\gamma^{-1}$

follows by the uniqueness of inverses. To this end, let $h \in H$ then,

$$\begin{aligned}
(\rho\gamma * \theta)(h) &= \sum[(\gamma \otimes I)\Delta(h_1)][(\gamma^{-1} \otimes S)\tau\Delta(h_2)] \\
&= \sum(\gamma(h_{11}) \otimes h_{12})(\gamma^{-1}(h_{22}) \otimes S(h_{21})) \\
&= \sum \gamma(h_1)\gamma^{-1}(h_4) \otimes h_2 S(h_3) \\
&= \sum \gamma(h_1)\gamma^{-1}(h_3) \otimes \varepsilon(h_2)1 \\
&= \sum \gamma(h_1)\gamma^{-1}(\varepsilon(h_2)h_3) \otimes 1 \\
&= \sum \gamma(h_1)\gamma^{-1}(h_2) \otimes 1 \\
&= \varepsilon(h)1 \otimes 1.
\end{aligned}$$

(ii) For $b \in B$, we are to show that $\sum b_0\gamma^{-1}(b_1) \in B^{coH} = A$. Since ρ is an algebra map we have $\rho(\sum b_0\gamma^{-1}(b_1)) = \sum \rho(b_0)\rho(\gamma^{-1}(b_1))$. By part (i), this becomes

$$\begin{aligned}
\sum \rho(b_0)\rho(\gamma^{-1}(b_1)) &= \sum(b_{00} \otimes b_{01})(\gamma^{-1}(b_{12} \otimes S(b_{11})) \\
&= \sum b_0\gamma^{-1}(b_3) \otimes b_1 S(b_2)
\end{aligned}$$

and it is easy to see that $\sum b_0\gamma^{-1}(b_3) \otimes b_1 S(b_2) = \sum b_0\gamma^{-1}(b_1) \otimes 1$. □

Proposition 5.24. *Let $A \subset B$ be an H-cleft extension. Then there exists a crossed product action $\cdot$ of H on A and a convolution invertible map $\sigma : H \otimes H \to A$ such that $B \cong A\#_\sigma H$ as left A-modules and right H-comodule algebras.*

Proof. Suppose that ρ is the structure map of B and $A \subset B$ is cleft via γ. We claim that H measures A via

$$h \cdot a = \sum \gamma(h_1)a\gamma^{-1}(h_2) \tag{5.2}$$

for $h \in H, a \in A$. This action is well defined because

$$\begin{aligned}
\rho(\sum \gamma(h_1)a\gamma^{-1}(h_2)) &= \sum(\rho\gamma(h_1))\rho(a)(\rho\gamma^{-1}(h_2)) \\
&= \sum(\gamma \otimes I)\Delta(h_1)\rho(a)(\rho\gamma^{-1}(h_2)), \text{ since } \gamma \text{ is } H\text{-comodule map} \\
&= \sum(\gamma \otimes I)\Delta(h_1)\rho(a)(\gamma^{-1} \otimes S)\tau\Delta(h_2), \text{ by Lemma 5.23, (1)} \\
&= \sum(\gamma(h_1) \otimes h_2)(a \otimes 1)(\gamma^{-1}(h_4) \otimes S(h_3)), \text{ since } a \in B^{coH} \\
&= \sum \gamma(h_1)a\gamma^{-1}(h_4) \otimes h_2S(h_3)
\end{aligned}$$

and the last line is $\sum \gamma(h_1)a\gamma^{-1}(h_2) \otimes 1$ which gives that $h \cdot a \in B^{coH} = A$. Next we observe that $h \cdot 1 = \sum \gamma(h_1)1\gamma^{-1}(h_2) = \varepsilon(h)1$. Moreover we have

$$\sum(h_1 \cdot a)(h_2 \cdot b) = \sum \gamma(h_1)a\gamma^{-1}(h_2)\gamma(h_3)b\gamma^{-1}(h_4)$$

and the right hand side can be simplified to $\sum \gamma(h_1)ab\gamma^{-1}(h_2)$. Hence our claim is proved.

We will now show that the map $\sigma : H \otimes H \to A$ given by

$$\sigma(h, k) = \sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2) \tag{5.3}$$

is the desired convolution invertible map. To verify that σ is well defined we look at the value $\rho(\sigma(h, k))$ and compute it as follows.

$$\begin{aligned}
\rho(\sigma(h, k)) &= \rho(\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2)) \\
&= \sum \rho(\gamma(h_1))\rho(\gamma(k_1))\rho(\gamma^{-1}(h_2k_2)) \\
&= \sum(\gamma \otimes I)\Delta(h_1)(\gamma \otimes I)\Delta(k_1)(\gamma^{-1} \otimes S)\tau\Delta(h_2k_2)
\end{aligned}$$

by Lemma 5.23, part (i) and using that γ is an H-comodule map. The last line can be rewritten as $\sum \gamma(h_{11})\gamma(k_{11})\gamma^{-1}(h_{22}k_{22}) \otimes h_{12}k_{12}S(h_{21}k_{21})$ and even in a more compact form like $\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_4k_4) \otimes h_2k_2S(k_3)S(h_3)$. We can replace $k_2S(k_3)$ by $\varepsilon(k_2)$ in this sum and reduce it to $\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_4k_3) \otimes h_2\varepsilon(k_2)S(h_3)$. It now becomes apparent that this sum is $\sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2) \otimes 1$ after similar successive steps. Hence $\sigma(h,k) \in B^{coH} = A$ and σ is well defined.

We claim that σ is convolution invertible with inverse

$$\sigma^{-1}(h,k) = \sum \gamma(h_1k_1)\gamma^{-1}(k_2)\gamma^{-1}(h_2). \tag{5.4}$$

Note that $\sigma * \sigma^{-1}(h,k) = \sum \sigma(h_1,k_1)\sigma^{-1}(h_2,k_2)$. Using (5.4) and (5.3) yields

$$\sigma * \sigma^{-1}(h,k) = \sum \gamma(h_1)\gamma(k_1)\gamma^{-1}(h_2k_2)\gamma(h_3k_3)\gamma^{-1}(k_4)\gamma^{-1}(h_4)$$

and one can show that this is $\varepsilon(h)\varepsilon(k)1$. Similarly $\sigma^{-1} * \sigma(h,k) = 1_{Hom(H\otimes H,A)}$.

In this case $A\#_\sigma H$ is associative algebra with unit. We check only the twisted module condition since cocycle condition can be checked similarly. By Remark 5.22, we assume that $\gamma(1) = 1 = \gamma^{-1}(1)$ so we have $1 \cdot a = \sum \gamma(1)a\gamma^{-1}(1) = a$. Moreover for $h, g \in H$ and $a \in A$ using (5.3) and (5.4) we see that

$$h \cdot (g \cdot a) = \sum \gamma(h_1)\gamma(g_1)a\gamma^{-1}(g_2)\gamma^{-1}(h_2).$$

On the other hand,

$$\begin{aligned}
&\sum \sigma(h_1,g_1)(h_2g_2 \cdot a)\sigma^{-1}(h_3,g_3) \\
&\qquad = \sum \gamma(h_1)\gamma(g_1)\gamma^{-1}(h_2g_2)\gamma(h_3g_3)a\gamma^{-1}(h_4g_4)\gamma(h_5,g_5)\gamma^{-1}(g_6)\gamma^{-1}(h_6) \\
&\qquad = \sum \gamma(h_1)\gamma(g_1)\gamma^{-1}(h_2g_2)\gamma(h_3\varepsilon(h_4)g_3\varepsilon(g_4))a\gamma^{-1}(g_5)\gamma^{-1}(h_5) \\
&\qquad = \sum \gamma(h_1)\gamma(g_1)\gamma^{-1}(h_2g_2)\gamma(h_3g_3)a\gamma^{-1}(g_4)\gamma^{-1}(h_4) \\
&\qquad = \sum \gamma(h_1\varepsilon(h_2))\gamma(g_1\varepsilon(g_2))a\gamma^{-1}(g_3)\gamma^{-1}(h_3) \\
&\qquad = \sum \gamma(h_1)\gamma(g_1)a\gamma^{-1}(g_2)\gamma^{-1}(h_2)
\end{aligned}$$

which proves that A is twisted H-module.

Finally we will show that the map $\phi : A\#_\sigma H \to B$, $a\#h \mapsto a\gamma(h)$ is an isomorphism of left A-modules and right H-comodule algebras. It is straightforward to see that ϕ is a morphism of such structures. Therefore we only show that $\psi : B \to A\#_\sigma H$ defined by $b \mapsto \sum b_0\gamma^{-1}(b_1)\#b_2$ is inverse to ϕ. Observe that Lemma 5.23, (ii) guarantees that ψ is well defined. For $b \in B$, we have $\phi\psi(b) = \sum b_0\gamma^{-1}(b_1)\gamma(b_2) = \sum b_0\varepsilon(b_1) = b$. Also if $a\#h \in A\#_\sigma H$, then $\psi\phi(a\#h) = \sum a_0\gamma(h)_0\gamma^{-1}(a_1\gamma(h)_1)\#a_2\gamma(h)_2$. But since $a \in B^{coH}$, we have $\sum a_0 \otimes a_1 \otimes a_2 = \sum a \otimes 1 \otimes 1$.

Hence $\psi\phi(a\#h) = \sum a\gamma(h)_0\gamma^{-1}(\gamma(h)_1)\#\gamma(h)_2$. As γ is an H-comodule map we get

$$\begin{aligned}\sum a\gamma(h)_0\gamma^{-1}(\gamma(h)_1)\#\gamma(h)_2 &= \sum a\gamma(h_1)\gamma^{-1}(h_2)\#h_3\\ &= \sum a\#\varepsilon(h_1)h_2\\ &= a\#h\end{aligned}$$

which proves that ϕ is a bijection. □

Proposition 5.25. *An associative crossed product $A\#_\sigma H$ with identity is a cleft H-comodule algebra.*

Proof. We have seen in Lemma 5.20 that $A\#_\sigma H$ is a right H-comodule algebra with $(A\#_\sigma H)^{coH} = A\#_\sigma 1 \cong A$. We claim that $A \hookrightarrow A\#_\sigma H$ is cleft via $\gamma : H \to A\#_\sigma H$ given by $\gamma(h) = 1\#h$. To prove this we will show that $\mu : H \to A\#_\sigma H$ defined by

$$\mu(h) = \sum \sigma^{-1}(S(h_2), h_3)\#S(h_1)$$

is inverse to γ with respect to convolution. For $h \in H$,

$$(\mu * \gamma)(h) = \sum[\sigma^{-1}(S(h_2), h_3)\#S(h_1)][1\#h_4]$$

and multiplication in crossed products gives

$$(\mu * \gamma)(h) = \sum \sigma^{-1}(S(h_2), h_3)(S(h_1)_1 \cdot 1)\sigma(S(h_1)_2, h_{41})\#S(h_1)_3 h_{42}.$$

By Corollary 3.7 we obtain

$$\begin{aligned}(\mu * \gamma)(h) &= \sum \sigma^{-1}(S(h_2), h_3)(S(h_{13}) \cdot 1)\sigma(S(h_{12}), h_{41})\#S(h_{11})h_{42} \\ &= \sum \sigma^{-1}(S(h_4), h_5)(S(h_3) \cdot 1)\sigma(S(h_2), h_6)\#S(h_1)h_7.\end{aligned}$$

Since H measures A and, S is an antimorphism of coalgebras the last line of above equality becomes $\sum \sigma^{-1}(S(h_4), h_5)\varepsilon(h_3)\sigma(S(h_2), h_6)\#S(h_1)h_7$. Using linearity of σ and S respectively, this sum is the same as $\sum \sigma^{-1}(S(h_4), h_5)\sigma(S(h_2\varepsilon(h_3)), h_6)\#S(h_1)h_7$ which can be easily simplified to $1\#\varepsilon(h)1$. Hence μ is a left inverse for γ.

Next we show that μ is also a right inverse. For $h \in H$

$$(\gamma * \mu)(h) = \sum 1(h_1 \cdot \sigma^{-1}(S(h_5), h_6))\sigma(h_2, S(h_4)_1)\#h_3 S(h_4)_2$$

and using similar arguments as above this reduces to

$$\sum 1(h_1 \cdot \sigma^{-1}(S(h_4), h_5))\sigma(h_2, S(h_3))\#1. \tag{5.5}$$

In order to further reduce it and obtain $\varepsilon(h)1\#1$, we need a connection between the crossed product action and σ^{-1}. Observe that using cocycle condition one gets that

$$h \cdot \sigma(k, m) = \sum \sigma(h_1, k_1)\sigma(h_2 k_2, m_1)\sigma^{-1}(h_3, k_3 m_2). \tag{5.6}$$

Moreover since H measures A, we have

$$\begin{aligned}\sum(h_1\cdot\sigma^{-1}(k_1,m_1))(h_2\cdot\sigma(k_2,m_2)) &= \sum h\cdot(\sigma^{-1}(k_1,m_1)\sigma(k_2,m_2))\\ &= \sum h\cdot(\varepsilon(k)\varepsilon(m)1)\\ &= \varepsilon(k)\varepsilon(m)(h\cdot 1)\\ &= \varepsilon(k)\varepsilon(m)\varepsilon(h)1.\end{aligned}$$

Hence we find that

$$h\cdot\sigma^{-1}(k,m)=\sum\sigma(h_1,k_1m_1)\sigma^{-1}(h_2k_2,m_2)\sigma^{-1}(h_3,k_3).$$

Using this, the sum in (5.5) is

$$\sum 1(h_1\cdot\sigma^{-1}(S(h_4),h_5)\sigma(h_2,S(h_3))\#1.$$

If we apply the equality (5.6) this becomes

$$\sum\sigma(h_{11},S(h_4)_1h_{51})\sigma^{-1}(h_{12}S(h_4)_2,h_{52})\sigma^{-1}(h_{13},S(h_4)_3)\sigma(h_2,S(h_3))$$

which can be reduced to $\varepsilon(h)1$. □

By previous two propositions we obtained the following characterization of crosssed products.

Theorem 5.26. *An H-extension $A\subset B$ is H-cleft iff $B\cong A\#_\sigma H$.*

5.3. Hopf Galois Extensions

For the surveys regarding Hopf Galois extensions, the reader is referred to [13] and [14].

Definition 5.27. *Let H be a Hopf algebra and A be a right H-comodule algebra with structure map $\rho : A\to A\otimes H, a\mapsto\sum a_0\otimes a_1$. We define the canonical map β :*

$A \otimes_{A^{coH}} A \to A \otimes H$ by $\beta(a \otimes b) = \sum ab_0 \otimes b_1$. Then the extension $A^{coH} \subset A$ is said to be Galois *(or A is* right H-Galois*) if β is bijective.*

Note that in this definition, bijectivity of β is not equivalent to bijectivity of $\beta' : A \otimes_{A^{coH}} A \to A \otimes H, a \otimes b \mapsto \sum a_0 b \otimes a_1$. However when the antipode of H is bijective we have the following proposition.

Proposition 5.28. *If the antipode S is bijective then*

(i) β is bijective iff β' is bijective
(ii) β is injective iff β' is injective
(iii) β is surjective iff β' is surjective.

Proof. We define a map $\phi : A \otimes H \to A \otimes H$, by $\phi(a \otimes h) = \rho(a)(1 \otimes S(h))$ for $a \in A, h \in H$. Then

$$\begin{aligned}
\phi\beta(a \otimes b) &= \sum a_0 b_{00} \otimes a_1 b_{01} S(b_1) \\
&= \sum a_0 b_0 \otimes a_1 b_1 S(b_2) \\
&= \sum a_0 b_0 \varepsilon(b_1) \otimes a_1 \\
&= \sum a_0 b \otimes a_1 \\
&= \beta'(a \otimes b)
\end{aligned}$$

for any $a, b \in A$. Now it suffices to show that ϕ is invertible. We claim that $\psi(a \otimes h) := (1 \otimes S^{-1}(h))\rho(a)$ is inverse to ϕ. Indeed we have

$$\begin{aligned}
\phi\psi(a \otimes h) &= \sum a_{00} \otimes a_{01} S(S^{-1}(h) a_1) \\
&= \sum a_0 \otimes a_1 S(a_2) S S^{-1}(h) \\
&= \sum a_0 \varepsilon(a_1) \otimes h \\
&= a \otimes h
\end{aligned}$$

and similarly $\psi\phi = I$ which proves that ϕ is bijective. □

Classical Galois extensions of fields can be considered as right H-Galois extensions for suitable Hopf algebras. The next Proposition explains this in detail.

Proposition 5.29. *Let $k \subset E$ be a field extension with intermediate field F. Suppose that G is a finite group which acts as k-automorphisms on E. Then $F \subset E$ is classically Galois with $Gal(E/F) = G$ iff E is a right $(kG)^*$-Galois with $E^{co(kG)^*} = F$.*

Proof. First suppose that $F \subset E$ is classically Galois with Galois group G. Then $[E : F] = |G|$. Since G acts on E we know by Proposition 5.11 that $(kG)^*$ coacts on E via $\rho(a) = \sum_{i=1}^{n}(x_i \cdot a) \otimes p_i$ where $G = \{x_1, ..., x_n\}$ and $p_i(x_j) = \delta_{i,j}x_j$. In this case we also have

$$\begin{aligned} E^{co(kG)^*} = \{e \in E \mid \rho(e) = e \otimes 1\} &= \{e \in E \mid \sum_{i=1}^{n}(x_i \cdot e) \otimes p_i = e \otimes \sum_{i=1}^{n} p_i\} \\ &= \{e \in E \mid x_i \cdot e = e \ \forall i\} \\ &= E^G \end{aligned}$$

and we know that $E^G = F$ since the extension is Galois. Hence $E^{co(kG)^*} = F$ and the Galois map $\beta : E \otimes_F E \to E \otimes_k (kG)^*$ is given by $\beta(a \otimes b) = \sum_i a(x_i \cdot b) \otimes p_i$. Suppose that $\{v_1, ..., v_n\}$ is a basis of E over F. If $\sum a_j \otimes v_j \in Ker\beta$, then $\sum_{j,k} a_j(x_k \cdot v_j) \otimes p_k = 0$. But since $\{p_k\}_k$ form a basis $\sum_j a_j(x_k \cdot v_j) = 0$ for every k. Then by independence of automorphisms $a_j = 0$ for all j. So $\sum a_j \otimes v_j = 0$ and β is injective. But the Galois map β is F-linear and $dim_F(E \otimes_F E) = dim_F(E \otimes (kG)^*) = n^2$ yield that β is bijective.

Conversely suppose that $F \subset E$ is a right $(kG)^*$-comodule algebra with structure map $\rho(a) = \sum_{h \in G} a_h \otimes p_h$ and $F = E^{co(kG)^*}$ where $\{p_h\}_{h \in G}$ is the dual basis. If β is bijective, then $dim_F(E \otimes_F E) = [E : F]^2$ and $dim_F(E \otimes_k (kG)^*) = [E : F]|G|$. Hence it follows that $[E : F] = |G|$ and $F \subset E$ is classically Galois. Also G acts on E as in Proposition 5.11. That is $g \cdot a = \sum_h < p_h, g > a_h = a_g$. Then we get

$$\begin{aligned} E^G = \{a \in E \mid g \cdot a = a \ \forall g \in G\} &= \{a \in E \mid a_g = a \ \forall g \in G\} \\ &= \{a \in E \mid \rho(a) = a \otimes \sum_{h \in G} p_h\}. \end{aligned}$$

But since $\sum_{h\in G} p_h = 1$ we get $E^G = E^{co(kG)^*}$. Hence $E^G = F$, which gives that $Gal(E/F) = G$. $\square$

Example 5.30. *Let H be a Hopf algebra and consider right H-comodule algebra structure on H as in Example* 5.10. *Then the Galois map β is given by $\beta(h\otimes g) = \sum hg_1\otimes g_2$. We show that $\psi(h\otimes g) := \sum hS(g_1)\otimes g_2$ is inverse to β so that $H^{coH} \subset H$ is Galois. Indeed we have*

$$\begin{aligned}\psi\beta(h\otimes g) = \sum hg_1S(g_{21})\otimes g_{22} &= \sum hg_1S(g_2)\otimes g_3\\ &= \sum h\otimes \varepsilon(g_1)g_2\\ &= h\otimes g\end{aligned}$$

and similarly $\beta\psi(h\otimes g) = h\otimes g$.

Example 5.31. *We will see later that $(A\#_\sigma H)^{coH} \cong A \hookrightarrow A\#_\sigma H$ is Galois. In fact the inverse of the Galois map β is given by $\beta^{-1}((a\#h)\otimes k) = \sum(a\#h)\gamma^{-1}(k_1)\otimes\gamma(k_2)$ where γ is the map defined in Proposition* 5.25.

The following theorem investigates Galois extensions in graded algebras.

Theorem 5.32. *Let A be a G-graded algebra. Then $A_1 \subset A$ is kG-Galois iff A is strongly graded.*

Proof. Recall first from Proposition 5.14 that a G-graded algebra A is a kG-comodule algebra via $\rho(a) = \sum_{g\in G} a_g\otimes g$ and $A^{cokG} = A_1$. Then the Galois map $\beta : A\otimes_{A_1} A \to A\otimes_k kG$ is given by $\beta(a\otimes b) = \sum_g ab_g\otimes g$. Suppose that A is strongly graded. For each $g\in G$, we may write $1 = \sum b_ic_i$ where $b_i \in A_{g^{-1}}, c_i\in A_g$ since we know that $1\in A_1 = A_g^{-1}A_g$. We define $\alpha : A\otimes kG \to A\otimes_{A_1} A, a\otimes g\mapsto \sum ab_i\otimes c_i$ where b_i's and c_i's are determined by g as above. Then we have

$$\begin{aligned}\beta\alpha(a\otimes g) = \beta(\sum_i ab_i\otimes c_i) &= \sum_{h,i} ab_i(c_i)_h\otimes h\\ &= \sum_i ab_ic_i\otimes g, \text{ since } c_i\in A_g\\ &= a\otimes g, \text{ since} \sum b_ic_i = 1.\end{aligned}$$

Also

$$\alpha\beta(a \otimes g) = \alpha(\sum_g ab_g \otimes g) = \sum_{g,i} ab_g c_i^g \otimes d_i^g$$

where $\sum c_i^g d_i^g = 1$ such that $c_i^g \in A_{g^{-1}}$ and $d_i^g \in A_g$ for every i. But since $b_g \in A_g$ and $c_i^g \in A_g^{-1}$ we get that $b_g c_i^g \in A_1$. Then the above sum is $\sum_{g,i} a \otimes b_g c_i^g d_i^g$ since the tensor is over A_1. Hence it follows that

$$\sum_{g,i} a \otimes b_g c_i^g d_i^g = \sum_g a \otimes b_g = a \otimes b$$

which shows that the Galois map β is bijective.

Conversely if $A_1 \subset A$ is kG-Galois then, surjectivity of β gives for every $g \in G$,

$$\sum_{i,h} a_i(b_i)_h \otimes h = 1 \otimes g$$

for some $a_i, b_i \in A$. Since the set G forms a basis for kG it follows that $\sum_i a_i(b_i)_g = 1$ and $\sum_i a_i(b_i)_h = 0$ for all $h \neq g$. But as A is the direct sum of its homogenous components we may assume that $a_i(b_i)_g \in A_1$ for every i. For a fixed i, this means that $a_i(b_i)_g = (a_i(b_i)_g)_1 = \sum_{kj=1} a_{ik}(b_i)_{gj} = (a_i)_{g^{-1}}(b_i)_g$. Hence we may also assume that $a_i \in A_{g^{-1}}$ whence the result follows. □

Example 5.33. *Let G be a finite group acting on the set X. Let $A = k^X$ denote the algebra of functions from X to k. We consider the Hopf algebra $H = k^G \cong (kG)^*$. The action of G on X gives a left G-action on A as follows.*

$$g \cdot a(x) = a(x \cdot g) \tag{5.7}$$

Then, by Lemma 5.11*, A becomes a right H-comodule algebra via*

$$\rho : A \longrightarrow A \otimes H$$

$$a \longmapsto \textstyle\sum_{g\in G} a \cdot g \otimes \delta_g.$$

*Observe that the map $\alpha : X \times G \to X \times X$ given by $(x, g) \mapsto (x, x \cdot g)$ is injective iff $x \cdot g = x \cdot h$ implies that $g = h$. But this occurs iff $x = x \cdot hg^{-1}$ implies that $1 = hg^{-1}$. Hence α is injective iff the action is free. Now, let $X \times_Y X = Im(\alpha)$ where $Y = X/G$. Suppose that B is the algebra of functions from X to k which are constant on G-orbits. Then, $B = A^G$ by equation (*5.7*). But we already know by Theorem* 5.11 *that $A^G = A^{coH}$. Hence we have that $B = A^{coH}$.*

The map α dualizes to

$$\alpha^* : (X \times X)^* \to (X \times G)^*$$

and, using the isomorphism $k^{S\times T} \cong k^S \otimes k^T$ for arbitrary sets S and T one obtains a map $\kappa : A \otimes_B A \to A \otimes H$.

For any $a, b \in A$, $x \in X$ and $g \in G$ we have that

$$\begin{aligned}
\kappa(a \otimes b)(x, g) &= f\alpha(x, g) \text{ where } f(z, t) = a(z) \otimes b(t) \\
&= f(x, x \cdot g) \\
&= a(x) \otimes b(x \cdot g) \\
&= a(x)b(x \cdot g) \otimes 1 \\
&= a(x)(g \cdot b)(x) \otimes 1 \\
&= a(g \cdot b)(x) \otimes \delta_g(g) \text{ by pointwise multiplication in } A \\
&= \left(\sum a(g \cdot b) \otimes \delta_g\right)(x, g) \\
&= (a \otimes 1)\rho(b)
\end{aligned}$$

which shows that κ is the Galois map. Clearly, $\alpha : X \times G \to X \times_Y X$ is bijective iff α is injective. But, by our initial observation the latter holds iff the action is free.

5.4. Galois Extensions with Normal Basis Property

Let $F \subset E$ be a finite Galois extension of fields with Galois group G. Then the extension has a normal basis. In other words, there exists $a \in E$ such that the set $\{x \cdot a \mid x \in G\}$ forms a basis for E over F. We will consider this property for H-extensions. See [2] for applications of this property to p-groups of automorphisms, derivations, and higher derivations of an algebra over a ring of characteristic p.

Definition 5.34. *A right H-extension $A \subset B$ has the right normal basis property if $B \cong A \otimes H$ as left A-modules and right H-comodules.*

The following Lemma shows that the above definition corresponds to usual definition.

Lemma 5.35. *Let H be a finite dimensional Hopf algebra and let $A \subset B$ be an H extension. Then B has a normal basis over A in the usual sense iff $B \cong A \otimes H$ as in above definition.*

Proof. Suppose that $dim H = n < \infty$. Since B is a right H-comodule algebra with $B^{coH} = A$, it follows by Proposition 5.15 that B is a left H^* algebra with $B^{H^*} = A$. So we think as H^* acts on B with $(Gal_A^B)' = A$. First assume that $\{f_1 \cdot b, ..., f_n \cdot b\}$ is a basis for B for some $b \in B$ where $\{f_i\}_i$ is a basis of H^*. We know by Theorem 4.26 that there is a nonzero $\varphi \in \int_{H^*}^{l}$ such that

$$\alpha : H \longrightarrow H^*$$

$$h \longmapsto (h \rightharpoonup \varphi)$$

is a left linear isomorphism. We define the map

$$\phi : A \otimes H \longrightarrow B$$

$$a \otimes h \longmapsto a((h \rightharpoonup \varphi) \cdot b)$$

Now since $\{f_1 \cdot b, ..., f_n \cdot b\}$ is a basis, ϕ is a left H^*-module map. Hence ϕ is a right H-comodule map. It is clear that ϕ is a left A-module isomorphism. Thus $A \otimes H \cong B$ as left A-modules.
Conversely suppose that $A \otimes H \cong B$ and let $\{f_1, ..., f_n\}$ be a basis for H^*. Then the set $\{1 \otimes \alpha^{-1}(f_1), ..., \alpha^{-1}(f_n)\}$ is an A basis for $A \otimes H$. Now if $\gamma : A \otimes H \to B$ is an isomorphism of left A-modules, then $\{f_1 \cdot \gamma(1 \otimes \alpha^{-1}(\varphi)), \ldots , f_n \cdot \gamma(1 \otimes \alpha^{-1}(\varphi))\}$ is an A-basis for B. □

We will now characterize the Galois extensions with normal basis property as cleft extensions (or as crossed products).

Theorem 5.36. *Let $A \subset B$ be an H-extension. Then the followings are equivalent.*

- *(i) $A \subset B$ is H-Galois and has the normal basis property.*
- *(ii) $A \subset B$ is H-cleft.*
- *(iii) $B \cong A\#_\sigma H$ as left A-modules and right H-comodules.*

Proof. We have seen the equivalence of (ii) and (iii) in Theorem 5.26. So it remains to show the equivalence of (i) to one of the other statements.

$(iii) \Rightarrow (i)$: First suppose that (iii) holds so that by Lemma 5.35, the normal basis property is satisfied. To prove that the extension is Galois we need an inverse α for the Galois map

$$\beta : B \otimes_A B \longrightarrow B \otimes_k H$$

$$a \otimes b \longmapsto (a \otimes 1)\rho(b).$$

Let the extension $A \subset B$ be cleft via the convolution invertible map $\gamma : H \to B$. We define

$$\alpha : B \otimes_k H \longrightarrow B \otimes_A B$$

$$b \otimes h \longmapsto \sum b\gamma^{-1}(h_1) \otimes \gamma(h_2)$$

and claim that it is inverse to β. Indeed we have

$$\begin{aligned}
\beta\alpha(b \otimes h) &= \beta(\sum b\gamma^{-1}(h_1) \otimes \gamma(h_2)) \\
&= \sum (b\gamma^{-1}(h_1) \otimes 1)(\rho\gamma(h_2)) \\
&= \sum (b\gamma^{-1}(h_1) \otimes 1)(\gamma(h_{21}) \otimes h_{22}) \text{ since } \gamma \text{ is a right } H\text{-comodule map} \\
&= \sum b\gamma^{-1}(h_1)\gamma(h_2) \otimes h_3 \\
&= \sum b\varepsilon(h_1) \otimes h_2 \\
&= \sum b \otimes \varepsilon(h_1)h_2 \\
&= b \otimes h
\end{aligned}$$

and conversely

$$\begin{aligned}
\alpha\beta(a \otimes b) &= \alpha(\sum ab_0 \otimes b_1) \\
&= \sum ab_0\gamma^{-1}(b_{11}) \otimes \gamma(b_{12}) \\
&= \sum ab_0\gamma^{-1}(b_1) \otimes \gamma(b_2) \\
&= \sum a \otimes_A b_0\gamma^{-1}(b_1)\gamma(b_2) \text{ by Lemma 5.23 and using } B^{coH} = A \\
&= \sum a \otimes b_0\varepsilon(b_1) \\
&= a \otimes b.
\end{aligned}$$

Hence we conclude that $A \subset B$ is H-Galois.

$(i) \Rightarrow (ii)$: Now assume that the extension $A \subset B$ is Galois so that the Galois map β is bijective. Also assume that $\phi : A \otimes H \to B$ is a left A-module and right

H-comodule isomorphism. We define a map

$$\gamma : H \longrightarrow B$$

$$h \longmapsto \phi(1 \otimes h)$$

and claim that it is a convolution invertible H-comodule map. First note that since ϕ is a right H-comodule map, for all $a \in A, h \in H$ we have

$$[\phi(a \otimes h)]_0 \otimes [\phi(a \otimes h)]_1 = \phi(a \otimes h_1) \otimes h_2.$$

In particular, for all $h \in H$,

$$[\phi(1 \otimes h)]_0 \otimes [\phi(1 \otimes h)]_1 = \phi(1 \otimes h_1) \otimes h_2$$

which is equivalent to the commutatvity of

$$\begin{tikzcd} H \arrow[r, "\gamma"] \arrow[d, "\Delta"'] & B \arrow[d, "\rho"] \\ H \otimes H \arrow[r, "\gamma \otimes I"'] & B \otimes H. \end{tikzcd}$$

Hence γ is a right H-comodule map. Now let $g \in Hom_A(B, A)$ be defined by $g := m(I \otimes \varepsilon)\phi^{-1}$ where m denotes the isomorphism $A \otimes k \to A$. We claim then that

$$\mu(h) := m(I \otimes g)\beta^{-1}(1 \otimes h)$$

is inverse to γ with respect to convolution. Before proceeding further we make three observations in order. Firstly, for any $h \in H$

$$g(\gamma(h)) = m(I \otimes \varepsilon)\phi^{-1}\gamma(h) = m(I \otimes \varepsilon)(1 \otimes h) = \varepsilon(h)1 \tag{5.8}$$

Secondly, for any $b, c \in B$ we have that

$$\begin{aligned}(I \otimes \Delta)\beta(b \otimes c) &= (I \otimes \Delta) \sum bc_0 \otimes c_1 \\ &= \sum bc_0 \otimes c_{11} \otimes c_{12} \\ &= \sum bc_0 \otimes c_{01} \otimes c_1 \\ &= (\beta \otimes I)(I \otimes \rho)(b \otimes c).\end{aligned}$$

In other words

$$(I \otimes \Delta)\beta = (\beta \otimes I)(I \otimes \rho). \tag{5.9}$$

Since β is invertible the equation (5.9) becomes

$$(\beta^{-1} \otimes I)(I \otimes \Delta) = (I \otimes \rho)\beta^{-1} \tag{5.10}$$

Now for any $h \in H$, putting $\beta^{-1}(1 \otimes h) := \sum_i a_i \otimes b_i$ gives that

$$(I \otimes \rho)\beta^{-1}(1 \otimes h) = \sum_i a_i \otimes b_{i0} \otimes b_{i1}$$

and

$$(\beta^{-1} \otimes I)(I \otimes \Delta)(1 \otimes h) = \sum \beta^{-1}(1 \otimes h_1) \otimes h_2.$$

Applying equation (5.10) to above equalities one gets

$$\sum_i a_i \otimes b_{i0} \otimes b_{i1} = \sum \beta^{-1}(1 \otimes h_1) \otimes h_2. \tag{5.11}$$

And lastly we note that for any $b \in B$, $b = \sum g(b_0)\gamma(b_1)$. This can be seen as follows:

$$\begin{aligned}
\sum g(b_0)\gamma(b_1) &= \sum m(I \otimes \varepsilon)\phi^{-1}(b_0)\gamma(b_1) \\
&= \sum \underbrace{m(I \otimes \varepsilon)\phi^{-1}(b_0)}_{\in A}\phi(1 \otimes b_1) \\
&= \sum \phi(m(I \otimes \varepsilon)\phi^{-1}(b_0) \otimes b_1) \text{ since } \phi \text{ is left } A\text{-module map} \\
&= \sum \phi([m(I \otimes \varepsilon) \otimes I][\phi^{-1} \otimes I]\rho(b)) \\
&= \sum \phi(m(I \otimes \varepsilon) \otimes I)(I \otimes \Delta)\phi^{-1}(b) \text{ since } \phi^{-1} \text{ is right } H\text{-comodule map} \\
&= \phi(I\phi^{-1}(b)) \text{ by counit property} \\
&= b.
\end{aligned} \tag{5.12}$$

We now turn back to proving that μ is inverse to γ with respect to convolution. We compute that

$$\begin{aligned}
(\gamma * \mu)(h) &= \sum \gamma(h_1)m(I \otimes g)\beta^{-1}(1 \otimes h_2) \\
&= \sum m(I \otimes g)\beta^{-1}(\gamma(h_1) \otimes h_2) \\
&= \sum m(I \otimes g)(\beta^{-1}(\rho\gamma(h)) \text{ since } \gamma \text{ is } H\text{-comodule map} \\
&= \sum m(I \otimes g)(\beta^{-1}\beta(1 \otimes \gamma(h))) \text{ by definition of } \beta \\
&= \sum m(I \otimes g)(1 \otimes \gamma(h)) \\
&= m(1 \otimes \varepsilon(h)) \text{ by equation (5.8)} \\
&= \varepsilon(h)1.
\end{aligned}$$

Finally we verify that μ is a left inverse to γ.

$$\begin{aligned}(\mu * \gamma)(h) &= \sum [m(I \otimes g)\beta^{-1}(1 \otimes h_1)]\gamma(h_2) \\ &= \sum [m(I \otimes g)(\sum a_i \otimes b_{i0})]\gamma(b_{i1}) \text{ by equation (5.11)} \\ &= \sum [m(\sum a_i \otimes g(b_{i0}))]\gamma(b_{i1}) \\ &= \sum [\sum a_i g(b_{i0})]\gamma(b_{i1}) \\ &= \sum a_i \sum g(b_{i0})\gamma(b_{i1}) \\ &= \sum a_i b_i \text{ by equation (5.12)} \\ &= \varepsilon(h)1 \text{ since } \beta^{-1}(1 \otimes h) = \sum a_i \otimes b_i \text{ and } (I \otimes \varepsilon)\beta = m\end{aligned}$$

which completes the proof.

□

REFERENCES

1. Chase, S. U. and M. E. Sweedler, *Hopf algebras and Galois theory*, Springer, Berlin, 1969.

2. Kreimer, H. F. and M. Takeuchi, "Hopf algebras and Galois extensions of an algebra", *Indiana University Mathematics Journal*, Vol. 30, pp. 675–692, 1981.

3. Durdevic, M., *Quantum principal bundles as Hopf Galois extensions*, arXiv:q-alg/9507022vl, 1995.

4. Schneider, H. J., "Principal homogeneous spaces for arbitrary Hopf algebras", *Israel Journal of Mathematics*, Vol. 72, pp. 167–195, 1990.

5. Wisbauer, R., *Coalgebras and bialgebras*, Lectures given at Cairo University and The American University in Cairo, Düsseldorf, Germany, 2004.

6. Dăscălescu, S., C. Năstăsescu and Ş. Raianu, *Hopf algebras, an introduction*, Marcel Dekker, New York–Basel, 2001.

7. Montgomery, S., *Hopf algebras and their actions on rings*, American Mathematical Society, Rhode Island–Providence, 1993.

8. Cohen, M., S. Gelaki and S. Westreich, "Hopf algebras", *Handbook of Algebra*, Vol. 4, pp. 173–239, 2006,.

9. Larson, R.G. and M.E. Sweedler, "An associative orthogonal bilinear form for Hopf algebras", *American Journal of Mathematics*, Vol. 91, pp. 75–93, 1969.

10. Schneider, H. J., , *Lectures on Hopf algebras*, Trabajos de Matemática, Córdoba, 1995.

11. Blattner, R. J. and S. Montgomery, "Crossed products and Galois extensions of

Hopf algebras", *Pacific Journal of Mathematics*, Vol. 137, pp. 37–54, 1989.

12. Sweedler, M. E., "Cohomology of algebras over Hopf algebras", *Transactions of the American Mathematical Society*, Vol. 133, pp. 205–239, 1968.

13. Montgomery, S., "Hopf Galois theory: a survey", in A. Baker and B. Richter (eds.), *New Topological Contexts for Galois Theory and Algebraic Geometry*, BIRS, 2008, Geometry and Topology Monographs, Coventry, 2009.

14. Schauenburg, P., "Hopf bi-Galois extensions", *Communications in Algebra*, Vol. 24, No. 12, pp. 3797–3825, 1996.