UNIVERSITY
of
GLASGOW

DEPARTMENT
of
MATHEMATICS

Homological Properties of Hopf Algebras

Ji-Hyang Lee

Dissertation Submitted for the Degree of Master of Science
in Mathematics to the University of Glasgow

October 2000

Declaration

The composition and structure of this thesis are my own; however, I do not claim to prove any original work during the course of the dissertation.

To In-Ju

Acknowledgements

My thanks go to my supervisor, Professor Kenneth Brown, for much help and advice. I would also like to thank Sophie Huczynska for help with Galois theory and for being a good friend in times of need!

I would especially like to thank my family, who have unfailingly supported and encouraged me in ways too numerous to mention and have patiently tolerated much ingratitude and ill-temper from me. I can only offer them my heartfelt thanks for everything they have done: I wouldn't have made it without you!

Finally, many thanks to John-Philip Hagemeister, who taught me LaTeX, and who has brightened up my life with a judicious mixture of hugs and his own (unique) brand of humour.

Summary

The main aim of this dissertation is to prove a version of the result [Bro98, Proposition 2.3], following the outline suggested in that paper. This result has a distinctly homological flavour, and unsurprisingly relies quite heavily on homological algebra for its proof. We have also drawn upon a wider variety of mathematical techniques, mostly ring theory and Hopf algebraic methods in our discussion. As by-products of the proof, we get a condition for Galois extensions and Frobenius extensions to be equivalent, and also a generalisation of a well-known theorem by Larsson and Sweedler. We discuss this in more detail below.

We state the proposition:

Proposition. *We let H be a Noetherian* $\mathbf{k}$*-Hopf algebra, where* $\mathbf{k}$ *is an algebraically closed field. Let K be a central affine sub-Hopf algebra of H with*

$$inj.dim_K(K) = Krull\ dim(K) = m.$$

Suppose further that H is a finitely generated K-module. Then

$$inj.dim_K(H) = inj.dim_K(K) = m.$$

Throughout this thesis, inj.dim refers to the injective dimension of the module (defined in Definition 3.2) and Krull dim is the Krull dimension of a commutative Noetherian ring which we also define in Definition 3.2. We also note the fact that if a commutative Noetherian ring has finite injective dimension, then inj.dim$(-)$ = Krull dim$(-)$, as above. The proof is split into four parts, which we summarise briefly here. In the first part, we show that for any ring R which is a Frobenius extension over a subring S the injective dimension of S as a module over itself is equal to the injective dimension of R as an S-module. Proof of this is obtained from Nakayama and Tsuzuku's fundamental paper ([NT60]) and some basic facts about projective modules. In the second part, we prove that, in the notation above, H is Frobenius over K.

This requires that we show H to be a Galois extension over K, which requires substantial preparation as discussed in Chapter 2. The key results come from Kreimer and Takeuchi's paper [KT81] and a paper by Schneider [Sch93]. This step also generalises the Larsson and Sweedler result mentioned before, which states that any finite-dimensional Hopf algebra is Frobenius over any sub-Hopf algebra. The third part shows that K is a Gorenstein ring. The fourth part uses some simple facts on projective modules to place the required restriction on the injective dimension of H as an H-module. These steps, taken together, prove the proposition. This proof is contained in the second section of Chapter 4.

Chapter 1 is concerned with the basic definition of a Hopf algebra and discusses some of their basic properties, including comodules, invariants and coinvariants, and smash products. We also introduce Sweedler's sigma notation and use it to describe many Hopf algebraic properties.

As indicated above, Chapter 2 contains the majority of the results needed to prove the proposition. We begin by defining and discussing normal sub-Hopf algebras and establish two key results which give an if and only if condition for a sub-Hopf algebra to be normal. This forms part of the proof of the proposition. The main point of the chapter, however, is to show that under certain conditions, Galois extensions are equivalent to Frobenius extensions. A key tool in proving this result is the notion of faithful flatness. We are interested in when a Hopf algebra is flat, faithfully flat, or free over a sub-Hopf algebra. There has been a substantial amount of work done in this area, some of which we discuss in detail, especially results by Schneider [Sch93]. This discussion forms the backbone of the chapter and establishes the crucial fact that the conditions in the proposition imply that H is faithfully flat over K. Finally, we discuss a result from Kreimer and Takeuchi's paper, which gives the condition for equivalence between Galois and Frobenius extensions that we require.

Chapter 3 deals with the technical homological results required for the first and third parts of the proof. We note the well-known fact that $\mathrm{Hom}_B(A,B) = \mathrm{Ext}^0_B(A,B)$, for rings $B \subseteq A$, and define the notion of a Gorenstein ring. We also discuss some basic facts about injective, projective and global dimension. We also consider a condition for the Krull dimension of a ring to equal the injective dimension of the ring as a module over itself, which is vital for the last stages of the proof. This chapter concludes with two technical results from ring theory, needed in the first part of the proof.

As mentioned, Chapter 4 deals with the proof of the proposition. However, the chapter also contains a short discussion on the special case when H is assumed to be commutative. We discuss this case further below.

Special Cases and a Possible Use

One of the most important results we need to establish is the faithful flatness of H over K. This requires substantial work in the general case, as discussed in Chapter 2. However, it is possible to simplify this situation by assuming a specific finiteness condition on the sub-Hopf algebra, namely, that the sub-Hopf algebra is finite-codimensional. We can then dispense with much of the work in Chapter 2. Instead we can proceed as indicated in [Sch93, Theorem 2.1], which shows that for any normal finite-codimensional ideal I of a Hopf algebra H, H is right and left faithfully coflat over H/I. Note that there is also a bijective correspondence between the set of all normal Hopf ideals I of a Hopf algebra H, such that H is right faithfully coflat over H/I for all I, and the set of all normal sub-Hopf algebras K of H such that H is right faithfully flat over K, which is also proved in Schneider's paper [Sch93, Theorem 1.4]. Therefore, the Hopf algebra H will be faithfully flat over any normal finite-codimensional sub-Hopf algebra K. Once this is established, it is comparatively straightforward to prove that H is Frobenius over K.

Another special case is the situation indicated above, where we require H to be commutative. This means that we can establish faithful flatness of H over K much more simply, as discussed in Chapter 4. Again, once we have this, it is relatively easy to show that H is Frobenius over K.

Finally, we might ask how this particular result can be used. One answer is that it can be applied to give strong homological conditions on certain classes of $\mathbf{k}$-Hopf algebras, namely those which are left and right Noetherian, are $\mathbf{k}$-affine, and satisfy a polynomial identity. The homological conditions in question are the *Auslander-Gorenstein* condition and the *Cohen-Macaulay* condition. We define and briefly discuss these concepts below.

Definition. Consider a ring R, and let M be a right R-module.

(1) The *grade* of the module M is

$$j(M) = \inf\{j \mid \mathrm{Ext}^j_R(M, R) \neq 0\}$$

(2) Suppose that M is a Noetherian R-module, and let N be any submodule of $\mathrm{Ext}^j_R(M, R)$. Then if for all $i \geq 0$, we have $j(N) \geq i$, R satisfies the *Auslander condition.*

(3) Suppose that R is Noetherian, has finite right and left injective dimension and satisfies the Auslander condition. Then R is *Auslander-Gorenstein.*

(4) Let M be a finitely generated non-zero Noetherian R-module, and consider the Krull dimension, Krull dim$(-)$. Suppose that for all such M,

$$j(M) + \text{Krull dim}(M) = \text{Krull dim}(R).$$

Then R is *Cohen-Macaulay* with respect to the Krull dimension Krull dim.

One can consider the Auslander-Gorenstein and Cohen Macaulay conditions together to be the translation of the Gorenstein property (which is defined for a commutative Noetherian ring) to the non-commutative case. In particular, the Cohen-Macaulay condition gives a link between the homological characteristics of a module and a measure of its size.

These properties are powerful tools in proving results for structure in modules and rings; a detailed discussion is not possible here, but the interested reader is referred to [Bjo89] and [BE90] for discussion of basic ideas and theory; more details of the way in which these results can be used may be found in [GL96] and [SZ94].

We are now in a position to state the result linking the proposition proved in this paper and the properties discussed above. This theorem comes from [BG98].

Theorem (Brown-Goodearl). *Let H be a* $\mathbf{k}$*-affine Noetherian Hopf algebras satisfying a polynomial identity, and suppose that H also has finite left and right injective dimension. Then H is Auslander-Gorenstein and Cohen-Macaulay, and, further,*

$$\textit{inj.dim}(H) = \textit{Krull dim}(H)$$

Contents

Chapter 1

Basic Hopf Algebra Theory

1.1 Algebras and Coalgebras

This section is concerned with some of the basic definitions needed to build up the notion of a Hopf algebra. The familiar definition of an algebra is of a vector space A over a field $\mathbf{k}$, which is a ring where multiplication satisfies the following property:

$$c(ab) = (ca)b = a(cb), \ \forall\, c \in \mathbf{k} \quad \text{and} \quad \forall\, a, b \in A.$$

We can thus identify $\mathbf{k}$ with the subring $\{\lambda 1 \mid \lambda \in \mathbf{k}\}$ of A.

We redefine this to give a definition which initially appears more abstract but is substantially easier to dualise.

Definition 1.1.1. An algebra is a triple (A, μ, η), composed of a vector space A over a field $\mathbf{k}$ and two linear maps $\mu : A \otimes A \longrightarrow A$ and $\eta : \mathbf{k} \longrightarrow A$ (the *product* and *unit* respectively), such that the following diagrams commute:

(1) *The Associativity Condition*

$$\begin{tikzcd}
A\otimes A\otimes A \arrow[r, "\mu\otimes id"] \arrow[d, "id\otimes\mu"] & A\otimes A \arrow[d, "\mu"] \\
A\otimes A \arrow[r, "\mu"] & \mathrm{A}
\end{tikzcd}$$

(2) *The Unit Condition*

$$\begin{tikzcd}
\mathbf{k}\otimes A \arrow[r, "\eta\otimes id"] \arrow[dr, "\cong"'] & A\otimes A \arrow[d, "\mu"] \\
& \mathrm{A}
\end{tikzcd}
\qquad
\begin{tikzcd}
A\otimes \mathbf{k} \arrow[r, "id\otimes\eta"] \arrow[dr, "\cong"'] & A\otimes A \arrow[d, "\mu"] \\
& \mathrm{A}
\end{tikzcd}$$

In addition, we say that the algebra is *commutative* if the following diagram commutes:

$$\begin{tikzcd}
A\otimes A \arrow[r, "\mu"] \arrow[dr, "\tau_{A,A}"] & \mathrm{A} \\
& A\otimes A \arrow[u, "\mu"']
\end{tikzcd}$$

We define $\tau_{V,W}$, for any two $\mathbf{k}$-vector spaces V and W to be the so-called 'flip' map, that is:

$$\tau_{V,W} : V\otimes W \longrightarrow W\otimes V, \quad \text{given by} \quad v\otimes w \mapsto w\otimes v.$$

An *algebra morphism* $f : (A, \mu, \eta) \longrightarrow (A', \mu', \eta')$ is a linear map $f : A \longrightarrow A'$ such that the following conditions hold:

(1) $\mu'\circ(f\otimes f) = f\circ\mu$

(2) $f\circ\eta = \eta'$

We consider a few simple examples of algebras.

Example 1.1.1. Consider an algebra $A = (A, \mu, \eta)$. Now consider an algebra with the same vector space, but with multiplication given by $\mu_{op} = \mu \otimes \tau_{A,A}$; this algebra is the *opposite algebra* A^{op}. Clearly, A is commutative if and only if $\mu = \mu_{op}$.

Example 1.1.2 (The Group Algebra). Let $\mathbf{k}$ be a field and G be a group. We define the *group algebra* to be the $\mathbf{k}$-vector space with G as basis. Elements of $\mathbf{k}G$ have the form $\sum_{g \in G} a_g g$, where $a_g \in \mathbf{k}$ and only finitely many of the a_g are non-zero. The algebra structure is given by

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{k \in G} c_k k,$$

where $c_k = \sum_{gh=k} a_g b_h$. We will return to this important example repeatedly in later discussion.

Example 1.1.3 (The Universal Enveloping Algebra). Consider a Lie algebra $\mathfrak{g}$. This is defined to be a $\mathbf{k}$-vector space with a bilinear map $[,] : \mathfrak{g} \otimes \mathfrak{g} \longrightarrow \mathfrak{g}$, satisfying the following two conditions for all $x, y, z \in \mathfrak{g}$:

(1) (Antisymmetry) $[x, y] = -[y, x]$,

(2) (Jacobi Identity) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$.

As an example of a Lie algebra, consider $\mathbb{R}^3$ with the usual cross vector product.

We assume for simplicity that $\mathfrak{g}$ is a finite-dimensional $\mathbf{k}$-vector space, so we may fix a basis $x_1, ..., x_n$ of $\mathfrak{g}$ and let a_{ijl} be the structure constants of the Lie bracket defined by

$$[x_i, x_j] = \sum_l a_{ijl} x_l, \quad \forall\, i, j.$$

We define the *universal enveloping algebra*, $U(\mathfrak{g})$, to be the associative $\mathbf{k}$-algebra generated by the $\{x_i\}$, subject to the relations

$$x_i x_j - x_j x_i = \sum_{l=1}^{n} a_{ijl} x_l \quad \forall\, 1 \leq i, j \leq n. \tag{1.1}$$

We discuss further properties of this example later.

The definition for the tensor product of two vector spaces is well-known. Here, however, we re-define it in the language of the definition given above.

Definition 1.1.2. Let $A = (A, \mu_A, \eta_A)$ and $B = (B, \mu_B, \eta_B)$ be two algebras. We define their *tensor product* to be the algebra $A \otimes B$ with product given by $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ and unit given by $1 \otimes 1$. In terms of the maps defined in Definition 1.1.1, these maps are given by

$$\mu_{A\otimes B} = (\mu_A \otimes \mu_B) \circ (id_A \otimes \tau_{A,B} \otimes id_A) \quad \text{and} \tag{1.2}$$

$$\eta_{A\otimes B} = (\eta_A \otimes \eta_B). \tag{1.3}$$

We now obtain a new algebraic structure by dualising the definition of an algebra, that is, we systematically reverse the direction of the arrows. This produces an object known as a *coalgebra*, which, together with the notion of an algebra, forms the framework out of which a Hopf algebra is constructed.

Definition 1.1.3. A *coalgebra* is a triple (C, Δ, ε), where C is a $\mathbf{k}$-vector space and the linear maps $\Delta : C \longrightarrow C \otimes C$ and $\varepsilon : C \longrightarrow \mathbf{k}$, respectively the *coproduct* and *counit*, satisfy the following commutative diagrams:

(1) *The Coassociativity Condition*

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

(2) *The Counit Condition*

$$\begin{tikzcd} C\otimes \mathbf{k} \arrow[dr, "\cong"'] & C\otimes C \arrow[l, "id\otimes\varepsilon"'] \\ & C \arrow[u, "\Delta"'] \end{tikzcd} \qquad \begin{tikzcd} \mathbf{k}\otimes C \arrow[dr, "\cong"'] & C\otimes C \arrow[l, "\varepsilon\otimes id"'] \\ & C \arrow[u, "\Delta"'] \end{tikzcd}$$

where the isomorphism in the above maps is given by $c \otimes \lambda \mapsto c\lambda$ and $\lambda \otimes c \mapsto \lambda c$ respectively, for $c \in C$ and $\lambda \in \mathbf{k}$.

The coalgebra is said to be *cocommutative* if the following diagram commutes:

$$\begin{tikzcd} C\otimes C & C \arrow[l, "\Delta"'] \arrow[d, "\Delta"] \\ & C\otimes C \arrow[ul, "\tau_{C,C}"] \end{tikzcd}$$

Definition 1.1.4. A *coalgebra morphism* $g : (C, \Delta, \varepsilon) \longrightarrow (C', \Delta', \varepsilon')$ is defined in the 'opposite' sense to that of an algebra morphism; it is a linear map $g : C \longrightarrow C'$ such that the following conditions hold:

(1) $(g\otimes g)\circ\Delta = \Delta'\circ g$,

(2) $\varepsilon'\circ g = \varepsilon$.

We now show that the notion of ideals and factor rings extends naturally to coalgebras.

Definition 1.1.5. Let I be a subspace of (C, Δ, ε), and suppose $\Delta(I) \subseteq I\otimes C + C\otimes I$ and $\varepsilon(I) = 0$. Then I is said to be a *coideal.* Further, the $\mathbf{k}$-space C/I is a coalgebra with multiplication and counit induced by Δ and ε, given by $\Delta(c + I) = ((\pi\otimes\pi)\circ\Delta)(c)$, and $\varepsilon(c + I) = \varepsilon(c)$, where $\pi : C \longrightarrow C/I$ is the canonical map. Consistency of these definitions is ensured by the fact that I is a coideal.

As for algebras, we define the tensor product of coalgebras.

Definition 1.1.6. Let $C = (C, \Delta_C, \varepsilon_C)$ and $D = (D, \Delta_D, \varepsilon_D)$ be coalgebras. The tensor product of C and D is defined as the coalgebra $C\otimes D$ with coproduct

$$\Delta_{C\otimes D} : C\otimes D \longrightarrow C\otimes D\otimes C\otimes D, \quad \text{given by} \quad \Delta_{C\otimes D} = (id_C\otimes\tau\otimes id_D)\circ(\Delta_C\otimes\Delta_D)$$

and counit

$$\varepsilon_{C\otimes D} : C\otimes D \longrightarrow \mathbf{k}, \quad \text{given by} \quad \varepsilon_{C\otimes D}(c\otimes d) = \varepsilon(c)\varepsilon(d).$$

We consider a few basic examples of coalgebras.

Example 1.1.4 (The Opposite Coalgebra). We use the flip to dualise the notion of the opposite algebra to coalgebras. Let $C = (C, \Delta, \varepsilon)$ be any coalgebra. Define $\Delta^{cop} = \tau_{C,C}\circ\Delta$. Then clearly Δ^{cop} satisfies the coassociativity rule, and $(C, \Delta^{cop}, \varepsilon)$ is a coalgebra, the *opposite coalgebra.*

Example 1.1.5 (The Coalgebra of a Set). Let X be a set and define

$$C = \mathbf{k}[X] = \oplus_{x \in X} \mathbf{k}x.$$

We can then impose a coalgebra structure on C by defining $\Delta(x) = x \otimes x$ and $\varepsilon(x) = 1$ for all $x \in X$. We extend these conditions naturally to C, so that

$$\begin{aligned} \Delta \sum_i (\lambda_i x_i) &= \sum_i \lambda_i \Delta(x_i) \quad \text{and} \\ \varepsilon(\sum_i \lambda_i x_i) &= \sum_i \lambda_i. \end{aligned}$$

We now return to the group algebra, which is the special case $X = G$. We may re-define its algebra structure as

$$\mu(g \otimes h) = gh \quad \text{and} \quad \eta(k) = 1_G \cdot k, \quad \forall\, k \in \mathbf{k}. \tag{1.4}$$

It is straightforward to show that these satisfy the associative and unit axioms. We show the case for μ; that for η is even simpler.

$$\begin{aligned} \mu((\mu \otimes id) \circ (g \otimes h \otimes k)) &= \mu(gh \otimes k) = ghk \quad \text{and} \\ \mu((id \otimes \mu) \circ (g \otimes h \otimes k)) &= \mu(g \otimes hk) = ghk, \end{aligned}$$

for all $g, h, k \in G$. We define the coalgebra structure by the following maps:

$$\Delta(g) = g \otimes g \quad \text{and} \quad \varepsilon(g) = 1. \tag{1.5}$$

where both of these are extended to $\mathbf{k}G$ in the natural manner indicated above. As above, we check the coassociativity axiom

$$\begin{aligned} (\Delta \otimes id) \circ \Delta(g) &= (\Delta \otimes id)(g \otimes g) = g \otimes g \otimes g \quad \text{and} \\ (id \otimes \Delta) \circ \Delta(g) &= (id \otimes \Delta)(g \otimes g) = g \otimes g \otimes g, \end{aligned}$$

for all $g \in G$. The calculation to show the counit axiom is even easier and is omitted.

1.1.1 Basic Theory

The Relationship Between Algebras and Coalgebras

We next examine the relationship between coalgebras and algebras, which we do by considering their *dual spaces.*

Definition 1.1.7.

(1) Let V be a vector space. Then $V^* = \mathrm{Hom}_{\mathbf{k}}(V, \mathbf{k})$ is the *dual* of V. We note without proof that $V^* \otimes V^* \subseteq (V \otimes V)^*$.

(2) We use the tensor product of V and V^* to define a bilinear form $\langle , \rangle : V^* \otimes V \longrightarrow \mathbf{k}$ via the map $\langle f, v \rangle = f(v)$.

The bilinear form defined above leads to the following definition.

Definition 1.1.8. Let V and W be vector spaces. Let $\phi : V \longrightarrow W$ be a $\mathbf{k}$-linear map. We define the *transpose* of ϕ to be the map $\phi^* : W^* \longrightarrow V^*$, given by

$$\phi^*(f)(v) = \langle f, \phi(v) \rangle = f(\phi(v)),$$

for all $f \in W^*$ and for all $v \in V$.

Lemma 1.1.1. *If $C = (C, \Delta, \varepsilon)$ is a coalgebra, then C^* is an algebra with product $\mu = \Delta^*$ and unit $\eta = \varepsilon^*$.*

Proof. We use the fact $C^* \otimes C^* \subseteq (C \otimes C)^*$ from above. We can then restrict the map Δ^* to a map $\mu : C^* \otimes C^* \longrightarrow C^*$, given by

$$\mu(f \otimes g)(x) = \Delta^*(f \otimes g)(x) = \langle f \otimes g, \Delta(x) \rangle = (f \otimes g)\Delta(x),$$

for all $f, g \in C^*$, and for all $x \in C$. We let $\eta = \varepsilon^*$. Then (C, μ, η) forms an algebra, as may be easily verified by looking at the diagram for the associativity condition. □

The converse of this statement is not true in general; if, for example, A is not finite-dimensional, then $A^* \otimes A^*$ is a proper subspace of $(A \otimes A)^*$. This means that the image of $\mu^* : A^* \longrightarrow (A \otimes A)^*$ need not necessarily be contained in $A^* \otimes A^*$. However, if A is finite-dimensional, the converse is true. We prove this result shortly when discussing tensor products of linear maps. In the general case, however, the best we can do is proceed with the so-called *finite dual* of A:

Definition 1.1.9. The *finite dual* of an algebra A, denoted by A^o, is the set of all $f \in A^*$ such that $f(I) = 0$ for some ideal I of A, where I satisfies the condition $\dim(A/I) < \infty$. We note the following results: A^o is a coalgebra if A is an algebra and has coproduct $\Delta = \mu^*$ and counit $\varepsilon = \eta^*$. Further, if A is commutative then A^o is cocommutative.

Example 1.1.6 (Return to the Coalgebra of a Set). We can apply Lemma 1.1.1 to the previous example of the coalgebra of a set, to get an algebra, $C^* = \mathrm{Hom}_{\mathbf{k}}(C, \mathbf{k})$, the algebra of functions on X with values in $\mathbf{k}$. The lemma shows that for $f, g \in C^*$ and $x \in C$,

$$\begin{aligned} \mu(f \otimes g)(x) &= (f \otimes g)(\Delta(x)) \\ &= (f \otimes g)(x \otimes x) \\ &= f(x) \otimes g(x) \\ &= f(x) \cdot g(x). \end{aligned}$$

Thus the algebra structure in C^* is given by pointwise multiplication. Also, for $\lambda \in \mathbf{k}$

$$\begin{aligned} \eta(\lambda) &= \varepsilon^*(\lambda) \\ &= \lambda \varepsilon^*(1) \\ &= \lambda. \end{aligned}$$

It is simple to check that μ and η satisfy the associativity and unit axioms.

Example 1.1.7 (The Group Algebra). We consider the group algebra, $C = \mathbf{k}G$, first as a coalgebra and then as an algebra. By Example 1.1.4, $\mathbf{k}G$ has a coalgebra structure, given by Equation 1.5. Thus the algebra structure on C^* (or on C^o) is given by pointwise multiplication, as in Example 1.1.6.

In general, $C = \mathbf{k}G$ is not a finite-dimensional algebra, so we cannot apply the converse of Lemma 1.1.1 in this case. We can, however, obtain the finite dual, which in this case is the so-called *set of representative functions,* $R_{\mathbf{k}}(G)$ on G. The algebra structure on C is given by Equation 1.4, so the coalgebra structure on C^o is therefore given by

$$\begin{aligned} \Delta_o f(x \otimes y) &= \mu^* f(x \otimes y) \\ &= \langle f, \mu(x \otimes y) \rangle \\ &= f(xy). \end{aligned}$$

This does not give an explicit formula for $\Delta_o f$ in terms of elements of $C^o \otimes C^o$, which is in fact only possible when C is finite-dimensional. In this case, one would choose a basis $\{b_g \,|\, g \in G\}$ of C^*, dual to the basis of G in kG. Then

$$\Delta_o b_g = \sum_{hk=g} b_h \otimes b_k.$$

The Sigma Notation

The following discussion considers a very useful form of notation, developed by Moss Sweedler and R. G. Heyneman, first published in [Swe69].

Suppose we have an element $x \in C = (C, \Delta, \varepsilon)$. Then the element $\Delta(x) \in C \otimes C$ has the form $\Delta(x) = \sum_i x_i' \otimes x_i''$. In *Sweedler's sigma notation*, this is written as

$$\Delta(x) = \sum\nolimits_x x_1 \otimes x_2.$$

For example, the coassociativity of Δ may be expressed in this form as

$$\Delta(x) = \sum\nolimits_x x_1 \otimes x_2.$$

$$\sum_x \left(\sum\nolimits_{x_1} (x_1)_1 \otimes (x_1)_2\right) \otimes x_2 = \sum_x x_1 \otimes \left(\sum\nolimits_{x_2} (x_2)_1 \otimes (x_2)_2\right).$$

By convention, we identify both sides of this expression with

$$\sum_x x_1 \otimes x_2 \otimes x_3.$$

We extend this inductively to get a similar expression for longer products.

We reformulate the condition for counitality as

$$\sum_x \varepsilon(x_1) x_2 = x = \sum_x x_1 \varepsilon(x_2), \tag{1.6}$$

and the cocommutative condition as

$$\sum\nolimits_x x_1 \otimes x_2 = \sum\nolimits_x x_2 \otimes x_1.$$

Finally, the comultiplication of the tensor product of two coalgebras C and D can rewritten as

$$\Delta_{C\otimes D}(x\otimes y) = \sum\nolimits_{x\otimes y}(x\otimes y)_1\otimes(x\otimes y)_2 = \sum\nolimits_{x\otimes y} x_1\otimes y_1\otimes x_2\otimes y_2, \tag{1.7}$$

for all $x \in C$ and $y \in D$. Note that for the remainder of this dissertation, we omit the subscript x on $\sum_x$ when possible.

Tensor Products of Linear Maps

We now return to the claim made earlier in this section that if A is finite dimensional, then the converse to Lemma 1.1.1 is true. The following discussion forms an important part of the proof.

Definition 1.1.10. Let U, U', V and V' be vector spaces, and consider the linear maps $f : U \longrightarrow U'$ and $g : V \longrightarrow V'$. We define the *tensor product* of f and g to be the map $f\otimes g : U\otimes V \longrightarrow U'\otimes V'$, given by $(f\otimes g)(u\otimes v) = f(u)\otimes g(v)$, for all $u \in U$ and $v \in V$. We use this to define a linear map

$$\gamma : \mathrm{Hom}(U,U')\otimes\mathrm{Hom}(V,V') \longrightarrow \mathrm{Hom}(U\otimes V, U'\otimes V'), \quad \text{via} \quad \gamma(f\otimes g)(u\otimes v) = f(u)\otimes g(v).$$

We are interested in when the map γ is an isomorphism. The following theorem deals with such a condition.

Theorem 1.1.2. *Let at least one of (U,U'), (V,V') or (U,V) be a pair of finite dimensional* $\mathbf{k}$*-vector spaces. Then the map γ given in Definition 1.1.10 is an isomorphism.*

Proof. We require the following standard algebraic identities. Let I be an indexing set.

$$\begin{aligned} \mathrm{Hom}(\oplus_{i\in I}U_i, U') &\cong \prod_{i\in I}\mathrm{Hom}(U_i,U') && (1.8)\\ (\oplus_{i\in I}U_i)\otimes U' &\cong \oplus_{i\in I}(U_i\otimes U') && (1.9)\\ \mathrm{Hom}(U,\prod_{i\in I}U_i') &\cong \prod_{i\in I}\mathrm{Hom}(U,U_i') && (1.10)\end{aligned}$$

We consider the case when U and U' are finite-dimensional; proof of the remaining two cases is achieved by applying the same technique as discussed below. Since U and U' are finite-dimensional, we may write $U = \oplus_{j\in J}\mathbf{k}u_j$, where $\{u_j\}_{j\in J}$ is a finite basis of U. Then

$$\mathrm{Hom}(\oplus_j\mathbf{k}u_j, U')\otimes\mathrm{Hom}(V,V') \cong \prod_j(\mathrm{Hom}(\mathbf{k}u_j,U'))\otimes\mathrm{Hom}(V,V') \quad \text{by Equation 1.8.}$$

Also,

$$\begin{aligned}\mathrm{Hom}((\oplus_j \mathbf{k}u_j)\otimes V, U'\otimes V') &\cong \mathrm{Hom}(\oplus_j(\mathbf{k}u_j\otimes V), U'\otimes V') \\ &\cong \prod_j \mathrm{Hom}(\mathbf{k}u_j\otimes V, U'\otimes V') \quad \text{by Equations 1.8 and 1.9.}\end{aligned}$$

Thus, after composition with these isomorphisms, γ is now a map from

$$(\prod_j \mathrm{Hom}(\mathbf{k}u_j, U'))\otimes\mathrm{Hom}(V, V') \xrightarrow{\gamma} \prod_j \mathrm{Hom}(\mathbf{k}u_j\otimes V, U'\otimes V').$$

However, J is a finite indexing set, so $\prod_j$ can be replaced by $\oplus_j$. So, applying Equation 1.9 once more, we have $\oplus_j(\mathrm{Hom}(\mathbf{k}u_j, U')\otimes\mathrm{Hom}(V, V')) \longrightarrow \oplus_j\mathrm{Hom}(\mathbf{k}u_j\otimes V, U'\otimes V')$, where the map γ' sends each j^{th} summand to the corresponding j^{th} summand. It is therefore enough to show that γ is an isomorphism in the special case $U = \mathbf{k}u_i$, that is, the map $\gamma : \mathrm{Hom}(\mathbf{k}u_i, U')\otimes\mathrm{Hom}(V, V') \longrightarrow \mathrm{Hom}(\mathbf{k}u_i\otimes V, U'\otimes V')$ is an isomorphism. Since $\mathbf{k}u_i$ is one-dimensional, we only need check that the following map is an isomorphism:

$$\gamma' : U'\otimes\mathrm{Hom}(V, V') \longrightarrow \mathrm{Hom}(V, U'\otimes V'), \tag{1.11}$$

given by $\gamma'(u'\otimes f)(v) = u'\otimes f(v)$, for $u' \in U'$, $v \in V$ and $f \in \mathrm{Hom}(V, V')$. To prove this, we use the fact that U' is finite dimensional and so can be written as $\oplus_{j' \in J'}\mathbf{k}u'_{j'}$, for some finite basis $\{u'_{j'}\}_{j' \in J'}$. By using Equations 1.9 and 1.10 in a manner similar to that above, we get that

$$U'\otimes\mathrm{Hom}(V, V') \cong \oplus_{j'}\mathbf{k}u'_{j'}\otimes\mathrm{Hom}(V, V')$$

and that

$$\mathrm{Hom}(V, U'\otimes V') \cong \prod_{j'} \mathrm{Hom}(V, \mathbf{k}u'_{j'}\otimes V') = \oplus_{j'}\mathrm{Hom}(V, \mathbf{k}u'_{j'}\otimes V').$$

We wish to show that the map γ' is an isomorphism. To show that it is injective, we consider $\ker(\gamma')$. Let $\sum_{j' \in J'} \lambda_{j'}u'_{j'}\otimes f_{j'}$, for $\lambda_{j'}u'_{j'} \in \mathbf{k}u'_{j'}$, and $f_{j'} \in \mathrm{Hom}_{\mathbf{k}}(V, V')$, be nonzero. Then clearly $\gamma'(\sum_{j' \in J'} \lambda_{j'}u'_{j'}\otimes f_{j'})$ is also nonzero. To show that γ' is onto, consider $g \in \oplus_{j'}\mathrm{Hom}(V, \mathbf{k}u'_{j'}\otimes V')$. So $g = g_1\oplus g_2\oplus\cdots\oplus g_n$, for $g_{j'} \in \mathrm{Hom}(V, \mathbf{k}u'_{j'}\otimes V')$. Clearly, for all such $g_{j'}$ we have $g_{j'}(v) = \lambda'_{j'}u'_{j'}\otimes v'_r$, for some $\lambda'_{j'}u'_{j'} \in \mathbf{k}u'_{j'}$ and $v'_r \in V'$. So there exists $\lambda'_{j'}u'_{j'}\otimes g'_{j'} \in \mathbf{k}u'_{j'}\otimes\mathrm{Hom}(V, V')$ such that $\gamma'(\lambda'_{j'}u'_{j'}\otimes g'_{j'})(v) = \lambda'_{j'}u'_{j'}\otimes v'_r$. Thus γ' is onto, and hence is bijective. $\square$

We are now in a position to prove the converse to Lemma 1.1.1.

Corollary 1.1.3. *Let $A = (A, \mu, \eta)$ be a finite-dimensional algebra. Then the map $\gamma : A^* \otimes A^* \longrightarrow (A \otimes A)^*$ is an isomorphism, given by $\gamma((f \otimes g)(a \otimes b)) = f(a) \otimes g(b)$. In this case, one may define A^* as a coalgebra via the maps*

$$\begin{aligned} \Delta &= \gamma^{-1} \circ \mu^* \quad \textit{and} \\ \varepsilon &= \eta^*, \end{aligned}$$

*where the superscript * defines the transpose of the map.*

Proof. All that is required here is to take $A = U = V$ and $U' = V' = \mathbf{k}$ in Theorem 1.1.2. To show that A^* is a coalgebra, we need only consider the respective commutative diagrams for associativity and the unit condition, and the corresponding diagrams for coalgebras. □

Example 1.1.8 (The Matrix Coalgebra). We let $A = M_n(\mathbf{k})$ be the algebra of $n \times n$ matrices with entries in $\mathbf{k}$. We define E_{ij} to be the matrix with entry 1 at the i, j position and zeros everywhere else. The set of the matrices E_{ij}, for all $1 \leq i, j \leq n$, forms a basis for $M_n(\mathbf{k})$. Define a basis dual to this one by $\{x_{ij}\}$. Then we define the dual coalgebra A^* by

$$\Delta(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj} \quad \text{and} \quad \varepsilon(x_{ij}) = \delta_{ij}.$$

We use Corollary 1.1.3 to check the validity of these definitions. For the counit, we have:

$$\varepsilon(x_{ij}) = x_{ij}(\eta(1)) = x_{ij} \sum_k E_{kk} = \sum_k \delta_{ik} \delta_{kj} = \delta_{ij},$$

which justifies the choice for ε. For Δ, we need to show that $\Delta = \gamma^{-1} \circ \mu^*$, that is, that $\gamma \circ \Delta = \mu^*$, where γ is the map defined in Corollary 1.1.3 above. We have

$$\begin{aligned} \mu^*(x_{ij})(E_{kl} \otimes E_{mn}) &= (x_{ij}(\mu(E_{kl} \otimes E_{mn}))) \\ &= (\delta_{lm} x_{ij}(E_{kn})) \\ &= (\delta_{lm} \delta_{ik} \delta_{jn}) \\ &= (\sum_p \delta_{ik} \delta_{lp} \delta_{pm} \delta_{jn}) \\ &= (\sum_p x_{ip}(E_{kl}) x_{pj}(E_{mn})) \\ &= \gamma(\sum_p x_{ip} \otimes x_{pj})(E_{kl} \otimes E_{mn}) \end{aligned}$$

So we must have $\Delta(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj}$ as shown above. Thus A^* does indeed have a coalgebra structure given by the maps defined.

Graded and Filtered Algebras

We consider the following technical ring theoretic concepts, which will be required in later chapters. We also include the corresponding definition of a graded ring for modules.

Definition 1.1.11. Let A be an algebra. Suppose that there exist subspaces $\{A_i\}_{i \in \mathbb{N}}$ of A with

$$A = \oplus_{i \in \mathbb{N}} A_i \quad \text{and} \quad A_i \cdot A_j \subset A_{i+j}$$

for all $i, j \in \mathbb{N}$. Then A is said to be *graded.* The elements of A_i are said to be *homogeneous of degree* i. The unit 1 of a graded algebra is always assumed to belong to A_0.

Example 1.1.9. Consider a free algebra $A = \mathbf{k}\{X\}$. Then A is graded by the length of the words, that is, each A_i is defined to be the subspace linearly generated by all monomials of degree i. The elements of X have degree 1.

We now consider the equivalent condition for modules.

Definition 1.1.12.

(1) Suppose A is a graded algebra as described above. Consider a right A-module M. Suppose that $M = \oplus_{n \in \mathbb{N}} M_n$ is a decomposition of Abelian groups, such that $M_i A_j \subseteq A_{i+j}$, for all $i, j \in \mathbb{N}$. This is a *grading* of the right A-module M. A module can have many different gradings.

(2) A *graded* module is a module with a fixed grading. We refer to the nonzero elements of each subgroup M_n as being *homogeneous of degree* n. If $m = \sum_{n \in \mathbb{N}} m_n$, for $m_n \in M_n$, then we define m_n as the n^{th} *homogeneous component* of m.

Definition 1.1.13. Let $\{A_i\}_{i \geq 0}$ be a family of subspaces of the algebra A which satisfy the conditions

$$\{0\} \subset A_0 \subset \cdots \subset A_i \subset \cdots \subset A$$

and

$$A = \cup_{i \geq 0} A_i, \quad \text{and} \quad A_i \cdot A_j \subset A_{i+j}$$

A is then said to be *filtered.*

Example 1.1.10. The *trivial filtration* for any algebra is given by the subspace $A_i = A$, for all i.

Example 1.1.11. Let $A = \oplus_{i \geq 0} A_i$ by a graded algebra. We can filter A by

$$A_i = \oplus_{0 \leq j \leq i} A_j,$$

for all $i \in \mathbb{N}$.

1.2 Bialgebras

This section is central to all that follows, since Hopf algebras are defined as special cases of bialgebras.

Suppose that H is a vector space with both an algebra structure (H, μ, η) and a coalgebra structure (H, Δ, ε). Given certain conditions (see Theorem 1.2.1) these two structures are equivalent. First we give $H \otimes H$ the induced structures of a tensor product of algebras and coalgebras; see Definitions 1.1.2 and 1.1.6 respectively. Now recall the definition of a coalgebra morphism from Definition 1.1.4.

Theorem 1.2.1. *Let H be a vector space with an algebra and coalgebra structure as given above. Then the following two statements are equivalent:*

(1) The maps μ and η are morphisms of coalgebras;

(2) The maps Δ and ε are morphisms of algebras.

Proof. This can be seen from an examination of the commutative diagrams associated with either statement. We note that μ is a morphism of coalgebras if and only if the following two diagrams are commutative (see Definition 1.1.4 for a justification).

$$\begin{tikzcd} H\otimes H \arrow[r, "\varepsilon\otimes\varepsilon"] \arrow[d, "\mu"] & \mathbf{k}\otimes\mathbf{k} \arrow[d, "id"] \\ H \arrow[r, "\varepsilon"] & \mathbf{k} \end{tikzcd} \qquad \begin{tikzcd} H\otimes H \arrow[r, "\mu"] \arrow[d, "(id\otimes\tau\otimes id)(\Delta\otimes\Delta)"'] & H \arrow[d, "\Delta"] \\ (H\otimes H)\otimes(H\otimes H) \arrow[r, "\mu\otimes\mu"] & H\otimes H \end{tikzcd}$$

We may also express the fact that η is a morphism of coalgebras via the following commutative diagrams.

$$\begin{tikzcd} \mathbf{k} \arrow[r, "\eta"] \arrow[d, "id"] & H \arrow[d, "\Delta"] \\ \mathbf{k}\otimes\mathbf{k} \arrow[r, "\eta\otimes\eta"] & H\otimes H \end{tikzcd} \qquad \begin{tikzcd} \mathbf{k} \arrow[r, "\eta"] \arrow[d, "id"'] & H \arrow[d, "\varepsilon"] \\ \mathbf{k}\otimes\mathbf{k} \arrow[r, "id"] & \mathbf{k} \end{tikzcd}$$

But Δ is an algebra morphism if and only if the following commutative diagrams hold:

$$\begin{array}{ccc} H\otimes H & \xrightarrow{\Delta\otimes\Delta} & (H\otimes H)\otimes(H\otimes H) \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle (\mu\otimes\mu)(id\otimes\tau\otimes id)} \\ H & \xrightarrow{\Delta} & H\otimes H \end{array} \qquad \begin{array}{ccc} \mathbf{k} & \xrightarrow{\eta} & H \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \Delta} \\ \mathbf{k}\otimes\mathbf{k} & \xrightarrow{\eta\otimes\eta} & H\otimes H \end{array}$$

and ε is an algebra morphism if and only if the following commutative diagrams hold:

$$\begin{array}{ccc} H\otimes H & \xrightarrow{\varepsilon\otimes\varepsilon} & \mathbf{k}\otimes\mathbf{k} \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle id} \\ H & \xrightarrow{\varepsilon} & \mathbf{k} \end{array} \qquad \begin{array}{ccc} \mathbf{k} & \xrightarrow{\eta} & H \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \varepsilon} \\ \mathbf{k} & \xrightarrow{id} & \mathbf{k} \end{array}$$

But these diagrams are the same as the previous four; hence the result. $\square$

This theorem leads naturally to the following definition.

Definition 1.2.1. A *bialgebra* is a quintuple $(H, \mu, \eta, \Delta, \varepsilon)$, where (H, μ, η) is an algebra, and (H, Δ, ε) is a coalgebra satisfying the equivalent conditions in the previous theorem. A map from H to H' is a bialgebra morphism if it is both an algebra morphism and a coalgebra morphism.

Note 1.2.1. The conditions stipulated in Theorem 1.2.1 can be translated into terms of algebra morphisms. This requires Δ and ε to satisfy:

$$\begin{aligned} \Delta(xy) &= \Delta(x)\Delta(y) && (1.12)\\ \Delta(1_H) &= 1_H\otimes 1_H && (1.13)\\ \varepsilon(xy) &= \varepsilon(x)\varepsilon(y) && (1.14)\\ \varepsilon(1_H) &= 1_H. && (1.15) \end{aligned}$$

In terms of Sweedler's sigma notation, $\Delta(xy) = \Delta(x)\Delta(y)$ can be expressed as

$$\sum\nolimits_{xy}(xy)_1\otimes(xy)_2 = \sum\nolimits_{(x)(y)} x_1y_1\otimes x_2y_2. \tag{1.16}$$

The other three relations can be expressed similarly. We will use this expression, and those above, freely throughout the rest of the text.

Clearly, we can define the notion of a tensor product of two bialgebras H and K to be the object $H \otimes K$ with induced structure maps from the tensor product of algebras and the tensor product of coalgebras. One might reasonably expect this new structure to be a bialgebra, and indeed this is the case. We show this formally in the following lemma.

Lemma 1.2.2. *Let H, K be bialgebras with Δ_H and Δ_K, and ε_H and ε_K the respective coproducts and counits. Then the tensor product $H \otimes K$ is also a bialgebra.*

Proof. Since H and K are bialgebras, we may define the tensor product as both a tensor product of algebras and of coalgebras with coproduct given by

$$\Delta_{H \otimes K} = (id_H \otimes \tau_{H,K} \otimes id_K) \circ (\Delta_H \otimes \Delta_K),$$

and counit given, for $h \in H$ and $k \in K$ as

$$\varepsilon_{H \otimes K}(h \otimes k) = \varepsilon_H(h)\varepsilon_K(k)$$

Rather than use Theorem 1.2.1 directly, we will use the requirements for $\Delta_{H \otimes K}$ and $\varepsilon_{H \otimes K}$ in Note 1.2.1 instead. We recall Definition 1.1.6 for the tensor product of coalgebras and Equation 1.7 which gives the comultiplication in sigma notation. Let $h, h' \in H$ and $k, k' \in K$. We begin by considering Equation 1.13 above. First we note that

$$\Delta_{H \otimes K}(h \otimes k) = \sum h_1 \otimes k_1 \otimes h_2 \otimes k_2.$$

Now, considering $(h \otimes k)(h' \otimes k)$ first, we get

$$\begin{aligned}
\Delta_{H \otimes K}((h \otimes k)(h' \otimes k')) &= \Delta_{H \otimes K}(hh' \otimes kk') \\
&= \sum\nolimits_{hh' \otimes kk'} (hh' \otimes kk')_1 \otimes (hh' \otimes kk')_2 \\
&= \sum\nolimits_{(hh')(kk')} (hh')_1 \otimes (kk')_1 \otimes (hh')_2 \otimes (kk')_2 \\
&= \sum\nolimits_{(h)(h')(k)(k')} h_1 h'_1 \otimes k_1 k'_1 \otimes h_2 h'_2 \otimes k_2 k'_2.
\end{aligned}$$

But

$$\sum\nolimits_{(h)(h')(k)(k')} h_1 h'_1 \otimes k_1 k'_1 \otimes h_2 h'_2 \otimes k_2 k'_2 = \sum (h_1 \otimes k_1 \otimes h_2 \otimes k_2)(h'_1 \otimes k'_1 \otimes h'_2 \otimes k'_2),$$

so therefore $\Delta_{H \otimes K}((h \otimes k)(h' \otimes k')) = \Delta_{H \otimes K}(h \otimes k)\Delta_{H \otimes K}(h' \otimes k')$. By setting

$$h = h' = k = k' = 1_{H \otimes K},$$

it is clear that $\Delta_{H \otimes K}(1_H \otimes 1_K) = 1_{H \otimes K} \otimes 1_{H \otimes K}$.

We now consider the conditions for ε. Consider $h, h' \in H$ and $k, k' \in K$ as before. Then

$$\begin{aligned}
\varepsilon((h\otimes k)(h'\otimes k')) &= \varepsilon(hh'\otimes kk') \\
&= \varepsilon(hh')\varepsilon(kk') \\
&= \varepsilon(h)\varepsilon(k)\varepsilon(h')\varepsilon(k') \quad \text{by properties of } \varepsilon \\
&= \varepsilon(h\otimes k)\varepsilon(h'\otimes k').
\end{aligned}$$

It is clear from this that $\varepsilon(1_{H\otimes K}) = 1_{H\otimes K}$. Hence $\Delta_{H\otimes K}$ and $\varepsilon_{H\otimes K}$ satisfy the equivalent conditions in Theorem 1.2.1 by Note 1.2.1. $\square$

1.2.1 Examples

Example 1.2.1 (The Polynomial Functions on $n\times n$ Matrices). Consider the ring defined as

$$\mathcal{O}(M_n(\mathbf{k})) = \mathbf{k}[X_{ij} : 1 \leq i, j \leq n].$$

This is a commutative polynomial algebra in the n^2 indeterminates X_{ij}. We want to show that it has a coalgebra structure and that the coproduct and counit are algebra morphisms. Define

$$\begin{aligned}
\Delta(X_{ij}) &= \sum_{k=1}^{n} X_{ik}\otimes X_{kj} \quad \text{and} \\
\varepsilon(X_{ij}) &= \delta_{ij}
\end{aligned}$$

Clearly, if these maps are extended multiplicatively and linearly to products and sums of the generators, they must also define algebra morphisms. We need to show that $(\mathcal{O}(M_n(\mathbf{k})), \Delta, \varepsilon)$ forms a coalgebra. Coassociativity is clear from:

$$\begin{aligned}
(\Delta\otimes id)\circ\Delta(X_{ij}) &= (\Delta\otimes id)(\sum_{k=1}^{n} X_{ik}\otimes X_{kj}) \\
&= \sum_{k=1}^{n}(\Delta(X_{ik})\otimes X_{kj}) \\
&= \sum_{k=1}^{n}\sum_{l=1}^{n}(X_{il}\otimes X_{lk})\otimes X_{kj} \\
&= \sum_{k=1}^{n}\sum_{l=1}^{n} X_{il}\otimes(X_{lk}\otimes X_{kj}) \\
&= (id\otimes\Delta)\circ\Delta(X_{ij}).
\end{aligned}$$

The counit axiom is also easy to prove:

$$\begin{aligned}
(\varepsilon \otimes id) \circ \Delta(X_{ij}) &= (\varepsilon \otimes id)(\sum_{k=1}^{n} X_{ik} \otimes X_{kj}) \\
&= \sum_{k=1}^{n} \delta_{ik} \otimes X_{kj} \\
&= 1 \otimes X_{ij} \\
&= (id \otimes \varepsilon) \circ \Delta(X_{ij}).
\end{aligned}$$

Thus $(\mathcal{O}(M_n(\mathbf{k})), \Delta, \varepsilon)$ is a coalgebra. By definition, Δ and ε are algebra morphisms, so $(\mathcal{O}(M_n(\mathbf{k})), \Delta, \varepsilon)$ is a bialgebra. We note that this bialgebra is commutative, but not cocommutative.

Example 1.2.2 (Return to the Coalgebra of a Set). Consider $C = \mathbf{k}[X] = \oplus_{x \in X} \mathbf{k}x$ once more. This time, we assume further that X has an associative map $\mu : X \times X \longrightarrow X$ with a left and right unit e (that is, a unital monoid structure). This map induces an algebra structure on C with unit e. Considering the maps Δ and ε, we see that

$$\begin{aligned}
\Delta(xy) &= xy \otimes xy = (x \otimes x)(y \otimes y) = \Delta(x)\Delta(y), \quad \text{and} \\
\varepsilon(xy) &= 1 = \varepsilon(x)\varepsilon(y).
\end{aligned}$$

So Δ and ε are morphisms of algebras (by the relations in Note 1.2.1).

Example 1.2.3 (The Group Algebra). As discussed in Example 1.1.7, this already has both an algebra and coalgebra structure, given by Equation 1.4 and Equation 1.5 respectively.

To show that this is a bialgebra, we will show that Δ and ε define algebra morphisms, i.e. that they satisfy the conditions given in Definition 1.1.1.

Consider the map $\Delta : (\mathbf{k}G) \longrightarrow (\mathbf{k}G \otimes \mathbf{k}G)$, where the algebras $\mathbf{k}G$ and $\mathbf{k}G \otimes \mathbf{k}G$ are given as $\mathbf{k}G = (\mathbf{k}G, \mu, \eta)$, and $\mathbf{k}G \otimes \mathbf{k}G = (\mathbf{k}G \otimes \mathbf{k}G, (\mu \otimes \mu)(id \otimes \tau \otimes id), (\eta \otimes \eta))$, where τ is the flip map. This is the tensor product of $\mathbf{k}G$ with itself (see Definition 1.1.2). We want to show that

$$((\mu \otimes \mu)(id \otimes \tau \otimes id)) \circ (\Delta \otimes \Delta) = \Delta \circ \mu \quad \text{and that} \quad \Delta \circ \eta = \eta \otimes \eta.$$

But for $g, h \in G$,

$$\begin{aligned}((\mu\otimes\mu)(id\otimes\tau\otimes id)\circ(\Delta\otimes\Delta)(g\otimes h) &= (\mu\otimes\mu)(id\otimes\tau\otimes id)((g\otimes g)\otimes(h\otimes h)) \\ &= (\mu\otimes\mu)(id\otimes\tau\otimes id))(g\otimes(g\otimes h)\otimes h) \\ &= \mu\otimes\mu(g\otimes h\otimes g\otimes h) \\ &= \mu\otimes\mu((g\otimes h)\otimes(g\otimes h)) \\ &= gh\otimes gh = \Delta(gh) = \Delta\circ\mu(g\otimes h),\end{aligned}$$

as required for the first condition. The second condition is even easier:

$$\Delta\circ\eta(k) = \Delta(1) = 1\otimes 1 = \eta\otimes\eta(g), \quad \forall\, k \in \mathbf{k}.$$

Thus Δ is an algebra morphism. To show that $\mathbf{k}G$ is a bialgebra, we need to show that ε is also an algebra morphism. We do this by noting the following fact:

If $\vartheta : G \longrightarrow H$ is a homomorphism of groups, where $H \subseteq G$, then $\vartheta' : \mathbf{k}G \longrightarrow \mathbf{k}H$, given by $\sum_{g\in G}\lambda_g g \mapsto \sum_{g\in G}\lambda_g\vartheta(g)$ is an algebra morphism.

We prove this by noting that $\mathbf{k}G = \mathbf{k}\langle g \mid g \in G\rangle$, so we need only check for $g \in G$. Let $g, g' \in G$. Because $\vartheta' = \vartheta$ on G, we have

$$\vartheta'(gg') = \vartheta(gg') = \vartheta(g)\vartheta(g') = \vartheta'(g)\vartheta'(g'),$$

so ϑ' is indeed an algebra morphism.

Note that $\varepsilon : \mathbf{k}G \longrightarrow \mathbf{k}$, given by $\sum_g \lambda_g g \mapsto \sum \lambda_g$, is just the case $H = \{1\}$ in the above. So ε is an algebra morphism. Hence $\mathbf{k}G$ is a bialgebra.

Example 1.2.4 (The Universal Enveloping Algebra). Consider the universal enveloping algebra defined in Example 1.1.3. Let $\{x_1, \cdots, x_n\}$ be a basis for $\mathfrak{g}$. This is in fact a bialgebra, as may be seen by considering the following maps:

$$\begin{aligned}\Delta : U(\mathfrak{g}) &\longrightarrow U(\mathfrak{g})\otimes U(\mathfrak{g}), \quad \text{given by } x_i \mapsto x_i\otimes 1 + 1\otimes x_i \quad \text{and} \\ \varepsilon : U(\mathfrak{g}) &\longrightarrow \mathbf{k}, \quad \text{given by } x_i \mapsto 0, \quad \forall\, i = 1, \cdots, n.\end{aligned}$$

As usual, we want to extend these maps to all of $U(\mathfrak{g})$ in order to make Δ and ε into algebra morphisms. Unlike in the previous examples, this is not a trivial matter, since we need to show that Equation 1.1 holds under Δ and ε. We show the case for Δ; that for ε is even simpler.

$$
\begin{aligned}
\Delta(x_ix_j - x_jx_i) &= \Delta(x_i)\Delta(x_j) - \Delta(x_j)\Delta(x_i) \\
&= (x_i\otimes 1 + 1\otimes x_i)(x_j\otimes 1 + 1\otimes x_j) - (x_j\otimes 1 + 1\otimes x_j)(x_i\otimes 1 + 1\otimes x_i) \\
&= x_ix_j\otimes 1 + x_i\otimes x_j + x_j\otimes x_i + 1\otimes x_ix_j - (x_jx_i\otimes 1 + x_j\otimes x_i + x_i\otimes x_j + 1\otimes x_jx_i) \\
&= (x_ix_j - x_jx_i)\otimes 1 + 1\otimes(x_ix_j - x_jx_i) \\
&= (\sum_{l=1}^{n} a_{ijl}x_l)\otimes 1 + 1\otimes(\sum_{l=1}^{n} a_{ijl}x_l) \\
&= \Delta(\sum_{l=1}^{n} a_{ijl}x_l).
\end{aligned}
$$

We already know that $U(\mathfrak{g})$ is an algebra from Example 1.1.3. We check that $(U(\mathfrak{g}), \Delta, \varepsilon)$ is a coalgebra. We do the check for coassociativity; the counit check is similar and is omitted.

$$
\begin{aligned}
(\Delta\otimes id)\circ\Delta(x_i) &= (\Delta\otimes id)(x_i\otimes 1 + 1\otimes x_i) \\
&= (x_i\otimes 1\otimes 1 + 1\otimes x_i\otimes 1 + 1\otimes x_i\otimes 1 + 1\otimes 1\otimes x_i).
\end{aligned}
$$

However,

$$
\begin{aligned}
(id\otimes\Delta)\circ\Delta(x_i) &= (id\otimes\Delta)(x_i\otimes 1 + 1\otimes x_i) \\
&= (x_i\otimes 1\otimes 1 + 1\otimes x_i\otimes 1 + 1\otimes 1\otimes x_i + 1\otimes 1\otimes x_i) \\
&= (\Delta\otimes id)\circ\Delta(x_i).
\end{aligned}
$$

Since we defined Δ and ε as algebra morphisms, this means that $(U(\mathfrak{g}), \Delta, \varepsilon)$ is a bialgebra.

These last two examples illustrate two very important classes of elements.

Definition 1.2.2.

(1) Let $C = (C, \Delta, \varepsilon)$ be a coalgebra and let $x \in C$. We say that x is *group-like* if $\Delta(x) = x\otimes x$, as for the elements of G in the group algebra $\mathbf{k}G$. We denote the set of group-like elements in C by $\mathcal{G}(C)$. Note that $\mathcal{G}(C)$ is in fact a monoid. Some authors also require that $\varepsilon(x) = 1$, for all $x \in \mathcal{G}(C)$; this is true but not strictly necessary, since $\varepsilon(x) = 1$ holds automatically for all $x \in \mathcal{G}(C)$. We show this in Proposition 1.3.5.

(2) Let $g, h \in \mathcal{G}(C)$. The element x of C is said to be *g,h-primitive* if $\Delta x = x\otimes g + h\otimes x$. The set of all g,h-primitives in C is denoted by $\mathcal{P}_{g,h}(C)$. We denote by $\mathcal{P}(C)$ the set $\{x \mid \Delta(x) = x\otimes 1 + 1\otimes x\}$; that is, the set of 1,1-primitives in C.

Remark 1.2.1. Under certain extra conditions, $\mathcal{G}(C)$ is a group. We delay proof of this to Proposition 1.3.5, which is part of our discussion of the antipode. We can, however, prove the following result immediately. The proof is from [Swe69, Theorem 3.2.1].

Lemma 1.2.3. *For a coalgebra C over a field $\mathbf{k}$, the set of group-like elements $\mathcal{G}(C)$ is $\mathbf{k}$-linearly independent.*

Proof. We proceed via contradiction. Suppose that $\mathcal{G}(C)$ is not linearly independent. Clearly, $0 \notin \mathcal{G}(C)$, since then $\varepsilon(0) = 0$, and we show in the proof of Proposition 1.3.5 that $\varepsilon(x) = 1$ for all $x \in \mathcal{G}(C)$. So any single element of $\mathcal{G}(C)$ will form a linearly independent set. Choose $n \in \mathbb{Z}$ minimal with respect to the condition that any set of n distinct elements is linearly independent, and there are $n+1$ distinct elements in $\mathcal{G}(C)$ which are not linearly independent. So, for distinct $g, h_1, \cdots, h_n$ in $\mathcal{G}(C)$ with $n \geq 1$, we have the following relation:

$$g = k_1 h_1 + \cdots + k_n h_n, \quad \text{for nonzero elements } k_1, \cdots, k_n \in \mathbf{k}.$$

Thus we have the following two identities for $\Delta(g)$:

$$\begin{aligned} \Delta(g) &= g \otimes g = \sum_{i,j=1}^{n} k_i k_j h_i \otimes h_j \\ \Delta(g) &= \sum_{i=1}^{n} k_i \Delta(h_i) = \sum_{i=1}^{n} k_i h_i \otimes h_i \end{aligned} \tag{1.17}$$

We defined the set $\{h_i\}$ to be linearly independent, and chose $k_1, \cdots, k_n \neq 0$. So $\{h_i \otimes h_j\}$ must be a linearly independent set, and so $n = 1$, by Equation 1.17. Therefore, $g = k_1 h_1$. But then, since we have $\varepsilon(g) = \varepsilon(h_1) = 1$, we must have $k_1 = 1$ and $g = h_1$,which is a contradiction since g and h_1 were chosen to be distinct. Therefore, $\mathcal{G}(C)$ must be linearly independent. □

Example 1.2.5. Let A be an algebra and $\mathbf{k}$ a field. Define the algebra

$$\mathrm{Alg}(A, \mathbf{k}) = \{f \in A^* \mid \text{f is an algebra map from A to } \mathbf{k}\}$$

Let μ be the multiplication on $\mathrm{Alg}(A, \mathbf{k})$. Now $\mathrm{Alg}(A, \mathbf{k}) \subseteq A^o$, since for all $f \in \mathrm{Alg}(A, \mathbf{k})$ and $a, b \in A$,

$$\begin{aligned} \mu^* f(a \otimes b) &= f(\mu(a \otimes b)) \\ &= f(ab) \\ &= f(a) f(b) \quad \text{since} \quad f \in \mathrm{Alg}(A, \mathbf{k}) \\ &= f(a) \otimes f(b) \\ &= \langle f \otimes f, a \otimes b \rangle. \end{aligned}$$

Therefore, $\mu^*(f) = f \otimes f \in A^* \otimes A^*$ and so $f \in A^o$. Thus $\mathrm{Alg}(A, \mathbf{k}) \subseteq \mathcal{G}(A^o)$. Now consider $g \in \mathcal{G}(A^o)$. This means that $\mu^*(g) = g \otimes g$. So for all $a, b \in A$

$$(\mu^* g)(a \otimes b) = (g \otimes g)(a \otimes b) = g(a)g(b).$$

But also

$$(\mu^* g)(a \otimes b) = \langle g, \mu(a \otimes b) \rangle = g(ab).$$

Thus $g(ab) = g(a)g(b)$, so $g \in \mathrm{Alg}(A, \mathbf{k})$, thus $\mathrm{Alg}(A, \mathbf{k}) = \mathcal{G}(A^o)$.

Example 1.2.6. If $C = \mathbf{k}G$, then $\mathcal{G}(\mathbf{k}G) = G$, since $\mathcal{G}(C)$ is a linearly independent set.

Example 1.2.7 (A Further Example of a Bialgebra). Let $q \in \mathbf{k}$ be nonzero, and define $\mathcal{O}(\mathbf{k}^2) = \mathbf{k}\langle x, y \mid xy = qyx \rangle$. We define a bialgebra structure on $\mathcal{O}(\mathbf{k}^2)$ via $\Delta(x) = x \otimes x$, $\Delta(y) = y \otimes 1 + x \otimes y$, $\varepsilon(x) = 1$ and $\varepsilon(y) = 0$. Clearly, $x \in \mathcal{G}(\mathcal{O}(\mathbf{k}^2))$ and $y \in \mathcal{P}_{1,x}(\mathcal{O}(\mathbf{k}^2))$.

1.3 Hopf Algebras

A Hopf algebra is a bialgebra with an additional linear transform, called the *antipode* imposed on it. This class of transform will be defined shortly, but first we require the following definitions.

1.3.1 The Antipode and Convolution

Definition 1.3.1. Let $A = (A, \mu, \eta)$ be an algebra and $C = (C, \Delta, \varepsilon)$ be a coalgebra, and consider $f, g \in \mathrm{Hom}_{\mathbf{k}}(C, A)$. The *convolution* product, $f * g$, for all such f and g, is defined to be the composition of the maps

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\mu} A.$$

That is, for all $c \in C$,

$$(f * g)(c) = \mu \circ (f \otimes g) \circ \Delta(c),$$

or in Sweedler's sigma notation,

$$(f * g)(c) = \sum_c f(c_1) g(c_2). \tag{1.18}$$

The convolution map in fact defines an algebra structure on $\mathrm{Hom}_{\mathrm{k}}(C, A)$, as can be seen in the following proposition, [Kas95, Proposition III.3.1(a)].

Proposition 1.3.1. *The vector space $Hom_{\mathrm{k}}(C, A)$ is an algebra under convolution with unit given by $\eta \circ \varepsilon$.*

Proof. We wish to show that the convolution is associative. We use Equation (1.18) and the fact that the product and coproduct from A and C are associative and coassociative respectively. For $f, g, h \in \mathrm{Hom}_{\mathrm{k}}(C, A)$ and $c \in C$, we get

$$((f*g)*h)(c) = \sum_{c} f(c_1)g(c_2)h(c_3) = (f*(g*h))(c).$$

Now consider $\eta \circ \varepsilon$ and recall Equation 1.6. Then, for $c \in C$, we have

$$((\eta \circ \varepsilon)*f)(c) = \sum_{c} \varepsilon(c_1)1f(c_2) = f(\sum_{c} \varepsilon(c_1)c_2) = f(c), \quad \text{via Equation 1.6.}$$

Similarly, one shows that $\eta \circ \varepsilon$ is a right unit under convolution. Thus $\mathrm{Hom}_{\mathrm{k}}(C, A)$ is an algebra. $\square$

We now consider a special case of this situation. Let H be a bialgebra and let $C = A = H$. This enables us to define the convolution on $\mathrm{End}_{\mathrm{k}}(H)$.

Definition 1.3.2. Consider a bialgebra $(H, \mu, \eta, \Delta, \varepsilon)$ and choose $S \in \mathrm{End}_{\mathrm{k}}(H)$. Then S is said to be an *antipode* of the bialgebra H if

$$S*id_H = id_H*S = \eta \circ \varepsilon,$$

that is, if it is an inverse for the identity, under the operation of convolution. This can be rewritten using Sweedler's notation as

$$\sum_{x} x_1 S(x_2) = \varepsilon(x)1_H = \sum_{x} S(x_1)x_2. \tag{1.19}$$

Definition 1.3.3. We can now define a Hopf algebra as being a bialgebra with an antipode. We denote a Hopf algebra with antipode S by $(H, \mu, \eta, \Delta, \varepsilon, S)$.

Definition 1.3.4.

(1) Let A and B be two Hopf algebras and let $g : A \longrightarrow B$ be a map. It is a *Hopf algebra morphism* if it is a morphism of the underlying bialgebras and commutes with the antipodes, that is $g(S_A a) = S_B g(a)$.

(2) Let I be a subspace of a Hopf algebra A. If I is a biideal and $SI \subseteq I$, then I is a *Hopf ideal*. Clearly, A/I is then a Hopf algebra with structures inherited from A.

Not all bialgebras are Hopf algebras since not all necessarily have antipodes. However, if a bialgebra does have an antipode, then it is unique. To see this, consider two antipodes S and S':

$$S = S*(\eta\circ\varepsilon) = S*(id*S') = (S*id)*S' = (\eta\circ\varepsilon)*S' = S'.$$

1.3.2 Some Properties of the Antipode

The following three results state some of the basic properties of the antipode. In each case, the proof is taken from [Kas95, Theorem III.3.4].

Theorem 1.3.2. *Let $H = (H, \mu, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra. Then S has the following properties:*

(1) S is an *anti-algebra morphism*; that is, for all $x, y \in H$,

$$\begin{aligned} S(xy) &= S(y)S(x) \\ S(1) &= 1, \end{aligned}$$

(2) S is an *anti-coalgebra morphism*; that is

$$\begin{aligned} \Delta\circ S &= (S\otimes S)\circ\Delta^{op} = \tau_{H,H}\circ(S\otimes S)\circ\Delta \qquad (1.20) \\ \varepsilon\circ S &= \varepsilon. \end{aligned}$$

We note for future reference that Equation 1.20 may be rewritten as:

$$\sum_{S(x)} S(x)_1 \otimes S(x)_2 = \sum_x S(x_2) \otimes S(x_1). \qquad (1.21)$$

Proof.

(1) Let $\alpha, \beta \in \operatorname{Hom}(H \otimes H, H)$ with $\alpha(x \otimes y) = S(y)S(x)$ and $\beta(x \otimes y) = S(xy)$, for all $x, y \in H$. To show that these maps are equivalent, it is enough to show that $(\beta * \mu) = (\mu * \alpha) = (\eta\varepsilon)$. For $(\beta * \mu)$ we have

$$\begin{aligned}
(\beta*\mu)(x\otimes y) &= \sum_{x\otimes y} \beta((x\otimes y)_1)\mu((x\otimes y)_2) \quad \text{by Equation 1.18} \\
&= \sum_{(x)(y)} \beta(x_1\otimes y_1)\mu(x_2\otimes y_2) \quad \text{by the bialgebra structure on } H\otimes H \\
&= \sum_{(x)(y)} S(x_1 y_1)x_2 y_2 \\
&= \sum_{(xy)} S(xy)_1(xy)_2 \quad \text{by Equation 1.16} \\
&= \eta\varepsilon(xy) \quad \text{by Equation 1.6.}
\end{aligned}$$

We proceed in a similar manner to show that $\mu * \alpha = \eta\varepsilon$.

$$\begin{aligned}
(\mu*\alpha)(x\otimes y) &= \sum_{x\otimes y} \mu((x\otimes y)_1)\alpha((x\otimes y)_2) \\
&= \sum_{(x)(y)} \mu(x_1\otimes y_1)\alpha(x_2\otimes y_2) \\
&= \sum_{(x)(y)} x_1 y_1 S(y_2)S(x_2) \\
&= \sum_{x} x_1(\sum_{y} y_1 S(y_2))S(x_2) \\
&= \sum_{x} x_1 \eta\varepsilon(y)S(x_2) \quad \text{by Equation 1.19} \\
&= \eta\varepsilon(x)\eta\varepsilon(y) \\
&= \eta\varepsilon(xy)
\end{aligned}$$

which proves the identity.

To show that $S(1) = 1$, we need only note that $1S(1) = (id * S(1)) = \eta\varepsilon(1) = 1$.

(2) To prove that $\Delta \circ S = \tau_{H,H} \circ (S \otimes S) \circ \Delta$, we first define $\alpha = \Delta \circ S$ and $\beta = \tau_{H,H} \circ (S \otimes S) \circ \Delta$. It is sufficient to show that $\alpha * \Delta = \Delta * \beta = (\eta \otimes \eta)\varepsilon$. Let $x \in H$. Then for α we have

$$\begin{aligned}
(\alpha * \Delta)(x) &= \sum \alpha(x_1)\Delta(x_2) \quad \text{by Equation 1.18} \\
&= \sum \Delta(S(x_1))\Delta(x_2) \\
&= \Delta(\sum S(x_1)x_2) \\
&= \Delta(\eta\varepsilon(x)) \quad \text{by Equation 1.6} \\
&= ((\eta \otimes \eta)\varepsilon)(x).
\end{aligned}$$

We now consider β. As before, let $x \in H$.

$$\begin{aligned}
(\Delta * \beta)(x) &= \sum \Delta(x_1)(\tau \circ (S \otimes S) \circ \Delta)(x_2) \\
&= \sum (x_1 \otimes x_2)(\tau \circ (S \otimes S))(x_3 \otimes x_4) \\
&= \sum (x_1 \otimes x_2)(S(x_4) \otimes S(x_3)) \\
&= \sum x_1 S(x_4) \otimes x_2 S(x_3) \\
&= \sum x_1 S(x_3) \otimes \varepsilon(x_2)1 \quad \text{by Equation 1.19} \\
&= \sum x_1 \varepsilon(x_2) S(x_3) \otimes 1 \quad \text{since } \varepsilon(x_2) \in \mathbf{k} \\
&= \sum x_1 S(x_2) \otimes 1 \quad \text{by Equation 1.6} \\
&= \varepsilon(x) 1 \otimes 1 \quad \text{by Equation 1.19} \\
&= (\eta \otimes \eta)(\varepsilon(x)).
\end{aligned}$$

We also wish to prove that $\varepsilon \circ S = \varepsilon$. But this is clear, since for all $x \in H$,

$$\begin{aligned}
\varepsilon \circ S(x) &= \varepsilon(S(\sum \varepsilon(x_1)x_2)) \\
&= \varepsilon(\sum \varepsilon(x_1)S(x_2)) \\
&= \sum \varepsilon(x_1)\varepsilon(S(x_2)) \\
&= \varepsilon(\sum x_1 S(x_2)) \\
&= \varepsilon(\eta\varepsilon(x)) \\
&= \varepsilon(x),
\end{aligned}$$

by Equation 1.6 and Equation 1.19.

□

Lemma 1.3.3. *Let H be a Hopf algebra. Then for all $x \in H$, the following are equivalent:*

(1) $S^2 = id_H$

(2) $\sum S(x_2)x_1 = \varepsilon(x)1$*, for all* $x \in H$

(3) $\sum x_2 S(x_1) = \varepsilon(x)1$*, for all* $x \in H$*.*

Proof. We show that the first and second statements are equivalent; showing that the first and third are equivalent follows in a similar fashion.

(1) $\Rightarrow$ (2): We suppose (1), and let $x \in H$. Note that $S^2(x) = \mathrm{id}_H(x) = x$. So

$$\begin{aligned}
\sum S(x_2)x_1 &= S^2(\sum S(x_2)x_1) \\
&= S(\sum S(x_1)S^2(x_2)) \quad \text{by properties of the antipode} \\
&= S(\sum S(x_1)x_2) \\
&= S(\varepsilon(x)1) \quad \text{by Equation 1.19} \\
&= \varepsilon(x)1.
\end{aligned}$$

(2) $\Rightarrow$ (1): The inverse is unique under convolution, so it is sufficient to show that S^2 is an inverse for S under convolution. By Theorem 1.3.2(1) and the fact that $\sum S(x_2)x_1 = \varepsilon(x)1$, we have, for $x \in H$,

$$\begin{aligned}
(S{*}S^2)(x) &= \sum_x S(x_1)S^2(x_2) \\
&= \sum_x S(S(x_2)x_1) \\
&= S(\sum_x S(x_2)x_1) \\
&= S(\varepsilon(x)1) \\
&= \varepsilon(x)S(1) \\
&= \varepsilon(x)1.
\end{aligned}$$

for all $x \in H$. So $S{*}S^2 = \eta\varepsilon$. The proof for (3) $\Leftrightarrow$ (1) is similar. $\square$

Corollary 1.3.4. *If H is commutative or cocommutative, then $S^2 = id_H$.*

Proof. We recall Equation 1.19:

$$\sum x_1 S(x_2) = \varepsilon(x)1 = \sum S(x_1)x_2,$$

for all $x \in H$. Suppose that H is commutative. Then we have

$$\sum S(x_2)x_1 = \varepsilon(x)1$$

which, by the lemma proved above, implies that $S^2 = id$. Similarly, if H is cocommutative, we have $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$, so

$$\sum S(x_2)x_1 = \varepsilon(x).$$

As before, by Lemma 1.3.3, we then have $S^2 = id$. □

We are now in a position to prove the claim made in Definition 1.2.2, i.e that the set of group-like elements is in fact a group under certain conditions.

Proposition 1.3.5. *Let H be a bialgebra. Then $\mathcal{G}(H)$ is a monoid under the multiplication of H with unit 1. Further, if H is a Hopf algebra with invertible antipode S, then $\mathcal{G}(H)$ is a group, where the inverse of every $x \in \mathcal{G}(H)$ is $S(x)$. Further, $\varepsilon(x) = 1$ for all $x \in \mathcal{G}(H)$.*

Proof. It is clear that $\mathcal{G}(H)$ is a monoid. Now suppose that H is a Hopf algebra. We only need to show that the inverse of any group-like element is $S(x)$. Let $x \in \mathcal{G}(H)$. First we want to show that $S(x)$ is actually in $\mathcal{G}(H)$:

$$\begin{aligned}
\Delta(S(x)) &= \sum_{(S(x))} S(x)_1 \otimes S(x)_2 \\
&= \sum_{(x)} S(x_2) \otimes S(x_1) \quad \text{by Equation 1.21} \\
&= \sum_{(x)} (S \otimes S)(x_2 \otimes x_1) \\
&= (S \otimes S)(\tau \circ \Delta(x)) \\
&= (S \otimes S)(x \otimes x) \\
&= S(x) \otimes S(x)
\end{aligned}$$

So $S(x)$ belongs to $\mathcal{G}(H)$. Now by Equation 1.19

$$xS(x) = S(x)x = \varepsilon(x)1$$

But by definition of Δ,

$$(id\otimes\varepsilon)\circ\Delta(x) = x\otimes 1, \quad \forall\, x \in H.$$

Also, for $x \in \mathcal{G}$,

$$(id\otimes\varepsilon)\circ\Delta(x) = (id\otimes\varepsilon)(x\otimes x) = x\otimes\varepsilon(x) = x\otimes 1.$$

So $\varepsilon(x) = 1$. We note that this argument may also be applied to coalgebras, so we may apply it to Lemma 1.2.3. Finally, $xS(x) = S(x)x = 1$, so x is invertible with inverse $S(x)$. Hence $\mathcal{G}(H)$ is a group. □

Definition 1.3.2 is not always particularly useful for detecting Hopf algebras, since attempting check the antipode condition for every element of a bialgebra may be quite difficult. The following lemma shows that one need only check the antipode condition on a generating set.

Lemma 1.3.6. *Let $H = (H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra, generated (as an algebra) by a subset X, and let $S : H \longrightarrow H^{op}$ be an algebra morphism, such that*

$$\sum\nolimits_{(x)} x_{(1)}S(x_{(2)}) = \varepsilon(x)1 = \sum\nolimits_{(x)} S(x_{(1)})x_{(2)}, \quad \forall\, x \in X.$$

Then S is an antipode for H.

Proof. All that is needed is to show that if the defining relation holds for x and y, then it must also hold for xy. To do this, we need Equations 1.19 and 1.20. Then, for all $x, y \in H$, we have

$$\begin{aligned}
\sum (xy)_1 S((xy)_2) &= \sum x_1 y_1 S(x_2 y_2)\\
&= \sum x_1 y_1 S(y_2) S(x_2)\\
&= \sum x_1 (\sum y_1 S(y_2)) S(x_2)\\
&= (\sum x_1 S(x_2))\varepsilon(y)\\
&= \varepsilon(x)\varepsilon(y)\\
&= \varepsilon(xy).
\end{aligned}$$

One may similarly prove that $\sum S((xy)_1)(xy)_2 = \varepsilon(xy)$. □

1.3.3 Some Examples of Hopf Algebras

Example 1.3.1 (The Finite Dual). If H is a Hopf algebra with antipode S, then so is H^o with antipode S^*. A proof of this can be found in [Mon93, p. 151].

Example 1.3.2 (The Group Algebra). We have already shown (Example 1.1.7) that the group algebra is a bialgebra. Now define the linear map

$$S : \mathbf{k}G \longrightarrow \mathbf{k}G; \quad g \mapsto g^{-1}, \quad \forall\, g \in G.$$

Recall the definition of the convolution map (Definition 1.3.2). To show that $\mathbf{k}G$ is a Hopf algebra, we need to show that S satisfies $S{*}id_H = id_H{*}S = \eta\circ\varepsilon$. But for all $g \in G$, we have:

$$(\mu\circ(id_G\otimes S)\circ\Delta)(g) = \mu \circ (id_G\otimes S)(g\otimes g) = \mu(g\otimes g^{-1}),$$

which clearly is equal to $(\mu\circ(S\otimes id_G)\circ\Delta)(g)$ and $(\eta\otimes\varepsilon)(g) = 1_G$. Thus, by Lemma 1.3.6, S is an antipode for $\mathbf{k}G$, so $\mathbf{k}G$ is a Hopf algebra.

Example 1.3.3 (Return to the Universal Enveloping Algebra). We have already shown in Example 1.2.4 that $U(\mathfrak{g})$ is a bialgebra. As in Example 1.3.2 above, to prove that it is Hopf algebra, we only need to prove that it has an antipode. Let $\{x_1, \cdots, x_n\}$ be a basis for $\mathfrak{g}$. We define the map

$$S : U(\mathfrak{g}) \longrightarrow U(\mathfrak{g}), \quad \text{given by} \quad x \mapsto -x, \quad \forall\, x \in \mathfrak{g}.$$

This is the antipode, as may be seen by the following computations:

$$\begin{aligned}(\mu\circ(id_{U(\mathfrak{g})}\otimes S)\circ\Delta)(x_i) &= \mu \circ (id_{U(\mathfrak{g})}\otimes S)(x_i\otimes 1 + 1\otimes x_i)\\ &= \mu(x_i\otimes 1 - 1\otimes x_i)\\ &= 0.\end{aligned}$$

Clearly, this is equal to $(\mu\circ(S\otimes id_G)\circ\Delta)(x_i)$. We also have

$$(\eta\circ\varepsilon)(x_i) = \eta(0_{\mathbf{k}}) = 0.$$

So, by Lemma 1.3.6, S is indeed an antipode, and $U(\mathfrak{g})$ is a Hopf algebra. An easy check shows that it is in fact a *cocommutative* Hopf algebra, that is, $\tau\circ\Delta(x_i) = \Delta(x_i)$ for all $x_i \in \mathfrak{g}$ where τ is the flip map. We prove this by the following calculation:

$$\tau \circ \Delta(x_i) = \tau(x_i\otimes 1 + 1\otimes x_i) = 1\otimes x_i + x_i\otimes 1 = x_i\otimes 1 + 1\otimes x_i = \Delta(x_i).$$

However, $U(\mathfrak{g})$ is not commutative in general, unless $\mathfrak{g}$ is Abelian.

Example 1.3.4 (The Quantised Enveloping Algebra of $\mathfrak{sl}(2)$). Let $\mathbf{k}$ be the field of complex numbers. The Lie algebra $\mathfrak{sl}(2)$ is defined as the algebra of 2×2 trace zero matrices with complex entries. We define the *quantum enveloping algebra* of $\mathfrak{sl}(2)$ to be the algebra

$$U_q = U_q(\mathfrak{sl}(2)), \quad \text{where} \quad q \in \mathbf{k} \text{ and } q \neq 0, 1, -1$$

generated by the variables E, F, K and K^{-1} with the following relations:

$$\begin{aligned} KK^{-1} &= K^{-1}K = 1, \quad KEK^{-1} = q^2 E \\ KFK^{-1} &= q^{-2}F \quad \text{and} \quad [E,F] = \frac{K - K^{-1}}{q - q^{-1}}. \end{aligned}$$

We now define the algebra maps $\Delta : U_q \longrightarrow U_q \otimes U_q$, $\varepsilon : U_q \longrightarrow \mathbf{k}$ and $S : U_q \longrightarrow U_q$ by:

$$\begin{aligned} \Delta(E) &= 1\otimes E + E\otimes K, \quad \Delta(F) = K^{-1}\otimes F + F\otimes 1, \\ \Delta(K) &= K\otimes K, \quad \Delta(K^{-1}) = K^{-1}\otimes K^{-1}, \\ \varepsilon(E) &= \varepsilon(F) = 0, \quad \varepsilon(K) = \varepsilon(K^{-1}) = 1 \quad \text{and} \\ S(E) &= -EK^{-1}, \quad S(F) = -KF, \quad S(K) = K^{-1} \quad \text{and } S(K^{-1}) = K, \end{aligned}$$

With these maps, U_q is then a Hopf algebra. This is not difficult to prove, but requires substantial calculation, so only an outline is given here; full details can be found in [Kas95, pp. 141–142]. We first must show that Δ is indeed a morphism of algebras from U_q to $U_q \otimes U_q$. It is sufficient to check that

$$\begin{aligned} \Delta(K)\Delta(K^{-1}) &= \Delta(K^{-1})\Delta(K) = 1, \\ \Delta(K)\Delta(E)\Delta(K^{-1}) &= q^2\Delta(E), \\ \Delta(K)\Delta(F)\Delta(K^{-1}) &= q^{-2}\Delta(F), \\ [\Delta(E), \Delta(F)] &= \frac{\Delta(K) - \Delta(K^{-1})}{q - q^{-1}}. \end{aligned}$$

We then need to check that Δ is coassociative; it is sufficient to do this on the four generators. We also need to show that ε defines a morphism of algebras from U_q to $\mathbf{k}$ and satisfies the counit axiom. It finally remains to check that S defines an antipode — to do this, we have to check that it is an algebra morphism from U_q to ${U_q}^{op}$.

This involves verifying that the following four relations hold:

$$\begin{aligned} S(K^{-1})S(K) &= S(K)S(K^{-1}) = 1 \\ S(K^{-1})S(E)S(K) &= q^2 S(E) \\ S(K^{-1})S(F)S(K) &= q^{-2}S(F) \\ [S(F), S(E)] &= \frac{S(K)-S(K^{-1})}{q-q^{-1}}. \end{aligned}$$

For example, consider

$$S(K^{-1})S(E)S(K) = -K(EK^{-1})K^{-1} = -q^2EK^{-1} = q^2S(E).$$

By Lemma 1.3.6, all that remains to be done after this is to check that the relation

$$\sum\nolimits_x x_1 S(x_2) = \varepsilon(x)1 = \sum\nolimits_x S(x_1)x_2,$$

holds when x is one of E, F, K, K^{-1}. For example, let $x = K$. Let $\mu : U_q \otimes U_q \longrightarrow U_q$, given by $u \otimes v = uv$, be the multiplication on U_q for all $u, v \in U_q$. Then

$$\mu \circ (id \otimes S) \circ \Delta(K) = \mu \circ (id \otimes S)(K \otimes K) = \mu(K \otimes K^{-1}) = 1,$$

and similarly for $\mu \circ (S \otimes id) \circ \Delta$. We also consider the case for $x = E$, which gives

$$\mu \circ (id \otimes S) \circ \Delta(E) = \mu \circ (id \otimes S)(1 \otimes E + E \otimes K) = \mu(1 \otimes (-EK^{-1}) + E \otimes K^{-1}) = -EK^{-1} + EK^{-1} = 0,$$

and similarly for $\mu \circ (S \otimes id) \circ \Delta$.

This is an example of a Hopf algebra which is neither commutative nor cocommutative.

Example 1.3.5. This example was first given by Sweedler, and describes the smallest noncommutative, noncocommutative Hopf algebra. We let $\mathbf{k}$ be a field with characteristic not equal to 2. Define

$$H_4 = \mathbf{k}\langle 1, g, x, gx \mid g^2 = 1,\ x^2 = 0,\ xg = -gx \rangle$$

with $\Delta(g) = g \otimes g$, $\Delta(x) = x \otimes 1 + g \otimes x$, and $\varepsilon(g) = 1$, $\varepsilon(x) = 0$. The antipode is given by $S(g) = g = g^{-1}$ and $S(x) = -gx$. We note that $g \in \mathcal{G}(H_4)$ and $x \in \mathcal{P}_{1,g}(H_4)$. We observe that H_4 has dimension 4 over $\mathbf{k}$.

For further reference, see [Taf71], where an infinite family of finite-dimensional Hopf algebras is constructed.

Example 1.3.6 (An Example of a Bialgebra Which is Not a Hopf Algebra). Recall Example 1.2.1. We claim that the element $\det(X)$ is group-like. Proof of the 2×2 case is obtained by a similar method to that given in Example 1.3.7 for the quantum determinant; proof of the general $n\times n$ case uses the same technique but is computationally tedious and so is omitted. Thus the bialgebra of polynomial functions on $n\times n$ matrices is not a Hopf algebra, because the group-like element $\det(X)$ is not generally invertible in $\mathcal{O}(M_n(\mathbf{k}))$. However, it is possible to construct two related bialgebras which are Hopf algebras, namely

$$\begin{aligned}\mathcal{O}(SL_n(\mathbf{k})) &= \mathcal{O}(M_n(\mathbf{k}))/(\det(X)-1),\\ \mathcal{O}(GL_n(\mathbf{k})) &= \mathcal{O}(M_n(\mathbf{k}))[(\det(X))^{-1}].\end{aligned}$$

These both have a bialgebra structure similar to that of $\mathcal{O}(M_n(\mathbf{k}))$ and antipodes defined by $SX = X^{-1}$, where X denotes the $n\times n$ matrix $[X_{ij}]$.

Example 1.3.7 (The Coordinate Ring of Quantum 2×2 Matrices). We begin by defining the coordinate ring of quantum $M_2(\mathbf{k})$. Choose $q \in \mathbf{k}$ such that q is not a root of unity. Then

$$\begin{aligned}\mathcal{O}_q(M_2(\mathbf{k})) &= \mathbf{k}\langle a,b,c,d\rangle, \quad \text{subject to the following relations}\\ ba &= q^{-1}ab \qquad ca = q^{-1}ac \qquad bc = cb\\ db &= q^{-1}bd \qquad dc = q^{-1}cd \qquad ad-da = (q-q^{-1})bc.\end{aligned}$$

There are two ways of expressing the coproduct and counit; see [Mon93, p. 219] for details of a method different to that shown here. Here, we define a comultiplication and counit as follows:

$$\begin{aligned}\Delta(a) &= a\otimes a + b\otimes c, \quad \Delta(b) = a\otimes b + b\otimes d\\ \Delta(c) &= c\otimes a + d\otimes c, \quad \Delta(d) = c\otimes b + d\otimes d\\ \varepsilon(a) &= \varepsilon(d) = 1, \quad \varepsilon(b) = \varepsilon(c) = 0.\end{aligned}$$

With these maps, $\mathcal{O}_k(M_2(\mathbf{k}))$ is a bialgebra. However, it is not a Hopf algebra, as may be seen by considering the quantum equivalent of the determinant, the *quantum determinant.* Let $X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and define the quantum determinant to be $\det_q(X) = ad - qbc$. We claim that $\det_q(X)$ is a group-like element. We prove this by the following calculation, which uses the relations on a,b,c,d given above.

$$
\begin{aligned}
\Delta(\det_q(X)) &= \Delta(ad-qbc)\\
&= \Delta(ad)-q\Delta(bc)\\
&= \Delta(a)\Delta(d)-q\Delta(b)\Delta(c)\\
&= (a\otimes a+b\otimes c)(c\otimes b+d\otimes d)-q(a\otimes b+b\otimes d)(c\otimes a+d\otimes c)\\
&= (ac\otimes ab+ad\otimes ad+bc\otimes cb+bd\otimes cd)-q(ac\otimes ba+ad\otimes bc+bc\otimes da+bd\otimes cd)\\
&= (ac\otimes ab+ad\otimes ad+bc\otimes cb+bd\otimes cd)-q(ac\otimes q^{-1}ab-ad\otimes bc-bc\otimes da-bd\otimes q^{-1}cd)\\
&= ad\otimes ad+bc\otimes cb-qad\otimes bc-qbc\otimes da.
\end{aligned}
$$

Also note that

$$
\begin{aligned}
\det_q(X)\otimes\det_q(X) &= (ad-qbc)\otimes(ad-qbc)\\
&= ad\otimes ad+q^2bc\otimes cb-qad\otimes bc-qbc\otimes ad\\
&= ad\otimes ad+q^2bc\otimes cb-qad\otimes bc-qbc\otimes(da+(q-q^{-1})cb)\\
&= ad\otimes ad+q^2bc\otimes cb-qad\otimes bc-qbc\otimes da-q^2cb\otimes cb+bc\otimes cb\\
&= ad\otimes ad-qad\otimes bc-qbc\otimes da+bc\otimes cb\\
&= ad\otimes ad+bc\otimes cb-qad\otimes bc-qbc\otimes da\\
&= \Delta(\det_q(X)),
\end{aligned}
$$

where the third line holds via the relation on $ad-da$. So $\det_q(X)$ is a group-like element and is not invertible in $\mathcal{O}_q(M_2(\mathbf{k}))$. Therefore, $\mathcal{O}_q(M_2(\mathbf{k}))$ cannot be a Hopf algebra.

It is possible to show that $\det_q(X)$ is central in $\mathcal{O}_q(M_2(\mathbf{k}))$. It is sufficient to prove this on the generating set; we do the case for a — those for the remaining generators are similar.

$$
\begin{aligned}
a(ad-qbc) &= a^2d-qabc\\
&= a(da+(q-q^{-1})bc)-qabc\\
&= ada-aq^{-1}bc\\
&= ada-bac\\
&= ada-qbca\\
&= (ad-qbc)a \quad \text{by the relations on } (a,b,c,d).
\end{aligned}
$$

Since $\det_q(X)$ is central, we may now proceed analogously to Example 1.3.6, and define the Hopf algebras

$$\begin{aligned} \mathcal{O}_q(SL_2(\mathbf{k})) &= \mathcal{O}_q(M_2(\mathbf{k}))/(\det_q(X) - 1), \\ \mathcal{O}_q(GL_2(\mathbf{k})) &= \mathcal{O}_q(M_2(\mathbf{k}))[(\det_q(X))^{-1}]. \end{aligned}$$

These inherit the bialgebra structure from $\mathcal{O}_q(M_2(\mathbf{k}))$, in the first case because $(\det_q(X) - 1)$ is a biideal. Their antipodes are uniquely determined by the condition

$$X(SX) = (SX)X = I_{2\times 2}.$$

To describe this, we discuss the quantum determinant of the adjoint matrix. We write $X = [X_{ij}] = \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$ and let Y_{ji} be the scalars obtained by deleting the i^{th} row and j^{th} column. We then define $S(X_{ij}) = (\det_q(X))^{-1}(-q)^{i-j}Y_{ji}$. That is, in terms of our original definition of X,

$$S\begin{bmatrix} a & b \\ c & d \end{bmatrix} = [ad - qbc]^{-1}\begin{bmatrix} d & -q^{-1}b \\ -qc & a \end{bmatrix}$$

If we set $q = 1$, then we get $\mathcal{O}(M_2(\mathbf{k}))$, the polynomial functions on 2×2 matrices. As one might expect, there is a corresponding definition for $\mathcal{O}_q(M_n(\mathbf{k}))$; for details on this, see [Mon93, pp. 220–221].

1.4 Modules and Comodules

Definition 1.4.1. Let A be a $\mathbf{k}$-algebra. We say that a $\mathbf{k}$-space M is a (left) *A-module* if there exists a $\mathbf{k}$-linear map $\alpha : A\otimes M \longrightarrow M$, such that the following diagrams commute:

$$\begin{tikzcd} A\otimes A\otimes M \arrow[r, "\mu\otimes id"] \arrow[d, "id\otimes\alpha"'] & A\otimes M \arrow[d, "\alpha"'] \\ A\otimes M \arrow[r, "\alpha"] & M \end{tikzcd} \qquad \begin{tikzcd} \mathbf{k}\otimes M \arrow[r, "\eta\otimes id"] \arrow[dr, "m"] & A\otimes M \arrow[d, "\alpha"] \\ & M \end{tikzcd}$$

where the map m denotes scalar multiplication. These axioms are the associativity and unit diagrams respectively.

We now dualise the definition of algebras acting on modules to the situation for coalgebras.

Definition 1.4.2. Let C be a $\mathbf{k}$-coalgebra. We say that a $\mathbf{k}$-space M is a (right) *C-comodule* if there exists a $\mathbf{k}$-linear map $\rho : M \longrightarrow M \otimes C$, such that the following diagrams commute:

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M\otimes C \arrow[d, "id\otimes\Delta"] \\ M\otimes C \arrow[r, "\rho\otimes id"] & M\otimes C\otimes C \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\rho"] \arrow[dr, "\otimes 1"'] & M\otimes C \arrow[d, "id\otimes\varepsilon"] \\ & M\otimes \mathbf{k} \end{tikzcd}$$

These diagrams represent the coassociativity and counit axioms respectively.

Definition 1.4.3.

(1) Let C be a $\mathbf{k}$-coalgebra, and let M, N be C-comodules with structure maps ρ and ν respectively. A linear map $g : M \longrightarrow N$ is a morphism of C-comodules if $(g\otimes id)\circ\rho = \nu\circ g$.

(2) Consider a right subcomodule D of C, that is, a subspace such that $\Delta(D) \subseteq D\otimes C$. Then D is a *right coideal* of C. Similarly, a *left coideal* E is a subspace of C satisfying $\Delta(E) \subseteq C\otimes E$.

There is a summation notation for right comodules. Let ρ be the comodule map. Then $\rho(m) = \sum m_0 \otimes m_1 \in M\otimes C$, for $m_0 \in m$ and $m_1 \in C$.

As one might expect, there is a close relationship between modules and comodules.

Lemma 1.4.1. *Let C be a coalgebra. Suppose M is a right C-comodule. Then M is also a left C^*-module.*

Proof. Let $\rho : M \longrightarrow M\otimes C$ be the comodule map via $\rho(m) = \sum m_0\otimes m_1$. Let $h \in C^*$. Then one may define M as a C^*-module via the map

$$h{\cdot}m = \sum \langle h, m_1\rangle m_0, \quad \text{where } \langle , \rangle \text{ is the bilinear form in Definition 1.1.8.}$$

□

The converse of this lemma is false in general, unless one assumes certain finiteness conditions. For example, consider the result [Mon93, Lemma 1.6.4]. This states that if M is a left A-module, it is a right A^o module (where A^o is the finite dual) if and only if $\{A{\cdot}m\}$ is finite dimensional, for all $m \in M$. Those modules for which the converse does hold are called *rational*; see [Abe80, p. 127] for further details. We consider such a module in Example 1.4.2.

1.4.1 Examples

Example 1.4.1.

(1) Let C be a coalgebra. Then C is a right comodule over itself with $\rho = \Delta$. By Lemma 1.4.1, we can define a left action of C^* on C via

$$f \rightharpoonup c = \sum \langle f, c_2 \rangle c_1,$$

for all $f \in C^*$ and $c \in C$.

We can also define this action in terms of right multiplication in C^*. Recall Equation 1.18, and consider $g, h \in C^*$ and $c \in C$. Then

$$\langle h, g \rightharpoonup c \rangle = \sum \langle g, c_2 \rangle \langle h, c_1 \rangle = (h * g)(c) = \langle hg, c \rangle.$$

In other words, the action $\rightharpoonup$ is the same as the transpose of right multiplication of C^* on itself. We may similarly define the right action of C^* on C, given by

$$c \leftharpoonup f = \sum \langle f, c_1 \rangle c_2.$$

Following a similar argument to that above, $\langle h, c \leftharpoonup g \rangle = \langle gh, c \rangle$, so $\leftharpoonup$ is the transpose of left multiplication of C^* on itself.

(2) One may proceed analogously with an algebra A, by defining the left action $a \rightharpoonup f$, for all $a \in A$ and $f \in A^*$, which is the transpose of right multiplication on A; that is,

$$\langle a \rightharpoonup f, b \rangle = \langle f, ba \rangle, \quad \forall\, b \in A.$$

If the element f is contained in the finite dual of A, we can then define $\Delta(f)$, and in a similar way to that above, we get $a \rightharpoonup f = \sum \langle f_2, a \rangle f_1$. Of course, we can make an equivalent definition for the transpose of left multiplication by a on A.

Example 1.4.2. Let D be a left C^*-submodule of the finite-dimensional coalgebra C. Then D is a right C-subcomodule, and so the converse to Lemma 1.4.1 holds in this case.

Proof. Fix a basis for C consisting of a basis $\{d_i \mid i = 1, \cdots, m\}$ of D, together with a basis $\{d_j \mid j = m+1, \cdots, n\}$ for a vector space complement to D in C. Let $d \in D$ and write

$$\Delta(d) = \sum_{i=1}^{n} d_i \otimes d_i',$$

for suitable $d_i' \in C$.

We say that the d_j are linearly independent mod(D). Now for any $f \in C^*$, $f \rightharpoonup c = \sum_{i=1}^{n} f(d_i')d_i \in D$. But $d_{m+1}, \cdots, d_n$ are independent mod(D), so $f(d_i') = 0$ for all $i > m$. This holds for all $f \in C^*$, so $d_i' = 0$ for all $i > m$; therefore $\Delta(d) \in D \otimes C$. Hence D is indeed a right C-comodule. $\square$

Example 1.4.3. Let $C = \mathbf{k}G$. Then M is a (right) $\mathbf{k}G$-comodule if and only if it is a G-graded $(\mathbf{k}G)$-module. Recall that a module is G-graded if $M = \oplus_{g \in G} M_g$.

Proof.
$\Rightarrow$: Let $m \in M$. We define the comodule map to be $\rho(m) = \sum m_g \otimes g$. We have

$$(id \otimes \Delta) \circ \rho(m) = (id \otimes \Delta)(\sum_{g \in G} m_g \otimes g) = \sum m_g \otimes g \otimes g.$$

But by the coassociative condition for comodules, this is equal to

$$(\rho \otimes id) \circ \rho(m) = (\rho \otimes id)(\sum_{g} (m_g \otimes g)) = \sum_{g,h} (m_g)_h \otimes h \otimes g.$$

This implies that $(m_g)_h = \delta_{g,h} m_g$. So $\rho(m_g) = \sum_g \delta_{g,h} m_g \otimes g = m_g \otimes g$. If we set $M_g = \{m_g \mid m_g \in M\}$, the sum is then direct. It remains to show that $\oplus_g M_g = M$. We do this by using the counit axiom to prove that $\sum m_g = m$, for all $m_g \in M$. We have $(id \otimes \varepsilon) \circ \rho(m) = \sum_g m_g \otimes 1$. But by the counit axiom, this is equal to $m \otimes 1$. Therefore, $\sum m_g = m$ as required.

$\Leftarrow$: Suppose that $M = \oplus_{g \in G} M_g$ is a G-graded $(\mathbf{k}G)$-module. We set $\rho(m) = m \otimes g$, for all $m \in M_g$. We want to check that the coassociative and counit axioms hold for this map. For all $m \in M_g$ we have

$$\begin{aligned}
(id \otimes \Delta) \circ \rho(m) &= (id \otimes \Delta)(m \otimes g) = m \otimes g \otimes g, \quad \text{and} \\
(\rho \otimes id) \circ \rho(m) &= (\rho \otimes id)(m \otimes g) = m \otimes g \otimes g,
\end{aligned}$$

so the coassociativity axiom holds. We verify the counit axiom via the following calculation:

$$(id \otimes \varepsilon) \circ \rho(m) = (id \otimes \varepsilon)(m \otimes g) = m \otimes 1,$$

which proves the result. $\square$

1.4.2 Invariants and Coinvariants

Definition 1.4.4.

(1) Let A be a Hopf algebra and let M be a left A-module. The *invariants* of A on M are defined to be the set

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

(2) Let M be a right A-comodule with comodule map ρ. Then the *set of coinvariants of A in M* is defined as the set

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

(3) Let J be a Hopf algebra and consider its dual J^*. The *space of left integrals*, denoted I_J, is given as

$$I_J = \{j \in J^* \mid ij = \varepsilon(i)j \;\forall\, i \in J^*\}.$$

The *space of right integrals* is given by

$${}_JI = \{\, j \in J^* | \, ji = \varepsilon(i)j \;\forall\, i \in J^*\}.$$

We postpone further discussion of these concepts until the next chapter.

(4) We make the observation that if $\vartheta : A \longrightarrow B$ is a Hopf algebra morphism, A is a right and left B-comodule via the maps

$$\begin{aligned}\rho &= (id_A\otimes\vartheta)\circ\Delta\\ \phi &= (\vartheta\otimes id_A)\circ\Delta\end{aligned}$$

We denote the set of coinvariants for ρ by A_ρ^{coB} and the set of coinvariants for ϕ by A_ϕ^{coB}. Thus,

$$\begin{aligned}A_\rho^{coB} &= \{a \in A \mid \rho(a) = a\otimes 1\}\\ A_\phi^{coB} &= \{a \in A \mid \phi(a) = 1\otimes a\}.\end{aligned}$$

We note the following basic fact about invariants and coinvariants.

Lemma 1.4.2. *Let A be a Hopf algebra. Then A_ρ^{coB} and A_ϕ^{coB} are subalgebras of A.*

Proof. We consider the case for A_ρ^{coB}. Let $x, y \in A_\rho^{coB}$. Then

$$\begin{aligned} \rho(x-y) &= \rho(x) - \rho(y) \\ &= (x \otimes 1) - (y \otimes 1) \\ &= (x-y) \otimes 1, \end{aligned}$$

so $(x-y) \in A_\rho^{coB}$. We also need to show that A_ρ^{coB} is closed under multiplication. We have

$$\begin{aligned} \rho(xy) &= \sum (xy)_0 \otimes (xy)_1 \\ &= \sum x_0 y_0 \otimes x_1 y_1 \\ &= \sum (x_0 \otimes x_1)(y_0 \otimes y_1) \\ &= (x \otimes 1)(y \otimes 1) \\ &= (xy \otimes 1), \end{aligned}$$

so clearly $xy \in A_\rho^{coB}$. It is clear that $\lambda x \in A_\rho^{coB}$ for all $\lambda \in \mathbf{k}$. Thus A_ρ^{coB} is a subalgebra of A. One uses a similar argument to show that A_ϕ^{coB} is also a subalgebra of A. □

Example 1.4.4.

(1) Let $H = \mathbf{k}G$, and let M be a left H-module. Consider the set of invariants,

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

It is sufficient to consider $h \in G$ only, since G forms a basis for H. Suppose that $m \in M^H$. Then $g \cdot m = \varepsilon(g)m = m$. So $M^H \subseteq M^G$, which is the set of elements of M fixed by G. Now let $m' \in M^G$. So $g \cdot m' = m' = 1m' = \varepsilon(g)m'$, since $\varepsilon(g) = 1$ for all $g \in G$. Thus $M^H = M^G$.

(2) With $H = \mathbf{k}G$ as above, let M be a right H-comodule with comodule map ρ. This means that it is a G-graded module, as shown in Example 1.4.3. Then $M^{coH} = \{m \in M \mid \rho(m) = m \otimes 1\}$, which is the identity component of the G-graded module M.

(3) Let $H = U(\mathfrak{g})$, and let M be a left H-module. Then the set of invariants is clearly $M^H = \{m \in M \mid g \cdot m = 0, \forall\, g \in \mathfrak{g}\}$, since $\varepsilon(g) = 0$ for all $g \in \mathfrak{g}$.

(4) Consider the Hopf algebra H. This is a left H-module algebra over itself via the so-called *adjoint action* of H on itself. This is given as $\mathrm{ad}_\ell(k)h = \sum k_1 h S(k_2)$, for $h, k \in H$. We discuss this important concept further in Definition 2.1.1. This gives $H^H = \{h \in H \mid k{\cdot}h = \mathrm{ad}_\ell(k)(h) = \varepsilon(k)h,\ \forall\, k \in H\}$. Let $Z(H)$ be the centre of H. We claim that $Z(H) = H^H$. Let $h \in Z(H)$. Then for all $k \in H$,

$$k{\cdot}h = \mathrm{ad}_\ell(k)h = \sum k_1 h S(k_2) = \sum k_1 S(k_2) h = \varepsilon(k)h$$

by Equation 1.19. So $Z(H) \subseteq H^H$. Now conversely, we consider $h \in H^H$. Let $k \in H$. Then

$$\begin{aligned} kh &= \sum k_1 \varepsilon(k_2) h \\ &= \sum k_1 h \varepsilon(k_2) \\ &= \sum k_1 h S(k_2) k_3 \\ &= \sum \mathrm{ad}_\ell(k_1)(h) k_2 \\ &= \sum \varepsilon(k_1) h k_2 \quad \text{because } h \in H^H \\ &= h \sum \varepsilon(k_1) k_2 \\ &= hk. \end{aligned}$$

Hence $H^H = Z(H)$.

The following result is taken from [Mon93, Lemma 1.7.2].

Lemma 1.4.3. *Let H be a Hopf algebra such that H^* is also a Hopf algebra. Let M be a right H-comodule with comodule map $\rho : M \longrightarrow M \otimes H$, given by $\rho(m) = \sum m_0 \otimes m_1$. It is thus a left H^*-module, by Lemma 1.4.1. Considering both structures on M, we have that $M^{H^*} = M^{\mathrm{co}H}$.*

Proof. We first show that $M^{H^*} \subseteq M^{\mathrm{co}H}$. Consider $m \in M^{H^*}$. Then for all $f \in H^*$,

$$\begin{aligned} f{\cdot}m &= \varepsilon(f)m \\ \Leftrightarrow \quad \sum f(m_1)m_0 &= \varepsilon(f)m && (1.22) \\ \Leftrightarrow \quad \sum f(m_1)m_0 &= f(1)m && (1.23) \end{aligned}$$

Now we note that the expression $\sum m_0 \otimes m_1$ can be written with the $\{m_0\}$ linearly independent over $\mathbf{k}$. We know that $m = \sum \varepsilon(m_1)m_0$ since $\varepsilon \in H^*$ and $m \in M^{H^*}$, so this implies that $f(m_1) = f(1)\varepsilon(m_1)$, for all m_1 and for all $f \in H^*$. But this is true if and only if $m_1 \in \mathbf{k}$, since if $m_1 \notin \mathbf{k}$, then we can find $f \in H^*$ such that $f(m_1) \neq \varepsilon(m_1)$. Once we know that all m_1 are in $\mathbf{k}$, there is in fact only one; without loss of generality, we can then let $m_1 = 1$. So $\rho(m) = \sum m_0 \otimes m_1 = m \otimes 1$. Thus $M^{H^*} \subseteq M^{coH}$. We now consider the opposite inclusion. Let $m \in M^{coH}$. Then $\rho(m) = m \otimes 1$ which implies $f \cdot m = f(1)m = \varepsilon(f)m$, by Equation 1.22. for H^*. This implies that $m \in M^{H^*}$, so $M^{coH} \subseteq M^{H^*}$. $\square$

1.4.3 Smash Products

Definition 1.4.5. Let H be a Hopf algebra. We say that an algebra A is a *(left) H-module algebra* if for all $h \in H$ and $a, b \in A$

(1) A is a (left) H-module with structure map $h \otimes a \mapsto h \cdot a$

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

(3) $h \cdot 1_A = \varepsilon(h) 1_A$.

As might be expected, there is a corresponding definition for comodules.

Definition 1.4.6. Let H be a Hopf algebra, and consider an H-algebra A with multiplication and unit given by μ and η respectively. We say that A is a (right) *H-comodule algebra* if

(1) A is a right H-comodule, with structure map $\rho : A \longrightarrow A \otimes H$

(2) The maps μ and η are also right H-comodule maps.

In other words, we have $\rho(ab) = \sum a_0 b_0 \otimes a_1 b_1$ for all $a, b \in A$ and $\rho(1) = 1 \otimes 1$.

The notion of H-module algebras is used in the following important definition.

Definition 1.4.7. Let H be a Hopf algebra, and A a left H-module algebra. Then the *smash product algebra $A \# H$* is defined as the algebra satisfying the following conditions:

(1) $A \# H = A \otimes H$, as $\mathbf{k}$-vector spaces. For $a \in A$ and $h \in H$, the element $a \otimes h$ is written as $a \# h$.

(2) Multiplication is defined as

$$(a\#h)(b\#k) = \sum a(h_1{\cdot}b)\#h_2k,$$

for $a, b \in A$, and $h, k \in H$.

Example 1.4.5.

(1) Clearly, $A \cong A\#1$ and $H \cong 1\#H$, so the element $a\#h$ is often written ah.

(2) Trivially, for any H and any A, the action $h{\cdot}a = \varepsilon(h)a$, for all $h \in H$ and $a \in A$ gives $A\#H \cong A{\otimes}H$, as algebras.

(3) Let H be an arbitrary Hopf algebra, and A an H-module algebra. Consider $h \in \mathcal{P}(H)$, the set of primitive elements of H. By definition, $\Delta(h) = h{\otimes}1 + 1{\otimes}h$, so

$$h{\cdot}(ab) = (h{\cdot}a)b + a(h{\cdot}b).$$

Thus h acts as a $\mathbf{k}$-derivation of A. Now suppose $H = U(\mathfrak{g})$, and let A be an H-module algebra. This is clearly equivalent to the requirement that A is an H-module such that elements of $\mathfrak{g}$ act as derivations on A. So obviously, the action of $\mathfrak{g}$ must determine that of $U(\mathfrak{g})$. The resulting smash product $A\#H$ is sometimes referred to as the differential polynomial ring. For example, consider the one dimensional Lie algebra, $\mathfrak{g} = \mathbf{k}x$, where x acts as a derivative δ of A. In this case, $A\#U(\mathbf{k}x) = A[x;\delta]$, which is the Ore extension where $xa = ax + \delta(a)$.

We now consider some results concerning smash products (taken from [KT81, Lemma 1.3 and Lemma 1.6]). Let H be a Hopf algebra, and let $\mathbf{k}$ be a field. Recall from Lemma 1.4.1 that if a $\mathbf{k}$-algebra A is a right comodule over the $\mathbf{k}$-coalgebra H, then it is also a left module over the $\mathbf{k}$-algebra H^*. For the remainder of this section, we assume that the $\mathbf{k}$-algebra A is a right H-comodule via the $\mathbf{k}$-algebra homomorphism $\gamma : A \longrightarrow A{\otimes}H$. We also define the subalgebra B of A by

$$B = \{b \in A \mid \phi(b) = u^*(\phi)b \quad \forall\, \phi \in H^*\},$$

where $u^* : H^* \longrightarrow \mathbf{k}$ is the transpose of the unit map u of H, that is, the augmentation of H^*. Thus $B = A^{H^*}$, and by Lemma 1.4.3, $B = A^{coH}$.

Lemma 1.4.4. *Let H and H^* be Hopf algebras and consider the* $\mathbf{k}$*-module A. Further assume that A is a right H-comodule algebra. Then A is also a left H^*-module algebra.*

Proof. Since A is a right H-comodule, it is a left H^*-module. Now consider $\phi \in H^*$. Then for all $a, b \in A$,

$$\begin{aligned}
\phi(ab) &= \sum \phi((ab)_1)(ab)_0 \quad \text{by definition of the } H^*\text{-module action in Lemma 1.4.1} \\
&= \sum \phi(a_1 b_1)(a_0 b_0) \\
&= \sum \phi_1(a_1)\phi_2(b_1) a_0 b_0 \\
&= \sum \phi_1(a)\phi_2(b),
\end{aligned}$$

for all elements a, b in A, where the second line holds because $(a_1 b_1) \in H$ and $\phi \in H^*$. Now consider the identity element 1 of A. Then

$$\begin{aligned}
\phi(1) &= u^*(\phi(1)) \\
&= u^*(\phi)\cdot 1, \qquad (1.24)
\end{aligned}$$

where the first line holds because $\phi(1) = 1$ and $u^*(1) = 1$. □

Proposition 1.4.5. *With A and B as defined above, B is the largest subalgebra of A such that elements of H^* act as right B-module endomorphisms of A.*

Proof. We let $\phi \in H^*$ and $b \in B$. Then for all $a \in A$,

$$\begin{aligned}
\phi(ab) &= \sum \phi_1(a) \cdot \phi_2(b) \\
&= \sum \phi_1(a)\cdot u^*(\phi_2)\cdot b \quad \text{by the definition of } B \text{ and because } b \in B \\
&= \sum \phi_1(a) \cdot \phi_2(1)\cdot b \quad \text{by Equations 1.24 and 1.24} \\
&= \phi(a)\cdot b, \quad \forall\, a \in A, \quad \text{by Equation 1.24.}
\end{aligned}$$

On the other hand, suppose that $\phi \in H^*$ and $b \in A$ is such that $\phi(ab) = \phi(a)\cdot b$ for all $a \in A$. Then $\phi(b) = \phi(1b) = \phi(1)\cdot b = u^*(\phi)\cdot b$. Hence the result follows. □

The following result is taken from [KT81, Lemma 1.2].

Lemma 1.4.6. *Let A be a* **k***-algebra, and let H be an arbitrary* **k***-Hopf algebra. Suppose A is a right H-comodule algebra via a map $\gamma : A \longrightarrow A \otimes H$, say $\gamma(a) = \sum a \otimes h_a$, and let B be the subalgebra $B = A^{coH}$. Now consider the maps $\alpha : A \otimes_B A \longrightarrow A \otimes H$, given via $a \otimes a' \mapsto \gamma(a)(a' \otimes 1)$ and $\alpha' : A \otimes_B A \longrightarrow A \otimes H$, given via $a \otimes a' \mapsto (a \otimes 1)\gamma(a')$ respectively the right and left A-module homomorphisms induced by γ. Then α is injective, surjective or bijective if and only if α' is injective, surjective or bijective.*

Proof. Consider the map $\xi \in \mathrm{End}(A\otimes H)$, given by $\xi(a\otimes h) = \gamma(a)(1\otimes S(h))$, for h in H and a in A. Now $\xi\circ\alpha' = \alpha$. We prove this in the following calculation.

$$\begin{aligned}
\xi\circ\alpha'(a\otimes a') &= \xi((a\otimes 1)\gamma(a')) \\
&= \xi((a\otimes 1)\sum(a'\otimes h_{a'})) \\
&= \xi\sum(aa'\otimes h_{a'}) \\
&= \sum\xi(aa'\otimes h_{a'}) \\
&= \sum\gamma(aa')(1\otimes S(h_{a'})) \\
&= \sum\gamma(a)\gamma(a')((1\otimes S(h_{a'}))) \quad \text{since } \gamma \text{ is an algebra homomorphism} \\
&= \sum\gamma(a)(a'\otimes h_{a'})(1\otimes S(h_{a'})) \\
&= \sum\gamma(a)(a'\otimes h_{a'}S(h_{a'})) \\
&= \gamma(a)(a'\otimes 1) \quad \text{by properties of the antipode.}
\end{aligned}$$

Further, ξ has inverse $\xi^{-1}(a\otimes h) = (1\otimes S^{-1}(h))\gamma(a)$, and so we obtain the result. $\square$

1.4.4 Flatness

Finally in this chapter, we define discuss some technical algebraic tools, which will be used extensively in the remaining chapters.

Definition 1.4.8.

(1) Consider an algebra A and let B be a right A-module. Then we say that B is a *flat* right A-module if it preserves exact sequences; that is, if $0 \longrightarrow M \xrightarrow{\alpha} N$ is an exact sequence for any left A-modules M and N then $0 \longrightarrow B\otimes_A M \xrightarrow{1\otimes\alpha} B\otimes_A N$ is also an exact sequence.

In other words, B is flat if for all injective maps $\alpha : M \longrightarrow N$ then $1\otimes\alpha : B\otimes_A M \longrightarrow B\otimes_A N$ is also injective.

(2) Let B be a right flat A-module, and suppose that B preserves and reflects exact sequences; that is, $0 \longrightarrow B\otimes_A M \xrightarrow{\beta\otimes 1} B\otimes_A N$ is an exact sequence if and only if $0 \longrightarrow M \xrightarrow{\beta} N$ is one too. Then B is a left *faithfully flat* A-module.

As above, we may re-state this in terms of injectivity: if B is faithfully flat, then $\beta : M \longrightarrow N$ is injective if and only if $\beta\otimes 1 : B\otimes_A M \longrightarrow B\otimes_A N$ is injective.

Definition 1.4.9. Now consider two Hopf algebras, A and B, and a Hopf algebra homomorphism $f : A \longrightarrow B$. We say f is *right (faithfully) flat* if B is a right (faithfully) flat A-module with module structure given by $b\otimes a \mapsto bf(a)$.

Chapter 2

Extensions and Normality

2.1 Normal Hopf Algebras

2.1.1 Definitions and Examples

We begin by defining the notion of a normal sub-Hopf algebra and then dualise this to get the definition of a normal Hopf ideal.

Definition 2.1.1. Let A be a Hopf algebra.

(1) We define the *left adjoint action* of A on itself by

$$(\mathrm{ad}_\ell a)(b) \;=\; \sum a_1 b S(a_2), \quad \forall\, a, b \,\in\, A.$$

(2) The *right adjoint action* is defined similarly as

$$(\mathrm{ad}_r a)(b) \;=\; \sum S(a_1) b a_2, \quad \forall\, a, b \,\in\, A.$$

(3) If a sub-Hopf algebra $B \subseteq A$ satisfies

$$(\mathrm{ad}_\ell A)B \subseteq B \quad \text{and} \quad (\mathrm{ad}_r A)B \subseteq B$$

then B is said to be a *normal* sub-Hopf algebra of A.

The following technical result enables us to give some examples of normal sub-Hopf algebras.

Lemma 2.1.1. *Let $B \subseteq A$ be a sub-Hopf algebra. Suppose the set $X \subseteq A$ is a set of algebra generators for A. If $ad_\ell(x)B \subseteq B$ and $ad_r(x)B \subseteq B$ for all $x \in X$, then B is a normal sub-Hopf algebra of A.*

Proof. We consider the case for ad_ℓ; the proof for ad_r is similar. Let $x, y \in X$ and $b \in B$. Then

$$\begin{aligned} \mathrm{ad}_\ell(xy)(b) &= \sum (xy)_1 bS((xy)_2) \\ &= \sum x_1 y_1 b(S(x_2 y_2)) \\ &= \sum x_1 y_1 bS(y_2)S(y_1) \\ &= \mathrm{ad}_\ell(x)\mathrm{ad}_\ell(y)(b), \end{aligned}$$

and clearly this last line is contained in B. By induction, we get that $\mathrm{ad}_\ell(\underline{x})(b) \in B$, for all monomials $\underline{x}$ on the generators X. Finally, we note that

$$\mathrm{ad}_\ell(\lambda a)(b) = \lambda \mathrm{ad}_\ell(a)(b),$$

for all $\lambda \in \mathbf{k}$ and $a, b \in A$. The result then follows. □

Example 2.1.1.

(1) (a) Let $H = \mathbf{k}G$, where $\mathbf{k}$ is a field and G is a finitely generated group. Then for all $g \in G$ we have

$$(\mathrm{ad}_\ell\, g)h = \sum g_1 h S(g_2) = ghg^{-1}, \quad \forall\, h \in H.$$

(b) Let $H = U(\mathfrak{g})$, the enveloping algebra of the Lie algebra $\mathfrak{g}$. Then for all $g \in \mathfrak{g}$, we have

$$(\mathrm{ad}_\ell\, g)h = gh - hg, \quad \forall\, h \in H.$$

(2) (a) Let N be a normal subgroup of the group G. Then by Lemma 2.1.1, it is clear that $\mathbf{k}N$ is a normal sub-Hopf algebra of $\mathbf{k}G$.

(b) Let $H = U(\mathfrak{g})$, as above, and let $\mathfrak{i}$ be a Lie ideal of the Lie algebra $\mathfrak{g}$. Then, as above, by Lemma 2.1.1, $U(\mathfrak{i})$ is clearly a normal sub-Hopf algebra of $U(\mathfrak{g})$.

We now dualise Definition 2.1.1.

Definition 2.1.2. Let A be a Hopf algebra. Consider the two maps

$$\begin{aligned} \psi_\ell : A &\longrightarrow A \otimes A, \quad \text{via } a \mapsto \sum a_1 S(a_3) \otimes a_2, \quad \text{and} \\ \psi_r : A &\longrightarrow A \otimes A, \quad \text{via } a \mapsto \sum a_2 \otimes S(a_1) a_3. \end{aligned}$$

These maps are respectively the left and right coactions of A on itself and are the duals of the respective adjoint actions. We see this by considering $\mathrm{ad}_\ell : A \otimes A \longrightarrow A$ as a left action, via $a \otimes a' \mapsto \sum a_1 a' S(a_2)$, for all $a, a' \in A$. This can be written as

$$\mathrm{ad}_\ell = \mu^2 \circ (id^2 \otimes S) \circ (id \otimes \tau) \circ (\Delta \otimes id),$$

where τ is the flip map, and $\mu^2 : A \otimes A \otimes A \longrightarrow A$ is given by $a \otimes b \otimes c \mapsto abc$, for all $a, b, c \in A$. But we can write ψ_ℓ in the following form:

$$\psi_\ell = (\mu \otimes id) \circ (id \otimes \tau) \circ (id^2 \otimes S) \circ \Delta^2.$$

where $\Delta^2(a) = (1 \otimes \Delta) \circ \Delta(a)$.

So ad_ℓ and ψ_ℓ are indeed formal duals. A similar argument gives the same result for ad_r and ψ_r.

Now consider a Hopf algebra homomorphism $h : A \longrightarrow B$. We say this is *conormal* if for all $x \in \ker(h)$ $(= h^{-1}(0))$

$$\psi_\ell(x) = \sum x_1 S(x_3) \otimes x_2 \in A \otimes \ker(h) \tag{2.1}$$

$$\psi_r(x) = \sum x_2 \otimes S(x_1) x_3 \in \ker(h) \otimes A. \tag{2.2}$$

A Hopf ideal $I \subseteq A$ is *normal* if the canonical map $\pi : A \longrightarrow A/I$ is conormal. In this case, $\pi^{-1}(0) = I$.

Recall that a Hopf ideal I is a biideal (that is, an ideal and a coideal) which also satisfies $SI \subset I$. Before we go on to discuss some examples of Hopf ideals, we consider the following useful result.

Lemma 2.1.2. *Let I be a Hopf ideal of the Hopf algebra H, and let $\pi : H \longrightarrow H/I$ be the canonical map. Therefore, in this case $\ker(\pi) = I$. Suppose further that $I = \sum_i x_i H$, some $x_i \in I$. Let $X \subseteq I$ be the set of all such x_i. Then we have the following two results:*

(1) If $\psi_r(x_i) \in I \otimes H$, for all x_i, then $\psi_r(I) \subseteq I \otimes H$. Similarly, if $\psi_\ell(x_i) \in H \otimes I$, for all x_i, then $\psi_\ell(I) \subseteq H \otimes I$.

(2) If $\Delta(x_i) \in I \otimes H + H \otimes I$, for all i, then $\Delta(I) \subseteq I \otimes H + H \otimes I$.

Proof.

(1) Without loss of generality, we may take an element j of I to be xh, for some $x \in X$ and $h \in H$. We want to show that

$$\psi_r(xh) = \sum (xh)_2 \otimes S(xh)_1 (xh_3) = \sum x_2 h_2 \otimes S(h_1) S(x_1) x_3 h_3 \in \ker(\pi) \otimes H,$$

where the second equality holds by the fact that S is an anti-algebra morphism and by Equation 1.21. We know that

$$\psi_r(x) = \sum x_2 \otimes S(x_1) x_3 \in \ker(\pi) \otimes H,$$

so $x_2 \in \ker(\pi)$. But $\ker(\pi)$ is an ideal, so we must also have $x_2 h_2 \in \ker(\pi)$ for all h_2. Thus $\psi_r(xh) \in \ker(\pi) \otimes H$. The proof for ψ_ℓ is similar.

(2) We prove this in much the same manner as above. As before, we may take an element j of I to be xh. Then $\Delta(xh) = \sum x_1 h_1 \otimes x_2 h_2$. But we know that $\sum x_1 \otimes x_2 \in I \otimes H + H \otimes I$. So either $x_1 \in I$ or $x_2 \in I$. Therefore, since I is an ideal, either $x_1 h_1 \in I$ or $x_2 h_2 \in I$, and so $\Delta(I) \subseteq I \otimes H + H \otimes I$.

□

Example 2.1.2. Let $H = U(\mathfrak{g})$, the enveloping algebra of a Lie algebra $\mathfrak{g}$. Suppose $\mathfrak{i}$ is a Lie ideal of $\mathfrak{g}$. We prove that $\mathfrak{i}U(\mathfrak{g}) = \{\sum_j \alpha_j u_j \mid \alpha_j \in \mathfrak{i},\ u_j \in U(\mathfrak{g})\}$ is a Hopf ideal of $U(\mathfrak{g})$. Clearly, $\mathfrak{i}U(\mathfrak{g})U(\mathfrak{g}) \subseteq \mathfrak{i}U(\mathfrak{g})$. Now let $\sum_j \alpha_j u_j \in \mathfrak{i}$. By the Poincaré-Birkhoff-Witt Theorem, $U(\mathfrak{g})$ has $\mathbf{k}$-basis X given by the ordered monomials on a basis of $\mathfrak{g}$. We wish to show that $U(\mathfrak{g})\mathfrak{i}U(\mathfrak{g}) \subseteq \mathfrak{i}U(\mathfrak{g})$. Let $\beta = \sum_{j=1}^m \beta_j u_j \in \mathfrak{i}U(\mathfrak{g})$, where $\beta_i \in \mathfrak{i}$ and $u_j \in U(\mathfrak{g})$. We note that $U(\mathfrak{g})$ is generated as a $\mathbf{k}$-algebra by the elements of $\mathfrak{g}$. Thus, to show that $u\beta \in \mathfrak{i}U(\mathfrak{g})$ for all $u \in U(\mathfrak{g})$, it is sufficient to use it for $u = x$, for all $x \in \mathfrak{g}$.

We have

$$x\beta = \sum_j x\beta_j u_j,$$

and for all j,

$$x\beta_j = \beta_j x + [x, \beta_j] \in \mathfrak{i}U(\mathfrak{g}),$$

because $\beta_j x \in \mathfrak{i}U(\mathfrak{g})$ and $[x, \beta_j] \in \mathfrak{i}$, since $\mathfrak{i}$ is an ideal of $\mathfrak{g}$. Hence $\mathfrak{i}U(\mathfrak{g})$ is an ideal.

To show that this is a coideal, we need to show that the two coideal axioms are satisfied, that is, $\varepsilon(\mathfrak{i}U(\mathfrak{g})) = 0$ and $\Delta(\mathfrak{i}U(\mathfrak{g})) \subset \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g}) + U(\mathfrak{g})\otimes\mathfrak{i}U(\mathfrak{g})$. Recall that $\varepsilon(g) = 0$ for all $g \in \mathfrak{g}$, so clearly $\varepsilon(\mathfrak{i}U(\mathfrak{g})) = 0$. By Lemma 2.1.2(2) above, it is sufficient to show that $\Delta(x) \in \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g}) + U(\mathfrak{g})\mathfrak{i}\otimes U(\mathfrak{g})$, for all $x \in \mathfrak{i}$. Now $\Delta(x) = x\otimes 1 + 1\otimes x$; clearly $\Delta(x) \in \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g}) + U(\mathfrak{g})\otimes\mathfrak{i}U(\mathfrak{g})$. Thus, by the lemma, $\Delta(\mathfrak{i}U(\mathfrak{g})) \subseteq \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g}) + U(\mathfrak{g})\mathfrak{i}\otimes U(\mathfrak{g})$.

Finally, we need to show that $\mathfrak{i}U(\mathfrak{g})$ satisfies the antipode condition. Consider $S(\sum\alpha_j u_j)$, where $\alpha_j \in \mathfrak{i}$ and $u_j \in U(\mathfrak{g})$ as above. Then

$$\begin{aligned} S(\textstyle\sum\alpha_j u_j) &= \textstyle\sum S(\alpha_j u_j) \\ &= \textstyle\sum S(u_j)S(\alpha_j) \quad \text{by properties of the antipode} \\ &= -\textstyle\sum S(u_j)\alpha_j \end{aligned}$$

But $S(u_j) \in U(\mathfrak{g})$, so $S(\sum\alpha_j u_j) \in U(\mathfrak{g})\mathfrak{i}$. But $U(\mathfrak{g})\mathfrak{i} = \mathfrak{i}U(\mathfrak{g})$, so $S(\mathfrak{i}U(\mathfrak{g})) = U(\mathfrak{g})\mathfrak{i} = \mathfrak{i}U(\mathfrak{g})$ as required.

Note 2.1.1. In fact, $U(\mathfrak{g})/\mathfrak{i}U(\mathfrak{g})$ is isomorphic to $U(\mathfrak{g}/\mathfrak{i})$. To prove this, we first consider the map $\phi : U(\mathfrak{g}) \longrightarrow U(\mathfrak{g}/\mathfrak{i})$, induced by the map $g \mapsto g + \mathfrak{i}$ for all $g \in \mathfrak{g}$. Clearly, $\mathfrak{i} \subseteq \ker(\phi)$, so $\mathfrak{i}U(\mathfrak{g}) \subseteq \ker(\phi)$. Our aim is to show that this is in fact an equality.

Let $\{x_1, \cdots, x_n\}$ be a basis for $\mathfrak{g}$, where we may suppose that a subset of this basis, say $\{x_1, \cdots, x_m\}$ is a basis for $\mathfrak{i}$. Thus, $\{x_{m+1} + \mathfrak{i}, \cdots, x_n + \mathfrak{i}\}$ is a basis for $\mathfrak{g}/\mathfrak{i}$. For $\underline{t} = t_1 t_2 \cdots t_n \in \mathbb{N}^n$ and $\underline{x} = (x_1 x_2 \cdots x_n) \in \mathfrak{g}^n$, write $\underline{x}^{\underline{t}} \in U(\mathfrak{g})$. Consider $u = \sum_{\underline{t}} \lambda_{\underline{t}} \underline{x}^{\underline{t}} \in \ker(\phi)$. Then

$$\phi(u) = \sum_{\underline{t}} \lambda_{\underline{t}} \overline{x}_{m+1}^{t_{m+1}} \cdots \overline{x}_n^{t_n} = 0,$$

where the sum is over all $\underline{t}$ with $t_1 = t_2 = \cdots = t_m = 0$ and $\overline{x}_j = x_j + \mathfrak{i}$. But the monomials $\{\overline{x}_{m+1}^{t_{m+1}}, \cdots, \overline{x}_n^{t_n}\}$ are all distinct and hence are linearly independent in $U(\mathfrak{g}/\mathfrak{i})$ by the Poincaré-Birkhoff-Witt Theorem for $U(\mathfrak{g}/\mathfrak{i})$. Therefore $\lambda_{\underline{t}} = 0$ for all $\underline{t}$ with $t_1 = t_2 = \cdots = t_m = 0$; therefore, $u \in \mathfrak{i}U(\mathfrak{g})$, so $\mathfrak{i}U(\mathfrak{g}) = \ker\phi$.

It is clear that $\phi : U(\mathfrak{g}) \longrightarrow U(\mathfrak{g}/\mathfrak{i})$ is onto, so we may apply the first Homomorphism theorem to get that $U(\mathfrak{g})/\mathfrak{i}U(\mathfrak{g}) \cong U(\mathfrak{g}/\mathfrak{i})$.

Finally, we consider an example of a normal Hopf ideal.

Example 2.1.3. As in Example 2.1.2, let $H = U(\mathfrak{g})$, and $\mathfrak{i}$ be a Lie ideal of the Lie algebra $\mathfrak{g}$. We claim that $\mathfrak{i}U(\mathfrak{g})$ is a normal Hopf ideal. By Lemma 2.1.2(1), it is enough to prove that $\psi_r(x) \in \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g})$ and $\psi_\ell(x) \in \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g})$ for $x \in \mathfrak{i}$. Consider the map $\pi : U(\mathfrak{g}) \longrightarrow U(\mathfrak{g})/\mathfrak{i}U(\mathfrak{g})$, induced by the map $g \mapsto g + \mathfrak{i}$, for all $g \in \mathfrak{g}$. Now consider $\psi_r(x)$ for some $x \in \mathfrak{i}$. Then

$$(1\otimes\Delta)\circ\Delta(x) = (1\otimes\Delta)(x\otimes 1 + 1\otimes x) = x\otimes 1\otimes 1 + 1\otimes x\otimes 1 + 1\otimes 1\otimes x. \tag{2.3}$$

Thus we have

$$\psi_r(x) = \sum x_2\otimes S(x_1)x_3 = 1\otimes(-x)1 + (x\otimes 1)1 + 1\otimes 1(x) = x\otimes 1.$$

But $x\otimes 1 \in \mathfrak{i}U(\mathfrak{g})\otimes U(\mathfrak{g})$ since $x \in \mathfrak{i}$. We use a similar argument for ψ_ℓ. As before, let $x \in \mathfrak{i}$. Applying Equation 2.3 above, we get

$$\psi_\ell(x) = \sum x_1 S(x_3)\otimes x_2 = (x)1\otimes 1 + 1(1)\otimes x + 1(-x)\otimes(1) = 1\otimes x.$$

But $x \in \mathfrak{i}$, so $1\otimes x \in U(\mathfrak{g})\otimes\mathfrak{i}U(\mathfrak{g})$.

Thus $\mathfrak{i}U(\mathfrak{g})$ is a normal Hopf ideal of $U(\mathfrak{g})$.

2.1.2 Results on Normality

In the group theoretic context, one may define the concept of normal in several different ways. Amongst other things, this section deals with some of the corresponding Hopf algebraic results. The following results are taken from [Mon93, Lemma 3.4.2 and Proposition 3.4.3].

Lemma 2.1.3.

(1) Let H be a Hopf algebra over a field $\mathbf{k}$ *and $K \subseteq H$ be a sub-Hopf algebra of H. Define the* augmentation ideal $K^+ = K \cap \ker(\varepsilon)$, *where $\varepsilon : H \longrightarrow \mathbf{k}$ is the augmentation map. Then if K is also normal, $HK^+ = K^+H$ is a normal Hopf ideal of H, and the canonical map $\pi : H \longrightarrow H/HK^+$ is a Hopf algebra morphism.*

(2) Let $\vartheta : H \longrightarrow J$ be a Hopf algebra morphism, and as discussed in Definition 1.4.4, consider H as a right and left J-comodule, where ρ and ϕ represent the respective comodule maps. Then H_ρ^{coJ} is stable under ad_ℓ and H_ϕ^{coJ} is stable under ad_r — that is, $(ad_\ell H)H_\rho^{coJ} \subset H_\rho^{coJ}$ and $(ad_r H)H_\phi^{coJ} \subset H_\phi^{coJ}$.

Proof.

(1) This proof is from [Mon93, Lemma 3.4.2] with the exception of the proof showing that HK^+ is normal, which is taken from [Sch93, Lemma 1.3]. We want to show that $HK^+ = K^+H$ and that $I = HK^+ = K^+H$ is a normal Hopf ideal. First, note the following identity. Let $h \in H$ and $k \in K$. Then

$$hk = \sum h_1 k\varepsilon(h_2) = \sum h_1 kS(h_2)h_3 = \sum(\mathrm{ad}_\ell h_1)(k)h_2 \quad \text{by Equation 1.19.}$$

Now since K is normal and $k \in K$, we have $(\mathrm{ad}_\ell h_1)(k) \in K$. If in addition $k \in K^+$, then $\varepsilon((\mathrm{ad}_\ell h_1)(k)) = 0$, so in this case, $hk \in K^+H$. Thus $HK^+ \subseteq K^+H$. By using ad_r, we can get the other containment. Clearly I is then an ideal. To show that I is a coideal, we need to show that $\Delta(I) \subseteq I\otimes H + H\otimes I$. By Lemma 2.1.2(2), we need only show that $\Delta(k^+) \in I\otimes H + H\otimes I$ for all $k^+ \in K^+$. But

$$\Delta(k^+) = \sum k_1^+ \otimes k_2^+.$$

Now K^+ is a Hopf ideal, so by definition $\Delta(k^+) \in K^+\otimes K + K\otimes K^+$. Therefore, either k_1^+ or k_2^+ is in K^+, and hence we must have $\Delta(k^+) \in I\otimes H + H\otimes I$. Thus $\Delta(I) \subseteq I\otimes H + H\otimes I$. By definition, $\varepsilon(I) = 0$, so it only remains to prove that $SI \subseteq I$. Consider an element $\sum_{i=1}^n h_i k_i^+$ in I. However, it is enough to consider a single summand at a time from this expression, so we define $i = hk^+$, for some $h \in H$ and $k^+ \in K^+$. Then $S(hk^+) = S(k^+)S(h)$. But K^+ is a sub-Hopf algebra, so $S(k^+) \in K^+$. Therefore, $S(hk^+) \in K^+H = HK^+$. So $S(I) \subseteq I$.

We now show that I is a normal Hopf ideal. By Lemma 2.1.2(1) it is enough to show that for all $k^+ \in K^+$, Equation 2.1 in Definition 2.1.2 holds. Let $\pi : H \longrightarrow H/I$ be the canonical map. As above, we must have either k_1^+ or k_2^+ contained in K^+. If $k_2^+ \in K^+$, then clearly $\psi_\ell(k^+) = \sum k_1^+ S(k_2^+)\otimes k_2^+ \in H\otimes \ker(\pi)$. We consider the case when $k_1^+ \in K^+$ and k_2^+ is not contained in K^+. We first note the following fact:
if $k^+ \in K^+$, then clearly $k^+ - \varepsilon(k^+) \in HK^+ = \ker(\pi)$; that is, $\mathrm{mod}(H)\otimes \ker(\pi)$, $-\otimes k^+ \equiv -\otimes\varepsilon(k^+)$. Recall also that $\varepsilon(k^+) \in \mathbf{k}$ for all $k^+ \in K^+$, and so may be moved freely across the tensor sign.

Now mod $H \otimes \ker(\pi)$,

$$\begin{aligned}
\sum k_1^+ S(k_3^+) \otimes k_2^+ &\cong \sum k_1^+ S(k_3^+) \otimes \varepsilon(k_2^+) \\
&= \sum k_1^+ \varepsilon(k_2^+) S(k_3^+) \otimes 1 \\
&= \sum k_1^+ S(k_2^+) \otimes 1 \\
&= \sum \varepsilon(k_1^+) \otimes 1 \\
&\cong 0,
\end{aligned}$$

where the final line holds because we assume $k_1^+ \in K^+$.

We follow a similar argument to show that Equation 2.2 from Definition 2.1.2 holds. As before, since $HK^+ = K^+H$, we need only consider $k^+ \in K^+$. In this case, if $k_2^+ \in K^+$, then clearly $\psi_r(k^+) = \sum k_2^+ \otimes S(k_1^+) k_3^+ \in \ker(\pi) \otimes H$. We consider the case when only $k_1^+ \in K^+$. Again, $\bmod \ker(\pi) \otimes H$,

$$\begin{aligned}
\sum k_2^+ \otimes S(k_1^+) k_3^+ &\cong \sum \varepsilon(k_2^+) \otimes S(k_1^+) k_3^+ \\
&= \sum 1 \otimes S(k_1^+) \varepsilon(k_2^+) k_3^+ \\
&= \sum 1 \otimes S(k_1^+) k_2^+ \\
&= \sum 1 \otimes \varepsilon(k_2^+) \\
&\cong 0,
\end{aligned}$$

where the last line holds for the same reason as above. Hence both Equations 2.1 and 2.2 hold, so HK^+ is a normal Hopf ideal.

(2) This proof comes from [Mon93, Lemma 3.4.2]. Choose $j \in H_\rho^{coK}$, so by definition, $\rho(j) = \sum j_1 \otimes \overline{j}_2 = j \otimes \overline{1}$, where $\overline{j} = \vartheta(j)$. Now let $h \in H$. Then

$$\begin{aligned}
\rho((\mathrm{ad}_\ell h) j) &= \rho(\sum h_1 j S(h_2)) \\
&= \sum (h_1)_1 j_1 (S(h_2))_1 \otimes (\overline{h}_1)_2 \overline{j}_2 (S(\overline{h}_2))_2 \\
&= \sum (h_1)_1 j_1 (S(h_2))_1 \otimes (\overline{h}_1)_2 \overline{j}_2 (S(\overline{h_2})_2) \\
&= \sum h_1 j S(h_4) \otimes \overline{h}_2 S(\overline{h}_3) \\
&= \sum h_1 \varepsilon(h_2) j S(h_3) \otimes \overline{1} \\
&= (\mathrm{ad}_\ell h)(j) \otimes \overline{1},
\end{aligned}$$

where the equality on the fifth line holds because $\sum h_2 S(h_3) = \varepsilon(h_2)$, and also because of Equation 1.19. Also note that $\varepsilon(h_2) \in \mathbf{k}$, and so, as before, may be freely commuted past elements in the tensor product.

Therefore, $(\mathrm{ad}_\ell K)H_\rho^{coK} \subseteq H_\rho^{coK}$. One uses a similar argument to get the inclusion for H_ϕ^{coK}.

□

Example 2.1.4. Let $H = \mathbf{k}G$, and $K = \mathbf{k}N$, where N is a normal subgroup of G. Consider the augmentation map $\varepsilon : \mathbf{k}G \longrightarrow \mathbf{k}$ given by $g \mapsto 1$, for all $g \in G$. Therefore,
$\mathbf{g} = \ker(\varepsilon) = \sum_{1 \neq g \in G} \mathbf{k}G(g-1)$. So $K^+ = \mathbf{n} = \sum_{1 \neq n \in N} \mathbf{k}N(n-1)$, which is an ideal of $\mathbf{k}N$. Thus $HK^+ = K^+H = \sum_{1 \neq n \in N} KG(n-1)$. We want to check that this is a normal Hopf ideal, as predicted by the first part of Lemma 2.1.3. Firstly, we note that we have $\varepsilon(HK^+) = 0$ by definition. To prove the remaining two conditions it is sufficient (by Lemma 2.1.2(2)) to consider an element $n-1$, for $1 \neq n \in N$. Now by definition of Δ for $\mathbf{k}G$,

$$\begin{aligned}
\Delta(n-1) &= \Delta(n) - \Delta(1)\\
&= n \otimes n - 1 \otimes 1\\
&= (n-1)\otimes n + (1 \otimes n) - 1 \otimes 1\\
&= (n-1)\otimes n + 1 \otimes (n-1) \in \mathbf{nk}G \otimes \mathbf{k}G + \mathbf{k}G \otimes \mathbf{nk}G
\end{aligned}$$

by definition of $\mathbf{nk}G$. Finally, we need to show that $S(\mathbf{nk}G) \subseteq \mathbf{nk}G$. But this is clear, since for all $1 \neq n \in N$, we have $S(n-1) = S(n) - S(1) = n^{-1} - 1$, which is clearly contained in $\mathbf{n}$. Thus $S(\mathbf{nk}G) \subseteq \mathbf{nk}G$.

It remains to show that $\mathbf{nk}G$ is normal. By Lemma 2.1.2(1), it is sufficient to show that Equations 2.1 and 2.2 in Definition 2.1.2 hold for $n-1$ with $n \in N$ only, since
$\mathbf{nk}G = \sum_{1 \neq n \in N}(n-1)\mathbf{k}G$. To do this, we first define the canonical map $\pi : \mathbf{k}G \longrightarrow \mathbf{k}G/\mathbf{nk}G$. We note that$\Delta(x) = x \otimes x$ for any $x \in G$. So, since Δ is linear,

$$(1 \otimes \Delta) \circ \Delta(n-1) = (n \otimes n \otimes n) - (1 \otimes 1 \otimes 1)$$

Thus

$$\psi_\ell(n-1) = \sum n_1 S(n_3) \otimes n_2 = (nn^{-1} \otimes n) - (1.1 \otimes 1) = 1 \otimes n - 1 \otimes 1 = 1 \otimes (n-1) \in \mathbf{k}G \otimes \mathbf{nk}G.$$

We follow the same argument for ψ_r:

$$\psi_r(n-1) = \sum n_2 \otimes S(n_1) n_3 = (n \otimes n^{-1} n) - (1 \otimes 1.1) = n \otimes 1 - 1 \otimes 1 = (n-1) \otimes 1 \in \mathbf{nk}G \otimes \mathbf{k}G.$$

Thus $\mathbf{nk}G$ is a normal Hopf ideal of $\mathbf{k}G$.

Example 2.1.5. Let $H = U(\mathfrak{g})$ and $K = U(\mathfrak{i})$. Then $\mathbf{n} = U(\mathfrak{i})^+ = U(\mathfrak{i}) \cap \ker(\varepsilon)$, where we take $\varepsilon : U(\mathfrak{g}) \longrightarrow \mathbf{k}$. But $g \mapsto 0$ for all $g \in \mathfrak{g}$, so $\mathbf{n} = U(\mathfrak{i}) \cap U(\mathfrak{g})^+ = U(\mathfrak{i})^+$. So $U(\mathfrak{g})\mathbf{n} = \mathbf{n}U(\mathfrak{g}) = U(\mathfrak{i})U(\mathfrak{g}) = \mathfrak{i}U(\mathfrak{g})$. We already know that this is a normal Hopf ideal by Example 2.1.3.

The converse to the first part of Lemma 2.1.3 is not true in general, but if one imposes the additional requirement that H be faithfully flat over K, then the converse does hold. In order to prove this, we need the following definition.

Definition 2.1.3. Consider two maps $g : M \longrightarrow N$ and $h : M \longrightarrow N$ of right A-modules. The *equalizer* of g and h is defined as $\ker(g, h) = \{m \in M \mid g(m) = h(m)\}$. We say the equalizer diagram $L \xrightarrow{i} M \underset{h}{\overset{g}{\rightrightarrows}} N$ is *exact* if $\mathrm{Im}(i) = \ker(g, h)$ and i is injective.

Remark 2.1.1. This is equivalent to requiring the sequence $0 \longrightarrow L \xrightarrow{i} M \xrightarrow{g-h} N$ to be exact, that is, we require $g - h$ to be injective and $\mathrm{Im}(i) = \ker(g - h) = \{m \in M \mid (g - h)(m) = 0\}$.

We also note the following result from [Wat79, Theorem 13.1].

Lemma 2.1.4. *Let S be a subring of the ring R. If R is left faithfully flat over S, then the map $M \longrightarrow M \otimes_S R$, given by $m \mapsto m \otimes 1$ is injective for all R-modules M.*

Proof. Consider a right S-module N and an S-module homomorphism $\vartheta : M \longrightarrow N$. Since we have assumed R to be left faithfully flat over S, if the S-module map $\vartheta \otimes 1 : M \otimes_S R \longrightarrow N \otimes_S R$ is injective, then $\vartheta : M \longrightarrow N$ must also be injective. Thus, it is sufficient to prove that $M \otimes R \longrightarrow (M \otimes R) \otimes R$, given by $m \otimes r \mapsto (m \otimes 1) \otimes r$ is injective. This is clearly true, since the composition of the S-module map $M \otimes_S S \otimes_S R \longrightarrow M \otimes_S R$, given by $m \otimes a \otimes b \mapsto m \otimes ab$ with the map $M \otimes_S R \longrightarrow M \otimes_S S \otimes_S R$, given by $m \otimes r \mapsto (m \otimes 1) \otimes r$, is the identity on $M \otimes_S S \otimes_S R$. □

We now prove the converse to Lemma 2.1.3(1), following the argument in [Mon93, Lemma 3.4.3], which in turn is based on that in [Sch92, 1.2 and 1.3].

Lemma 2.1.5. *Let B be a sub-Hopf algebra of the Hopf algebra A with A right or left faithfully flat over B. Suppose that $AB^+ = B^+A$, and define $\overline{A} = A/AB^+$. As discussed previously, A has an $\overline{A}$-comodule structure. We let $\pi : A \longrightarrow \overline{A}$ be the canonical map. Then,*

(1) $B = A_\rho^{co\overline{A}} = A_\phi^{co\overline{A}}$, where $A_\rho^{co\overline{A}}$ and $A_\psi^{co\overline{A}}$ are the subalgebras given in Definition 1.4.4.

(2) B is a normal sub-Hopf algebra of A.

Proof. We use the fact that A is faithfully flat over B and the definition of $\overline{A}$-coinvariants to show that two different equalizer diagrams are exact. We then compare these diagrams and use them to construct a commutative diagram, which gives $B = A_\rho^{co\overline{A}} = A_\phi^{co\overline{A}}$.

First consider the diagram $B \subset A \overset{g}{\underset{h}{\rightrightarrows}} A \otimes_B A$, where $g(a) = a \otimes 1$ and $h(a) = 1 \otimes a$. We show that these maps are right B-module homomorphisms. Let $b \in B$. Then clearly,
$h(ab) = (1 \otimes ab) = (1 \otimes a)b$. Now consider $g(ab) = ab \otimes 1$. Since the tensor product is over B, we may move any $b \in B$ across the tensor sign; therefore, $g(ab) = a \otimes b = (a \otimes 1)b$. So g and h are right B-module homomorphisms.

We need to show that for $i : B \longrightarrow A$, where i is the inclusion map, we have $\mathrm{Im}(i) = \ker(g-h)$. Now $\ker(g-h) = \{m \in M \mid g(m) = h(m)\}$. Let $b \in B$. Since both g and h are right B-module homomorphisms, we then have

$$\begin{aligned} g(b) &= g(1)b = (1 \otimes 1)b \quad \text{and} \\ h(b) &= h(1)b = (1 \otimes 1)b \end{aligned}$$

Thus, for all $b \in B$, we have $g(b) = h(b)$, therefore $B \subseteq \ker(g-h)$.

We show the opposite inclusion by contradiction. Let $K = \ker(g-h)$ which is a right B-submodule of A, since $(g-h)$ is a right B-module homomorphism. Suppose that $K \neq B$. Therefore, $K/B \neq 0$. Now

$$0 \longrightarrow B \longrightarrow K \longrightarrow K/B \longrightarrow 0$$

is exact by the fact that K is a submodule. Since A is faithfully flat, this implies that

$$0 \longrightarrow B \otimes_B A \longrightarrow K \otimes_B A \longrightarrow (K/B) \otimes_B A \longrightarrow 0 \tag{2.4}$$

is exact, so $(K/B) \otimes_B A \neq 0$. Now let $\sum_i k_i \otimes_B a_i \in K \otimes_B A$. This implies that

$$\begin{aligned} \sum k_i \otimes_B a_i &= \sum (k_i \otimes 1) a_i \\ &= \sum (1 \otimes k_i) a_i \quad \text{since } K = \ker(g-h) \\ &= \sum 1 \otimes k_i a_i, \end{aligned}$$

which clearly is contained in $B \otimes_B A$. Thus, we must have $K \otimes_B A = B \otimes_B A$, which contradicts the exactness of Equation 2.4. Therefore $B = K$.

Next we consider the diagram $A_\rho^{co\overline{A}} \subset H \rightrightarrows A\otimes\overline{A}$ with the two maps on the right given by $a \mapsto a\otimes\overline{1}$ and $\sum a_1\otimes\overline{a}_2$. We have $AB^+ = B^+A$, which gives that $\overline{A}$ is a Hopf algebra. Thus, the canonical map $A \longrightarrow \overline{A}$ is a morphism of Hopf algebras, so, by definition of $\overline{A}$-coinvariants, the diagram is exact.

Our next step is to combine the two diagrams. First we consider the map $\beta : A\otimes_B A \longrightarrow A\otimes\overline{A}$, given by $a\otimes b \mapsto \sum ab_1\otimes\overline{b}_2$ (this is the *Galois* map defined in the next section). Consider the map $\alpha : A\otimes\overline{A} \longrightarrow A\otimes_B A$, given via $a\otimes\overline{b} \mapsto \sum aS(b_1)\otimes b_2$. We claim that $\alpha\circ\beta = \beta\circ\alpha = id$. We prove this as follows:

$$\begin{aligned}
(\beta\circ\alpha)(a\otimes\overline{b}) &= \beta(\sum a(b_1)\otimes b_2)\\
&= \sum(aS(b_1))(b_2)_1\otimes(\overline{b}_2)_2\\
&= \sum aS(b_1)b_2\otimes\overline{b}_3\\
&= \sum a\varepsilon(b_2)\otimes\overline{b}_3\\
&= \sum a\otimes\varepsilon(b_1)\overline{b}_2\\
&= a\otimes\sum\varepsilon(b_1)\overline{b}_2\\
&= a\otimes\overline{b},
\end{aligned}$$

where the second last line holds by the counitality condition on ε. For $\alpha\circ\beta$, we have a similar argument:

$$\begin{aligned}
(\alpha\circ\beta)(a\otimes b) &= \alpha(\sum ab_1\otimes\overline{b}_2)\\
&= \sum ab_1S(b_2)_1\otimes(b_2)_2\\
&= \sum ab_1S(b_2)\otimes b_3\\
&= \sum a\varepsilon(b_2)\otimes b_3\\
&= \sum a\otimes\varepsilon(b_1)b_2\\
&= a\otimes b,
\end{aligned}$$

where the last line holds for the same reason as above. So β is bijective.

We now need to check that $B \subseteq A_\rho^{co\overline{A}}$. Then for $b \in B$,

$$\begin{aligned}
\rho(b) &= (id\otimes\pi)\circ\Delta(b) \\
&= (id\otimes\pi)(\sum b_1\otimes b_2) \\
&= \sum b_1\otimes\pi(b_2) \\
&= \sum b_1\otimes\varepsilon(b_2) \\
&= \sum b_1\varepsilon(b_2)\otimes 1 \\
&= b\otimes 1,
\end{aligned}$$

where the fifth line holds because $\varepsilon(b_2) \in \mathrm{k}$. To show that the fourth line holds, we note that the restriction of π to B, that is, $\pi : B \longrightarrow \overline{B}$, is the same as the augmentation map $\varepsilon : B \longrightarrow \mathrm{k}$. Then since B is a sub-Hopf algebra, we have $\Delta(B) \subseteq B\otimes B$, so we get $\pi(b_2) = \varepsilon(b_2)$ as required.

We thus obtain the following commutative diagram:

$$\begin{tikzcd}
B \arrow[r] \arrow[d, "j"] & A \arrow[r, "\rightrightarrows"] \arrow[d, "="] & A\otimes_B A \arrow[d, "\beta"] \\
A_\rho^{co\overline{A}} \arrow[r] & A \arrow[r, "\rightrightarrows"] & A\otimes\overline{A}
\end{tikzcd}$$

where j is the inclusion map. Since the two equalizer diagrams are exact, and also since β is bijective, by the commutativity of the diagram we must have that j is bijective, and hence that $B = A_\rho^{co\overline{A}}$. By repeating the argument with $\overline{A}\otimes A$, we show that $B = A_\phi^{co\overline{A}}$. But then, by Lemma 2.1.3(2), $(\mathrm{ad}_\ell A)B$ and $(\mathrm{ad}_r A)B$ are contained in B; thus B is normal. $\square$

2.2 Galois and Frobenius Extensions

We now deal with the notion of *Galois* and *Frobenius* extensions.

Definition 2.2.1. Choose an arbitrary Hopf algebra J, and let A be a right J-comodule algebra with structure map given by $\rho : A \longrightarrow A\otimes J$. Let $B = A_\rho^{coJ}$. Then A is said to be a *J-extension* over B.

Definition 2.2.2. Let $B \subseteq A$ be a J-extension, where J an arbitrary Hopf algebra. Suppose further that the map $\beta : A\otimes_B A \longrightarrow A\otimes_{\mathrm{k}} J$, defined as $a\otimes a' \mapsto (a\otimes 1)\rho(a')$ is bijective for all $a, a' \in A$. Then A is said to be a *right J-Galois extension* of B.

Note 2.2.1. At first glance, the definition above seems one-sided; why was a *left* Galois extension not also defined? In fact, this can be done, via the map $\beta'(a\otimes a') = \rho(a)(a'\otimes 1)$. However, if the antipode S is bijective, then the two definitions are equivalent in the following way: β is injective, surjective or bijective if and only if β' is injective, surjective or bijective. This was proved in Lemma 1.4.6.

Before discussing any examples, we note the following well-known lemma by Dedekind:

Lemma 2.2.1. (Dedekind's Lemma) *Let E be a field, and let $S = \{\sigma_1 \cdots, \sigma_n\}$ be a finite set of automorphisms of E. Let $\phi : S \longrightarrow E$ be a function such that*

$$\sum_i \phi(\sigma_i)(\sigma_i \cdot a) = 0, \tag{2.5}$$

for all $a \in E$. Then $\phi(\sigma_i) = 0$ for all i.

Proof. A proof may be found in [Isa94, p. 346]. □

Example 2.2.1. Let $\mathbf{k} \subset E$ be a field, and let G be a finite group acting as $\mathbf{k}$-automorphisms on E. Let $F = E^G = \{A \in E \mid g \cdot a = a, \ \forall\, g \in G\}$. The group algebra $\mathbf{k}G$ acts on E, so its dual $(\mathbf{k}G)^*$ coacts by Lemma 1.4.1.

It is a standard result from classical Galois theory that E/F is classically Galois with group G if and only if G acts faithfully on E if and only if $[E : F] = G$. We now suppose that G does act faithfully. Thus we set $|G| = n$ and let $G = \{x_1, \cdots, x_n\}$. Let $\{b_1, \cdots, b_n\}$ be a basis of E/F. Define a basis $\{p_1, \cdots, p_n\}$ of $(\mathbf{k}G)^*$ dual to the basis $\{x_1, \cdots, x_n\}$ of $\mathbf{k}G$. Since E is a left $\mathbf{k}G$-module, by Lemma 1.4.1, it is a right $(\mathbf{k}G)^*$-comodule. We may thus define the coaction $\rho : E \longrightarrow E\otimes_{\mathbf{k}}(\mathbf{k}G)^*$, given by $\rho(a) = \sum_{i=1}^{n}(x_i \cdot a)\otimes p_i$ for all $a \in E$. This is determined by the action of G on E. In order to consider the Galois map, we need first to need show that the coinvariants of E, $E^{co(\mathbf{k}G)^*}$, are contained in F. But this is clear, since by Lemma 1.4.3, $E^{co(\mathbf{k}G)^*} = E^{\mathbf{k}G} = \{a \in E \mid h \cdot a = \varepsilon(h)a, \ \forall\, h \in \mathbf{k}G\}$. Now for all $g \in G$, $\varepsilon(g) = 1$, so clearly if $a \in E^{\mathbf{k}G}$, then $a \in E^G$ also. We may thus consider the Galois map, $\beta : E\otimes_F E \longrightarrow E\otimes(\mathbf{k}G)^*$, given by $\beta(a\otimes b) = \sum_i a(x_i \cdot b)\otimes p_i)$. Now let $v = \sum_j a_j \otimes b_j \in \ker(\beta)$. Then $\beta(v) = \sum_i(\sum_j a_j(x_i \cdot b)\otimes p_i) = 0$. Since the $\{p_i\}$ are independent, we must have

$$\sum_j a_j(x_i \cdot b_j) = 0, \quad \forall i. \tag{2.6}$$

Now let

$$X = \begin{bmatrix} x_1 \cdot b_1 & \cdots & x_1 \cdot b_n \\ \vdots & \ddots & \vdots \\ x_n \cdot b_1 & \cdots & x_n \cdot b_n \end{bmatrix},$$

which is contained in $M_{n\times n}(E)$. Let R_i be the i^{th} row of X. If $\sum_{i=1}^{n} \lambda_i R_i = 0$ for some $\lambda_i \in E$, then $\sum_{i=1}^{n} \lambda_i x_i \cdot b_j = 0$ for all j. Therefore, $(\sum_{i=1}^{n} \lambda_i x_i) \cdot b_j = 0$ for all j. Now $E = \sum_j F b_j$ so $(\sum_{i=1}^{n} \lambda_i x_i) \cdot a = 0$ for all $a \in E$. Further, $\sum_{i=1}^{n} \lambda_i x_i \in \mathrm{End}_F(E)$, so by Dedekind's Lemma, we must have $\sum_{i=1}^{n} \lambda_i x_i = 0$, which contradicts the linear independence of $\{x_i\}$. Therefore, X must be invertible. Hence, in Equation 2.6 above, since X has column rank of n, we must have $a_j = 0$ for all j. Hence β is injective. Also note that both $E \otimes_F E$ and $E \otimes (\mathbf{k}G)^*$ are finite dimensional F-algebras, which gives that β is an isomorphism.

Example 2.2.2. This example is from [GP87].

For any K, we define H_K to be the *circle Hopf algebra.* This has algebra structure given by $H_K = K[c,s]/(c^2 + s^2 - 1, cs)$, where $K[c,s]$ is the polynomial algebra, and coalgebra structure given by $\Delta(c) = c\otimes c - s \otimes s$, $\Delta(s) = c \otimes s + s \otimes c$, $\varepsilon(c) = 1$, $\varepsilon(s) = 0$, $S(c) = c$ and $S(s) = -s$.

Now consider $F = \mathbb{Q}$ and $E = F(\omega)$, where ω is the real fourth root of two. The extension $F \subset E$ is not Galois for any group G; however, it is $(H_K)^*$-Galois for $K = \mathbb{Q}$. The action of H_K on E is given below:

$\cdot$	1	ω	ω^2	ω^3
c	1	0	$-\omega^2$	0
s	0	$-\omega$	0	ω^3

A proof of the fact that $\mathbb{Q} \subset E$ is (H_K^*)-Galois can be found in [GP87] and [Chi89].

Example 2.2.3. Let $H = \mathbf{k}G$, and let N be a normal subgroup of G. Then $\mathbf{k}N \subset \mathbf{k}G$ is a Galois extension.

Consider the canonical map $\pi : \mathbf{k}G \longrightarrow \mathbf{k}(G/N)$. Now define the map $\rho = (id \otimes \pi) \circ \Delta$, where Δ is the comultiplication map of $\mathbf{k}G$. Then $\mathbf{k}G$ is a right $\mathbf{k}(G/N)$-comodule via ρ. This is justified in Definition 1.4.4.

Recall that $\Delta(g) = g \otimes g$ for all $g \in G$, so the comodule map is given by $\rho(g) = g \otimes (g + \mathbf{k}N) = g \otimes \overline{g}$. Thus, for all $x, y \in G$ the Galois map $\beta : \mathbf{k}G \otimes_{\mathbf{k}N} \mathbf{k}G \longrightarrow \mathbf{k}G \otimes \mathbf{k}(G/N)$ is given by

$$\begin{aligned} \beta(x \otimes y) &= (x \otimes 1)\rho(y) \\ &= (x \otimes 1)(y \otimes (y + \mathbf{nk}N)) \\ &= xy \otimes (y + \mathbf{nk}N) \\ &= xy \otimes \overline{y}, \end{aligned}$$

where $\mathbf{n}$ is the augmentation ideal of $\mathbf{k}N$. Clearly, β is onto, since for all $a \otimes \overline{b}$, where $a \in G$ and $\overline{b} = bN \in G/N$, there exists $c \otimes d \in \mathbf{k}G$ with $\beta(c \otimes d) = a \otimes \overline{b}$; that is, we take $c = ab^{-1}$ and $d = b$. To show that it is also injective, we note that the map $g \otimes \overline{h} \mapsto gh^{-1} \otimes h$, for all $g \otimes \overline{h} \in \mathbf{k}G \otimes \mathbf{k}(G/N)$ with $g \in G$ and $\overline{h} = hN \in G/N$, is an inverse for β, and so β is bijective. Thus, $\mathbf{k}N \subseteq \mathbf{k}G$ is a $\mathbf{k}(G/N)$-Galois extension.

Finally, we consider Frobenius extensions. First, however, we require the following lemma.

Lemma 2.2.2. *Let $S \subseteq R$ be two rings. Then $Hom_S({}_SR, {}_SS)$ is a (R, S)-bimodule via the maps $(r \cdot \phi)(x) = \phi(xr)$ and $(\phi \cdot s)(x) = \phi(x)s$ for all $s \in S$, $r, x \in R$ and $\phi \in Hom_S({}_SR, {}_SS)$.*

Proof. This proof is from [Bea99, Proposition 2.6.7(b)].

Consider the map $r \cdot \phi : R \longrightarrow S$ given above. We want to show that this is an S-homomorphism, and then that it defines a left R-module structure. Clearly, $r \cdot \phi$ is an S-module homomorphism, since for all $x_1, x_2 \in R$,

$$\begin{aligned} r \cdot \phi(x_1 + x_2) &= \phi((x_1 + x_2)r) \\ &= \phi(x_1 r + x_2 r) \\ &= \phi(x_1 r) + \phi(x_2 r) \\ &= r \cdot \phi(x_1) + r \cdot \phi(x_2) \end{aligned}$$

and for all $s \in S$ and $x \in R$,

$$\begin{aligned} s(r \cdot \phi)(x) &= s\phi(xr) \\ &= \phi(sxr) \\ &= r \cdot \phi(sx). \end{aligned}$$

Let $r, r_1, r_2, x \in R$ and $\phi, \phi_1, \phi_2 \in \mathrm{Hom}_S(R, S)$. The following computations verify that this map defines a left R-module structure on $\mathrm{Hom}_S(R, S)$.

$$\begin{aligned}
(r_1 + r_2) \cdot \phi(x) &= \phi(x(r_1 + r_2)) \\
&= \phi(xr_1 + xr_2) \\
&= \phi(xr_1) + \phi(xr_2) \\
&= r_1 \cdot \phi(x) + r_2 \cdot \phi(x) \\
&= (r_1 \cdot \phi + r_2 \cdot \phi)(x)
\end{aligned}$$

$$\begin{aligned}
r \cdot (\phi_1 + \phi_2)(x) &= (\phi_1 + \phi_2)(xr) \\
&= \phi_1(xr) + \phi_2(xr) \\
&= r \cdot \phi_1(x) + r \cdot \phi_2(x) \\
&= (r \cdot \phi_1 + r \cdot \phi_2)(x)
\end{aligned}$$

$$\begin{aligned}
((r_1 r_2) \cdot \phi)(x) &= \phi(x r_1 r_2) \\
&= \phi((x r_1) r_2) \\
&= r_2 \cdot \phi(x r_1) \\
&= (r_1 \cdot (r_2 \cdot \phi))(x).
\end{aligned}$$

Thus, $\mathrm{Hom}_S(R, S)$ is a left R-module.

The proof that the map $\phi \cdot s : R \longrightarrow S$ defined in the lemma is an S-homomorphism is similar to that above. We also need to check that this map imposes a right S-module structure on $\mathrm{Hom}_S(R, S)$. This follows in a similar manner to the calculations given above; we prove the first condition here. Let $s_1, s_2 \in S$.

$$\begin{aligned}
\phi \cdot (s_1 + s_2)(x) &= \phi(x)(s_1 + s_2) \\
&= \phi(x)s_1 + \phi(x)s_2 \\
&= (\phi \cdot s_1)(x) + (\phi \cdot s_2)(x) \\
&= (\phi \cdot s_1 + \phi \cdot s_2)(x).
\end{aligned}$$

The remaining conditions follow similarly. $\square$

Definition 2.2.3. Let $S \subseteq R$ be two rings. Suppose that R is a finitely generated left projective S-module and that ${}_R R_S \cong \mathrm{Hom}_S({}_S R, {}_S S)$ as (R, S)-bimodules. Then R is a Frobenius extension of S.

Before considering any examples, we define the following important concept, and also consider a useful result for Frobenius algebras.

Definition 2.2.4.

(1) Let S be a subring of the ring R. We define an *associative form* from R to S to be a biadditive map $\langle , \rangle : R \times R \longrightarrow S$ which satisfies

$$\langle sr, t\rangle = s\langle r, t\rangle, \quad \langle r, ts\rangle = \langle r, t\rangle s, \quad \text{and} \quad \langle rt, x\rangle = \langle r, tx\rangle,$$

for all $s \in S$ and $r, t, x \in R$.

(2) Let $\langle , \rangle : R \times R \longrightarrow S$ be an associative form. Let $X = \{x_1, \cdots, x_n\}$ and $Y = \{y_1, \cdots, y_n\}$ be two finite subsets satisfying

$$r = \sum_{i=1}^{n} y_i \langle x_i, r\rangle = \sum_{i=1}^{n} \langle r, y_i\rangle x_i \quad \text{for all } r \in R.$$

We say that X and Y form a *dual projective pair relative to* $\langle , \rangle$.

Remark 2.2.1. We note that the S-linear mappings $\alpha_i : R \longrightarrow S$, given by $\alpha_i(r) = \langle r, y_i\rangle$, together with the set $\{x_1, \cdots, x_n\}$, are a projective basis for R as an S-module.

The following theorem is taken from [BF93].

Theorem 2.2.3. *Let S be a subring of the ring R. Then R is a Frobenius extension of S if and only if there exists an associative form $\langle , \rangle$ from R to S, relative to which a dual projective pair exists.*

Proof.
$\Rightarrow$: Since R is a Frobenius extension of S, there exists an isomorphism $\alpha : R \longrightarrow \mathrm{Hom}_S({}_SR, S)$ of (R, S)-bimodules. We use this to define a bilinear form $\langle , \rangle : R \times R \longrightarrow S$, given by $\langle x, y\rangle = \alpha(y)(x)$ for all $x, y \in R$. To show that this is an associative form, we must show that it satisfies the requirements given in Definition 2.2.4. Consider $\langle sx, y\rangle = \alpha(y)(sx)$, where $s \in S$. Then

$$\begin{aligned} \alpha(y)(sx) &= s\alpha(y)(x), \quad \text{since } \alpha(y) \in \mathrm{Hom}_S(R, S) \\ &= s\langle x, y\rangle. \end{aligned}$$

To show that $\langle x, ys\rangle = \langle x, y\rangle s$, we note that α is a right S-module isomorphism. Thus:

$$\begin{aligned}\langle x, ys\rangle &= \alpha(ys)(x)\\ &= (\alpha(y)s)(x)\\ &= \alpha(y)(x)s\\ &= \langle x, y\rangle s.\end{aligned}$$

Finally, using the second definition of the bimodule action given in Definition 2.2.4, we show that $\langle xr, y\rangle = \langle x, ry\rangle$ for all $x, y, r \in R$.

$$\begin{aligned}\langle x, ry\rangle &= \alpha(ry)(x)\\ &= (r{\cdot}\alpha(y))(x) \quad \text{since } \alpha \text{ is an R-homomorphism}\\ &= \alpha(y)(xr) \quad \text{by Lemma 2.2.2}\\ &= \langle xr, y\rangle.\end{aligned}$$

So $\langle , \rangle : R\otimes R \longrightarrow S$ is indeed an associative form.

Now let $x_1, \cdots, x_n$ in R and $\alpha_1, \cdots, \alpha_n$ in $\mathrm{Hom}_S(R, S)$ form a projective basis for the S-module R. We want to show that these sets form a dual projective pair. Since $\alpha_i \in \mathrm{Hom}_S(R, S)$, we can always find an element y_i, where $1 \leq i \leq n$, such that $\alpha(y_i) = \alpha_i$. Now let $r \in R$. Then for all such r,

$$r = \sum_{i=1}^{n} \alpha_i(r)x_i = \sum_{i=1}^{n} \alpha(y_i)(r)x_i = \sum_{i=1}^{n} \langle r, y_i\rangle x_i$$

Now suppose that we have $\phi \in \mathrm{Hom}_S(R, S)$. Applying this to the second equality above gives

$$\phi(r) = \phi \sum \alpha(y_i)(r)x_i = \sum \phi(\alpha(y_i)(r)x_i) = \sum \alpha(y_i)(r)\phi(x_i) \quad \text{since } \alpha(y_i)(r) \in S.$$

Then by using the definition of the right S-action given on $\mathrm{Hom}_S(R, S)$ in Lemma 2.2.2, we get

$$\phi = \sum_{i=1}^{n} \alpha(y_i) \cdot \phi(x_i)$$

If we further assume that $\phi = \alpha(r)$, this gives $\alpha(r) = \alpha(\sum_{i=1}^{n} y_i\langle x_i, r\rangle)$; therefore, $r = \sum_{i=1}^{n} y_i\langle x_i, r\rangle$. Thus $\{x_1, \cdots, x_n\}$ and $\{\alpha_1, \cdots, \alpha_n\}$ are a dual projective pair.

$\Leftarrow$: As already discussed in Remark 2.2.1, R has a finite projective basis as an S-module, and so is a finitely-generated projective S-module. To show that R is a Frobenius extension of S, we thus need to prove that $R \cong \mathrm{Hom}_S(R, S)$. Consider the map $\gamma : R \longrightarrow \mathrm{Hom}_S({}_SR, S)$, given by $r \mapsto \langle -, r\rangle$. We need to show that this is an isomorphism of (R, S)-bimodules. It is clearly a right S-module homomorphism, since by definition of associative forms,

$$\gamma(rs) = \langle -, rs\rangle = \langle -, r\rangle s,$$

for $r \in R$ and $s \in S$. Now consider $a, r \in R$. We have $\gamma(ar) = \langle -, ar\rangle$. If $x \in R$, then

$$\begin{aligned}
\langle x, ar\rangle &= \langle xa, r\rangle \\
&= \gamma(r)(xa) \\
&= a \cdot \gamma(r)(x),
\end{aligned}$$

where $\cdot$ is the action of R on $\mathrm{Hom}_S(R, S)$. Thus γ is also a left R-module homomorphism. Further, suppose that $\langle x, r\rangle = 0$ for all $x \in R$. By nondegeneracy, this implies that $r = 0$. Thus $\ker(\gamma) = 0$, and so γ is injective. To show that γ is onto, we consider $h \in \mathrm{Hom}_S({}_SR, S)$. Then for all $r \in R$, we have

$$\begin{aligned}
h(r) &= h(\sum_i \langle r, y_i\rangle x_i) \\
&= \sum_i \langle r, y_i\rangle h(x_i) \\
&= \sum_i \langle r, y_i\rangle h(\sum_j \langle x_i, y_j\rangle x_j) \\
&= \sum_{i,j} \langle r, y_i\rangle \langle x_i, y_j\rangle h(x_j) \\
&= \sum_j \langle \sum_i \langle r, y_i\rangle x_i, y_j\rangle h(x_j) \\
&= \sum_j \langle r, y_j\rangle h(x_j) \\
&= \langle r, \textstyle\sum_j y_j h(x_j)\rangle.
\end{aligned}$$

Thus, $h = \gamma(\sum_j y_j h(x_j))$, hence γ is onto, therefore bijective. So R is a Frobenius extension of S. $\square$

Let R be a Frobenius extension over S, and let $\langle , \rangle : R \longrightarrow S$ be the associative form given in Theorem 2.2.3 above. Consider the map $\pi : R \longrightarrow S$, given by $\pi(r) = \langle r, 1\rangle = \langle 1, r\rangle$. The map π is referred to as the Frobenius homomorphism associated to the Frobenius extension.

Example 2.2.4. Let $H = \mathbf{k}G$, and let be N a subgroup of G of finite index, so we may write $G = \cup_{i=1}^{t} Ng_i$, where $g_1 = 1$. We show that $\mathbf{k}N \subseteq \mathbf{k}G$ is a Frobenius extension.

We first need to establish that $\mathbf{k}G$ is a projective $\mathbf{k}N$ module, but this is clear, since N has finite index. Then $\mathbf{k}G$ is a free $\mathbf{k}N$-module with basis a set of coset representatives for N in G, and hence is a finitely generated projective $\mathbf{k}N$-module.

Secondly, we need to establish an isomorphism of $(\mathbf{k}G, \mathbf{k}N)$-bimodules between $\mathbf{k}G$ and $\mathrm{Hom}_{\mathbf{k}N}({}_{\mathbf{k}N}\mathbf{k}G, \mathbf{k}N)$. First, consider the left $\mathbf{k}N$-homomorphism $\pi : \mathbf{k}G \longrightarrow \mathbf{k}N$ given by $\gamma = \sum_{i=1}^{t} \gamma_i g_i \mapsto \gamma_1$ for $\gamma_i \in \mathbf{k}N$. We may thus define the map $\langle , \rangle : \mathbf{k}G \otimes \mathbf{k}G \longrightarrow \mathbf{k}N$, given by $\langle , \rangle : (\alpha, \beta) \mapsto \pi(\beta\alpha)$.

We now need to prove that the map $\vartheta : \mathbf{k}G \longrightarrow \mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N)$, given by $\alpha \mapsto f_\alpha$, where $f_\alpha(\beta) = \pi(\beta\alpha)$ for all $\alpha, \beta \in \mathbf{k}G$, is an isomorphism of $(\mathbf{k}G, \mathbf{k}N)$-bimodules. We must show that f_α is in $\mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N)$, that is, that f_α is a left $\mathbf{k}N$-module homomorphism. It is clear that the condition for addition holds. Now consider $\omega \in \mathbf{k}N$. Then

$$\begin{aligned} f_\alpha(\omega\beta) &= \pi(\omega\beta\alpha) \\ &= \omega\pi(\beta\alpha) \\ &= \omega f_\alpha(\beta), \end{aligned}$$

where the second line holds because π is a left $\mathbf{k}N$-module homomorphism.
So $f_\alpha \in \mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N)$.

We must also show that ϑ is a left $\mathbf{k}G$-module homomorphism and a right $\mathbf{k}N$-module homomorphism. We consider the case for $\mathbf{k}G$ first. Let $\alpha, \gamma \in \mathbf{k}G$. Now $\gamma\alpha \mapsto f_{\gamma\alpha}$. Then for all $\beta \in \mathbf{k}G$, we have

$$\begin{aligned} f_{\gamma\alpha} &= \pi(\beta\gamma\alpha) \\ &= \vartheta(\alpha)(\beta\gamma) \\ &= \gamma\cdot\vartheta(\alpha)\vartheta(\beta), \end{aligned}$$

where $\cdot$ is the left action of $\mathbf{k}G$ on $\mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N)$.

To show that ϑ is a right $\mathbf{k}N$-module homomorphism, we consider $\alpha\omega \mapsto f_{\alpha\omega}$. Then for all $\omega \in \mathbf{k}N$ and for $\alpha \in \mathbf{k}G$,

$$\begin{aligned} f_{\alpha\omega}(\beta) &= \pi(\beta\alpha\omega) \\ &= \pi(\sum_{i=1}^{t} u_i g_i \omega) \quad \text{where } \beta\alpha = \sum_i u_i g_i \quad \text{for } u_i \in \mathbf{k}N \\ &= \pi(u_1\omega + \sum_{i=2}^{t} u_i g_i \omega) \quad \text{since } g_1 = 1. \end{aligned}$$

Note that each $g_i\omega$ is a linear combination of group elements in $\cup_{i=2}^{t} N g_i$. This implies that

$$\begin{aligned} \pi(u_1\omega + \sum_{i=2}^{t} u_i g_i \omega) &= u_1\omega \\ &= \pi(\beta\alpha)(\omega) \\ &= f_\alpha(\beta)\omega \\ &= (f_\alpha \cdot \omega)(\beta). \end{aligned}$$

So ϑ is a $(\mathbf{k}G), \mathbf{k}N)$-bimodule homomorphism as claimed.

Finally, we show that ϑ is bijective. We first consider the case for injectivity. Consider $\alpha = \sum_i g_i \alpha_i'$, with $\alpha_i' \in \mathbf{k}N$ for all i and assume $\alpha \in \neq 0$. This implies that there exists at least one j such that $\alpha_j' \neq 0$. Then

$$\begin{aligned} f_\alpha(g_j^{-1}) &= \pi(g_j^{-1}(\sum_i g_i \alpha_i)) \\ &= \pi(\alpha_j' + \omega), \quad \text{where } \omega \in \sum_{i=2}^{t} \mathbf{k}N g_i \\ &= \alpha_j' \neq 0. \end{aligned}$$

Thus ϑ is injective.

We show that ϑ is also onto. We have

$$\mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N) = \oplus_{i=1}^{t} \mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}N g_i, \mathbf{k}N) \cong \oplus_i f_i \mathbf{k}N,$$

where

$$f_i : \begin{cases} g_i \longrightarrow 1 \\ g_j \longrightarrow 0, \quad j \neq i \end{cases}$$

We know that ϑ is a right $\mathbf{k}N$-module homomorphism. We also note that $\mathrm{Im}(\vartheta)$ contains a $\mathbf{k}N$-generating set of $\mathrm{Hom}_{\mathbf{k}N}(\mathbf{k}G, \mathbf{k}N)$. Therefore, if we can show that there exists $\sigma \in \mathbf{k}G$ such that $f_\sigma = f_i$ for all i, ϑ is onto. Consider the element g_i^{-1}. Then

$$\begin{aligned} f_{g_i^{-1}}(g_j) &= \pi(g_j g_i^{-1}) \\ &= \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases} \end{aligned}$$

since in this case $g_j g_i^{-1} \notin N$. So $f_{g_i^{-1}} = f_i$; hence ϑ is onto and thus bijective.

So we have a $(\mathbf{k}G, \mathbf{k}N)$-bimodule isomorphism between $\mathbf{k}G$ and $\mathrm{Hom}_{\mathbf{k}N}({}_{\mathbf{k}N}\mathbf{k}G, \mathbf{k}N)$, and hence $\mathbf{k}G$ is a Frobenius extension over $\mathbf{k}N$.

The following examples are taken from [BF93].

Example 2.2.5. This example generalises Example 2.2.4 above to the case of any strongly G-graded ring. Recall that a ring R is *graded* by the group G if $R = \oplus_{g \in G} R_g$ where R_g is an Abelian subgroup of R for all g, and $R_g R_h \subseteq R_{gh}$ for all $g, h \in G$. If equality holds in this expression for all $g, h \in G$, then R is said to be *strongly graded* by G. The strongly graded condition is equivalent to the existence of the sets $\{x_{1,g} \cdots, x_{m(g),g}\} \subset R_g$ and $\{y_{1,g}, \cdots, y_{m(g),g}\} \subset R_{g^{-1}}$ with $\sum_{i=1}^{m(g)} y_{i,g} x_{i,g} = 1$ for all $g \in G$. Suppose that R is strongly graded by G, and also that $S = \oplus_{g \in H} R_g$, where H is a subgroup of finite index in G. Then we claim that R is a Frobenius extension over S.

To prove this, we define the Frobenius homomorphism as $\pi(\sum_{g \in G} r_g) = \sum_{g \in H} r_g$. This means that the associative form is given by

$$\langle \sum_{g \in G} r_g, \sum_{g' \in G} r'_{g'} \rangle = \langle (\sum_{g \in G} r_g)(\sum_{g' \in G} r'_{g'}), 1 \rangle = \sum_{gg' \in H} r_g r'_{g'}$$

Now let K be a subset of G such that $\{Hg \mid g \in K\}$ is a complete set of right cosets for H in G. Then the sets

$$\begin{aligned} X : &= \{x_{i,g} \mid g \in K, \ 1 \leq i \leq m(g)\} \subset R_g \quad \text{and} \\ Y : &= \{y_{i,g} \mid g \in K, \ 1 \leq i \leq m(g)\} \subset R_{g^{-1}} \end{aligned}$$

form a dual projective pair, and thus R is a Frobenius extension of S.

2.3 Faithful Flatness

2.3.1 Overview

The main aim of this chapter is to show some of the circumstances under which a Hopf algebra is flat, faithfully flat or free over a subalgebra. We also give a condition for the properties of flatness and faithful flatness to be equivalent. There has been a substantial amount of work done in this field, and only a small number of results are included here. Before discussing these, however, we give the following brief overview of some known results.

The Finite Dimensional Case

Assuming finite dimension substantially simplifies the situation; work by Warren Nichols and M. Bettina Zoeller in the late eighties shows that under this condition a Hopf algebra is always free over any sub-Hopf algebra. Note that (H, K)-Hopf modules have not yet been defined; we direct the reader to Definition 2.3.2 below.

Theorem 2.3.1 (The Nichols-Zoeller Theorem). *Let H be a finite dimensional Hopf algebra over a field $\mathbf{k}$, and let K be a sub-Hopf algebra. Then for any (H, K)-Hopf module M, we have that M is free as a K-module. In particular, since H is a (H, K)-Hopf module, H is free over K.*

Proof. This is proved in [NRZ89]. □

The Infinite Dimensional Case

In this case, as might be expected, the situation is much less straightforward. Indeed, it is known that H is not generally free over a sub-Hopf algebra K unless K is finite-dimensional and has certain other properties, as the following example (due to Oberst and Schneider) shows.

Example 2.3.1. Let F be a field, and let E be a field extension of F of degree 2 with Galois group $G = \{1, \sigma\}$. The action of σ on $\mathbb{Z}$ is given by $z \mapsto -z$. Then G acts on the group algebra $E\mathbb{Z}$ by its actions on E and G. We set $H = (E\mathbb{Z})^G$ and $K = (E(n\mathbb{Z}))^G \subset H$. If n is even, H is not free over K.

Proof. See [OS74]; a proof may also be found in [Mon93, Example 3.5.2]. □

We now consider some special cases when H is free over K. We recall the notion of *semisimplicity*: a finite dimensional algebra R is said to be semisimple if every left R-module is completely reducible. The first part of the following theorem is a generalisation of the Nichols-Zoeller Theorem for the infinite-dimensional case.

Theorem 2.3.2. *Let H be a Hopf algebra as above, and let K be a finite-dimensional sub-Hopf algebra of H. Suppose that one of the following hold:*

(1) K is semisimple,

(2) K is normal;

then H is free over K.

Proof.

(1) Proved in [NRZ92, Theorem 4].

(2) Proved in [Sch93].

□

The case for faithful flatness has been the subject of much interest recently, since this property is almost as useful as freeness in many situations. However, it is still an open question whether a Hopf algebra H is always faithfully flat over a sub-Hopf algebra K. It is known to be true if H is commutative (see Lemma 2.3.7 and Lemma 4.1.1), or if the *coradical* of H is cocommutative, where the coradical is the sum of those subcoalgebras of H which have no proper subcoalgebras. We discuss a further condition for faithful flatness in the remainder of this chapter.

2.3.2 Conditions Giving Faithful Flatness

We begin with the following technical result from ring theory.

Definition 2.3.1. Let R be a ring. R is said to be *weakly finite* if for all finitely generated free left R-modules M and for all surjective $\phi \in \mathrm{End}_R(M)$, ϕ is also bijective.

Example 2.3.2. Let R be a left Noetherian ring. Then R is weakly finite.

Proof. Let M be a finitely generated free R-module. Consider an R-module homomorphism $\phi : M \longrightarrow M$ such that ϕ is onto. Let $K = \ker(\phi)$. Suppose that $K \neq 0$. Then we have $M/K \cong M$ by the first Homomorphism Theorem, and there exists $K_1 \supsetneq K$ such that $\frac{M/K}{K_1/K} \cong M/K \cong M$. Therefore, $M/K_1 \cong M$. We may continue in this way, producing an infinite ascending chain of submodules of M. But this contradicts our initial assumption that R is left Noetherian, hence $K = \{0\}$. Therefore ϕ is bijective. □

Definition 2.3.2. Let $\mathbf{k}$ be a field. Let K be a sub-Hopf algebra of the Hopf algebra H over the field $\mathbf{k}$. Consider a right K-module M. Suppose that M is also a right H-comodule, via the map $\rho : M \longrightarrow M \otimes H$, such that ρ is a K-linear structure map, that is,

$$\rho(mk) = \sum m_0 k_1 \otimes m_1 k_2,$$

for all $m \in M$ and $k \in K$. Then M is said to be a right (H, K)-Hopf module.

Example 2.3.3.

(1) Let $M = H$. Then H is a right (H, K)-Hopf module via the comultiplication map $\Delta = \rho$.

(2) Let N be any right H-module. Then $M = N \otimes H$ is a right (H, K)-Hopf module via the map $\rho = id \otimes \Delta$.

We now consider the following technical results, which are taken from [Tak72] and [Sch93] and are required for the proof of Theorem 2.3.9.

Proposition 2.3.3. *Let B be a sub-Hopf algebra of the Hopf algebra A. Any right (A, B)-module is a filtered union of those of its (A, B)-sub-Hopf modules which are finitely generated as right B-modules.*

Proof. See [Tak72, Corollary 2.3]. □

Lemma 2.3.4. *Let A be a Hopf algebra with bijective antipode, and let $B \subseteq A$ be a sub-Hopf algebra. Then if A is flat as a right B-module, it is also faithfully flat as a right B-module.*

Proof. See [MW94, Theorem 2.1]. □

The following proposition is taken from [Tak72, Proposition 2.4].

Proposition 2.3.5. *Let $B \subseteq A$ be Hopf algebras and suppose that every finitely generated right (A,B)-Hopf module is flat. Then A is right faithfully flat over B.*

Proof. Proposition 2.3.3 implies every right (A,B)-module is a flat B-module, because a direct limit of flat modules is flat. For a proof of this, see the discussion on direct limits and flat modules in [Rot79]. Since A is a right (A,B)-Hopf module, it is therefore a flat B-module. Thus, by Lemma 2.3.4, A is a faithfully flat right B-module. □

The following lemma is taken from [Sch93, Lemma 3.1].

Lemma 2.3.6. *Let A be a Hopf algebra, and $B \subseteq A$ a central sub-Hopf algebra. Let M be any (A,B)-Hopf module. We define the central localisation of M at B^+ (the augmentation ideal of B) as $M_{B^+} = M \otimes_B B_{B^+}$. If A is weakly finite, then the central localisation of M at B^+ is a flat B-module.*

Proof. Consider an (A,B)-Hopf module M. By Proposition 2.3.3, this is a filtered union of finitely generated B-modules which are (A,B)-Hopf modules. We may thus assume that M is a finitely generated B-module, since a union of flat modules is also flat. Let r be the rank of M/MB^+ over $\mathbf{k}$. We begin by showing that $M \otimes_B A$ is free of rank r as a right A-module. Because M is a Hopf module, we can define the homomorphism of right A-modules

$$\gamma : M \otimes_B A \longrightarrow M/MB^+ \otimes A;\ m \otimes a \mapsto \sum \overline{m}_1 \otimes m_2 a,$$

Consider the right A-module homomorphism $\sigma : M/MB^+ \otimes A \longrightarrow M \otimes_B A$, given by $\overline{m} \otimes a \mapsto \sum m_1 \otimes S(m_2) a$. We claim that γ is an isomorphism. This is proved by showing that $\sigma \circ \gamma = \gamma \circ \sigma = id$. Consider $\gamma \circ \sigma$, and let $\overline{m} \in M/MB^+$ and $a \in A$. Then

$$\begin{aligned}
\gamma(\sigma(\overline{m} \otimes a)) &= \gamma(\sum m_1 \otimes S(m_2) a) \\
&= \sum (\overline{m}_1)_1 \otimes (m_1)_2 S(m_2) a \\
&= \sum \overline{m}_1 \otimes m_2 S(m_3) a \\
&= \sum \overline{m}_1 \otimes \varepsilon(m_2) a \\
&= \sum \overline{m}_1 \varepsilon(m_2) \otimes a \\
&= \overline{m} \otimes a.
\end{aligned}$$

Let $m \in M$ and $a \in A$. Then for $\sigma \circ \gamma$ we have

$$\begin{aligned}
\sigma(\gamma(m \otimes a)) &= \sigma(\sum \overline{m}_1 \otimes m_2 a) \\
&= \sum (m_1)_1 \otimes S(m_1)_2 m_2 a \\
&= \sum m_1 \otimes S(m_2) m_3 a \\
&= \sum m_1 \otimes \varepsilon(m_2) a \\
&= \sum m_1 \varepsilon(m_2) \otimes a \\
&= m \otimes a.
\end{aligned}$$

Thus γ is indeed an isomorphism. So $M \otimes_B A$ is free of rank r as a right A-module.

Since $M_{B^+}/M_{B^+}B^+ \cong M/MB^+$ has dimension r, Nakayama's lemma gives that the B_{B^+}-linear map

$$f : \oplus^r B_{B^+} \longrightarrow M_{B^+}$$

is surjective. We want to show that this is also injective, which we do by showing that there exists a ring extension $B_{B^+} \subset S$ such that $f \otimes 1_S$ is injective; that is, the map $f \otimes 1_S : \oplus^r B_{B^+} \otimes S \longrightarrow M_{B^+} \otimes S$ is injective. Consider the surjective right A_{B^+}-linear mapping $f \otimes_{B_{B^+}} A_{B^+} : \oplus^r B_{B^+} \otimes_{B_{B^+}} A_{B^+} \longrightarrow M_{B^+} \otimes_{B_{B^+}} A_{B^+}$. Now $\oplus^r B_{B^+} \otimes_{B_{B^+}} A_{B^+} \cong \oplus^r A_{B^+}$, since A_{B^+} is the B-module obtained by extension of scalars from B_{B^+}. We also have that $M_{B^+} \otimes_{B_{B^+}} A_{B^+} \cong (M \otimes_B A)_{B^+} \cong \oplus^r A_{B^+}$, as right A_{B^+}-modules. This shows that $f \otimes_{B_{B^+}} A_{B^+} \in \mathrm{End}(\oplus^r A_{B^+})$ is surjective, and therefore, since A_{B^+} is weakly finite, $f \otimes_{B_{B^+}} A_{B^+}$ is bijective. Hence M_{B^+} is free of rank r over B_{B^+}, and thus flat over B. □

Lemma 2.3.7. *Let A be a commutative Hopf algebra and let B be a Hopf subalgebra. Then A is a flat B-module for all such B.*

Proof. A proof of this can be found in [MW94, Theorem 3.4]. □

The next lemma is from [Sch93, Lemma 3.2]. To prove it, we need Hilbert's Nullstellensatz. A statement and proof of this can be found in [Rei88, p. 54–56].

Lemma 2.3.8. *Assume that* $\mathbf{k}$ *is an algebraically closed field and let A be a Hopf algebra over* $\mathbf{k}$*. Let $B \subset A$ be a central affine sub-Hopf algebra, such that M_{B^+} is flat over B for all (A, B)-Hopf modules M. Then any (A, B)-Hopf module is flat over B.*

Proof. Let J be a maximal ideal of B. Then by the Nullstellensatz, we have $B/J \cong \mathbf{k}$. Define $\pi : B \longrightarrow B/J$ to be the canonical map, and let $\alpha : B \longrightarrow B$, given by $b \mapsto \sum \pi(S(b_1))b_2$ be the induced automorphism of B which maps B^+ onto J.

Let X be a right B-module, and β be any algebra automorphism of B. We define X_β to be the 'twisted' B-module with underlying $\mathbf{k}$-module X and with B-module structure given by the map $x \circ_\beta b = x\beta(b)$ for all $x \in X$ and $b \in B$. Now let Y be any left B-module. Then $X_\beta \otimes_B Y \cong X \otimes_B ({}_{\beta^{-1}}Y)$, as can be seen by considering the tensor product. Therefore, if M is flat, so is M_β.

Consider an (A, B)-Hopf module M, and let $m \in M$ and $b \in B$. For all such m and b, we define the map $\Delta_{M_\alpha} : M_\alpha \longrightarrow M_\alpha \otimes A$ by $\Delta_{M_\alpha} = \Delta_M$. Then for all $m \in M$ and $b \in B$,

$$\Delta_M(m\alpha(b)) = \sum m_0 \pi(S(b_1))b_2 \otimes m_1 b_3 = \sum m_0 \alpha(b_1) \otimes m_1 b_2 = \Delta_M(m)b.$$

So M_α is an (A, B)-Hopf module, where M_α is the twisted B-module discussed above. Also note that $M = M_\alpha$ as A-comodules. Since M_{B+} is flat by assumption, so is $(M_\alpha)_{B+}$ by the discussion above. Now we have

$$(M_{B+})_{\alpha^{-1}} \cong M_J,$$

as B-modules. So M_J is B-flat by the discussion above. Since J was chosen to be any maximal ideal, we therefore have that M is B-flat. □

This theorem is from [Sch93, Theorem 3.3].

Theorem 2.3.9. *Let A be a left or right Noetherian Hopf algebra, and $B \subseteq A$ an affine central sub-Hopf algebra. Then any (A, B)-Hopf module is flat over B, and so A is thus a faithfully flat B-module.*

Proof. Let M be an (A, B)-Hopf module. Let B_i denote the (A, B)-sub-Hopf modules from Proposition 2.3.3. Now M is an (A, B_i)-Hopf module for all B_i, so by Lemma 2.3.6, the localisation $M_{B_i^+}$ is a flat B_i-module. Since B_i is finitely generated for all i, Lemma 2.3.8 gives that M is B_i flat. Thus since B is a filtered union of the B_i, M must be B-flat. Then by Proposition 2.3.5, A is a faithfully flat B module. □

Remark 2.3.1. In summary, we see that if $B \subseteq A$ is a central sub-Hopf algebra and A is right or left Noetherian, then A is faithfully flat over B. It is possible to eliminate both the Noetherian and central conditions; however, it is then necessary to impose the condition that B is finite codimensional (that is, $\dim A/AB^+ < \infty$) and normal instead. This is a particular case of the result [Sch93, Theorem 2.1].

We now show that faithful flatness, together with the condition that B is normal, gives that A is Galois over B.

Lemma 2.3.10. *Let A be Hopf algebra, and let $B \subseteq A$ be a normal sub-Hopf algebra. Let $A/AB^+ = \overline{A}$. Then A has a right $\overline{A}$-comodule structure, since $\pi : A \longrightarrow \overline{A}$ is a Hopf morphism. Suppose further that A is faithfully flat over B. Then A is right $\overline{A}$-Galois over B.*

Proof. First we note that B is normal, so $AB^+ = B^+A$ by Lemma 2.1.3. This lemma also implies that the canonical map $\pi : A \longrightarrow \overline{A}$ is a morphism of Hopf algebras, and so A has an $\overline{A}$-comodule structure, given by the map $\rho = (id_A \otimes \pi) \circ \Delta$. Since A is faithfully flat over B, Lemma 2.1.5 implies that $B = A^{co\overline{A}}$, so A is an extension over B. We need to show that the Galois map $\beta : A \otimes_B A \longrightarrow A \otimes_{\mathrm{k}} \overline{A}$, defined as $a \otimes a' \mapsto (a \otimes 1)\rho(a')$ for all $a, a' \in A$, is bijective. Now

$$\begin{aligned}
a \otimes b \mapsto (a \otimes 1)\rho(b) &= (a \otimes 1)(id_A \otimes \pi) \circ \Delta(b) \\
&= (a \otimes 1)(id_A \otimes \pi)(\sum b_1 \otimes b_2) \\
&= (a \otimes 1)\sum (id_A \otimes \pi)(b_1 \otimes b_2) \\
&= (a \otimes 1)\sum b_1 \otimes \bar{b}_2 \\
&= \sum (a \otimes 1)(b_1 \otimes \bar{b}_2) \\
&= \sum a b_1 \otimes \bar{b}_2.
\end{aligned}$$

There is an inverse map α to β, given by $\alpha : a \otimes \bar{b} \mapsto \sum aS(b_1) \otimes b_2$. These are the maps from Lemma 2.1.5, so, following the same argument, we get that $\beta \circ \alpha = \alpha \circ \beta = id$. Thus β is bijective, so A is an $\overline{A}$-Galois extension of B. □

Remark 2.3.2. Most of our results in this section have been for central sub-Hopf algebras, not normal ones. However, the central condition implies normality, as the following calculations show. Let K be a central sub-Hopf algebra of the Hopf algebra H. Choose $h \in H$ and $k \in K$. Then

$$\begin{aligned}
\mathrm{ad}_\ell(h)k &= \sum h_1 k S(h_2) \\
&= \sum h_1 S(h_2) k \\
&= \sum \varepsilon(h_1) k \\
&= \varepsilon(h) k.
\end{aligned}$$

But $\varepsilon(h) \in \mathbf{k}$, so $\varepsilon(h)k \in K$. Hence $\mathrm{ad}_\ell(H)K \subseteq K$. One uses a similar argument to show that $\mathrm{ad}_r(H)K \subseteq K$; thus K is normal.

Remark 2.3.3. If $B \subseteq A$ is a normal sub-Hopf algebra, and A is also a finitely generated B-module, B is then finite codimensional. By Remark 2.3.1, $B \subseteq A$ is thus Hopf Galois.

2.4 The Set of Integrals

Under certain extra conditions, Galois and Frobenius extensions are actually equivalent. Theorem 2.4.3 (from [KT81, Theorem 1.7(5)]) below gives one such condition. This is proved for algebras in general in [KT81], but we are specifically interested in the special case of Hopf algebras over a field $\mathbf{k}$. Before we do so, however, we recall Definition 1.4.4 and discuss two important properties of I_J. The following result is a special case of the result [KT81, Proposition 1.1], where the ring R is a field.

Proposition 2.4.1. *Let J be a Hopf algebra finitely generated as a $\mathbf{k}$-module, and let A be an algebra which is a J-Galois extension over a subalgebra B. Then the set I_J is a rank one projective $\mathbf{k}$-module, and further, $I_J \otimes J \cong J^*$.*

Proof. Since $\mathbf{k}$ is a field, I_J is automatically a projective $\mathbf{k}$-module and a $\mathbf{k}$-module direct summand of J^*. The fact that I_J is a rank one $\mathbf{k}$-module is proved in [Mon93, Theorem 2.1.3(1)]. □

Example 2.4.1. Let $B \subseteq A$ be an $\overline{A}$-Galois extension, where B is a finite codimensional sub-Hopf algebra of A and $\overline{A} = A/AB^+$. Then $I_{\overline{A}}$ is free of dimension one.

Proof. As in Definition 1.4.4, $I_{\overline{A}} = \overline{A}^{*co\overline{A}} \subseteq \overline{A}^*$. Now $\overline{A}$ is finite-dimensional, so $\overline{A}^*$ is also finite dimensional, hence free. Thus $I_{\overline{A}} \subseteq \overline{A}^*$ is free, and since it is of rank one, by Proposition 2.4.1, $\dim(I_{\overline{A}}) = 1$. □

Theorem 2.4.2. *Let H be a finite dimensional Hopf algebra, and let the Hopf algebra A be a H-Galois extension of the sub-Hopf algebra B. Then A is a finitely generated projective right B-module and $I_H \otimes A \cong Hom_B(A, B)$ as (B, A)-bimodules.*

Proof. A proof can be found in [KT81, Theorem 1.7]. □

We are now in a position to state and prove the result linking Galois and Frobenius extensions.

Theorem 2.4.3. *Let $B \subseteq A$ be an J-Galois extension of algebras A and B (over a field $\mathbf{k}$), where J is a finite-dimensional Hopf algebra. Then $B \subseteq A$ is a Frobenius extension.*

Proof. By Theorem 2.4.2, we know that A is a finitely generated right B-module. We note also from Theorem 2.4.2 that $I_J \otimes A \cong \mathrm{Hom}_B(A, B)$ as (B, A)-bimodules. Let $\{i\}$ be a basis for I_J. Now we can define a homomorphism $\alpha : A \longrightarrow I_J \otimes A$ by $a \mapsto i \otimes a$. This is clearly injective, and is also onto, since for all $ki \otimes a \in I_J \otimes A$, where $k \in \mathbf{k}$, there exists $ka \in A$ such that $\alpha(ka) = ki \otimes a$. Thus $A \cong I_J \otimes A$ and so $A \cong \mathrm{Hom}_B(A, B)$ as (B, A)-bimodules. Thus A is Frobenius over B. □

Example 2.4.2. In fact, when $\mathbf{k}$ is a field, I_J is always free since it is a finite dimensional $\mathbf{k}$-module. In this case, A is automatically a Frobenius extension over B. Thus our previous two examples, $U(\mathfrak{i}) \subseteq U(\mathfrak{g})$ and $\mathbf{k}N \subseteq \mathbf{k}G$, for $|G : N| < \infty$, are both Frobenius extensions.

Chapter 3

Homological Algebra and Module Theory

This is a collection of results from basic homological algebra and module theory which will be needed later in the proof of the proposition.

Definition 3.1. Let R be a ring, and let A be an R-module with projective resolution

$$\cdots P_n \xrightarrow{d'_n} P_{n-1} \longrightarrow \cdots \xrightarrow{d'_1} P_0 \xrightarrow{d'_0} A \longrightarrow 0$$

where the P_i are projective R-modules. Now let B be an R-module, and define the sequence

$$0 \longrightarrow \mathrm{Hom}_R(A, B) \xrightarrow{d_0} \mathrm{Hom}_R(P_0, B) \xrightarrow{d_1} \cdots \xrightarrow{d_{n-1}} \mathrm{Hom}_R(P_n, B) \xrightarrow{d_n} \cdots$$

We then define $\mathrm{Ext}^n_R(A, B) = \ker(d_{n+1})/\mathrm{Im}(d_n)$, for $n \geq 1$, with $\mathrm{Ext}^0_R(A, B) = \ker(d_1)$.

Theorem 3.1. Let A be an R-module for some ring R. Then

$$\mathrm{Hom}_R(A, B) = \mathrm{Ext}^0_R(A, B). \tag{3.1}$$

Further, the groups $\mathrm{Ext}^n_R(A, B)$ are independent of the choice of projective resolution of A.

Proof. The first follows from the fact that $\mathrm{Hom}_R(-, B)$ is left exact. A detailed proof can be found in [DF99, Proposition 17.1.3]. Proof of the second part can be found in [DF99, Theorem 17.1.6]. □

Note 3.1. One may also calculate $\mathrm{Ext}^n_R(A,B)$ by using the injective resolution as follows. We let A be an R-module as before with injective resolution

$$0 \longrightarrow M \xrightarrow{\hat{d'}_0} E_0 \xrightarrow{\hat{d'}_1} \cdots \xrightarrow{\hat{d'}_n} E_n \xrightarrow{\hat{d'}_{n+1}} \cdots$$

where E_i are injective R-modules for all i. We then let A be an R-module and apply the functor $\mathrm{Hom}_R(A,-)$ to give

$$0 \longrightarrow \mathrm{Hom}_R(A,M) \xrightarrow{\hat{d}_0} \mathrm{Hom}_R(A,E_0) \xrightarrow{\hat{d}_1} \cdots \xrightarrow{\hat{d}_n} \mathrm{Hom}_R(A,E_n) \xrightarrow{\hat{d}_{n+1}} \cdots$$

We can then define $\mathrm{Ext}^n_R(A,M) = \ker(\hat{d}_n)/\mathrm{Im}(\hat{d}_{n-1})$. These two definitions give the same answer; for a proof of this, see [Rot79, Theorem 7.8].

Definition 3.2.

(1) The *injective dimension of the R-module M*, written $\mathrm{id}(M)$, is defined to be the least n such that there exists an injective resolution of M:

$$0 \longrightarrow M \longrightarrow E_0 \longrightarrow E_1 \cdots \longrightarrow E_n \longrightarrow 0$$

If no such n exists, then we say that $\mathrm{id}(M) = \infty$.

(2) We similarly define the *projective dimension* of M, $\mathrm{pd}(A)$, as the least value of n such that there exists a projective resolution of M:

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow M \longrightarrow 0$$

Again, if no such resolution exists, $\mathrm{pd}(M) = \infty$.

(3) The *Krull dimension* of a Noetherian commutative ring R is defined to be the supremum of the length of all chains of prime ideals of the ring.

We discuss a further property of the injective dimension shortly but first consider the following result from [Rot79, Theorem 3.12].

Proposition 3.2. Let P be a projective module, and suppose that the module map $\gamma : M \longrightarrow P$ is onto. Then $M = \ker(\gamma) \oplus P'$, where $P' \cong P$.

The next result is taken from [NT60, Corollary 10].

Proposition 3.3. Let A be a Frobenius extension over the subring B such that $A = B \oplus X$ for some left and right B-module X. Then

$$\text{inj.dim}_B(B) = \text{inj.dim}_B(A).$$

Definition 3.3. Let R be a ring and M an R-module.

(1) The *left global dimension*, l.gl.dim(R) of R is defined to be $\sup\{\text{pd}(M) \mid {}_RM\}$. One may also define it in terms of injective dimension: l.gl.dim$(R) = \sup\{\text{id}(M) \mid {}_RM\}$. This is proved in [Rot79, Theorem 9.10].

(2) The *right global dimension*, r.gl.dim$R$ of R is defined similarly, but in terms of right R-modules, as opposed to left ones. Thus, r.gl.dim$(R) = \sup\{\text{pd}(M) \mid M_R\}$. As above, we may also define this using injective dimension.

Under certain circumstances, right and left global dimension are equal. The following theorem, from [Rot79, Theorem 9.23], gives one such condition.

Theorem 3.4. Let R be left and right Noetherian. Then l.gl.dim(R) = r.gl.dim(R).

Definition 3.4. Let R be a commutative Noetherian ring.

(1) R is said to be *smooth* if gl.dim$(R) < \infty$.

(2) If id$(R) < \infty$, then R is said to be a *Gorenstein* ring.

It is clear that a smooth ring is also Gorenstein.

The next theorem is an extract taken from [Rot79, Theorem 9.5], which is more general than required for our purposes here. The forward implication can be seen from Note 3.1.

Theorem 3.5. Let A be an R-module, where R is a ring. Then inj.dim$(A) \leq m < \infty$ if and only if $\text{Ext}^i_A(-, A) = 0$ for all $i \geq m+1$.

Next, we have a special case of a result involving injective dimension and Krull dim, proved in [Bas63, Lemma 3.3].

Theorem 3.6. Let A be a commutative Noetherian ring and consider it as a module over itself. If $\text{inj.dim}(A) < \infty$, then $\text{inj.dim}(A) = \text{Krull dim}(A)$.

Finally, we note the following results from module theory, proved in [NT60] and [Bea99, Proposition 2.6.9] respectively. Recall the notion of Frobenius extensions from Definition 2.2.3; that is, $A \cong \text{Hom}_B({}_BA, {}_BB)$ as (A, B)-bimodules.

Theorem 3.7. Let A be a Frobenius extension over B, and let M be a left B-module. Then $A \otimes_B M \cong \text{Hom}_B({}_BA, {}_BM)$ as (B, A)-bimodules.

Proof. First we note that the map $\gamma : A \otimes_B M \longrightarrow \text{Hom}_B(\text{Hom}_B({}_BA, B), {}_BM)$, via $\gamma(a \otimes m)\phi = \phi(a)m$, for $a \in A$, $m \in M$ and $\phi \in \text{Hom}_B(A_B, B)$ is a homomorphism of (B, A)-bimodules. By [NT60, Proposition 1], this is in fact an isomorphism of (B, A)-bimodules. Therefore,

$$\gamma : A \otimes_B M \cong \text{Hom}_B(\text{Hom}_B({}_BA, B), {}_BM).$$

But we have ${}_BA \cong \text{Hom}_B(A_B, B)$; thus

$$A \otimes_B M \cong \text{Hom}_B(\text{Hom}_B(A_B, B_B), {}_BM) \cong \text{Hom}_B({}_BA, {}_BM). \tag{3.2}$$

□

Lemma 3.8. Let R and S be rings and let ${}_SU_R$ be a bimodule. For any left R and S-modules M and N respectively, we have the following isomorphism

$$\gamma : \text{Hom}_S(U \otimes_R M, N) \cong \text{Hom}_R(M, \text{Hom}_S(U, N))$$

Proof. Consider a homomorphism $f \in \text{Hom}_S(U \otimes_R M, N)$. Then for all $m \in M$, we define $f_m : U \longrightarrow N$ by $f_m(u) = f(u \otimes m)$ for all $u \in U$. We then define $\gamma(f) : M \longrightarrow \text{Hom}_S(U, N)$ by $(\gamma(f))(m) = f_m$. We are now required to check that f_m is indeed in $\text{Hom}_S(U, N)$, that $\gamma(f)$ is an R-homomorphism and that γ is a group homomorphism. These calculations are routine and are omitted. It is also easy to show that γ is injective; surjectivity is shown by constructing an inverse for γ. The details involve further computations and are also omitted. □

Chapter 4

The Proposition

4.1 The Commutative Case

This section deals with the special case which arises when the Hopf algebra is commutative.

Lemma 4.1.1. *Let A be a commutative Hopf algebra and let B be a sub-Hopf algebra, such that both have bijective antipodes. Then A is faithfully flat over B.*

Proof. We note that A is a flat B-module via Lemma 2.3.7. Then by Lemma 2.3.4, it is also a faithfully flat B-module. $\square$

The following definition is needed for Theorem 4.1.2.

Definition 4.1.1. Let R be a ring as above. We say that R is *reduced* if R has no nonzero nilpotent elements.

Definition 4.1.2. Let A be a finitely generated algebra (not necessarily commutative) over an algebraically closed field $\mathbf{k}$. Then A is an *affine* $\mathbf{k}$-*algebra*.

The following theorem is taken from [Wat79, Theorem 11.4 and 11.6].

Theorem 4.1.2.

(1) Any commutative Hopf algebra H over a field of characteristic zero is reduced.

(2) Suppose H is commutative and affine over any field. Then it is reduced if and only if H is also smooth.

Proof.

(1) This is proved in [Wat79, Theorem 11.4].

(2) This is proved in [Wat79, Theorem 11.6].

□

4.2 Proof of the Proposition

Proposition 4.2.1. *Let* $\mathbf{k}$ *be an algebraically closed field, and let H be a Noetherian* $\mathbf{k}$*-Hopf algebra with a central (hence normal) affine sub-Hopf algebra K with Krull dimension m, such that H is a finite K-module. Then H as a module over K has finite injective dimension m.*

Proof.

(1) Claim: *For any ring $B \subset A$ which is a Frobenius extension, the left (right) injective dimension of A is bounded above by the left (right) injective dimension of B.*

The above claim was proved in [NT60], the first paper on general Frobenius extensions, and is essentially done by showing that $\mathrm{Ext}^i_A(-, A)$ and $\mathrm{Ext}^i_B(-, B)$ are equivalent functors on left A-modules. By Equation 3.1, in the case $i = 0$ this is reduced to showing that $\mathrm{Hom}_A(-, A)$ and $\mathrm{Hom}_B(-, B)$ are equivalent functors .

We thus consider the cases $i = 0$ and $i > 0$ separately. We begin with $i = 0$, since $i > 0$ follows from this case. Let M be a left A-module. Then

$$\begin{aligned} \mathrm{Hom}_A(M, A) &= \mathrm{Hom}_A(M, \mathrm{Hom}_B({}_BA, {}_BB)) \quad \text{since A is a Frobenius extension} \\ &\cong \mathrm{Hom}_B(A \otimes_A M, B) \quad \text{by Lemma 3.8} \\ &\cong \mathrm{Hom}_B(M, B) \quad \text{since M is a left A-module.} \end{aligned}$$

Therefore,

$$\mathrm{Hom}_A(-,A) = \mathrm{Hom}_B(-,B),$$

since M was chosen to be any left A-module.

Now let $i > 0$. Consider a left A-module M, and consider an A-projective resolution of M,

$$\cdots \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

For all left A-projective P_i, we claim that P_i is also left B-projective. Since ${}_AP_i$ is projective, it is a direct summand of a free left A module; say ${}_AF = {}_AP_i \oplus {}_AN$ for some right A-module N. But we may then consider both F and N as left B-modules. Clearly, F is a projective B-module since it is a direct sum of copies of the B-projective module A. So we get that ${}_BF = {}_BP_i \oplus {}_BN$; therefore P_i is also a left projective B-module.

So the projective resolution above is also a B-projective resolution for M. Then apply $\mathrm{Hom}_A(-,A)$ and $\mathrm{Hom}_B(-,B)$ to the resolution. But by the case for $i = 0$, we have that $\mathrm{Hom}_A(-,A) = \mathrm{Hom}_B(-,B)$. Then by definition of $\mathrm{Ext}^i_A(-,A)$, we have

$$\mathrm{Ext}^i_A(-,A) \approx \mathrm{Ext}^i_B(-,B), \quad \forall\, i \geq 0,$$

since M was chosen to be any left A-module. Now suppose that $\mathrm{inj.dim}(B) = m > 0$. By Theorem 3.5, $\mathrm{Ext}^i_B(-,B) = 0$ for all $i \geq m+1$, so $\mathrm{Ext}^i_A(-,A) = 0$, for all $i \geq m+1$. Thus A must have injective dimension equal to or less than m.

(2) Claim: *H is a Frobenius extension of K.* Since H is defined to be a Noetherian Hopf algebra, and K is a central sub-Hopf algebra, we may apply Theorem 2.3.9. Thus H is faithfully flat as an K-module. Define $\overline{H} = H/HK^+$. We now consider H as a right $\overline{H}$-comodule. By Remark 2.3.2, K is a normal sub-Hopf algebra. We may now apply Lemma 2.3.10, which gives that H is $\overline{H}$-Galois over K. Now, by Example 2.4.2, the set of integrals in $\overline{H}$, $I_{\overline{H}}$, is free since $\mathbf{k}$ is a field. Thus, by Theorem 2.4.3, H is a Frobenius extension over K.

(3) Claim: *K is a commutative affine $\mathbf{k}$-Hopf algebra, and is therefore Gorenstein.*

There are two possible situations to consider: $\mathrm{char}(\mathbf{k}) = 0$ and $\mathrm{char}(\mathbf{k}) = p > 0$.

When $\mathrm{char}(\mathbf{k}) = 0$, the case is trivial, since then by the first part of Theorem 4.1.2, the Hopf algebra is reduced. Applying the second part of Theorem 4.1.2 then gives that the Hopf algebra is smooth, hence Gorenstein.

Suppose now that $\mathrm{char}(\mathbf{k}) = p$ for some positive p. To prove this case, we first define the *Frobenius map* $K \longrightarrow K$ by $x \mapsto x^p$ for $x \in K$. We show that this is an algebra homomorphism by the argument below.

Let $K = \mathbf{k}\langle x_1, \cdots, x_t\rangle$ for some set of generators $\{x_1, \cdots, x_t\}$ of K. Let $P = \mathbf{k}[\hat{x}_1 \cdots, \hat{x}_t]$ be the polynomial algebra, so $K \cong P/I$ for some ideal I of P. Define a map

$$\phi : P \longrightarrow P, \quad \text{given by} \quad \hat{x}_i \mapsto (\hat{x}_i^p).$$

We extend this map linearly to P and in the obvious way to all monomials; that is, $\hat{x}_1^{r_1}, \cdots, \hat{x}_t^{r_t} \mapsto (\hat{x}_1^{r_1}, \cdots, \hat{x}_t^{r_t})^p$. To show that this is a $\mathbf{k}$-algebra homomorphism, we must show that it is a ring homomorphism and that $\phi : \mathbf{k} \longrightarrow \mathbf{k}$ is the identity. Let $\hat{x}_i, \hat{x}_j \in P$. Then

$$\phi(\hat{x}_i + \hat{x}_j) = (\hat{x}_i + \hat{x}_j)^p = (\hat{x}_i)^p + (\hat{x}_j)^p,$$

where the last equality holds since $\mathrm{char}(\mathbf{k}) = p$. The multiplicative condition is clear. It is also clear that $\phi(k) = k$ for all $k \in \mathbf{k}$. Finally, we prove that $\phi(I) \subseteq I$ for all ideals I. Let $\hat{y}_i \in I$. Then $\phi(\hat{y}_i) = \hat{y}_i^p$, which must be in I, since I is an ideal. Therefore, ϕ induces an algebra homomorphism on $P/I \cong K$. Thus the Frobenius map defined above is an algebra homomorphism.

We use this map to obtain a reduced sub-Hopf algebra of K and then use this to show that K has finite injective dimension. We do this by choosing $n \in \mathbb{N}$ such that the image C of K under the n^{th} power of the Frobenius map is reduced. Hence by the second part of Theorem 4.1.2, C is smooth. We now wish to apply the steps above to C, but to do this, we need to show that C is a sub-Hopf algebra of K.

Lemma 4.2.2. *Consider the Frobenius map $\sigma : K \longrightarrow K$, given by $\sigma(k) = k^p$. Choose $n \in \mathbb{N}$ such that $\sigma^n(K) = C$ has no nonzero nilpotent elements. Then C is a sub-Hopf algebra of K.*

Proof. To show that C is a sub-Hopf algebra, we need to show that

$$\begin{aligned} \Delta(C) &\subseteq C \otimes C \quad \text{and} \\ S(C) &\subseteq C. \end{aligned}$$

We note that for all $c \in C$, there exists $k \in K$ such that $k^{p^n} = c$. Thus $\Delta(c) = \Delta(k^{p^n})$. So we have

$$\begin{aligned} \Delta(c) &= \Delta(k)^{p^n} \\ &= (\sum k_1 \otimes k_2)^{p^n} \\ &= \sum k_1^{p^n} \otimes k_2^{p^n} \quad \text{because} \quad \mathrm{char}(\mathbf{k}) = p \end{aligned}$$

Clearly $\sum k_1^{p^n} \otimes k_2^{p^n} \in C \otimes C$. We know that $\Delta(k) \in K \otimes K$, so $\Delta(k)^{p^n} = \Delta(k^{p^n}) \in K^{p^n}$. Therefore, $\Delta(K^{p^n}) \subseteq K^{p^n}$, that is, $\Delta(C) \subseteq C$. Next we consider the condition for S.

Recall that S is an anti-algebra morphism, so $S(hk) = S(k)S(h)$ for all $h, k \in H$. As above, we let $c = k^{p^n}$. So we have

$$\begin{aligned} S(k^{p^n}) &= S(kk^{p^n-1}) \\ &= S(k^{p^n})S(k) \\ &= \underbrace{S(k)\cdots S(k)}_{p^n} \\ &= S(k)^{p^n}. \end{aligned}$$

Since K is a sub-Hopf algebra, $S(k) \in K$. Therefore, $(S(k))^{p^n} = S(k^{p^n}) \in K^{p^n}$. Thus $S(K^{p^n}) \subseteq K^{p^n}$, so $S(C) \subseteq C$ as required. So C is a sub-Hopf algebra of K. $\square$

We may now apply the results (1) and (2) above to show that K must be Gorenstein. We do this by showing that K is a Frobenius extension over C. Note first K is commutative, and so faithfully flat over C by Lemma 4.1.1. Commutativity also implies that $KC^+ = C^+K$; we then apply Lemma 2.1.5 to give that C is normal. So by (2) above, K is a Frobenius extension of C. Finally, we need to show that $\text{inj.dim}_K(K) = \text{inj.dim}_K(H)$. We have already shown that C is smooth, hence Gorenstein, and thus has finite injective dimension over itself. From (1) above we see that K must then have finite injective dimension as a module over itself and so is also Gorenstein.

(4) We are now in a position to prove that $\text{inj.dim}_K(H) = \text{inj.dim}_K(K)$. We first note that by Theorem 3.6, $\text{inj.dim}_K(K) = \text{Krull dim}(K)$. By steps (1) and (2) above, we have

$$\text{Krull dim}(K) = \text{inj.dim}_K(K) \geq \text{inj.dim}_H(H) \geq \text{inj.dim}_K(H). \tag{4.1}$$

H is a flat K-module, so $\text{inj.dim}_H(H) \geq \text{inj.dim}_K({}_KH)$, since the flatness of H implies that any injective H-module is also an injective K-module. By Theorem 2.4.2, H is a projective K-module. Also, since $K \subseteq H$, the identity map $i : H \longrightarrow K$ is onto. We may thus apply Proposition 3.2, which gives us that $H \cong \ker(i) \oplus K$. Clearly, $\ker(i)$ is a left and right K-module. Therefore, by Proposition 3.3, we must have

$$\text{inj.dim}_K(H) = \text{inj.dim}_K(K) = \text{Krull dim}(K) = m.$$

But then combining the equation above and Equation 4.1, we must have that

$$\text{inj.dim}_H(H) = \text{inj.dim}_K(H) = \text{Krull dim}(K) = m,$$

which proves the proposition.

$\square$

Bibliography

[Abe80] Eiichi Abe. *Hopf Algebras.* Cambridge University Press, 1980.

[Bas63] Hyman Bass. On the ubiquity of Gorenstein rings. *Mathematische Zeitschrift*, 82:8–28, 1963.

[BE90] J.-E. Bjork and E. K. Ekstrom. Filtered Auslander-Gorenstein rings. In *Colloque en l'Honneur de J. Dixmier*, pages 424–448. Birkhauser, Basel, 1990.

[Bea99] John A. Beachy. *Introductory Lectures on Rings and Modules*, volume 47 of *London Mathematical Society Student Texts.* Cambridge University Press, 1999.

[BF93] Allen D. Bell and Rolf Farnsteiner. On the theory of Frobenius extensions and its application to Lie superalgebras. *Transactions of the American Mathematical Society*, 335(1):407–424, 1993.

[BG98] K. A. Brown and K. R. Goodearl. Homological aspects of Noetherian PI Hopf algebras. *Journal of Algebra*, 198:240–265, 1998.

[Bjo89] J.-E. Bjork. The Auslander condition on Noetherian rings. In *Seminaire Dubreil-Malliavin*, volume 1404 of *Lecture Notes in Mathematics*, pages 137–173. Springer-Verlag, 1989.

[Bro98] Kenneth A. Brown. Representation theory of Noetherian Hopf algebras satisfying a polynomial identity. In *Trends in the Representation Theory of Finite-Dimensional Algebras*, volume 229 of *AMS Contemporary Mathematics*, pages 49–79. American Mathematical Society, 1998.

[Chi89] L. Childs. On the Hopf Galois theory for separable field extensions. *Communications in Algebra*, 17:809–825, 1989.

[DF99] David S. Dummit and Richard M. Foote. *Abstract Algebra.* Prentice Hall, 2nd edition, 1999.

[GL96] K. R. Goodearl and T. H. Lenagan. Catenarity in quantum algebras. *Journal of Pure and Applied Algebra*, 111:123–146, 1996.

[GP87] C. Greither and B. Paregis. Hopf Galois theory for separable field extensions. *Journal of Algebra*, 106:57–70, 1987.

[Isa94] I. Martin Isaacs. *Algebra: A Graduate Course.* Brooks/Cole Publishing Company, 1994.

[Kas95] Christian Kassel. *Quantum Groups.* Springer Verlag, 1995.

[KT81] H. F. Kreimer and M. Takeuchi. Hopf algebras and Galois extensions of an algebra. *Indiana University Mathematics Journal*, 30(5):675–692, 1981.

[Mon93] Susan Montgomery. *Hopf Algebras and Their Actions on Rings*, volume 82 of *Regional Conference Series in Mathematics.* American Mathematical Society, 1993.

[MW94] Akira Masuoka and David Wigner. Faithful flatness of Hopf algebras. *Journal of Algebra*, 170:156–164, 1994.

[NRZ89] W. D. Nichols and M. B. Richmond (Zoeller). A Hopf algebra freeness theorem. *American Journal of Mathematics*, 111:381–385, 1989.

[NRZ92] W. D. Nichols and M. B. Richmond (Zoeller). Freeness of infinite dimensional Hopf algebras. *Communications in Algebra*, 20(5):1489–1492, 1992.

[NT60] Tadasi Nakayama and Tosiro Tsuzuku. On Frobenius extensions I. *Nagoya Mathematics Journal*, 17:89–110, 1960.

[OS74] U. Oberst and H.-J. Schneider. Untergruppen formeller Gruppen von endlichen Index. *Journal of Algebra*, 31:10–44, 1974.

[Rei88] Miles Reid. *Undergraduate Algebraic Geometry*, volume 12 of *London Mathematical Society Student Texts.* Cambridge University Press, 1988.

[Rot79] Joseph J. Rotman. *Introduction to Homological Algebra*, volume 85 of *Pure and Applied Mathematics.* Academic Press, 1979.

[Sch92] Hans-Jürgen Schneider. Normal basis and transitivity of crossed products for Hopf algebras. *Journal of Algebra*, 152:289–312, 1992.

[Sch93] Hans-Jürgen Schneider. Some remarks on exact sequences of quantum groups. *Commmunications in Algebra*, 21(9):3337–3357, 1993.

[Swe69] Moss E. Sweedler. *Hopf Algebras.* W. A. Benjamin, Inc., 1969.

[SZ94] J. T. Stafford and J. J. Zhang. Homological properties of (graded) Noetherian PI rings. *Journal of Algebra*, 168:540–546, 1994.

[Taf71] E. J. Taft. The order of the antipode of a finite dimensional Hopf algebra. *Proceedings of the National Academy of Science*, 68:2631–2633, 1971.

[Tak72] M. Takeuchi. A correspondence between Hopf ideals and Sub-Hopf algebras. *Manuscripta Mathematica*, 7:251–270, 1972.

[Wat79] William C. Waterhouse. *Introduction to Affine Group Schemes*. Springer Verlag, 1979.