On finite-dimensional Hopf algebras and their classifications

Michael John Hilgemann
Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/etd

Part of the Mathematics Commons

Recommended Citation
https://lib.dr.iastate.edu/etd/11549

This Dissertation is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
On finite-dimensional Hopf algebras and their classifications

by

Michael John Hilgemann

A dissertation submitted to the graduate faculty
in partial fulfillment of the requirements for the degree of
DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:
Siu-Hung Ng, Major Professor
Ling Long
Jonathan Smith
Sung-yell Song
Stephen Willson

Iowa State University
Ames, Iowa
2010

Copyright © Michael John Hilgemann, 2010. All rights reserved.
DEDICATION

This thesis is dedicated to my parents, Marvin and Debby, for all the love and support.
# TABLE OF CONTENTS

## ABSTRACT

### CHAPTER 1. INTRODUCTION AND PRELIMINARIES

1. Introduction
2. Overview of Thesis
3. Finite-dimensional Algebras
   - 1.3.1 Associative Algebras
   - 1.3.2 Representation Theory of Associative Algebras
   - 1.3.3 Semisimplicity
   - 1.3.4 Frobenius Algebras

### CHAPTER 2. THE THEORY OF HOPF ALGEBRAS

2.1 Coalgebra Theory
   - 2.1.1 Coalgebras
   - 2.1.2 Duality Between Algebras and Coalgebras
2.1.3 Comodules
2.2 Hopf Algebras
   - 2.2.1 Bialgebras
   - 2.2.2 Hopf Algebras
2.2.3 Representation Theory of Hopf Algebras
2.3 Further Hopf Algebra Theory
   - 2.3.1 Integrals
   - 2.3.2 Semisimplicity of Hopf Algebras
   - 2.3.3 The Nichols-Zoeller Theorem
2.3.4 Extensions of Hopf Algebras ........................................... 63
2.3.5 Biproducts ................................................................. 67

CHAPTER 3. CLASSIFICATIONS OF FINITE-DIMENSIONAL HOPF ALGEBRAS ........................................... 70
3.1 Introduction ................................................................. 70
3.2 Hopf Algebras of Dimension $p$ .......................................... 71
3.3 Hopf Algebras of Dimension $p^2$ ....................................... 73
3.4 Hopf Algebras of Dimension $pq$ ........................................ 74
3.5 Hopf Algebras of Dimension $pqr$ ...................................... 76

CHAPTER 4. NON-SEMISIMPLE HOPF ALGEBRAS OF DIMENSION 2$p^2$ ......................................................... 83
4.1 Preliminaries ................................................................. 83
4.2 The Order of the Antipode ............................................... 92
4.3 Non-semisimple Hopf Algebras of Dimension 2$p^2$ ................. 98

CHAPTER 5. CONCLUSION AND FURTHER WORK .................. 103
5.1 Conclusion ................................................................. 103
5.2 Further Work .............................................................. 104

APPENDIX ................................................................. 107

BIBLIOGRAPHY ........................................................... 110

ACKNOWLEDGEMENTS .................................................. 116
ABSTRACT

In this thesis, we investigate the classification problem for finite-dimensional Hopf algebras. If \( p \) is an odd prime, we show that a non-semisimple Hopf algebra of dimension \( 2p^2 \) over an algebraically closed field of characteristic zero must be pointed or isomorphic to the dual of a pointed Hopf algebra. Based on previously established classification results, this completes the classification of Hopf algebras of these dimensions.
CHAPTER 1. INTRODUCTION AND PRELIMINARIES

1.1 Introduction

The concept of a Hopf algebra arose in the 1940’s in relation to the work of Heinz Hopf in algebraic topology and cohomology [22]. They also appeared, in some sense, in the theory of algebraic groups in the various works of Dieudonné, Cartier, and Hochschild. Beginning with the work of Milnor and Moore [36], a general theory of Hopf algebras was then developed in the 1960’s and 1970’s continuing in the works of Larson, Radford, Sweedler, Taft, and Wilson, among others. The first book on the subject of Hopf algebra was written by Sweedler and published in 1969 [59]. Later, these algebraic objects took on a prominent role in the theory of quantum groups that became popular in the 1980’s and early 1990’s, when Drinfel’d [14] won the Fields Medal for his contributions to the area. Hopf algebras now play an important role in many areas of mathematics and are linked with such topics as Lie algebras, Galois theory, knot theory, conformal field theory, quantum mechanics, tensor categories, and combinatorics, among others. The algebraic foundations of Hopf algebras have been greatly developed over the past decades, and the problem of classifying Hopf algebras has garnered many interesting results. For more information on the beginning history of Hopf algebras, see the survey of Andruskiewitsch and Ferrer [3].

As algebraic objects, Hopf algebras can be thought of as generalizations or linearizations of groups. Briefly, a Hopf algebra is a vector space over a field $k$ equipped with linear structure maps that mimic many of the fundamental aspects of groups. In particular, every finite-dimensional Hopf algebra $H$ is an associative algebra which has a linear operator $S$ called an antipode, which generalizes the group inverse operation. In fact, the group algebra $k[G]$ of any group $G$ is a Hopf algebra with multiplication induced by the group product and an antipode...
induced by the group inverse operation.

The concept of duality is very important in the study of finite-dimensional Hopf algebras. A Hopf algebra is not only an associative algebra, but it is also a coassociative coalgebra, which is a concept dual to that of an algebra in the sense of category theory. That is, if we define the concept of an algebra using commutative diagrams, then the defining diagrams of a coalgebra will be the same but with all arrows reversed. The main defining linear structures of a coalgebra $C$ are a comultiplication map, often denoted by $\Delta : C \to C \otimes C$, and a counit map $\epsilon : C \to \mathbb{k}$. A Hopf algebra is both an algebra and a coalgebra in which the structure maps satisfy a certain compatibility condition. Due to this dual nature, the linear dual $H^*$ of any finite-dimensional Hopf algebra $H$ is also a Hopf algebra.

The similarity between groups and Hopf algebras is demonstrated in some important properties shared by both types of algebraic structures and their representations. The category of modules or representations of a Hopf algebra is very similar to the category of representations of a group. If $V$ and $W$ are left modules of the group $G$, then both the tensor product $V \otimes W$ and the linear dual $V^*$ are left modules of $G$. To form the action of $G$ on $V \otimes W$, one employs the diagonal map $\Delta : G \to G \times G$ defined by $\Delta(g) = (g, g)$ for all $g \in G$, and to define the action of $G$ on $V^*$, one employs the group inverse operation. In a similar way, if $H$ is a Hopf algebra, then the comultiplication $\Delta$ of the coalgebra structure of $H$ can be used to turn the tensor product $V \otimes W$ of two left $H$-modules $V$ and $W$ into another left $H$-module, and, if $V_1$, $V_2$, and $V_3$ are three $H$-modules, the coassociativity of $\Delta$ implies that $(V_1 \otimes V_2) \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3)$ as $H$-modules. Moreover the antipode $S$ can be used to turn $V^*$ into another left $H$-module and the counit $\epsilon$ of $H$ defines a trivial representation on the base field $\mathbb{k}$.

Other familiar properties of finite groups appear as generalized results on finite-dimensional Hopf algebras. For example, the Lagrange Theorem for finite groups states that the order of a subgroup $H$ of a finite group $G$ divides the order of the group $G$. The corresponding result for finite-dimensional Hopf algebras, known as the Nichols-Zoeller Theorem [45], implies that the dimension of a Hopf subalgebra always divides the dimension of the larger Hopf algebra. A few other notable properties of finite groups which generalize to finite-dimensional Hopf
algebras will be discussed in this thesis, including notions related to normal Hopf subalgebras and extensions of Hopf algebras. Both of these generalize the corresponding definitions in group theory and have properties similar to the group case.

In 1975, Kaplansky [24] published a list of 10 unsolved conjectures dealing with Hopf algebras. Among this list was the conjecture that every Hopf algebra over an algebraically closed field of characteristic zero of prime dimension must be isomorphic to a group algebra. Also appearing was the conjecture that there is a finite number of isomorphism classes of Hopf algebras of a given finite dimension. The first conjecture, proven by Zhu [62] and published in 1994, began the program of trying to classify finite-dimensional Hopf algebras based on the prime decomposition of their dimensions. However, the second conjecture was proven false. In the case that $p$ is an odd prime, it has been shown that there exist infinitely many isomorphism classes of Hopf algebras of dimension $p^4$ (see [6], [7], and [19]). Despite this negative result, there is a general push to classify all Hopf algebras over an algebraically closed field of characteristic zero whose dimensions are a product of just a few primes.

As mentioned above, the classification of Hopf algebras of prime dimension $p$ has been completed, and all of these Hopf algebras are isomorphic to the group algebra of the cyclic group of order $p$. Further results have completed the classification of Hopf algebras of dimension $p^2$ for $p$ a prime (see [35] and [41]), and Hopf algebras of dimension $2p$ for $p$ an odd prime (see [33] and [43]). It has further been shown by Gelaki and Westreich [20] and by Etingof and Gelaki [15] that semisimple Hopf algebras of dimension $pq$ over such a field are trivial, for $p$ and $q$ distinct odd primes. That is, such Hopf algebras are isomorphic to group algebras or the duals of group algebras. However, the non-semisimple case has not yet been completed. There is strong evidence to support a claim that there exists no non-semisimple Hopf algebra of dimension $pq$ over an algebraically closed field of characteristic zero (see [16], [39], and [44]).

The work that has been done in classifying Hopf algebras with dimensions a product of one or two primes has laid significant groundwork for the study of Hopf algebras over an algebraically closed field of characteristic zero with dimensions a product of three primes. In particular, there has been significant work done on classifying Hopf algebras of dimension
$p^3$ for $p$ a prime and Hopf algebras of dimension $2p^2$ where $p$ is an odd prime. In both of these cases, the semisimple Hopf algebras of these dimensions and those non-semisimple Hopf algebras which possess a property known as being \textit{pointed} have been completely classified. In this thesis, we shall complete the classification of Hopf algebras over an algebraically closed field of characteristic zero of dimension $2p^2$, where $p$ is an odd prime, by showing that such a Hopf algebra is either pointed or isomorphic to the dual of such a pointed Hopf algebra. We will also comment on other classifications which still remain open, such as the classification of Hopf algebras of dimension $p^3$ for $p$ a prime.

1.2 Overview of Thesis

In the remainder of this chapter, we shall review some basic terminology, notation, and results dealing with finite-dimensional associative algebras and their representations. We will also discuss results dealing with semisimple algebras and Frobenius algebras that will be used in this thesis.

In the second chapter, we shall review an extensive amount of background material related to the study of Hopf algebras. In the first section, we give an outline of basic definitions and theory related to coalgebras, and then proceed into the study of bialgebras, Hopf algebras, and their representations in the second section. The third section deals with further theory involving Hopf algebras that is vital to the study of finite-dimensional Hopf algebras and their classifications, which includes the study of integrals, semisimple Hopf algebras, the Nichols-Zoeller Theorem, and extensions of Hopf algebras.

In the third chapter, we shall give a brief overview of the completed results in the classification of finite-dimensional Hopf algebras based on the decomposition of the dimension into a product of primes. The classification of finite-dimensional Hopf algebras is generally broken into two cases: semisimple and non-semisimple Hopf algebras. We outline the completed classifications and those which have yet to be completed. In particular, we give a complete classification of Hopf algebras over an algebraically closed field of characteristic zero whose dimensions are $p$, $p^2$, or $2p$ for a prime $p$, as well as the complete classification of semisimple
Hopf algebras of dimensions $pq$, $p^3$ and $2p^2$ for primes $p$ and $q$. Lastly we detail the completed classification of non-semisimple pointed Hopf algebras of dimension $p^3$ and $2p^2$, for $p$ an odd prime.

In the fourth chapter, we focus on the study of non-semisimple Hopf algebras of dimension $2p^2$ over an algebraically closed field of characteristic zero, where $p$ is an odd prime. We begin by proving some general results on finite-dimensional Hopf algebras and extensions of such Hopf algebras. In the second section, we then show that the antipode of any such Hopf algebra has order $2p$. Lastly, we use this fact to show that any non-semisimple Hopf algebra of dimension $2p^2$ has the property that it is either pointed or dual to a pointed Hopf algebra. This completes the classification of Hopf algebras of such dimensions.

Lastly, in the fifth chapter, we will give a brief summary of the implications of the main result as well as an overview of further study related to the classification of finite-dimensional Hopf algebras. In particular, we detail known results dealing with the classification of non-semisimple Hopf algebras of dimension $p^3$, for $p$ a prime, which is still incomplete, and we comment on other possible directions for future research.

Throughout this thesis, we shall denote by $k$ a field and any unadorned tensor product $\otimes$ shall be considered to be over $k$ unless otherwise stated. We will use the notation $\dim V$ for the dimension of a vector space $V$ over its field $k$ and denote by $\text{End}(V) = \text{End}_k(V)$ the set of linear endomorphisms of the vector space $V$ over $k$. If $\phi \in \text{End}(V)$, then we denote by $\text{Tr}(\phi)$ the trace of $\phi$. If $V$ is a vector space, we shall for convenience identify

\[ k \otimes V \cong V \cong V \otimes k \]

using the obvious identification

\[ k \otimes v = kv = v \otimes k \]

for all $k \in k$ and $v \in V$. 
1.3 Finite-dimensional Algebras

We first quickly review some basics of associative algebras and their representations and establish notation that shall be used throughout this thesis. We also discuss the notions and major results of projective modules, semisimple algebras, and Frobenius algebras that will be needed in the remainder of this work. These well-known results can be found in the books by Curtis and Reiner [11], Lam [28, 27], and Pierce [47], which are standard works in the theory of algebras and their representations.

1.3.1 Associative Algebras

We begin with the definition of an associative algebra over the field $k$.

**Definition 1.3.1.** Let $A$ be a vector space over $k$. Then $A$ is a $k$-algebra (or algebra over $k$) if there exist linear maps $M : A \otimes A \to A$, called the multiplication, and $u : k \to A$, called the unit, such that the diagrams of linear maps commute.

We will denote the image of the element $a \otimes b$ under the multiplication map $M$ by

$$M(a \otimes b) = ab$$

for all $a, b \in A$, and we denote by $u(1) = 1_A$ the multiplicative identity of $A$. The first commutative diagram implies that

$$a(bc) = (ab)c$$

for all $a, b, c \in A$, a property referred to as the associativity of $A$. The second and third commutative diagrams imply that $1_A a = a = a 1_A$ for all $a \in A$. 
Given two algebras $A$ and $B$ over $k$, a linear map $f : A \to B$ is called an **algebra homomorphism** if the diagrams commute. That is, $f : A \to B$ is an algebra homomorphism if

$$f(ab) = f(a)f(b) \quad \text{and} \quad f(1_A) = 1_B$$

for all $a, b \in A$. If $A$ and $B$ are two algebras over $k$ such that there exists a bijective algebra homomorphism between them, then we say that $A$ is isomorphic to $B$ as algebras. We denote this by $A \cong B$ when the context is clear.

A linear subspace $B$ of an algebra $A$ is called a **subalgebra** of $A$ if $ab \in B$ for all $a, b \in B$ and $1_A \in B$. A subspace $I$ of $A$ is called a **left ideal** of $A$ if $ab \in I$ for all $a \in A$ and $b \in I$, and similarly, $I$ is called a **right ideal** of $A$ if $ba \in I$ for all $a \in A$ and $b \in I$. If $I$ is both a left and right ideal of $A$, then $I$ is simply referred to as an **ideal** of $A$. In this case, we can define an algebra structure on the quotient vector space $A/I$ by defining

$$(a + I)(b + I) = ab + I \quad \text{and} \quad 1_{A/I} = 1_A + I$$

for all $a, b \in A$. We refer to the algebra $A/I$ as the quotient algebra of $A$ with respect to $I$. Moreover, the canonical surjection $\pi : A \to A/I$ defined by

$$\pi(a) = a + I$$

for all $a \in A$ is an algebra homomorphism. We say that an algebra $A$ is **simple** if its only ideals are $A$ and $\{0\}$.

**Example 1.3.2.** The field $k$ is an algebra over itself using the trivial multiplication and unit maps defined by

$$M(1 \otimes 1) = 1 \text{ and } u(1) = 1$$

and extended linearly. We often refer to $k$ as the trivial algebra.
Example 1.3.3. Given two algebras $A$ and $B$ over the same field $k$, we can define an algebra structure on the tensor product $A \otimes B$ referred to as the tensor product algebra of $A$ and $B$. The multiplication is given by

$$M ((a_1 \otimes b_1) \otimes (a_2 \otimes b_2)) = a_1 a_2 \otimes b_1 b_2$$

for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$. The multiplicative unit of $A \otimes B$ is $1_A \otimes 1_B$.

An algebra $A$ over $k$ is called **commutative** if $ab = ba$ for all $a, b \in A$. This is equivalent to the commutativity of the diagram

\[
\begin{array}{ccc}
A \otimes A & \xrightarrow{M} & A \\
\downarrow{\tau} & & \downarrow{M} \\
A \otimes A & & 
\end{array}
\]

where $\tau : A \otimes A \to A \otimes A$ is the linear ‘twist’ map given by

$$\tau(a \otimes b) = b \otimes a$$

for all $a, b \in A$.

Example 1.3.4. Let $n$ be a positive integer. Then the vector space $M_n(k)$ of all $n \times n$ matrices over $k$ is an $n^2$-dimensional non-commutative algebra over $k$ with the usual matrix multiplication and matrix identity element $I$. It is a standard result that $M_n(k)$ is a simple algebra.

Similarly, given an $n$-dimensional vector space $V$ over $k$, the set $\text{End}(V)$ of linear operators of $V$ is an algebra over $k$. The multiplication is function composition and the multiplicative identity is the identity map. The algebra $\text{End}(V)$ is isomorphic to the matrix algebra $M_n(k)$.

1.3.2 Representation Theory of Associative Algebras

We next review some basics of the representation theory of associative algebras, including characters, simple modules, indecomposable modules, and projective modules.

**Definition 1.3.5.** Let $A$ be an algebra over $k$. Then an algebra homomorphism

$$\rho : A \to \text{End}(V)$$
for some finite-dimensional vector space $V$ over $k$ is called a representation of $A$. The dimension $n$ of $V$ is referred to as the degree of the representation $\rho$.

For the most part, we shall adopt the viewpoint of modules over an algebra in place of representations. The two concepts are equivalent.

**Definition 1.3.6.** Let $A$ be an algebra over $k$ and let $V$ be a finite-dimensional vector space over $k$. We call $V$ a **left $A$-module** if there exists a linear map $\mu : A \otimes V \to V$ such that the diagrams

$$
\begin{array}{ccc}
A \otimes A \otimes V & \xrightarrow{id \otimes \mu} & A \otimes V \\
M \otimes \text{id} & \downarrow & \downarrow \mu \\
A \otimes V & \xrightarrow{\mu} & V
\end{array}
\text{ and }
\begin{array}{ccc}
k \otimes V & \xrightarrow{n \otimes \text{id}} & A \otimes V \\
\text{id} & \downarrow & \downarrow \mu \\
V & \xrightarrow{\mu} & V
\end{array}
$$

of linear maps commute.

Similarly, we call $V$ a **right $A$-module** if there exists a linear map $\mu : V \otimes A \to V$ such that the diagrams

$$
\begin{array}{ccc}
V \otimes A \otimes A & \xrightarrow{\mu \otimes \text{id}} & V \otimes A \\
\text{id} \otimes M & \downarrow & \downarrow \mu \\
V \otimes A & \xrightarrow{\mu} & V
\end{array}
\text{ and }
\begin{array}{ccc}
V \otimes k & \xrightarrow{\text{id} \otimes u} & V \otimes A \\
\text{id} & \downarrow & \downarrow \mu \\
V & \xrightarrow{\mu} & V
\end{array}
$$

commute.

Most often, given a left $A$-module $V$, we shall denote the image of $a \otimes v$ under $\mu$ by

$$
\mu(a \otimes v) = a \cdot v
$$

with similar notation used for right $A$-modules. In particular, for a left $A$-module $V$, the commutative diagrams above translate to

$$
a \cdot (b \cdot v) = ab \cdot v \quad \text{and} \quad 1_A \cdot v = v
$$

for all $a, b \in A$ and $v \in V$.

Giving a left or right $A$-module is equivalent to defining a representation of the algebra $A$. Specifically, if $V$ is a (left) $A$-module, then we can define $\rho : A \to \text{End}(V)$ by

$$
\rho(a)(v) = a \cdot v
$$
for all $a \in A$ and $v \in V$. Also, given a representation $\rho : A \to \text{End}(V)$, the vector space $V$ is a (left) $A$-module by defining

$$a \cdot v = \rho(a)(v)$$

for all $a \in A$ and $v \in V$.

If $\rho : A \to \text{End}(V)$ is a representation of $A$, then the map $\chi_\rho : A \to k$ defined by

$$\chi_\rho(a) = \text{Tr}(\rho(a))$$

for all $a \in A$ is called the character of the representation $\rho$. Similarly, if the representation $\rho$ affords the $A$-module $V$, then we say that $\chi_V = \chi_\rho$ is the character associated to the $A$-module $V$.

Assume that $V$ and $W$ are two left $A$-modules, with actions $\mu_V$ and $\mu_W$, respectively. A linear map $f : V \to W$ is called a left module homomorphism if the diagram

$$
\begin{array}{ccc}
A \otimes V & \xrightarrow{id \otimes f} & A \otimes W \\
\mu_V \downarrow & & \downarrow \mu_W \\
V & \xrightarrow{f} & W
\end{array}
$$

commutes. That is, $f : V \to W$ is a module homomorphism if

$$f(a \cdot v) = a \cdot f(v)$$

for all $a \in A$ and $v \in V$. A similar definition can be given for a right module homomorphism.

**Example 1.3.7.** Let $A$ be a finite-dimensional algebra over $k$. Then $A$ itself is both a left and right $A$-module using the multiplication of $A$ as the action. When necessary, we denote this left $A$-module by $AA$, which is called the regular representation of $A$.

If $V$ is a vector space and $n$ is a positive integer, denote by $nV$ the vector space

$$nV = V \oplus V \oplus \cdots \oplus V$$

which is a direct sum of $n$ copies of $V$. If $A$ is a finite-dimensional algebra and $V$ is a finite-dimensional $A$-module, then we say that $V$ is a free $A$-module if

$$V \cong nA$$
for some positive integer $n$. Note that the action of $A$ on $nA$ is given by

$$a \cdot (a_1, a_2, \cdots, a_n) = (aa_1, aa_2, \cdots, aa_n)$$

for all $a, a_1, a_2, \cdots, a_n \in A$. It is obvious that if $A$ is a finite-dimensional algebra and $V$ is a finite-dimensional free $A$-module, then $\dim A$ divides $\dim V$.

Given an $A$-module $V$, a subspace $W$ of $V$ is called a **submodule** of $V$ if $a \cdot w \in W$ for all $a \in A$ and $w \in W$. In this case, $W$ is itself an $A$-module where the action is simply the restriction of the action $\mu : A \otimes V \to V$ to $A \otimes W$. We say that an $A$-module $V$ is **irreducible** or **simple** if it contains no submodules other than $V$ and $\{0\}$. If $V$ is a simple $A$-module, then the character $\chi$ associated to $V$ is called an irreducible character.

Let $k$ be an algebraically closed field and $A$ an algebra over $k$, with $V$ and $W$ finite-dimensional irreducible $A$-modules. By Schur’s Lemma, we have that the space $\text{Hom}_A(V, W)$ of $A$-module homomorphisms from $V$ to $W$ has dimension either 0 or 1, depending on whether $V \not\cong W$ or $V \cong W$, respectively.

For an $A$-module $V$, we define the **socle** $\text{Soc}(V)$ of $V$ to be the sum of all simple submodules of $V$. For a finite-dimensional algebra $A$ and an $A$-module $V$, we denote by $[V]$ the isomorphism class of all $A$-modules isomorphic to $V$. We also denote by $\text{Irr}(A)$ the set of all isomorphism classes of irreducible $A$-modules. An important fact about any finite-dimensional algebra $A$ over $k$ is that the set $\text{Irr}(A)$ is finite.

Let $A$ be an algebra over $k$ and let $V$ be an $A$-module. We say that $V$ is **indecomposable** if whenever we can write

$$V \cong W_1 \oplus W_2$$

for submodules $W_1$ and $W_2$ of $V$, then either $W_1 \cong 0$ or $W_2 \cong 0$. Clearly any simple $A$-module is indecomposable. Note also that any finite-dimensional $A$-module $V$ can be decomposed as a direct sum of indecomposable $A$-modules. By the Krull-Schmidt Theorem, this decomposition is unique up to isomorphism and the ordering of the indecomposable factors.

Let $A$ be a finite-dimensional algebra over $k$ and let

$$A A = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$
be a decomposition of the regular representation $AA$ of $A$ into indecomposable $A$-modules. Then each indecomposable module $V_i$ is called a principal indecomposable $A$-module. Again, these modules are uniquely determined up to isomorphism and up to ordering of the decomposition.

Let $A$ be an algebra over $\mathbb{k}$. We say that $e \in A$ is an idempotent if $e^2 = e$. We say that two idempotents $e_1, e_2 \in A$ are orthogonal if $e_1e_2 = e_2e_1 = 0$. We call an idempotent $e \in A$ a primitive idempotent if whenever $e = e_1 + e_2$ for two orthogonal idempotents $e_1, e_2 \in A$, then either $e_1 = 0$ or $e_2 = 0$. We note if $e \in A$ is an idempotent, then $e$ is a primitive idempotent if and only if $Ae$ is an indecomposable left $A$-module (or equivalently, $eA$ is an indecomposable right $A$-module). Thus every principal indecomposable left $A$-module is isomorphic to $Ae$ for some primitive idempotent $e \in A$, and if

$$1 = e_1 + e_2 + \cdots + e_n$$

is a sum of primitive idempotents $e_1, e_2, \cdots, e_n \in A$, then

$$AA = Ae_1 \oplus Ae_2 \oplus \cdots \oplus Ae_n$$

is the decomposition of the regular $A$-module $AA$ into principal indecomposable $A$-modules.

An $A$-module $P$ is projective if whenever we have a module homomorphism $\phi : P \to V$ and a surjective module homomorphism $\pi : W \to V$ there exists a module homomorphism $f : P \to W$ such that $f \circ \pi = \phi$. In other words, there exists a module homomorphism $f : P \to W$ such that the diagram

$$\begin{array}{ccc}
P & \xrightarrow{\phi} & V \\
\downarrow{f} & & \downarrow{\pi} \\
W & \rightarrow & V \\
\end{array}$$

commutes. It is well-known that $P$ is a projective $A$-module if and only if $P$ is isomorphic to a direct summand of a free $A$-module. In particular, every principal indecomposable $A$-module $V$ is projective. Moreover, for a finite-dimensional algebra $A$, $P$ is projective if and only if $P$ is isomorphic to a direct sum of principal indecomposable modules of $A$. 
If $A$ is an algebra and $V$ is an $A$-module, following Lam’s definition in [28, Definition 24.9] we say that the module $P$ is a **projective cover** of $V$ if $P$ is a projective module and there exists a surjective module homomorphism

$$\theta : P \to V$$

such that if $Q$ is any submodule of $P$ such that $\theta(Q) = V$, then $Q = P$. If such a projective cover exists, it is unique up to isomorphism, and we therefore denote by $P(V)$ the projective cover of the module $V$. If $A$ is a finite-dimensional algebra over a field $k$, then every finite-dimensional $A$-module has a projective cover.

Dual to the notion of a projective module is that of an injective module. An $A$-module $Q$ is **injective** if whenever we have a module homomorphism $\phi : V \to Q$ and an injective module homomorphism $\iota : V \to W$ there exists a module homomorphism $f : W \to Q$ such that $f \circ \iota = \phi$. In other words, there exists a module homomorphism $f : W \to Q$ such that the diagram

$$
\begin{array}{ccc}
0 & \to & V \\
& \downarrow{\phi} & \downarrow{f} \\
& W & \to & Q
\end{array}
$$

commutes.

### 1.3.3 Semisimplicity

Let $A$ be a finite-dimensional algebra over $k$. An ideal $I$ of $A$ is called **nilpotent** if $I^m = 0$ for some positive integer $m$. We define the **Jacobson radical** $J(A)$ of $A$ to be the sum of all nilpotent left ideals of $A$. Equivalently, $J(A)$ is the sum of all nilpotent right ideals of $A$. We have that $J(A)$ is an ideal of $A$ and $J(A/J(A)) = 0$.

We say that the finite-dimensional algebra $A$ over the algebraically closed field $k$ of characteristic zero is **semisimple** if it satisfies any of the following equivalent conditions:

1. $J(A) = 0$;
2. A is direct product of matrix algebras over \( k \). That is, there exist positive integers \( t, n_1, n_2, \ldots, n_t \) such that

\[
A \cong M_{n_1}(k) \times M_{n_2}(k) \times \cdots \times M_{n_t}(k)
\]
as algebras;

3. Any \( A \)-module \( V \) is completely reducible. That is, for any submodule \( W_0 \) of \( V \), there exists a submodule \( W_1 \) of \( V \) such that

\[
V \cong W_0 \oplus W_1
\]
as modules.

If \( A \) is a semisimple algebra over \( k \), then any \( A \)-module \( V \) is a direct sum

\[
V \cong W_1 \oplus W_2 \oplus \cdots \oplus W_n
\]
of simple \( A \)-modules \([W_1],[W_2], \ldots, [W_n]\) \( \in \text{Irr}(A) \), which are unique up to isomorphism and the ordering of the modules. Moreover, if \( A \) is a semisimple algebra then the indecomposable \( A \)-modules are exactly the irreducible \( A \)-modules, and so every \( A \)-module is isomorphic to a direct sum of principal indecomposable \( A \)-modules, and every \( A \)-module is projective.

### 1.3.4 Frobenius Algebras

Next we briefly discuss a class of algebras which contains the class of finite-dimensional Hopf algebras. Let \( A \) be a finite-dimensional algebra over \( k \). We say that \( A \) is a Frobenius algebra if there exists a non-degenerate bilinear form \( \beta : A \times A \to k \) which is associative in the sense that

\[
\beta(ab, c) = \beta(a, bc)
\]
for all \( a, b, c \in A \).

As is well-known, if \( A \) is a finite-dimensional Frobenius algebra, then an \( A \)-module \( V \) is projective if and only if \( V \) is injective. Also, we have a nice decomposition of \( A \) into principal indecomposable modules. By [11, Section 61], if \( A \) is a finite-dimensional Frobenius algebra
over the algebraically closed field $\mathbb{k}$ and $V$ is an irreducible $A$-module, then the number of times that the principal indecomposable module $P(V)$ appears as a component of $AA$ is $\dim V$. That is

\[
AA \cong \bigoplus_{[V] \in \text{Irr}(A)} (\dim V) \cdot P(V)
\]
as modules. As an important consequence,

\[
\dim A = \sum_{[V] \in \text{Irr}(A)} (\dim V)(\dim P(V)).
\]
CHAPTER 2. THE THEORY OF HOPF ALGEBRAS

2.1 Coalgebra Theory

2.1.1 Coalgebras

We define first the fundamental notion of a coalgebra, which is dual to that of an algebra over a field in the sense that if we reverse all the arrows in the defining diagrams of an algebra, we get the concept of a coalgebra. Standard references for the basic theory of coalgebras and comodules, as well as Hopf algebras, can be found in [1], [12], [25], [37], [54], and [59]. These results can be found in some or all of these references.

Definition 2.1.1. Let $C$ be a vector space over the field $k$. Then $C$ is a coalgebra over $k$ if there exist $k$-linear maps

$$ \Delta : C \to C \otimes C \quad \text{and} \quad \epsilon : C \to k $$

such that the diagrams

$$ C \xrightarrow{\Delta} C \otimes C \xrightarrow{\Delta \otimes \text{id}} (C \otimes C) \otimes (C \otimes C) $$

$$ C \otimes C \xrightarrow{\text{id} \otimes \Delta} (C \otimes C) \otimes C $$

$$ C \otimes C \xrightarrow{\text{id} \otimes \epsilon} C \otimes k $$

of linear maps commute.

That is, $C$ is a coalgebra if

$$ (\Delta \otimes \text{id}_C) \Delta(c) = (\text{id}_C \otimes \Delta) \Delta(c) \quad (2.1) $$

and

$$ (\epsilon \otimes \text{id}_C) \Delta(c) = c = (\text{id}_C \otimes \epsilon) \Delta(c) \quad (2.2) $$
for all $c \in C$, where we have identified

$$k \otimes C = C = C \otimes k$$

as stated previously. We call $\Delta$ the *comultiplication* and $\epsilon$ the *counit* of the coalgebra $C$, and equation (2.1) is referred to as the coassociativity of the coalgebra. In addition, we will refer to equation (2.2) as the counit property of the coalgebra. To avoid confusion, we will sometimes refer to the coalgebra $C$ as the triple $(C, \Delta, \epsilon)$. However, if the comultiplication and counit are understood, we will often just denote the coalgebra $(C, \Delta, \epsilon)$ by $C$.

Given two coalgebras $(C, \Delta_C, \epsilon_C)$ and $(D, \Delta_D, \epsilon_D)$ over the field $k$, a linear map $f : C \to D$ is called a **coalgebra homomorphism** (or coalgebra map) if the diagrams

$$
\begin{array}{ccc}
C & \xrightarrow{\Delta_C} & C \otimes C \\
\downarrow{f} & & \downarrow{f \otimes f} \\
D & \xrightarrow{\Delta_D} & D \otimes D
\end{array}
\quad
\begin{array}{ccc}
C & \xrightarrow{f} & D \\
\downarrow{\epsilon_C} & & \downarrow{\epsilon_D} \\
k & \searrow{\epsilon_D}
\end{array}
$$

commute.

That is, $f : C \to D$ is a coalgebra homomorphism if

$$(f \otimes f)(\Delta_C(c)) = \Delta_D(f(c)) \quad \text{and} \quad \epsilon_D(f(c)) = \epsilon_C(c)$$

(2.3)

for all $c \in C$. We say that a coalgebra $(C, \Delta_C, \epsilon_C)$ is isomorphic to a coalgebra $(D, \Delta_D, \epsilon_D)$ if there exists a bijective coalgebra homomorphism $f : C \to D$, and we denote this by $C \cong D$ when the context is clear.

If $(C, \Delta, \epsilon)$ is a coalgebra and $D$ is a vector subspace of $C$, then we say that $D$ is a **subcoalgebra** if $\Delta(D) \subseteq D \otimes D$. In this case, $(D, \Delta|_D, \epsilon|_D)$ is a coalgebra contained in the coalgebra $(C, \Delta, \epsilon)$.

Dual to the notion of a commutative algebra, a coalgebra $(C, \Delta, \epsilon)$ is called **cocommutative** if $\tau \circ \Delta = \Delta$, where $\tau : C \otimes C \to C \otimes C$ is the linear ‘twist’ map defined by

$$\tau(c \otimes d) = d \otimes c$$
for all \(c, d \in C\).

With the above definitions, we have the category \(k\)-Coalg whose objects are coalgebras over \(k\) and whose morphisms are the collections \(\text{Hom}_{\text{Coalg}}(C, D)\) of coalgebra homomorphisms between the objects \(C, D \in k\)-Coalg. We next give a few basic examples of coalgebras.

**Example 2.1.2.** The ground field \(k\) is a coalgebra by defining
\[
\Delta(1) = 1 \otimes 1 \quad \text{and} \quad \epsilon(1) = 1
\]
and extended linearly to all of \(k\).

**Example 2.1.3.** Let \(S\) be any non-empty set, and define \(k[S]\) to be the \(k\)-vector space with the canonical basis \(S\). Then by defining
\[
\Delta(s) = s \otimes s \quad \text{and} \quad \epsilon(s) = 1
\]
for all \(s \in S\), we have a cocommutative coalgebra \((k[S], \Delta, \epsilon)\) by extending \(\Delta\) and \(\epsilon\) linearly to all of \(k[S]\). Note that the dimension of the coalgebra \(k[S]\) is just the cardinality of the set \(S\).

**Remark 2.1.4.** It is easy to verify that if \(S\) and \(T\) are two non-empty sets, then
\[
k[S] \otimes k[T] \cong k[S \times T]
\]
as coalgebras.

**Definition 2.1.5.** Let \(C\) be a coalgebra. Then any non-zero element \(g \in C\) such that \(\Delta(g) = g \otimes g\) is called a **group-like** element of \(C\). We will denote by \(G(C)\) the set of all group-like elements of a coalgebra \(C\).

Note that if \(g \in G(C)\), then the counit property (2.2) ensures that \(\epsilon(g) = 1\). Note also that if \(S\) is a non-empty set, then \(G(k[S]) = S\). The next proposition states that \(G(C)\) is actually a linearly independent subset of \(C\). In particular, \(k[G(C)]\) is a subcoalgebra of \(C\) of dimension \(|G(C)|\). We omit the proof for brevity.

**Proposition 2.1.6.** Let \(C\) be a coalgebra and assume \(G(C)\) is non-empty. Then \(G(C)\) is a linearly independent subset of the vector space \(C\).
We will use notation attributed to Sweedler for the image of an element under the comultiplication of a coalgebra $C$. We write
\[ \Delta(c) = \sum_{(c)} c_1 \otimes c_2 \]
for $c \in C$, where the summation is understood to be over a finite number of elements of the form $c_i \otimes d_i$ for $c_i, d_i \in C$. While this may be an abuse of notation, it will be very useful in calculations. For example, the coassociativity property (2.1) may be written
\[ \sum_{(c)} (c_1)_1 \otimes (c_1)_2 \otimes c_2 = \sum_{(c)} c_1 \otimes (c_2)_1 \otimes (c_2)_2 \]
for all $c \in C$. We will therefore denote
\[ ((\Delta \otimes \text{id}_C)\Delta)(c) = (\text{id}_C \otimes \Delta)\Delta(c) = \sum_{(c)} c_1 \otimes c_2 \otimes c_3 \]
for all $c \in C$. If $\Delta_1 = \text{id}_C$ and $\Delta_2 = \Delta$, then we define
\[ \Delta_n = (\Delta \otimes \text{id}_C \otimes \cdots \otimes \text{id}_C)\Delta_{n-1} \]
for integers $n \geq 3$. By coassociativity, we can therefore denote
\[ \Delta_n(c) = \sum_{(c)} c_1 \otimes c_2 \otimes \cdots \otimes c_n \]
for all $c \in C$ without ambiguity.

Also note that the counit property (2.2) of the coalgebra $C$ may be written
\[ \sum_{(c)} \epsilon(c_1)c_2 = c = \sum_{(c)} \epsilon(c_2)c_1 \]
for all $c \in C$ and that if $C$ is a cocommutative coalgebra, then
\[ \sum_{(c)} c_1 \otimes c_2 = \sum_{(c)} c_2 \otimes c_1 \]
for all $c \in C$. Moreover, if $f : C \to D$ is a coalgebra homomorphism, then the first identity of (2.3) becomes
\[ \sum_{(c)} f(c_1) \otimes f(c_2) = \sum_{(f(c))} f(c)_1 \otimes f(c)_2 \]
for all $c \in C$.

For simplicity, we will often suppress the subscript in the summation or even the summation symbol itself in the use of Sweedler notation for comultiplication. For example, we may write

$$\Delta(c) = c_1 \otimes c_2$$

for $c \in C$, where it is understood that the right-hand side is a finite summation of elements of the form $c_i \otimes d_i$ for $c_i, d_i \in C$.

Next we describe the tensor product coalgebra construction, which is similar to the tensor product algebra structure of two algebras over the same field.

**Example 2.1.7.** Let $(C, \Delta_C, \epsilon_C)$ and $(D, \Delta_D, \epsilon_D)$ be two coalgebras over the field $\mathbb{k}$. Then we can construct a coalgebra on the tensor product vector space $C \otimes D$, called the **tensor product coalgebra**, by defining

$$\Delta = (\text{id}_C \otimes \tau \otimes \text{id}_D) \circ (\Delta_C \otimes \Delta_D) : C \otimes D \to C \otimes D \otimes C \otimes D$$

and

$$\epsilon = \epsilon_C \otimes \epsilon_D : C \otimes D \to \mathbb{k}$$

where $\tau : C \otimes D \to D \otimes C$ is the linear ‘twist’ map. That is,

$$\Delta(c \otimes d) = \sum c_1 \otimes d_1 \otimes c_2 \otimes d_2$$

and

$$\epsilon(c \otimes d) = \epsilon_C(c)\epsilon_D(d)$$

for all $c \in C$ and $d \in D$.

Dual to the notion of an ideal of an algebra is that of a coideal of a coalgebra. With coideals, we will be able to construct quotient coalgebras on the corresponding quotient vector spaces.

**Definition 2.1.8.** Let $C$ be a coalgebra and $I$ a subspace of $C$. Then $I$ is a **left coideal** of $C$ if $\Delta(I) \subseteq C \otimes I$. Similarly, $I$ is called a **right coideal** of $C$ if $\Delta(I) \subseteq I \otimes C$. We say that $I$ is a **coideal** of $C$ if $\Delta(I) \subseteq C \otimes I + I \otimes C$ and $\epsilon(I) = 0$. 
Note that if $C$ is a coalgebra then $C$ and $\{0\}$ are both trivially coideals of $C$. Note also that if $I$ is a coideal of $C$, then $I$ is not necessarily either a left coideal or a right coideal of $C$. However, if $I$ is either a left or right coideal of $C$ such that $\epsilon(I) = 0$, then $I$ is a coideal of $C$.

**Proposition 2.1.9.** Let $C$ and $D$ be coalgebras over $\mathbb{k}$ and $f : C \rightarrow D$ a coalgebra homomorphism. Then $f(C)$ is a subcoalgebra of $D$ and $\ker(f)$ is a coideal of $C$.

**Proof.** To see that $f(C)$ is a subcoalgebra of $D$, we use the fact that $f$ is a coalgebra homomorphism. Namely,

$$\Delta(f(c)) = f(c_1) \otimes f(c_2) = f(c_1) \otimes f(c_2) \in f(C) \otimes f(C)$$

for all $c \in C$.

Lastly, to see that $\ker(f)$ is a coideal of $C$, we first note that

$$\ker(f \otimes f) = C \otimes \ker(f) + \ker(f) \otimes C.$$  

Also,

$$(f \otimes f) \circ \Delta_C = \Delta_D \circ f$$

implies that

$$(f \otimes f)\Delta_C (\ker(f)) = \Delta_D f (\ker(f)) = 0$$

and hence

$$\Delta_C (\ker(f)) \subseteq \ker(f \otimes f) = C \otimes \ker(f) + \ker(f) \otimes C.$$  

This shows that $\ker(f)$ is a coideal of $C$. \qed

Just as we are able to define a quotient algebra structure on $A/I$ given an algebra $A$ and an ideal $I$, we are able to define a coalgebra structure on the quotient vector space $C/I$ given a coalgebra $C$ and a coideal $I$ of $C$.

**Proposition 2.1.10.** Let $(C, \Delta, \epsilon)$ be a coalgebra and $I$ a coideal of $C$, and let

$$\pi : C \rightarrow C/I$$

be the canonical linear surjection. Then there is a unique coalgebra structure on $C/I$ such that $\pi$ is a coalgebra homomorphism.
Proof. Note first that

$$(\pi \otimes \pi)\Delta(I) \subseteq (\pi \otimes \pi)(C \otimes I + I \otimes C) = 0$$

and so there exists a unique linear map

$$\Delta' : C/I \to C/I \otimes C/I$$

such that the diagram

$$\begin{array}{ccc}
C & \xrightarrow{\pi} & C/I \\
\Delta \downarrow & & \downarrow \Delta' \\
C \otimes C & \xrightarrow{\pi \otimes \pi} & C/I \otimes C/I
\end{array}$$

commutes. Note that this map is defined by

$$\Delta'(c + I) = \sum (c_1 + I) \otimes (c_2 + I)$$

for all $c \in C$. The coassociativity of $\Delta'$ follows at once from the coassociativity of $\Delta$.

Moreover, the fact that $\epsilon(I) = 0$ implies that there exists a unique linear map

$$\epsilon' : C/I \to k$$

such that the diagram

$$\begin{array}{ccc}
C & \xrightarrow{\pi} & C/I \\
\epsilon \downarrow & & \downarrow \epsilon' \\
k & \xrightarrow{\epsilon} & k
\end{array}$$

commutes. This map is given by

$$\epsilon'(c + I) = \epsilon(c)$$

for all $c \in C$. Moreover,

$$\epsilon'(c_1 + I)(c_2 + I) = \pi(\epsilon(c_1)c_2) = \pi(c) = c + I$$

and similarly

$$\epsilon'(c_2 + I)(c_1 + I) = c + I$$
for all \( c \in C \), and so \( \Delta' \) and \( \epsilon' \) give \( C/I \) the structure of a coalgebra. The commutativity of the above two diagrams shows that

\[
\pi : C \to C/I
\]

is a coalgebra homomorphism, and the uniqueness follows from the uniqueness of \( \Delta' \) and \( \epsilon' \) as above.

We will call a coalgebra \( C \) **simple** if it contains no non-zero proper subcoalgebras. Obviously a direct sum of coalgebras is again a coalgebra. That is, if \( (C, \Delta_C, \epsilon_C) \) and \( (D, \Delta_D, \epsilon_D) \) are coalgebras over \( k \), then the vector space \( C \oplus D \) is a coalgebra with comultiplication given by

\[
\Delta (c + d) = \Delta(c) + \Delta(d)
\]

and counit given by

\[
\epsilon (c + d) = \epsilon_C(c) + \epsilon_D(d)
\]

for all \( c \in C \) and \( d \in D \). We will call \( C \) **cosemisimple** if it is a direct sum of simple subcoalgebras.

**Definition 2.1.11.** Let \( C \) be a coalgebra over \( k \). The **coradical** \( C_0 \) of \( C \) is the sum of all simple subcoalgebras \( C \). We call \( C \) **pointed** if every simple subcoalgebra of \( C \) is one-dimensional.

Let \( C \) be a one-dimensional coalgebra \( C \) and let \( c \) be any non-zero element of \( C \). Then \( \Delta(c) = k(c \otimes c) \) for some non-zero \( k \in k \). Note then that

\[
\Delta(kc) = k\Delta(c) = k^2(c \otimes c) = kc \otimes kc.
\]

That is, there exists \( g \in C \) such that

\[
\Delta(g) = g \otimes g
\]

and so \( C \) necessarily contains a group-like element. This implies that every one-dimensional coalgebra \( C \) is of the form \( k\{g\} \) for some \( g \in G(C) \). This observation implies that if \( C \) is pointed, then every simple subcoalgebra of \( C \) is generated by a group-like element, and so \( C \) is pointed if and only if \( C_0 = k[G(C)] \).
2.1.2 Duality Between Algebras and Coalgebras

For any vector space $V$ over the field $k$, we denote by

$$V^* = \text{Hom}_k(V, k)$$

the linear dual of $V$. It is the vector space consisting of all linear maps from $V$ to the field $k$. Note that $k \cong k^*$ as vector spaces over $k$.

If $V$ and $W$ are vector spaces over $k$, then there is a linear inclusion map

$$V^* \otimes W^* \hookrightarrow (V \otimes W)^*$$

given by

$$(f \otimes g)(v \otimes w) = f(v)g(w)$$

for all $v \in V$, $w \in W$, $f \in V^*$, and $g \in W^*$. If $V$ and $W$ happen to be finite-dimensional, then

$$\dim(V^* \otimes W^*) = \dim(V \otimes W)^*$$

and so

$$V^* \otimes W^* \cong (V \otimes W)^*$$

as vector spaces. If both $V$ and $W$ are infinite-dimensional then we do not have this isomorphism.

Given vector spaces $V$ and $W$ over $k$ and a linear map $\phi : V \rightarrow W$, we define the map

$$\phi^* : W^* \rightarrow V^*$$

called the adjoint of $\phi$, given by

$$\phi^*(f)(v) = f(\phi(v))$$

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

We now describe how the dual vector space $C^*$ of a coalgebra $C$ can be given the structure of an algebra. We do not need an assumption on the dimension of the coalgebra $C$ to do this. The multiplication of this algebra is the composition

$$M : C^* \otimes C^* \hookrightarrow (C \otimes C)^* \xrightarrow{\Delta^*} C^*$$
using the adjoint of the comultiplication $\Delta$ of $C$. If we denote by $f \ast g$ the product of $f, g \in C^*$, then the above definition implies that

$$(f \ast g)(c) = \sum f(c_1)g(c_2) \quad (2.4)$$

for all $c \in C$. Moreover, the unit map $u : k \to C^*$ of this algebra is given by the composition

$$u : k \cong k^* \xrightarrow{\epsilon^*} C^*$$

and so the multiplicative unit of $C^*$ is $1_{C^*} = u(1)$ where

$$1_{C^*}(c) = \epsilon(c) \quad (2.5)$$

for all $c \in C$. In other words, the unit of $C^*$ is the counit $\epsilon$ of $C$.

**Proposition 2.1.12.** Let $(C, \Delta, \epsilon)$ be a coalgebra over $k$. Then $(C^*, M, u)$ as defined above is an algebra over $k$.

**Proof.** First we verify the associativity of the multiplication, which follows from the coassociativity of $\Delta$. For any $f, g, h \in C^*$ and $c \in C$, we have

$$((f \ast g) \ast h)(c) = (f \ast g)(c_1)h(c_2) = f(c_1)g(c_2)h(c_3) = f(c_1)(g \ast h)(c_2) = (f \ast (g \ast h))(c)$$

which shows that $(f \ast g) \ast h = f \ast (g \ast h)$. Therefore the multiplication is associative.

Next we verify that $\epsilon$ is the multiplicative unit of $C^*$. For any $f \in C^*$ and $c \in C$ we have

$$(f \ast \epsilon)(c) = f(c_1)\epsilon(c_2) = f(c_1\epsilon(c_2)) = f(c)$$

and therefore $f \ast \epsilon = f$. Similarly, $\epsilon \ast f = f$, and therefore $\epsilon$ is the multiplicative unit of $C^*$. \qed
Dually, given an algebra $A$ we can define a coalgebra structure on the dual space $A^*$ in the case that $A$ is finite-dimensional. The reason that $A$ needs to be finite-dimensional is due to the fact that we will need a linear map

$$(A \otimes A)^* \to A^* \otimes A^*$$

which is just the inverse of the bijective inclusion

$$A^* \otimes A^* \hookrightarrow (A \otimes A)^*$$

discussed previously.

So let $(A, M, u)$ be an algebra over $k$. Then a linear comultiplication on $A^*$ can be defined by the composition

$$\Delta : A^* \stackrel{M^*}{\to} (A \otimes A)^* \cong A^* \otimes A^*$$

and a counit map on $A^*$ can be defined by the composition

$$\epsilon : A^* \stackrel{u^*}{\to} k^* \cong k.$$

In other words

$$\Delta(f)(a \otimes b) = f(ab) \quad (2.6)$$

and

$$\epsilon(f) = f(1_A) \quad (2.7)$$

for all $f \in A^*$ and $a, b \in A$, where $1_A = u(1)$ is the multiplicative unit of the algebra $A$.

**Proposition 2.1.13.** Let $(A, M, u)$ be a finite-dimensional algebra over $k$. Then $(A^*, \Delta, \epsilon)$ as defined above is a coalgebra.

**Proof.** First we establish the coassociativity of the comultiplication, which follows from asso-
ciativity of the multiplication. For any \( f \in A^* \) and \( a, b, c \in A \), we have

\[
(\Delta \otimes \text{id}_{A^*})\Delta(f)(a \otimes b \otimes c) = (\Delta(f_1) \otimes f_2)(a \otimes b \otimes c) = \Delta(f_1)(a \otimes b) \otimes f_2(c) = f_1(ab)f_2(c) = f_1(a)f_2(bc) = f_1(a) \otimes \Delta(f_2)(b \otimes c) = (\text{id}_{A^*} \otimes \Delta)\Delta(f)(a \otimes b \otimes c)
\]

which shows that \( \Delta \) is coassociative.

To verify the counit property, note that for any \( f \in A^* \) and \( a \in A \) we have

\[
(\epsilon \otimes \text{id}_{A^*})\Delta(f)(a) = (\epsilon \otimes \text{id}_{A^*})(f_1 \otimes f_2)(a) = \epsilon(f_1)f_2(a) = f_1(1_A)f_2(a) = f(1_Aa) = f(a)
\]

and so \( (\epsilon \otimes \text{id}_{A^*})\Delta(f) = f \). Similarly, \( (\text{id}_{A^*} \otimes \epsilon)\Delta(f) = f \), showing that \( \epsilon \) is in fact the counit of \( A^* \). Therefore \( A^* \) is a coalgebra.

The duality between algebras and coalgebras as illustrated above will be key for Hopf algebras as we will define later, which have both an algebra structure and a coalgebra structure. The fact that the dual of a coalgebra is an algebra and that the dual of a finite-dimensional algebra is a coalgebra will imply that the dual of a finite-dimensional Hopf algebra will also be a Hopf algebra. The duality between finite-dimensional algebras and coalgebras also implies the following relationship between algebra and coalgebra homomorphisms. The proof of this proposition follows simply from the commutative diagrams defining the particular homomorphisms, and so the proof is omitted.
Proposition 2.1.14. Let $C$ and $D$ be coalgebras over $k$ and let $A$ and $B$ be finite-dimensional algebras over $k$.

(a) If $f : C \to D$ is a coalgebra homomorphism, then $f^* : D^* \to C^*$ is an algebra homomorphism.

(b) If $f : A \to B$ is an algebra homomorphism, then $f^* : B^* \to A^*$ is a coalgebra homomorphism.

Duality gives a connection between the subcoalgebras of a coalgebra $C$ and the ideals of the algebra $C^*$. A similar role is also played between the subalgebras of $C^*$ and the coideals of $C$. We illustrate these in the next results, where we assume that all coalgebras and algebras are finite-dimensional. Some of these results hold for the infinite-dimensional case, but we shall be concerned only with the finite-dimensional case in this thesis. Recall that if $W$ is a subspace of the vector space $V$ over $k$, then

$$W^\perp = \{ f \in V^* \mid f(w) = 0 \text{ for all } w \in W \}$$

is the subspace of $V^*$ orthogonal to $W$. Similarly, if $X$ is a subspace of $V^*$, then

$$X^\perp = \{ v \in V \mid f(v) = 0 \text{ for all } f \in X \}$$

is the subspace of $V$ orthogonal to $X$. For brevity, we omit the proof of the following results.

Proposition 2.1.15. Let $A$ be a finite-dimensional algebra over $k$ and let $C$ be a finite-dimensional coalgebra over $k$. Assume that $B$ is a linear subspace of $A$ and that $D$ is a linear subspace of $C$.

(a) $B$ is a subalgebra of $A$ if and only if $B^\perp$ is a coideal of the coalgebra $A^*$. In this case $A^*/B^\perp \cong B^*$ as coalgebras.

(b) A subspace $I$ of $A^*$ is a coideal of $A^*$ if and only if $I^\perp$ is a subalgebra of $A$.

(c) $D$ is a subcoalgebra of $C$ if and only if $D^\perp$ is an ideal of the algebra $C^*$. In this case $C^*/D^\perp \cong D^*$ as algebras.

(d) A subspace $I$ of $C^*$ is an ideal of $C^*$ if and only if $I^\perp$ is a subcoalgebra of $C$. 
2.1.3 Comodules

In this subsection, we dualize the notion of a module acting on an algebra to that of a comodule coacting on a coalgebra. Recall that, given an associative algebra $A$ with linear multiplication $M : A \otimes A \to A$ and a unit map $u : k \to A$, a left $A$-module is a vector space $V$ equipped with a linear map
\[ \mu : A \otimes V \to V \]
such that the diagrams
\[
\begin{array}{ccc}
A \otimes A \otimes V & \xrightarrow{id \otimes \mu} & A \otimes V \\
\downarrow M \otimes id & & \downarrow \mu \\
A \otimes V & \xrightarrow{\mu} & V
\end{array}
\quad
\begin{array}{ccc}
k \otimes V & \xrightarrow{u \otimes id} & A \otimes V \\
\downarrow id & & \downarrow \mu \\
A \otimes V & \xrightarrow{\mu} & V
\end{array}
\]
commute. Setting $\mu(a \otimes v) = a \cdot v$ for all $a \in A$ and $v \in V$, this translates to
\[ a \cdot (b \cdot v) = ab \cdot v \quad \text{and} \quad 1_A \cdot v = v \]
for all $a, b \in A$ and $v \in V$. A similar definition holds for a right $A$-module. Reversing the arrows in these diagrams, we arrive at the definition of a comodule.

**Definition 2.1.16.** Let $(C, \Delta, \epsilon)$ be a coalgebra and $V$ a vector space over $k$. We say that $V$ is a left $C$-comodule if there exists a linear map $\rho : V \to C \otimes V$ such that the diagrams
\[
\begin{array}{ccc}
V & \xrightarrow{\rho} & C \otimes V \\
\downarrow \rho & & \downarrow \Delta \otimes id \\
C \otimes V & \xrightarrow{id \otimes \rho} & C \otimes C \otimes V
\end{array}
\quad
\begin{array}{ccc}
V & \xrightarrow{\rho} & C \otimes V \\
\downarrow \rho & & \downarrow \epsilon \otimes id \\
V \otimes k & & V \otimes k
\end{array}
\]
commute. Similarly, we call $V$ a right $C$-comodule if there exists a linear map $\rho : V \to V \otimes C$ such that the diagrams
\[
\begin{array}{ccc}
V & \xrightarrow{\rho} & V \otimes C \\
\downarrow \rho & & \downarrow \rho \otimes id \\
V \otimes C & \xrightarrow{id \otimes \Delta} & V \otimes C \otimes C
\end{array}
\quad
\begin{array}{ccc}
V & \xrightarrow{\rho} & V \otimes C \\
\downarrow \rho & & \downarrow \rho \otimes \epsilon \\
V \otimes C & \xrightarrow{id \otimes \rho} & V \otimes k
\end{array}
\]
commute.
We will often denote a left or right comodule by \((V, \rho)\) and refer to \(\rho\) as the left or right coaction of \(V\) on \(C\). Then \((V, \rho)\) is a left \(C\)-comodule if the coaction satisfies
\[
(id_C \otimes \rho)\rho(v) = (\Delta \otimes id_V)\rho(v) \quad \text{and} \quad (\epsilon \otimes id_V)\rho(v) = v
\] (2.8)
for all \(v \in V\), and \((V, \rho)\) is a right \(C\)-comodule if the coaction satisfies
\[
(\rho \otimes id_C)\rho(v) = (id_V \otimes \Delta)\rho(v) \quad \text{and} \quad (id_V \otimes \epsilon)\rho(v) = v
\] (2.9)
for all \(v \in V\).

We now adapt the Sweedler notation to coactions. If \((V, \rho)\) is a right \(C\)-comodule, then we write
\[
\rho(v) = \sum v_0 \otimes v_1
\]
for all \(v \in V\), where each \(v_0 \in V\) and \(v_1 \in C\). So equation (2.9) becomes
\[
\sum (v_0)_0 \otimes (v_0)_1 \otimes v_1 = \sum v_0 \otimes (v_1)_1 \otimes (v_1)_2
\] (2.10)
and
\[
\sum \epsilon(v_1)v_0 = v
\]
for all \(v \in V\). We can denote the element in (2.10) now by
\[
\sum v_0 \otimes v_1 \otimes v_2.
\]
Similarly, if \((V, \rho)\) is a left \(C\)-comodule we write
\[
\rho(v) = \sum v_{-1} \otimes v_0
\]
for all \(v \in V\), where \(v_0 \in V\) and \(v_{-1} \in C\). In this case, equation (2.8) becomes
\[
\sum v_{-1} \otimes (v_0)_{-1} \otimes (v_0)_0 = \sum (v_{-1})_1 \otimes (v_{-1})_2 \otimes v_0
\] (2.11)
and
\[
\sum \epsilon(v_{-1})v_0 = v
\]
for all \(v \in V\). We denote the element in (2.11) by
\[
\sum v_{-2} \otimes v_{-1} \otimes v_0,
\]
a slightly different adaptation of our original Sweedler notation.
Example 2.1.17. If $C$ is a coalgebra, then we may consider $C$ as either a left or right $C$-comodule where the coaction is given by the comultiplication

$$\Delta : C \to C \otimes C.$$ 

The coassociativity and counit properties give, respectively, the corresponding properties for a $C$-comodule. \hfill \Box

Given a coalgebra $C$ over $k$, we can define homomorphisms between $C$-comodules by dualizing the notion of a module homomorphism. Let $(V, \rho_V)$ and $(W, \rho_W)$ be (right) $C$-comodules and assume that

$$f : V \to W$$

is a $k$-linear map. Then we say that $f$ is a **comodule homomorphism** (or comodule map) if the diagram

$$\begin{array}{ccc}
V & \xrightarrow{f} & W \\
\rho_V & & \rho_W \\
V \otimes C & \xrightarrow{f \otimes \text{id}_C} & W \otimes C
\end{array}$$

commutes.

In other words, $f : V \to W$ is a right $C$-comodule homomorphism if

$$(f \otimes \text{id}_C)(\rho_V(v)) = \rho_W(f(v))$$

for all $v \in V$. In Sweedler notation for a right $C$-comodule, this can be written

$$\sum f(v_0) \otimes v_1 = \sum f(v_0) \otimes f(v_1)$$

for all $v \in v$, where it is understood that $v_0 \in V$ and $f(v_0) \in W$ and both $v_1, f(v_1) \in C$. A similar definition of a comodule homomorphism can be given for left $C$-comodules.

If $(V, \rho)$ is a (right) $C$-comodule and $W$ is a linear subspace of $V$, then we say that $W$ is a **subcomodule** of $V$ if $\rho(W) \subseteq W \otimes C$. In this case, $W$ is itself a (right) $C$-comodule with the coaction given by the restriction of $\rho$ to $W$, and the inclusion map $i : W \hookrightarrow V$ is a $C$-comodule homomorphism. A comodule $V$ is called **simple** if it contains no proper non-zero subcomodules. The next result establishes that the image and kernel of a comodule
homomorphism are subcomodules, which should come as no surprise. The proof is standard and is omitted for brevity.

**Proposition 2.1.18.** Let $C$ be a coalgebra over $\mathbb{k}$ and let $V$ and $W$ be two (right) $C$-comodules with $f : V \to W$ a comodule homomorphism. Then $\operatorname{Im}(f)$ is a subcomodule of $W$ and $\ker f$ is a subcomodule of $V$.

If $V$ is a right $C$-comodule and $W$ is a subcomodule, then the quotient vector space $V/W$ inherits a right $C$-comodule structure via

$$
\rho_{V/W} : V/W \to V/W \otimes C
$$

defined by

$$
\rho(v + W) = (v_0 + W) \otimes v_1
$$

for all $v \in V$. We refer to $V/W$ as a quotient $C$-comodule of $V$ with respect to $W$, and the canonical linear surjection

$$
\pi : V \to V/W
$$

is a comodule homomorphism.

We next establish a consequence of the duality between modules and comodules.

**Proposition 2.1.19.** Let $C$ be a coalgebra. If $V$ is a right $C$-comodule, then $V$ is a left $C^*$-module.

**Proof.** If $\rho : V \to V \otimes C$ is the comodule struture map, with

$$
\rho(v) = \sum v_0 \otimes v_1,
$$

then we define

$$
f \cdot v = \sum f(v_1)v_0
$$

for all $f \in C^*$ and $v \in V$. To see that this actually defines a module action, note that

$$
(f \ast g) \cdot v = \sum f(v_1)g(v_2)v_0 = f \cdot \sum g(v_1)v_0 = f \cdot (g \cdot v)
$$
and
\[ \epsilon \cdot v = \sum \epsilon(v_1)v_0 = v \]
for all \( f, g \in C^* \) and \( v \in V \), which follows from the identities (2.9).

A similar result holds for left \( C \)-comodules and right \( C^* \)-modules, where \( C \) is a coalgebra.

In the case that \( A \) is a finite-dimensional algebra, we also have the following.

**Proposition 2.1.20.** Let \( A \) be a finite-dimensional algebra. If \( V \) is a left \( A \)-module, then \( V \) is a right \( A^* \)-comodule.

**Proof.** Assume \( \dim V = n \) and \( \{ w_1, w_2, \ldots, w_n \} \) is a basis for \( V \) over \( \mathbb{k} \). Therefore, for \( v \in V \) there exist \( \alpha_i(a) \in \mathbb{k} \) such that
\[ a \cdot v = \sum_{i=1}^{n} \alpha_i(a)w_i \]
for \( a \in A \). It is easy to verify that \( \alpha_i \) defines an element in \( A^* \) for each \( 1 \leq i \leq n \). Setting
\[ \sum_{i=1}^{n} w_i \otimes \alpha_i = \sum v_0 \otimes v_1 \]
we can define \( \rho : V \to V \otimes A^* \) by
\[ \rho(v) = \sum v_0 \otimes v_1 \]
for \( v \in V \).

To verify that \( \rho : V \to V \otimes A^* \) actually defines a coaction, we must show that the identities in (2.9) hold for all \( v \in V \). We note first that for any \( v \in V \) we have
\[ ((v_1)_1 \otimes (v_1)_2)(a \otimes b)v_0 = v_1(ab)v_0 \]
\[ = ab \cdot v \]
\[ = a \cdot (b \cdot v) \]
\[ = a \cdot v_1(b)v_0 \]
\[ = v_1(b)(a \cdot v_0) \]
\[ = v_1(b)(v_0)_1(a)(v_0)_0 \]
\[ = ((v_0)_1 \otimes v_1)(a \otimes b)(v_0)_0 \]
for all \( a, b \in A \). Therefore
\[
\sum v_0 \otimes (v_1)_1 \otimes (v_1)_2 = \sum (v_0)_0 \otimes (v_0)_1 \otimes v_1
\]
for all \( v \in V \). To see that the second identity of (2.9) holds, note that for any \( v \in V \) we have
\[
(id_V \otimes \epsilon)(v_0 \otimes v_1) = \epsilon(v_1)v_0
\]
\[
= v_1(1_A)v_0
\]
\[
= 1_A \cdot v
\]
\[
= v
\]
which shows that
\[
(id_V \otimes \epsilon)\left(\sum v_0 \otimes v_1\right) = v
\]
for all \( v \in V \). Therefore \( \rho \) is a coaction on \( A^* \) as desired, finishing the proof. \( \square \)

2.2 Hopf Algebras

2.2.1 Bialgebras

We now define the notion of a bialgebra, which is, roughly speaking, both an algebra and a coalgebra with a certain compatibility condition. Recall that for any algebra \( A \), both \( A \otimes A \) and \( k \) may be regarded as algebras, and that for any coalgebra \( C \), both \( C \otimes C \) and \( k \) may be regarded as coalgebras.

**Definition 2.2.1.** Let \( H \) be a vector space over \( k \) such that \((H, M, u)\) is an algebra and \((H, \Delta, \epsilon)\) is a coalgebra. Then \( H \) is called a **bialgebra** if both \( \Delta : H \to H \otimes H \) and \( \epsilon : H \to k \) are algebra homomorphisms.

In other words, to say that \((H, M, \Delta, u, \epsilon)\) is a bialgebra means that \( H \) is an algebra and a coalgebra such that
\[
\Delta(ab) = \Delta(a)\Delta(b), \quad \Delta(1_H) = 1_H \otimes 1_H
\]
\[
\epsilon(ab) = \epsilon(a)\epsilon(b), \quad \epsilon(1_H) = 1
\]
for all $a, b \in H$, where $u(1) = 1_H$ is the multiplicative unit of $H$.

If $H$ and $K$ are bialgebras over $k$, then we shall call a linear map

$$f : H \rightarrow K$$

a **bialgebra homomorphism** if it is both an algebra homomorphism and a coalgebra homomorphism. If $K$ is a subspace of the bialgebra $H$ such that $K$ is a subalgebra and a subcoalgebra, then $K$ is referred to as a **sub-bialgebra**. Similarly, if $H$ is a bialgebra over $k$ and $I$ is a vector space over $k$ that is both an ideal and a coideal, then $I$ is called a **biideal** of $H$. The vector space $H/I$ then becomes a bialgebra with the quotient algebra and quotient coalgebra structures, known as a quotient bialgebra.

**Example 2.2.2.** If $M$ is a monoid, then the $k$-vector space $k[M]$ is a bialgebra with the algebra structure induced by the product of the monoid and coalgebra structure defined by the diagonal map

$$\Delta(a) = a \otimes a$$

for all $a \in M$. The fact that the comultiplication $\Delta$ is an algebra homomorphism follows easily from the equality

$$\Delta(ab) = ab \otimes ab = (a \otimes a)(b \otimes b) = \Delta(a)\Delta(b)$$

for all $a, b \in M$.

**Example 2.2.3.** Any field $k$ is a bialgebra over itself, with trivial multiplication and comultiplication maps. Also, if $H$ is a bialgebra, then $H \otimes H$ is a bialgebra with the tensor product algebra structure and the tensor product coalgebra structure.

If $H$ is a bialgebra with multiplicative unit $1_H$, then the set $G(H)$ of group-like elements of $H$ contains $1_H$ and is a monoid contained in $H$. The fact that $G(H)$ is closed under multiplication follows from the fact that $\Delta$ is an algebra homomorphism:

$$\Delta(gh) = \Delta(g)\Delta(h) = (g \otimes g)(h \otimes h) = gh \otimes gh$$

for all $g, h \in G(H)$. Moreover, $k[G(H)]$ is a sub-bialgebra contained in $H$. Any bialgebra $H$ contains the trivial sub-bialgebra $k[1_H]$ which is isomorphic to the trivial bialgebra $k$. 
Definition 2.2.4. Let $H$ be a bialgebra and $g, h \in G(H)$. Then a non-zero element $x \in H$ is called a $(g, h)$-skew primitive element if

$$\Delta(x) = x \otimes g + h \otimes x.$$ 

We will refer to a $(1_H, 1_H)$-skew primitive element of $H$ as simply a primitive element of $H$. Denote by $P_{g,h}(H)$ the set of $(g, h)$-skew primitive elements of $H$ and, for simplicity, denote by $P(H)$ the set of all primitive elements of $H$.

Note that if $x \in H$ is a $(g, h)$-skew primitive element of $H$ for some $g, h \in G(H)$, then

$$\epsilon(x) = 0$$

which follows from the fact that $\epsilon(g) = \epsilon(h) = 1$ and the counit property. Moreover, for all $x, y \in P(H)$ we have that $[x, y] = xy - yx \in P(H)$. Assuming that $P(H)$ is non-empty, we have that $P(H)$ is a Lie algebra contained in $H$.

Note also that every element of the form $\xi(g - h)$ is a $(g, h)$-skew primitive element of $H$ for $g, h \in G(H)$ and any $\xi \in k$. Elements of this form will be referred to as trivial $(g, h)$-skew primitive elements of $H$.

Remark 2.2.5. If $H$ is a bialgebra containing a primitive element, then $H$ is infinite-dimensional (see [1, Section 2.1.1]). This follows from the fact that $H$ contains the universal enveloping algebra of $P(H)$, which is infinite-dimensional. See [23, Chapter 5] for more information on universal enveloping algebras of Lie algebras.

Now let $H$ be a finite-dimensional bialgebra over $k$. Then the dual vector space $H^*$ is both an algebra and a coalgebra, and it follows easily that $H^*$ is in fact also a bialgebra, known as the dual bialgebra of $H$. Since $H$ is finite-dimensional, it can be easily seen that $(H^*)^*$ is isomorphic to $H$ as bialgebras via the canonical isomorphism $\Phi : H \rightarrow (H^*)^*$ defined by

$$\Phi(h)(f) = f(h)$$

for all $h \in H$ and $f \in H^*$. The next proposition nicely characterizes the group-like elements of the dual bialgebra $H^*$. 
Proposition 2.2.6. Let $H$ be a finite-dimensional bialgebra over $\mathbb{k}$. Then
\[ G(H^*) = \text{Alg}(H, \mathbb{k}) \]
the algebra homomorphisms from $H$ to $\mathbb{k}$.

Proof. Given any $f \in \text{Alg}(H, \mathbb{k})$, it is easy to see that $\Delta(f) = f \otimes f$ since
\[ \Delta(f)(a \otimes b) = f(ab) = f(a)f(b) = (f \otimes f)(a \otimes b) \]
for all $a, b \in H$ by (2.4), and so $\Delta(f) = f \otimes f$. Conversely, if $\Delta(f) = f \otimes f$, then
\[ f(ab) = \Delta(f)(a \otimes b) = (f \otimes f)(a \otimes b) = f(a)f(b) \]
for all $a, b \in H$, and so $f \in \text{Alg}(H, \mathbb{k})$. \qed

Lastly, we note that the dual notions of commutativity and cocommutativity in a bialgebra are related in the following way.

Proposition 2.2.7. If $H$ is a finite-dimensional bialgebra, then $H$ is cocommutative if and only if $H^*$ is commutative, and $H$ is commutative if and only if $H^*$ is cocommutative.

2.2.2 Hopf Algebras

We are almost ready to define the main object of study in this thesis, a Hopf algebra. A Hopf algebra is a bialgebra with an additional linear structure map. To define this map, we will need the notion of a convolution product.

Let $(A, M, u)$ be an algebra over $\mathbb{k}$ and let $(C, \Delta, \epsilon)$ be a coalgebra over $\mathbb{k}$. Then the vector space $\text{Hom}_{\mathbb{k}}(C, A)$ of linear maps from $C$ to $A$ is an algebra with the multiplication defined by
\[ f \ast g = M \circ (f \otimes g) \circ \Delta \]
for all $f, g \in \text{Hom}_{\mathbb{k}}(C, A)$. That is,
\[ (f \ast g)(c) = \sum f(c_1)g(c_2) \quad (2.12) \]
for all $c \in C$, using Sweedler’s summation notation. This multiplication is referred to as the convolution product of the linear maps $f, g \in \text{Hom}_{\mathbb{k}}(C, A)$, and the algebra $\text{Hom}_{\mathbb{k}}(C, A)$
is called the convolution algebra. The coassociativity of $C$ and the associativity of $A$ result in the convolution product being associative. The unit and counit properties of $A$ and $C$, respectively, imply that

$$u \circ \epsilon : C \rightarrow A$$

is the multiplicative unit of this convolution algebra.

We turn now to the case when $H$ is a bialgebra over $\mathbb{k}$. By the above construction we have a convolution algebra structure on the vector space $\text{Hom}_k(H, H)$ of linear operators of $H$ where $u \circ \epsilon \in \text{Hom}_k(H, H)$ is the multiplicative identity. In particular, the identity map $\text{id}_H$ is an element of $\text{Hom}_k(H, H)$ and we may consider whether or not this map is invertible in the convolution algebra.

**Definition 2.2.8.** Let $H$ be a bialgebra over $\mathbb{k}$. A linear map $S : H \rightarrow H$ is called an antipode of $H$ if $S$ is the convolution inverse of $\text{id}_H$ in $\text{Hom}_k(H, H)$. If such a map exists, we call $H$ a Hopf algebra.

To say that $S$ is an antipode of the bialgebra $H$ means that

$$S \ast \text{id}_H = \text{id}_H \ast S = u \circ \epsilon$$

or that

$$\sum S(h_1)h_2 = \sum h_1S(h_2) = \epsilon(h)1_H$$

for all $h \in H$, again using Sweedler’s summation notation. Moreover, if such an antipode exists, it is the inverse of an element in a convolution algebra and is hence unique. If necessary, we will denote a Hopf algebra $H$ by $(H, M, \Delta, u, \epsilon, S)$ where $M$ it the multiplication, $\Delta$ is the comultiplication, $u$ is the unit map, $\epsilon$ is the counit, and $S$ is the antipode. We next describe some basic properties of the antipode of a Hopf algebra which will be used frequently in the rest of this paper. Briefly, this result shows that $S$ is an algebra anti-homomorphism and a coalgebra anti-homomorphism.

**Proposition 2.2.9.** Let $H$ be a Hopf algebra over $\mathbb{k}$ with antipode $S$. Then

(a) $S(hk) = S(k)S(h)$
(b) \( S(1_H) = 1_H \)

c) \( \sum S(h)_1 \otimes S(h)_2 = \sum S(h_2) \otimes S(h_1) \)

d) \( \epsilon(S(h)) = \epsilon(h) \)

for all \( h, k \in H \).

Proof. (a) Consider the linear maps

\[ N : H \otimes H \to H \quad \text{and} \quad P : H \otimes H \to H \]

in the convolution algebra \( \text{Hom}(H \otimes H, H) \) given by

\[ N(h \otimes k) = S(k)S(h) \quad \text{and} \quad P(h \otimes k) = S(hk) \]

for all \( h, k \in H \). We will show that \( N \) and \( P \) are both inverses of the multiplication map \( M \) under the convolution product and hence \( N = P \).

First note that

\[
(M \ast N)(h \otimes k) = M(h_1 \otimes k_1)N(h_2 \otimes k_2)
\]
\[
= h_1 k_1 S(k_2)S(h_2)
\]
\[
= \epsilon(k)h_1 S(h_2)
\]
\[
= \epsilon(h)\epsilon(k)1_H
\]
\[
= (\epsilon \otimes \epsilon)(h \otimes k)1_H
\]

and that

\[
(M \ast P)(h \otimes k) = M(h_1 \otimes k_1)P(h_2 \otimes k_2)
\]
\[
= h_1 k_1 S(h_2 k_2)
\]
\[
= (hk)_1 S((hk)_2)
\]
\[
= \epsilon(hk)1_H
\]
\[
= \epsilon(h)\epsilon(k)1_H
\]
\[
= (\epsilon \otimes \epsilon)(h \otimes k)1_H
\]
for all $h, k \in H$. This implies that $N$ and $P$ are both left inverses of $M$ under convolution. Similarly, $N$ and $P$ are both right inverses of $M$ under convolution, and hence $N = P$, proving part 1.

(b) Since $\Delta(1_H) = 1_H \otimes 1_H$, we have that
\[ S(1_H) = S(1_H)1_H = \epsilon(1_H)1_H = 1_H \]
using the antipode property of $S$. This shows that $S(1_H) = 1_H$ and part 2 is proven.

(c) We use the same technique that we applied in part 1. We consider the linear maps
\[ Q : H \to H \otimes H \text{ and } R : H \to H \otimes H \]
in the convolution algebra $\text{Hom}(H, H \otimes H)$ given by
\[ Q(h) = S(h)_1 \otimes S(h)_2 \text{ and } R(h) = S(h_2) \otimes S(h_1) \]
for all $h \in H$. We will again show that $Q = R$ by showing that $Q$ and $R$ are both the convolution inverse of $\Delta : H \to H \otimes H$.

For all $h \in H$ we have that
\[
(D \ast Q)(h) = \Delta(h_1)Q(h_2)
= (h_1 \otimes h_2)(S(h_3)_1 \otimes S(h_3)_2)
= h_1S(h_3)_1 \otimes h_2S(h_3)_2
= \Delta(h_1S(h_2))
= \epsilon(h)\Delta(1_H)
= \epsilon(h)(1_H \otimes 1_H)
\]
and

\[(\Delta \ast R)(h) = \Delta(h_1)R(h_2)\]
\[= (h_1 \otimes h_2)(S(h_4) \otimes S(h_3))\]
\[= h_1S(h_4) \otimes h_2S(h_3)\]
\[= h_1S(h_3) \otimes \epsilon(h_2)1_H\]
\[= h_1\epsilon(h_2)S(h_3) \otimes 1_H\]
\[= h_1S(h_2) \otimes 1_H\]
\[= \epsilon(h)(1_H \otimes 1_H)\]

which shows that both \(Q\) and \(R\) are left inverses of \(\Delta\) under convolution. Similarly, \(Q\) and \(R\) are right inverses of \(\Delta\) under convolution, and therefore \(Q = R\), which proves part 3.

(d) Lastly, we show that \(\epsilon(S(h)) = \epsilon(h)\) for all \(h \in H\). Applying \(\epsilon\) to the identity

\[h_1S(h_2) = \epsilon(h)1_H\]

yields

\[\epsilon(h_1)\epsilon(S(h_2)) = \epsilon(h)\epsilon(1_H) = \epsilon(h).\]

That is,

\[\epsilon(S(h)) = \epsilon(S(\epsilon(h_1)h_2)) = \epsilon(h_1)\epsilon(S(h_2)) = \epsilon(h)\]

for all \(h \in H\), proving part 4 and finishing the proof.

\[\square\]

For Hopf algebras \(H\) and \(K\) over \(\mathbb{k}\), a bialgebra homomorphism

\[f : H \rightarrow K\]

is called a **Hopf algebra homomorphism** if

\[S_K(f(h)) = f(S_H(h))\]
or all $h \in H$, where $S_H$ is the antipode of $H$ and $S_K$ is the antipode of $K$. This condition is actually superfluous. It is known (see for example [12, Proposition 4.2.5]) that if $H$ and $K$ are Hopf algebras and $f : H \to K$ is a bialgebra homomorphism, then $S_K \circ f = f \circ S_H$ and so $f$ is a Hopf algebra homomorphism.

If $H$ is a Hopf algebra with antipode $S$, then a sub-bialgebra $K$ of $H$ is called a Hopf subalgebra of $H$ if $S(K) \subseteq K$. Also, if $I$ is a biideal of $H$, then $I$ is called a Hopf ideal of $H$ if $S(I) \subseteq I$, and the quotient bialgebra $H/I$ is a Hopf algebra, called a quotient Hopf algebra. The antipode $S_{H/I}$ of $H/I$ in this case is given by

$$S_{H/I}(h + I) = S(h) + I$$

for all $h \in H$, where $S$ is the antipode of $H$.

Remark 2.2.10. It is interesting to note that any sub-bialgebra $A$ of a finite-dimensional Hopf algebra $H$ must be a Hopf subalgebra of $H$. Passman and Quinn [46, Lemma 6] proved this by showing first that the subspace

$$F = \{ f \in \text{Hom}_k(H, H) : f(A) \subseteq A \}$$

of the convolution algebra $\text{Hom}_k(H, H)$ is closed under convolution product. Since $\text{id}_H \in F$ and $\text{Hom}_k(H, H)$ is finite-dimensional, they then show that the convolution inverse $S$ of $\text{id}_H$ must also be in $F$. Therefore, $S(A) \subseteq A$ and so $A$ is a Hopf subalgebra of $H$.

We next present a few key examples of Hopf algebras that will be used in the remainder of this thesis. The most basic example of a Hopf algebra is that of a group algebra.

Example 2.2.11. Let $G$ be a group. Then the group algebra $\mathbb{k}[G]$ is a Hopf algebra with canonical basis $G$. The antipode map is induced by the group inverse, so that

$$S(g) = g^{-1}$$

for all $g \in G$, and extended linearly to all of $\mathbb{k}[G]$. The fact that $S$ is the antipode of $\mathbb{k}[G]$ follows from the identity

$$S(g_1)g_2 = g_1^{-1}g = 1_G = gg^{-1} = g_1S(g_2)$$
for all \( g \in G \), since \( \Delta(g) = g \otimes g \) and \( \epsilon(g) = 1 \) for each \( g \in G \). Since \( G \) is a basis for \( \mathbb{k}[G] \), we have that \( S \) is the antipode of \( \mathbb{k}[G] \).

Note that if \( H \) is any Hopf algebra, then the set \( G(H) \) of group-like elements of \( H \) contains \( 1_H \) and forms a group under multiplication. Moreover, \( \mathbb{k}[G(H)] \) is a Hopf subalgebra of \( H \) of dimension \( |G| \). Note that as before, \( \mathbb{k}[G] \) is cocommutative for any group \( G \), and this Hopf algebra is commutative if and only if \( G \) is abelian.

A key property of finite-dimensional Hopf algebras is that the linear dual is also a Hopf algebra.

**Proposition 2.2.12.** Let \( H \) be a finite-dimensional Hopf algebra with antipode \( S \). Then the dual vector space \( H^* \) is a Hopf algebra with antipode \( S^* \).

**Proof.** From before we know that \( H^* \) is a bialgebra with structure maps induced by the adjoint maps of the structures of \( H \). We therefore need only show that \( S^* \) is the antipode of \( H^* \). To this end, we have that

\[
(S^*(f_1) * f_2)(h) = S^*(f_1)(h_1)f_2(h_2) = f_1(S(h_1))f_2(h_2) = f(S(h_1)h_2) = \epsilon(h)f(1_H)
\]

for all \( f \in H^* \) and \( h \in H \). Similarly,

\[
(f_1 * S^*(f_2))(h) = \epsilon(h)f(1_H)
\]

for all \( h \in H \) and \( f \in H^* \). Therefore, since \( \epsilon_{H^*}(f) = f(1_H) \) and \( 1_{H^*} = \epsilon \), we have that \( S^* \) is the convolution inverse of \( \text{id}_{H^*} \) and therefore \( S^* \) is the antipode of \( H^* \).

**Example 2.2.13.** Let \( G \) be a finite group. Then the dual Hopf algebra \( \mathbb{k}[G]^* \) is another important example of a Hopf algebra. The multiplication in \( \mathbb{k}[G]^* \) is induced by the adjoint of comultiplication in \( \mathbb{k}[G] \) and the comultiplication is induced by the adjoint of multiplication in
\[ \k[G]. \] Moreover, the antipode of \( \k[G] \) is induced by the adjoint of the antipode of \( \k[G] \), which is itself induced by the inverse group operation.

We can describe \( \k[G]^* \) in a simple fashion by considering the canonical basis \( G \) of \( \k[G] \) and the corresponding dual basis \( \{ p_g : g \in G \} \) of \( \k[G]^* \), where

\[ p_g(h) = \delta_{g,h} \]

for all \( g, h \in G \). Then the structure maps of \( \k[G] \) are given by

\[ p_g p_h = \delta_{g,h} p_g, \quad \Delta(p_g) = \sum_{g=ab} p_a \otimes p_b \]

\[ 1_{\k[G]^*} = \sum_{g \in G} p_g, \quad \epsilon(p_g) = \delta_{1,g}, \]

and

\[ S(p_g) = p_{g^{-1}} \]

for all \( g, h \in G \). Note that

\[ \{ p_g : g \in G \} \]

is a set of orthogonal idempotents in \( \k[G]^* \) which sum to the identity of \( \k[G]^* \).

Clearly, for any finite group \( G \), the Hopf algebra \( \k[G]^* \) is commutative, and \( \k[G]^* \) is cocommutative if and only if \( G \) is abelian.

\[ \square \]

**Example 2.2.14.** Let \( H \) and \( K \) be Hopf algebras over \( k \). Then the tensor product \( H \otimes K \) is a Hopf algebra over \( k \) with the tensor product algebra and tensor product coalgebra structures.

The antipode of \( H \otimes K \) is given by \( S_H \otimes S_K \), where \( S_H \) and \( S_K \) are the antipodes of \( H \) and \( K \), respectively.

The next well-studied examples of Hopf algebras, called Taft algebras, will be important in the remainder of this thesis. They are the primary examples of non-commutative, non-cocommutative finite-dimensional Hopf algebras (see [60]).

**Example 2.2.15.** Let \( k \) be an algebraically closed field of characteristic zero. Let \( n \geq 2 \) be a positive integer and let \( \xi \) be a primitive \( n \)-th root of unity in \( k \). Define the Taft algebra \( T_n(\xi) \)
to be the algebra generated by the elements $g$ and $x$ subject to the relations

$$x^n = 0, \ g^n = 1, \ gx = \xi xg.$$  

It follows easily that $T_n(\xi)$ is an $n^2$-dimensional non-commutative algebra with basis

$$\{x^i g^j : 0 \leq i, j \leq n - 1\}.$$  

Moreover, $T_n(\xi)$ has the structure of a Hopf algebra with comultiplication and counit defined by

$$\Delta(g) = g \otimes g, \ \Delta(x) = 1 \otimes x + x \otimes g,$$

$$\epsilon(g) = 1, \ \epsilon(x) = 0$$

and extended linearly and as algebra homomorphisms to all of $T_n(\xi)$. The antipode of the Taft algebra $T_n(\xi)$ is defined by

$$S(g) = g^{-1}, \ S(x) = -xg^{-1}$$

and extended linearly and as an algebra antihomomorphism to all of $T_n(\xi)$. The antipode of the Taft algebra $T_n(\xi)$ is defined by

It is well-known that $T_n(\xi)^* \cong T_n(\xi)$ and $T_n(\xi) \cong T_n(\xi')$ if and only if $\xi = \xi'$. Moreover,

$$G(T_n(\xi)) \cong \mathbb{Z}_n$$

as groups, where $\mathbb{Z}_n \cong \langle g \rangle$ is the cyclic group of order $n$.  

2.2.3 Representation Theory of Hopf Algebras

Throughout this section, let $H$ be a Hopf algebra over the field $k$. Since $H$ is both an algebra and a coalgebra, we have both a category $H \mathcal{M}$ of (left) $H$-modules and a category $\mathcal{M}^H$ of (right) $H$-comodules to consider. When necessary, we will use $H\text{-mod}_{\text{fin}}$ to denote the category of finite-dimensional modules over $H$.

Recall that if $G$ is a finite group, then the category of group representations (or $k[G]$-modules) is a tensor category. Given two (left) $k[G]$-modules $V$ and $W$, we can define a left $k[G]$-module structure on the tensor product $V \otimes W$ by

$$g \cdot (v \otimes w) = g \cdot v \otimes g \cdot w$$
for all \( g \in G, v \in V, \) and \( w \in W. \)

Note also that if \( A \) is any finite-dimensional algebra over \( \mathbb{k} \) and \( V \) is a left \( A \)-module, then the linear dual \( V^* \) always has the structure of a right \( A \)-module by defining

\[
(f \cdot a)(v) = f(a \cdot v)
\]

for all \( f \in V^*, v \in V \) and \( a \in A. \) If happens to be isomorphic to the group algebra \( \mathbb{k}[G] \) for a finite group \( G, \) we can use the inverse group operation to turn \( V^* \) in a left \( A \)-module. In particular, if \( V \) if a left \( \mathbb{k}[G] \)-module then \( V^* \) is also a left \( \mathbb{k}[G] \)-module by defining

\[
(g \cdot f)(v) = f(g^{-1} \cdot v)
\]

for all \( f \in V^*, v \in V, \) and \( g \in G. \)

The category \( \mathcal{H} \mathcal{M} \) of (left) modules over a Hopf algebra \( H \) is also a tensor category with duals using the comultiplication and antipode. Specifically, if \( V \) and \( W \) are left \( H \)-modules, then \( V \otimes W \) is a left \( H \)-modules with action defined by

\[
h \cdot (v \otimes w) = \sum h_1 \cdot v \otimes h_2 \cdot w
\]

(2.13)

for all \( h \in H, v \in V, \) and \( w \in W. \) In addition, \( V^* \) is a left \( H \)-module with action defined by

\[
(h \cdot f)(v) = f(S(h) \cdot v)
\]

(2.14)

for all \( h \in H, f \in V^*, \) and \( v \in V. \) If \( H = \mathbb{k}[G] \) for a finite group \( G, \) these actions correspond to the above discussed actions for the tensor product and dual of group representations.

Similarly, the category \( \mathcal{M}^H \) of (right) \( H \)-comodules is also a tensor category. Given right \( H \)-comodules \( V \) and \( W \) with coactions \( \rho_V : V \rightarrow V \otimes H \) and \( \rho_W : W \rightarrow W \otimes H, \) respectively, we can define a right \( H \)-comodule structure

\[
\rho_{V \otimes W} : V \otimes W \rightarrow V \otimes W \otimes H
\]

on \( V \otimes W \) by defining

\[
\rho_{V \otimes W}(v \otimes w) = \sum v_0 \otimes w_0 \otimes v_1 w_1
\]

(2.15)

for all \( v \in V \) and \( w \in W, \) using Sweedler’s notation for coactions.
Recall that a coalgebra $C$ is called pointed if every simple subcoalgebra of $C$ is one-dimensional. That is, $C$ is pointed if and only if the coradical $C_0$ of $C$ is $k[G(C)]$. In the case that $H$ is a Hopf algebra, we have then that $H$ is pointed if and only if every simple subcoalgebra of $H$ is one-dimensional. In the case that the Hopf algebra is finite-dimensional, we have the following useful characterization of a pointed Hopf algebra.

**Proposition 2.2.16.** Let $H$ be a finite-dimensional Hopf algebra. Then $H$ is pointed if and only if every simple $H^*$-module is one-dimensional.

The space of invariants of an $H$-module and the space of invariants of an $H$-comodule will be defined next. These useful notions will be used throughout.

**Definition 2.2.17.** Let $H$ be a Hopf algebra and let $V$ be a left $H$-module. Then the set

$$V^H = \{v \in V : h \cdot v = \epsilon(h)v \text{ for all } h \in H\}$$

is called the **invariants** of $H$ in $V$. We use same notation for the invariants if $V$ is a right $H$-module.

**Definition 2.2.18.** Let $H$ be a Hopf algebra and let $V$ be a right $H$-comodule with coaction $\rho : V \to V \otimes H$. Then the set

$$V^{\text{co}H} = \{v \in V : \rho(v) = v \otimes 1_H\}$$

is called the **coinvariants** of $H$ in $V$. We use the same notation for the coinvariants if $V$ is a left $H$-comodule.

Note that both the spaces of invariants and coinvariants are vector subspaces of the corresponding modules and comodules, respectively. In fact $V^H$ is a submodule of $V$ whenever $V$ is an $H$-module, and $V^{\text{co}H}$ is a subcomodule of $V$ whenever $V$ is an $H$-comodule.

We next define the notion of a Hopf module over a Hopf algebra. These structures play an important role in the theory of Hopf algebras.

**Definition 2.2.19.** Let $H$ be a Hopf algebra and assume $V$ is a right $H$-module and a right $H$-comodule with coaction $\rho : V \to V \otimes H$. Then $H$ is a right $H$-Hopf module if $\rho$ is a right
$H$-module homomorphism, where $H$ is considered to be a right $H$-module via multiplication
and $V \otimes H$ is given the tensor product module structure described above. In other words, $V$
is a Hopf module if

$$\rho(v \cdot h) = \sum v_0 \cdot h_1 \otimes v_1 h_2$$

for all $v \in V$ and $h \in H$. We can similarly define a left $H$-Hopf module as a left $H$-module
and left $H$-comodule in which the coaction map is a left $H$-module homomorphism.

Denote the category of right $H$-Hopf modules by $M^H_H$ and the category of left $H$-Hopf
modules by $M^H_H$. We can similarly define the category $^H_MH$ consisting of those vector spaces
$V$ which are right $H$-modules and left $H$-comodules such that the coaction $\rho : V \rightarrow H \otimes V$
is a right module homomorphism, and the category $^H_M^H$ consisting of those vector spaces $V$
which are left $H$-modules and right $H$-comodules such that the coaction $\rho : V \rightarrow V \otimes H$ is a
left module homomorphism.

We will also need a slight generalization of Hopf modules. Let $H$ be a Hopf algebra and
$K$ a Hopf subalgebra of $H$. Then $H$ is a left and right $K$-module under multiplication. Then
the category $M^K_H$ of right $(H,K)$-Hopf modules consists of those vector spaces $V$ which are
right $H$-comodules and right $K$-modules such that the coaction $\rho : V \rightarrow V \otimes H$ is a right
$K$-module homomorphism. We also have the other three categories $^H_K M$, $^K_M^H$, and $^H_M K$,
derived similarly.

**Example 2.2.20.** For any Hopf algebra $H$, $H$ is an $H$-Hopf module (of any kind) using
multiplication as the action and comultiplication as the coaction.

**Example 2.2.21.** Let $H$ be a Hopf algebra and let $V$ be any finite-dimensional vector space
equipped with the trivial (right) $H$-module action given by

$$v \cdot h = \epsilon(h)v$$

for all $h \in H$ and $v \in V$. Then $V \otimes H$ is a right $H$-Hopf module with the coaction given by

$$\rho(v \otimes h) = v \otimes h_1 \otimes h_2$$
for all $v \in V$ and $h \in H$, and action given by the tensor product module of $V \otimes H$. That is,

$$(v \otimes h) \cdot k = \epsilon(k_1)v \otimes hk_2 = v \otimes hk$$

for all $h, k \in H$ and $v \in V$. Any right $H$-Hopf module isomorphic to one of the form $V \otimes H$ for some vector space $V$ is called a trivial right Hopf module. Similarly, $H \otimes V$ is a trivial left $H$-Hopf module for any vector space $V$.

The next result, known as the Fundamental Theorem of Hopf Modules, asserts that every Hopf module is in fact trivial.

**Theorem 2.2.22.** [Fundamental Theorem of Hopf Modules] If $V \in \mathcal{M}_H^H$, then $V$ is isomorphic to the trivial right $H$-Hopf module $V^{\text{co}H} \otimes H$.

**Proof.** Define the linear maps $\phi : V^{\text{co}H} \otimes H \rightarrow V$ and $\psi : V \rightarrow V \otimes H$ by

$$\phi(w \otimes h) = w \cdot h \quad \text{and} \quad \psi(v) = v_0 \cdot S(v_1) \otimes v_2$$

for all $h \in H$, $v \in V$, and $w \in V^{\text{co}H}$, where we are denoting the right action of $H$ on $V$ using $\cdot$ and the right coaction by

$$\rho(v) = v_0 \otimes v_1$$

for all $v \in V$ as usual.

First we claim that $\psi(V) \subseteq V^{\text{co}H} \otimes H$. To see this, note that

$$\rho(v_0 \cdot S(v_1)) = (v_0 \cdot S(v_1))_0 \otimes (v_0 \cdot S(v_1))_1$$

$$= v_0 \cdot S(v_2)_1 \otimes v_1 S(v_2)_2$$

$$= v_0 \cdot S(v_3)_1 \otimes v_1 S(v_2)$$

$$= v_0 \cdot S(v_2) \otimes \epsilon(v_1)_1$$

$$= v_0 \cdot S(v_1) \otimes 1_H$$

since $V$ is a Hopf module and $S$ is a coalgebra antihomomorphism. This implies that $v_0 \cdot S(v_1) \in V^{\text{co}H}$ for all $v \in V$. 
Next we verify that $\phi$ and $\psi : V \rightarrow V^\text{co} H \otimes H$ are bijections by showing that $\psi = \phi^{-1}$.

First,

$$\phi (\psi(v)) = \phi (v_0 \cdot S(v_1) \otimes v_2)$$

$$= (v_0 \cdot S(v_1)) \cdot v_2$$

$$= v_0 \cdot S(v_1)v_2$$

$$= \epsilon(v_1)v_0 \cdot 1_H$$

$$= v$$

for all $v \in V$. Secondly,

$$\psi (\phi(v \otimes h)) = \psi (v \cdot h)$$

$$= (v \cdot h)_0 \cdot S ((v \cdot h)_1) \otimes (v \cdot h)_2$$

$$= (v_0 \cdot h_1) \cdot S ((v_1h_2)_1) \otimes (v_1h_2)_2$$

$$= (v_0 \cdot h_1) \cdot S (v_1h_2) \otimes v_2h_3$$

$$= v_0 \cdot h_1S(h_2)S(v_1) \otimes v_2h_3$$

$$= v_0 \cdot S(v_1) \otimes v_2\epsilon(h_1)h_2$$

$$= v_0 \cdot S(v_1) \otimes v_2h$$

and using the fact that $\rho(v) = v \otimes 1_H$, we have that

$$\psi (\phi(v \otimes h)) = v_0 \cdot S(v_1) \otimes v_2h$$

$$= v \cdot S(1_H) \otimes h$$

$$= v \otimes h$$

for all $v \in V^\text{co} H$ and $h \in H$. Therefore $\phi \circ \psi = \text{id}_V$ and $\psi \circ \phi = \text{id}_{V^\text{co} H \otimes H}$.

Lastly, we need to show that $\phi$ is an $H$-module homomorphism and an $H$-comodule homo-
morphism. To see that $\phi$ is an $H$-module homomorphism, note that

$$
\phi \left( (v \otimes h) \cdot k \right) = \phi (v \otimes hk) \\
= v \cdot hk \\
= (v \cdot h) \cdot k \\
= \phi (v \otimes h) \cdot h
$$

for all $h, k \in H$ and $v \in V^{coH}$. To see that $\phi$ is an $H$-comodule homomorphism, we note that

$$
\rho \left( \phi (v \otimes h) \right) = \rho (v \cdot h) \\
= (v \cdot h)_0 \otimes (v \cdot h)_1 \\
= v_0 \cdot h_1 \otimes v_1 h_2 \\
= v \cdot h_1 \otimes 1_H h_2 \\
= v \cdot h_1 \otimes h_2 \\
= (\phi \otimes \text{id}_H) (v \otimes h_1 \otimes h_2) \\
= (\phi \otimes \text{id}_H) (\rho' (v \otimes h))
$$

for all $v \in V^{coH}$ and $h \in H$, since $V$ is a Hopf module and

$$
\sum v_0 \otimes v_1 = v \otimes 1_H.
$$

Here we have denoted by $\rho'$ the coaction

$$
\rho' : V \otimes H \to V \otimes H \otimes H
$$

of the trivial $H$-Hopf module $V \otimes H$. Therefore we have shown that $V \cong V^{coH} \otimes H$ as Hopf modules, finishing the proof.

\[\square\]

2.3 Further Hopf Algebra Theory

2.3.1 Integrals

Assume throughout that $H$ is a finite-dimensional Hopf algebra over a field $\mathbb{k}$. The next main object of our attention for the moment will be the invariants of $H$ in the regular rep-
presentation of $H$. These invariants, called integrals, play an extremely important part in the study of finite-dimensional Hopf algebras.

**Definition 2.3.1.** A left integral in $H$ is an element $\Lambda \in H$ such that

$$h\Lambda = \epsilon(h)\Lambda$$

for all $h \in H$. Similarly, a right integral in $H$ is an element $\Gamma \in H$ such that

$$\Gamma h = \epsilon(h)\Gamma$$

for all $h \in H$.

It is easy to see that the set of left integrals and the set of right integrals in $H$ are both linear subspaces of $H$. We denote by $\mathcal{I}_l^l$ the space of left integrals in $H$ and by $\mathcal{I}_r^r$ the space of right integrals in $H$. Obviously $\mathcal{I}_l^l$ is a left ideal of $H$ and $\mathcal{I}_r^r$ is a right ideal of $H$. In fact, noting that

$$h(\Lambda k) = \epsilon(h)\Lambda k \quad \text{and} \quad (k\Gamma)h = \epsilon(h)k\Gamma$$

by associativity, for all $h, k \in H$, $\Lambda \in \mathcal{I}_l^l$, and $\Gamma \in \mathcal{I}_r^r$, we have that $\mathcal{I}_l^l$ is also a right ideal of $H$ and $\mathcal{I}_r^r$ is also a left ideal of $H$.

**Remark 2.3.2.** An element $\gamma \in H^*$ is a left integral in $H^*$ if and only if

$$f(h_1)\gamma(h_2) = (f * \gamma)(h) = \epsilon(f)\gamma(h) = f(1_H)\gamma(h)$$

for all $h \in H$ and $f \in H^*$. Therefore $\gamma \in \mathcal{I}_l^{l^*}$ is equivalent to

$$\gamma(h_2)h_1 = \gamma(h)1_H$$

(2.16)

for all $h \in H$. Similarly, $\lambda \in \mathcal{I}_r^{r^*}$ if and only if

$$\lambda(h_1)h_2 = \lambda(h)1_H$$

(2.17)

for all $h \in H$. 

Example 2.3.3. Let $G$ be a finite group. Then

$$\Lambda = \sum_{g \in G} g \in k[G]$$

is easily seen to be both a left and right integrals in $k[G]$, and every integral in $k[G]$ is a scalar multiple of $\Lambda$. In addition,

$$p_{1_G} \in k[G]^*$$

generates both the left and right integrals of $k[G]^*$, where

$$p_{1_G}(g) = \delta_{1_G,g}$$

for all $g \in G$.

A Hopf algebra $H$ such that $\int_H^l = \int_H^r$ is said to be unimodular. As the above examples demonstrate, both $k[G]$ and $k[G]^*$ are unimodular for any finite group $G$.

Example 2.3.4. The Taft algebra $T_n(\xi)$ is not unimodular for any $n \geq 2$ and $\xi$ a primitive $n$-th root of unity. For example, the four-dimensional Taft algebra $T_2 = T_2(-1)$ is not unimodular since $\int_{T_2}^l = k[x + gx]$ and $\int_{T_2}^r = k[x - gx]$.

In both of the above examples, the spaces of left and right integrals are one-dimensional. That is, the left and right integrals in these Hopf algebras exist and are unique up to a scalar multiple. The existence and uniqueness of integrals in a general finite-dimensional Hopf algebra will be established next, as shown by Larson and Sweedler [31], but to show this we first need to establish that the dual $H^*$ of any finite-dimensional Hopf algebra $H$ is a right $H$-Hopf module using an appropriate action and coaction.

Continue to denote by $H$ a finite-dimensional Hopf algebra. Define the left action

$$\rightarrow: H \otimes H^* \rightarrow H^*$$

of $H$ on $H^*$ by

$$(h \rightarrow f)(k) = f(kh) \quad (2.18)$$

and the right action

$$\leftarrow: H^* \otimes H \rightarrow H^*$$
of $H$ on $H^*$ by

$$ (f \leftarrow h)(k) = f(hk) \quad (2.19) $$

for all $f \in H^*$ and $h, k \in H$. Now define the right action $\leftarrow$ of $H$ on $H^*$ and the left action $\rightarrow$ of $H$ on $H^*$ by

$$ f \leftarrow h = S(h) \rightarrow f \quad \text{and} \quad h \rightarrow f = f \leftarrow S(h) \quad (2.20) $$

for all $f \in H^*$ and $h \in H$.

We note that, given $h \in H$ and $f, g \in H^*$

$$ (h \rightarrow f \ast g)(k) = f(k_1h_1)g(k_2h_2) = (h_1 \rightarrow f) \ast (h_2 \rightarrow g)(k) $$

for all $k \in H$. Therefore

$$ h \rightarrow (f \ast g) = (h_1 \rightarrow f) \ast (h_2 \rightarrow g) \quad (2.21) $$

for all $h \in H$ and $f, g \in H^*$.

As we have already seen, since $H^*$ is a left $H^*$-module under multiplication, we have that $H^*$ is a right $H$-comodule. If we let $\{\phi_1, \phi_2, \cdots, \phi_n\}$ be a basis for $H^*$ and $f \in H^*$, then there exist $h_1, h_2, \cdots, h_n \in H$ such that

$$ g \ast f = \sum_{i=1}^{n} g(h_i)\phi_i = \sum_{(f)} g(f_1)f_0 $$

for all $g \in H^*$. The coaction $\rho : H^* \rightarrow H^* \otimes H$ is then given by

$$ \rho(f) = \sum f_0 \otimes f_1 $$

for all $f \in H^*$, where

$$ g \ast f = \sum g(f_1)f_0 $$

for all $g \in H^*$.

**Lemma 2.3.5.** Let $H$ be a finite-dimensional Hopf algebra. Then $H^*$ is a right $H$-Hopf module using the action and coaction

$$ \leftarrow : H^* \otimes H \rightarrow H^* \quad \text{and} \quad \rho : H^* \rightarrow H^* \otimes H $$

as above.
Now we use this lemma to show some very important properties of finite-dimensional Hopf algebras. We will not only show that every finite-dimensional Hopf algebra contains a unique left integral and unique right integral (up to scalar multiplication) but this will also allow us to show that the antipode $S$ of any finite-dimensional Hopf algebra $H$ is a linear bijection.

**Proposition 2.3.6.** Let $H$ be a finite-dimensional Hopf algebra over $\mathbb{k}$ with antipode $S$. Then $\int^l_H$ and $\int^r_H$ are both one-dimensional. In addition, $S$ is bijective and $S \left( \int^l_H \right) = \int^r_H$.

**Proof.** First we show that $\dim \left( \int^l_H \right) = 1$. By Lemma 2.3.5, $H^* \in \mathcal{M}_H^H$ and so by the Fundamental Theorem of Hopf Modules,

$$H^* \cong (H^*)^{co H} \otimes H$$

as Hopf modules, where the right side is a trivial $H$-Hopf module and

$$(H^*)^{co H} = \{ f \in H^* : \rho(f) = f \otimes 1_H \}$$

where $\rho(f) = \sum f_0 \otimes f_1$ is the coaction defined by

$$g * f = \sum g(f_1)f_0$$

for all $g \in H^*$. Since $\dim H^* = \dim H$, we have that $\dim (H^*)^{co H} = 1$. But $(H^*)^{co H} = \int^l_{H^*}$ and so $\dim \left( \int^{l}_{H^*} \right) = 1$. Since $(H^*)^{*} \cong H$, replacing $H$ with $H^*$ gives the desired result. A similar proof shows that $\dim \left( \int^{r}_H \right) = 1$.

To show that $S : H \rightarrow H$ is bijective, it suffices to show that $S$ is injective since $H$ is a finite-dimensional vector space. In the proof of Theorem 2.2.22, we saw that the map

$$\phi : \int^l_{H^*} \otimes H \rightarrow H^*$$

defined by

$$\phi(\lambda \otimes h) = \lambda \leftarrow h$$

is a linear bijection. To show that $S$ is injective, assume that $\lambda$ is a non-zero integral in $H^*$ and $h \in H$ such that $S(h) = 0$. We have

$$\lambda \leftarrow h = S(h) \rightarrow \lambda = 0$$
which implies that $h = 0$ by the bijectivity of the above map. This proves that $S$ is injective and also bijective.

Lastly, to see that $S \left( \int_H^l \right) = \int_H^r$, we simply calculate. For any $h \in H$ and $\Lambda \in \int_H^l$,

$$S(\Lambda)h = S \left( S^{-1}(h)\Lambda \right) = S \left( \epsilon \left( S^{-1}(h) \right) \Lambda \right) = \epsilon(h)S(\Lambda)$$

since $\epsilon \circ S^{-1} = \epsilon$, which shows that $S(\Lambda) \in \int_H^r$, finishing the proof. \qed

Next we introduce a special group-like element defined in every finite-dimensional Hopf algebra using integrals. Let $\Lambda \in H$ be a non-zero left integral of $H$. Since $\Lambda h \in \int_H^l$ for any $h \in H$ and $\int_H^l$ is one-dimensional, it follows that there exists an element $\alpha(h) \in k$ such that

$$\Lambda h = \alpha(h)\Lambda.$$

It is easy to see that $\alpha$ defines a linear functional in $H^*$. In fact, $\alpha \in \text{Alg}(H,k)$ since

$$\alpha(h)\alpha(k)\Lambda = \Lambda hk = \alpha(hk)\Lambda$$

for all $h, k \in H$, and hence $\alpha \in G(H^*)$. We refer to $\alpha \in G(H^*)$ as the **distinguished group-like element** of $H^*$, and it is obvious that $\alpha$ is independent of the choice of $\Lambda \in \int_H^l$. Dually, if we consider a non-zero right integral $\lambda \in H^*$, there exists $g \in G(H)$ such that

$$f \ast \lambda = f(g)\lambda$$

for all $f \in H^*$. We call $g \in G(H)$ the distinguished group-like element of $H$. Note that if $g \in G(H)$ is the distinguished group-like element of $H$, then

$$f(h_1)\lambda(h_2) = f(g)\lambda(h)$$

for all $h \in H$ and $f \in H^*$, and hence this is equivalent to

$$\lambda \mapsto h = \lambda(h)g$$

for all $h \in H$, where we are denoting

$$\mapsto: H^* \otimes H \to H$$
as the left action of $H^*$ on $H$ defined by

$$f \mapsto h = \sum f(h_2)h_1$$

(2.22)

for all $f \in H^*$ and $h \in H$. We can also similarly define

$$\leftarrow: H \otimes H^* \to H$$

as the right action of $H^*$ on $H$ defined by

$$h \leftarrow f = \sum f(h_1)h_2$$

(2.23)

for all $f \in H^*$ and $h \in H$. Note that we are using the same symbols to define these actions as in (2.18) and (2.19), but it should be clear from context which action we are referring to.

It is worth noting that since $g \in G(H)$ and $\alpha \in G(H^*)$, both $g$ and $\alpha$ are invertible elements of $H$ and $H^*$, respectively, and that both of these elements have finite order if $H$ is finite-dimensional. Note also that $H$ is unimodular if and only if $\alpha = 1_H$ and $H^*$ is unimodular if and only if $g = 1_H$, where $\alpha$ and $g$ are the distinguished group-like elements of $H^*$ and $H$, respectively.

The antipode of a finite-dimensional Hopf algebra $H$ is closely connected to the distinguished group-like elements of $H$ and $H^*$. This is established in the following celebrated result of Radford [49].

**Theorem 2.3.7.** Let $H$ be a finite-dimensional Hopf algebra with antipode $S$. Assume that $g \in G(H)$ and $\alpha \in G(H^*)$ are the distinguished group-like elements of $H$ and $H^*$, respectively, as defined above. Then

$$S^4(h) = g (\alpha \mapsto h \leftarrow \alpha^{-1}) \ g^{-1}$$

for all $h \in H$.

This result implies that, for a finite-dimensional Hopf algebra over $k$, the order of the antipode is always finite. In particular,

$$\text{ord}(S^2) \mid 2 \cdot \text{lcm} (\text{ord}(g), \text{ord}(\alpha))$$

(2.24)
where \( \text{ord}(g) \) and \( \text{ord}(\alpha) \) are finite since \( \dim H \) is finite. For example, if \( H \) and \( H^* \) are unimodular, then \( S^4 = \text{id}_H \).

To close this subsection, we prove that every finite-dimensional Hopf algebra is a Frobenius algebra. Recall by Proposition 2.3.6 that every finite-dimensional Hopf algebra contains an integral that is unique up to a scalar. Any non-zero integral \( \lambda \in H^* \) defines the corresponding non-degenerate associative bilinear form on \( H \).

**Proposition 2.3.8.** Let \( H \) be a finite-dimensional Hopf algebra over \( k \) and let \( \lambda \in H^* \) be a non-zero integral in \( H^* \). Then the bilinear form \( \beta : H \rightarrow k \) defined by

\[
\beta(h, k) = \lambda(hk)
\]

is non-degenerate. In particular, this is a non-degenerate bilinear associative form on \( H \), and hence \( H \) is a Frobenius algebra.

### 2.3.2 Semisimplicity of Hopf Algebras

We refer to Hopf algebra as **semisimple** if it is semisimple as an algebra. We next discuss the relationship between the semisimplicity of a finite-dimensional Hopf algebra over \( k \) and the antipode and integrals of the Hopf algebra. The first result deals with the integral and its relationship to the semisimplicity of a Hopf algebra, which generalizes Mashke’s Theorem for group algebras of finite groups. This result can be found in [37], [54], and [59].

**Theorem 2.3.9.** Let \( H \) be a finite-dimensional Hopf algebra over \( k \) and let \( \Lambda \in \mathcal{I}_H^l \) be a left non-zero integral and \( \Gamma \in \mathcal{I}_H^r \) be a right non-zero integral in \( H \). Then \( H \) is semisimple if and only if \( \epsilon(\Lambda) \neq 0 \), and also \( H \) is semisimple if and only if \( \epsilon(\Gamma) \neq 0 \).

**Proof.** First assume that \( H \) is semisimple, which is equivalent to every \( H \)-module being completely reducible. Since \( \ker \epsilon \) is an ideal of \( H \), it is a left \( H \)-submodule of the regular representation \( H^*H \). Therefore, there exists a left ideal \( I \) of \( H \) such that

\[
H = I \oplus \ker \epsilon.
\]
For any $z \in I$ and $h \in H$, we have that

$$h - \epsilon(h)1 \in \ker \epsilon$$

and hence

$$(h - \epsilon(h)1_H)z \in \ker \epsilon.$$ Therefore

$$hz = (h - \epsilon(h)1_H)z + \epsilon(h)z = \epsilon(h)z$$

since $z \in I$, which implies that $I \subseteq \int_H^l$. Note that $\ker \epsilon \neq H$ since $\epsilon(1_H) = 1$, and hence $I = \int_H^l$ since $\int_H^l$ is one-dimensional. Therefore, for any non-zero left integral $\Lambda$, we have that $\Lambda \notin \ker \epsilon$. Similarly, for any non-zero $\Gamma \in \int_H^r$, $\epsilon(\Gamma) \neq 0$.

Conversely, assume that $\epsilon\left(\int_H^l\right) \neq 0$. Let $\Lambda \in \int_H^l$ such that $\epsilon(\Lambda) = 1$. We show that any $H$-module is completely reducible. To that end, let $V$ be an $H$-module with a submodule $W$, with $\pi : V \to W$ any linear projection map. Now define $\pi' : V \to W$ by

$$\pi'(v) = \sum \Lambda_1 \cdot \pi(S(\Lambda_2) \cdot v)$$

for all $v \in V$, where $\Delta(\Lambda) = \Lambda_1 \otimes \Lambda_2$. Our goal is then to show that $\pi'$ is an $H$-module projection onto $W$.

First note that if $w \in W$, then

$$\pi'(w) = \sum \Lambda_1 \cdot \pi(S(\Lambda_2) \cdot w)$$

$$= \sum \Lambda_1 \cdot (S(\Lambda_2) \cdot w)$$

$$= \sum \Lambda_1 S(\Lambda_2) \cdot w$$

$$= \epsilon(\Lambda) \cdot w = w$$

since $\pi$ is a projection to $W$, $\epsilon(\Lambda) = 1$, and by the antipode property of $S$. Since $\pi'$ is clearly linear, we have then that $\pi'$ is a linear projection onto $W$.

Lastly, we show that $\pi'$ is an $H$-module homomorphism. It is first worth noting that

$$\Delta(\Lambda) \otimes h = \Delta(h_1) \otimes \epsilon(h_1)h_2 = \Delta(h_1\Lambda) \otimes h_2$$

$$= \Delta(h_1\Lambda) \otimes h_2 = h_1\Lambda_1 \otimes h_2\Lambda_2 \otimes h_3$$
for all \( h \in H \), since \( \Lambda \in \mathcal{I}_H \). Therefore, for any \( v \in V \) and \( h \in H \), we have

\[
\pi'(h \cdot v) = \Lambda_1 \cdot \pi(S(\Lambda_2) \cdot (h \cdot v))
\]

\[
= h_1 \Lambda_1 \cdot \pi(S(h_2 \Lambda_2) \cdot (h_3 \cdot v))
\]

\[
= h_1 \Lambda_1 \cdot \pi(S(\Lambda_2)S(h_2)h_3 \cdot v)
\]

\[
= h \Lambda_1 \cdot \pi(S(\Lambda_2) \cdot v)
\]

\[
= h \cdot \pi'(v)
\]

and so \( \pi' : V \to W \) is an \( H \)-module projection map. We therefore have that \( \ker \pi' \) is an \( H \)-module complement for \( W \) in \( V \), and so \( V \) is completely reducible. This implies that \( H \) is semisimple. A similar argument works for right integrals.

Remark 2.3.10. Let \( G \) be a finite group and \( k \) any field. Then as mentioned before,

\[
\Lambda = \sum_{g \in G} g
\]

generates the space of integrals of \( k[G] \). Mashke’s Theorem states that \( k[G] \) is semisimple if and only if \( |G| \) does not divide the characteristic of \( k \). However, \( |G| = \epsilon(\Lambda) \), and so \( \epsilon(\Lambda) \neq 0 \) if and only if \( |G| \) does not divide the characteristic of \( k \). Therefore the above result does indeed generalize Mashke’s Theorem to finite-dimensional Hopf algebras. For this reason, the above theorem is often referred to as Mashke’s Theorem for Hopf algebras.

Finite-dimensional Hopf algebras over an algebraically closed field \( k \) of characteristic zero also enjoy an intimate connection between the antipode of the Hopf algebra and the semisimplicity of the Hopf algebra. For a finite group \( G \) and an algebraically closed field \( k \) of characteristic 0, it is obvious by Mashke’s Theorem that \( k[G] \) is semisimple. Moreover, the dual Hopf algebra \( k[G]^* \) is also semisimple. The fact that the antipodes of these Hopf algebras, which are induced by the inversion operation of the group \( G \), have order 2 is not a coincidence. The next result, proven by Larson and Radford [29, 30], will be extremely important in our study of Hopf algebras, both semisimple and non-semisimple.

**Theorem 2.3.11.** Let \( H \) be a finite-dimensional Hopf algebra with antipode \( S \) over the algebraically closed field \( k \) of characteristic 0. Then the following statements are equivalent:
1. \( H \) is semisimple.

2. \( H^* \) is semisimple.

3. \( S^2 = \text{id}_H \).

4. \( \text{Tr}(S^2) \neq 0 \).

Note that \( H^* \) is semisimple if and only if \( H \) is cosemisimple as a coalgebra. As a result of this powerful theorem, we can easily show that any cocommutative or commutative Hopf algebra over an algebraically closed field of characteristic zero is trivial. We say a Hopf algebra \( H \) is trivial if there exists a group \( G \) such that \( H \cong \mathbb{k}[G] \) or \( H \cong \mathbb{k}[G]^* \).

**Corollary 2.3.12.** Let \( \mathbb{k} \) be an algebraically closed field of characteristic zero.

(a) If \( H \) is a commutative Hopf algebra over \( \mathbb{k} \), then \( H \cong \mathbb{k}[G]^* \) for some group \( G \) with \( |G| = \dim H \).

(b) If \( H \) is a cocommutative Hopf algebra over \( \mathbb{k} \), then \( H \cong \mathbb{k}[G] \) for some group \( G \) with \( |G| = \dim H \).

**Proof.** To prove the first part, we first show that if \( H \) is commutative, then \( S^2 = \text{id}_H \), where \( S \) is the antipode of \( H \). To show that \( S^2 = \text{id}_H \), it suffices to show that \( S^2 \) is the convolution inverse of the antipode \( S \). Note that for any \( h \in H \)

\[
(S * S^2)(h) = S(h_1)S^2(h_2) \\
= S^2(h_2)S(h_1) \\
= S(h_1S(h_2)) \\
= \epsilon(h)S(1_H) \\
= \epsilon(h)1_H
\]

and so \( S^2 \) is the (right) convolution inverse of \( S^2 \). Therefore \( S^2 = \text{id}_H \).

Now, by Theorem 2.3.11, this implies that \( H \) is semisimple and so, as an algebra, \( H \) is a direct product of matrix algebras. Since \( \mathbb{k} \) is algebraically closed and commutative, we know
that
\[ H \cong k \times k \times \cdots \times k \]
as an algebra, where \( k \) appears \( n = \dim H \) times. In particular, this implies that there are exactly \( n \) algebra homomorphisms from \( H \) to \( k \). In other words, \( H^* \) has exactly \( n \) group-like elements and so, by the linear independence of group-like elements, \( H^* \cong k[G] \) for some finite group \( G \) with \( |G| = \dim H \). It then follows by duality that \( H \cong k[G]^* \).

The second statement follows from the first by noting that \( (H^*)^* \cong H \) and if \( H \) is cocommutative, then \( H^* \) is commutative. \( \square \)

### 2.3.3 The Nichols-Zoeller Theorem

As we have seen, many of the nice properties of finite groups and group algebras actually hold for general finite-dimensional Hopf algebras. We discuss next another such result, the Nichols-Zoeller Theorem \([45]\), which is of fundamental importance in the study of finite-dimensional Hopf algebras and their classifications. This result will generalize the classic Lagrange Theorem for groups, which states that the order of a subgroup of a finite group divides the order of the group.

**Theorem 2.3.13** (Nichols-Zoeller Theorem). Let \( H \) be a finite-dimensional Hopf algebra over \( k \) and let \( K \) be a Hopf subalgebra of \( H \). Then every right \((H,K)\)-Hopf module is free as a right \( K \)-module. In particular, since \( H \in \mathcal{M}_K^H \) we have that \( H \) is a free right \( K \)-module.

So if \( H \) is a finite-dimensional Hopf algebra and \( K \) is a Hopf subalgebra of \( H \), this theorem implies that \( \dim K \) divides \( \dim H \). This is the obvious generalization of the Lagrange Theorem in group theory, since \( k[A] \) is a Hopf subalgebra of \( k[G] \) for any subgroup \( A \) of \( G \).

**Corollary 2.3.14.** Let \( H \) be a finite-dimensional Hopf algebra over \( k \). If \( K \) is a Hopf subalgebra of \( H \), then \( \dim K \) divides \( \dim H \). In particular, \( |G(H)| \) divides \( \dim H \) and \( \text{ord}(g) \) divides \( \dim H \) for any \( g \in G(H) \).

**Proof.** The first statement follows immediately by the Nichols-Zoeller Theorem since \( H \) is a free \( K \)-module. The second statement follows from the fact that \( k[G(H)] \) is a Hopf subalgebra.
of $H$ of dimension $|G|$ and $\text{ord}(g)$ divides $|G|$ for any $g \in G$.

### 2.3.4 Extensions of Hopf Algebras

Recall that for a group $G$, a subgroup $N$ is called normal if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Using the antipode, we generalize this definition to Hopf algebras.

**Definition 2.3.15.** Let $H$ be a Hopf algebra over $\mathbb{k}$. Then a Hopf subalgebra $A$ of $H$ is called **normal** if

$$\sum h_1 a S(h_2) \in A \quad \text{and} \quad \sum S(h_1) a h_2 \in A$$

for all $h \in H$ and $a \in A$.

Clearly $\mathbb{k}[1_H] \cong \mathbb{k}$ and $H$ are both trivial examples of normal Hopf subalgebras for any Hopf algebra $H$. We next give some useful equivalent formulations of normal Hopf subalgebras, which can be found in [37, Section 3.4] and [40, Corollary 16]. For any Hopf subalgebra $A$ of $H$, let $A^+ = A \cap \ker \epsilon$ where $\epsilon$ is the counit of $H$.

**Proposition 2.3.16.** Let $A$ be a Hopf subalgebra of the finite-dimensional Hopf algebra $H$. Then the following statements are equivalent.

1. $A$ is a normal Hopf subalgebra of $H$.
2. $A^+ H = HA^+$
3. $A^+ H \subseteq HA^+$ or $HA^+ \subseteq A^+ H$

We also have that if $A$ is a normal Hopf subalgebra of $H$, then $A^+ H = HA^+$ is a Hopf ideal of $H$, since $A^+ H = HA^+$ implies $A^+ H$ is an ideal of $H$ and the facts that

$$\Delta(A^+ H) \subseteq \Delta(A^+) \Delta(H) \quad \text{and} \quad \epsilon(A^+ H) \subseteq \epsilon(A^+) \epsilon(H) = 0$$

imply that $A^+ H$ is a coideal of $H$. We can therefore consider the quotient Hopf algebra $H/(A^+ H)$. Moreover, if $\pi : H \to H/(A^+ H)$ is the usual Hopf algebra surjection, then

$$A = H^{\text{co}\pi} = \{h \in H : (\text{id}_H \otimes \pi)\Delta(h) = h \otimes 1_{H/(A^+ H)}\}.$$
Now with the notion of normal Hopf subalgebras, we can define an extension of Hopf algebras. Following [53], we say that a sequence
\[ 1 \longrightarrow A \xrightarrow{i} H \xrightarrow{\pi} B \longrightarrow 1 \] (2.25)
of finite-dimensional Hopf algebras is **exact** if \( i \) and \( \pi \) are injective and surjective Hopf algebra homomorphisms, respectively, such that \( i(A) \) is a normal Hopf subalgebra of \( H \) and \( \ker \pi = H\iota(A)^+ \). In this case, we say that \( H \) is a Hopf algebra **extension** of \( B \) by \( A \). In the exact sequence we are denoting by 1 the trivial Hopf algebra isomorphic to \( k \).

By duality, we can consider the dual sequence of the above exact sequence (2.25) given by
\[ 1 \longrightarrow B^* \xrightarrow{\pi^*} H^* \xrightarrow{\iota^*} A^* \longrightarrow 1 \] (2.26)
in which it is obvious that \( \pi^* \) and \( \iota^* \) are injective and surjective Hopf algebra homomorphisms, respectively. Furthermore, the sequence (2.26) is also an exact sequence of Hopf algebras. That is, a finite-dimensional Hopf algebra \( H \) is an extension of \( B \) by \( A \) if and only if \( H^* \) is an extension of \( A^* \) by \( B^* \).

Next we discuss the notion of a crossed product which will be used to prove our main results. Let \( A \) be an algebra over \( k \) and let \( H \) be a Hopf algebra over \( k \) and suppose there is a \( k \)-linear map \( H \otimes A \rightarrow A \) denoted by \( \cdot \) such that
\[ h \cdot 1_A = \epsilon(h)1_A \quad \text{and} \quad h \cdot ab = \sum (h_1 \cdot a)(h_2 \cdot b) \]
for all \( h \in H \) and \( a, b \in A \). Let \( \sigma : H \otimes H \rightarrow A \) be a \( k \)-linear map which is invertible in the convolution algebra \( \text{Hom}_k(H \otimes H, A) \). We denote \( \sigma(h \otimes k) \) by \( \sigma(h, k) \) for all \( h, k \in H \). Also denote by \( \overline{\sigma} \) the convolution inverse of \( \sigma \).

**Definition 2.3.17.** Let \( H \), \( A \), and \( \sigma \) be as above. Denote by \( A \#_\sigma H \) the set \( A \otimes H \) as a vector space with multiplication given by
\[ (a \# h)(b \# k) = \sum a(h_1 \cdot b)\sigma(h_2, k_1) \# h_3 k_2 \]
for all \( h, k \in H \) and \( a, b \in A \). We call \( A \#_\sigma H \) a **crossed product algebra** if the multiplication is associative and \( 1_A \# 1_H \) is the multiplicative identity of \( A \#_\sigma H \).
Here we denote by \( a \# h \) the element \( a \otimes h \) in the crossed product algebra \( A \#_\sigma H \), for each \( a \in A \) and \( h \in H \). See [37, Chapter 7] for more information about crossed products. If \( A \) and \( H \) are as above, then from [8] and [13] we know that \( A \#_\sigma H \) is a crossed product algebra if and only if

\[
h \cdot (k \cdot a) = \sum \sigma(h_1, k_1)(h_2 k_2 \cdot a)\sigma(h_3, k_3)
\]

for all \( h, k \in H \) and \( a \in A \), and \( \sigma \) is a normalized 2-cocycle. That is,

\[
\sigma(h, 1_H) = \sigma(1_H, h) = \epsilon(h)1_H
\]

for all \( h \in H \), and

\[
\sum [h_1 \cdot \sigma(k_1, l_1)]\sigma(h_2, k_2 l_2) = \sigma(h_1, k_1)\sigma(h_2 k_2, l)
\]

for all \( h, k, l \in H \). See also [12, Chapter 6] for a proof of this fact.

We next give another characterization of crossed products which will prove useful. Let \( A \) and \( B \) algebras over \( k \) and \( H \) a Hopf algebra over \( k \). Following [37], we say that an inclusion \( i : A \hookrightarrow B \) of \( k \)-algebras is a right \( H \)-extension of \( A \) if \( B \) is a right \( H \)-comodule, with structure map \( \rho : B \to B \otimes H \), such that

\[
\rho(bc) = \sum b_0 c_0 \otimes b_1 c_1 \quad \text{and} \quad \rho(1_B) = 1_B \otimes 1_H
\]

for all \( b, c \in B \), and \( i(A) = B^{coH} \) where

\[
B^{coH} = \{ b \in B : \rho(b) = b \otimes 1_H \}.
\]

We further say the right \( H \)-extension \( i : A \hookrightarrow B \) is \( H \)-cleft if there exists a right \( H \)-comodule map \( \gamma : H \to B \) which is convolution invertible in the convolution algebra \( \text{Hom}_k(H, B) \) and \( \gamma(1_H) = 1_B \). Denote by \( \overline{\gamma} \) the convolution inverse of \( \gamma \). The characterization we seek is found in the following result of Blattner and Montgomery [9, Theorem 1.18].

**Theorem 2.3.18.** A right \( H \)-extension \( i : A \hookrightarrow B \) is \( H \)-cleft if and only if \( B \cong A \#_\sigma H \) as a crossed product for some normalized 2-cocycle \( \sigma : H \otimes H \to A \).

In particular, if the \( H \)-extension \( i : A \hookrightarrow B \) is \( H \)-cleft via \( \gamma : H \to B \), then the crossed product \( B \cong A \#_\sigma H \) is given by the linear map \( H \otimes A \to A \) defined by

\[
h \cdot a = \sum \gamma(h_1)a\overline{\gamma}(h_2)
\]
for all \( h \in H \) and \( a \in A \), and the normalized 2-cocycle is given by

\[
\sigma(h, k) = \sum \gamma(h_1)\gamma(k_1)\overline{\gamma}(h_2k_2)
\]

for all \( h, k \in H \). Conversely, if \( A\#_\sigma H \) is a crossed product then we define \( \gamma : H \to A\#_\sigma H \) and its convolution inverse \( \overline{\gamma} \) by

\[
\gamma(h) = 1_{A\#} \quad \text{and} \quad \overline{\gamma}(h) = \sum \overline{\sigma}(S(h_2), h_3) \#S(h_1)
\]

for all \( h \in H \), where \( S \) is the antipode of \( H \). It follows that the \( H \)-extension \( A \hookrightarrow A\#_\sigma H \) is \( H \)-cleft.

In this case, the algebra isomorphism \( \Phi : A\#_\sigma H \to B \) given by

\[
\Phi(a\# h) = a\gamma(h)
\]

for all \( a \in A \) and \( h \in H \) is both a left \( A \)-module and right \( H \)-comodule homomorphism. Here, \( A\#_\sigma H \) is a left \( A \)-module via

\[
b \cdot (a\# h) = ba\# h
\]

and a right \( H \)-comodule via

\[
\rho(a\# h) = a\# h_1 \otimes h_2
\]

for all \( a, b \in A \) and \( h \in H \).

The next theorem follows from results of Schneider [52].

**Theorem 2.3.19.** Let \( H \) and \( K \) be finite-dimensional Hopf algebras and \( \pi : H \to K \) a Hopf algebra surjection. If

\[
H^{\co \pi} = \{ h \in H : (\text{id}_H \otimes \pi)\Delta(h) = h \otimes 1_K \}
\]

then

\[
\dim H^{\co \pi} = \frac{\dim H}{\dim K} \quad \text{and} \quad H \cong H^{\co \pi\#_\sigma K}
\]

as algebras for some normalized 2-cocycle \( \sigma \) with coaction given by \( \rho = (\text{id}_H \otimes \pi) \circ \Delta \).

Blattner and Montgomery [9, Theorem 2.6] also proved the following useful result dealing with the semisimplicity of crossed products.
Theorem 2.3.20. Let $A$ and $K$ be finite-dimensional semisimple Hopf algebras over $k$. If

$$H \cong A \#_{\sigma} K$$

as a crossed product for some normalized 2-cocycle $\sigma$, then $H$ is semisimple.

Summarizing, if $A$ is a normal Hopf subalgebra of the finite-dimensional Hopf algebra $H$ over $k$, then $HA^+$ is a Hopf ideal of $H$ and

$$1 \rightarrow A \xrightarrow{\iota} H \xrightarrow{\pi} HA^+ \rightarrow 1$$

is an exact sequence of Hopf algebras, with $\iota$ inclusion and $\pi$ the canonical surjection. Moreover

$$H \cong H^{co\pi} \#_{\sigma} H/HA^+$$

as algebras for some normalized 2-cocycle $\sigma$. Since $A$ is a Hopf subalgebra of $H$ isomorphic to $H^{co\pi}$, we have that $H$ is semisimple if both $A$ and $H/HA^+$ are semisimple.

2.3.5 Biproducts

In this last subsection, we briefly discuss the construction of Radford biproducts of Hopf algebras. In this subsection, denote by $H$ a Hopf algebra over the field $k$. First we define $H$-module algebras and $H$-comodule coalgebras.

Definition 2.3.21. Let $A$ be a $k$-algebra which is also a left $H$-module where $\cdot$ denotes the action. Then we say that $A$ is a left $H$-module algebra if

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

and $h \cdot 1_A = \epsilon(h)1_A$ for all $h \in H$ and $a, b \in A$.

Definition 2.3.22. Let $C$ be a $k$-coalgebra which is also a left $H$-comodule under the coaction $\rho : C \rightarrow H \otimes C$. Then we say that $C$ is a left $H$-comodule coalgebra if

$$\sum (c_1)_1(c_2)_1 \otimes (c_1)_0 \otimes (c_2)_0 = \sum c_{-1} \otimes (c_0)_1 \otimes (c_0)_2$$

and $\sum c_{-1}\epsilon(c_0) = \epsilon(c)1_H$ for all $c \in C$. 
Note that $A$ is a left $H$-module algebra if $A$ is an algebra such that the multiplication map $M$ and unit map $u$ are module homomorphisms. Also, $C$ is a left $H$-comodule coalgebra if $C$ is a coalgebra such that the comultiplication $\Delta$ and counit $\epsilon$ are comodule homomorphisms. If a vector space $B$ is both an $H$-module algebra and an $H$-comodule coalgebra, it is sometimes possible to construct a Hopf algebra structure on the tensor product vector space $B \otimes H$, called a biproduct.

**Definition 2.3.23.** Let $B$ be a left $H$-module algebra and a left $H$-comodule coalgebra with coaction $\rho$. Define a multiplication map on $B \otimes H$ by

$$(a \otimes h)(b \otimes k) = a(h_1 \cdot b) \otimes h_2 k$$

(called a smash product) and a comultiplication on $B \otimes H$ by

$$\Delta (a \otimes h) = (a_1 \otimes (c_2)_{-1} h_1) \otimes ((c_2)_0 \otimes h_2)$$

(called a smash coproduct) for all $a, b \in B$ and $h, k \in H$. We say that

$$B \otimes H = B \times H$$

is a **biproduct bialgebra** if $B \times H$ is a bialgebra using the above multiplication and comultiplication, with counit $\epsilon_B \otimes \epsilon_H$ and multiplicative identity $1_B \otimes 1_H$.

Radford gives necessary and sufficient conditions on the structures of $B$ for $B \times H$ to be a biproduct bialgebra [50, Theorem 1]. If $B$ is an $H$-module algebra and an $H$-comodule coalgebra such that $B \times H$ is a biproduct bialgebra and $\text{id}_B$ has an inverse $S_B$ in the convolution algebra $\text{Hom}_k(B, B)$, then we can form a Hopf algebra structure on $B \times H$. This is also a result of Radford [50, Proposition 2].

**Proposition 2.3.24.** Let $B$ be an $H$-module algebra and an $H$-comodule coalgebra such that $B \times H$ is a biproduct bialgebra. If $S_H$ is the antipode of $H$ and $S_B$ is the convolution inverse of $\text{id}_B$, then $B \times H$ is a Hopf algebra with antipode

$$S(b \otimes h) = \sum (1_B \otimes S_H(b_1 h)) (S_B(b_0) \otimes 1_H)$$

for all $b \in B$ and $h \in H$. In this case, we call $B \times H$ a biproduct Hopf algebra.
The next result of Radford [50, Theorem 3] characterizes biproduct Hopf algebras in terms of a certain pair of Hopf algebra maps. Note that if $B \times H$ is a biproduct bialgebra, then the linear map $\pi: B \times H \to H$ defined by $\pi(b \otimes h) = \epsilon(b)h$ for all $b \in B$ and $h \in H$ is a surjective bialgebra homomorphism such that $\pi \circ i = \text{id}_H$, where $i: H \to B \times H$ is defined by $i(h) = 1_B \otimes h$ for all $h \in H$ is an injective bialgebra homomorphism. This result gives a converse of this observation.

**Theorem 2.3.25.** Let $H$ be a Hopf algebra over $k$ with antipode $S$ and suppose $A$ and $B$ are bialgebras over $k$. Suppose that $\pi: A \to H$ is a surjective bialgebra homomorphism and $i: H \to A$ is an injective bialgebra homomorphism such that $\pi \circ i = \text{id}_H$. Set $\Pi = \text{id}_A \ast (i \circ S \circ \pi)$ and $B = \Pi(A)$. Then $B \times H$ is a biproduct bialgebra isomorphic to $A$.

In the above situation, Radford showed that $B = \Pi(A)$ is a subalgebra of $A$ and has a unique coalgebra structure such that $\Pi$ is a coalgebra homomorphism. Also, $B$ is a left $H$-module algebra under the adjoint action

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

for all $h \in H$ and $b \in B$, and $B$ is a left $H$-comodule coalgebra under the coadjoint coaction

$$\rho(b) = \sum \pi(b_1) S(\pi(b_3)) \otimes b_2$$

for all $b \in B$. Moreover, the linear mapping given by $b \otimes h \mapsto b i(h)$ for all $b \in B$ and $h \in H$ defines a bialgebra isomorphism from $B \times H$ to $A$. 
CHAPTER 3. CLASSIFICATIONS OF FINITE-DIMENSIONAL HOPF ALGEBRAS

3.1 Introduction

Next we come to the main topic of this thesis, the classification of finite-dimensional Hopf algebras. In 1975, Kaplansky [24] published a list of 10 conjectures dealing with Hopf algebras. The last of these conjectures hypothesized that for every positive integer $n$, there are only finitely many isomorphism classes of $n$-dimensional Hopf algebras over an algebraically closed field $k$ of characteristic zero. While the conjecture does hold for semisimple Hopf algebras, a result of Stefan [56], as well as for Hopf algebras with some simple dimensions that are factorized as a product of just a few primes, the conjecture is actually false in general. It was shown independently by Andruskiewitsch and Schneider [6], by Beattie, Dăscălescu, and Grünenfelder [7], and by Gelaki [19] that for every odd prime $p$ there is an infinite family of non-isomorphic non-semisimple Hopf algebras of dimension $p^4$.

Despite this result, progress has been made in recent years in classifying Hopf algebras over an algebraically closed field of characteristic zero with dimensions a product of three or fewer primes. First, we note an important result proven by Masuoka [35] dealing with semisimple Hopf algebras of prime power dimension. For any group $G$, we denote by $Z(G)$ the center of $G$.

**Theorem 3.1.1.** Let $H$ be a semisimple Hopf algebra over an algebraically closed field $k$ of characteristic zero. If $\dim H = p^n$ for some prime $p$ and positive integer $n$, then $H$ contains a non-trivial central group-like element. In particular, $|G(H)| \geq |Z(G(H))| > 1$.

We will need another general result on non-semisimple finite-dimensional Hopf algebras
which contain non-trivial skew primitive elements. Let \( M \) and \( N \) be non-negative integers such that \( M \mid N \), and let \( \xi \in \mathbb{k} \) be a primitive \( M \)-th root of unity. Let \( \mu \in \{0, 1\} \), with \( \mu = 0 \) if \( M = N \). Define the Hopf algebra \( K_\mu(N, \xi) \) to be the algebra generated by the elements \( g, x \) with relations

\[
x^M = \mu(1 - g^M), \quad g^N = 1, \quad gx = \xi xg
\]

with comultiplication given by

\[
\Delta(g) = g \otimes g, \quad \Delta(x) = 1 \otimes x + x \otimes g
\]

and antipode

\[
S(g) = g^{-1}, \quad S(x) = -xg^{-1}.
\]

It follows by a result of Andruskiewitsch and Schneider [6] that \( \dim K_\mu(N, \xi) = MN \). Note that if \( M = N \), then \( K_\mu(N, \xi) \) is just a Taft algebra \( T_N(\xi) \) of dimension \( N^2 \).

The result we need, which guarantees the existence of a Hopf subalgebra of the form \( K_\mu(N, \xi) \) in the case there exists a skew primitive element in a finite-dimensional Hopf algebra, is due to Andruskiewitsch and Natale [4, Proposition 1.8] and is given next.

**Theorem 3.1.2.** Let \( H \) be a non-semisimple finite-dimensional Hopf algebra over \( \mathbb{k} \). If \( H \) contains a non-trivial \((g, h)\)-skew primitive element for some \( g, h \in G(H) \), then \( H \) contains a Hopf subalgebra \( K \) isomorphic to \( K_\mu(N, \xi) \) for some root of unity \( \xi \in \mathbb{k} \) and some \( \mu \in \{0, 1\} \).

Beginning in the next section we will detail some of the completed results on the classification of finite-dimensional Hopf algebras based on the prime factorization of the dimension. We begin with Hopf algebras of prime dimension.

### 3.2 Hopf Algebras of Dimension \( p \)

If \( H \) is a Hopf algebra over \( \mathbb{k} \) of dimension \( p \), where \( p \) is a prime, then it follows immediately by the Nichols-Zoeller Theorem that \( H \) contains no non-trivial Hopf subalgebras. In fact, for a prime \( p \), Zhu [62] showed that if \( H \) is a Hopf algebra of dimension \( p \) over an algebraically closed field of characteristic zero, then \( H \) is isomorphic to a group algebra. Since any group of prime order is cyclic, we have the following classification.
Theorem 3.2.1. If $H$ is a Hopf algebra over the algebraically closed field $\mathbb{k}$ of characteristic zero and $\dim H = p$, for $p$ a prime, then $H \cong \mathbb{k}[\mathbb{Z}_p]$.

Proof. We break our proof into cases. First assume that $H$ is semisimple. By Theorem 3.1.1, we know that $H$ contains a non-trivial group-like element $g \in G(H)$. That is, $|G(H)| > 1$ and so by the Nichols-Zoeller Theorem, $|G(H)| = p$. Therefore $H \cong \mathbb{k}[G]$ for some finite group $G$ of order $p$. Since every group of prime order is cyclic, we immediately have that $H \cong \mathbb{k}[\mathbb{Z}_p]$.

Second, assume that $H$ is not semisimple. Then $H$ or the dual Hopf algebra $H^*$ is not unimodular or both $H$ and $H^*$ are unimodular. If either $H$ or $H^*$ is not unimodular, then we know that either $H$ or $H^*$ contains a non-trivial distinguished group-like element. By the above argument, either $H \cong \mathbb{k}[\mathbb{Z}_p]$ or $H^* \cong \mathbb{k}[\mathbb{Z}_p]$. However, since $\mathbb{k}[\mathbb{Z}_p]$ is self-dual, we have that $H \cong \mathbb{k}[\mathbb{Z}_p]$. Note that this is actually a contradiction as any group algebra is unimodular.

Lastly, we make the assumption that $H$ is not semisimple and $H$ and $H^*$ are both unimodular. By the theorem of Larson and Radford, Theorem 2.3.11, we know that $H$ being non-semisimple is equivalent to $\text{Tr}(S^2) = 0$, where $S$ is the antipode of $H$. Moreover, since $H$ and $H^*$ are unimodular, the distinguished group-like elements of $H$ and $H^*$ are $g = 1_H$ and $\alpha = \epsilon$, respectively. By Radford’s formula for $S^4$, Theorem 2.3.7, we have then that $S^4 = \text{id}_H$. This further implies that the eigenvalues of $S^2$ are either 1 or $-1$. Since $\text{Tr}(S^2) = 0$, the eigenspaces of $S^2$ associated to each of the eigenvalues 1 and $-1$ must have the same dimension. Therefore $\dim H = p$ must be even. However, it is easily verified that any Hopf algebra of dimension 2 is trivial, and so this case results in another contradiction.

Therefore $H$ is semisimple and hence $H \cong \mathbb{k}[\mathbb{Z}_p]$ as desired. \hfill $\square$

In particular, note that every Hopf algebra of prime dimension is semisimple, commutative, and cocommutative. We next investigate Hopf algebras which have dimensions a product of two primes. We see that in the dimension $p^2$ case, for $p$ a prime, we must consider both semisimple and non-semisimple Hopf algebras.
3.3 Hopf Algebras of Dimension $p^2$

Recall that for any prime $p$ and any primitive $p$-th root of unity $\xi$, we can define the Taft algebra $T_p(\xi)$ of dimension $p^2$ as the algebra generated by $g$ and $x$ subject to the relations

$$x^n = 0, \quad g^n = 1, \quad gx = \xi x g.$$ 

and with basis

$$\{x^i g^j : 0 \leq i, j \leq p - 1\}.$$ 

$T_p(\xi)$ has comultiplication and counit given by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = 1 \otimes x + x \otimes g$$

$$\epsilon(g) = 1, \quad \epsilon(x) = 0$$

and an antipode defined by

$$S(g) = g^{-1}, \quad S(x) = -xg^{-1}.$$ 

We have mentioned before that $T_p(\xi)$ is a non-semisimple self-dual Hopf algebra of dimension $p^2$ and that $T_p(\xi_1) \cong T_p(\xi_2)$ if and only if $\xi_1 = \xi_2$. So the classification of Hopf algebras of dimension $p^2$ will include some non-semisimple examples. In particular, these non-semisimple examples of Hopf algebras of dimension $p^2$ are pointed.

In general, one may consider the classification of semisimple and non-semisimple finite-dimensional Hopf algebras separately. For $p$ a prime, Masuoka [35] proved that every semisimple Hopf algebra of dimension $p^2$ is trivial. Since every group of order $p^2$ is abelian, this implies that there are only two isomorphism classes of semisimple Hopf algebras of dimension $p$. Namely, either $H \cong k[Z_{p^2}]$ or $H \cong k[Z_p \times Z_p]$ for every semisimple Hopf algebra $H$ over $k$ with $\dim H = p^2$.

The classification of non-semisimple Hopf algebras of dimension $p^2$ has also been completed. Andruskiewitsch and Schneider [5] first showed the following result.

**Theorem 3.3.1.** Let $H$ be a non-semisimple Hopf algebra over the algebraically closed field $k$ of characteristic zero. If $\dim H = p^2$ for some prime $p$ and the order of the antipode $S$ of $H$
is $2p$, then $H$ is pointed and hence isomorphic to a Taft algebra $T_p(\xi)$ for some primitive $p$-th root of unity $\xi$.

It had already been shown by Kaplansky [24] that any non-semisimple Hopf algebra over $k$ of dimension 4 is isomorphic to a Taft algebra. Ng [41] finished the classification by showing that if $H$ is a non-semisimple Hopf algebra over $k$ of dimension $p^2$ for an odd prime $p$, then the antipode $S$ of $H$ has order $2p$. By Andruskiewitsch and Schneider’s result in Theorem 3.3.1, $H$ must then be isomorphic a Taft algebra. It is worth noting that this classification implies that all non-semisimple Hopf algebras of dimension $p^2$ over $k$ are pointed. In total, the classification of Hopf algebras over $k$ of dimension $p^2$ for $p$ a prime is given in the following theorem.

**Theorem 3.3.2.** Let $H$ be a Hopf algebra over an algebraically closed field $k$ of characteristic zero such that $\dim H = p^2$ for a prime $p$.

(a) If $H$ is semisimple, then $H \cong k[\mathbb{Z}_{p^2}]$ or $H \cong k[\mathbb{Z}_p \times \mathbb{Z}_p]$.

(b) If $H$ is not semisimple, then $H \cong T_p(\xi)$ for some primitive $p$-th root of unity $\xi \in k$.

### 3.4 Hopf Algebras of Dimension $pq$

The classification of Hopf algebras of dimension $pq$ for $p$ and $q$ distinct primes is another story. Such semisimple Hopf algebras were studied by Etingof and Gelaki [15], Gelaki and Westreich [20], and Sommerhauser [55]. It was shown by Etingof and Gelaki [15] that if $H$ is a semisimple Hopf algebra of dimension $pq$ for distinct odd primes $p$ and $q$, then $H$ must be a trivial Hopf algebra. In particular, we have the following result.

**Theorem 3.4.1.** Let $H$ be a semisimple Hopf algebra over an algebraically closed field $k$ of characteristic zero. If $\dim H = pq$ for distinct primes $p$ and $q$, then $H \cong k[G]$ or $H \cong k[G]^*$ for some finite group $G$ of order $pq$.

It has been conjectured that in fact any Hopf algebra of dimension $pq$ for $p \neq q$ must be semisimple and hence trivial. There is significant evidence to support this conjecture. First,
Natale [39] showed that if $H$ is a quasi-triangular Hopf algebra of dimension $pq$ over $k$ then $H$ is semisimple and hence trivial. Briefly, a quasi-triangular Hopf algebra $H$ is one in which the tensor category of $H$-modules is braided.

The conjecture is true if one of the primes is 2. It was shown by Ng [43] that any Hopf algebra of dimension $2p$ over $k$ must be semisimple, where $p$ is an odd prime. In doing so, he proved the following useful result [43, Corollary 2.2] dealing with Hopf algebras with even dimensions not divisible by 4.

**Theorem 3.4.2.** Let $H$ be a Hopf algebra over an algebraically closed field $k$ of characteristic zero. If $\dim H = 2n$ for some odd integer $n$ and $H$ is not semisimple, then $H$ or $H^*$ is not unimodular.

In particular, this result implies that at least one of the distinguished group-like elements $g \in G(H)$ or $\alpha \in G(H^*)$ is non-trivial. This was used to show the main result of that paper, which is given next.

**Theorem 3.4.3.** Let $H$ be a Hopf algebra over an algebraically closed field $k$ of characteristic zero. If $\dim H = 2p$ for $p$ and odd prime, then $H$ is semisimple.

That is, if $\dim H = 2p$ then

$$H \cong k[Z_{2p}], \quad H \cong k[D_{2p}], \text{ or } H \cong k[D_{2p}]^*$$

where $D_{2p}$ is the dihedral group of order $2p$. Thus the classification of Hopf algebras of dimension $2p$ over $k$, for $p$ an odd prime, has been completed and there are three isomorphism classes of such Hopf algebras.

The classification of Hopf algebras of dimension $pq$ for odd primes $p < q$ is still incomplete. However, Etingof and Gelaki [16] proved that if

$$2 < p < q \leq 2p + 1$$

then every Hopf algebra over $k$ of dimension $pq$ is semisimple and hence trivial. This result was improved by Ng [44], as the next result states.
Theorem 3.4.4. Let $H$ be a Hopf algebra over an algebraically closed field $k$ of characteristic zero. If $\dim H = pq$ and

$$2 < p < q \leq 4p + 11$$

then $H$ is semisimple.

3.5 Hopf Algebras of Dimension $pqr$

The established classification results for Hopf algebras with dimensions a product of one or two primes have laid a foundation for the study of Hopf algebras which have dimensions a product of three primes. In particular, there have been results in the three cases that the dimension of the Hopf algebra is $p^3$, $pq^2$, or $pqr$ for distinct primes $p, q, r$. In particular, since the classifications of Hopf algebras of dimensions $p$, $p^2$, and $2p$ have been completed, significant progress is possible in the classification of Hopf algebras of dimensions $p^3$, $2p^2$, and $4p$, for $p$ an odd prime. We will focus on the two cases of dimension $p^3$ and dimension $2p^2$ in this thesis.

In both of these cases, semisimple Hopf algebras of these dimensions have been fully classified. For semisimple Hopf algebras of dimension 8, it was shown by Masuoka [34] that there exists only one isomorphism class of Hopf algebras which is not trivial. That is, there is only one isomorphism class of these Hopf algebras which is not a group algebra or dual to the group algebra of a group of order 8. For a general odd prime $p$, Masuoka [32] then completed the classification of semisimple Hopf algebras of dimension $p^3$ over $k$ when he showed that there are exactly $p + 1$ isomorphism classes of non-trivial semisimple Hopf algebras of these dimensions. Each of these non-trivial semisimple Hopf algebras $H$ is an extension of $k[Z_p]$ by $k[Z_p \times Z_p]^*$. That is, there is an exact sequence

$$1 \to k[Z_p \times Z_p]^* \xrightarrow{\iota} H \xrightarrow{\pi} k[Z_p] \to 1$$

where $\iota$ and $\pi$ are injective and surjective Hopf algebra homomorphisms, respectively. Note that there are five non-isomorphic groups of order $p^3$, namely

$$Z_{p^3}, Z_p \times Z_{p^2}, Z_p \times Z_p \times Z_p, G_1, \text{ and } G_2$$
where $G_1 = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes \mathbb{Z}_p$ and $G_2 = \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_p$ are non-trivial semi-direct products, each being unique up to isomorphism. Since $G_1$ and $G_2$ are the only non-abelian groups in this list, we have exactly seven trivial Hopf algebras of dimension $p^3$, namely

$k[\mathbb{Z}_{p^3}], k[\mathbb{Z}_p \times \mathbb{Z}_{p^2}], k[\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p], k[G_1], k[G_2], k[G_1]^*, \text{ and } k[G_2]^*$.

Altogether, Masuoka’s result implies that there are $p + 8$ isomorphism classes of semisimple Hopf algebras of dimension $p^3$ over $k$.

Semisimple Hopf algebras of dimension $2p^2$ for $p$ and odd prime have also been classified completely. Masuoka [33] constructed a semisimple Hopf algebra $B_0$ (which he denoted by $A_\zeta$) of dimension $2p^2$ which is neither commutative or cocommutative. It is an extension of the group algebra $k[\mathbb{Z}_2]$ by the dual group algebra $k[\mathbb{Z}_p \times \mathbb{Z}_p]^*$. He showed that $B_0$ is the unique semisimple Hopf algebra $H$ of dimension $2p^2$ such that $|G(H)| = p^2$. Natale [38] completed the classification by showing that non-trivial semisimple Hopf algebras of dimension $2p^2$ are isomorphic to $B_0$ or $B_0^*$. It was also shown that $G(B_0^*) \cong \mathbb{Z}_{2p}$ and so $B_0$ is not a self-dual Hopf algebra, giving exactly two isomorphism classes of non-trivial Hopf algebras of dimension $2p^2$ over $k$.

The Hopf algebra $B_0^*$ can be described as a smash product Hopf algebra $k[D_{2p}]^* \# k[\mathbb{Z}_p]$, where $D_{2p}$ is the dihedral group of order $2p$. A smash product $A \# H$ is a crossed product with trivial cocycle

$$\sigma(h, k) = \epsilon(h)\epsilon(k)1_A$$

for all $h, k \in H$. If we write

$$D_{2p} = \langle a, b \mid b^p = 1, a^2 = 1, aba = b^{-1} \rangle$$

then there is a right action $\triangleleft$ of $\mathbb{Z}_p$ on $D_{2p}$ as automorphisms defined by

$$b \triangleleft g = b, \quad a \triangleleft g = ba$$

where $\mathbb{Z}_p = \langle g \rangle$. This action induces a left action of $k[\mathbb{Z}_p]$ on $k[D_{2p}]^*$ defined by

$$g \cdot p_x = p_{x\triangleleft g}$$
for all $x \in D_{2p}$, where $p_x \in k[D_{2p}]^*$ is defined by $p_x(y) = \delta_{x,y}$ for all $x, y \in D_{2p}$. We use this action to describe the algebra structure of $k[D_{2p}]^* \# k[Z_p]$, which, as a vector space, is equal to $k[D_{2p}]^* \otimes k[Z_p]$. The multiplication is given by

$$(p_x \# g)(p_y \# h) = \sum p_x(g \cdot p_y) \# gh$$

for all $x, y \in D_{2p}$ and $g, h \in Z_p$. The comultiplication is given by the usual tensor coalgebra comultiplication.

In both cases of dimension $p^3$ or $2p^2$, the non-semisimple pointed Hopf algebras over $k$ have been completely classified. We discuss the case when $\dim H = p^3$ for a prime $p$ first. The classification of Hopf algebras of dimension 8 was first completed by Williams [61], and this result was later proved independently Stefan [57]. For $p$ an odd prime, the classification of pointed non-semisimple Hopf algebras of dimension $p^3$ was proved independently in three papers by Andruskiewitsch and Schneider [6], by Caenepeel and Dascalescu [10], and by Stefan and van Oystaeyen [58] using different methods.

Denote by $\xi \in k$ a primitive $p$-th root of unity. Then the complete list of pointed non-semisimple Hopf algebras of dimension $p^3$, for $p$ a prime, is given as follows:

1. The tensor product Hopf algebra $T_p(\xi) \otimes k[Z_p]$;
2. The algebra $\widetilde{T}_p(\xi)$ generated by $g, x$ subject to the relations

$$g^{p^2} = 1, \quad x^p = 0, \quad \text{and} \quad gx = \xi^{1/p} xg$$

with comultiplication given by

$$\Delta(g) = g \otimes g \quad \text{and} \quad \Delta(x) = x \otimes g^p + 1 \otimes x;$$

3. The algebra $\hat{T}_p(\xi)$ generated by $g, x$ subject to the relations

$$g^{p^2} = 1, \quad x^p = 0, \quad \text{and} \quad gx = \xi xg$$

with comultiplication given by

$$\Delta(g) = g \otimes g \quad \text{and} \quad \Delta(x) = x \otimes g + 1 \otimes x;$$
4. The algebra $r(\xi)$ generated by $g, x$ subject to the relations

$$g^{p^2} = 1, \ x^p = 1 - g^p, \text{ and } gx = \xi xg$$

with comultiplication given by

$$\Delta(g) = g \otimes g \text{ and } \Delta(x) = x \otimes g + 1 \otimes x;$$

5. The Frobenius-Lusztig kernel $u_\xi(sl_2)$ which is the algebra generated by $g, x, y$ subject to the relations

$$g^p = 1, \ x^p = 0, \ y^p = 0, \ xy - yx = g - g^{-1}$$

$$gx = \xi^2 xg, \ gy = \xi^{-2} yg$$

with comultiplication given by

$$\Delta(g) = g \otimes g, \ \Delta(x) = x \otimes g + 1 \otimes x, \text{ and } \Delta(y) = y \otimes 1 + g^{-1} \otimes y :$$

6. The algebra $h(\xi, m)$ generated by $g, x, y$ subject to the relations

$$g^p = 1, \ x^p = 0, \ y^p = 0, \ gx = \xi xg, \text{ and } gy = \xi^m yg$$

where $m \in \mathbb{Z}_p$, with comultiplication given by

$$\Delta(g) = g \otimes g, \ \Delta(x) = x \otimes g + 1 \otimes x, \text{ and } \Delta(y) = y \otimes 1 + g^m \otimes y.$$

There are no isomorphisms between the separate types of Hopf algebras in this list. Also for the first five types, the Hopf algebras are not isomorphic for different choices of primitive $p$-th root of unity $\xi \in \mathbb{k}$. For the last type, $h(\xi, m) \cong h(\xi', m')$ if and only if $\xi' = \xi^{-m^2}$ and $m' = m^{-1}$. Moreover, the duals of the algebras $u_\xi(sl_2)$ and $r(\xi)$ are not pointed while the duals of the other Hopf algebras are pointed and hence represented in this list.

In particular, there are no known examples of Hopf algebras of dimension $p^3$ over $\mathbb{k}$ which are neither pointed nor the dual of a pointed Hopf algebra. The study of non-semisimple Hopf algebras of dimension $p^3$ has been carried out by García [18]. In his paper, García breaks the possible non-semisimple Hopf algebras of dimension $p^3$ into ten cases, and manages to show the
structure of the Hopf algebra in eight of the ten cases, and in each case they are either a pointed
Hopf algebra or dual to such a Hopf algebra. It is conjectured that every non-semisimple of
dimension $p^3$ for $p$ a prime is either pointed or dual to a pointed Hopf algebra.

Pointed non-semisimple Hopf algebras of dimension $2p^2$, for $p$ an odd prime, have also been
classified. For $p$ a prime, let

$$ j \in \{1, 2, 4, \cdots, 2p - 2\} \text{ and } \mu \in \{0, 1\} $$

such that $\mu = 0$ whenever $j = 1$. Also let $\tau \in \mathbb{k}$ be a $2p$-th root of unity such that the order
of $\tau$ is a multiple of $p$, with the order of $\tau$ being $p$ in the case that $j \neq 1$. Define the algebra
$A(\tau, j, \mu)$ to be the $\mathbb{k}$-algebra generated by the elements $g$ and $x$ subject to the relations

$$ g^{2p} = 1, \quad x^p = \mu (1 - g^p), \quad gx = \tau xg $$

which is a $2p^2$-dimensional algebra with basis

$$ \{x^i g^j : 0 \leq i \leq p - 1, 0 \leq j \leq 2p - 1\} $$

over $\mathbb{k}$. Then $A(\tau, j, \mu)$ is a Hopf algebra with comultiplication given by

$$ \Delta(g) = g \otimes g, \quad \Delta(x) = x \otimes 1 + g^j \otimes x $$

and extended linearly and as an algebra homomorphism to all of $A(\tau, j, \mu)$. Note that $g$ is a
group-like element of $A(\tau, j, \mu)$ of order $2p$ and $x$ is a $(1, g^j)$-skew primitive element of $A(\tau, j, \mu)$.

Andruskiewitsch and Natale [4] showed the following result, completing the classification
of pointed Hopf algebras of dimension $2p^2$ over $\mathbb{k}$.

**Theorem 3.5.1.** Let $H$ be a non-semisimple pointed Hopf algebra of dimension $2p^2$ over the
algebraically closed field $\mathbb{k}$ of characteristic zero. Then $H$ is isomorphic to one of the following
Hopf algebras:

1. $A(\xi, 1, 0)$, where $\xi$ is a primitive $p$-th root of unity;
2. $A(\xi, 1, 1)$, where $\xi$ is a primitive $p$-th root of unity;
3. $A(\tau, 2r, 0)$, where $\tau$ is a fixed primitive $2p$-th root of unity and $1 \leq r \leq p - 1$;
4. \( A(\xi, 2, 0) \cong T_p(\xi) \otimes k[Z_2] \), where \( \xi \) is a primitive \( p \)-th root of unity.

where \( T_p(\xi) \) is a Taft algebra of dimension \( p^2 \).

There are exactly \( p - 1 \) isomorphism classes of each type of pointed Hopf algebra of dimension \( 2p^2 \) in the list above. For the first, second, and fourth types, these isomorphism classes depend on the choice of primitive \( p \)-th root of unity. For the third type \( A(\tau, 2r, 0) \), we fix the primitive \( 2p \)-th root of unity \( \tau \in k \), and any Hopf algebra of this type is isomorphic to one of the form \( A(\tau, 2r, 0) \) for some \( 1 \leq r \leq p - 1 \). Therefore there are exactly \( 4(p - 1) \) isomorphism classes of non-semisimple pointed Hopf algebras of dimension \( 2p^2 \) over \( k \).

In their paper, Andruskiewitsch and Natale pointed out that the dual of the Hopf algebra \( A(\xi, 1, 0) \) is isomorphic to a Hopf algebra of the form \( A(\tau, 2r, 0) \) where \( \tau \) is a primitive \( 2p \)-th root of unity. Moreover, the Hopf algebra

\[
A(\xi, 2, 0) \cong T_p(\xi) \otimes k[Z_2]
\]

is self-dual. In particular, the duals of any Hopf algebra of the forms \( A(\xi, 1, 0) \), \( A(\tau, 2r, 0) \), and \( A(\xi, 2, 0) \) are pointed non-semisimple Hopf algebras of dimension \( 2p^2 \), where \( \xi \) is a primitive \( p \)-th root of unity, \( \tau \) is a primitive \( 2p \)-th root of unity, and \( 1 \leq r \leq p - 1 \). However, \( A(\xi, 1, 1)^* \) is not a pointed Hopf algebra, as noted by Radford in [48]. Therefore there are exactly \( 5(p - 1) \) isomorphism classes of non-semisimple Hopf algebras of dimension \( 2p^2 \) over \( k \) which are pointed or isomorphic to the dual of a pointed Hopf algebra.

The general non-semisimple case when \( p = 3 \) has been studied by Fukuda [17]. He showed that any non-semisimple Hopf algebra over \( k \) of dimension 18 is either pointed or isomorphic to the dual of a pointed Hopf algebra. This would lead to the conjecture that any non-semisimple Hopf algebra of dimension \( 2p^2 \) over \( k \) is either pointed or dual to a pointed Hopf algebra, where \( p \) is an odd prime. In the remainder of this thesis, we shall explore the proof of this conjecture.

Before moving on, we note an important result of Andruskiewitsch and Natale [4, Lemma A.2] that can be used to determine when some finite-dimensional Hopf algebras are pointed. In dealing with non-semisimple finite-dimensional Hopf algebra \( H \) of dimension \( pq^2 \) where \( p \) and \( q \) are distinct primes, they showed that it suffices to show that the coradical \( H_0 \) of \( H \) is a
Hopf subalgebra when determining if $H$ is pointed. Recall that the coradical $H_0$ of $H$ is the sum of all simple subcoalgebras of the Hopf algebra $H$. We will employ this result in the next chapter in showing our main result, Theorem 4.3.5.

**Theorem 3.5.2.** Let $p$ and $q$ be distinct primes and let $H$ be a non-semisimple Hopf algebra over $\mathbb{k}$ of dimension $pq^2$. If the coradical $H_0$ of $H$ is a Hopf subalgebra of $H$, then $H$ is pointed.
Chapter 4. Non-semisimple Hopf Algebras of Dimension $2p^2$

In this chapter, we prove our main result, Theorem 4.3.5, which states that if $p$ is an odd prime and $H$ is a non-semisimple Hopf algebra over an algebraically closed field of characteristic zero, then $H$ or $H^*$ is pointed. We first need to discuss some preliminary results dealing with finite-dimensional Hopf algebras and their extensions. All results in this chapter first appeared in [21]. Throughout this chapter, let $H$ denote a finite-dimensional Hopf algebra over an algebraically closed field $k$ of characteristic zero.

4.1 Preliminaries

Let $a \in H$ be a group-like element of order $m$. Then $k[a]$ is a commutative Hopf subalgebra of $H$. Let $\omega \in k$ be a primitive $m$-th root of unity and define

$$e_{a,j} = \frac{1}{m} \sum_{i \in \mathbb{Z}_m} \omega^{-ij} a^i$$

(4.1)

for $j \in \mathbb{Z}_m$, where

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

is the cyclic group of order $m$. Then $\{e_{a,j}\}_{j \in \mathbb{Z}_m}$ is a complete set of primitive idempotents of $k[a]$. That is,

$$e_{a,i} \cdot e_{a,j} = \delta_{ij} e_{a,i}, \quad \text{and} \quad \sum_{j \in \mathbb{Z}_m} e_{a,j} = 1.$$ 

Therefore, for any right $k[a]$-module $V$, we always have the $k[a]$-module decomposition

$$V = \bigoplus_{i \in \mathbb{Z}_m} Ve_{a,i}.$$
Note that $k[a] = \bigoplus_{j \in \mathbb{Z}_m} k e_{a,j}$ as ideals of $k[a]$. If $V$ is a free right $k[a]$-module, then $\text{ord}(a)$ divides $\dim V$ and
\[
\dim V e_{a,j} = \frac{\dim V}{\text{ord}(a)}.
\]
Obviously, the same conclusion can be drawn for left $k[a]$-modules $V$. Moreover, one can construct the complete set of primitive idempotents $\{e_{\beta,j}\}$ for each group-like element $\beta \in H^*$ in the same way.

**Lemma 4.1.1.** Let $H$ be a finite-dimensional Hopf algebra over $k$ with antipode $S$. Suppose $a \in G(H)$ and $\beta \in G(H^*)$ such that $\beta(a) = 1$, and write $H_{ij}$ for $He_{a,i} \leftarrow e_{\beta,j}$ for $i \in \mathbb{Z}_{\text{ord}(a)}$ and $j \in \mathbb{Z}_{\text{ord}(\beta)}$.

(a) We have the $k$-linear space decomposition $H = \bigoplus_{i,j} H_{ij}$, and
\[
\dim H_{ij} = \frac{\dim H}{\text{ord}(a) \cdot \text{ord}(\beta)} \text{ for all } i, j.
\]

(b) If $H$ is not semisimple, then $\text{Tr}(S^2|_{H_{ij}}) = 0$ for all $i, j$.

**Proof.** (a) By the Nichols-Zoeller Theorem (Theorem 2.3.13), $H$ is a free right $k[a]$-module. It follows by the preceding remark that $\dim He_{a,i} = \dim H/\text{ord}(a)$ for $i \in \mathbb{Z}_{\text{ord}(a)}$, and
\[
H = \bigoplus_{i \in \mathbb{Z}_{\text{ord}(a)}} He_{a,i}.
\]
Since $\beta(a) = 1$,
\[
(ha^i) \leftarrow \beta = \beta(h_1 a^i) h_2 a^i = \beta(h_1) h_2 a^i = (h \leftarrow \beta)a^i
\]
for all integers $i$ and $h \in H$.

For simplicity, let $e = e_{a,i}$ for some $i \in \mathbb{Z}_{\text{ord}(a)}$. Then $(he) \leftarrow \beta = (h \leftarrow \beta)e$ for $h \in H$.

In particular, $He$ is a right $k[\beta]$-module under the action $\leftarrow$.

Consider the left $k[\beta]$-module action on $He$ defined by
\[
\beta \rightarrow x = x \leftarrow (\beta^{-1}) \text{ for all } x \in He.
\]
Since $He$ is a left $H$-module, we recall by Proposition 2.1.20 that it admits a natural right $H^*$-comodule structure

$$\rho : He \to He \otimes H^*$$

with $\rho(x) = \sum x_0 \otimes x_1$ defined by $hx = \sum x_0 x_1(h)$ for all $h \in H$. It is straightforward to check that

$$\rho(\beta \cdot x) = \beta \cdot \rho(x)$$

for all $x \in He$. Hence, $He$ is a Hopf module in $k[\beta]M^H$. By the Nichols-Zoeller Theorem, we find $He$ is a free left $k[\beta]$-module under the action $\cdot$.

By the preceding remark again, we have

$$He = \bigoplus_j e_{\beta,j} \to He,$$

and

$$\dim (e_{\beta,j} \to He) = \frac{\dim H e}{\text{ord}(\beta)} = \frac{\dim H}{\text{ord}(a) \cdot \text{ord}(\beta)}.$$

Since $e_{\beta,j} \to x = x \leftarrow e_{\beta,-j}$, we obtain

$$He = \bigoplus_j H_{ij}, \quad \text{and} \quad \dim H_{ij} = \frac{\dim H}{\text{ord}(a) \cdot \text{ord}(\beta)}.$$

Moreover,

$$H = \bigoplus_{i,j} H_{ij}$$

as vector spaces, which finishes the proof.

(b) Let $E_i$ and $F_j$ respectively denote the $k$-linear operators on $H$ defined by

$$E_i(h) = he_{a,i}, \quad F_j(h) = h \leftarrow e_{\beta,j}$$

for $i \in \mathbb{Z}_{\text{ord}(a)}$ and $j \in \mathbb{Z}_{\text{ord}(\beta)}$. Then both $E_i$ and $F_j$ are projections on $H$ and

$$H_{ij} = F_j E_i(H).$$

Since $a \in G(H)$ and $\beta \in G(H^*)$, we have that

$$S^2(a) = a \quad \text{and} \quad \beta \circ S^2 = (S^*)^2(\beta) = \beta$$

and so the operator $S^2$ commutes with both $E_i$ and $F_j$. Therefore, $S^2(H_{ij}) \subseteq H_{ij}$, and so

$$\text{Tr}(S^2|_{H_{ij}}) = \text{Tr}(S^2 \circ F_j \circ E_i) = \text{Tr}(E_i \circ S^2 \circ F_j).$$
It then follows by a result of Radford [51, Proposition 2(a)] that

\[ \text{Tr}(S^2_{|H_{ij}}) = \lambda(e_{a,i})e_{\beta,j}(\Lambda) = \sum_{l,k} \gamma_{lk} \lambda(a^l)\beta^k(\Lambda) \]  

(4.2)

for some \( \gamma_{lk} \in \mathbb{k} \), where \( \lambda \in H^* \) is a right integral, and \( \Lambda \in H \) is a left integral such that \( \lambda(\Lambda) = 1 \). The properties of integrals mentioned in Remark 2.3.2 imply that

\[ \lambda(a^l)a^l = \lambda(a^l)1, \quad \beta^k(\Lambda)\beta^k = \beta^k(\Lambda)\epsilon \]  

(4.3)

for all integers \( l, k \). Since \( H \) is not semisimple, \( \lambda(1_H) = \epsilon(\Lambda) = 0 \) by Mashke’s Theorem for Hopf algebras (Theorem 2.3.9). If \( a^l \) is not trivial, then the first equality of (4.3) and the linear independence of distinct group-like elements (Proposition 2.1.6) imply that \( \lambda(a^l) = 0 \). Similarly, we can also conclude \( \beta^k(\Lambda) = 0 \) for all integers \( k \). In view of (4.2), \( \text{Tr}(S^2_{|H_{ij}}) = 0 \) for all \( i, j \).

The next sequence of propositions on some extensions of finite-dimensional Hopf algebras will be used to show our main result in the next two sections, and may be of interest in their own right.

**Proposition 4.1.2.** Let \( H, A \) be finite-dimensional Hopf algebras over \( \mathbb{k} \) of dimension \( 2n \) and \( n \), respectively, where \( n \) is an odd integer.

(a) If there exists a Hopf algebra surjection \( \pi : H \to A \), then

\[ R = H^{\text{co}\pi} = \{ h \in H \mid (\text{id}_H \otimes \pi)\Delta(h) = h \otimes 1_A \} \]

is a normal Hopf subalgebra of \( H \) isomorphic to \( \mathbb{k}[\mathbb{Z}_2] \).

(b) If \( A \) is a Hopf subalgebra of \( H \), then \( A \) is a normal Hopf subalgebra of \( H \).

*Proof.* (a) It is well-known that \( R \) is a left coideal subalgebra of \( H \) of dimension

\[ \dim R = \frac{\dim H}{\dim A} = 2 \]
and $HR^+ \subseteq R^+H$. In view of Proposition 2.3.16, it suffices to show that $R$ contains a non-trivial group-like element. Let $x$ be a non-zero element of $R$ such that $\epsilon(x) = 0$. Then $\{1, x\}$ is a basis for $R$ and $\Delta(x) = a \otimes 1 + b \otimes x$ for some $a, b \in H$. By applying $\text{id}_H \otimes \epsilon$ and $\epsilon \otimes \text{id}_H$ to $\Delta(x)$, we find

$$x = \epsilon(1)a + \epsilon(x)b = \epsilon(a)1 + \epsilon(b)x$$

using the counit property of $H$, and so $x = a$ and $\epsilon(b) = 1$. Noting that $(\text{id}_H \otimes \Delta)\Delta(x) = (\Delta \otimes \text{id}_H)\Delta(x)$ by coassociativity, we find

$$a \otimes 1 \otimes 1 + b \otimes a \otimes 1 + b \otimes b \otimes x = a \otimes \Delta(1) + b \otimes \Delta(x) = \Delta(a) \otimes 1 + \Delta(b) \otimes x$$

or that $\Delta(b) = b \otimes b$, since $\{1, x\}$ is a linearly independent set. In other words, $b$ is a group-like element of $H$, and so $x$ is a $(1, b)$-skew primitive element. Since $H$ is finite-dimensional and $x \neq 0$ we must have that $b \neq 1$ by Remark 2.2.5. Note that $\{x\}$ is a basis for $\ker \epsilon|_R$, and $bxb^{-1} \in R$. Since

$$\epsilon(bxb^{-1}) = 0$$

we have that $bxb^{-1} = \zeta x$ for some primitive $M$-th root of unity $\zeta \in k$ where $M \mid \text{ord}(b)$.

Suppose $x$ is a non-trivial $(1, b)$-skew primitive element. Then, by Theorem 3.1.2, $\zeta \neq 1$ and $x, b$ generate a Hopf subalgebra $K \cong K_\mu(\text{ord}(b), \zeta)$ for some $\mu \in \{0, 1\}$. In particular,

$$M^2 \mid \dim K \mid \dim H.$$ 

On the other hand, since $\epsilon(x^2) = 0$, $x^2 = \gamma x$ for some $\gamma \in k$. Therefore, $(bxb^{-1})^2 = \gamma bxb^{-1}$ which implies $\gamma \zeta^2 = \gamma \zeta$. Thus $\gamma = 0$ and hence $x^2 = 0$. As a consequence, $K \cong K_0(\text{ord}(b), \zeta)$ and $M = 2$ is the nilpotency index of $x$. In particular, $4 \mid \dim H$, a contradiction. Therefore, $x$ must be a trivial $(1, b)$-skew primitive element, and hence $x = \nu(1 - b)$ for some non-zero $\nu \in k$. Since both $1, x \in R$, this implies $b \in R$, and so $R = k[b]$, finishing the proof of part (a).

(b) Consider the dual of the inclusion map $A \hookrightarrow H$, which is a Hopf algebra surjection $\pi : H^* \twoheadrightarrow A^*$. By part (a), $(H^*)^{\co \pi} \cong k[\mathbb{Z}_2]$ is a normal Hopf subalgebra of $H^*$, and so
we have the following exact sequence of Hopf algebras:

\[ 1 \to k[\mathbb{Z}_2] \to H^* \xrightarrow{\pi} A^* \to 1. \]

Dualizing this exact sequence, we get that \( A \) is a normal Hopf subalgebra of \( H \), as desired.

\[ \square \]

**Remark 4.1.3.** Proposition 4.1.2 (b) is a generalization of [26, Proposition 2] to non-semisimple Hopf algebras of dimension \( 2n \) with \( n \) odd. This result partially generalizes to finite-dimensional Hopf algebras the well-known result of finite groups which states that a subgroup \( H \) of index \( p \) of a finite group \( G \) must be a normal subgroup, where \( p \) is the smallest prime dividing \( |G| \).

The following result generalizes Lemma 5.1 in [41]. This proposition and its corollary provide a useful way of eliminating certain cases in the next section, especially since we will be dealing with non-semisimple Hopf algebras.

**Proposition 4.1.4.** Let \( H \) be a finite-dimensional Hopf algebra over \( k \). If there exist semisimple Hopf subalgebras \( A \subseteq H \) and \( K \subseteq H^* \) such that

\[ \dim H = (\dim A)(\dim K) \quad \text{and} \quad \gcd(\dim A, \dim K) = 1 \]

then \( H \) is semisimple.

**Proof.** Define the Hopf algebra surjection

\[ \pi : H \cong H^{**} \xrightarrow{i^*} K^* \]

where \( i : K \to H^* \) is inclusion. As gcd(\( \dim A, \dim K \)) = 1, it follows that the image of \( A \) under \( \pi \) is one-dimensional, and so \( \pi(A) = k[1] \). Note then that for any \( a \in A \), \( \pi(a) = \gamma(a)1 \), for some \( \gamma(a) \in k \). Applying \( \epsilon \) yields

\[ \epsilon(a) = \epsilon(\pi(a)) = \gamma(a)\epsilon(1) = \gamma(a) \]

since \( \pi \) is a coalgebra homomorphism. Therefore \( \pi(a) = \epsilon(a)1 \), which further implies that

\[ a_1 \otimes \pi(a_2) = a_1 \otimes \epsilon(a_2)1 = a \otimes 1 \]
for any \( a \in A \). Therefore

\[
A \subseteq H^{\text{co} \pi} = \{ h \in H \mid h_1 \otimes \pi(h_2) = h \otimes 1_{K^*} \}.
\]

But \( \dim H^{\text{co} \pi} = \dim H/ \dim K = \dim A \) and so \( A = H^{\text{co} \pi} \). It follows by Schneider’s result in Theorem 2.3.19 that \( H \) is isomorphic to a cross product algebra \( A \#_{\sigma} K^* \) for some 2-cocycle \( \sigma \). By Blattner and Montgomery’s result in Theorem 2.3.20, the semisimplicity of \( A \) and \( K^* \) implies the semisimplicity of \( H \).

**Corollary 4.1.5.** Suppose \( n \) is an odd integer. If \( H \) is a 2\( n \)-dimensional Hopf algebra over the field \( k \), and \( H \) contains a semisimple Hopf subalgebra of dimension \( n \), then \( H \) is semisimple.

**Proof.** Let \( K \) be a semisimple Hopf subalgebra of \( H \) with \( \dim K = n \). Then there is a Hopf algebra surjection \( \pi : H^* \to K^* \) and \( K^* \) is semisimple. By Proposition 4.1.2, we have the exact sequence of Hopf algebras

\[
1 \to k[\mathbb{Z}_2] \to H^* \xrightarrow{\pi} K^* \to 1.
\]

That is, \( H^* \) has a semisimple Hopf subalgebra of dimension 2. By Proposition 4.1.4, \( H \) is semisimple. \( \square \)

The next proposition implies the existence of some semisimple Hopf subalgebras in the dual of an extension of a finite group algebra by a Taft algebra. We will need this result in the proof of Lemma 4.3.4 in the last section of this chapter.

**Proposition 4.1.6.** Let \( H \) be a finite-dimensional Hopf algebra over \( k \) and \( A \) a normal Hopf subalgebra of \( H \) such that \( H/HA^+ \) is isomorphic to \( k[G] \) for some finite group \( G \). If the Jacobson radical \( J \) of \( A \) is a Hopf ideal of \( A \), then \( HJ \) is a Hopf ideal of \( H \), and we have the exact sequence

\[
1 \to A/J \to H/HJ \to k[G] \to 1
\]

of Hopf algebras. In particular, \( H^* \) admits a semisimple Hopf subalgebra of dimension \( |G| \dim(A/J) \).

**Proof.** Since \( H/HA^+ \cong k[G] \) as Hopf algebras, by results of Schneider [52], the (right) \( k[G] \)-extension \( A \leftarrow H \) is \( H \)-cleft. Therefore, there exists a convolution invertible right \( k[G] \)-
comodule map $\gamma : \mathbb{k}[G] \to H$ with the convolution inverse $\overline{\gamma}$ such that

$$\gamma(1) = 1_H \quad \text{and} \quad \gamma(g)A\overline{\gamma}(g) \subseteq A$$

for all $g \in G$, and

$$\sigma(g, h) = \gamma(g)\gamma(h)\overline{\gamma}(gh)$$

for $g, h \in G$ defines a 2-cocycle $\sigma : \mathbb{k}[G] \otimes \mathbb{k}[G] \to A$, by Theorem 2.3.18. Moreover, the $k$-linear map

$$\Phi : A \#_k \mathbb{k}[G] \to H$$

defined by

$$\Phi(a \# g) = a\gamma(g)$$

is an algebra isomorphism (see the remark after Theorem 2.3.18 or [37, Chapter 7]). In particular, $H = \bigoplus_{g \in G} A\gamma(g)$ as $k$-vector spaces.

Notice that $\gamma(g)$ is an invertible element of $H$ with inverse $\overline{\gamma}(g)$ for all $g \in G$, since

$$\gamma(g)\overline{\gamma}(g) = \gamma \ast \overline{\gamma}(g) = 1_H.$$ 

Therefore, $a \mapsto \gamma(g)a\overline{\gamma}(g)$ defines an algebra automorphism on $A$. In particular, this mapping preserves $J$ and so

$$J = \gamma(g)J\overline{\gamma}(g).$$

Thus,

$$\gamma(g)A = A\gamma(g), \quad \gamma(g)J = J\gamma(g) \quad \text{for all} \quad g \in G$$

and so

$$JH = \sum_{g \in G} JA\gamma(g) = \sum_{g \in G} J\gamma(g) = \sum_{g \in G}\gamma(g)J = \sum_{g \in G} \gamma(g)AJ = HJ,$$

implying that $HJ$ is a nilpotent Hopf ideal of $H$.

If $a \in A \cap HJ$, then $Aa \subseteq HJ$ is also nilpotent, and so $a \in J$. Therefore, the natural map $\iota : A/J \to H/HJ$ induced from the inclusion map $i : A \to H$ is also injective. Since $A$ is normal in $H$, $\iota(A/J)$ is normal in $H/HJ$. Let $\pi : H/HJ \to H/HA^+$ be the natural surjection.
It is immediately seen that \( \ker \pi = HA^+/HJ = (H/HJ)_\nu(A/J)^+ \). Therefore, the sequence of finite-dimensional Hopf algebras

\[
1 \to A/J \xrightarrow{\iota} H/HJ \xrightarrow{\pi} H/HA^+ \to 1
\]

is exact. Consequently, \( H/HJ \) is a crossed product \( A/J \#_{\tau} \mathbb{k}[G] \), for some 2-cocycle \( \tau \), and hence semisimple by Theorem 2.3.20. Moreover, \( \dim H/HJ = |G| \dim(A/J) \). Due to the canonical Hopf algebra surjection

\[
\nu : H \to H/HJ
\]

we have that

\[
\nu^* : (H/HJ)^* \to H^*
\]

is a Hopf algebra injection and so \((H/HJ)^*\) is isomorphic to a Hopf subalgebra of \(H^*\). Therefore the second statement of the proposition follows as \((H/HJ)^*\) is also semisimple by Theorem 2.3.11.

We close this section with a few results on linear algebra which will be used frequently together with Lemma 4.1.1 to determine the order of an antipode in the next section. The first two results are known, and we prove the third.

**Lemma 4.1.7.** Let \( V \) be a finite-dimensional vector space over the field \( \mathbb{k} \), \( p \) a prime, and \( T \) a linear automorphism on \( V \) such that \( \text{Tr}(T) = 0 \).

(a) [5, Lemma 2.6] If \( T^{2p} = \text{id}_V \), then \( \text{Tr}(T^p) = pd \) for some integer \( d \).

(b) [43, Lemma 1.4] If \( T^n = \text{id}_V \) for some positive integer \( n \), then \( p \) divides the dimension of \( V \).

(c) If \( \dim V = p \) and \( T^m = \text{id}_V \) for some positive integer \( m = 2^np \), where \( p \) is odd, then

\( T^p = \xi \text{id}_V \) for some \( 2^n \)-th root of unity \( \xi \in \mathbb{k} \).

*Proof.* We prove part (c). The statement is obviously true for \( n = 0 \). We assume \( n \geq 1 \). Let \( \omega \in \mathbb{k} \) be a primitive \( m \)-th root of unity, and \( V_\omega \) the eigenspace of \( T \) associated to the eigenvalue
We consider the polynomial
\[
f(x) = \sum_{b=0}^{m-1} (\dim V_b)x^b \in \mathbb{Z}[x].
\]
Since
\[
0 = \text{Tr}(T) = \sum_{b=0}^{m-1} (\dim V_b)\omega^b = f(\omega),
\]
we have \(f(x) = g(x)\Phi_m(x)\) for some \(g(x) \in \mathbb{Z}[x]\) where \(\Phi_k\) denotes the \(k\)-th cyclotomic polynomial. Therefore,
\[
\text{Tr}(T^p) = f(\omega^p) = g(\omega^p)\Phi_m(\omega^p).
\] (4.4)
Note that \(\{\omega^{pi} | i = 0, \ldots, 2^n-1\}\) is a basis for \(\mathbb{Q}(\omega^p)\) and \(\Phi_m(x) = \Phi_p(-x^{2^n-1})\). Therefore,
\[
\Phi_m(\omega^p) = \Phi_p(-\omega^p)^{2^n-1} = \Phi_p(1) = p.
\] (4.5)
Let \(W_i\) be the eigenspace of \(T^p\) associated to the eigenvalue \(\omega^{pi}\). Since
\[
\omega^{p(i+2^n-1)} = -\omega^{pi} \text{ for } i = 0, \ldots, 2^n-1,
\]
we have
\[
\text{Tr}(T^p) = \sum_{i=0}^{2^n-1} (\dim W_i - \dim W_{2^n-1+i})\omega^{pi}.
\]
There exists \(i\) such that \(\dim W_i - \dim W_{2^n-1+i} \neq 0\) otherwise \(\dim V\) is even. By equations (4.4) and (4.5), \(p \mid \dim W_i - \dim W_{2^n-1+i}\). Since \(\dim V = p\), only one of the eigenspaces \(W_i, W_{2^n-1+i}\) is non-zero and any other eigenspace of \(T^p\) is trivial. Thus \(T^p = \xi \text{id}_V\) for some \(2^n\)-th root of unity \(\xi \in k\).

### 4.2 The Order of the Antipode

Throughout the remainder of this chapter, we will assume that \(H\) is a non-semisimple Hopf algebra of dimension \(2p^2\) over \(k\) with antipode \(S\), where \(p\) is an odd prime. We will prove in this section that the antipodes of these Hopf algebras have order \(2p\) (Theorem 4.2.5).

To establish this result, we first consider the distinguished group-like elements \(g \in G(H)\) and \(\alpha \in G(H^*)\). Since
\[
4 \nmid \dim H = 2p^2
\]
it follows by Theorem 3.4.2 that one of the distinguished group-like elements \( g \) or \( \alpha \) is non-trivial. In view of the Nichols-Zoeller Theorem, we have

\[
\text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = 2, p, 2p, p^2 \text{ or } 2p^2.
\]

Without loss of generality, we may assume

\[
\text{ord}(g) \geq \text{ord}(\alpha) \tag{4.6}
\]

by duality. Under this assumption, \( \text{ord}(g) > 1 \).

Let us write \( e_i \) for the idempotent \( e_{g,i} \in k[g] \) defined in (4.1), and \( f_j \) for \( e_{\alpha,j} \in k[\alpha] \). We define

\[
H_{ij} = He_i \leftarrow f_j \tag{4.7}
\]

for all \( i \in \mathbb{Z}_{\text{ord}(g)} \) and \( j \in \mathbb{Z}_{\text{ord}(\alpha)} \). It follows by the remarks before Lemma 4.1.1 that

\[
\dim He_i = \frac{\dim H}{\text{ord}(g)}, \quad \text{and} \quad \text{Tr}(S^2|_{He_i}) = 0
\]

for all \( i \in \mathbb{Z}_{\text{ord}(g)} \). If \( \alpha(g) = 1 \), then we also have by Lemma 4.1.1 that

\[
\dim H_{ij} = \frac{\dim H}{\text{ord}(g) \cdot \text{ord}(\alpha)} \quad \text{and} \quad \text{Tr}(S^2|_{H_{ij}}) = 0 \quad \text{for all } i, j.
\]

We first eliminate those values of \( \text{lcm}(\text{ord}(g), \text{ord}(\alpha)) \) which are not possible.

**Lemma 4.2.1.** *The only possible values of \( \text{lcm}(\text{ord}(g), \text{ord}(\alpha)) \) are \( p \) and \( 2p \).*

*Proof.* Assume that either \( \text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = 2p^2 \) or \( p^2 \). Since \( \text{ord}(g) \geq \text{ord}(\alpha) \), it follows that \( \text{ord}(g) = p^2 \) in both cases. So \( g \) generates a \( p^2 \)-dimensional semisimple Hopf subalgebra of \( H \), which has dimension \( 2p^2 \). By Corollary 4.1.5, \( H \) must be semisimple, which is a contradiction.

If \( \text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = 2 \) then \( \text{ord}(g) = 2 \) and \( \text{ord}(\alpha) = 1 \) or 2. By the remarks before Lemma 4.1.1, \( \dim He_i = p^2 \) and \( \text{Tr}(S^2|_{He_i}) = 0 \) for \( i \in \mathbb{Z}_2 \). Using Radford’s formula Theorem 2.3.7, we have that \( S^8 = \text{id}_H \). In particular, \( (S^2|_{He_i})^4 = \text{id}_{He_i} \). It follows by Lemma 4.1.7 (b) that \( 2 | \dim He_i = p^2 \), another contradiction. \( \square \)
Note that if $\text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = p$ or $2p$, then \(\text{ord}(g) = p\) or $2p$ as we are assuming $\text{ord}(g) \geq \text{ord}(\alpha)$. We first eliminate the possibility that $\text{ord}(g) = p$ and $\text{ord}(\alpha) = 2$.

**Lemma 4.2.2.** The pair $(\text{ord}(g), \text{ord}(\alpha))$ cannot be $(p, 2)$.

**Proof.** Suppose $\text{ord}(g) = p$ and $\text{ord}(\alpha) = 2$. Then by Radford’s formula Theorem 2.3.7, $S^{2p} = \text{id}_H$. We also have that

$$\alpha(g)^2 = \alpha(g^2) = \alpha(1) = 1 = \epsilon(g) = \alpha^p(g) = \alpha(g)^p$$

and so $\alpha(g) = 1$ since $p$ is odd. From Lemma 4.1.1 we get

$$\dim H_{ij} = \frac{\dim H}{\text{ord}(g) \cdot \text{ord}(\alpha)} = p$$

and $\text{Tr}(S^2|_{H_{ij}}) = 0$ for all $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_2$, and $H$ is a direct sum of the subspaces $H_{ij}$ defined in (4.7). By Lemma 4.1.7(c) it follows that $(S^2|_{H_{ij}})^p = \zeta_{ij}\text{id}_{H_{ij}}$ for some 4-th root of unity $\zeta_{ij} \in k$. Since $e_i \leftarrow f_0 = e_i$, and $S^2(e_i) = e_i$, $\zeta_{i0} = 1$ for all $i \in \mathbb{Z}_p$. Let

$$V_j = \bigoplus_i H e_i \leftarrow f_j = H \leftarrow f_j$$

for $j \in \mathbb{Z}_2$. Then $S^{2p}|_{V_0} = \text{id}_{V_0}$. Thus, for $x \in V_0$ we have

$$x = S^{4p}(x) = \alpha \rightarrow x \leftarrow \alpha = \alpha \rightarrow x$$

by Radford’s formula Theorem 2.3.7.

Let $L(\alpha)$ denote the linear operator on $H$ defined by $L(\alpha)(x) = \alpha \rightarrow x$. Then

$$L(\alpha)^2 = \text{id}_H, \quad \text{Tr}(L(\alpha)) = 0, \quad \text{and} \quad \text{Tr}(L(\alpha)|_{V_0}) = p^2.$$

Since $L(\alpha)(V_1) \subseteq V_1$, we have that $L(\alpha)|_{V_1} = -\text{id}_{V_1}$. Therefore

$$\alpha \rightarrow x \leftarrow \alpha = x$$

for all $x \in V_1$, and hence $S^{4p} = \text{id}_H$. It follows that $\zeta_{ij} = \pm 1$ for all $i, j$. Since $p$ is odd, it follows by [42, Corollary 3.2] that the subspace

$$H_- = \{x \in H \mid S^{2p}(x) = -x\}$$
is of even dimension. Since $S^{2p}|_{V_0} = \text{id}_{V_0}$, we have that $H_- \subseteq V_1$.

Let $V_{j+}, V_{j-}$ denote the eigenspaces of $S^{2p}|_{V_j}$ associated to the eigenvalues $1$ and $-1$, respectively. Since the $p$ distinct eigenvalues of $S^2|_{H_1}$ are

$$\zeta_{i1}, \zeta_{i1}\omega, \ldots, \zeta_{i1}\omega^{p-1}$$

where $\omega \in k$ is a primitive $p$-th root of unity and $\zeta_{i1} = \pm 1$ for all $i$, we find

$$\dim\{x \in V_1 \mid S^{2p}(x) = x\} = p \dim V_{1+}, \quad \dim H_- = p \dim V_{1-}.$$ 

Let $\lambda \in H^*$ be a non-zero right integral. We claim that $(x, y) = \lambda(xy)$ defines a non-degenerate alternating form on $V_{1+}$. It follows by [51] that

$$(x, y) = \lambda(xy) = \lambda(S^2(y \rightsquigarrow \alpha)x) = -\lambda(yx) = -(y, x)$$

for all $x, y \in V_{1+}$. Moreover,

$$\lambda(S^2(v)) = \alpha(g)\lambda(v) = \lambda(v) = \lambda(\alpha \rightarrow v) \quad \text{for all } v \in H.$$ 

Therefore, $\lambda(v) = 0$ for any $v \in H$ which satisfies $S^2(v) = \mu v$ or $\alpha \rightarrow v = \mu v$ for some $\mu \in k$ with $\mu \neq 1$. Let $x \in V_{1+}$ such that $\lambda(xy) = 0$ for all $y \in V_{1+}$. Then $\lambda(xy') = 0$ for all $y' \in H$. By the non-degeneracy of $\lambda$ on $H$ as in Proposition 2.3.8, we have $x = 0$ and hence $(\cdot, \cdot)$ is non-degenerate on $V_{1+}$. Since we have a non-degenerate alternating form on $V_{1+}$, it follows that $\dim V_{1+}$ is even. Note that

$$p \dim V_{1+} + \dim H_- = \dim V_1 = p^2$$

and hence $p^2$ is even, a contradiction.

We now proceed to show that $S^{2p} = \text{id}_H$ for the remaining possibilities of $\text{lcm}(\text{ord}(g), \text{ord}(\alpha))$. We will use this to deduce in the next section that $H$ or $H^*$ is pointed.

**Lemma 4.2.3.** If $\text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = 2p$, then $S^{2p} = \text{id}_H$. 

Proof. Under this hypothesis, $S^{8p} = \text{id}_H$ by Radford’s formula Theorem 2.3.7. Moreover, either $\text{ord}(g) = 2p$ or $(\text{ord}(g), \text{ord}(\alpha)) = (p, 2)$. The second case can be eliminated by the preceding lemma. Therefore

$$\text{ord}(g) = 2p \quad \text{and} \quad \dim H_{ei} = p$$

for $i \in \mathbb{Z}_{2p}$. Fix $i \in \mathbb{Z}_{2p}$ and set $T_i = S^2|_{H_{ei}}$. Then $T_i^{4p} = \text{id}_{H_{ei}}$ and $\text{Tr}(T_i) = 0$. By Lemma 4.1.7(c), we have $T_i^p = \zeta_i \text{id}_{H_{ei}}$ where $\zeta_i \in k$ is a 4-th root of unity. Note that

$$T_i(e_i) = S^2(e_i) = e_i.$$ 

Therefore, $\zeta_i = 1$ and so $T_i^p = \text{id}_{H_{ei}}$ for all $i \in \mathbb{Z}_{2p}$. Hence, we get that $S^{2p} = \text{id}_H$ as desired. \hfill \Box

We now deal with the remaining case in the following lemma.

**Lemma 4.2.4.** If $\text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = p$, then $S^{2p} = \text{id}_H$.

**Proof.** The proof will be presented in steps (i)-(v).

(i) Since $\text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = p$, $S^{4p} = \text{id}_H$ by Radford’s formula (Theorem 2.3.7). In particular, the possible eigenvalues of $S^{2p}$ are $\pm 1$. Define

$$H_+ = \{ x \in H \mid S^{2p}(x) = x \} \quad \text{and} \quad H_- = \{ x \in H \mid S^{2p}(x) = -x \}.$$ 

Then we have

$$\dim H_+ + \dim H_- = 2p^2 \quad \text{and} \quad \text{Tr}(S^{2p}) = \dim H_+ - \dim H_-.$$ \hfill (4.8)

(ii) The pair $(\text{ord}(g), \text{ord}(\alpha))$ can either be $(p, 1)$ or $(p, p)$. In both cases, $\text{ord}(g) = p$. Hence $\text{lcm}(\text{ord}(g), \text{ord}(S^4)) = p$, and it follows by [42, Proposition 1.3] that $\dim H_-$ is an even integer.

(iii) We claim that if $(\text{ord}(g), \text{ord}(\alpha)) = (p, p)$, then $\alpha(g) \neq 1$. Otherwise, we can apply Lemma 4.1.1 and get

$$\dim H_{ij} = 2, \quad \text{Tr}(S^2|_{H_{ij}}) = 0, \quad \text{and} \quad H = \bigoplus_{i,j \in \mathbb{Z}_p} H_{ij}$$

where $H_{ij}$ is defined in (4.7). By (i), we find $(S^2|_{H_{ij}})^{2p} = \text{id}_{H_{ij}}$, and so $S^2|_{H_{ij}}$ has exactly two distinct eigenvalues $\pm \xi$ for some $p$-th root of unity $\xi \in k$. Therefore, $\pm 1$ are the two distinct
eigenvalues of $S^{2p}|_{H_{ij}}$. This implies $\dim H_- = \dim H_+ = p^2$ which contradicts (ii).

(iv) We claim that $\text{Tr}(S^{2p}) = p^2d$ for some integer $d$. If $(\text{ord}(g),\text{ord}(\alpha)) = (p,1)$, then $H$ is a unimodular Hopf algebra with $S^{4p} = \text{id}_H$ by (ii). It follows immediately by [41, Lemma 4.3] that $\text{Tr}(S^{2p}) = p^2d$ for some integer $d$. We may now assume $(\text{ord}(g),\text{ord}(\alpha)) = (p,p)$. Let $B = k[g]$ and $I = k[\alpha]^\perp$, which is a Hopf ideal of $H$, and $\overline{H} = H/I \cong k[\alpha]^* \cong B$ by Proposition 2.1.15.

Let $\pi : H \rightarrow B$ be the natural surjection of Hopf algebras. By (iii), $\alpha(g) \neq 1$ and so $g - 1 \notin k[\alpha]^\perp$, or equivalently $\pi(g) \neq 1_{\overline{H}}$. Since $\dim \overline{H} = p$, $\pi(B) = \overline{H}$. Therefore, the composition $\pi \circ i : B \rightarrow \overline{H}$ is an isomorphism of Hopf algebras, where $i : B \rightarrow H$ is inclusion. Thus, there exists a surjective Hopf algebra map $\nu : H \rightarrow B$ such that $\nu \circ i = \text{id}_B$. Hence, by Radford’s result Theorem 2.3.25, $H$ is isomorphic to the biproduct $R \times B$ where $R$ is the right coinvariant given by

$$R = H^{co\nu} = \{ h \in H \mid (\text{id}_H \otimes \nu)\Delta(h) = h \otimes 1_B \}.$$ 

Due to the results in [5, Section 4], $R$ is invariant under $S^2$ and $S^2 = S^2|_R \otimes S^2|_B$ if one identifies $H$ with $R \times B$. Let $T = S^2|_R$. Since $S^2|_B = \text{id}_B$ and

$$0 = \text{Tr}(S^2) = \text{Tr}(T)\text{Tr}(\text{id}_B) = \text{Tr}(T)p,$$

it follows that $\text{Tr}(T) = 0$. Also we have that $T^{2p} = \text{id}_R$ as $S^{4p} = \text{id}_H$. Thus by Lemma 4.1.7(b), $\text{Tr}(T^p) = pd$ for some integer $d$. Therefore,

$$\text{Tr}(S^{2p}) = \text{Tr}(T^p)\text{Tr}(\text{id}_B) = p^2d$$

as claimed.

(v) The equalities in (4.8) imply that $d$ is an even integer. Since

$$-2p^2 \leq \text{Tr}(S^{2p}) \leq 2p^2,$$

it follows that $d$ can only be $-2, 0, or 2$. Note that if $d = -2$ then $S^{2p} = -\text{id}_H$, which is not possible as $S^{2p}(1_H) = 1_H$. If $d = 0$ then $\text{Tr}(S^{2p}) = 0$ and hence $\dim H_+ = \dim H_- = p^2$. But this contradicts (ii) which asserts that $\dim H_-$ is even. Hence $d = 2$ and so $\text{Tr}(S^{2p}) = 2p^2$ which implies that $S^{2p} = \text{id}_H$, as desired.
With the beginning remarks and these four lemmas, we have proven the following theorem.

**Theorem 4.2.5.** Let $p$ be an odd prime, and $H$ a non-semisimple Hopf algebra over $\mathbb{k}$ of dimension $2p^2$. Then the order of the antipode of $H$ is $2p$.

### 4.3 Non-semisimple Hopf Algebras of Dimension $2p^2$

In this section, we will show that if $H$ is a non-semisimple Hopf algebra of dimension $2p^2$ over $\mathbb{k}$, for $p$ an odd prime, then $H$ or $H^*$ is pointed. This completes the proof of our main result. Recall that by Proposition 2.2.16, the dual $H^*$ of a finite-dimensional Hopf algebra $H$ over $\mathbb{k}$ is pointed if all simple $H$-modules are one-dimensional.

We continue to assume that $H$ is a non-semisimple Hopf algebra of dimension $2p^2$ over the field $\mathbb{k}$ with the antipode $S$, where $p$ is an odd prime. Again, we let $g \in G(H)$ and $\alpha \in G(H^*)$ denote the distinguished group-like elements. From Theorem 4.2.5, we know that the order of the antipode $S$ of $H$ is $2p$, and we also know from the previous section that

\[ \text{lcm}(\text{ord}(g), \text{ord}(\alpha)) = p \text{ or } 2p. \]

By duality, we will assume $\text{ord}(\alpha) \geq \text{ord}(g)$ in this section. Therefore, $\text{ord}(\alpha) = p$ or $2p$. Note that the opposite assumption was made in the previous section.

Let $V$ be a left $H$-module. Continue to denote by $V^*$ the usual linear dual of $V$ with left $H$-module action given by

\[ (h \cdot f)(k) = f(S(h) \cdot v) \]

for all $f \in V^*$, $v \in V$, and $h \in H$. For an algebra automorphism $\sigma$ on $H$, let $\sigma V$ be the $H$-module with underlying space $V$ and action given by

\[ h \cdot \sigma v = \sigma(h) \cdot v \]

for all $h \in H$ and $v \in V$. It is easy to verify that the natural isomorphism $j : V \to V^{**}$ of vector spaces is also an $H$-module map from $S^2 V$ to $V^{**}$. Hence,

\[ S^2 V \cong V^{**} \quad \text{for} \quad V \in H\text{-mod fin}. \quad (4.9) \]
Let \( P(V) \) denote the projective cover of \( V \in \text{H-mod}_{\text{fin}} \). For \( \beta \in G(H^*) \), we define \( k_\beta \) as the one-dimensional \( H \)-module which affords the irreducible character \( \beta \). That is, the action in this case is given by
\[
h \cdot k = \beta(h)k
\]
for all \( h \in H \) and \( k \in k \). We will simply denote by \( k \) the trivial one-dimensional \( H \)-module \( k \).

Let us continue to denote by \([V]\) the isomorphism class of a simple \( H \)-module \( V \). The cyclic group \( G = \langle \alpha \rangle \) acts on the set \( \text{Irr}(H) \) of all isomorphism classes of simple \( H \)-modules by setting
\[
\beta[V] = [k_\beta \otimes V]
\]
for all \( \beta \in G \) and \([V] \in \text{Irr}(H)\), where \( k_\beta \otimes V \) has the usual tensor product module structure as in equation (2.13). We denote the \( G \)-orbit of \([V] \) in \( \text{Irr}(H) \) by \( O(V) \). Since \( k_\beta \otimes - \) is a \( k \)-linear equivalence on \( \text{H-mod}_{\text{fin}} \), we have \( P(k_\beta \otimes V) \cong k_\beta \otimes P(V) \) and thus \( \dim P(W) = \dim P(V) \) for all \([W] \in O(V)\). In particular, \( \dim P(k) = \dim P(k_\beta) \) for all \( \beta \in G \). Suppose \([V_0], [V_1], \cdots, [V_t]\) is a complete set of representatives of \( G \)-orbits in \( \text{Irr}(H) \) with \( V_0 = k \).

Since \( H \) is a finite-dimensional Frobenius algebra by Proposition 2.3.8, the regular left \( H \)-module \( HH \) has the decomposition
\[
HH \cong \bigoplus_{[V] \in \text{Irr}(H)} (\dim V) \cdot P(V)
\]
(4.10)
\[
\cong \bigoplus_{\beta \in \langle \alpha \rangle} P(k_\beta) \oplus \bigoplus_{i=1}^t \dim V_i \left( \bigoplus_{[W] \in O(V_i)} P(W) \right)
\]
of principal modules. This decomposition implies that
\[
\dim H = \text{ord}(\alpha) \dim P(k) + \sum_{i>0} |O(V_i)| \dim V_i \cdot \dim P(V_i).
\]
(4.11)

We can now demonstrate that \( \dim P(k) \) can only take two possible values.

**Lemma 4.3.1.** The value of \( \dim P(k) \) can either be \( p \) or \( 2p \).

**Proof.** We have that
\[
P(k) \cong P(k^{**}) \cong P(k)^{**} \cong s^2 P(k)
\]
by (4.9). Since \( S^{2p} = \text{id}_H \), by Lemma B in the Appendix, there exists an \( H \)-module isomorphism
\[
\phi : P(\k) \rightarrow S^2P(\k)
\]
such that \( \phi^p = \text{id}_{P(\k)} \). It follows by a result of Ng [44, Lemma 1.3] that \( \text{Tr}(\phi) = 0 \). In view of [5, Lemma 2.6] or Lemma 4.1.7(b), \( \dim P(\k) = np \) for some positive integer \( n \). But then by equation (4.11),
\[
2p^2 = \dim H \geq p \dim P(\k) = np^2
\]
and so \( n = 1 \) or \( 2 \). Therefore \( \dim P(\k) = p \) or \( 2p \).

In view of Lemma 4.3.1 and the beginning remarks of this section, we find
\[
(\text{ord}(\alpha), \dim P(\k)) = (2p, 2p), (p, 2p), (2p, p) \text{ or } (p, p).
\] (4.12)

The following lemma settles the first three cases.

**Lemma 4.3.2.** The pair \( (\text{ord}(\alpha), \dim P(\k)) \neq (2p, 2p) \). If \( (\text{ord}(\alpha), \dim P(\k)) \) is equal to either \( (p, 2p) \) or \( (2p, p) \), then \( H^* \) is pointed.

**Proof.** Let
\[
H_\alpha = \bigoplus_{\beta \in \langle \alpha \rangle} P(\k_\beta).
\]
Then \( H_\alpha \) is isomorphic to a left submodule of \( HH \), and so \( \dim H_\alpha \leq \dim H = 2p^2 \). By the preceding remark
\[
\dim H_\alpha = \text{ord}(\alpha) \dim P(\k).
\]
Therefore, it cannot be possible to have \( (\text{ord}(\alpha), \dim P(\k)) = (2p, 2p) \). If \( (\text{ord}(\alpha), \dim P(\k)) = (p, 2p) \) or \( (2p, p) \), then \( \dim H_\alpha = \dim H \) and hence \( H \cong H_\alpha \) as left \( H \)-modules. Since all the simple quotients of \( H_\alpha \) are one-dimensional, every simple \( H \)-module is one-dimensional. Therefore, \( H^* \) is pointed by Proposition 2.2.16.

Next we handle the remaining case that \( \text{ord}(\alpha) = \dim P(\k) = p \). Following the terminology in [16], an \( H \)-module \( V \) is called \( \alpha \)-stable if \( \k_\alpha \otimes V \cong V \). We have two subcases; either there exists an \( \alpha \)-stable simple \( H \)-module, or all simple \( H \)-modules are not \( \alpha \)-stable.
Lemma 4.3.3. If \( \text{ord}(\alpha) = \dim P(k) = p \), and all the simple \( H \)-modules are not \( \alpha \)-stable, then \( H^* \) is pointed.

Proof. Since \( \dim P(k) = p = \text{ord}(\alpha) \), it follows by (4.11) that there exists a simple \( H \)-module \( V \) such that \([V] \notin O(k)\). Since

\[
\text{Hom}_H(V^* \otimes P(V), k) \cong \text{Hom}_H(P(V), V \otimes k) \cong \text{Hom}_H(P(V), V)
\]

and \( \dim \text{Hom}_H(P(V), V) = 1 \), we get \( \dim \text{Hom}_H(V^* \otimes P(V), k) = 1 \). Thus, \( P(k) \) is a direct summand of \( V^* \otimes P(V) \). In particular,

\[
\dim V \dim P(V) = \dim(V^* \otimes P(V)) \geq \dim P(k) = p.
\]

Since \( V \) is not \( \alpha \)-stable and \( \text{ord}(\alpha) = p \), we have \( |O(V)| = p \) and so (4.11) implies

\[
2p^2 = \dim H \geq p \dim P(k) + p \dim V \dim P(V) \geq 2p^2.
\]

Therefore, \( \dim V \dim P(V) = p \) which forces \( \dim V = 1 \) and \( \dim P(V) = p \). Thus all simple \( H \)-modules are one-dimensional and so \( H^* \) is pointed. \( \square \)

Lemma 4.3.4. If \( \text{ord}(\alpha) = \dim P(k) = p \), and there exists an \( \alpha \)-stable simple \( H \)-module, then \( H \) is pointed.

Proof. Assume \( V \) is an \( \alpha \)-stable simple \( H \)-module. Then \( O(V) = \{[V]\} \) and \( P(V) \) is also \( \alpha \)-stable. By another result of Ng [44, Lemma 1.4], both \( \dim V \) and \( \dim P(V) \) are multiples of \( p \). Let \( \dim V = np \) and \( \dim P(V) = mp \) for some positive integers \( n \leq m \). By (4.11), we have the inequality

\[
2p^2 = \dim H \geq p \dim P(k) + \dim V \dim P(V) \geq p^2 + nmp^2 = (nm + 1)p^2
\]

which implies \( n = m = 1 \). Hence \( P(V) = V \) and \( \text{Irr}(H) = O(k) \cup \{[V]\} \) by (4.11). It was shown in [44, Lemma 1.1] that if \( W \) is a simple \( H \)-module, then

\[
\text{Soc}(P(W)) \cong k_{\alpha^{-1}} \otimes ^*W
\]
where, in this case, we are denoting by \( *V \) the linear dual \( V^* \) of \( V \) but with \( H \)-module action given by

\[
(h \cdot f)(v) = f(S^{-1}(h) \cdot v)
\]

for all \( h \in H \), \( v \in V \), and \( f \in V^* \). Taking \( W = k \), we get that the socle of \( P(k) \) is \( k_{n-1} \). Therefore,

\[
\text{Hom}_H(P(V), P(k)) = \text{Hom}_H(V, P(k)) = 0
\]

since \( V \not\cong k_{n-1} \). Since \( V \) is the only simple \( H \)-module of dimension greater than 1, all the composition factors of \( P(k) \) are one-dimensional. Now let \( E \) be the full subcategory of all \( M \in H\text{-mod}_{\text{fin}} \) whose composition factors are one-dimensional. So \( E \) is a proper tensor subcategory of \( H\text{-mod}_{\text{fin}} \) with \( P(k) \in E \), and all the simple objects of \( E \) are one-dimensional. There is a Hopf ideal \( I \) of \( H \) such that \( E \) is equivalent to \( H/I\text{-mod}_{\text{fin}} \). Since \( P(k) \) is indecomposable of dimension \( p \), \( H/I \) is not semisimple by a result noted in [16, Section 2]. Thus, the Hopf algebra \( H/I \) is a proper quotient, and it must have dimension \( p^2 \) as all other possibilities (being \( 2, p, 2p \)) are semisimple Hopf algebras by Theorems 3.2.1 and 3.4.3. It follows by Theorem 3.3.2 that \( H/I \cong T_p \) where \( T_p \) is a Taft algebra of dimension \( p^2 \). By Proposition 4.1.2, we have an exact sequence of Hopf algebras

\[
1 \rightarrow k[Z_2] \rightarrow H \rightarrow T_p \rightarrow 1.
\]

Dualizing this sequence, we get the exact sequence

\[
1 \rightarrow T_p \rightarrow H^* \rightarrow k[Z_2] \rightarrow 1
\]

since both \( T_p \) and \( k[Z_2] \) are self-dual. It is well-known that the Jacobson radical \( J \) of the Taft algebra \( T_p \) is a Hopf ideal, and \( T_p/J \cong k[Z_p] \). Applying Proposition 4.1.6, we find \( H \) contains a semisimple Hopf subalgebra \( K \) of dimension \( 2p \). Since \( S^{2p} = id_H \), Theorem 3.3.1 implies that \( K \) is the coradical of \( H \). It follows immediately by Theorem 3.5.2 that \( H \) is pointed. \( \square \)

Combining Lemmas 4.3.1, 4.3.2, 4.3.3, and 4.3.4, we complete the proof of our main result. That is, we have proven the following theorem.

**Theorem 4.3.5.** Let \( p \) be an odd prime and \( k \) an algebraically closed field of characteristic zero. If \( H \) is a non-semisimple Hopf algebra over \( k \) of dimension \( 2p^2 \), then \( H \) or \( H^* \) is pointed.
CHAPTER 5. CONCLUSION AND FURTHER WORK

5.1 Conclusion

With the proof of Theorem 4.3.5 now complete, we have shown that, for any odd prime \( p \), every non-semisimple Hopf algebra of dimension \( 2p^2 \) over an algebraically closed field \( k \) of characteristic zero is pointed or dual to a pointed Hopf algebra. Recall that the classification of pointed Hopf algebras of dimension \( 2p^2 \) given in Theorem 3.5.1 lists exactly \( 4(p-1) \) pointed Hopf algebras of dimension \( 2p^2 \) over \( k \) and that \( 3(p-1) \) of these Hopf algebras have pointed duals. Therefore there are exactly \( 5(p-1) \) non-semisimple Hopf algebras of dimension \( 2p^2 \) which are pointed or dual to a pointed Hopf algebra.

We therefore have the following complete classification of Hopf algebras of dimension \( 2p^2 \) over \( k \), where \( p \) is an odd prime. We use the notation established in Chapter 3.

**Theorem 5.1.1.** Let \( H \) be a Hopf algebra over an algebraically closed field \( k \) of characteristic zero of dimension \( 2p^2 \), where \( p \) is an odd prime. Then exactly one of the following holds:

1. \( H \) is a trivial Hopf algebra;

2. \( H \) is a non-trivial semisimple Hopf algebra isomorphic to either \( B_0 \) or \( B_0^* \);

3. \( H \) is a non-semisimple pointed Hopf algebra isomorphic to one of the \( 4(p-1) \) Hopf algebras of the form \( A(\xi, 1, 0) \), \( A(\xi, 1, 1) \), \( A(\tau, 2r, 0) \), \( A(\xi, 2, 0) \), where \( \xi \) is a primitive \( p \)-th root of unity, \( \tau \) is a fixed primitive \( 2p \)-th root of unity, and \( 1 \leq r \leq p-1 \);

4. \( H \) is a non-semisimple non-pointed Hopf algebra isomorphic to the Hopf algebra \( A(\xi, 1, 1)^* \) for some primitive \( p \)-th root of unity \( \xi \).
Hence, the classification of finite-dimensional Hopf algebras over an algebraically closed field \( \mathbb{k} \) of characteristic zero is complete for Hopf algebras of dimensions \( p, p^2, 2q, \) and \( 2q^2 \), where \( p \) is a prime and \( q \) is an odd prime.

5.2 Further Work

As mentioned in Chapter 3, the classifications of both semisimple and non-semisimple pointed Hopf algebras of dimension \( p^3 \) over \( \mathbb{k} \), for \( p \) an odd prime, are complete. There is no known example of a non-semisimple Hopf algebra of dimension \( p^3 \) which is neither pointed nor dual to a pointed Hopf algebra. Therefore, one would conjecture that any non-semisimple Hopf algebra of dimension \( p^3 \) over \( \mathbb{k} \) is pointed or isomorphic to the dual of a pointed Hopf algebra. As already stated, this conjecture has been studied by García.

In his paper [18], García breaks the possible non-semisimple Hopf algebras of dimension \( p^3 \) into cases, based on the possible groups of group-like elements in the Hopf algebra \( H \) and its dual \( H^* \). Specifically, since \( 4 \nmid \dim H \), the result due to Ng in Theorem 3.4.2 implies that either \( H \) or \( H^* \) is not unimodular. Therefore \( G(H) \) or \( G(H^*) \) is non-trivial. By duality, we can assume that \( |G(H)| \geq |G(H^*)| \), and by the Nichols-Zoeller Theorem (Theorem 2.3.13) we have that one of the following holds:

1. \( |G(H)| = p^2, |G(H^*)| = p^2 \);
2. \( |G(H)| = p^2, |G(H^*)| = p \);
3. \( |G(H)| = p^2, |G(H^*)| = 1 \);
4. \( |G(H)| = p, |G(H^*)| = p \);
5. \( |G(H)| = p, |G(H^*)| = 1 \).

Further, since any group of order \( p^2 \) or \( p \) is abelian, we can specify the exact isomorphism classes of group-like elements possible in each case.
Following García’s terminology, we say that a Hopf algebra is of type \((p_{i_1}, \ldots, p_{i_s}; p_{j_1}, \ldots, p_{j_t})\) if \(G(H) \cong \mathbb{Z}_{p_{i_1}} \times \cdots \times \mathbb{Z}_{p_{i_s}}\) and \(G(H^*) \cong \mathbb{Z}_{p_{j_1}} \times \cdots \times \mathbb{Z}_{p_{j_t}}\). García gave the following result [18, Theorem 3.5].

**Theorem 5.2.1.** Let \(H\) be a Hopf algebra over \(k\) of dimension \(p^3\), for \(p\) a prime.

1. Neither \(H\) nor \(H^*\) is of the type \((1; 1), (p, p; 1), (p, p; p^2)\), or \((p^2; 1)\).

2. If \(H\) is non-semisimple and of type \((p, p; p, p), (p^2; p), or (p^2; p^2)\), then \(H\) is pointed.

The only possible cases that are then left to consider are non-semisimple \(p^3\)-dimensional Hopf algebras of types \((p; 1)\) and \((p; p)\). García shows a few general results about such Hopf algebras of type \((p; p)\), but is not able to complete either of these subcases. Combining the techniques that García uses and the techniques illustrated in this thesis, it may be possible to finish the classification of Hopf algebras of dimension \(p^3\) for a prime \(p\) by proving the following conjecture.

**Conjecture 5.2.2.** Let \(H\) be a non-semisimple Hopf algebra of dimension \(p^3\) over an algebraically closed field of characteristic zero, where \(p\) is a prime. Then \(H\) or \(H^*\) is pointed.

Another direction for possible future research involves Hopf algebras of dimension \(2pq\), where \(p < q\) are odd primes. Recall from the discussion in Chapter 3 that the classification of Hopf algebras of dimension \(pq\), for \(p\) and \(q\) distinct odd primes, is not yet complete. However, as we noted in Theorem 3.4.4, Ng has shown that if \(2 < p < q \leq 4p + 11\), then such a Hopf algebra must be semisimple and hence trivial.

More generally, it has been conjectured by Andruskiewitsch [2] that if \(H\) is a Hopf algebra over an algebraically closed field \(k\) of characteristic zero, with

\[
\dim H = p_1 p_2 \cdots p_k
\]

for distinct primes \(p_1, p_2, \ldots, p_k\), then \(H\) is semisimple. Therefore if \(H\) is a Hopf algebra of dimension \(2pq\) for distinct odd primes \(p\) and \(q\), then we expect \(H\) to be semisimple. Since the classification of Hopf algebras of dimension \(2p\) is complete (Theorem 3.4.3) and implies that
every Hopf algebra of dimension $2p$ or $2q$ is semisimple, we may be able to show the following conjecture as a specific case of the broader conjecture.

**Conjecture 5.2.3.** Let $\mathbb{k}$ be an algebraically closed field of characteristic zero and let $p < q$ be odd primes such that any Hopf algebra of dimension $pq$ over $\mathbb{k}$ is semisimple. Then any Hopf algebra of dimension $2pq$ over $\mathbb{k}$ is also semisimple.

In particular, proving this conjecture would show that if $2 < p < q \leq 4p + 11$, then any Hopf algebra of dimension $2pq$ over $\mathbb{k}$ is semisimple. Note however that the techniques used in this thesis have already been applied to the $pq$-dimensional case to achieve Theorem 3.4.4, and so new techniques will need to be implemented in order to show that every Hopf algebra of dimension $pq$ over $\mathbb{k}$ is semisimple. It may be useful and possible, however, to show that any Hopf algebra of dimension $3p$, for $p > 3$ a prime, is semisimple.

Finally, recall that Proposition 4.1.2 (b) shows that if $A$ is an $n$-dimensional Hopf subalgebra of a $2n$-dimensional Hopf algebra $H$, where $n$ is odd, then $A$ is a normal Hopf subalgebra of $H$. As noted before, this partially generalizes the well-known result for finite groups, which states that if $H$ is a subgroup of index $p$ of a finite group $G$ and $p$ is the smallest prime dividing $|G|$, then $H$ is a normal subgroup of $G$. One may hope to prove the following generalization to Hopf algebras, suggested by Susan Montgomery.

**Conjecture 5.2.4.** Let $H$ be a Hopf algebra of dimension $np$ over $\mathbb{k}$, where $p$ is a prime and $n$ is a positive integer such that every prime dividing $n$ is greater than $p$. If $A$ is a Hopf subalgebra of $H$ of dimension $n$, then $A$ is a normal Hopf subalgebra of $H$.

Since no other general result other than Proposition 4.1.2 (b) is known dealing with this conjecture, it would be useful to verify the above conjecture for $p = 3$. In particular, this case may help in completing the classification of Hopf algebras of dimension $3p$, where $p > 3$ is a prime.
Recall that if $A$ is an algebra over $\mathbb{k}$, $\sigma : A \to A$ is an algebra automorphism, and $V$ is an $A$-module, then $\sigma V$ denotes the $A$-module with underlying vector space $V$ and action given by
\[
a \cdot_{\sigma} v = \sigma(a) \cdot v
\]
for all $a \in A$ and $v \in V$.

An linear operator $\sigma : V \to V$ is called **diagonalizable** if there exists a basis $\mathcal{B}$ of $V$ such that the matrix representing $\sigma$ in this basis is a diagonal matrix. A diagonalizable operator $\sigma : V \to V$, also known as a semisimple operator, is one in which the eigenvectors of $\sigma$ constitute a basis of $V$. A linear operator $\sigma : V \to V$ is called unipotent if
\[
id_V - \sigma : V \to V
\]
is a nilpotent operator.

If $\sigma : V \to V$ is a linear automorphism, then there exist unique commuting operators $\sigma_s$ and $\sigma_u$ on $V$ such that
\[
\sigma = \sigma_s \circ \sigma_u
\]
with $\sigma_s$ semisimple and $\sigma_u$ unipotent. This is called the **Jordan-Chevalley decomposition** of the operator $\sigma$.

The following lemma has been used in [44, Lemmas 1.4 and 2.2]. We include a proof for the sake of completeness.

**Lemma A.** Let $A$ be an algebra over an algebraically closed field $\mathbb{k}$, and $\sigma$ a diagonalizable (or semisimple) algebra automorphism on $A$. If $V$ is a finite-dimensional $A$-module isomorphic to
$\sigma V$, then there exists an isomorphism of $A$-modules

$$\phi : V \to \sigma V$$

such that $\phi$ is diagonalizable.

**Proof.** Let $\psi : V \to \sigma V$ be an isomorphism of $A$-modules, and $\rho : A \to \text{End}_k(V)$ the representation of $A$ associated with the $A$-module $V$. Then we have

$$\psi \circ \rho(a) = \rho(\sigma(a)) \circ \psi$$

for all $a \in A$. Suppose $a \in A$ is an eigenvector of $\sigma$ corresponding to the eigenvalue $\gamma$ such that $\rho(a) \neq 0$. Then we have $C_\psi(\rho(a)) = \gamma \rho(a)$ where $C_\psi : \text{End}_k(V) \to \text{End}_k(V)$ is given by

$$C_\psi(g) = \psi \circ g \circ \psi^{-1}$$

for all $g \in \text{End}_k(V)$. In particular, $\rho(a)$ is an eigenvector of $C_\psi$. If $\psi = \psi_s \circ \psi_u$ is the Jordan-Chevalley decomposition of $\psi$, with $\psi_s$ the semisimple part and $\psi_u$ the unipotent part of $\psi$, then $C_{\psi_s}$ is diagonalizable, $C_{\psi_u}$ is unipotent and $C_\psi = C_{\psi_s} \circ C_{\psi_u}$ is the Jordan-Chevalley decomposition of $C_\psi$. Thus, $C_{\psi_s}(\rho(a)) = \gamma \rho(a)$ or

$$\psi_s \circ \rho(a) = \rho(\sigma(a)) \circ \psi_s .$$

for any eigenvector $a \in A$ of $\sigma$. Since $\sigma$ is diagonalizable, $A$ has a basis of eigenvectors of $\sigma$, and so this equality holds for all $a \in A$. Therefore, $\psi_s$ is our desired isomorphism of $A$-modules. \qed

For the purpose of this thesis and future development, we need to establish a more general version of a part of the results obtained in [44, Lemmas 1.4 and 2.2(i)].

**Lemma B.** Let $A$ be a finite-dimensional algebra over an algebraically closed field $k$ of characteristic zero, and $\sigma$ an algebra automorphism on $A$ of order $n$. If $V$ is a finite-dimensional indecomposable $A$-module which is isomorphic to $\sigma V$, then there exists an isomorphism of $A$-modules $\phi : V \to \sigma V$ such that $\phi^n = \text{id}_V$. 
Proof. We simply extract the proof from [44, Lemma 1.4]. It follows by Lemma A that there exists a diagonalizable operator $\phi$ on $V$ such that

$$\phi(av) = \sigma(a)\phi(v)$$

for all $a \in A$ and $v \in V$. Thus, $\phi^n$ is an $A$-module automorphism on $V$, since $\sigma$ has order $n$. Since $\text{End}_A(V)$ is a finite-dimensional local $k$-algebra, $\phi^n = c \cdot \text{id}_V$ for some non-zero scalar $c \in k$. Therefore, if we take $t \in k$ to be an $n$-th root of $c$, then $\frac{1}{t}\phi$ is a desired $A$-module isomorphism. \qed
BIBLIOGRAPHY


ACKNOWLEDGEMENTS

I would like to thank everyone who has helped me write this thesis or in any other aspect of graduate school. In particular, I want to thank my adviser, Richard Ng, for all the help and guidance in the process of earning of my degree. I also want to thank the other members of my committee, Dr. Long, Dr. Smith, Dr. Song, and Dr. Willson, for their support. Special thanks goes to Melanie for all the assistance and advice that she has given to me and all the other graduate students in the Mathematics department. Lastly, I want to thank all my friends at Iowa State for all the fun these past five years.