1996

Semisimplicity for Hopf algebras

Michelle Diane Stutsman

SEMISIMPLICITY FOR HOPF ALGEBRAS

A Project
Presented to the
Faculty of
California State University,
San Bernardino

In Partial Fulfillment
of the Requirements for the Degree
Master of Arts
in
Mathematics

by
Michelle Diane Stutsman
December 1996

SEMISIMPLICITY FOR HOPF ALGEBRAS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Michelle Diane Stutsman

December 1996

Approved by:

[redacted]

Davida Fischman, Chair, Mathematics

12/5/96

Date

[redacted]

Rolland Trapp, Mathematics

[redacted]

Joel Stein, Mathematics

[redacted]

J. Terry Hallet, Graduate Coordinator

[redacted]

Paul Vicknair, Department Chair

Abstract

Hopf algebras are an important area in mathematical research, as Hopf algebras and their actions unify and generalize diverse areas of mathematics and physics. A Hopf algebra H is a special type of algebra that combines an algebra structure with a coalgebra structure, and has an antipode. The antipode is an inverse of the identity map under convolution multiplication in $\mathrm{Hom}(H, H)$.

In this project we state the basic definitions needed to develop a theory of Hopf algebras; in particular, we define algebras and modules, and the dual concepts: coalgebras and comodules. Additionally, we set forth some classical examples of Hopf algebras: the group algebra kG, the linear dual of the group algebra $(kG)^*$, and the universal enveloping algebra $U(L)$ of the Lie algebra L. We then focus on finite dimensional semisimple Hopf algebras.

Semisimple algebras are algebras that can be decomposed into a direct sum of simpler, better understood, pieces; these are simple algebras. Thus it is very useful to know when an algebra is semisimple. In particular, Maschke's theorem is an important tool in understanding the structure of group algebras. The theorem states that a finite dimensional group algebra is a semisimple algebra if and only if the order of the group is not zero in the field k [M 1898]. This theorem has been generalized to Hopf algebras [LS 69]. We give proofs of both theorems and show how the Hopf algebra proof generalizes the classical one. A key tool in the proof of the generalized theorem was the space of integrals in H.

Along the way, we study the concept of semisimplicity in general, to see that every semisimple algebra can be written as a direct product of simple algebras and that this direct product is unique up to isomorphism. Finally, we describe the dual concept, cosemisimplicity, and see that this leads to a "dual Maschke Theorem."

Acknowledgements

I would like to thank Dr. Davida Fischman for all of her help and patience throughout this project process. I would like to thank my husband Bill for his support throughout my Masters degree. And, most importantly I would like to thank my Mom and Dad for their guidance and support throughout my life.

Table of Contents

Abstract iii

Acknowledgements iv

1 Modules and Algebras 1

2 Semisimplicity 18

3 Maschke's Theorem for Group Algebras 28

4 Hopf Algebras 34

5 Integrals 59

6 Maschke's Theorem for Hopf Algebras 63

7 Cosemisimplicity 69

A Linear Algebra 76

B List of Symbols 81

References 82

1 Modules and Algebras

The fundamental concepts of abstract algebra were laid out between 1920 and 1940. In the following years, homological algebra was formed through methods of algebraic topology. It was through Heinz Hopf's work in the late 1930's and early 1940's on the homology and cohomology of topological groups that the basis for Hopf algebras was formed. Heinz Hopf did not formalize the concept himself, as he was considering Poincaré duality on compact manifolds to turn the comultiplication into a multiplication. However it can be seen that the homology or cohomology of a topological group forms a graded Hopf algebra. ([H 41], [Be 85], [Kp 75], [BM 89])

In this paper we mainly consider a special type of Hopf algebra, a finite dimensional semisimple Hopf algebra. We will first go over some of the basic definitions and theorems of semisimplicity and Hopf algebras. Then we will study the property of semisimplicity in a finite dimensional group algebra, and extend this concept to Hopf algebras through a generalization of Maschke's Theorem to finite dimensional Hopf algebras. We are following the formulation and notation of [Mo 93] and [S 69B] for Hopf algebras, and [FD 93]for general ring theoretic ideas and theorems.

We first define a module; this is a generalization of a vector space over a field where the base field is replaced by a ring. Modules first became important in algebra during the late 1920's due to Emmy Noether's insight as to the potential of the module concept [J 74]. Now let us look at a formal definition of a module.

Definition 1.1 Let R be a ring. A **left** R**-module** is an Abelian group M, written additively, on which R acts linearly; that is, there is a map $R \times M \rightarrow M$, called the action of R on M, and denoted by $(r, m) \mapsto r \cdot m$ for $r \in R$, and $m \in M$, for which

1. $(r+s) \cdot m = r \cdot m + s \cdot m$,

2. $r \cdot (m+n) = r \cdot m + r \cdot n$,

3. $(rs) \cdot m = r(s \cdot m)$,

4. $1 \cdot m = m$

$\forall\, r, s \in R$ and $m, n \in M$.

Next, let us review some basic examples of modules.

Example 1.2 The set of complex numbers, $\mathbb{C}$, is a module over the set of real numbers, $\mathbb{R}$, via left multiplication. That is $r \cdot (a+bi) = ra + rbi \quad \forall\, r \in \mathbb{R}$ and $a + bi \in \mathbb{C}$.

We know that $\mathbb{R}$ is a ring, and that $\mathbb{C}$ is an additive Abelian group, so all that needs to be shown are the remaining four properties of a module. Let $a+bi, c+di \in \mathbb{C}$, where $a, b, c, d \in \mathbb{R}$, and let $r, s \in \mathbb{R}$. Then:

1.
$$\begin{aligned}(r+s) \cdot (a+bi) &= ra + rbi + sa + sbi \\ &= r \cdot (a+bi) + s \cdot (a+bi),\end{aligned}$$

2.
$$\begin{aligned}r \cdot [(a+bi) + (c+di)] &= r \cdot [(a+c) + (b+d)i] \\ &= r(a+c) + r(b+d)i \\ &= ra + rc + (rb + rd)i \\ &= ra + rc + rbi + rdi \\ &= ra + rbi + rc + rdi \\ &= r \cdot (a+bi) + r \cdot (c+di),\end{aligned}$$

3.
$$\begin{aligned}(rs) \cdot (a+bi) &= rsa + rsbi \\ &= r \cdot (sa + sbi) \\ &= r \cdot [s \cdot (a+bi)],\end{aligned}$$

4.
$$\begin{aligned}1 \cdot (a+bi) &= 1a + 1bi \\ &= a + bi.\end{aligned}$$

Thus $\mathbb{C}$ is an $\mathbb{R}$-module.

Example 1.3 The set of $n \times n$ matrices over a field k, $M_n(k)$, is a k-module via left scalar multiplication. That is $\forall\, r \in k$ and $M \in M_n(k)$, where $m_{ij} \in k \quad \forall\, i,j \in \{1,2,\ldots,n\}$,

$$r \cdot M = \begin{pmatrix} rm_{11} & rm_{12} & \cdots & rm_{1n} \\ rm_{21} & rm_{22} & \cdots & rm_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ rm_{n1} & rm_{n2} & \cdots & rm_{nn} \end{pmatrix}.$$

The set of $n \times n$ matrices $M_n(k)$ is an (additive) Abelian group and since k is a field, k is in particular a ring. So all that needs to be shown are the remaining four properties of a module. Let $M, N \in M_n(k)$, where $m_{ij}, n_{ij} \in k \quad \forall\, i,j \in \{1,\ldots,n\}$, and let $r, s \in k$. Then:

1.

$$\begin{aligned}
(r+s)\cdot M &= \begin{pmatrix} (r+s)m_{11} & (r+s)m_{12} & \cdots & (r+s)m_{1n} \\ (r+s)m_{21} & (r+s)m_{22} & \cdots & (r+s)m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ (r+s)m_{n1} & (r+s)m_{n2} & \cdots & (r+s)m_{nn} \end{pmatrix} \\
&= \begin{pmatrix} rm_{11}+sm_{11} & \cdots & rm_{1n}+sm_{1n} \\ rm_{21}+sm_{21} & \cdots & rm_{2n}+sm_{2n} \\ \vdots & \ddots & \vdots \\ rm_{n1}+sm_{n1} & \cdots & rm_{nn}+sm_{nn} \end{pmatrix} \\
&= \begin{pmatrix} rm_{11} & \cdots & rm_{1n} \\ rm_{21} & \cdots & rm_{2n} \\ \vdots & \ddots & \vdots \\ rm_{n1} & \cdots & rm_{nn} \end{pmatrix} + \begin{pmatrix} sm_{11} & \cdots & sm_{1n} \\ sm_{21} & \cdots & sm_{2n} \\ \vdots & \ddots & \vdots \\ sm_{n1} & \cdots & sm_{nn} \end{pmatrix} \\
&= r\cdot M + s\cdot M,
\end{aligned}$$

2.

$$
\begin{aligned}
r\cdot(M+N) &= r\cdot\begin{pmatrix} m_{11}+n_{11} & m_{12}+n_{12} & \cdots & m_{1n}+n_{1n} \\ m_{21}+n_{21} & m_{22}+n_{22} & \cdots & m_{2n}+n_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1}+n_{n1} & m_{n2}+n_{n2} & \cdots & m_{nn}+n_{nn} \end{pmatrix} \\
&= \begin{pmatrix} r(m_{11}+n_{11}) & r(m_{12}+n_{12}) & \cdots & r(m_{1n}+n_{1n}) \\ r(m_{21}+n_{21}) & r(m_{22}+n_{22}) & \cdots & r(m_{2n}+n_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ r(m_{n1}+n_{n1}) & r(m_{n2}+n_{n2}) & \cdots & r(m_{nn}+n_{nn}) \end{pmatrix} \\
&= \begin{pmatrix} rm_{11}+rn_{11} & \cdots & rm_{1n}+rn_{1n} \\ rm_{21}+rn_{21} & \cdots & rm_{2n}+rn_{2n} \\ \vdots & \ddots & \vdots \\ rm_{n1}+rn_{n1} & \cdots & rm_{nn}+rn_{nn} \end{pmatrix} \\
&= \begin{pmatrix} rm_{11} & \cdots & rm_{1n} \\ rm_{21} & \cdots & rm_{2n} \\ \vdots & \ddots & \vdots \\ rm_{n1} & \cdots & rm_{nn} \end{pmatrix} + \begin{pmatrix} rn_{11} & \cdots & rn_{1n} \\ rn_{21} & \cdots & rn_{2n} \\ \vdots & \ddots & \vdots \\ rn_{n1} & \cdots & rn_{nn} \end{pmatrix} \\
&= r\cdot M + r\cdot N,
\end{aligned}
$$

3.

$$
\begin{aligned}
(rs)\cdot M &= \begin{pmatrix} (rs)m_{11} & (rs)m_{12} & \cdots & (rs)m_{1n} \\ (rs)m_{21} & (rs)m_{22} & \cdots & (rs)m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ (rs)m_{n1} & (rs)m_{n2} & \cdots & (rs)m_{nn} \end{pmatrix} \\
&= \begin{pmatrix} r(sm_{11}) & r(sm_{12}) & \cdots & r(sm_{1n}) \\ r(sm_{21}) & r(sm_{22}) & \cdots & r(sm_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ r(sm_{n1}) & r(sm_{n2}) & \cdots & r(sm_{nn}) \end{pmatrix} \\
&= r\cdot\begin{pmatrix} sm_{11} & sm_{12} & \cdots & sm_{1n} \\ sm_{21} & sm_{22} & \cdots & sm_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ sm_{n1} & sm_{n2} & \cdots & sm_{nn} \end{pmatrix} \\
&= r\cdot(s\cdot M),
\end{aligned}
$$

4.

$$1 \cdot M = \begin{pmatrix} 1m_{11} & 1m_{12} & \cdots & 1m_{1n} \\ 1m_{21} & 1m_{22} & \cdots & 1m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1m_{n1} & 1m_{n2} & \cdots & 1m_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{pmatrix}$$

$$= M.$$

Thus $M_n(k)$ is a k-module.

A module can be defined equivalently using "map diagrams." We want to redefine this concept here in this way. Similarly, after defining an algebra in the traditional way, we will redefine an algebra using map diagrams so that we may dualize the map diagrams (or turn all of the arrows around). This dualization will yield more structures such as comodules and coalgebras, which are used to form Hopf algebras.

Note that the following definition of a module uses an algebra A, whereas Definition 1.1 used a ring R. The algebra A is required here so that the tensor product may be used. If we used the ring R, this tensor product would not be possible.

Definition 1.4 For a k-algebra A, a (left) **A-module** is a k-space M with three k-linear maps: multiplication $\mu : A \otimes A \to A$, unit $\eta : k \to A$, and the action $\gamma : A \otimes M \to M$ such that the following diagrams commute:

1.

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

2.

$$\begin{tikzcd}
k \otimes M \arrow[r, "\eta\otimes id"] \arrow[dr, "\text{scalar mult.}"'] & A \otimes M \arrow[d, "\gamma"] \\
 & M
\end{tikzcd}$$

To see that this definition is equivalent to Definition 1.1 for a module when $R = A$ is an algebra, we will first show that Definition 1.4 implies Definition 1.1. Note that Definition 1.4 always implies Definition 1.1 since an algebra is a ring. But when we show Definition 1.1 implies Definition 1.4 we need $R = A$ a k-algebra so that the tensor product is defined.

From Definition 1.4 we know that M is a k-space, so in particular M is an Abelian group (by the definition of a vector space). We also have a k-linear map $\gamma : A \otimes M \to M$ giving the action. Using this linearity we get

$$(a + b) \cdot m = a \cdot m + b \cdot m$$

and

$$a \cdot (m + n) = a \cdot m + a \cdot n,$$

the first two properties of a module in Definition 1.1. Using elements on the commutative diagrams, where $a, b \in A$, and $m \in M$, we get

$$\begin{tikzcd}
a \otimes b \otimes m \arrow[r, "\mu\otimes id"] \arrow[d, "id\otimes\gamma"'] & ab \otimes m \arrow[d, "\gamma"] \\
a \otimes b \cdot m \arrow[r, "\gamma"] & a \cdot (b \cdot m) = (ab) \cdot m
\end{tikzcd}$$

Thus $(ab) \cdot m = a \cdot (b \cdot m)$, property three in the original module definition. From the second diagram we get

$$\begin{tikzcd}
1_k \otimes m \arrow[r, "\eta\otimes id"] \arrow[dr] & 1_A \otimes m \arrow[d, "\gamma"] \\
 & m = 1_A \cdot m
\end{tikzcd}$$

Thus $1_A \cdot m = m$, the fourth property of a module. So, Definition 1.4 implies Definition 1.1.

To show Definition 1.1 implies Definition 1.4, consider the following. From Definition 1.1 we know that M is an additive Abelian group, plus the additional four properties:

1. $(r + s) \cdot m = r \cdot m + s \cdot m$,

2. $r \cdot (m + n) = r \cdot m + r \cdot n$,

3. $(rs) \cdot m = r(s \cdot m)$,

4. $1 \cdot m = m$

$\forall\, r, s \in R,\ m, n \in M$. Together these facts make M a vector space and meet the criterion for the two diagrams to be commutative. Notice that R is a ring, thus all that needs to be shown is that R is a k-module. But $R = A$ is a k-algebra (we will recall this definition of an algebra in Definition 1.5). Therefore, R is a k-module. Thus Definition 1.1 implies Definition 1.4, and the two definitions are equivalent.

The concept of an algebra has been known longer than that of a module: in 1903 the American Leonard Eugene Dickson (1874-1954), the first person to recieve a doctorate in mathematics from the University of Chicago, published an axiomatic definition of a linear associative algebra over an abstract field [BM 89]. The following is a generally accepted definition of an algebra today.

Definition 1.5 An (associative) **algebra** over a field k is an (associative) ring A which is also a module over k, such that the ring and module multiplication are "associative" in the following way:

$$x(ab) = (xa)b = a(xb) \quad \forall\, x \in k,\ a, b \in A.$$

A is also called a **k-algebra**.

Note that one can also define an algebra over a commutative ring R in the same manner.

Next let us look at two basic examples of algebras; these continue the examples (1.2 and 1.3) of modules given previously.

Example 1.6 The set of complex numbers $\mathbb{C}$ is an algebra over the real numbers $\mathbb{R}$.

From Example 1.2, we know that $\mathbb{C}$ is an $\mathbb{R}$-module. So, all that needs to be shown is the "associativity" of multiplication of $\mathbb{C}$ and $\mathbb{R}$.

Let $a+bi, c+di \in \mathbb{C}$ where $a,b,c,d \in \mathbb{R}$, and let $x \in \mathbb{R}$. Then,

$$\begin{aligned}
x[(a+bi)(c+di)] &= x[(ac-bd)+(ad+bc)i] \\
&= x(ac-bd)+x(ad+bc)i \\
&= xac-xbd+xadi+xbci \\
&= (xa+xbi)(c+di) \\
&= [x(a+bi)](c+di)
\end{aligned}$$

and

$$\begin{aligned}
[x(a+bi)](c+di) &= (xa+xbi)(c+di) \\
&= xac+xadi+xbci-xbd \\
&= axc+axdi+bixc-bxd \\
&= (a+bi)(xc+xdi) \\
&= (a+bi)[x(c+di)].
\end{aligned}$$

Thus $\mathbb{C}$ is an $\mathbb{R}$-algebra.

Example 1.7 The $n \times n$ matrices over the field k, $M_n(k)$, is an algebra over the field k.

From Example 1.3, we know that $M_n(k)$ is a k-module. So, all that needs to be shown is the "associativity" between $M_n(k)$ and k.

Let $M, N \in M_n(k)$ where $m_{ij}, n_{ij} \in k \quad \forall\, i,j \in \{1,2,\ldots,n\}$, and let $x \in k$.

Then,

$$
\begin{aligned}
x(MN) &= x\left[\begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{pmatrix}\begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1n} \\ n_{21} & n_{22} & \cdots & n_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n1} & n_{n2} & \cdots & n_{nn} \end{pmatrix}\right] \\
&= x\begin{pmatrix} \sum_{i=1}^n m_{1i}n_{i1} & \sum_{i=1}^n m_{1i}n_{i2} & \cdots & \sum_{i=1}^n m_{1i}n_{in} \\ \sum_{i=1}^n m_{2i}n_{i1} & \sum_{i=1}^n m_{2i}n_{i2} & \cdots & \sum_{i=1}^n m_{2i}n_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n m_{ni}n_{i1} & \sum_{i=1}^n m_{ni}n_{i2} & \cdots & \sum_{i=1}^n m_{ni}n_{in} \end{pmatrix} \\
&= \begin{pmatrix} x\sum_{i=1}^n m_{1i}n_{i1} & x\sum_{i=1}^n m_{1i}n_{i2} & \cdots & x\sum_{i=1}^n m_{1i}n_{in} \\ x\sum_{i=1}^n m_{2i}n_{i1} & x\sum_{i=1}^n m_{2i}n_{i2} & \cdots & x\sum_{i=1}^n m_{2i}n_{in} \\ \vdots & \vdots & \ddots & \vdots \\ x\sum_{i=1}^n m_{ni}n_{i1} & x\sum_{i=1}^n m_{ni}n_{i2} & \cdots & x\sum_{i=1}^n m_{ni}n_{in} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^n xm_{1i}n_{i1} & \sum_{i=1}^n xm_{1i}n_{i2} & \cdots & \sum_{i=1}^n xm_{1i}n_{in} \\ \sum_{i=1}^n xm_{2i}n_{i1} & \sum_{i=1}^n xm_{2i}n_{i2} & \cdots & \sum_{i=1}^n xm_{2i}n_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n xm_{ni}n_{i1} & \sum_{i=1}^n xm_{ni}n_{i2} & \cdots & \sum_{i=1}^n xm_{ni}n_{in} \end{pmatrix} \\
&= \begin{pmatrix} xm_{11} & xm_{12} & \cdots & xm_{1n} \\ xm_{21} & xm_{22} & \cdots & xm_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ xm_{n1} & xm_{n2} & \cdots & xm_{nn} \end{pmatrix}\begin{pmatrix} n_{11} & n_{12} & \cdots & n_{1n} \\ n_{21} & n_{22} & \cdots & n_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{n1} & n_{n2} & \cdots & n_{nn} \end{pmatrix} \\
&= (xM)N,
\end{aligned}
$$

and

$$
\begin{aligned}
(xM)N &= \begin{pmatrix} \sum_{i=1}^n xm_{1i}n_{i1} & \sum_{i=1}^n xm_{1i}n_{i2} & \cdots & \sum_{i=1}^n xm_{1i}n_{in} \\ \sum_{i=1}^n xm_{2i}n_{i1} & \sum_{i=1}^n xm_{2i}n_{i2} & \cdots & \sum_{i=1}^n xm_{2i}n_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n xm_{ni}n_{i1} & \sum_{i=1}^n xm_{ni}n_{i2} & \cdots & \sum_{i=1}^n xm_{ni}n_{in} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{i=1}^n m_{1i}xn_{i1} & \sum_{i=1}^n m_{1i}xn_{i2} & \cdots & \sum_{i=1}^n m_{1i}xn_{in} \\ \sum_{i=1}^n m_{2i}xn_{i1} & \sum_{i=1}^n m_{2i}xn_{i2} & \cdots & \sum_{i=1}^n m_{2i}xn_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n m_{ni}xn_{i1} & \sum_{i=1}^n m_{ni}xn_{i2} & \cdots & \sum_{i=1}^n m_{ni}xn_{in} \end{pmatrix} \\
&= \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{pmatrix} \begin{pmatrix} xn_{11} & xn_{12} & \cdots & xn_{1n} \\ xn_{21} & xn_{22} & \cdots & xn_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ xn_{n1} & xn_{n2} & \cdots & xn_{nn} \end{pmatrix} \\
&= M(xN).
\end{aligned}
$$

Thus $M_n(k)$ is a k-algebra.

Note: Throughout the rest of this paper we will make the convention that k will denote a field and A will denote an algebra over k.

Just as a module may be defined by maps, so can an algebra. An equivalent definition of an algebra using maps is the following:

Definition 1.8 An (associative) **k-algebra** is a k-vector space A together with two k-linear maps: multiplication $\mu : A \otimes A \to A$, and unit $\eta : k \to A$, such that the following two diagrams commute:

1. Associativity

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

2. Unit

$$
\begin{tikzcd}
 & A \otimes A \arrow[dd, "\mu"] & \\
k \otimes A \arrow[ur, "\eta \otimes id"] \arrow[dr] & & A \otimes k \arrow[ul, "id \otimes \eta"'] \arrow[dl] \\
 & A &
\end{tikzcd}
$$

where the two lower maps in part two of the definition are given by scalar multiplication. The unit diagram gives the usual identity element in A by setting $1_A = \eta(1_k)$.

To see that this definition of an algebra is equivalent to Definition 1.5, first assume A satisfies Definition 1.8. Since A is assumed to be a k-vector space $\forall\, a, b \in A$ and $r, s \in k$ the following are true by the definition of a vector space (Definition A.1):

1. $(r+s)a = ra + sa$,

2. $r(a+b) = ra + rb$,

3. $(rs)a = r(sa)$,

4. $1 \cdot a = a$,

5. $a + b = b + a$,

6. $a + 0 = 0 + a = a$,

7. $-a = (-1)a$,

8. $0 \cdot a = 0$,

9. $(a+b)+c = a+(b+c)$.

The first four are the properties for A to be a k-module. The next five properties ensure that A is an additive Abelian group, so it remains to show the multiplication properties of A.

Applying the associativity map to $a, b, c \in A$ we get the following:

$$\begin{tikzcd}
a \otimes b \otimes c \arrow[r, "\mu\otimes id"] \arrow[d, "id\otimes\mu"'] & ab \otimes c \arrow[d, "\mu"] \\
a \otimes bc \arrow[r, "\mu"] & \begin{array}{c}(ab)c \\ a(bc)\end{array}
\end{tikzcd}$$

Commutativity of this diagram gives $(ab)c = a(bc)$.

Applying the unit map to $a \in A$ we get the following:

$$\begin{tikzcd}
 & 1_A \otimes a \arrow[dd, "\mu"] \\
1_k \otimes a \arrow[ur, "\eta\otimes id"] \arrow[dr] & \\
 & \begin{array}{c}1_A \cdot a \\ 1_k \cdot a = a\end{array}
\end{tikzcd}$$

and

$$\begin{tikzcd}
a \otimes 1_A \arrow[dd, "\mu"'] & \\
 & a \otimes 1_k \arrow[ul, "id\otimes\eta"'] \arrow[dl] \\
\begin{array}{c}a \cdot 1_A \\ a \cdot 1_k = a\end{array} &
\end{tikzcd}$$

The commutativity of these diagrams gives the equalities $1_A \cdot a = a$ and $a \cdot 1_A = a$.

Next, using the fact that μ is a k-linear map we get the distributive properties of rings. Let $a, b, c \in A$, then

$$\begin{aligned} a(b+c) &= \mu(a, b+c) \\ &= \mu(a,b) + \mu(a,c) \\ &= ab + ac, \end{aligned}$$

and

$$\begin{aligned} (a+b)c &= \mu(a+b, c) \\ &= \mu(a,c) + \mu(b,c) \\ &= ac + bc. \end{aligned}$$

Thus A is a ring and a k-module.

For the ring and module compatiblity properties, use the fact that η is a k-linear map. Let $x \in k$ and $a, b \in A$, then

$$\begin{aligned} x(ab) &= x1_A(ab) && \text{definition of unit} \\ &= x\eta(1_k)(ab) && \text{definition } \eta(1_k) = 1_A \\ &= \eta(x)(ab) && \text{linearity of } \eta \\ &= [\eta(x)a]b && \text{associativity in } A \\ &= (xa)b && \text{linearity of } \eta \text{ and fact } \eta(1_k) = 1_A \end{aligned}$$

and

$$\begin{aligned} (xa)b &= [(xa)1_A]b && \text{definition of unit} \\ &= [(xa)\eta(1_k)]b && \text{definition } \eta(1_k) = 1_A \\ &= [x(a\eta(1_k))]b && \text{associativity of } A \text{ as a } k\text{-vector space} \\ &= [a\eta(x)]b && \text{image of } \eta \text{ is in the center of } A \text{ [Ks 95]} \\ &= a[\eta(x)b] && \text{associativity in } A \\ &= a(xb) && \text{linearity of } \eta \text{ and fact } \eta(1_k) = 1_A. \end{aligned}$$

Thus Definition 1.8 implies Definition 1.5.

To show Definition 1.5 implies Definition 1.8, consider the following from Definition 1.5. We know that A is a module over k, a field, thus A is a k-vector space. Since A is an associative ring from Definition 1.5, we know that for $a, b \in A$, $\quad (ab)c = a(bc)$ and $1_A a = a = a 1_A$, thus the associativity and unit diagrams hold. So, Definition 1.5 implies Definition 1.8 and they may be considered equivalent.

Next let us look at an example using this new definition of an algebra. This example is the group algebra kG which Arthur Cayley (1821-1895) introduced in a paper he wrote in 1854 [W 85].

Example 1.9 For any group G the group algebra kG is a k-algebra.

First, let us define the group algebra kG. Let G be an additive group. The group algbebra kG is the set of all formal finite linear combinations of elements of G. That is,

$$kG = \left\{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in k \right\}$$

with formal addition and component-wise multiplication; these behave similarly to addition and multiplication of polynomials.

Here is an example of formal addition:

$$\alpha_1 g + \alpha_2 g + \alpha_3 h = (\alpha_1 + \alpha_2) g + \alpha_3 h$$

$\forall\ \alpha_i \in k$, and $g, h \in G$. The following is an example of component-wise multiplication:

$$(\alpha_1 g + \alpha_2 h)(\alpha_3 g + \alpha_4 l) = \alpha_1 \alpha_3 g^2 + \alpha_1 \alpha_4 gl + \alpha_2 \alpha_3 hg + \alpha_2 \alpha_4 hl$$

$\forall\ \alpha_i \in k$, and $g, h, l \in G$.

To show that kG is an algebra, first note that kG is a vector space, as kG is the set of linear combination of elements of a group G over a field k. Next define multiplication on kG as the map $\mu : kG \otimes kG \to kG$ given by

$$\mu \left(\sum_{g \in G} \alpha_g g \otimes \sum_{h \in G} \beta_h h \right) = \sum_{h, g \in G} \alpha_g \beta_h gh$$

and $\eta : k \to kG$ via

$$\eta(1_k) = 1_G$$

where 1_G is the identity of G. Note μ is bilinear since $\forall\ \alpha, \beta \in k$, and $g, h, l \in kG$:

$$\begin{aligned} \mu((\alpha g + \beta h) \otimes j) &= (\alpha g + \beta h)j && \text{def of } \mu \\ &= (\alpha g)j + (\beta h)j && \text{distributivity} \\ &= \alpha(gj) + \beta(hj) && \alpha, \beta \in k \\ &= \alpha\mu(g \otimes j) + \beta\mu(h \otimes j) && \text{def of } \mu, \end{aligned}$$

and

$$\begin{aligned} \mu(g \otimes (\alpha h + \beta j)) &= g(\alpha h + \beta j) && \text{def of } \mu \\ &= g(\alpha h) + g(\beta j) && \text{distributivity} \\ &= \alpha(gh) + \beta(gj) && \alpha, \beta \in k \\ &= \alpha\mu(g \otimes h) + \beta\mu(g \otimes j) && \text{def of } \mu. \end{aligned}$$

To see that the associativity and unit maps commute, let $g, h, l \in G$ and $\alpha, \beta, \gamma \in k$. Then

$$\sum_{g\in G} \alpha_g g \otimes \sum_{h\in G} \beta_h h \otimes \sum_{l\in G} \gamma_l l \overset{\mu\otimes id}{\mapsto} \sum_{g,h\in G} \alpha_g \beta_h gh \otimes \sum_{l\in G} \gamma_l l \overset{\mu}{\mapsto} \sum_{g,h,l\in G} (\alpha_g\beta_h)\gamma_l(gh)l.$$

In the other direction,

$$\sum_{g\in G} \alpha_g g \otimes \sum_{h\in G} \beta_h h \otimes \sum_{l\in G} \gamma_l l \overset{id\otimes\mu}{\mapsto} \sum_{g\in G} \alpha_g g \otimes \sum_{h,l\in G} \beta_h \gamma_l hl \overset{\mu}{\mapsto} \sum_{g,h,l\in G} \alpha_g(\beta_h\gamma_l)g(hl).$$

These maps commute, since

$$\sum_{g,h,l} (\alpha_g\beta_h)\gamma_l(gh)l = \sum_{g,h,l} \alpha_g(\beta_h\gamma_l)g(hl)$$

by the associativity of the field k and the group G.

For the unit map, the left-hand side yields:

$$1_k \otimes \sum_{g\in G} \alpha_g g \overset{\eta\otimes id}{\mapsto} 1_G \otimes \sum_{g\in G} \alpha_g g \overset{\mu}{\mapsto} 1_G \cdot \sum_{g\in G} \alpha_g g$$

and in the other direction,

$$1_k \otimes \sum_{g\in G} \alpha_g g \overset{\cong}{\mapsto} \sum_{g\in G} \alpha_g g.$$

And the right-hand side of the unit diagram yields:

$$\sum_{g\in G} \alpha_g g \otimes 1_k \overset{id\otimes\eta}{\mapsto} \sum_{g\in G} \alpha_g g \otimes 1_G \overset{\mu}{\mapsto} \left(\sum_{g\in G} \alpha_g g\right) \cdot 1_G$$

and in the other direction,

$$\sum_{g \in G} \alpha_g g \otimes 1_k \overset{\cong}{\mapsto} \sum_{g \in G} \alpha_g g.$$

These diagrams commute since 1_G is the unit in kG. Thus

$$1_G \cdot \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g g \cdot 1_G.$$

So kG is a k-algebra.

To complete this section on algebras, we need the following definition.

Definition 1.10 Let A and B be algebras over a field k. A map $f : A \to B$ is an **algebra morphism** if the following properties are true $\forall\, a_1, a_2 \in A$, and $\alpha \in k$:

1. $f(a_1 a_2) = f(a_1) f(a_2)$,

2. $f(a_1 + a_2) = f(a_1) + f(a_2)$,

3. $f(\alpha a_1) = \alpha f(a_1)$.

We will see examples of algebra morphisms in Chapter 4.

2 Semisimplicity

Semisimplicity allows us to decompose a structure such as an algebra or a module into a direct sum of simpler, better understood pieces. Before we can define semisimplicity we need to look at the definitions of the pieces.

Definition 2.1 A subset N of a module M is called an R-**submodule** of M if N is an (additive) subgroup of M and if $r \cdot n \in N \ \forall \ \ r \in R, \ n \in N$.

A basic example is the following:

Example 2.2 A ring R is an R-module over itself via left multiplication, and the R-submodules of R are the (left) ideals of R.

The "simpler" pieces we mentioned above are defined as follows:

Definition 2.3 A non-zero **module** M is **simple** if it contains no proper non-zero submodule, that is the only submodules of M are $\{0\}$ and M itself.

Let us look at some examples of simple modules.

Example 2.4 The ring of real numbers $\mathbb{R}$ is a simple module over itself, where the module action is left multiplication.

This is true since the $\mathbb{R}$-submodules of $\mathbb{R}$ are the left ideals of $\mathbb{R}$. But $\mathbb{R}$ is a field, and the only ideals in a field are $\{0\}$ and the field itself. Thus $\mathbb{R}$ has no non-zero proper submodules and is therefore simple. This is a particular case of the following example, since $\mathbb{R}$ is also a field.

Example 2.5 Any field k is a simple module.

The only submodules of a field are $\{0\}$ and the field itself. Therefore any field is a simple module over itself.

Before we move onto the next example, we need the following definition.

Definition 2.6 A **ring** is **simple** if it has no non-trivial two-sided ideals.

Example 2.7 The ring $M_n(k)$ is a simple ring.

To verify that this is true, we prove the following more general proposition.

Proposition 2.8 $M_n(R)$ is a simple ring if and only if R is a simple ring.

To help prove this proposition, we first need the following lemma.

Lemma 2.9 A subset J of $M_n(R)$ is a (left/right/two-sided) ideal of $M_n(R)$ if and only if $J = M_n(I)$ for some (left/right/two-sided) ideal I of R.

Proof: ($\Leftarrow$) Let I be a left ideal of R, that is, $ri \in I \quad \forall\, r \in R,\ i \in I$. Let $i_{kj} \in I$ and $r_{kj} \in R$. Then

$$\begin{pmatrix} r_{11} & r_{12} & r_{13} & \cdots & r_{1n} \\ r_{21} & r_{22} & r_{23} & \cdots & r_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & r_{n3} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} i_{11} & i_{12} & i_{13} & \cdots & i_{1n} \\ i_{21} & i_{22} & i_{23} & \cdots & i_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ i_{n1} & i_{n2} & i_{n3} & \cdots & i_{nn} \end{pmatrix} =$$

$$\begin{pmatrix} \sum_{j=1}^n r_{1j}i_{j1} & \sum_{j=1}^n r_{1j}i_{j2} & \cdots & \sum_{j=1}^n r_{1j}i_{jn} \\ \sum_{j=1}^n r_{2j}i_{j1} & \sum_{j=1}^n r_{2j}i_{j2} & \cdots & \sum_{j=1}^n r_{2j}i_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^n r_{nj}i_{j1} & \sum_{j=1}^n r_{nj}i_{j2} & \cdots & \sum_{j=1}^n r_{nj}i_{jn} \end{pmatrix} \in M_n(I)$$

since $r_{kj}i_{lm} \in I \quad \forall\, k, j, l, m \in \{1, 2, \ldots, n\}$ and I is closed under addition and multiplication. Therefore $M_n(I)$ is a left ideal of $M_n(R)$. A similar calculation shows that if I is a right ideal of R then $M_n(I)$ is a right ideal of $M_n(R)$. Hence, if I is a left/right/two-sided ideal of R then $M_n(I)$ is a left/right/two-sided ideal of $M_n(R)$.

($\Rightarrow$) Let $J \subseteq M_n(R)$ be a left ideal of $M_n(R)$. This means $M_n(R)J \subseteq J$. Define $I \subset R$ to be

$$I = \{x \in R \mid x \quad \text{is an element in some matrix of } J\}$$

then $\forall\, X \in J, x = (x_{ij})$,

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & 1 & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & x_{ij} & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in J$$

since J is a left ideal of $M_n(R)$. This means each element in I can be written in a matrix in J with just that element and all other elements 0. We claim that I is an ideal of R. Let $r \in R$ and $x_{ij} \in I$, then

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & r & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & x_{ij} & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & rx_{ij} & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \in J.$$

Thus $rx_{ij} \in I \quad \forall\, r \in R$, so I is a left ideal of R. A similar calculation shows that if J is a right ideal of $M_n(R)$ then I is a right ideal of R. Hence if J is a left/right/two-sided ideal of $M_n(R)$ then I is a left/right/two-sided ideal of R. $\square$

Now we are ready to prove Proposition 2.8.

Proof of Proposition 2.8: ($\Rightarrow$) Let $M_n(R)$ be a simple ring, and let I be an ideal of R. Then $M_n(I)$ is an ideal of $M_n(R)$ by Lemma 2.9. But $M_n(R)$ is simple, that is $M_n(R)$ has no non-trivial ideals. Therefore $M_n(I)$ must be $\{0\}$ or $M_n(R)$. Hence, the only possible ideals of R are $\{0\}$ or R by Lemma 2.9. Thus R is simple.

($\Leftarrow$) Let R be a simple ring. This means that R has no non-trivial two-sided ideals. Let J be an ideal of $M_n(R)$. By Lemma 2.9, the only ideals of $M_n(R)$ are of the form $M_n(I)$, where I is an ideal of R. So, $J = M_n(I)$, for some ideal I of R, but the only ideals of R are $\{0\}$ and R. Thus $J = M_n(0) = \{0\}$ or $J = M_n(R)$. Hence $M_n(R)$ is a simple ring. $\square$

Using Proposition 2.8 to verify Example 2.7, we see that $M_n(k)$ is simple if and only if k is simple. But k is a field, and so by Example 2.5 k is simple. Therefore $M_n(k)$ is also simple.

Now that we have the definitions of submodule and simple module/ring, we are ready for the definition of a semisimple module/ring.

Definition 2.10 A **module** M is called **semisimple** if it is a direct sum (not necessarily finite) of simple modules.

For a basic example of semisimplicity, consider a vector space.

Example 2.11 A vector space V is a semisimple k-module.

Let $\{e_1, e_2, \ldots, e_n\}$ be a basis for V, where e_i is the vector with 1 in the ith place and zeros elsewhere. Each e_i generates a one-dimensional subspace, $E_i = ke_i \quad \forall\, i \in \{1, 2, \ldots, n\}$. Since $\dim_k E_i = 1 \quad \forall\, i$, each E_i has only one basis element, thus no other submodule besides itself may be generated. Hence each E_i is simple. Next look at the direct sum of the E_i's. This direct sum is possible since $E_i \cap E_j = \{0\} \quad \forall\, i, j \in \{1, 2, \ldots, n\}$.

$$E_1 \oplus E_2 \oplus \cdots \oplus E_n = \{\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n \mid \alpha_i \in k \quad \forall\, i\} = V$$

Thus V is semisimple.

For the next example we need the definition of a semisimple ring.

Definition 2.12 A ring R is a (left) **semisimple ring** if R is semisimple as a left R-module.

Example 2.13 Any division ring D is simple, hence semisimple.

Recall that the R-submodules of R are precisely the left ideals of R (Example 2.2). But the only ideals in D are the trivial ideals since D contains a multiplicative inverse for every non-zero element. So the only D-submodules of D are D and $\{0\}$. Thus D is simple, hence semisimple.

To prepare for future work with Hopf algebras we need to know what a simple algebra and a semisimple algebra are; these are defined analogously to rings.

Definition 2.14 An algebra is said to be a **simple algebra** if it has no non-trivial two-sided ideals.

Definition 2.15 An algebra is said to be a **semisimple algebra** if it is a direct sum of simple (left) ideals.

We state here an important classical example of a semisimple algebra; the result was proven by Maschke (see Theorem 3.1). Recall the definition of the group algebra kG in Example 1.9. Then:

Example 2.16 For any finite group G, the group algebra kG is semisimple if $|G|$ is invertible in k.

The following definition and proposition are needed for the next example.

Definition 2.17 Let M be an R-module. Then M is called a **cyclic module** if there exists an element $m \in M$ such that $M = R \cdot m$.

Proposition 2.18 Let M be an R-module. Then the following are equivalent:

1. M is simple.
2. M is cyclic and every non-zero element is a generator, that is $M = R \cdot m$ for every $0 \neq m \in M$.
3. $M \cong R/I$ for some maximal left ideal I of R.

Proof: (1) $\Rightarrow$ (2) Let $0 \neq m \in R$. Then $R \cdot m$ is a non-zero submodule of M since $1 \in R$, so $1 \cdot m = m \neq 0$. But M is simple, so $R \cdot m = M$, which means M is cyclic.
(2) $\Rightarrow$ (3) Define $\varphi : R \to R \cdot m$ via $\varphi(r) = r \cdot m$; then φ is a surjective module map by the hypothesis. Let $I = \ker\varphi$. I is a maximal ideal of R, for if I were not maximal, there would be a non-generating element of M. By the Fundamental Homomorphism Theorem, which states that for a ring homomorphism φ from R to $S, R/\ker\varphi \cong \varphi(R)$ [Ga 94], we have $R/I \cong R \cdot m = M$.
(3) $\Rightarrow$ (1) Let M' be a non-zero submodule of M. (3) says that $M \cong R/I$. The Correspondence Theorem for Modules states that there is a one-to-one correspondence between the set of all submodules of M that contain N and the set of all submodules of M/N for the natural projection map $\pi : M \to M/N$ [AW 92]. So there is an ideal I' such that $I \subset I'$. But I is maximal. Thus $I' = R$, which means $M' = M$. So M is simple. $\square$

For the next two examples we need the following definition:

Definition 2.19 The **endomorphism ring** of the R-module M, denoted $\mathrm{End}_R(M)$, is the set of R-module homomorphisms from M to M. That is, $\mathrm{End}_R(M)$ is the set of maps $f : M \to M$ satisfying $\forall\, m, n \in M$ and $r \in R$:

1. $f(m+n) = f(m) + f(n)$
2. $f(r \cdot m) = r \cdot f(m)$

$\mathrm{End}_R(M)$ is an R-algebra via composition of functions:

$$(fg)(m) = (f \circ g)(m) = f(g(m)).$$

The unit of $\mathrm{End}_R(M)$ is the identity map $id : M \to M$.

We are now ready for our next two examples.

Example 2.20 Any finite dimensional vector space V over a division ring D is a simple $\mathrm{End}_D(V)$-module via $f \cdot v = f(v) \quad \forall\, f \in \mathrm{End}_D(V)$ and $v \in V$.

This is indeed an action of $\mathrm{End}_D(V)$ on V since

$$f \cdot (g \cdot v) = f \cdot g(v) = f(g(v)) = (f \circ g)(v) = (fg) \cdot v,$$

and

$$id \cdot v = id(v) = v \quad \forall\, v \in V,\ f, g \in \ \mathrm{End}_D(V).$$

To show that V is a simple $\mathrm{End}_D(V)$-module, we show that part (2) of Proposition 2.18 is satisfied.

Let $\{e_1, e_2, \ldots, e_n\}$ be a basis for V. Consider $v \in V$. If $v \neq 0$, then v is a linear combination of the basis elements of V. Let $x \in V$, then

$$\begin{array}{rcll} x & = & \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n & \text{some } \alpha_i \in D \\ & = & \alpha_1 f(e_i) + \alpha_2 f(e_j) + \cdots + \alpha_n f(e_k) & \text{since a basis element is mapped to} \\ & & & \text{another basis element by } f \in \mathrm{End}_D(V) \\ & = & f(\alpha_1 e_i + \alpha_2 e_j + \cdots + \alpha_n e_k) & \text{homomorphism} \\ & = & f(v) & \text{for some } v \in V \\ & = & f \cdot v. & \end{array}$$

So $V \subset \mathrm{End}_D(V) \cdot v$. And $\mathrm{End}_D(V) \cdot v \subset V$ since V is a $\mathrm{End}_D(V)$-module. Thus $\mathrm{End}_D(V) \cdot v = V$. So V is cyclic and every $v \in V$ is a generator of V as an $\mathrm{End}_D(V)$-module. Hence V is a simple $\mathrm{End}_D(V)$-module by Proposition 2.18.

Example 2.21 Let V be a finite dimensional vector space over a division ring D. Then $\mathrm{End}_D(V)$ is a semisimple algebra.

Let $\{e_1, e_2, \ldots, e_n\}$ be a basis for V, and define a map

$$\varphi : \mathrm{End}_D(V) \to V \oplus V \oplus \cdots \oplus V \qquad \text{via} \qquad \varphi(f) = (f(e_1), f(e_2), \ldots, f(e_n)).$$

We will show that this map is an isomorphism of $\mathrm{End}_D(V)$-modules. This will mean that $\mathrm{End}_D(V)$ is a semisimple $\mathrm{End}_D(V)$-module since each copy of V is a simple $\mathrm{End}_D(V)$-module (Example 2.20).

We first show that φ is additive, that is $\varphi(f+g) = \varphi(f) + \varphi(g) \quad \forall\, f, g \in \mathrm{End}_D(V)$.

$$\begin{array}{rcll}
\varphi(f+g) & = & ((f+g)(e_1), (f+g)(e_2), \ldots, (f+g)(e_n)) & \text{def of } \varphi \\
& = & (f(e_1)+g(e_1), f(e_2)+g(e_2), \ldots, f(e_n)+g(e_n)) & \text{sum of functions} \\
& = & (f(e_1), f(e_2), \ldots, f(e_n)) + (g(e_1), g(e_2), \ldots, g(e_n)) & \\
& = & \varphi(f) + \varphi(g) & \text{def of } \varphi.
\end{array}$$

The $\mathrm{End}_D(V)$ action on itself is given as usual by left multiplication, which here means composition of functions. $\mathrm{End}_D(V)$ acts on $V \oplus V \oplus V \oplus \cdots \oplus V = V^{(n)}$ "componentwise" (or "diagonally"):

$$f \cdot (v_1, v_2, \ldots, v_n) = (f \cdot v_1, f \cdot v_2, \ldots, f \cdot v_n).$$

We now show that φ commutes with these actions, that is $f \cdot \varphi(g) = \varphi(f \cdot g)$ $\forall\, f, g \in \mathrm{End}_D(V)$.

$$\begin{array}{rcll}
\varphi(f \cdot g) & = & ((f \cdot g)(e_1), (f \cdot g)(e_2), \ldots, (f \cdot g)(e_n)) & \text{def of } \varphi \\
& = & (f(g(e_1)), f(g(e_2)), \ldots, f(g(e_n))) & \text{by left multiplication} \\
& = & f \cdot \varphi(g) & \text{def of } \varphi.
\end{array}$$

So far we have seen that φ is an $\mathrm{End}_D(V)$-module homomorphism.

Next, consider $\ker\varphi$:

$$\begin{array}{rcll}
\ker\varphi & = & \{f \mid \varphi(f) = 0\} & \text{def of kernel} \\
& = & \{f \mid (f(e_1), f(e_2), \ldots, f(e_n)) = 0\} & \text{def of } \varphi \\
& = & \{f \mid f(e_i) = 0 \quad \forall\, i \in \{1, 2, \ldots, n\}\} & \\
& = & \{0\} & \text{since } f \text{ is 0 on the whole basis.}
\end{array}$$

So φ is one-to-one.

To show that φ is onto, let $(v_1, v_2, \ldots, v_n) \in V \oplus V \oplus \cdots \oplus V$. Define n^2 endomorphisms of V by $f_{ij}(e_i) := e_j$; then $\{f_{ij}\}$ is a basis for $\mathrm{End}_D(V)$, and

$$\begin{array}{rcl}
\varphi(f_{ij}) & = & (f_{ij}(e_1), f_{ij}(e_2), \ldots, f_{ij}(e_n)) \\
& = & (0, \ldots, e_j, \ldots, 0)
\end{array}$$

where e_j is in the i^{th} position. Since each v_i is a linear combination of basis elements, there is a linear combination of $\{(0, \ldots, e_j, \ldots, 0)\}$ that equals

$(v_1, v_2, \ldots, v_n)$. That is $\forall\, \alpha_{ij} \in k$,

$$\begin{aligned}(v_1, v_2, \ldots, v_n) &= (\sum_{i=1}^{n} \alpha_{1i} e_i, \ldots, \sum_{i=1}^{n} \alpha_{ni} e_i) \\ &= (\sum_{i=1}^{n} \alpha_{1i} f_{1i}(e_1), \ldots, \sum_{i=1}^{n} \alpha_{ni} f_{ni}(e_n)) \\ &= (\sum_{i=1}^{n} \alpha_{1i} \varphi(f_{1i}), \ldots, \sum_{i=1}^{n} \alpha_{ni} \varphi(f_{ni})).\end{aligned}$$

Thus φ is onto and we are done showing that φ is an isomorphism. So $\mathrm{End}_D(V)$ is semisimple.

Next, we will look at two important theorems in the theory of semisimplicity. The proofs of these two classical theorems may be found in *Noncommutative Algebra* by Benson Farb and R. Keith Dennis as well as in many other places. These two classical theorems for semisimplicity are attributed to Joseph Henry Maclagan Wedderburn (1882-1948) who was the first to develop a general theory of algebras over an arbitrary field [W 85]. Before we state these two theorems we need to define the direct product; this differs from the direct sum in that direct products can involve an infinite number of rings.

Definition 2.22 [AW 92] Let $R_1, R_2, \ldots, R_n$ be finitely many rings and let $\prod_{i=1}^{n} R_i = R_1 \times R_2 \times \cdots \times R_n$ denote the cartesian product set. On the set $\prod_{i=1}^{n} R_i$ we define addition and multiplication componentwise, that is,

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

and

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

to make $\prod_{i=1}^{n} R_i$ into a ring called the **direct product** of $R_1, R_2, \ldots, R_n$.

Theorem 2.23 (Wedderburn Structure Theorem) Every semisimple ring R is isomorphic to a finite direct product of matrix rings over division rings. If R is also commutative, then R is isomorphic to a finite direct product of fields.

Theorem 2.24 (Uniqueness Theorem for Semisimple Rings) If

$$R = \prod_{i=1}^{n} R_i \quad \text{and} \quad R = \prod_{j=1}^{m} R'_j$$

are two product decompositions of a ring R, where each R_i and R'_j is a simple ring, then $n = m$ and there is a one-to-one correspondence $\psi : \{R_i\} \to \{R_j\}$ such that $R_i = \psi(R_i)$.

Together these two theorems say that every semisimple algebra can be written as a direct product of simple algebras and that this direct product is unique up to isomorphism. We will see an example of this later in Example 7.7 where we look at the linear dual to the group algebra $(kG)^*$.

3 Maschke's Theorem for Group Algebras

The goal of this chapter is to prove Maschke's Theorem for group algebras. Heinriche Maschke was a German mathematician who emigrated to America in 1891 in order to work in a university.

Heinrich Maschke was born in Breslau, Germany on October 24, 1853. As a child Maschke showed exceptional mathematical talent and in 1872 he entered the University of Heidelberg. Later he went to Berlin to study under Weierstrass, Kummer, and Kronecker. From there Maschke went to Göttingen, where he received a doctoral degree in 1880.

Maschke then went back to Berlin to teach at the Luisenstädtische Gymnasium. He was quite a successful teacher. However he felt that he would not be permanently satisfied by teaching arithmetic and the basics of algebra and geometry. Maschke's chances for aquiring a position at the university looked slim so he began to study electrotechnics at the Polytechnicum in Charlottenburg in his free time. He then left his teaching position and spent several months in electrical work before coming to the United States where he hoped eventually to acquire a position at a university. He arrived in New York April 1, 1891 where he quickly found a job as an electrician for the Weston Electric Instrument Company of Newark, New Jersey. In the following year he was called to the University of Chicago, then a newly founded university, to become an assistant professor of mathematics. There he was able to teach a multitutde of mathematical subjects as he worked his way up to full professor during his sixteen year career there. One student, G. A. Bliss, stated that Maschke was "brillant but sagacious and without doubt one of the most delightful lecturers on geometry of all times" [SG 34].

In addition to his fulfilling teaching duties, Maschke continued to study mathematics, especially the theory of finite groups of linear substitutions and the theory of quadratic differential quantics. Maschke developed a symbolic method of treatment for quadratic differential quantics. He also played an important role in bringing the importance of group theory to the American mathematicians. He was active in the American Mathematical Society and he gave an address "On Present Problems of Algebra and Analysis" to the St. Louis International Congress of Mathematicians in 1904. Maschke died on March 1, 1908 as a result of an operation he had due to internal disorders.

Maschke proved the following theorem in its matrix form for the case where the field is the field of complex numbers $\mathbb{C}$. The result was published in the article "*Über den arithmetischen Charakter der Substitutionen endlicher Substitutions gruppen*" of Math. Annalen volume 50 in 1898. The validity of his result for any field k where the characteristic of k does not divide the order of the group G was first noted by Leonard Eugene Dickson ([J 80], [Ma 33], [SG 34], [Bo 08]).

Theorem 3.1 (Maschke's Theorem) Let G be a finite group, and k a field. The order of G, $|G|$, is invertible in k if and only if the group algebra kG is a semisimple ring.

Before we prove this theorem we will establish a lemma and a theorem about general modules. These will be used here and later in proving Maschke's Theorem for Hopf algebras.

Lemma 3.2 If M and N are A-modules and $f : M \to N$ is an A-module map then:

1. $\ker f$ is an A-submodule of M
2. $\operatorname{im} f$ is an A-submodule of N.

Proof:

1. Take $m \in \ker f$, $a \in A$; then

$$\begin{aligned} f(a \cdot m) &= a \cdot f(m) && f \text{ is an } A\text{-module map} \\ &= a \cdot 0 && m \in \ker f \\ &= 0. \end{aligned}$$

   So, $a \cdot m \in \ker f$. Next let $m, n \in \ker f$; then

$$\begin{aligned} f(m+n) &= f(m) + f(n) && f \text{ is linear} \\ &= 0 + 0 && m, n \in \ker f \\ &= 0. \end{aligned}$$

   Thus $\ker f$ is an additive subgroup and furthermore an A-submodule of M.

2. Let $f(m) \in \mathrm{im} f$, $a \in A$, then

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

   since f is an A-module map. So $a \cdot f(m) \in \mathrm{im} f$. Next let $f(m), f(n) \in \mathrm{im} f$, then

$$f(m) + f(n) = f(m+n)$$

   since f is linear. So $\mathrm{im} f$ is an additive subgroup. Thus $\mathrm{im} f$ is an A-submodule. □

The following theorem gives equivalent conditions to being a semisimple module. This is an essential ingredient in proving Maschke's Theorem both for group algebras and for Hopf algebras. The proof of Theorem 3.3 is not included here, but it may be found in *Algebra - An Approach via Module Theory* by William A. Adkins and Steven H. Weintraub [AW 92].

Theorem 3.3 If M is an R-module, then the following are equivalent:

1. M is a semisimple module.

2. Every submodule of M is complemented, that is for every submodule $N \subset M$ there exists a submodule $N' \subset M$ such that $N \oplus N' = M$.

3. Every submodule of M is a sum (not necessarily direct) of simple R-modules.

In the following proof we consider kG as a left module over itself via left multiplication. Recall that an algebra is called semisimple if it is semisimple as a module over itself via left multiplication. We are now ready for the proof of Theorem 3.1, Maschke's Theorem, which states that for a finite group G, $|G|^{-1} \in k$ if and only if the group algebra kG is semisimple.

Proof of Theorem 3.1 [J 80]**:** ($\Rightarrow$) Let M be a kG-module, and let N be a kG-submodule of M, that is $\forall\, n \in N$, and $g \in G$, $g \cdot n \in N$. By Corollary A.8 we know that there exists a k-linear projection $\pi : M \to N$.

Now let us define a new map $\tilde{\pi} : M \to N$ by

$$\tilde{\pi}(m) = |G|^{-1} \sum_{g \in G} g^{-1} \cdot (\pi(g \cdot m)) \quad \forall\, m \in M.$$

The map $\tilde{\pi}$ is a kG-module projection onto N since the following conditions hold.

First for $m, n \in M$,

$$\begin{aligned}
\tilde{\pi}(m+n) &= |G|^{-1} \sum_{g \in G} g^{-1} \pi g \cdot (m+n) \\
&= |G|^{-1} \sum_{g \in G} g^{-1} \pi (g \cdot m + g \cdot n) \\
&= |G|^{-1} \sum_{g \in G} g^{-1} \cdot (\pi(g \cdot m) + \pi(g \cdot n)) && \text{linearity of } \pi \\
&= |G|^{-1} \sum_{g \in G} g^{-1} \pi g \cdot m + g^{-1} \pi g \cdot n \\
&= |G|^{-1} \sum_{g \in G} g^{-1} \pi g \cdot m + |G|^{-1} \sum_{g \in G} g^{-1} \pi g \cdot n \\
&= \tilde{\pi}(m) + \tilde{\pi}(n).
\end{aligned}$$

So $\tilde{\pi}$ is k-linear. Moreover, $\forall\, h, g \in G$,

$$\begin{aligned} h^{-1}\tilde{\pi}(h \cdot m) &= |G|^{-1} \sum_{g \in G} h^{-1} g^{-1} \pi(g \cdot (h \cdot m)) \\ &= |G|^{-1} \sum_{g \in G} (gh)^{-1} \pi((gh) \cdot m) && \text{associativity} \\ &= |G|^{-1} \sum_{g \in G} g^{-1} \pi(g \cdot m) && \text{since } \textstyle\sum_{g \in G} \\ &= \tilde{\pi}(m). \end{aligned}$$

So $\tilde{\pi}(h \cdot m) = h \cdot \tilde{\pi}(m) \quad \forall\, m \in M$. Thus $\tilde{\pi}$ is a kG-module homomorphism.

To show $\tilde{\pi}$ is onto N consider the following. For $n \in N$, $\pi(n) = n$ and since N is a kG-submodule $g \cdot n \in N$, so $\pi(g \cdot n) = g \cdot n \quad \forall$. Hence $g^{-1} \cdot \pi(g \cdot n) = g^{-1} g \cdot n = n$ and so

$$\tilde{\pi}(n) = |G|^{-1} \sum_{g \in G} g^{-1} \pi(g \cdot n) = |G|^{-1} \sum_{g \in G} n = |G|^{-1} |G| n = n,$$

thus showing that $N \subset \tilde{\pi}(M)$. Now, for any $m \in M$, $\pi(m) \in N$ so $\pi(g \cdot m) \in N$. But N is a submodule so $g^{-1} \cdot \pi(g \cdot m) \in g^{-1} \cdot N \subset N$. Hence $\tilde{\pi}(m) \in N$. Thus $\tilde{\pi}$ is a projection onto N.

We claim that $\ker\tilde{\pi}$ is a kG-complement to N. Since $\tilde{\pi}$ is a k-linear projection onto N, $\ker\tilde{\pi}$ is a vector space complement to N. Also, since $\tilde{\pi}$ is a kG-module map, $\ker\tilde{\pi}$ is a kG-submodule by Lemma 3.2. Therefore, N has a kG-complement, $\ker\tilde{\pi}$, in M, that is $M = N \oplus \ker\tilde{\pi}$. So by the equivalence of Theorem 3.3 (1) and (2), M is semisimple.

($\Leftarrow$) Consider the element $z = \sum_{g \in G} g \in kG$. Then $\forall\, h \in G$, $hz = z$ since

$$hz = h \sum_{g \in G} g = \sum_{g \in G} hg = \sum_{g \in G} g = z.$$

So $k\{z\}$ is a left ideal of kG.

Now look at z^2:

$$\begin{aligned}
z^2 &= (\sum_{g\in G} g)z && \text{since } z = \textstyle\sum_{g\in G} g \\
&= \sum_{g\in G} gz && \text{linearity} \\
&= \sum_{g\in G} z && \text{since } gz = z \quad \forall\, g \in G \\
&= |G|z && \text{adding } z, |G| \text{ times}
\end{aligned}$$

This means that $z^2 = |G|z$.

Assume now that $|G| = 0$. Then z is a non-zero central element (that is, $hz = zh \quad \forall\, h \in G$) such that $z^2 = 0$. Thus $Z = z(kG)$ is a two-sided ideal and $Z^2 = 0$, since

$$Z^2 = z(kG)z(kG) = z^2(kG)^2 = 0.$$

To complete the proof, we use the concept of a nilpotent ideal: an ideal I is called nilpotent if there exists $n \in \mathbb{Z}$ such that $I^n = 0$. We adapt [L 66] Section 3.3 Proposition 1 and state it for our more special case: If A is a finite dimensional semisimple algebra then A has no non-trivial nilpotent ideals. However, we know that kG is finite dimensional and semisimple by assumption, so it can have no non-trivial nilpotent ideals. So $Z \neq 0$, and $Z^2 = 0$ is a contradiction. Thus $|G| \neq 0$, and since k is a field this is equivalent to saying $|G|^{-1} \in k$. $\square$

4 Hopf Algebras

Hopf algebras arose through the work of Heinz Hopf, especially the work described in his paper [H 41]. Algebraic topologists abstracted from his work and derived the concept of a graded Hopf algebra. Later in the 1960's Hopf algebras began to be studied from a purely algebraic point of view, and the abstract concept of a Hopf algebra was defined.

Heinz Hopf was born November 19, 1894 in Breslau, Germany where he attended school and started his university career. During World War I his studies were interrupted for service in the military. In 1920 Hopf continued his education in Berlin, where he earned his Ph.D. in topological research in 1925 and his "Habilitation" in 1926. In 1931 Hopf became a full professor at the Eidgenössische Technische Hochschule in Zurich.

Most of Heinz Hopf's work was on algebraic topology where he used his great geometric intuition. Hopf inspired a variety of important ideas in various fields including topology, homology, and differential geometry. As a lecturer Hopf was clear, as his voice was well modulated, and his speech was slow and strongly articulated. He was also a fascinating lecturer as he would ask marvelous questions and greatly encourage his students. According to Peter J. Hilton, Hopf gave the impression to his readers that "you could have done this, I'm just setting it out." Henry Whitehead said "For Hopf, mathematics was always a question." [AA 85] Heinz Hopf died in Zollikon, Switzerland on June 3, 1971 ([Ks 95], [Gi 72], [P 94], [Ab 77], [AA 85]).

Our definitions and notation will mostly follow [Mo 93]; this is essentially the notation and definitions of [Ab 77] and [S 69B]. The first step in defining Hopf algebras is to dualize the definition of an algebra. Here we see the beauty of the "diagram definitions", and make essential use of them.

Definition 4.1 A **k-coalgebra** (with counit) is a k-vector space C together with two k-linear maps, **comultiplication** $\Delta : C \to C \otimes C$ and **counit** $\varepsilon : C \to k$, such that the following diagrams are commutative:

1. Coassociativity

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

2. Counit

$$\begin{tikzcd}
& C \arrow[dl, "1\otimes"'] \arrow[dr, "\otimes 1"] \arrow[dd, "\Delta"] & \\
k \otimes C & & C \otimes k \\
& C \otimes C \arrow[ul, "\varepsilon \otimes id"] \arrow[ur, "id \otimes \varepsilon"'] &
\end{tikzcd}$$

The two upper maps in the counit diagram are $c \mapsto 1 \otimes c$ and $c \mapsto c \otimes 1$, for any $c \in C$.

Note that the image under Δ of $c \in C$ is a sum of tensored pairs: $\Delta c = \sum_i c_i \otimes d_i$, for some $c_i, d_i \in C$. This quickly becomes very tedious and confusing; for example, using this notation the coassociativity diagram would give:

$$\begin{tikzcd}
c \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & \sum_i c_i \otimes d_i \arrow[d, "\Delta\otimes id"] \\
\sum_i c_i \otimes d_i \arrow[r, "id\otimes\Delta"] & \begin{array}{c} \sum_{i,j} a_{ij} \otimes b_{ij} \otimes d_i \\ \sum_{i,j} c_i \otimes e_{ij} \otimes f_{ij} \end{array}
\end{tikzcd}$$

That is $\sum_{i,j} a_{ij} \otimes b_{ij} \otimes d_i = \sum_{i,j} c_i \otimes e_{ij} \otimes f_{ij}$. To solve this problem, Heyneman and Sweedler introduced the following "sigma notation"for a coalgebra C and comultiplication Δ:

$$\Delta c = \sum c_{(1)} \otimes c_{(2)} = \sum c_1 \otimes c_2 \quad \forall c \in C.$$

Now the coassociativity diagram gives

$$\sum (c_1)_1 \otimes (c_1)_2 \otimes c_2 = \sum c_1 \otimes (c_2)_1 \otimes (c_2)_2.$$

This justifies the use of the following convention:

$$\sum c_1 \otimes c_2 \otimes c_3 := \sum (c_1)_1 \otimes (c_1)_2 \otimes c_2 = \sum c_1 \otimes (c_2)_1 \otimes (c_2)_2.$$

The subscripts are only symbolic "placeholders", they do not indicate a specific element of C. The original notation included the parentheses on subscripts, but they are often dropped to simplify the notation. We will omit the parentheses in this paper. Sigma notation is also used in physics where sometimes even the summation symbol may be ommitted. Others such as Kassel, use superscript numbers or prime marks in place of the subscripts, that is

$$\Delta c = \sum c' \otimes c''.$$

In sigma notation the counit diagram implies the following equation:

$$c = \sum \varepsilon(c_1) c_2 = \sum c_1 \varepsilon(c_2),$$

since

$$c \overset{\Delta}{\mapsto} \sum c_1 \otimes c_2 \overset{\varepsilon\otimes id}{\mapsto} \sum \varepsilon(c_1) \otimes c_2 = \sum 1 \otimes \varepsilon(c_1)c_2$$

and

$$c \overset{1\otimes}{\mapsto} 1 \otimes c.$$

Since $\{1\}$ is linearly independent we now have $c = \sum \varepsilon(c_1)c_2$. Similarly for the right portion of the diagram:

$$c \overset{\Delta}{\mapsto} \sum c_1 \otimes c_2 \overset{id\otimes\varepsilon}{\mapsto} \sum c_1 \otimes \varepsilon(c_2) = \sum c_1\varepsilon(c_2) \otimes 1$$

and

$$c \overset{\otimes 1}{\mapsto} c \otimes 1.$$

Thus $c = \sum c_1\varepsilon(c_2) = \sum \varepsilon(c_2)c_1$ since $\varepsilon(c_2) \in k$.

Analogously to algebra morphisms we define the concept of coalgebra morphisms.

Definition 4.2 Let C and D be coalgebras, with comultiplications Δ_C and Δ_D, and counits ε_C and ε_D, respectively. Then a map $f : C \to D$ is a **coalgebra morphism** if $\Delta_D \circ f = (f \otimes f)\Delta_C$ and if $\varepsilon_C = \varepsilon_D \circ f$. In map diagrams this means the following two diagrams commute.

1.

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes C \arrow[r, "f\otimes f"] & D \otimes D \end{tikzcd}$$

2.

$$\begin{tikzcd} C \arrow[rr, "f"] \arrow[drr, "\varepsilon_C"'] & & D \arrow[d, "\varepsilon_D"] \\ & & k \end{tikzcd}$$

Analogously to modules, we define the concept of comodules.

Definition 4.3 For a k-coalgebra C, a (right) C-**comodule** is a k-space M with a k-linear map $\rho : M \to M \otimes C$ such that the following diagrams commute:

1.

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

2.

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

In sigma notation we denote $\rho(m) = \sum m_0 \otimes m_1 \in M \otimes C$. Then the commutativity diagrams yield the following equations:

$$(id \otimes \Delta) \circ \rho(m) = (\rho \otimes id) \circ \rho(m) = \sum m_0 \otimes m_1 \otimes m_2.$$

So $\sum m_0 \otimes (m_1)_1 \otimes (m_1)_2 = \sum (m_0)_0 \otimes (m_0)_1 \otimes m_1 = \sum m_0 \otimes m_1 \otimes m_2$. And,

$$(id \otimes \varepsilon) \circ \rho(m) = \sum \varepsilon(m_1) m_0 \otimes 1 = m \otimes 1.$$

So $\sum \varepsilon(m_1) m_0 = m$. Originally this notation was introduced as $\sum_m m_{(0)} \otimes m_{(1)} \otimes m_{(2)}$ by Moss E. Sweedler in his 1968 paper *Cohomology of Algebras over Hopf Algebras.* The parentheses have been dropped for convience as in the sigma notation for coalgebras [S 69A], [S 68].

We are now ready to combine the algebra and coalgebra structures to get bialgebras.

Definition 4.4 A k-space B is a **bialgebra** if (B, μ, η) is an algebra, (B, Δ, ε) is a coalgebra, and either of the following (equivalent) conditions holds:

1. The maps Δ and ε are algebra morphisms. Comultiplication Δ is an algebra morphism if $\forall\, b, c \in B$ and $\alpha, \beta \in k$,

$$\Delta(bc) = (\Delta b)(\Delta c) = (\sum b_1 \otimes b_2)(\sum c_1 \otimes c_2) = \sum b_1 c_1 \otimes b_2 c_2$$

and

$$\Delta(\alpha\beta) = (\Delta\alpha)(\Delta\beta) = (\alpha \otimes 1)(\beta \otimes 1) = \alpha\beta \otimes 1.$$

The map ε is an algebra morphism if $\forall\, b, c \in B$ and $\alpha \in k$,

$$\varepsilon(bc) = \varepsilon(b)\varepsilon(c)$$

and

$$\varepsilon(\alpha) = \alpha.$$

2. The maps μ and η are coalgebra morphisms. Multiplication μ is a coalgebra morphism if $\forall\, b, c \in B$,

$$\Delta \circ \mu(b \otimes c) = (\mu \otimes \mu)\Delta(b \otimes c) = \sum b_1 c_1 \otimes b_2 c_2.$$

And η is a coalgebra morphism if $\forall\, \alpha \in k$,

$$\varepsilon(\alpha) = \varepsilon \circ \eta(\alpha).$$

We now have one last definition before we are able to define Hopf algebras. This definition defines a new multiplication on $\mathrm{Hom}_k(C, A)$.

Definition 4.5 Let C be a coalgebra and A an algebra. Define **convolution multiplication** on $\mathrm{Hom}_k(C, A)$ as

$$(f * g)(c) = \mu(f \otimes g)(\Delta c) = \sum f(c_1)g(c_2)$$

$\forall\, f, g \in \mathrm{Hom}_k(C, A)$ and, $c \in C$.

Then $\mathrm{Hom}_k(C, A)$ is a k-algebra under this multiplication and the usual addition of functions. The unit of $\mathrm{Hom}_k(C, A)$ is $\eta\varepsilon$. In sigma notation, convolution multiplication is given by $(f * g)(c) = \sum f(c_1)g(c_2)$ since

$$\begin{aligned}
(f * g)(c) &= \mu(f \otimes g)(\Delta c) \\
&= \mu(f \otimes g) \textstyle\sum c_1 \otimes c_2 \\
&= \mu \textstyle\sum f(c_1) \otimes g(c_2) \\
&= \textstyle\sum f(c_1)g(c_2).
\end{aligned}$$

The unit element in $\mathrm{Hom}_k(C, A)$ is $\eta\varepsilon$ since,

$$\begin{aligned}
(f * \eta\varepsilon)(c) &= \textstyle\sum f(c_1)\eta(\varepsilon(c_2)) && \text{by definition of } * \\
&= \textstyle\sum f(c_1)\varepsilon(c_2)\eta(1_k) && \varepsilon(c_2) \in k \\
&= \textstyle\sum f(c_1)\varepsilon(c_2)1_A && \text{definition: } \eta(1_k) = 1_A \\
&= \textstyle\sum f(c_1\varepsilon(c_2))1_A && \text{linearity of } f \\
&= f(\textstyle\sum c_1\varepsilon(c_2))1_A && \text{linearity of } f \\
&= f(c)1_A && c = \textstyle\sum c_1\varepsilon(c_2) \\
&= f(c) && f(c) \in A
\end{aligned}$$

and

$$\begin{aligned}
(\eta\varepsilon * f)(c) &= \textstyle\sum \eta(\varepsilon(c_1))f(c_2) && \text{definition of } * \\
&= \textstyle\sum \eta(1_k)\varepsilon(c_1)f(c_2) && \varepsilon(c_2) \in k \\
&= \textstyle\sum 1_A\varepsilon(c_1)f(c_2) && \eta(1_k) = 1_A \\
&= \textstyle\sum 1_A f(\varepsilon(c_1)c_2) && \text{linearity of } f \\
&= 1_A f(\textstyle\sum \varepsilon(c_1)c_2) && \text{linearity of } f \\
&= 1_A f(c) && c = \textstyle\sum \varepsilon(c_1)c_2 \\
&= f(c) && f(c) \in A.
\end{aligned}$$

Thus $(f * \eta\varepsilon)(c) = f(c) = (\eta\varepsilon * f)(c)$.

A Hopf algebra is a special type of bialgebra:

Definition 4.6 Let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra. Then H is a **Hopf algebra** if there exists an element $S \in \mathrm{Hom}_k(H, H)$ which is inverse to id_H under convolution multiplication. S is called an **antipode** for H. In sigma notation, this means

$$(S * id_H)(h) = \sum (Sh_1)h_2 = \varepsilon(h)1_H = \sum h_1(Sh_2) = (id * S)(h)$$

$\forall\, h \in H$, since $(\eta\varepsilon)(h) = \varepsilon(h)\eta(1_k) = \varepsilon(h)1_H$.

Note that the antipode of a given Hopf algebra is unique because it is defined as an inverse function.

The following proposition gives an important property of the antipode S: it shows that S is an antihomomorphism.

Proposition 4.7 [S 69B] Let H be a Hopf algebra with antipode S. Then S is an antihomomorphism; that is $S(gh) = S(h)S(g) \quad \forall\, g, h \in H$.

Proof: Let H be a Hopf algebra and define the maps $\nu, \varrho \in \mathrm{Hom}(H \otimes H, H)$ via $\nu(g \otimes h) = S(h)S(g)$ and $\varrho(g \otimes h) = S(gh)$ where S is the antipode of H and $g, h \in H$. We will show that $\nu = \varrho$.

$$\begin{array}{rcll}
(\varrho * \mu)(g \otimes h) & = & \sum \varrho((g \otimes h)_1)\mu((g \otimes h)_2) & \text{definition of } * \\
& = & \sum \varrho(g_1 \otimes h_1)\mu(g_2 \otimes h_2) & \text{definition of } \Delta \\
& = & \sum S(g_1 h_1) g_2 h_2 & \text{definition of } \varrho \text{ and } \mu \\
& = & \sum S((gh)_1)(gh)_2 & \Delta \text{ is multiplicative} \\
& = & \varepsilon(gh) \cdot 1_H & \text{definition of antipode} \\
& = & (\eta\varepsilon)(gh) &
\end{array}$$

$$
\begin{aligned}
(\mu * \nu)(g \otimes h) &= \sum \mu((g \otimes h)_1)\nu((g \otimes h)_2) && \text{definition of } * \\
&= \sum \mu(g_1 \otimes h_1)\nu(g_2 \otimes h_2) && \text{definition of } \Delta_{H\otimes H} \\
&= \sum g_1 h_1 S(h_2) S(g_2) && \text{definition of } \mu \text{ and } \nu \\
&= \textstyle\sum_g g_1 (\sum_h h_1 S(h_2)) S(g_2) && \text{associativity} \\
&= \textstyle\sum_g g_1 \varepsilon(h) S(g_2) && \text{definition of } S \\
&= \sum g_1 S(g_2) \varepsilon(h) && \text{linearity of } \varepsilon \\
&= \varepsilon(g)\varepsilon(h) 1_H && \text{definition of } S \\
&= \varepsilon(gh) 1_H && \varepsilon \text{ is multiplicative} \\
&= (\eta\varepsilon)(gh)
\end{aligned}
$$

So $\varrho * \mu = \mu * \nu = \eta\varepsilon$ which implies

$$
\begin{aligned}
\varrho * \mu * \nu &= \mu * \nu * \nu \\
\varrho * \eta\varepsilon &= \eta\varepsilon * \nu \\
\varrho &= \nu
\end{aligned}
$$

since $\eta\varepsilon$ is the unit in $\mathrm{Hom}(H \otimes H, H)$. Thus $S(gh) = S(h)S(g) \quad \forall\, h, g \in H$. □

Now let us look at some examples of coalgebras, bialgebras, and Hopf algebras.

Example 4.8 The group algebra kG.

Recall from Example 1.9 that kG is an algebra via the maps μ and η, where

$$\mu(\sum_{g\in G} \alpha_g g \otimes \sum_{h\in G} \beta_h h) = \sum_{h,g} \alpha_g \beta_h gh$$

and

$$\eta(1_k) = 1_G.$$

Now to see that kG is a coalgebra, we need to define Δ and ε. Let

$$\Delta(g) = g \otimes g \quad \text{and} \quad \varepsilon(g) = 1 \quad \forall g \in G$$

and extend these maps linearly, thus for an element $\sum_{g\in G} \alpha_g g \in kG$

$$\Delta\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g g \otimes g$$

and

$$\varepsilon\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g \varepsilon(g) = \sum_{g\in G} \alpha_g$$

To verify that these maps give a coalgebra, we need to check the coassociativity and counit maps and see that the diagrams commute.

Coassociativity:

$$\begin{tikzcd}
g \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & g \otimes g \arrow[d, "\Delta \otimes id"] \\
g \otimes g \arrow[r, "id \otimes \Delta"] & g \otimes (g \otimes g) = (g \otimes g) \otimes g
\end{tikzcd}$$

Counit:

$$\begin{tikzcd}
 & g \arrow[dl, "1\otimes"'] \arrow[dr, "\otimes 1"] \arrow[dd, "\Delta"] & \\
1 \otimes g = \varepsilon(g) \otimes g & & g \otimes 1 = g \otimes \varepsilon(g) \\
 & g \otimes g \arrow[ul, "\varepsilon \otimes id"] \arrow[ur, "id \otimes \varepsilon"'] &
\end{tikzcd}$$

These maps do commute since $\varepsilon(g) = 1 \quad \forall\, g \in G$. For a general element in kG commutativity still holds by linearity. Thus kG is a coalgebra.

Now, since kG is an algebra and a coalgebra, all that needs to be shown is that Δ and ε are algebra morphisms, in order to verify that kG is a bialgebra.

1. $\Delta\left((\sum_{g\in G}\alpha_g g)(\sum_{h\in H}\beta_h h)\right)$

$$\begin{aligned}
&= \Delta(\sum_{g,h}\alpha_g\beta_h gh) && \text{definition of multiplication}\\
&= \sum_{g,h}\alpha_g\beta_h\Delta(gh) && \text{linearity of } \Delta\\
&= \sum_{g,h}\alpha_g\beta_h(gh\otimes gh) && \text{since } g,h\in G\\
&= \sum_{g,h}\alpha_g\beta_h(g\otimes g)(h\otimes h) && \text{def of tensor product multiplication}\\
&= \sum_{g\in G}\alpha_g(g\otimes g)\sum_{h\in H}\beta_h(h\otimes h) && \text{def of multiplication in } kG\\
&= \Delta(\sum_{g\in G}\alpha_g g)\Delta(\sum_{h\in H}\beta_h h) && \text{definition of } \Delta.
\end{aligned}$$

2. $\Delta(1_{kG}) = 1_{kG}\otimes 1_{kG}$ for $1\in G$ since $1_{kG}=1_G$.

3. $\varepsilon\left((\sum_{g\in G}\alpha_g g)(\sum_{h\in G}\beta_h h)\right)$

$$\begin{aligned}
&= \varepsilon(\sum_{g,h}\alpha_g\beta_h gh) && \text{definition of multiplication}\\
&= \sum_{g,h}\alpha_g\beta_h\varepsilon(gh) && \text{linearity of } \varepsilon\\
&= \sum_{g,h}\alpha_g\beta_h\cdot 1_k && gh\in G, \text{ definition of } \varepsilon\\
&= \sum_{g,h}\alpha_g\beta_h && \alpha_g\beta_h\in k\\
&= (\sum_{g\in G}\alpha_g\cdot 1_k)(\sum_{h\in G}\beta_h\cdot 1_k) && \text{definition of multiplication and unit}\\
&= \varepsilon(\sum_{g\in G}\alpha_g g)\varepsilon(\sum_{h\in G}\beta_h h) && \text{definition of } \varepsilon.
\end{aligned}$$

4. $\varepsilon(1_{kG}) = 1_k$ since $1_{kG} = 1_G\in G$.

Since the necessary conditions for Δ and ε to be algebra morphisms are met, kG is a bialgebra.

To verify that kG is a Hopf algebra, we must show that kG has an antipode. Define $S(g) := g^{-1} \quad \forall\, g\in G$ and extend linearly, that is

$$S(\sum_{g\in G}\alpha_g g) = \sum_{g\in G}\alpha_g S(g) = \sum_{g\in G}\alpha_g g^{-1}.$$

S is the antipode for kG since

$$\varepsilon(g)1_G = 1_k \cdot 1_G = 1_G,$$

and

$$(S * id)(g) = (S \otimes id)\Delta g = S(g)g = g^{-1}g = 1_G,$$

and

$$(id * S)(g) = (id \otimes S)\Delta g = gS(g) = gg^{-1} = 1_G.$$

Thus $1_G = \varepsilon(g) \cdot 1_G = S(g)g = gS(g)$. So the group algebra kG is a Hopf algebra.

Coalgebras can have a property analogous to commutativity in algebras; this is called **cocommutativity**, and means that for any c in the coalgebra, $\sum c_1 \otimes c_2 = \sum c_2 \otimes c_1$. When $H = kG$, we see that comultiplication is indeed cocommutative since

$$\Delta(\sum_{g \in G} \alpha_g g) = \sum_{g \in G} \alpha_g g \otimes g = \sum_{g \in G} g \otimes \alpha_g g.$$

Given a vector space V, define its linear dual to be $V^* := \mathrm{Hom}_k(V, k)$. For the case of $H = kG$ with G a finite group, the linear dual $H^* = (kG)^*$ gives us our next example of a Hopf algebra.

Example 4.9 The linear dual of the group algebra $(kG)^*$ for a finite group G.

The linear dual of the group algebra is defined to be the set $(kG)^*$ =Hom(kG, k). This space has a basis of linear projections onto the field. This is the "dual basis" to $\{g\}_{g \in G}$. Define $p_g : kG \to k$ via

$$p_g(h) = \begin{cases} 1 & \text{if } g = h \\ 0 & \text{otherwise} \end{cases}$$

and extend linearly. Then $\{p_g\}_{g \in G}$ is a basis of $(kG)^*$. The linear dual of the group algebra, $(kG)^*$, is a k-vector space under formal addition, and is an algebra with multiplication given by

$$p_g p_h = \begin{cases} p_h & \text{if } g = h \\ 0 & \text{otherwise} \end{cases}$$

and extended linearly. Note that $(kG)^*$ is a commutative algebra, dual to the fact that kG is cocommutative.

The linear dual of the group algebra, $(kG)^*$, is a coalgebra through the maps Δ and ε,

$$\Delta(p_g) := \sum_{h \in G} p_{gh^{-1}} \otimes p_h$$

and

$$\varepsilon(p_g) := \left\{ \begin{array}{ll} 1 & \text{if } g = 1 \\ 0 & \text{otherwise} \end{array} \right\} = \delta_{g,1}.$$

Notice that $\sum_{g \in G} p_g = 1_{(kG)^*}$. This follows from:

$$\left(\sum_{g \in G} p_g\right) p_h = \sum_{g \in G} p_g p_h = p_h \quad \text{since} \quad p_g p_h = \begin{cases} 1 & g = h \\ 0 & g \neq h. \end{cases}$$

Similarly, $p_h\left(\sum_{g \in G} p_g\right) = p_h$.

To see that $(kG)^*$ is a coalgebra, we will show that the coassociativity and counit diagrams commute.

Coassociativity:

$$\begin{aligned}
(\Delta \otimes id)\Delta p_g &= (\Delta \otimes id) \sum_{xy=g} p_x \otimes p_y && \text{definition of } \Delta p_g \\
&= \sum_{xy=g} (\Delta p_x) \otimes p_y \\
&= \sum_{xy=g, uv=x} p_u \otimes p_v \otimes p_y && \text{definition of } \Delta p_g \\
&= \sum_{uvy=g} p_u \otimes p_v \otimes p_y && \text{substitution}
\end{aligned}$$

and

$$\begin{aligned}
(id \otimes \Delta)\Delta p_g &= (id \otimes \Delta) \sum_{xy=g} p_x \otimes p_y && \text{definition of } \Delta p_g \\
&= \sum_{xy=g} p_x \otimes (\Delta p_y) \\
&= \sum_{xy=g, uv=y} p_x \otimes p_u \otimes p_v && \text{definition of } \Delta p_g \\
&= \sum_{xuv=g} p_x \otimes p_u \otimes p_v && \text{substitution.}
\end{aligned}$$

But $\sum_{uvy=g} p_u \otimes p_v \otimes p_y = \sum_{xuv=g} p_x \otimes p_u \otimes p_v$ so we are done.
Counit:

$$\begin{aligned}
(\varepsilon \otimes id) \circ \Delta p_g &= (\varepsilon \otimes id) \sum_{xy=g} p_x \otimes p_y && \text{definition of } \Delta p_g \\
&= \sum_{xy=g} \varepsilon(p_x) \otimes p_y \\
&= 1 \otimes p_g && \varepsilon(p_x) = \delta_{x,1}.
\end{aligned}$$

Also,

$$\begin{aligned}
(id \otimes \varepsilon)\Delta p_g &= (id \otimes \varepsilon) \sum_{xy=g} p_x \otimes p_y && \text{definition of } \Delta p_g \\
&= \sum_{xy=g} p_x \otimes \varepsilon(p_y) \\
&= p_g \otimes 1.
\end{aligned}$$

We now verify that Δ and ε are algebra morphisms to see that $(kG)^*$ is a bialgebra.

1.

$$\Delta(p_g p_h) = \begin{cases} \Delta(p_g) & \text{if } g = h \\ 0 & \text{otherwise} \end{cases}$$

and

$$\begin{aligned}
(\Delta p_g)(\Delta p_h) &= \left(\sum_{l \in G} p_{gl^{-1}} \otimes p_l\right)\left(\sum_{m \in G} p_{hm^{-1}} \otimes p_m\right) \\
&= \sum_{l,m \in G} p_{gl^{-1}} p_{hm^{-1}} \otimes p_l p_m \\
&= \begin{cases} \sum_{l \in G} p_{gl^{-1}} p_{hl^{-1}} \otimes p_l & \text{if } l = m \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} \sum_{l \in G} p_{gl^{-1}} \otimes p_l & \text{if } g = h \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} \Delta p_g & \text{if } g = h \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

So $\Delta(p_g p_h) = (\Delta p_g)(\Delta p_h)$.

2.

$$\begin{aligned}
\Delta(1) &= \Delta(\sum_{g\in G} p_g) \\
&= \sum_{g\in G} \Delta p_g \\
&= \sum_{g\in G}(\sum_{l\in G} p_{gl^{-1}} \otimes p_l) \\
&= \sum_{g,l} p_{gl^{-1}} \otimes p_l \\
&= \sum_{l\in G}\left(\sum_{g\in G} p_{gl^{-1}}\right) \otimes p_l \\
&= 1 \otimes \sum_{l\in G} p_l \qquad\qquad \text{because } \sum_{g\in G} p_g = 1 \\
&= 1 \otimes 1.
\end{aligned}$$

3.

$$\begin{aligned}
\varepsilon(p_g p_h) &= \begin{cases} \varepsilon(p_g) & \text{if } g = h \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} 1 & \text{if } g = h = 1 \\ 0 & \text{otherwise} \end{cases} \\
&= \varepsilon(p_g)\varepsilon(p_h).
\end{aligned}$$

4.

$$\begin{aligned}
\varepsilon(1) &= \varepsilon(\sum_{g\in G} p_g) \\
&= \sum_{g\in G}(\varepsilon(p_g)) \\
&= \sum_{g\in G} \delta_{g,1} \\
&= 1.
\end{aligned}$$

Thus the linear dual of the group algebra $(kG)^*$ is a bialgebra, as we have shown that it is a coalgebra, algebra, and Δ and ε are algebra morphisms.

To show that $(kG)^*$ is a Hopf algebra we need an antipode. Define

$S(p_g) := p_{g^{-1}}$. To verify that this is an antipode we will compute:

$$\begin{aligned}
(S * id)(p_g) &= \mu(S \otimes id)(\Delta p_g) \\
&= \mu(S \otimes id)(\sum_{l \in G} p_{gl^{-1}} \otimes p_l) \\
&= \mu(\sum_{l \in G} S(p_{gl^{-1}}) \otimes p_l) \\
&= \sum_{l \in G} p_{lg^{-1}} p_l \\
&= \begin{cases} \sum_{l \in G} p_l & \text{if } lg^{-1} = l, \text{ that is } g = 1 \\ 0 & \text{if } lg^{-1} \neq l, \text{ that is } g \neq 1 \end{cases} \\
&= \begin{cases} 1 & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} \\
&= \varepsilon(p_g),
\end{aligned}$$

and

$$\begin{aligned}
(id * S)(p_g) &= \mu(id \otimes S)(\Delta p_g) \\
&= \mu(id \otimes S)(\sum_{l \in G} p_{gl^{-1}} \otimes p_l) \\
&= \mu \sum_{l \in G} p_{gl^{-1}} \otimes S(p_l) \\
&= \sum_{l \in G} p_{gl^{-1}} p_{l^{-1}} \\
&= \begin{cases} \sum_{l \in G} p_{l^{-1}} & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} \\
&= \begin{cases} 1 & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} \\
&= \varepsilon(p_g).
\end{aligned}$$

Thus $(kG)^*$ is a Hopf algebra.

This next example is based on the Lie algebras that are due to the Norwegian mathematician Sophus Lie. Lie was born in December 1842 and is the founder of the theory of Lie Groups. Originally Lie called these 'finite continuous groups'. Lie did much of his work during the 1870's and 1880's, well before the concept of Hopf algebras was defined.

Example 4.10 The Universal Enveloping Algebra $U(L)$ of the Lie algebra L.

Before we see what the Universal Enveloping Algebra of the Lie algebra is we need to define some preliminary concepts. These concepts are in fact extremely important in their own right.

Let L be a vector space. Define $T^0(L) = k, T^1(L) = L$ and $T^n(L) = L^{\otimes n}$ (the tensor product of n copies of L) if $n > 1$. Then the **tensor algebra** $T(L)$ is defined to be:

$$T(L) := \oplus_{n\geq 0} T^n(L) = k \oplus L \oplus L \otimes L \oplus \cdots.$$

This is indeed an algebra, where multiplication is defined to be juxtaposition and the unit is $1_{T(L)} = 1_k$.

A **Lie algebra L** is a vector space with a bilinear map $[\ ,\ ] : L \otimes L \to L$ that satisfies the following two conditions $\forall\, x, y, z \in L$.

1. antisymmetry: $[x, y] = -[y, x]$
2. Jacobi identity: $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$

An important example of a Lie algebra is given when A is an associative algebra. We define a Lie bracket on A via

$$[a, b] = ab - ba.$$

The structure thus defined satisfies the two identities and is denoted $L = A^-$.

To define the **Universal Enveloping Algebra of** L, denoted $U(L)$, we need a tensor algebra $T(L)$ and an ideal $I(L)$ generated by elements of the form $[a, b] - (ab - ba)$ for $a, b \in L$. Then

$$U(L) := T(L)/I(L)$$

[Ks 95].

We are now ready to define the coalgebra structure maps for $U(L)$:
$\Delta : U(L) \to U(L) \otimes U(L)$ via

$$\Delta(1) := 1 \otimes 1$$

$$\Delta(l) := l \otimes 1 + 1 \otimes l \quad \forall\, l \in L$$

and $\varepsilon : U(L) \to k$ via

$$\varepsilon(1) := 1_k$$

$$\varepsilon(l) := 0 \quad \forall\, l \in L.$$

Extend Δ and ε linearly and multiplicatively to $U(L)$.

To verify the coassociativity map, we must show $(\Delta \otimes id)\Delta = (id \otimes \Delta)\Delta$. Let $l \in L$, then

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

and

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

Thus $(\Delta \otimes id)\Delta(l) = (id \otimes \Delta)\Delta(l)$.

To verify the counit map, we must show $l = \mu(\varepsilon \otimes id)\Delta(l) = \mu(id \otimes \varepsilon)\Delta(l)$. Let $l \in L$, then:

$$\begin{aligned}
\mu(\varepsilon \otimes id)\Delta(l) &= \mu(\varepsilon \otimes id)(l \otimes 1 + 1 \otimes l) \\
&= \mu(\varepsilon(l) \otimes 1 + \varepsilon(1) \otimes l) \\
&= \mu(0 \otimes 1 + 1 \otimes l) \\
&= 0 \cdot 1 + 1 \cdot l \\
&= l,
\end{aligned}$$

and

$$\begin{aligned}
\mu(id \otimes \varepsilon)\Delta(l) &= \mu(id \otimes \varepsilon)(l \otimes 1 + 1 \otimes l) \\
&= \mu(l \otimes \varepsilon(1) + 1 \otimes \varepsilon(l)) \\
&= \mu(l \otimes 1 + 1 \otimes 0) \\
&= l \cdot 1 + 1 \cdot 0 \\
&= l.
\end{aligned}$$

Thus $U(L)$ is a coalgebra.

The Universal Enveloping Algebra $U(L)$ of the Lie algebra L is now a bialgebra, as its algebra structure is inherited from the tensor algebra $T(L)$, and Δ

and ε are defined to be linear and multiplicative, so they are automatically algebra morphisms.

For $U(L)$ to be a Hopf algebra, an antipode is needed. Define $S(l) := -l \quad \forall\, l \in L$ and $S(1) = 1$. Extend S linearly and antimultiplicatively on L, that is $S(xy) = S(y)S(x) \quad \forall\, x, y \in L$. This extends to antimultiplicativity on $U(L)$ by the nature of multiplication on $U(L)$. To verify that this S is the antipode we must show that $\varepsilon(l) = \mu(S \otimes id)(\Delta l) = \mu(id \otimes S)(\Delta l)$. Indeed

$$\varepsilon(l) = 0 \quad \forall\, l \in L,$$

and

$$\begin{aligned}\mu(S \otimes id)(\Delta l) &= \mu(S \otimes id)(l \otimes 1 + 1 \otimes l)\\ &= \mu(S(l) \otimes 1 + S(1) \otimes l)\\ &= S(l) \cdot 1 + S(1) \cdot l\\ &= S(l) + 1 \cdot l\\ &= -l + l\\ &= 0,\end{aligned}$$

and

$$\begin{aligned}\mu(id \otimes S)(\Delta l) &= \mu(id \otimes S)(l \otimes 1 + 1 \otimes l)\\ &= \mu(l \otimes S(1) + 1 \otimes S(l))\\ &= l \cdot 1 + 1 \cdot (-l)\\ &= l + (-l)\\ &= 0.\end{aligned}$$

So, $\varepsilon(l) = \mu(S \otimes id)(\Delta l) = \mu(id \otimes S)(\Delta l)$. Moreover,

$$\varepsilon(1) = 1,$$

and

$$\begin{aligned}\mu(S \otimes id)(\Delta 1) &= \mu(S \otimes id)(1 \otimes 1)\\ &= \mu(S(1) \otimes 1)\\ &= S(1) \cdot 1\\ &= 1 \cdot 1\\ &= 1,\end{aligned}$$

and

$$\begin{aligned}\mu(id \otimes S)(\Delta 1) &= \mu(id \otimes S)(1 \otimes 1)\\ &= \mu(1 \otimes S(1))\\ &= 1 \cdot 1\\ &= 1.\end{aligned}$$

So, $\varepsilon(1) = \mu(S \otimes id)(\Delta 1) = \mu(id \otimes S)(\Delta 1)$. Thus S is the antipode for $U(L)$ and $U(L)$ is a Hopf algebra.

Not every set that is a coalgebra and an algebra is necessarily a bialgebra or Hopf algebra. This next example is one such case.

Example 4.11 The set of $n \times n$ matrices with elements from the field k, $M_n(k)$, is an algebra and a coalgebra, but not a bialgebra.

Consider $M_n(k)$ an algebra as usual, and let E_{ij} denote the matrix with 1 in the ij^{th} place and zero everywhere else. $M_n(k)$ becomes a coalgebra when we define the maps Δ and ε as follows:

$$\Delta(E_{ij}) := \sum_{k=1}^{n} E_{ik} \otimes E_{kj}$$

and

$$\varepsilon(E_{ij}) := \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

and extend linearly to $M_n(k)$.

To verify that these two maps make $M_n(k)$ a coalgebra, we need to check that the coassociativity and counit diagrams commute.

Coassociativity:

$$E_{ij} \overset{\Delta}{\mapsto} \sum_{l} E_{il} \otimes E_{lj} \overset{id \otimes \Delta}{\mapsto} \sum_{l,k} E_{il} \otimes E_{lk} \otimes E_{kj},$$

and

$$E_{ij} \overset{\Delta}{\mapsto} \sum_{k} E_{ik} \otimes E_{kj} \overset{\Delta \otimes id}{\mapsto} \sum_{k,l} E_{il} \otimes E_{lk} \otimes E_{kj}.$$

This diagram commutes since $\sum_{k,l} E_{il} \otimes E_{lk} \otimes E_{kj} = \sum_{l,k} E_{il} \otimes E_{lk} \otimes E_{kj}$.

Counit:

$$E_{ij} \overset{\Delta}{\mapsto} \sum_{k} E_{ik} \otimes E_{kj} \overset{\varepsilon \otimes id}{\mapsto} \sum_{k} \delta_{ik} \otimes E_{kj},$$

and

$$E_{ij} \overset{1\otimes}{\mapsto} 1 \otimes E_{ij}.$$

Also,

$$E_{ij} \overset{\Delta}{\mapsto} \sum_k E_{ik} \otimes E_{kj} \overset{id\otimes\varepsilon}{\mapsto} \sum_k E_{ik} \otimes \delta_{kj},$$

and

$$E_{ij} \overset{\otimes 1}{\mapsto} E_{ij} \otimes 1.$$

These maps commute since $\sum_k \delta_{ik} \otimes E_{kj} = \delta_{ii} \otimes E_{ij} = 1 \otimes E_{ij}$ and $\sum_k E_{ik} \otimes \delta_{kj} = E_{ij} \otimes \delta_{jj} = E_{ij} \otimes 1$. Thus $M_n(k)$ is a coalgebra.

However, $M_n(k)$ is not a bialgebra. To see this we must show that Δ and/or ε are not algebra morphisms. In fact, neither is an algebra map; we show counter examples for both:

1.

$$\varepsilon(E_{12}E_{21}) = \varepsilon(E_{11}) = 1,$$

but

$$\varepsilon(E_{12})\varepsilon(E_{21}) = 0 \cdot 0 = 0.$$

$1 \neq 0$, thus $\varepsilon(E_{12}E_{21}) \neq \varepsilon(E_{12})\varepsilon(E_{21})$.

2.

$$\Delta(E_{11}E_{22}) = \Delta(0) = 0,$$

but

$$\Delta(E_{11})\Delta(E_{22}) = (\sum_{k=1}^{n} E_{1k} \otimes E_{k1})(\sum_{l=1}^{n} E_{2l} \otimes E_{l2})$$

$$\begin{aligned}
&= (E_{11} \otimes E_{11} + E_{12} \otimes E_{21} + \cdots + E_{1n} \otimes E_{n1})(E_{21} \otimes E_{12} + \cdots + E_{2n} \otimes E_{n2}) \\
&= E_{11}E_{21} \otimes E_{11}E_{12} + \cdots + E_{12}E_{21} \otimes E_{21}E_{12} + \cdots + E_{1n}E_{2n} \otimes E_{n1}E_{n2} \\
&= 0 \otimes 0 + 0 \otimes 0 + \cdots + E_{11} \otimes E_{22} + \cdots + 0 \otimes 0 \\
&= E_{11} \otimes E_{22}.
\end{aligned}$$

$0 \neq E_{11} \otimes E_{22}$, so $\Delta(E_{11}E_{22}) \neq \Delta(E_{11})\Delta(E_{22})$. Each of these examples is a sufficient test to show that Δ and ε are not algebra morphisms. Thus $M_n(k)$ is not a bialgebra.

As the Hopf algebra combines the algebra and coalgebra structure, so the Hopf module combines the module and comodule structures. Notice we are defining a right H-Hopf module which uses the right H-module structure along with the right H-comodule structure.

Definition 4.12 For a k-Hopf algebra H, a **right H-Hopf module** is a k-space M such that:

1. M is a right H-module, via $\gamma : M \otimes H \to M$.
2. M is a right H-comodule, via $\rho : M \to M \otimes H$.
3. ρ is a right H-module map, that is

$$\sum (m \cdot h)_0 \otimes (m \cdot h)_1 = \sum m_0 \cdot h_1 \otimes m_1 h_2 \quad \forall\, m \in M, h \in H.$$

This is known as the coherence condition.

An important result on Hopf modules is the Fundamental Theorem of Hopf Modules. To understand and prove this theorem we need the following two definitions.

Definition 4.13 Let M be a left H-module. The **invariants** of H on M are the set

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

Definition 4.14 Let M be a right H-comodule. The **coinvariants** of H in M are the set

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

Theorem 4.15 (Fundamental Theorem of Hopf Modules) Let M be a right H-Hopf module. Then $M \cong M^{coH} \otimes H$ as right H-Hopf modules.

Proof: Define $P : M \to M$ to be the composite map

$$M \xrightarrow{\rho} M \otimes H \xrightarrow{id \otimes S} M \otimes H \xrightarrow{\gamma} M,$$

that is $P(m) := \sum_m m_0 \cdot Sm_1$ for $m \in M$. Next define

$$\alpha : M^{coH} \otimes H \to M \quad \text{via} \quad m' \otimes h \mapsto m' \cdot h$$

and

$$\beta : M \to M \otimes H \quad \text{via} \quad m \mapsto \sum_m m_0 \cdot (Sm_1) \otimes m_2,$$

that is $\beta = (P \otimes id)\rho$.

We will first show that $\beta(M) \subseteq M^{coH} \otimes H$.

$$\begin{aligned}
\rho(\sum_m m_0 \cdot Sm_1) &= \sum_m (m_0 \cdot Sm_1)_0 \otimes (m_0 \cdot Sm_1)_1 && \text{def of } \rho \\
&= \sum_m (m_0)_0 \cdot (Sm_1)_1 \otimes (m_0)_1 (Sm_1)_2 && \text{coherence condition} \\
&= \sum_m (m_0)_0 \cdot Sm_2 \otimes (m_0)_1 Sm_1 && S \text{ is antihomomorphism} \\
&= \sum_m m_0 \cdot Sm_3 \otimes m_1 Sm_2 && \text{“coassociativity” of coaction} \\
&= \sum_m m_0 \cdot Sm_2 \otimes \varepsilon(m_1) && \text{def of antipode} \\
&= \sum_m m_0 \cdot Sm_1 \otimes 1_H && \text{def of counit}
\end{aligned}$$

This means that $\sum_m m_0 \cdot Sm_1 \in M^{coH}$.

Next we will show that α and β are inverse maps. That is for $m \in M$:

$$\begin{aligned}
\alpha\beta(m) &= \alpha(\sum_m m_0 \cdot (Sm_1) \otimes m_2) && \text{def of } \beta \\
&= \sum_m (m_0 \cdot (Sm_1)) \cdot m_2 && \text{def of } \alpha \\
&= \sum_m m_0 \cdot ((Sm_1)m_2) && \text{“associativity” of action} \\
&= \sum_m m_0 \cdot \varepsilon(m_1) && \text{def of antipode} \\
&= m && \text{counit, def of comodule}
\end{aligned}$$

Also for $m' \in M^{coH}$:

$$\begin{aligned}
\beta\alpha(m' \otimes h) &= \beta(m' \cdot h) && \text{def of } \alpha \\
&= (P \otimes id)\rho(m' \cdot h) && \text{def of } \beta \\
&= (P \otimes id)(\sum_h m' \cdot h_1 \otimes 1_H h_2) && H \text{ Hopf module, } m' \in M^{coH} \\
&= (P \otimes id)(\sum_h m' \cdot h_1 \otimes h_2) && \\
&= \sum_h (m' \cdot h_1)_0 \cdot S(m' \cdot h_1)_1 \otimes h_2 && \text{def of } P \\
&= \sum_h m'_0 \cdot h_1 \cdot S(m'_1 \cdot h_2) \otimes h_3 && \text{coherence condition} \\
&= \sum_h m' \cdot h_1 \cdot S(1_H \cdot h_2) \otimes h_3 && m' \in M^{coH} \\
&= \sum_h m' \cdot (h_1(Sh_2)) \otimes h_3 && \text{associativity} \\
&= \sum_h m'\varepsilon(h_1) \otimes h_2 && \text{def of antipode} \\
&= \sum_h m' \otimes \varepsilon(h_1)h_2 && \text{linearity} \\
&= m' \otimes h && \text{def of counit.}
\end{aligned}$$

Thus α and β are both one-to-one and onto.

Lastly we will show that α and β are H-module maps. For this to be true, α and β must each be right H-module maps and right H-comodule maps. To verify that α is a right H-module map consider the following $\forall\, m' \in M^{coH}$ and $g, h \in H$:

$$m' \otimes h \otimes g \overset{\alpha\otimes id}{\mapsto} (m' \cdot h) \otimes g \overset{\gamma}{\mapsto} (m' \cdot h) \cdot g,$$

and

$$m' \otimes h \otimes g \overset{\gamma\otimes id}{\mapsto} (m' \cdot h) \otimes g \overset{\alpha}{\mapsto} (m' \cdot h) \cdot g$$

which are equal. To show that α is a right H-comodule map consider $\forall\, m' \in M^{coH}$ and $h \in H$:

$$m' \otimes h \overset{\alpha}{\mapsto} m' \cdot h \overset{\rho}{\mapsto} \sum_h m' \cdot h_1 \otimes 1_H \cdot h_2 = \sum_h m' \cdot h_1 \otimes h_2,$$

and

$$m' \otimes h \overset{id \otimes \Delta}{\mapsto} m' \otimes \sum_h h_1 \otimes h_2 \overset{\alpha \otimes id}{\mapsto} \sum_h m' \cdot h_1 \otimes h_2$$

which are also equal.

The linear inverse β is also a right H-module map and a right H-comodule map. Thus α is an isomorphism of H-Hopf modules, which means $M \cong M^{coH} \otimes H$.

□

Note that a similar proof works for any left H-Hopf module.

5 Integrals

Before we see how Maschke's Theorem generalizes to Hopf algebras we need to define integrals in a Hopf algebra H.

Definition 5.1 A **left integral** in H is an element $t \in H$ such that $ht = \varepsilon(h)t, \quad \forall\, h \in H$; a **right integral** in h is an element $t' \in H$ such that $t'h = \varepsilon(h)t', \quad \forall\, h \in H$. We denote the space of left integrals by $\int_H^l$ and the space of right integrals by $\int_H^r$. The Hopf algebra H is called **unimodular** if $\int_H^l = \int_H^r$. In such a case we write $\int_H = \int_H^l = \int_H^r$.

Our basic examples of Hopf algebras also contain integrals when they are finite dimensional.

Example 5.2 Consider the group algebra $H = kG$ for a finite group G (see Example 4.8). Then the element $t = \sum\limits_{g \in G} g$ is both a left and a right integral in H although G is not necessarily Abelian.

To verify that t is a left integral, let $h \in kG$; then

$$ht = h(\sum_{g \in G} g) = \sum_{g \in G} hg = \sum_{g \in G} g = t,$$

and

$$\varepsilon(h)t = 1_k \cdot \sum_{g \in G} g = \sum_{g \in G} g = t.$$

Hence $ht = \varepsilon(h)t \quad \forall\, h \in H$, and so $t \in \int_H^l$.

For the right integral property, let $h \in kG$ and $t' = \sum\limits_{g \in G} g$. Then

$$t'h = (\sum_{g \in G} g)h = \sum_{g \in G} gh = \sum_{g \in G} g = t',$$

and

$$\varepsilon(h)t' = 1_k \cdot \sum_{g \in G} g = \sum_{g \in G} g = t'.$$

Hence $t'h = \varepsilon(h)t' \quad \forall\, h \in H$, and so $t' \in \int_H^r$.

Thus $t = \sum_{g \in G} g$ is a left and a right integral in H and so H is unimodular.

Example 5.3 For a finite group G, let $H = (kG)^*$, the linear dual of the group algebra (see Example 4.9). Then $t = p_1$ is a left and a right integral.

To verify that t is a left integral, let $p_g \in (kG)^*$ and $t = p_1$. Then

$$p_g t = p_g p_1 = \begin{cases} p_1 & \text{if } g = 1 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\varepsilon(p_g)t = \varepsilon(p_g)p_1 = \begin{cases} p_1 & \text{if } g = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Thus $p_g t = \varepsilon(p_g)t$. In $(kG)^*$, $\{p_g\}_{g \in G}$ is a basis. So for a general element $h = \sum_{g \in G} \alpha_g p_g \in (kG)^*$, $ht = \varepsilon(h)t$ by linearity.

Recall from Example 4.9 that $(kG)^*$ is commutative. Thus $t = p_1$ is also a right integral for $(kG)^*$ since $th = ht = \varepsilon(h)t$. So p_1 is both a left and a right integral in H and it follows that $H = (kG)^*$ is unimodular.

This next theorem tells us that every finite dimensional Hopf algebra contains a non-zero set of left integrals, and moreover, no integral is unique.

Theorem 5.4 Let H be a finite dimensional Hopf algebra, then the set of integrals is a 1-dimensional vector space.

Proof: First note that $M = H$ is a right H^*-Hopf module via the action:

$$H \otimes H^* \to H \quad \text{via} \quad h \leftharpoonup f = \sum \langle f, h_1 \rangle h_2 = \sum_h f(h_1)h_2$$

and the coaction ρ where $\{l_1, \ldots, l_n\}$ is a basis of H and $f_1, \ldots, f_n \in H^*$ such that $\forall\, l \in H, lh = \sum_i \langle l, f_i \rangle l_i$:

$$\rho : H \to H \otimes H^* \quad \text{via} \quad \rho(h) = \sum_i l_i \otimes f_i.$$

For the details of this dualization of an H-action to an H^*-coaction see [Mo 93] Lemma 2.1.4.

Thus by the Fundamental Theorem of Hopf Modules (Theorem 4.15),

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

as right H^*-Hopf modules. However $M^{co(H^*)} = M^H$. To see this let $m \in M^{co(H^*)}$, then

$$\begin{aligned} \rho(m) &= \sum m_0 \otimes m_1 && \text{def of } \rho \quad (*) \\ &= m \otimes \varepsilon && \text{def of coinvariants of } H^*, \text{ and } \varepsilon = 1_{H^*}. \end{aligned}$$

For any $h \in H$,

$$\begin{aligned} h \cdot m &= \sum m_0 m_1(h) && \text{dualization of action to coaction} \\ &= m\varepsilon(h) && \text{substitution } (*) \text{ above} \\ &= \varepsilon(h)m && \varepsilon(h) \text{ is a scalar} \end{aligned}$$

which means $m \in M^H$, the invariants of H. Thus $M^{co(H^*)} \subseteq M^H$.

For the other inclusion, let $m \in M^H$. Then

$$\begin{aligned} h \cdot m &= \varepsilon(h)m && \text{def of invariant} \\ &= m\varepsilon(h) && \varepsilon(h) \text{ is a scalar.} \end{aligned}$$

But $h \cdot m = \sum m_0 m_1(h)$, thus $m\varepsilon(h) = \sum m_0 m_1(h)$. So

$$\begin{aligned} \rho(m) &= \sum m_0 \otimes m_1 && \text{def of } \rho \\ &= m \otimes \varepsilon. \end{aligned}$$

This is [Mo 93] Lemma 1.7.2 applied to the finite dimensional case, where it states that for a finite-dimensional H^*: let M be a left H-module such that it is also a right H^*-comodule, then $M^H = M^{co(H^*)}$. This means $m \in M^{co(H^*)}$, the coinvariants of H^*. Thus $M^H \subseteq M^{co(H^*)}$, so $M^H = M^{co(H^*)}$.

Substituting this fact into the isomorphism of Hopf modules gives

$$M \cong M^H \otimes H^*.$$

Now let $M = H$ (an H^*-Hopf module), then

$$H \cong H^H \otimes H^*.$$

Notice that the $\dim H = \dim H^*$, thus $\dim H^H = 1$. But

$$H^H = \{h \in H \mid ht = \varepsilon(h)t \quad \forall\, h, t \in H\} = \int_H^l .$$

Thus $\dim \int_H^l = 1$. $\square$

6 Maschke's Theorem for Hopf Algebras

Now that we have the necessary background on Hopf algebras, recall Maschke's Theorem for group algebras from Chapter 3:

Theorem 3.1 (Maschke's Theorem) Let G be a finite group. Then kG is semisimple if and only if $|G|^{-1} \in k$.

Let us look at this theorem in terms of integrals. Recall from Example 5.2 that for the group algebra kG, $t = \sum_{g \in G} g \in \int_{kG}$. Next consider $\varepsilon(t)$,

$$\varepsilon(t) = \varepsilon(\sum_{g \in G} g) = \sum_{g \in G} \varepsilon(g) = \sum_{g \in G} 1_k = |G|.$$

So $\varepsilon(t) = |G|$, the order of G. Since $\varepsilon(t) \in k$, it follows that $|G| \in k$ by substitution, and since k is a field $|G|^{-1} \in k$ if and only if $\varepsilon(t) \neq 0$.

Maschke's Theorem is thus a particular case of the more general theorem for Hopf algebras:

Theorem 6.1 (Maschke's Theorem for Hopf Algebras) [LS 69] Let H be any finite-dimensional Hopf algebra. Then H is semisimple if and only if $\varepsilon(\int_H^l) \neq 0$ if and only if $\varepsilon(\int_H^r) \neq 0$.

Before we prove this theorem there are several general lemmas we need to establish in addition to Lemma 3.2 and Theorem 3.3. The following lemma is a particular case of a more general theorem that says that the kernel and image of any algebra morphism are ideals. This lemma also gives an additional proof that the algebra of $n \times n$ matrices is not a Hopf algebra. For $M_n(k)$ is a simple algebra (Example 2.7), hence it has no non-trivial ideals (Definition 2.6). But as we see here, every Hopf algebra must contain at least one non-trivial ideal.

Lemma 6.2 The kernel of the counit map, $\ker\varepsilon$, is an ideal of H.

Proof: Let $h \in H, x \in \ker\varepsilon$, then

$$\begin{aligned} \varepsilon(xh) &= \varepsilon(x)\varepsilon(h) && \varepsilon \text{ is an algebra morphism} \\ &= 0\varepsilon(h) && x \in \ker\varepsilon \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} \varepsilon(hx) &= \varepsilon(h)\varepsilon(x) && \varepsilon \text{ is an algebra morphism} \\ &= \varepsilon(h)0 && x \in \ker\varepsilon \\ &= 0. \end{aligned}$$

Thus $xh, hx \in \ker\varepsilon$, which means $\ker\varepsilon$ is an ideal of H. □

Lemma 6.3 Suppose an algebra A can be written as a direct sum $A = I \oplus J$, with I a left ideal and J a right ideal. Then $JI = 0$. In particular, if $H = I \oplus \ker\varepsilon$, then $(\ker\varepsilon)I = 0$.

Proof: An algebra $A = I \oplus J$ implies that $I \cap J = \{0\}$. But I is a left ideal, and J is a right ideal. Thus $JI \subseteq J \cap I = \{0\}$. □

In the following proof we consider H as a left module over itself via left multiplication. Recall that an algebra is called semisimple if it is semisimple as a module over itself via left multiplication, and that in this context submodules are precisely the left ideals of the algebra. We are now ready for the proof of Theorem 6.1, Maschke's Theorem for Hopf algebras. We follow the proofs in [Mo 93] and [S 69B].

Proof of Theorem 6.1: (semisimple $\Rightarrow \varepsilon(\int_H^l) \neq 0$ and $\varepsilon(\int_H^r) \neq 0$)
Let H be a semisimple finite dimensional Hopf algebra. By Lemma 6.2, we know that $\ker\varepsilon$ is an ideal of H and thus a submodule of H. By Theorem 3.3 condition (2) we know that every submodule of H is a direct summand, therefore we may write $H = I \oplus \ker\varepsilon$ for some non-zero left ideal I of H.

Next, we claim that $I \subseteq \int_H^l$. To show this, let $z \in I$ and $h \in H$. We want to show that $hz = \varepsilon(h)z \quad \forall\, h \in H$. Note that $h - \varepsilon(h)\cdot 1_H \in \ker\varepsilon$ since

$$\begin{array}{rcll} \varepsilon(h - \varepsilon(h)\cdot 1_H) & = & \varepsilon(h) - \varepsilon(\varepsilon(h)\cdot 1_H) & \text{linearity of } \varepsilon \\ & = & \varepsilon(h) - \varepsilon(h)\varepsilon(1_H) & \text{linearity of } \varepsilon \\ & = & \varepsilon(h) - \varepsilon(h)1_k & \varepsilon(1_H) = 1_k \\ & = & \varepsilon(h) - \varepsilon(h) & \varepsilon(h) \in k \\ & = & 0 & \text{additive inverse property.} \end{array}$$

Using this fact together with Lemma 6.3 we see that

$$\begin{array}{rcll} hz & = & [h - \varepsilon(h)]z + \varepsilon(h)z & \text{add and subtract } \varepsilon(h)z \\ & = & 0 + \varepsilon(h)z & h - \varepsilon(h)\cdot 1_H \in \ker\varepsilon, \text{ and Lemma 6.3} \\ & = & \varepsilon(h)z & 0 \text{ is additive identity.} \end{array}$$

Thus $z \in \int_H^l$ by the definition of left integral, and so $I \subseteq \int_H^l$.

Applying the Dimension Theorem (Theorem A.4) for vector spaces to our case, we have $\dim(\ker\varepsilon) + \dim(\operatorname{im}\varepsilon) = \dim H$. Now, ε is a linear map, so $\operatorname{im}\varepsilon$ is a vector space. Also, $\operatorname{im}\varepsilon \neq 0$ since $\varepsilon(1) = 1$; moreover $\operatorname{im}\varepsilon \subset k$, and $\dim k = 1$, so $\dim(\operatorname{im}\varepsilon) = 1$. Thus $\dim(\ker\varepsilon) = \dim(H) - 1$. But $I \oplus \ker\varepsilon = H$; hence $\dim I + (\dim(H) - 1) = \dim H$. Therefore $\dim I = 1$, that is I is a one-dimensional space.

Since I is one-dimensional $I \neq 0$, so we take $0 \neq z \in I$. Now $0 \neq \varepsilon(z) \subset \varepsilon(I) \subset \varepsilon(\int_H^l)$. Hence $\varepsilon(\int_H^l) \neq 0$.

The proof to show $\varepsilon(\int_H^r) \neq 0$ is similar, with changes in that I is a right ideal of H, and to show that $I \subseteq \int_H^r$, we compute for $z \in I$ and $h \in H$:

$$\begin{array}{rcll} zh & = & z[h - \varepsilon(h)] + z\varepsilon(h) & \text{add and subtract } z\varepsilon(h) \\ & = & 0 + z\varepsilon(h) & h - \varepsilon(h)\cdot 1_H \in \ker\varepsilon \\ & = & \varepsilon(h)z & 0 \text{ is additive identity.} \end{array}$$

Thus $z \in \int_H^r$, and I is one-dimensional by the same reasoning as above. So, for $0 \neq z \in I$, $\varepsilon(z) \neq 0$. Hence $\varepsilon(\int_H^r) \neq 0$.

$\Big(\varepsilon(\int_H^l) \neq 0$ **or** $\varepsilon(\int_H^r) \neq 0 \Rightarrow$ **semisimple**$\Big)$

Let $\varepsilon(\int_H^l) \neq 0$. Then we may choose $t \in \int_H^l$ such that $\varepsilon(t) = 1$, since for any $z \in \int_H^l$, with $\varepsilon(z) \neq 0$, $\varepsilon[\varepsilon(z)^{-1}z] = \varepsilon(z)^{-1}\varepsilon(z) = 1$. Thus we may set $t = \varepsilon(z)^{-1}z$.

Next, let M be any (left) H-module, and let $N \subseteq M$ be an H-submodule. We claim that N has an H-complement in M, that is there exists a submodule $X \subseteq M$ such that $M = N \oplus X$. By showing N has an H-complement, we will then know by Theorem 3.3 that M is semisimple as an H-module.

To find this H-complement of N, note that in particular N is a k-subspace of M and consider $\pi : M \to N$ a k-linear projection (Definition A.7 and Corollary A.8 for the existence of such a map).

Now define a new map $\tilde{\pi} : M \to N$ by

$$\tilde{\pi}(m) = \sum_t t_1 \cdot \pi(St_2 \cdot m) \quad \forall\, m \in M.$$

The map $\tilde{\pi}$ is a k-linear projection onto N since, $\quad \forall\, n \in N$

$$\begin{aligned}
\tilde{\pi}(n) &= \sum_t t_1 \cdot \pi(St_2 \cdot n) && \text{substitution} \\
&= \sum_t t_1 St_2 \cdot n && \text{definition of } \pi \text{ and linearity} \\
&= \varepsilon(t) n && \text{definition of antipode} \\
&= n && \varepsilon(t) = 1.
\end{aligned}$$

And for any $m \in M, \pi(m) \in N$ so $\pi(St_2 \cdot m) \in N$. But N is an H-submodule so $t_1 \cdot \pi(St_2 \cdot m) \in t \cdot N \subseteq N$. Hence $\tilde{\pi}(m) \in N$. So $M = N \oplus \ker\tilde{\pi}$ as vector spaces.

Furthermore, $\tilde{\pi}$ is an H-module map. To see this, let $h \in H$ and $m \in M$, then

$$\begin{aligned}
h \cdot \tilde{\pi}(m) &= h \cdot [\sum_t t_1 \cdot \pi(St_2 \cdot m)] && \text{application of } \tilde{\pi} \\
&= \sum_t h \cdot t_1 \cdot \pi(St_2 \cdot m) && \text{linearity} \\
&= \sum_{t,h} h_1 \varepsilon(h_2) t_1 \cdot \pi(St_2 \cdot m) && \text{counit diagram} \\
&= \sum_{t,h} h_1 t_1 \cdot \pi((St_2)\varepsilon(h_2) \cdot m) && \text{linearity of } \pi \\
&= \sum_{t,h} h_1 t_1 \cdot \pi((St_2)(Sh_2)h_3 \cdot m) && \text{definition of antipode} \\
&= \sum_{t,h} h_1 t_1 \cdot \pi(S(h_2 t_2)h_3 \cdot m) && \text{antipode is an antihomomorphism} \\
&= \sum_t t_1 \cdot \pi((St_2)h \cdot m) && \text{(*) - see below} \\
&= \tilde{\pi}(h \cdot m) && \text{defintion of } \tilde{\pi}.
\end{aligned}$$

Where (*) holds since

$$
\begin{aligned}
\sum_{t,h} h_1t_1 \otimes S(h_2t_2) \otimes h_3 &= (id \otimes S \otimes id)(\sum_{t,h} h_1t_1 \otimes h_2t_2 \otimes h_3) & \\
&= (id \otimes S \otimes id)(\sum_{h} \Delta(h_1t) \otimes h_2) & \text{def of counit} \\
&= (id \otimes S \otimes id)(\sum_{h} \Delta(\varepsilon(h_1)t) \otimes h_2) & \text{def left integral} \\
&= (id \otimes S \otimes id)(\sum_{h} \Delta t \otimes \varepsilon(h_1)h_2) & \varepsilon(h_1) \in k \\
&= (id \otimes S \otimes id)(\Delta t \otimes h) & \text{def of unit} \\
&= \sum_{t} t_1 \otimes S(t_2) \otimes h. &
\end{aligned}
$$

The space $\ker\tilde{\pi}$ is an H-submodule by Lemma 3.2, since $\tilde{\pi}$ is an H-module map. Therefore, N has an H-complement, $\ker\tilde{\pi}$ in M. So by Theorem 3.3 M is a semisimple H-module.

The argument for $\varepsilon(\int_H^r) \neq 0$ is similar, except that M is a (right) H-module, and the projection $\tilde{\pi}$ must be defined appropriately. In this case we take $t \in \int_H^r$ with $\varepsilon(t) = 1$. The map $\tilde{\pi} : M \to N$ is then defined to be:

$$\tilde{\pi}(m) = \sum_{t} \pi(m \cdot St_1) \cdot t_2 \quad \forall\, m \in M.$$

To see that $\tilde{\pi}$ is a projection onto N, consider $\forall\, n \in N$:

$$
\begin{aligned}
\tilde{\pi}(n) &= \sum_{t} \pi(n \cdot St_1) \cdot t_2 & \text{substitution} \\
&= \sum_{t} \pi(n) \cdot (St_1) \cdot t_2 & \text{linearity of } \pi \\
&= \sum_{t} n \cdot (St_1)t_2 & \text{definition of } \pi \\
&= n\varepsilon(t) & \text{definition of antipode} \\
&= n & \varepsilon(t) = 1.
\end{aligned}
$$

And for any $m \in M, \pi(m) \in N$ so $\pi(m \cdot St_1) \in N$. But N is an H-submodule so $\pi(m \cdot St_1) \cdot t_2 \in N \cdot t \subseteq N$. Hence $\tilde{\pi}(m) \in N$.

Furthermore $\tilde{\pi}$ is an H-module map since

$$
\begin{array}{rcll}
\tilde{\pi}(m)\cdot h & = & [\sum_t \pi(m\cdot St_1)\cdot t_2]\cdot h & \text{application of } \tilde{\pi} \\
 & = & \sum_t \pi(m\cdot St_1)\cdot t_2 h & \text{linearity} \\
 & = & \sum_{t,h} \pi(m\cdot St_1)\cdot t_2\varepsilon(h_1)h_2 & \text{counit diagram} \\
 & = & \sum_{t,h} \pi(m\cdot \varepsilon(h_1)(St_1))\cdot t_2h_2 & \text{linearity of } \pi \\
 & = & \sum_{t,h} \pi(m\cdot h_1(Sh_2)(St_1))\cdot t_2h_3 & \text{def of antipode} \\
 & = & \sum_{t,h} \pi(m\cdot h_1S(t_1h_2))\cdot t_2h_3 & \text{antihomomorphism} \\
 & = & \sum_t \pi(m\cdot hS(t_1))\cdot t_2 & \text{(**) - see below} \\
 & = & \tilde{\pi}(m\cdot h) & \text{definition of } \tilde{\pi}.
\end{array}
$$

Where $(**)$ holds because

$$
\begin{array}{rcll}
\sum_{t,h} h_1\otimes S(t_1h_2)\otimes t_2h_3 & = & (id\otimes S\otimes id)(\sum_{t,h} h_1\otimes t_1h_2\otimes t_2h_3) & \\
 & = & (id\otimes S\otimes id)(\sum_h h_1\otimes \Delta(th_2)) & \text{def of counit} \\
 & = & (id\otimes S\otimes id)(\sum_h h_1\otimes \Delta(\varepsilon(h_2)t)) & \text{def of rt integral} \\
 & = & (id\otimes S\otimes id)(\sum_h h_1\varepsilon(h_2)\otimes \Delta t) & \varepsilon(h_2)\in k \\
 & = & (id\otimes S\otimes id)(h\otimes \Delta t) & \text{def of unit} \\
 & = & \sum_t h\otimes St_1\otimes t_2 &
\end{array}
$$

Hence M is semisimple. $\square$

7 Cosemisimplicity

We continue along the lines of dualizing by looking at cosemisimplicity, the dual of semisimplicity. In dualizing algebras to coalgebras usually the algebra needs to be finite dimensional; whereas this is not necessarily the case for dualizing coalgebras to algebras. Coalgebras have a property called "local finiteness" where every element of a coalgebra belongs to a finite dimensional subcoalgebra.

To see how to dualize in general, look at a vector space V, then the linear dual $V^* = \mathrm{Hom}_k(V, k)$. In constructing dual maps, consider the map $f : V \to U$ where V and U are vector spaces. The dual map $f^* : U^* \to V^*$ is defined by

$$f^*(u^*)(v) := (u^*)(f(v)) \quad \forall\, u^* \in U^*, v \in V.$$

We will use this fact throughout this section.

First let us define some of the "dual" concepts to subalgebra, simplicity and semisimplicity.

Definition 7.1 [S 69B] Suppose C is a coalgebra and D is a subspace with $\Delta(D) \subseteq D \otimes D$. Then D is a **subcoalgebra** of C.

Definition 7.2 Let C be any coalgebra.

1. C is **simple** if it has no proper subcoalgebras.

2. C is **cosemisimple** if it is a direct sum of simple subcoalgebras.

The following proposition shows us how an algebra is related to a coalgebra.

Proposition 7.3 If C is a coalgebra then C^* is an algebra.

Proof: Let (C, Δ, ε) be a coalgebra. The linear dual $C^* = \mathrm{Hom}_k(C, k)$. Define $\mu = \Delta^* : (C \otimes C)^* \to C^*$. Note that $C^* \otimes C^* \hookrightarrow (C \otimes C)^*$ by

$(f \otimes g)(c \otimes d) = f(c)g(d) \quad \forall\, f, g \in C^*$ and $c, d \in C$. So we can restrict μ to $C^* \otimes C^*$ where

$$\mu(f \otimes g)(c) := (f \otimes g)(\Delta(c)).$$

This gives the multiplication map on C^*, the "dual algebra structure." Next define $\eta = \varepsilon^* : k^* \to C^*$. But $k \cong k^*$, so η can be restricted to k where

$$\eta(f)(c) := f(\varepsilon(c)).$$

For C^* to be an algebra the associativity and unit diagrams must commute.

First check the associativity diagram, $\forall\, f, g, h \in C^*$:

$$(f \otimes g \otimes h) \overset{\mu \otimes id}{\mapsto} (fg) \otimes h \overset{\mu}{\mapsto} (fg)h,$$

and

$$(f \otimes g \otimes h) \overset{id \otimes \mu}{\mapsto} f \otimes (gh) \overset{\mu}{\mapsto} f(gh).$$

These are equal since composition of functions is an associative operation.

To check the unit diagram, $\forall\, f \in C^*$:

$$1_k \otimes f \overset{\eta \otimes id}{\mapsto} \eta(1_k) \otimes f = 1_{C^*} \otimes f \overset{\mu}{\mapsto} 1_{C^*} f = f,$$

and

$$1_k \otimes f \mapsto 1_k f = f.$$

Also,

$$f \otimes 1_k \overset{id \otimes \eta}{\mapsto} f \otimes \eta(1_k) = f \otimes 1_{C^*} \overset{\mu}{\mapsto} f 1_{C^*} = f,$$

and

$$f \otimes 1_k \mapsto f 1_k = f,$$

which are also equal. Thus the associativity and unit diagrams commute, and C^* is an algebra. $\square$

The following proposition gives us the correlation between ideals in algebras and subcoalgebras in coalgebras. This correlation is important in proving Proposition 7.5.

Proposition 7.4 [S 69B] Let C be a coalgebra. Then:

1. If $D \subseteq C$ is a subcoalgebra, then $D^{\perp} \subseteq C^*$ is a two-sided ideal of C^* where $D^{\perp} = \{f \in C^* \mid f(d) = 0 \quad \forall\, d \in D\}$.

2. If $I \subseteq C^*$ is any two-sided ideal, then $I^{\perp} \subseteq C$ is a subcoalgebra where $I^{\perp} = \{c \in C \mid g(c) = 0 \quad \forall\, g \in I\}$.

We follow [S 69B] in the proof of this propostion.

Proof:

1. Let $D \subseteq C$ be a subcoalgebra. Let $i : D \to C$ to be the inclusion map (Definition A.9). The inclusion map is a coalgebra map, as $\forall\, d \in D$:

$$\begin{aligned}(\Delta \circ i)(d) &= \Delta(i(d)) \\ &= \Delta(d) \\ &= \sum_d d_1 \otimes d_2 \\ &= \sum_d i(d_1) \otimes i(d_2) \\ &= (i \otimes i) \sum_d d_1 \otimes d_2 \\ &= (i \otimes i)\Delta(d),\end{aligned}$$

and

$$(\varepsilon \circ i)(d) = \varepsilon(i(d)) = \varepsilon(d).$$

This coalgebra map induces an algebra map $i^* : C^* \to D^*$ given by

$$i^*(f)(d) := f(i(d)) = f(d).$$

The set $\ker(i^*) = \{f \in C^* \mid i^*(f) = 0\} = \{f \in C^* \mid f(d) = 0 \quad \forall\, d \in D\} = D^\perp$. Moreover, $\ker(i^*)$ is an ideal of C^*, since $\forall\, f \in C^* g \in \ker(i^*)$ and $d \in D$:

$$i^*(fg)(d) = fg(i(d)) = f(g(d)) = f(0) = 0,$$

and

$$i^*(gf)(d) = gf(i(d)) = gf(d) = 0.$$

Thus $D^\perp = \ker(i^*)$ is a two-sided ideal of C^*.

2. Let $I \subseteq C^*$ be a two-sided ideal. Let $I^\perp = \{c \in C \mid g(c) = 0 \quad \forall\, g \in I\}$. Take $x \in I^\perp$ and say $\Delta(x) = \sum_i y_i \otimes z_i$ where $\{y_i\} \cup \{z_i\} \subset C$. Assume $\{z_i\}$ is linearly independent. Then if $\Delta(x) \notin I^\perp \otimes C$ this means $y_i \notin I^\perp$ for some i. Without loss of generality we may assume $i = 1$; then $y_1 \notin I^\perp$, that is there exists $h \in I$ such that $h(y_1) \neq 0$. Next choose $f \in C^*$ such that $f(z_j) = \delta_{1j}$. Since I is an ideal, $hf \in I$. Thus $hf(x) = 0$. But $hf(x) = (h \otimes f)\Delta(x)$ by the dual algebra structure. Hence

$$\begin{aligned} 0 = hf(x) &= (h \otimes f)\Delta(x) \\ &= (h \otimes f)\sum_i y_i \otimes z_i \\ &= \sum_i h(y_i) \otimes f(z_i) \\ &\neq 0 \quad \text{since } h(y_1) \neq 0 \end{aligned}$$

This is a contradiction. Thus $\Delta(x) \in I^\perp \otimes C$. Similarly $\Delta(x) \in C \otimes I^\perp$. This means

$$\Delta(x) \in (I^\perp \otimes C) \cap (C \otimes I^\perp) = I^\perp \otimes I^\perp.$$

Hence $I^\perp$ is a subcoalgebra of C. □

This next proposition allows us to see that some properties are carried through the dualization process.

Proposition 7.5 If C is a coalgebra, then:

1. C is simple if and only if C^* is a simple algebra.

2. If C is cosemisimple then C^* is a semisimple algebra.

3. If C is finite dimensional and C^* is a semisimple algebra, then C is cosemisimple.

Proof:

1. ($\Rightarrow$) Assume that C is a simple coalgebra. This means that C has no proper subcoalgebras, that is the only subcoalgebras of C are $\{0\}$ and C itself. Let $I \subseteq C^*$ be a two-sided ideal of C^*. By Proposition 7.4 (2) this means there exists a subcoalgebra $I^\perp = \{c \in C \mid f(c) = 0 \quad \forall\, f \in I\} \subset C$. But C is a simple coalgebra, so $I^\perp = \{0\}$ or $I^\perp = C$. If $I^\perp = \{0\}$, then $I = C$. If $I^\perp = C$, then $I = \{0\}$. Thus C^* is a simple algebra.

   ($\Leftarrow$) Assume that C^* is a simple algebra and let $D \subseteq C$ be a subcoalgebra. By Proposition 7.4 (1) $D^\perp = \{f \in C^* \mid f(d) = 0 \quad \forall\, d \in D\}$ is a two-sided ideal of C^*. But C^* is simple, therefore $D^\perp = \{0\}$ or $D^\perp = C^*$. If $D^\perp = \{0\}$ then $D = C$. If $D^\perp = C^*$ then $D = \{0\}$. Thus C is a simple coalgebra.

2. Assume that C is cosemisimple. Then $C = \oplus_i C_i$ where each C_i is a simple subcoalgebra for every i. By (2) C_i^* is a simple algebra for every i. However,

   $$C^* = (\oplus_i C_i)^* \cong \oplus_i C_i^*$$

   Thus C^* is a semisimple algebra.

3. Is proved similarly. □

Together the next two examples show Proposition 7.5 in action.

Example 7.6 The group algebra kG is cosemisimple.

Let $\{g\}_{g\in G}$ be a basis of kG. Then every $g \in G$ generates a one-dimensional subcoalgebra kg, as dim$kg = 1$. Each kg is simple since there is only one basis element, which means that there are no non-trivial subcoalgebras. Since $\{g\}_{g\in G}$ is a basis for kG,

$$kG = k\sum_{g\in G} g = \sum_{g\in G} kg.$$

Also $\cap_{g\in G}kg = \{0\}$. Thus $kG = \oplus_{g\in G}kg$. Hence kG is cosemisimple.

Example 7.7 The linear dual of the group algebra $(kG)^*$ is semisimple.

By Example 7.6 the group algebra kG is cosemisimple. So according to Proposition 7.5 part (2) the linear dual of the group algebra $(kG)^*$ is semisimple as an algebra. We write $(kG)^*$ explicitly as a direct sum of simple algebras as in Example 2.11. A basis for $(kG)^*$ is $\{p_g\}_{g\in G}$. So $(kG)^* = \oplus_{g\in G}kp_g$ where kp_g is a simple algebra for every $g \in G$. Notice that each kp_g is an algebra because $p_gp_g = p_g$, which means multiplication is closed and p_g is its own unit.

The space of left integrals in H is 1-dimensional and is an ideal in H. Any Hopf algebra with a finite dimensional ideal is finite dimensional itself. So this definition of left integrals in H won't help in the infinite dimensional case. This next definition for a left integral on H will work for the infinte dimensional case.

Definition 7.8 Let H be a Hopf algebra. An element $T \in H^*$ is a **left integral on H** if $\forall\ f \in h^*$,

$$fT = f(1_H)T.$$

We denote the space of left integrals on H by $\mathcal{I}^l_H \subset H^*$.

Compare this definition of a left integral on H with Definition 5.1, a left integral in H. Notice that when H is finite dimensional, an integral on H is the same as an integral in H^*. This is because $\varepsilon_{H^*}(f) = f(1_H)$, the unit in H^*.

We now dualize Maschke's Theorem for Hopf Algebras (Theorem 6.1) to a dual theorem for coalgebras. Recall that Maschke's Theorem for Hopf algebras says a finite dimensional Hopf algebra H is semisimple if and only if $\varepsilon(\int_H^l) \neq 0$. The concept of semisimplicity has a dual concept of cosemisimplicity. For $\varepsilon(\int_H^l) \neq 0$ to dualize, consider what this means for an integral on H. In H^*, $\varepsilon_{H^*}(T) = T(1_H) = 1_k$. Thus we have the following Dual Maschke Theorem.

Theorem 7.9 (Dual Maschke Theorem) Let H be any Hopf algebra and $T \in H^*$. Then H is cosemisimple (as a coalgebra) if and only if there exists a left integral T on H satisfying $T(1_H) = 1_k$.

We will prove just the finite dimensional case here as it is just a direct application of Maschke's Theorem for Hopf algebras.

Proof: ($\Rightarrow$) Let H be a finite-dimensional cosemisimple Hopf algebra and $T \in H^*$. By Propositions 7.5 (2), H^* is semisimple, which means $\varepsilon_{H^*}(\int_{H^*}^l) \neq 0$ by Maschke's Theorem for Hopf algebras (Theorem 6.1). Thus $\varepsilon_{H^*}(T) = T(1_H) = 1_k$.
($\Leftarrow$) Let H be a finite-dimensional Hopf algebra where there exists a left integral $T \in H^*$ on H such that $T(1_H) = 1_k$. Notice that $\varepsilon_{H^*}(T) = T(1_H) = 1_k \neq 0$. Thus $\varepsilon_{H^*}(\int_{H^*}^l) \neq 0$. Therefore by Maschke's Theorem for Hopf algebras (Theorem 6.1), H^* is semisimple, which means H is cosemisimple by Proposition 7.5 (2). □

A Linear Algebra

The following section contains some classical linear algebra definitions and results used throughout this paper. The sources that were used for this section were [Ga 94], [An 84], and [WT 79].

Definition A.1 A set V is said to be a **vector space** over a field k if V is an Abelian group under addition and if $\forall\ a \in k,\ v \in V$, there is an element $av \in V$ such that the following conditions hold $\forall\ a, b \in k$ and $u, v \in V$:

1. $a(v+u) = av + au$,
2. $(a+b)v = av + bv$,
3. $a(bv) = (ab)v$,
4. $1_k v = v$.

Proposition A.2 Let V be a finite dimensional vector space. Any linearly independent set $\{u_1, u_2, \ldots, u_t\}$ in V can be extended to a basis of V.

Proof: Let $\{u_1, u_2, \ldots, u_t\}$ be a linearly independent set in V. Either $\{u_1, u_2, \ldots, u_t\}$ spans V and is itself a basis of V or there exists $v \in V$ that is not a linear combination of $\{u_1, u_2, \ldots, u_t\}$. We claim that $\{u_1, u_2, \ldots, u_t, v\}$ is linearly independent. To see this, let $\alpha_i \in k \quad \forall\ i = 1, \ldots, t+1$ such that

$$\alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_t u_t + \alpha_{t+1} v = 0.$$

If $\alpha_{t+1} \neq 0$ then we may solve for v to get

$$v = \frac{-\alpha_1}{\alpha_{t+1}} u_1 - \frac{\alpha_2}{\alpha_{t+1}} u_2 - \cdots - \frac{\alpha_t}{\alpha_{t+1}} u_t.$$

But v was not a linear combination of $\{u_1, u_2, \ldots, u_t\}$. Thus $\alpha_{t+1} = 0$, and since $\{u_1, u_2, \ldots, u_t\}$ is linearly independent, we know $\alpha_i = 0 \quad \forall\, i \in \{1, 2, \ldots, t\}$. If $\{u_1, u_2, \ldots, u_t, v\}$ does not span V, then there is a $v' \in V$ that is not a linear combination of $\{u_1, u_2, \ldots, v_t, v\}$. Repeat the process as we did for v. Continue adding basis elements in the same manner until we get a set that spans V. This process must end after a finite number of steps, since V is finite dimensional. The result is a basis of V containing the original linearly independent set. $\square$

Theorem A.3 Let $f : V \to W$ be a linear map of vector spaces. Then:

1. $\ker f$ is a subspace of V,
2. $\operatorname{im} f$ is a subspace of W.

Proof:

1. Let $u, v \in \ker f$ and $\alpha, \beta \in k$. Then

$$\begin{array}{rcll} f(\alpha u + \beta v) & = & \alpha f(u) + \beta f(v) & f \text{ is linear} \\ & = & \alpha 0 + \beta 0 & u, v \in \ker f \\ & = & 0. & \end{array}$$

   Thus $\alpha u + \beta v \in \ker f$, so $\ker f \subseteq V$.

2. Let $u, v \in V$ and $x, y \in \operatorname{im} f$ such that $f(u) = x$ and $f(v) = y$. Let $\alpha, \beta \in k$. Then

$$\begin{array}{rcll} \alpha x + \beta y & = & \alpha f(u) + \beta f(v) & \text{substitution} \\ & = & f(\alpha u + \beta v) & \text{linearity of } f. \end{array}$$

   Thus $\alpha x + \beta y \in \operatorname{im} f$, so $\operatorname{im} f \subseteq W$. $\square$

Theorem A.4 (Dimension Theorem) Let V and W be vector spaces, and $f : V \to W$ be a linear map. Then:

$$\dim(\ker f) + \dim(\operatorname{im} f) = \dim V.$$

Proof: Denote $\dim V = n$, and let $\{v_1, v_2, \ldots, v_r\}$ be a basis for $\ker f$. By Proposition A.2, this basis may be extended to form a basis $\{v_1, \ldots, v_r, \ldots, v_n\}$ of V. We will show that $\mathcal{B} = \{f(v_{r+1}), f(v_{r+2}), \ldots, f(v_n)\}$ is a basis for $\mathrm{im} f$.

First we will show that $\mathcal{B}$ spans $\mathrm{im} f$. Let $b \in \mathrm{im} f$; then $b = f(v)$ for some $v \in V$. Let $\alpha_i \in k \quad \forall\, i \in \{1, 2, \ldots, n\}$. Then

$$\begin{array}{rcll} b & = & f(v) & \text{as defined} \\ & = & f(\sum\limits_{i=1}^{n} \alpha_i v_i) & v \text{ is a linear combination of basis elements} \\ & = & \sum\limits_{i=1}^{n} \alpha_i f(v_i) & \text{linearity of } f \\ & = & \sum\limits_{i=1}^{r} \alpha_i \cdot 0 + \sum\limits_{i=r+1}^{n} \alpha_i f(v_i) & \{v_1, v_2, \ldots, v_r\} \in \ker f \\ & = & \sum\limits_{i=r+1}^{n} \alpha_i f(v_i). & \end{array}$$

Thus $\mathcal{B}$ spans $\mathrm{im} f$.

Next, we must show that $\mathcal{B}$ is linearly independent. Suppose

$$0 = \sum_{i=r+1}^{n} \alpha_i f(v_i) = f(\sum_{i=r+1}^{n} \alpha_i v_i)$$

which means $\sum\limits_{i=r+1}^{n} \alpha_i v_i \in \ker f$. Therefore

$$\begin{array}{lrcl} & \sum\limits_{i=r+1}^{n} \alpha_i v_i & = & \sum\limits_{i=1}^{r} \alpha_i v_i \\ \text{so} & 0 & = & \sum\limits_{i=1}^{r} \alpha_i v_i - \sum\limits_{i=r+1}^{n} \alpha_i v_i. \end{array}$$

But the v_i's are linearly independent. Thus $\alpha_i = 0 \quad \forall i \in \{1, 2, \ldots, n\}$. In particular $\alpha_i = 0 \quad \forall i \in \{r+1, r+2, \ldots, n\}$. So $\mathcal{B}$ is linearly independent, which means $\mathcal{B}$ is a basis for $\mathrm{im} f$.

Thus $\dim(\ker f) + \dim(\mathrm{im} f) = r + (n - r) = n = \dim V$. $\square$

Definition A.5 Suppose V is a vector space and U is a subspace of V. The subspace U is said to have a (linear) **complement** W if there exists a subspace $W \subset V$ such that $U \oplus W = V$.

Proposition A.6 For any subspace U of V, U has a linear complement.

Proof: Let $U \subseteq V$ be a subspace with basis $u_1, u_2, \ldots, u_t$. By Proposition A.2 $\{u_1, u_2, \ldots, u_t\}$ may be extended to form a basis of V. Call this basis $\mathcal{B} = \{u_1, u_2, \ldots, u_t, w_1, \ldots, w_r\}$. Set $W = \mathrm{sp}\{w_1, w_2, \ldots w_r\}$. Since $\mathcal{B}$ is a basis of V, for any element $v \in V$ there exist $\alpha_i, \beta_j \in k$ for $i \in \{1, 2, \ldots, t\}, j \in \{1, 2, \ldots, r\}$ such that

$$v = (\sum_{i=1}^{t} \alpha_i u_i) + (\sum_{j=1}^{r} \beta_j w_j) \in U + W.$$

Thus $V \subset U + W$ and similarly $U + W \subset V$, so $V = U + W$.

All elements of U are of the form $\sum_{i=1}^{t} \alpha_i u_i$, and all elements of W are of the form $\sum_{j=1}^{r} \beta_j w_j$. Take $x \in U \cap W$, which means that $x = \sum_{i=1}^{t} \alpha_i u_i$, and also $x = \sum_{j=1}^{r} \beta_j w_j$. Thus

$$\sum_{i=1}^{t} \alpha_i u_i = \sum_{j=1}^{r} \beta_j w_j,$$

which implies

$$\sum_{i=1}^{t} \alpha_i u_i - \sum_{j=1}^{r} \beta_j w_j = 0.$$

But u_i and w_j form a basis of V. Thus they are linearly independent. So, $\alpha_i = \beta_j = 0 \quad \forall\, i, j$, which means $x = 0$. Hence $U \cap W = \{0\}$. So U has a linear complement W in V. $\square$

Definition A.7 Let M be an A-module and N a submodule of M. A map $\pi : M \to N$ is called a k**-linear projection** onto N if π is linear and $\pi(n) = n \quad \forall\, n \in N$.

Corollary A.8 For any subspace U of V there exists a k-linear projection $\pi : V \to U$.

Proof: Let $U \subseteq V$ be a k-subspace. By Proposition A.6 there exists a subspace W such that $V = U \oplus W$. This means we may choose a basis $\{u_1, u_2, \ldots, u_r, w_1, w_2, \ldots, w_s\}$ of V. Next define a map $\pi : V \to U$ via

$$\pi(u_i) = u_i \quad \forall\, i \in \{1, 2, \ldots, r\}$$

$$\pi(w_i) = 0 \quad \forall\, i \in \{1, 2, \ldots, s\}$$

and extend linearly. The map π is k-linear by its definition, and a projection since $\forall\, u \in U, u = \sum_{i=1}^{r} \alpha_i u_i$, so

$$\begin{aligned} \pi(u) &= \pi\left(\sum_{i=1}^{r} \alpha_i u_i\right) & \\ &= \sum_{i=1}^{r} \alpha_i \pi(u_i) & \text{linearity} \\ &= \sum_{i=1}^{r} \alpha_i u_i & \text{def of } \pi \\ &= u. & \end{aligned}$$

□

Definition A.9 For sets A and B with $A \subset B$, the function $i : A \to B$, defined by $i(x) = x \quad \forall\, x \in A$ is called the **inclusion map**.

B List of Symbols

SYMBOL	MEANING
G	group
R	ring
M	module, unless otherwise noted
A	algebra
k	ground field
V	vector space
D	division ring
μ	multiplication
η	unit
id	identity map
γ	module map
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$M_n(k)$	the $n \times n$ matrices over a field k
m_{ij}, n_{ij}	elements of a matrix in (i, j)-place
kG	the group algebra
$\lvert G \rvert$	order of a group G
$\otimes$	tensor product
Δ	comultiplication
ε	counit
C	coalgebra
ρ	comodule map
B	bialgebra
$*$	convolution product
$\mathrm{Hom}(C, A)$	homomorphisms from C to A
S	antipode
H	Hopf algebra
$(kG)^*$	linear dual of the group algebra kG for a finite group G
δ_{ij}	Kronecker delta
$U(L)$	Universal Enveloping Algebra of the Lie algebra L
$\int_H^l$	space of left integrals in a Hopf algebra H
$\int_H^r$	space of right integrals in a Hopf algebra H

References

[Ab 77] Eiichi Abe, *Hopf Algebras*, Cambridge University Press, Cambridge, 1980 (original Japanese version published by Iwanami Shoten, Tokyo, 1977).

[AA 85] Donald J. Albers and G. L. Alexanderson, *Mathematical People: Profiles and Interviews*, Birkhäuser, Boston, 1985.

[AW 92] William A. Adkins and Steven H. Weintraub, *Algebra - An Approach via Module Theory*, Graduate Texts in Mathematics 136, Springer-Verlag, New York, 1992.

[An 84] Howard Anton, *Elementary Linear Algebra*, John Wiley & Sons, New York, 1984.

[Be 85] George M. Bergman, *Everybody Knows What A Hopf Algebra Is*, AMS Contemporary Mathematics 43 (1985), 25-48.

[Bo 08] Oskar Bolza, *Heinrich Maschke: His Life and Work*, Bulletin of the American Mathematical Society 15 (Nov. 1908), 85-95.

[BM 89] Carl B. Boyer and Uta C. Merzabach, *A History of Mathematics*, John Wiley & Sons, New York, 1989.

[FD 93] Benson Farb and R. Keith Dennis, *Noncommutative Algebra*, Graduate Texts in Mathematics 144, Springer-Verlag, New York, 1993.

[Ga 94] Joseph A. Gallian, *Contemporary Abstract Algebra*, D.C. Heath and Company, Lexington, MA, 1994.

[Gi 72] Charles Coulston Gillispie, *Dictionary of Scientific Biography* vol. VI, Charles Scribner's Sons, New York, 1972.

[H 41] Heinz Hopf, *Über die Topologie der Gruppen-Mannigfaltigkeiten und ihre Verallgemeinerungen*, Annals of Mathematics 42 (1941), 22-52.

[H 83] Heinz Hopf, *Differential Geometry in the Large*, Lecture Notes in Mathematics 1000, Springer-Verlag, Heidelberg, 1983.

[J 74] Nathan Jacobson, *Basic Algebra I*, W. H. Freeman and Company, San Francisco, 1974.

[J 80] Nathan Jacobson, *Basic Algebra II*, W. H. Freeman and Company, San Francisco, 1980.

[Kp 75] Irving Kaplansky, *Bialgebras*, University of Chicago Lecture Notes, 1975.

[Ks 95] Christian Kassel, *Quantum Groups*, Graduate Texts in Mathematics 155, Springer-Verlag, New York, 1995.

[L 66] Joachim Lambek, *Rings and Modules*, Chelsea Press, New York, 1966.

[LS 69] R. G. Larson and M. Sweedler, *An Associative Orthogonal Bilinear Form for Hopf Algebras*, American Journal of Mathematics 91 (1969), 75-93.

[Ma 33] Dumas Malone, *Dictionary of American Biography* vol. XII, Charles Scribner's Sons, New York, 1933.

[M 1898] Heinriche Maschke, *Über den arithmetischen Charakter der Substitutionen endlicher Substitutions gruppen*, Math. Annalen 50 (1898), 492-498.

[Mo 93] Susan Montgomery, *Hopf Algebras and Their Actions on Rings*, Regional Conference Series in Mathematics 82, American Mathematical Society, Providence, 1993.

[P 94] Jean-Paul Pier, *Development of Mathematics 1900 - 1950*, Birkhäuser, Basel, 1994.

[SG 34] David E. Smith and Jekuthiel Ginsburg, *A History of Mathematics in America Before 1900*, The Mathematical Association of America, Chicago, 1934.

[S 68] Moss E. Sweedler, *Cohomology of Algebras over Hopf Algebras*, Trans. American Mathematical Society 127 (1968), 205-239.

[S 69A] Moss E. Sweedler, *Integrals for Hopf Algebras*, Annals of Mathematics 89 (1969), 323-335.

[S 69B] Moss E. Sweedler, *Hopf Algebras*, W. A. Benjamin, New York, 1969.

[W 85] B. L. van der Waerden, *A History of Algebra From al-Khwārizmī to Emmy Noether*, Springer-Verlag, Heidelberg, 1985.

[WT 79] Richard E. Williamson and Hale F. Trotter, *Multivariable Mathematics*, Prentice-Hall, Englewood Cliffs, NJ, 1979.