LECTURES ON HOPF ALGEBRAS

HANS-JÜRGEN SCHNEIDER

Notes by Sonia Natale

Preface

These notes contain the material presented in a series of five lectures at the University of Córdoba in September 1994. The intent of this brief course was to give a quick introduction to Hopf algebras and to prove as directly as possible (to me) some recent results on finite-dimensional Hopf algebras conjectured by Kaplansky in 1975. In particular, in the last part of the course I gave a complete proof from scratch of Zhou's theorem (1994): Any finite-dimensional Hopf algebra over the complex numbers of prime dimension p is isomorphic to the group algebra of the group of order p.

I would like to thank Nicolás Andruskiewitsch and the members of the Mathematics Department of the FaMAF (University of Córdoba) for the kind invitation to visit Córdoba and for their warm hospitality. I also wish to thank the students in my class for their attention and for most enjoyable hours after the lectures.

My special thanks are due to Sonia Natale who has written up the notes of a condensed course with great care and insight.

H.-J. Schneider

Supported by a grant of DAAD-Antorchas, a Subsidio of the SECyT (U.N. Córdoba) and the CIEM.

§1 Definitions and examples

In what follows, we will consider a commutative ring k (later on k will be a field); the symbols Hom and $\otimes$ will mean Hom_k and $\otimes_k$ respectively.

By an algebra R over k (or simply an algebra) we understand a unitary, associative k-algebra R, with identity $1 = 1_R$. The category of k-algebras will be denoted by Alg_k. If R is an algebra, then R^{op} denotes the opposite algebra (i.e. the k-module R with multiplication $a._{op}b = ba$).

For an algebra R, ${}_R\mathcal{M}$ (respectively $\mathcal{M}_R$) will denote the category of left (respectively right) R-modules. Recall that a k-module M is a left (respectively right) R-module, if and only if, there exists an algebra map: $R \longrightarrow \mathrm{End}(M)$ (respectively $R^{op} \longrightarrow \mathrm{End}(M)$).

Remarks on representation theory.

1. Let G be a group, $H := kG$ its group algebra; V, W in ${}_H\mathcal{M}$. Then k, $V \otimes W$, and $V^* = \mathrm{Hom}(V, k)$ can be made into left H-modules by setting:

$$g.1 = 1,$$
$$g.(v \otimes w) = g.v \otimes g.w,$$
$$(g.\phi)(v) = \phi(g^{-1}.v),$$

for all $g \in G, v \in V, w \in W, \phi \in V^*$.

We note that the algebra maps which define the module structures in each case are given by:

$$\epsilon : \ kG \longrightarrow k,$$
$$kG \xrightarrow{\Delta} kG \otimes kG \longrightarrow \mathrm{End}(V) \otimes \mathrm{End}(W) \longrightarrow \mathrm{End}(V \otimes W),$$
$$kG \xrightarrow{\mathcal{S}} kG^{op} \xrightarrow{\text{transpose}} \mathrm{End}(V^*),$$

where $\epsilon(g) = 1$, $\Delta(g) = g \otimes g$, $\mathcal{S}(g) = g^{-1}$, $\forall g \in G$.

2. Let us now consider a Lie algebra $\mathfrak{g}$, $H = U(\mathfrak{g})$ its universal enveloping algebra. Then the Lie algebra maps:

$$\mathfrak{g} \longrightarrow k, \quad x \mapsto 0,$$
$$\mathfrak{g} \longrightarrow \mathfrak{g} \times \mathfrak{g}, \quad x \mapsto (x, x),$$
$$\mathfrak{g} \longrightarrow \mathfrak{g}^{op}, \quad x \mapsto -x,$$

together with the universal properties defining H, give rise to algebra maps:

$$\epsilon : H \longrightarrow k,$$
$$\Delta : H \longrightarrow H \otimes H \backsimeq U(\mathfrak{g} \times \mathfrak{g}),$$
$$\mathcal{S} : H \longrightarrow H^{op} \backsimeq U(\mathfrak{g}^{op}).$$

Explicitly

$$\epsilon(x) = 0,$$
$$\Delta(x) = 1 \otimes x + x \otimes 1,$$
$$\mathcal{S}(x) = -x,$$

$x \in \mathfrak{g}$.

If V and W are left H-modules, with corresponding actions $H \longrightarrow \mathrm{End}(V)$ and $H \longrightarrow \mathrm{End}(W)$, then the composition

$$H \xrightarrow{\Delta} H \otimes H \longrightarrow \mathrm{End}(V) \otimes \mathrm{End}(W) \longrightarrow \mathrm{End}(V \otimes W)$$

provides $V \otimes W$ a left H-module structure. This is uniquely determined by the condition

$$x.(v \otimes w) = x.v \otimes w + v \otimes x.w,$$

$x \in \mathfrak{g}$, $v \in V$, $w \in W$.

In an analogous way, but now using the antipode, we may let H act over V^*, via:

$$H \xrightarrow{\mathcal{S}} H^{op} \xrightarrow{\text{transpose}} \mathrm{End}(V^*)$$

This dual action is determined by $(x.\phi)(v) = \phi(-x.v)$, $x \in \mathfrak{g}$, $v \in V$, $\phi \in V^*$.

Finally, we shall consider k as H-module via $\epsilon : H \longrightarrow k$, this is uniquely determined by $x.1 = 0$, for all $x \in \mathfrak{g}$.

We want to consider algebras such that tensor products and duals of modules are again modules, as in the examples above.

First we need the definition of coalgebra. Observe that an associative, unitary k-algebra is a pair (A, m), where A is a k-module and $m : A \otimes A \longrightarrow A$ is a k-linear map, called the *multiplication,* such that:

1. The following diagram is commutative:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{m \otimes \mathrm{id}} & A \otimes A \\ {\scriptstyle \mathrm{id} \otimes m}\downarrow & & \downarrow{\scriptstyle m} \\ A \otimes A & \xrightarrow[m]{} & A \end{array}$$

2. There exists a k-linear map $u : k \longrightarrow A$ such that the following diagrams commute:

$$\begin{array}{ccccc} k \otimes A & \xrightarrow{u \otimes \mathrm{id}} & A \otimes A & \xleftarrow{\mathrm{id} \otimes u} & A \otimes k \\ \downarrow & & \downarrow{\scriptstyle m} & & \downarrow \\ A & = & A & = & A, \end{array}$$

where the maps $k \otimes A \longrightarrow A$ and $A \otimes k \longrightarrow A$ are the canonical ones. Such a u is necessarily unique. The first of these diagrams says that the algebra A is associative and the second gives the existence of a unit $u(1) = 1_A$ in A.

By reversing arrows, we get the dual notion.

Definition. A *coalgebra* over k is a pair (C, Δ), where C is a k-module and $\Delta : C \to C \otimes C$ is a k-linear map called the *comultiplication,* such that:

1. The following diagram commutes:

$$\begin{array}{ccc} C \otimes C \otimes C & \xleftarrow{\Delta \otimes \mathrm{id}} & C \otimes C \\ {\scriptstyle \mathrm{id} \otimes \Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ C \otimes C & \xleftarrow[\Delta]{} & C. \end{array}$$

2. There exists a k-linear map $\epsilon : C \to k$, such that the following diagrams commute:

$$\begin{array}{ccccc} k \otimes C & \xleftarrow{\epsilon \otimes \mathrm{id}} & C \otimes C & \xrightarrow{\mathrm{id} \otimes \epsilon} & C \otimes k \\ \uparrow & & \uparrow{\scriptstyle \Delta} & & \uparrow \\ C & = & C & = & C. \end{array}$$

The map ϵ is called the *counit* and is uniquely determined by the pair (C, Δ).

The kernel of ϵ will be denoted by C^+.

If (C, Δ_C), (D, Δ_D) are coalgebras, a k-linear map: $f : C \to D$ is said a *coalgebra map,* if the following diagrams commute:

$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_D} \\ C \otimes C & \xrightarrow[f \otimes f]{} & D \otimes D, \end{array}$$

$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ {\scriptstyle \epsilon_C}\downarrow & & \downarrow{\scriptstyle \epsilon_D} \\ k & = & k. \end{array}$$

Remark. More generally, one can define algebras and coalgebras in monoidal categories, that is k-linear categories $\mathcal{C}$ provided with a "tensor" functor $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$, plus an associativity constraint (see below). The opposite category $\mathcal{C}^{op}$ of a category $\mathcal{C}$ has the same objects but the arrows are reversed: $\mathrm{Hom}_{\mathcal{C}^{op}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$. In this way, a coalgebra in $\mathcal{C}$ is the same as an algebra in $\mathcal{C}^{op}$.

Examples. 1. If S is any set and $C = kS$ is the free k-module with basis S, then C becomes a coalgebra if we set: $\Delta(s) = s \otimes s$, $\epsilon(s) = 1$, $s \in S$.

2. The universal enveloping algebra of a Lie algebra $\mathfrak{g}$ is a coalgebra with the coproduct Δ and counit ϵ just considered.

Now we dualize the definition of a module over a k-algebra.

Definition. Let C be a coalgebra over k. A *right comodule* over C is a pair (M, Δ_M), where M is a k-module and $\Delta_M : M \longrightarrow M \otimes C$ is a k-linear map (the comodule structure), such that the following diagrams commute:

$$\begin{array}{ccc} M & \xrightarrow{\Delta_M} & M \otimes C \\ {\scriptstyle \Delta_M}\downarrow & & \downarrow{\scriptstyle \Delta_M \otimes id} \\ M \otimes C & \xrightarrow[id \otimes \Delta]{} & M \otimes C \otimes C, \end{array}$$

$$\begin{array}{ccc} M & \xrightarrow{\Delta_M} & M \otimes C \\ \downarrow & & \downarrow{\scriptstyle id \otimes \epsilon} \\ M \otimes k & = & M \otimes k. \end{array}$$

A k-linear map $\phi : M \longrightarrow N$ between right C-comodules M, N, is said a *comodule map* if the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ {\scriptstyle \Delta_M}\downarrow & & \downarrow{\scriptstyle \Delta_N} \\ M \otimes C & \xrightarrow[\phi \otimes id]{} & N \otimes C \end{array}$$

The left C-comodules are defined in a similar fashion. We will denote $\mathcal{M}^C$ and ${}^C\mathcal{M}$, respectively, the categories of right and left C-comodules. Consider a k-module A; it could happen that A has both an algebra and coalgebra structure. In case these structures "paste" well, we give A a special name:

Definition. We say that a triple (A, m, Δ) is a *bialgebra,* if (A, m) is an algebra with unit u, (A, Δ) is a coalgebra with counit ϵ and $\Delta : A \longrightarrow A \otimes A$, $\epsilon : A \longrightarrow k$ are algebra maps. A k-linear map $\phi : A \longrightarrow B$, where A and B are bialgebras is said a *bialgebra map* if it is both an algebra and a coalgebra map.

Remarks.

1. In the definition $A \otimes A$ is considered with the natural algebra structure.

In general the tensor product of two algebras A and B has a natural algebra structure determined by

$$(a \otimes b)(c \otimes d) = ac \otimes bd, \quad \forall a, c \in A, b, d \in B.$$

Equivalently, the multiplication $m_{A \otimes B}$ is the composition

$$A \otimes B \otimes A \otimes B \xrightarrow{\mathrm{id} \otimes \tau \otimes \mathrm{id}} A \otimes A \otimes B \otimes B \xrightarrow{m_A \otimes m_B} A \otimes B.$$

Here τ denotes the "twist" map: $\tau : a \otimes b \mapsto b \otimes a$.

Now, if C and D are coalgebras, then the tensor product $C \otimes D$ can be made into a coalgebra in a natural way, with the comultiplication

$$C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes D \otimes D \xrightarrow{\mathrm{id} \otimes \tau \otimes \mathrm{id}} C \otimes D \otimes C \otimes D.$$

The counit is given by

$$C \otimes D \xrightarrow{\epsilon_C \otimes \epsilon_D} k \otimes k \backsimeq k.$$

One can then check that in the definition of bialgebra the condition of Δ and ϵ being algebra maps may be replaced by the (equivalent) condition of m and u being coalgebra maps.

2. The kernel of the counit ϵ in a bialgebra A is a two sided ideal of codimension 1, called the *augmentation ideal.*

Examples of bialgebras are kG, the group algebra of a group G, with the algebra and coalgebra structures considered at the beginning (notice that we do not make use here of the existence of inverses for elements of G), and the universal enveloping algebra of a Lie algebra $\mathfrak{g}$, where Δ and ϵ are as treated earlier. In particular, any symmetric algebra has a bialgebra structure. The next definition will allow us to give a characterization of a bialgebra in terms of its left modules when considered as an algebra.

Definition. A triple $(\mathcal{C}, \otimes, I)$, where $\mathcal{C}$ is a category, $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor called *formal tensor product,* and I is an object of $\mathcal{C}$ called *unit object,* is said a *monoidal category* if for any objects U, V, W of $\mathcal{C}$ there exists natural isomorphisms between functors from $\mathcal{C} \times \mathcal{C} \times \mathcal{C}$ to $\mathcal{C}$ (respectively $\mathcal{C}$ to $\mathcal{C}$)

$$a_{U,V,W} : (U \otimes V) \otimes W \to U \otimes (V \otimes W),$$

$$r_V : V \otimes I \to V, \quad l_V : I \otimes V \to V,$$

such that the following diagrams are commutative:

$$\begin{array}{ccc}
(U \otimes V) \otimes (W \otimes X) & = & (U \otimes V) \otimes (W \otimes X) \\
{\scriptstyle a_{U\otimes V,W,X}}\uparrow & & \downarrow{\scriptstyle a_{U,V,W\otimes X}} \\
((U \otimes V) \otimes W) \otimes X & & U \otimes (V \otimes (W \otimes X)) \\
{\scriptstyle a_{U,V,W}\otimes \mathrm{id}}\downarrow & & \uparrow{\scriptstyle \mathrm{id} \otimes a_{V,W,X}} \\
(U \otimes (V \otimes W)) \otimes X & \xrightarrow[a_{U,V\otimes W,X}]{} & U \otimes ((V \otimes W) \otimes X),
\end{array}$$

$$\begin{array}{ccc}
(V \otimes I) \otimes W & \xrightarrow{a_{V,I,W}} & V \otimes (I \otimes W) \\
{\scriptstyle r_V \otimes \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \mathrm{id} \otimes l_W} \\
V \otimes W & = & V \otimes W.
\end{array}$$

A first example of a monoidal category is the category of left k-modules ${}_k\mathcal{M}$, with the tensor product over k and unit object $I = k$. The associativity and unit constraints are just the usual isomorphisms of k-modules:

$$a_{U,V,W}((u \otimes v) \otimes w) = u \otimes (v \otimes w),$$
$$l_V(1 \otimes v) = v,$$
$$r_V(v \otimes 1) = v.$$

Remark. In any monoidal category one can define algebras and coalgebras, and their modules and comodules. However, to define bialgebras one needs in addition a commutativity constraint, or *braiding*

$$c_{U,V} : U \otimes V \to V \otimes U.$$

This leads to the important notion of bialgebras in braided categories. In these notes, we shall only consider the traditional braided category of k-modules, where the braiding is the usual twist map.

Other examples of monoidal categories are the categories of left modules over the algebras kG and $U(\mathfrak{g})$. In both cases this structure is inherited from that of ${}_k\mathcal{M}$. The next proposition gives a characterization of the k-algebras with this property.

Proposition 1.1. *Let (A, m) be a k-algebra and let $\Delta : A \to A \otimes A$, $\epsilon : A \to k$ be given algebra maps. We consider $k \in {}_A\mathcal{M}$ via ϵ. Let $\otimes : {}_A\mathcal{M} \times {}_A\mathcal{M} \to {}_A\mathcal{M}$ be the functor which associates to each pair of A-modules M, N their tensor product over k, $M \otimes N$, with the A-action:*

$$A \xrightarrow{\Delta} A \otimes A \to \mathrm{End}(M) \otimes \mathrm{End}(N) \to \mathrm{End}(M \otimes N).$$

Then $({}_A\mathcal{M}, \otimes, k)$ is a monoidal category, with canonical associativity and unit constraints, if and only if (A, m, Δ) is a bialgebra (with counit ϵ).

Proof.

Suppose (A, m, Δ) is a bialgebra. The coassociativity of Δ implies that $\forall U, V, W \in {}_A\mathcal{M}$ the canonical isomorphisms of k-modules

$$(U \otimes V) \otimes W \backsimeq U \otimes (V \otimes W),$$

are isomorphisms of A-modules. Moreover, the commutativity of the diagrams

$$\begin{array}{ccccc} A \otimes k & \xleftarrow{\mathrm{id} \otimes \epsilon} & A \otimes A & \xrightarrow{\epsilon \otimes \mathrm{id}} & k \otimes A \\ \downarrow & & \uparrow{\scriptstyle \Delta} & & \downarrow \\ A & = & A & = & A, \end{array}$$

imply, respectively, that the left and right unit constraints

$$V \otimes k \xrightarrow[v \otimes 1 \mapsto v]{} V, \quad \text{and} \quad k \otimes V \xrightarrow[1 \otimes v \mapsto v]{} V,$$

are isomorphisms of A-modules. So $({}_A\mathcal{M}, \otimes, k)$ is a monoidal category.

Conversely, suppose that $({}_A\mathcal{M}, \otimes, k)$ is a monoidal category. For the coassociativity of Δ use the fact that

$$(A \otimes A) \otimes A \xrightarrow[(x\otimes y)\otimes z \mapsto x\otimes(y\otimes z)]{} A \otimes (A \otimes A),$$

is an isomorphism of A-modules.

Also, the canonical maps

$$k \otimes A \to A, \quad A \otimes k \to A,$$

are A-isomorphisms, which implies that ϵ is the counit. $\square$

Now we are in a position to define the objects which will concern us in the sequel.

Definition. We say that a bialgebra (H, m, Δ) is a *Hopf algebra* if there exists a k-linear map $\mathcal{S} : H \to H$, called the *antipode,* such that the following diagrams are commutative:

$$\begin{array}{ccccc} H\otimes H & \xleftarrow{\Delta} & H & \xrightarrow{\Delta} & H\otimes H \\ {\scriptstyle \mathrm{id}\otimes\mathcal{S}}\downarrow & & {\scriptstyle u\epsilon}\downarrow & & \downarrow{\scriptstyle \mathcal{S}\otimes\mathrm{id}} \\ H\otimes H & \xrightarrow[m]{} & H & \xleftarrow[m]{} & H\otimes H \end{array}$$

Examples. 1. If G is a group, the group algebra kG is a Hopf algebra, with antipode given by $\mathcal{S}(g) = g^{-1}$, $g \in G$.

2. The universal enveloping algebra $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ is a Hopf algebra, with antipode $\mathcal{S}(x) = -x$, $x \in \mathfrak{g}$. In particular any symmetric algebra over k is a Hopf algebra.

3. Let V be a k-module, then the tensor algebra $T(V)$ over V is a Hopf algebra with the usual algebra structure and where $\Delta(v) = 1 \otimes v + v \otimes 1$, $\epsilon(v) = 0$, $\mathcal{S}(v) = -v$, $v \in V$.

If k is a field, this example is but a particular case of the previous one, we see this as follows:

Tensor algebras and free Lie algebras.

Let k be a field. A Lie algebra $\mathfrak{g}$ over k is said to be *free* on a set X if

a) X generates $\mathfrak{g}$ as a Lie algebra.

b) Given a Lie algebra $\mathfrak{m}$ over k, and a map $\phi : X \to \mathfrak{m}$, there exists a (unique) Lie algebra morphism $\psi : \mathfrak{g} \to \mathfrak{m}$ that extends ϕ.

It is not difficult to see that given a set X, if such an algebra exists, it is unique (up to isomorphism). As to its existence, consider the k-space V with basis X. Let $T(V)$ be the tensor algebra over V, and call $\mathfrak{g}$ the Lie subalgebra of $T(V)$ (with the bracket $[a, b] = ab - ba$) generated by V.

It is clear that X generates $\mathfrak{g}$. If $\phi : X \to \mathfrak{m}$ is any map, we can extend it to a k-linear map $\phi_1 : V \to \mathfrak{m} \subseteq U(\mathfrak{m})$ (observe that here we are making use of the PBW theorem, which use is legitimate under the assumption that k is a field). By the universal property of $T(V)$, ϕ_1 has a unique extension to an algebra map $T(V) \to U(\mathfrak{m})$. Call ψ the restriction of this map to $\mathfrak{g}$, then ψ extends ϕ and is clearly a Lie algebra map.

We assert that the universal enveloping algebra of a free Lie algebra $\mathfrak{g}$ on X is isomorphic to the tensor algebra over the k-vector space with basis X.

To see this, let $\mathcal{A}$ be an associative algebra over k and let $\omega : \mathfrak{g} \longrightarrow \mathcal{A}$ be a Lie algebra map. Then, by the universal property of $T(V)$, there exists a unique algebra map $\Omega : T(V) \longrightarrow \mathcal{A}$ such that $\Omega(x) = \omega(x), \forall x \in X$, but this is equivalent to saying (as X generates $\mathfrak{g}$) that $\Omega(x) = \omega(x), \forall x \in \mathfrak{g}$.

So $T(V) \backsimeq U(\mathfrak{g})$. Moreover, the Hopf algebra structures in $T(V)$ when considered as a tensor algebra and as an enveloping algebra are the same.

4. The following example is due to Taft (1971):

Let k be a field, and N a natural number. Assume that there exists a primitive N-th root of unity ξ in k. Consider the algebra H generated over k by two elements g and x subject to the relations: $g^N = 1$, $x^N = 0$, $xg = \xi gx$. We claim that there are algebra maps $\Delta : H \longrightarrow H \otimes H$, $\mathcal{S} : H \longrightarrow H^{op}$, $\epsilon : H \longrightarrow k$ uniquely determined by

$$\Delta(g) = g \otimes g, \quad \Delta(x) = 1 \otimes x + x \otimes g$$
$$\epsilon(x) = 0, \quad \epsilon(g) = 1$$
$$\mathcal{S}(g) = g^{-1}, \quad \mathcal{S}(x) = -xg^{-1}$$

We work out the details for Δ and let $\mathcal{S}$, ϵ to the reader. Clearly $\Delta(g)^N = 1$ and $\Delta(x)$, $\Delta(g)$ ξ-commute, i.e., $\Delta(x)\Delta(g) = \xi\Delta(g)\Delta(x)$. For the remaining relation we need the next lemma.

In the polynomial algebra $\mathbb{Z}[\mathbf{q}]$, we consider the $\mathbf{q}$-binomial coefficients

$$\binom{n}{i}_{\mathbf{q}} = \frac{(n)!_{\mathbf{q}}}{(n-i)!_{\mathbf{q}}(i)!_{\mathbf{q}}}, \quad \text{where } (n)!_{\mathbf{q}} = (n)_{\mathbf{q}} \dots (2)_{\mathbf{q}}(1)_{\mathbf{q}}, \quad \text{and } (n)_{\mathbf{q}} = 1 + \mathbf{q} + \cdots + \mathbf{q}^{n-1},$$

for $n \in \mathbb{N}$, $0 \leq i \leq n$.

One proves that $\binom{n}{i}_{\mathbf{q}} \in \mathbb{Z}[\mathbf{q}]$ by induction on n, using the identity

$$(*) \qquad \mathbf{q}^k \binom{n}{k}_{\mathbf{q}} + \binom{n}{k-1}_{\mathbf{q}} = \binom{n+1}{k}_{\mathbf{q}},$$

for $1 \leq k \leq n$.

Now, if A is an associative algebra over k and $q \in k$, then $\binom{n}{i}_q$ denotes the specialization of $\binom{n}{i}_{\mathbf{q}}$ at q.

Lemma (Quantum binomial formula). *Let A be an associative algebra over k, $q \in k$. If $x, y \in A$ are two elements that q-commute, i.e. $xy = qyx$, then the following formula holds for every $n \in \mathbb{N}$:*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i}_q y^i x^{n-i}.$$

Proof. By induction on n, again using the identity (*).

Now, if ξ is a primitive N-th root of unity, it follows from the definitions that $\binom{N}{i}_\xi = 0$ for $0 < i < N$. Then, as $1 \otimes x$ and $x \otimes g$ ξ-commute, we have:

$$\Delta(x)^N = (1 \otimes x + x \otimes g)^N = \sum_{i=0}^{N} \binom{N}{i}_\xi (x \otimes g)^i (1 \otimes x)^{N-i} =$$
$$(x \otimes g)^N + (1 \otimes x)^N = x^N \otimes g^N + 1 \otimes x^N = 0.$$

So Δ is a well defined algebra map $\Delta : H \to H \otimes H$.

Thus H is a Hopf algebra (of finite dimension N^2, with basis $g^i x^j$, $0 \leq i, j \leq N-1$).

Definition. Let H be a Hopf algebra and τ denote the twist map in $H \otimes H$. We say H is *cocommutative* if $\tau \circ \Delta = \Delta$.

For instance, the algebras introduced in examples 1 and 2 are cocommutative, while the Taft algebras are not in general. If G is a finite group, then the group algebra kG is a finite dimensional cocommutative Hopf algebra (it is commutative iff G is abelian). When k is an algebraically closed field of characteristic 0, then it can be shown that these are the only possible ones, that is: every finite dimensional Hopf algebra over k which is cocommutative is isomorphic to a group algebra kG, for some finite group G. The next example shows this is not true when the characteristic of k is positive.

The u-algebra of a restricted Lie algebra. Let k be a field of characteristic $p > 0$. A Lie algebra $\mathcal{L}$ over k is called a restricted Lie algebra if there is a map $\mathcal{L} \to \mathcal{L}$, denoted $a \mapsto a^{[p]}$, $a \in \mathcal{L}$, such that

$$(\alpha a)^{[p]} = \alpha^p a^{[p]},$$
$$\mathrm{ad}(b^{[p]}) = (\mathrm{ad}\, b)^p,$$
$$(a+b)^{[p]} = a^{[p]} + b^{[p]} + \sum_{i=1}^{p-1} s_i(a,b)$$

for $a, b \in \mathcal{L}$, $\alpha \in k$, where ad denotes the adjoint representation of $\mathcal{L}$ on itself and $is_i(a,b)$ is the coefficient of λ^{i-1} in the expansion of $\mathrm{ad}(\lambda a + b)^{p-1}(a)$.

A k-linear map $f : \mathcal{L} \to \mathcal{A}$ between restricted Lie algebras $\mathcal{L}$ and $\mathcal{A}$ is a *morphism of restricted Lie algebras* if it is a morphism of Lie algebras and $f(a^{[p]}) = f(a)^{[p]}$, $\forall a \in \mathcal{L}$.

For instance, if $\mathcal{A}$ is an associative k-algebra, we think of $\mathcal{A}$ as a Lie algebra by means of the natural bracket: $[a,b] = ab - ba$, $a, b \in \mathcal{A}$. Then the map $a \mapsto a^p$, $a \in \mathcal{A}$, makes $\mathcal{A}$ into a restricted Lie algebra.

Let now $\mathcal{L}$ be a restricted Lie algebra, U its universal enveloping algebra, and $\mathcal{B}$ the ideal in U generated by all the elements $a^p - a^{[p]}$, $a \in \mathcal{L}$. Denote by $\mathcal{U}$ the quotient algebra

$\mathcal{U} = U/\mathcal{B}$. Then, the natural map $\phi : \mathcal{L} \to \mathcal{U}$ is a morphism of restricted Lie algebras. The pair $(\phi,\mathcal{U})$ is universal for $\mathcal{L}$ in the following sense: if $\mathcal{A}$ is an associative algebra and $f : \mathcal{L} \to \mathcal{A}$ is a morphism of restricted Lie algebras, then there exists a unique algebra map $F : \mathcal{U} \to \mathcal{A}$, such that $f = F \circ \phi$.

$\mathcal{U}$ is called the u-algebra of $\mathcal{L}$. By the universal property of $\mathcal{U}$, we have that the (restricted) morphisms

$$\begin{aligned} \mathcal{L} &\to k, \quad a \mapsto 0, \\ \mathcal{L} &\to \mathcal{L} \times \mathcal{L}, \quad a \mapsto (a, a), \\ \mathcal{L} &\to \mathcal{L}^{op}, \quad a \mapsto -a, \end{aligned}$$

define algebra maps:

$$\begin{aligned} \Delta &: \mathcal{U} \to \mathcal{U} \otimes \mathcal{U}, \\ \epsilon &: \mathcal{U} \to k, \\ \mathcal{S} &: \mathcal{U} \to \mathcal{U}^{op}, \end{aligned}$$

uniquely determined by

$$\begin{aligned} \Delta(a) &= 1 \otimes a + a \otimes 1, \\ \epsilon(a) &= 0, \\ \mathcal{S}(a) &= -a, \end{aligned}$$

$a \in \mathcal{L}$, which make it into a cocommutative Hopf algebra.

The next theorem is analogous to the PBW theorem for Lie algebras:

Theorem 1.2. *Let $\mathcal{L}$ be a restricted Lie algebra and let $\mathcal{U}$ its u-algebra.Then:*

1. *The map $\phi : \mathcal{L} \to \mathcal{U}$ is an injective morphism of restricted Lie algebras.*
2. *If $\{u_i\}_{i\in I}$ is an ordered basis for $\mathcal{L}$, then the set of monomials:*

$$u_{i_1}^{k_1} u_{i_2}^{k_2} \dots u_{i_r}^{k_r} : \quad i_1 \le i_2 \le \dots \le i_r, \quad 0 \le k_j \le p-1.$$

is a basis for $\mathcal{U}$.

Proof. See [2, Th.12, p. 191].

As a consequence, if $\mathcal{L}$ has finite dimension n, then $\mathcal{U}$ is also finite dimensional, with $\dim \mathcal{U} = p^n$.Then, $\mathcal{U}$ is a finite dimensional cocommutative Hopf algebra and it is *not* isomorphic to any group algebra. To see this we first introduce some terminology:

Definition. Let H be a Hopf algebra. $h \in H$ is said a *group-like* element if $h \neq 0$ and $\Delta(h) = h \otimes h$, and it is said a *primitive* element if $\Delta(h) = 1 \otimes h + h \otimes 1$.

The sets of group-like and primitive elements of H are denoted respectively $G(H)$ and $P(H)$.

If $h \in G(H)$, then $\epsilon(h) = 1$; similarly, if $h \in P(H)$, then $\epsilon(h) = 0$.

$G(H)$ is a subgroup of the group of units of H, and $P(H)$ is a Lie subalgebra of H with the bracket $[a, b] = ab - ba$.

Observation. If k is a field, distinct group-like elements are linearly independent, so if G is a group, then the set of group-like elements in kG is precisely G.

Lemma 1.3. *Let k be a field. If H is a Hopf algebra over k which is generated (as an algebra) by primitive elements, then the set of group-like elements of H is trivial.*

Proof. Let $\{x_i\}_{i\in I}$ denote the family of nonzero primitive elements of H and for each $n \geq 0$, let A_n be the linear span in H of elements of the form ${x_{i_1}}^{k_1} \dots {x_{i_m}}^{k_m}$, such that k_j are nonnegative integers with $k_1 + \cdots + k_m = n$.

Then the collection $\{A_n\}_{n\geq 0}$ satisfies the next two properties:

1. $A_n \subseteqq A_{n+1}$, $\bigcup_{n\geq 0} A_n = H$.
2. $\Delta(A_n) \subseteqq \sum_{i=0}^{n} A_i \otimes A_{n-i}$.

Now, if $g \in G(H)$, because of property 1, there exists m such that $g \in A_n$, so we can choose m to be minimal with this property. Suppose $g \notin k = A_0$, then there exists $f \in H^*$ such that $f(A_0) = 0$ but $f(g) = 1$.

As $g \in A_m$, we may write

$$\Delta(g) = \sum_{i=0}^{m} a_i \otimes a_{m-i},$$

with $a_j \in A_j$, and this implies that

$$g =< \mathrm{id} \otimes f, \Delta(g) >= \sum_{i=0}^{m-1} a_i f(a_{m-i}) \in A_{m-1}.$$

But this contradicts the minimality of m. Thus $g \in k$, and so $g = 1$ as asserted. □

Lemma (1.3), together with the previous observation, show that the u-algebra of a restricted nontrivial Lie algebra cannot be isomorphic to a group algebra kG.

Sigma Notation.

We introduce the notation, due to Sweedler, that will be used from now on.

If C is a coalgebra, $c \in C$, then $\Delta(c)$, as an element of $C \otimes C$ has a representation of the form

$$\Delta(c) = \sum_i c_i \otimes c^i,$$

where c_i, c^i are elements of C. We indicate such an expression in the abbreviated form

$$\Delta(c) = \sum c_{(1)} \otimes c_{(2)}.$$

Some authors use instead $\Delta(c) = \sum c_1 \otimes c_2$. In what follows we shall omit the sumation symbol, for the sake of brevity. So that,

$$\Delta(c) = c_{(1)} \otimes c_{(2)}.$$

If V is a right comodule for C with comodule structure map Δ_V, then we write for $v \in V$

$$\Delta_V(v) = \sum v_{(0)} \otimes v_{(1)},$$

where $v_{(0)}$ represents elements of V, and $v_{(1)}$ is understood to be in C. Again, we shall omit the sumation symbol.

For instance, if C is a coalgebra, the coassociativity of Δ reads, in sigma notation

$$(c_{(1)})_{(1)} \otimes (c_{(1)})_{(2)} \otimes c_{(2)} = c_{(1)} \otimes (c_{(2)})_{(1)} \otimes (c_{(2)})_{(2)},$$

$\forall c \in C$, so we may indicate $\Delta_2(c) := (\Delta \otimes \mathrm{id}) \circ \Delta(c) = (\mathrm{id} \otimes \Delta) \circ \Delta(c)$ in the form

$$\Delta_2(c) = c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$

Defining inductively $\Delta_1 = \Delta$, $\Delta_{n+1} : C \to C^{\otimes(n+2)}$, $\Delta_{n+1} = (\Delta \otimes \mathrm{id}^n) \circ \Delta_{n-1}$, $n \geq 2$, we see there is no ambiguity in writting

$$\Delta_n(c) = c_{(1)} \otimes \cdots \otimes c_{(n+1)}.$$

In this vein, the composition $f \circ \Delta_n$ can be expressed as

$$f \circ \Delta_n(c) = f(c_{(1)}, ..., c_{(n)}).$$

For instance, the conditions on ϵ take the form

$$\epsilon(c_{(1)})c_{(2)} = c = c_{(1)}\epsilon(c_{(2)}).$$

Also, if H is a Hopf algebra with antipode $\mathcal{S}$, then we must have, $\forall h \in H$

$$\mathcal{S}(h_{(1)})h_{(2)} = \epsilon(h)1 = h_{(1)}\mathcal{S}(h_{(2)}).$$

Convolution Product.

Definition. Let (C, Δ) be a coalgebra, (A, m) an algebra. For $f, g \in \mathrm{Hom}(C, A)$ we define the *convolution product* of f and g to be the element of $\mathrm{Hom}(C, A)$, denoted $f * g$, which results from the composition

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

In sigma notation we have, for $c \in C$, $(f * g)(c) = f(c_{(1)})g(c_{(2)})$.

In the next example, following Wigner [20], it is shown that the convolution product allows to give simpler proofs of some old results on free Lie algebras (cf. [2, V.4]).

Example. Let V be a k-module and consider the Hopf algebra structure in the tensor algebra $T(V)$ indicated earlier. Let $\phi : T(V) \to T(V)$ the k-linear map defined by:

$$\begin{aligned} \phi(1) &= 0, \\ \phi(v) &= v, \\ \phi(v_1 v_2 \dots v_n) &= [v_1[v_2[\dots v_n] \dots]] = \mathrm{ad}(v_1)(\phi(v_2 \dots v_n)). \end{aligned}$$

for $v, v_1, \dots, v_n \in V$, $n \geq 2$. Call $\mathfrak{g}$ the Lie subalgebra of $T(V)$ generated by V. Then:

a) $\forall x \in T_n(V)$, $\phi * \mathrm{id}(x) = nx$.

b) (Theorem of Dynkin, Specht and Wever). Suppose $\mathrm{char}\, k = 0$. If $x \in T_n(V)$, the following statements are equivalent:

(i) $x \in \mathfrak{g}$.
(ii) $\Delta(x) = 1 \otimes x + x \otimes 1$.
(iii) $\phi(x) = nx$.

Then in particular, if k is a field of characteristic 0, and $\mathfrak{g}$ is a free Lie algebra over k, the Lie algebra of primitive elements in $U(\mathfrak{g})$ is precisely $\mathfrak{g}$. (We remark this still remains true if $\mathfrak{g}$ is not free).

Proof.
a) By induction on n. The statement is trivially true if $n = 0, 1$. Let $n \geq 2$.
Assume $x = vy$, with $y \in T_{n-1}(V)$, $v \in V$. Write

$$\Delta(y) = 1 \otimes y + \sum_i y_i \otimes z_i,$$

where $y_i \in T^+(V)$. In particular $\forall v \in V$,

$$\phi(vy_i) = v\phi(y_i) - \phi(y_i)v.$$

We have

$$\phi * \mathrm{id}(y) = \sum_i \phi(y_i) z_i,$$

and so, as $\Delta(v) = v \otimes 1 + 1 \otimes v$,

$$\phi * \mathrm{id}(x) = \phi * \mathrm{id}(vy) = \phi(v_{(1)}y_{(1)})v_{(2)}y_{(2)} = \phi(y_{(1)})vy_{(2)} + \phi(vy_{(1)})y_{(2)} =$$
$$\phi(1)vy + \sum_i \phi(y_i)vz_i + \phi(v)y + \sum_i \phi(vy_i)z_i =$$
$$vy + v(\phi * \mathrm{id})(y) = vy + (n-1)vy = nx.$$

b) (i) $\Rightarrow$ (ii). Follows from the observation that the set of primitive elements of a Hopf algebra is a Lie subalgebra.
(ii) $\Rightarrow$ (iii). By a) we can write $\phi * \mathrm{id}(x) = nx$, but by (ii) this equals $\phi(1)x + \phi(x)1 = \phi(x)$.
(iii) $\Rightarrow$ (i). Because $\phi(x) = nx \in \mathfrak{g}$ and $\mathrm{char}\, k = 0$.

Properties of the convolution product.

Proposition 1.4. *Let C be a coalgebra with counit ϵ, and let A be an algebra with unit u. Then $(\mathrm{Hom}(C, A), *)$ is an algebra with unit $u\epsilon$.*

Proof. It is easy to see that $*$ defines an associative multiplication in $\mathrm{Hom}(C, A)$. We show that $u\epsilon$ is the unit. Let $f \in \mathrm{Hom}(C, A)$, then $\forall c \in C$,

$$(f * u\epsilon)(c) = f(c_{(1)})\epsilon(c_{(2)})1_A = f(c_{(1)}\epsilon(c_{(2)})) = f(c).$$

Similarly $u\epsilon * f = f$. $\square$

If B is a bialgebra then by proposition (1.4), the convolution product makes $\mathrm{Hom}(B,B)$ into an algebra. In the case of Hopf algebras there is a very close relation between this algebra structure and the antipode.

Recall that if (A,m_A), (B,m_B) are algebras, a map $f:A\longrightarrow B$ is an *antialgebra map* if $(f\circ m_A)=m_B{}^{op}\circ(f\otimes f)$ and $f\circ u_A=u_B$. That is, $f(xy)=f(y)f(x)$, $\forall x,y\in A$ and $f(1)=1$.

If (C,Δ_C), (D,Δ_D) are coalgebras we say that a map $g:C\longrightarrow D$ is an *anticoalgebra map* if $\Delta_D\circ g=(g\otimes g)\circ\Delta_C{}^{cop}$ and $\epsilon_D\circ g=\epsilon_C$. In sigma notation, the first condition reads

$$g(c)_{(1)}\otimes g(c)_{(2)}=g(c_{(2)})\otimes g(c_{(1)}),\quad \forall c\in C.$$

Theorem 1.5. *Let H be a Hopf algebra. Then the antipode $\mathcal{S}$ is the inverse of the identity map* $\mathrm{id}:H\longrightarrow H$ *with respect to the convolution product in* $\mathrm{Hom}(H,H)$. *In particular it is unique. We have also:*

a) $\mathcal{S}$ is an antialgebra map.

b) $\mathcal{S}$ is an anticoalgebra map.

c) The following statements are equivalent:

i) $\mathcal{S}^2=\mathrm{id}$.

ii) $x_{(2)}\mathcal{S}(x_{(1)})=\epsilon(x)1,\forall x\in H$.

iii) $\mathcal{S}(x_{(1)})x_{(2)}=\epsilon(x)1,\forall x\in H$.

In particular, if H is commutative or cocommutative then $\mathcal{S}^2=\mathrm{id}$.

d) Let H, K are Hopf algebras (with antipodes denoted respectively by $\mathcal{S}_H$ and $\mathcal{S}_K$). If $\phi:H\longrightarrow K$ is a bialgebra map, then ϕ is a Hopf algebra map, i.e. $\phi\mathcal{S}_H=\mathcal{S}_K\phi$.

Proof. The first assertion follows immediately from the definition of the antipode.

To prove a), consider the algebra structure in $\mathrm{Hom}(H\otimes H,H)$, given by the convolution product. Call $m:H\otimes H\longrightarrow H$ the multiplication in H. We claim that

$$\mathcal{S}\circ m=m^{-1}=m^{op}\circ(\mathcal{S}\otimes\mathcal{S}).$$

Here m^{-1} is the inverse of m with respect to the convolution product. To see this, let $x,y\in H$, then

$$((\mathcal{S}\circ m)*m)(x\otimes y)=\mathcal{S}\circ m(x_{(1)}\otimes y_{(1)})m(x_{(2)}\otimes y_{(2)})=$$
$$\mathcal{S}(x_{(1)}y_{(1)})x_{(2)}y_{(2)}=\epsilon(x)\epsilon(y)1_H=\epsilon(x\otimes y)1_H.$$

Also

$$((m^{op}\circ(\mathcal{S}\otimes\mathcal{S}))*m)(x\otimes y)=\mathcal{S}(y_{(1)})\mathcal{S}(x_{(1)})x_{(2)}y_{(2)}=\epsilon(x)\epsilon(y)1_H=\epsilon(x\otimes y)1_H.$$

In a similar way $m*(\mathcal{S}\circ m)=m*(m^{op}\circ(\mathcal{S}\otimes\mathcal{S}))=u\epsilon$.

By the uniqueness of the inverse, we obtain the desired identity.

We have also

$$\mathcal{S}(1)=\mathcal{S}*\mathrm{id}(1)=1.$$

For b) use the identity $\Delta \circ \mathcal{S} = \Delta^{-1} = (\mathcal{S} \otimes \mathcal{S}) \circ \Delta^{cop}$ in $\mathrm{Hom}(H, H \otimes H)$.

If $x \in H$, applying ϵ to the equality

$$\epsilon(x)1 = \mathcal{S}(x_{(1)})x_{(2)},$$

we get

$$\epsilon(x) = \epsilon(\mathcal{S}(x_{(1)}\epsilon(x_{(2)})) = \epsilon \circ \mathcal{S}(x).$$

c) i) $\Rightarrow$ ii). Suppose $\mathcal{S}^2 = \mathrm{id}$. If $x \in H$, using the fact that $\mathcal{S}$ is an antialgebra map, one gets

$$x_{(2)}\mathcal{S}(x_{(1)}) = \mathcal{S}^2(x_{(2)})\mathcal{S}(x_{(1)}) = \mathcal{S}(x_{(1)}\mathcal{S}(x_{(2)})) = \mathcal{S}(\epsilon(x)1) = \epsilon(x)1.$$

ii) $\Rightarrow$ i). Let $x \in H$, then

$$\mathcal{S}^2 * \mathcal{S}(x) = \mathcal{S}^2(x_{(1)})\mathcal{S}(x_{(2)}) = \mathcal{S}(x_{(2)}\mathcal{S}(x_{(1)})) = \mathcal{S}(\epsilon(x)1) = \epsilon(x)1.$$

This shows that $\mathcal{S}^2 * \mathcal{S} = u\epsilon$. Multiplying by id on the right, we obtain i).

Thus we saw that i) $\Leftrightarrow$ ii). Similarly i) $\Leftrightarrow$ iii), which finishes the prove of c).

d) To see this, use the identities

$$\phi\mathcal{S}_H = \phi^{-1} = \mathcal{S}_K\phi$$

which hold in $\mathrm{Hom}(H, K)$. $\square$

Remark. Let H be a Hopf algebra. We saw that the antipode $\mathcal{S}$ is an antialgebra map, and so it is an algebra map $H \longrightarrow H^{op}$. Let V be a left H-module. Then the dual k-module V^* results a right H-module and we can make it into a left H-module, by composing

$$H \xrightarrow{\mathcal{S}} H^{op} \longrightarrow \mathrm{End}(V^*).$$

That is,

$$h.\alpha(v) = \alpha(\mathcal{S}(h).v), \quad \forall h \in H, \alpha \in V^*, v \in V.$$

We have, moreover, that the evaluation map $V^* \otimes V \longrightarrow V$ is in this way a map of left H-modules (where $V^* \otimes V$ is considered as an H-module via Δ).

The following is a geometric approach to Hopf algebras. For more details see reference [4].

Hopf algebras and affine schemes.

In what follows $\mathcal{A}_k$ will denote the category of commutative k-algebras. We indicate by $\mathfrak{S}$, $\mathfrak{G}$, respectively, the categories of sets and groups.

For each $R \in \mathcal{A}_k$, consider the functor $\mathrm{Alg}(R, \_) : \mathcal{A}_k \longrightarrow \mathfrak{S}$, which associates to each commutative k-algebra A the set $\mathrm{Alg}(R, A)$, of all algebra maps from R to A, and to each morphism $\phi : A \longrightarrow B$, the map $\mathrm{Alg}(R, \phi) : \mathrm{Alg}(R, A) \longrightarrow \mathrm{Alg}(R, B)$, given by $\mathrm{Alg}(R, \phi)(f) = \phi \circ f$.

We denote this functor by $\mathrm{Sp}\, R$ and call it the *spectrum* of R.

For instance, if $R = k[T_1, \ldots, T_n]$, the polynomial algebra in n variables over k, then $\operatorname{Sp} R \backsimeq \operatorname{Af}_n$, where Af_n is the functor *affine n-space* :

$$\operatorname{Af}_n(A) = A^n, \quad \operatorname{Af}_n(\phi) = \phi^n : A^n \longrightarrow B^n,$$

for $A, B \in \mathcal{A}_k$, $\phi : A \longrightarrow B$.

Definitions.

We say a functor $X : \mathcal{A}_k \longrightarrow \mathfrak{S}$ is an *affine scheme* over k if it is representable, i.e., if there exists a natural isomorphism $X \backsimeq \operatorname{Sp} R$ for some $R \in \mathcal{A}_k$.

A *group scheme* is a functor $G : \mathcal{A}_k \longrightarrow \mathfrak{G}$ which, when composed with the forgetful functor $\mathfrak{G} \longrightarrow \mathfrak{S}$, is an affine scheme over k.

In dealing with Hopf algebras, we have the next

Proposition 1.6. *If H is a Hopf algebra, and A a commutative algebra, then* $\operatorname{Alg}(H, A)$ *is a subgroup of the group of units of* $\operatorname{Hom}(H, A)$.

Proof. It is clear that the unit $u\epsilon$ is an algebra map $H \longrightarrow A$.

Let $f, g \in \operatorname{Alg}(H, A)$. Then for $x, y \in H$,

$$(f * g)(xy) = f(x_{(1)}y_{(1)})g(x_{(2)}y_{(2)}) = \\ f(x_{(1)})g(x_{(2)})f(y_{(1)})g(y_{(2)}) = (f * g)(x)(f * g)(y).$$

So $f * g \in \operatorname{Alg}(H, A)$.

If $\mathcal{S}$ is the antipode in H, we claim that for $f \in \operatorname{Alg}(H, A)$, $f^{-1} = f \circ \mathcal{S}$. Note that because $\mathcal{S}$ is an antialgebra map and A is commutative, $f \circ \mathcal{S} \in \operatorname{Alg}(H, A)$. Now, if $x \in H$, we have

$$(f * f \circ \mathcal{S})(x) = f(x_{(1)})f(\mathcal{S}(x_{(2)})) = f(x_{(1)}\mathcal{S}(x_{(2)})) = f(\epsilon(x)1_H) = \epsilon(x)1_A.$$

Similarly, $f \circ \mathcal{S} * f = u\epsilon$. So the assertion is proved. □

Corollary 1.7. *If H is a commutative Hopf algebra, then its spectrum* $\operatorname{Sp} H$ *is an affine group scheme.* □

We have moreover, that if R, S are commutative algebras, and $\phi : R \longrightarrow S$ is an algebra map, then ϕ induces functorially a natural transformation

$$\phi^* : \operatorname{Sp} S \longrightarrow \operatorname{Sp} R,$$

in the form $\phi^*(\xi) = \xi \circ \phi$.

This observation, together with corollary (1.7), give us a (contravariant) functor from the category of commutative Hopf algebras into the category of affine group schemes.

In fact this functor is an antiequivalence of categories. We go now to this point.

If $X : \mathcal{A}_k \to \mathfrak{S}$ is any functor, the set of all natural transformations $X \to \mathrm{Af}_1$ can be given a k-algebra structure by setting

$$(f+g)_A(x) = f_A(x) + g_A(x),$$

for $A \in \mathcal{A}_k$, and $x \in X(A)$, defining in analogous way fg and λf, for $\lambda \in k$.

We denote this algebra by $k[X]$.

Observation. The universal property of the tensor product implies that a direct product $X \times Y$ of affine schemes is again an affine scheme with $k[X \times Y] = k[X] \otimes k[Y]$.

If $X, Y : \mathcal{A}_k \to \mathfrak{S}$ are functors and $f : X \to Y$ is a natural transformation, then f induces functorially a k-algebra map $f^* : k[X] \to k[Y]$, by $f^*(\tau) = \tau \circ f$, $\tau \in k[Y]$.

Recall that if $\mathcal{C}$ is a category, and $F : \mathcal{C} \to \mathfrak{S}$ is a functor, then Yoneda 's lemma asserts that for any object $A \in \mathcal{C}$, the collection of all natural transformations $\tau : F \to \mathrm{Hom}_{\mathcal{C}}(A, \_)$ is in one to one correspondence with $F(A)$. This correspondence sends $\tau \mapsto \tau_A(\mathrm{id}_A)$.

Now, as a consequence of Yoneda 's lemma, we have that if $R, S \in \mathcal{A}_k$ the collection of all natural transformations $\mathrm{Sp}\, R \to \mathrm{Sp}\, S$ is in one to one correspondence with $\mathrm{Alg}(S, R)$. More exactly, this bijection is defined by associating to each $\tau : \mathrm{Sp}\, R \to \mathrm{Sp}\, S$, the map $\tau_R(\mathrm{id}_R) \in \mathrm{Alg}(S, R)$.

If $R \in \mathcal{A}_k$, the algebra isomorphism

$$\mathrm{Alg}(k[T], R) \to R, \quad f \mapsto f(T),$$

gives an isomorphism of k-algebras

$$k[\mathrm{Sp}\, R] \to R.$$

Let G be an affine group scheme. Then the group structures on $G(A)$, $A \in \mathcal{A}_k$, define natural transformations

$$\begin{gathered} m : G \times G \to G, \\ 1 : \mathrm{Sp}\, k \to G, \\ i : G \to G^{op}, \end{gathered}$$

which give rise to algebra maps

$$\begin{gathered} \Delta : k[G] \to k[G] \otimes k[G], \\ \epsilon : k[G] \to k, \\ \mathcal{S} : k[G] \to k[G]^{op}. \end{gathered}$$

Translation of the group axioms on G, say that $k[G]$ is a Hopf algebra where Δ, ϵ and $\mathcal{S}$ are the comultiplication, the counit and the antipode, respectively.

By the above, the functor $G \mapsto k[G]$, from the category of affine group schemes into the category of commutative Hopf algebras is a quasi inverse of $H \mapsto \operatorname{Sp} H$, and thus the latter is an antiequivalence of categories.

Examples.

1) Let $G = GL(n, \_)$ be the functor that associates to each commutative k-algebra A, the group $GL(n, A)$ of all $n \times n$ matrices with entries in A and determinant 1. Then G is an affine group scheme and the Hopf algebra that represents it is $k[X_{ij} : 1 \leq i, j \leq n; Y]/(Y \det(X_{ij}) - 1)$, which is isomorphic to the localization of $k[X_{ij} : 1 \leq i, j \leq n]$ in the powers of $\det(X_{ij})$. The Hopf algebra structure is given by

$$\Delta(X_{ij}) = \sum_{k=0}^{n} X_{ik} \otimes X_{kj}, \quad \Delta(Y) = Y \otimes Y,$$
$$\epsilon(X_{ij}) = \delta_{ij}, \quad \epsilon(Y) = 1,$$
$$\mathcal{S}(X_{ij}) = (-1)^{i+j} Y \det(A_{ij}),$$

where A_{ij} denotes the submatrix of (X_{ij}) obtained eliminating the j-th row and the i-th column, i.e., $\mathcal{S}(X_{ij})$ is the i, j-entry of $(X_{ij})^{-1}$.

2) Consider the affine group scheme $\mathbb{U}(\_) : \mathcal{A}_k \longrightarrow \mathfrak{G}$, that takes A to its group of units $\mathbb{U}(A)$. That is, $\mathbb{U}(\_) = GL(1, \_)$.

In this case the representing Hopf algebra is $H = k[T, T^{-1}]$, the algebra of Laurent polynomials in T over k, with

$$\Delta(T) = T \otimes T, \quad \epsilon(T) = 1,$$
$$\mathcal{S}(T) = T^{-1}.$$

H is isomorphic to the group algebra over the additive group of integers, $k\mathbb{Z}$.

3) **The circular group**

Let $C : \mathcal{A}_k \longrightarrow \mathfrak{G}$ be the functor such that

$$C(A) = \{(a, b) \in A \times A : a^2 + b^2 = 1\}.$$

for each commutative k-algebra A. $C(A)$ has a group structure provided by

$$(a, b)(c, d) = (ac - bd, ad + bc).$$

In fact, C is an affine group scheme, called the *circular group,* whose representing algebra is the so called *trigonometric algebra:* $H = k[s, c]/(s^2 + c^2 - 1)$, with Hopf algebra structure determined by

$$\Delta(c) = c \otimes c - s \otimes s, \quad \Delta(s) = c \otimes s + s \otimes c,$$
$$\epsilon(c) = 1, \quad \epsilon(s) = 0,$$
$$\mathcal{S}(c) = c, \quad \mathcal{S}(s) = -s.$$

Remark. Assume that 2 is invertible in k. Then C is isomorphic to $\mathbb{U}$ if k contains a square root of -1, i.

In fact i induces an isomorphism of Hopf algebras between the representing algebras, $k[T, T^{-1}] \longrightarrow H$, in the form $T \mapsto c + is$. At the group level, the isomorphism $C(A) \to A^*$ is given by

$$(a, b) \mapsto a + ib;$$

the inverse is

$$x \mapsto (\frac{x + x^{-1}}{2}, \frac{x - x^{-1}}{2i}).$$

The dual algebra of a Hopf algebra.

Let C be a coalgebra. Then we know that the dual k-module $C^* = \mathrm{Hom}(C, k)$ is an algebra with the convolution product. We will denote this product by fg (instead of $f * g$), for $f, g \in C^*$. Then we have, $\forall c \in C$

$$\begin{aligned} < fg, c > &= < f, c_{(1)} >< g, c_{(2)} >, \\ 1_{C^*} &= \epsilon. \end{aligned} \tag{1}$$

Observe that the map $C^* \otimes C^* \longrightarrow C^*$ which define this algebra structure is obtained by restricting to $C^* \otimes C^* \subseteq (C \otimes C)^*$ the transpose of $\Delta : C \longrightarrow C \otimes C$, and the unit $k \longrightarrow C^*$ is the transpose of the counit $\epsilon : C \longrightarrow k$.

Let A be a finite dimensional k-algebra. We shall identify $A^* \otimes A^*$ with $(A \otimes A)^*$ via the natural isomorphism. So the transposes of the multiplication $m : A \otimes A \longrightarrow A$ and the unit $u : k \longrightarrow A$ define maps

$$\Delta : A^* \longrightarrow A^* \otimes A^*, \quad \text{and} \quad \epsilon : A^* \longrightarrow k.$$

It is easy to see that (A^*, Δ) is a coalgebra with counit ϵ.

Explicitly, for $f \in A^*$ and $x, y \in A$

$$< \Delta(f), x \otimes y > = < f, xy >, \quad \text{and} \quad \epsilon(f) = < f, 1 > . \tag{2}$$

In other words, $\Delta(f) = f_{(1)} \otimes f_{(2)}$ means $\langle f, xy \rangle = \langle f_{(1)}, x \rangle \langle f_{(2)}, y \rangle$.

If (A, m, Δ) is a finite dimensional bialgebra, with unit u and counit ϵ, then Δ and ϵ are algebra maps. This implies that their transposes Δ^* and ϵ^* are coalgebra maps (with the coalgebra structure in A^* provided by the transposes m^* and u^* of m and u, respectively). So (A^*, Δ^*, m^*) is also a bialgebra.

Proposition 1.8. *Let H be a finite dimensional Hopf algebra with antipode $\mathcal{S}$ and let H^* be the dual bialgebra. Then H^* is a Hopf algebra with antipode $\mathcal{S}^*$. We have also that if k is a field, the evaluation map $H \longrightarrow H^{**}$ is an isomorphism of Hopf algebras.*

Proof. Left to the reader. □

We will denote also by Δ, ϵ and $\mathcal{S}$ for the comultiplication, the counit and the antipode in H^*.

Remarks.

1) Let H be a finite dimensional Hopf algebra. It is clear from the definitions that H is commutative iff H^* is cocommutative and viceversa.

2) The grouplike elements in H^* are the algebra maps $H \longrightarrow k$. The primitive elements are the derivations of H, i.e., the linear maps $D : H \longrightarrow k$ such that $D(ab) = \epsilon(a)D(b) + D(a)\epsilon(b)$, $a, b \in H$.

3) In case A is not a finite dimensional algebra, then the inclusion $A^* \otimes A^* \subseteq (A \otimes A)^*$ is proper, so we can no more consider the coalgebra structure in A^* as above. In this case we take the *finite dual* of A, which is defined as

$$A^o = \{f \in A^* : \exists I \subseteq A, \text{ideal of finite codimension, with } f(I) = 0\}.$$

It can be shown that if H is a Hopf algebra then H^o is also a Hopf algebra *dual* to H, in the sense that it satisfies equations (1) and (2).

Examples.

1) Let G be a group, and consider the Hopf algebra kG. Then the dual Hopf algebra kG^* may be identified with the algebra of functions over G, k^G, where the algebra structure is pointwise multiplication. If k is a field and G is a *finite* group, then there is an isomorphism of Hopf algebras $kG \backsimeq k^{G^*}$, given by the evaluation map $g \mapsto E_g$, where $E_g(h) = h(g)$, $g \in G, h \in k^G$.

2) Let $A = M_n(k)$ be the algebra of all $n \times n$ matrices with entries in k. Identifying A with A^* via the trace (i.e., $< X, Y >= \mathrm{Tr}(XY)$, $X, Y \in A$), we get a coalgebra structure in A. The comultiplication, Δ, is given by

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

where E_{ij} denotes the matrix having all entries equal to zero, except for a 1 in the entry ij. The counit is $\epsilon = \mathrm{Tr} : A \longrightarrow k$.

Observe that A is not a bialgebra with this comultiplication.

3) Let H be the Taft algebra over the field k. Then H is isomorphic to H^*. This can be seen as follows.

Let $G \in H^*$ the algebra map defined by

$$G(g) = \xi^{-1}, \quad G(x) = 0,$$

and let X be the k-linear map $X : H \longrightarrow k$, such that

$$X(g^i x) = 1, \quad 0 \leq i \leq N-1,$$
$$X(g^i x^j) = 0, \quad 0 \leq i, j \leq N-1, j \neq 1.$$

Then the map $g \mapsto G$, $x \mapsto X$, gives an isomorphism of Hopf algebras $H \longrightarrow H^*$.

§2 Hopf modules and integrals

This section covers the main results of Larson and Sweedler's fundamental paper [8].

Definition. Let H be a Hopf algebra over k. A k-module V is called a (right) *Hopf module* for H, if it satisfies the three conditions:

1) V is a right H-module.

2) V is a right H-comodule.

3) *Compatibility condition:* $\Delta_V(v.x) = v_{(0)}.x_{(1)} \otimes v_{(1)}x_{(2)}$, $\forall\ x \in H, v \in V$.

If V, W are Hopf modules, a k-linear map $f : V \longrightarrow W$ is said a *Hopf module map,* if it is both a module and a comodule map.

Remark. If $\Delta_V : V \longrightarrow V \otimes H$ is the comodule structure map on V, then condition 3) says that Δ_V is a morphism of H-right modules, with the right H-action on $V \otimes H$ given by Δ: $(v \otimes g).h = v.h_{(1)} \otimes gh_{(2)}$.

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

If V is a right Hopf module, the *invariant* and *covariant* submodules of V are defined, respectively, to be

$$V^H = \{v \in V : v.h = \epsilon(h)v, \forall h \in H\},$$

and

$$V^{\mathrm{co}\,H} = \{v \in V : \Delta_V(v) = v \otimes 1\}.$$

Given a k-module W, the tensor product $W \otimes H$ can be made into a H-Hopf module by setting

$$(w \otimes h).g = w \otimes hg,$$
$$\Delta_{W\otimes H}(w \otimes h) = w \otimes h_{(1)} \otimes h_{(2)}.$$

$\forall w \in W, h, g \in H$. Such Hopf modules will be called *trivial*.

The following theorem asserts that all Hopf modules are trivial.

Theorem 2.1. Fundamental Theorem of Hopf modules (Larson - Sweedler, 1969). *Let V be a right H-Hopf module. Then the multiplication map*

$$\rho : V^{\mathrm{co}\,H} \otimes H \xrightarrow[v\otimes h \mapsto v.h]{} V,$$

is an isomorphism of Hopf modules (where $V^{\mathrm{co}\,H} \otimes H$ has the trivial Hopf module structure).

Proof.

We first show that $\phi : V \longrightarrow V^{\mathrm{co}\,H}$, given by $\phi(v) = v_{(0)}.\mathcal{S}(v_{(1)})$ is a well defined linear map.

For this, let $v \in V$ and calculate

$$\Delta_V(\phi(v)) = \Delta_V(v_{(0)}.\mathcal{S}(v_{(1)})) = v_{(0)}.\mathcal{S}(v_{(3)}) \otimes v_{(1)}.\mathcal{S}(v_{(2)}) =$$
$$v_{(0)}.\mathcal{S}(v_{(2)}) \otimes \epsilon(v_{(1)})1 = v_{(0)}.\mathcal{S}(v_{(1)}) \otimes 1 = \phi(v) \otimes 1.$$

So $\phi(v) \in V^{\mathrm{co}\,H}$ as we wanted.

Now we claim that $(\phi \otimes \mathrm{id})\Delta_V : V \to V^{\mathrm{co}\,H} \otimes H$ is the inverse of ρ.

Let $v \in V$, then

$$\rho \circ (\phi \otimes \mathrm{id})\Delta_V(v) = \phi(v_{(0)}).v_{(1)} = v_{(0)}.\mathcal{S}(v_{(1)})v_{(2)} = v_{(0)}\epsilon(v_{(1)}) = v.$$

If $v \in V^{\mathrm{co}\,H}$, $h \in H$, we have

$$(\phi\otimes\mathrm{id})\Delta_V \circ \rho(v\otimes h) = \phi((v.h)_{(0)})\otimes(v.h)_{(1)} = \phi(v.h_{(1)})\otimes h_{(2)} = v.h_{(1)}\mathcal{S}(h_{(2)})\otimes h_{(3)} = v\otimes h.$$

This finishes the proof, since both maps are morphisms of right H-Hopf modules. □

Definition. Let H be a Hopf algebra. The k-linear spaces of left and right integrals in H are defined, respectively, as follows:

$$\mathcal{I}_l(H) = \{h \in H : xh = \epsilon(x)h, \forall x \in H\},$$

and

$$\mathcal{I}_r(H) = \{h \in H : hx = \epsilon(x)h, \forall x \in H\}.$$

H is called *unimodular* if $\mathcal{I}_l(H) = \mathcal{I}_r(H)$.

Observation. With this definition, for instance the space of (left) integrals in H is the (left) ideal of invariants with respect to the action of H on itself by left multiplication. It is clear that it is also a right ideal.

Examples.

1) Let H be finite dimensional. Then $\phi \in H^*$ is a left integral, if and only if,

$$h_{(1)} < \phi, h_{(2)} > = < \phi, h > 1_H,$$

$\forall h \in H$.

2) Let G be a finite group, and let kG its group algebra. Then kG is unimodular, with $\mathcal{I}_l = \mathcal{I}_r = k(\sum_{g\in G} g)$.

(The definition of left integral in $kG = k^{G^*}$, which is the space of all distributions on G, coincides with that of left invariant measure, i.e., those linear functionals α on k^G such that $< \alpha, \phi > = < \alpha, L_g\phi >$, $\forall \phi \in k^G$, $g \in G$. Here L_g denotes the left translation by g in k^G: $< L_g\phi, h > = \phi(gh)$).

3) Let H be the Taft algebra of dimension N^2 over the field k. Then the spaces of left and right integrals are respectively

$$\mathcal{I}_l(H) = k(\sum_{j=0}^{N-1} g^j x^{N-1}),$$

and

$$\mathcal{I}_r(H) = k(\sum_{j=0}^{N-1} \xi^j g^j x^{N-1}).$$

Let H be a Hopf algebra, and let V be a right H-comodule with comodule structure map Δ_V. Then V is a left H^*-module via

$$H^* \otimes V \xrightarrow{\mathrm{id}\otimes\Delta_V} H^* \otimes V \otimes H \xrightarrow{\mathrm{id}\otimes\tau} H^* \otimes H \otimes V \xrightarrow{<,>\otimes\mathrm{id}} k \otimes V \to V,$$

where $<,>: H^* \otimes H \to k$ is the evaluation map: $h^* \otimes h \mapsto < h^*, h >$.

Explicitly,

$$(*) \qquad h^*.v =< h^*, v_{(1)} > v_{(0)},$$

$v \in V$, $h^* \in H^*$.

A left H^*-module V with the property that there exists a right H-comodule structure on V such that (*) holds is called *rational*.

For finite dimensional H, it is possible to show that all left H^*-modules are rational.

Let $\dim H$ be finite. The above allows us to consider H^* as a right H-comodule as we indicate now.

H^* is a left H^*-module via left multiplication. So it is a rational H^*-module. We can then consider the right coaction $\rho : H^* \to H^* \otimes H$, such that

$$(1) \qquad \rho(f) = f_{(0)} \otimes f_{(1)} \quad \Leftrightarrow \quad < p, h_{(1)} >< f, h_{(2)} >=< p, f_{(1)} >< f_{(0)}, h >,$$

$\forall p \in H^*$, $h \in H$.

On the other hand, we have that H^* is a left (respectively right) H-module via the transpose of right (respectively left) multiplication in H. This action is denoted by $h \rightharpoonup h^*$ (respectively $h^* \leftharpoonup h$), for $h \in H$, $h^* \in H^*$.

By means of the antipode, we get left and right actions of H on H^*:

$$h \rightharpoonup h^* = h^* \leftharpoonup \mathcal{S}(h), \quad \text{and} \quad h^* \leftharpoonup h = \mathcal{S}(h) \rightharpoonup h^*.$$

These actions are determined by

$$< h^* \leftharpoonup h, g >=< h^*, g\mathcal{S}(h) >, \quad < h \rightharpoonup h^*, g >=< h^*, \mathcal{S}(h)g >,$$

for $h^* \in H^*$, $g, h \in H$.

In particular, H^* is a right H-module via $h^* \leftharpoonup h$. If H is finite dimensional, recalling the right coaction ρ of H on H^* given by (1), we find that H^* is both a right module and comodule for H. Moreover, we have:

Lemma 2.2 (Larson - Sweedler, 1969). *Let H be a finite dimensional Hopf algebra. Then H^* is a right Hopf module, with action $\leftharpoonup$ and coaction ρ.*

Proof.

We must show that $\forall f \in H^*$, and $\forall h \in H$, $\rho(f \leftharpoonup h) = f_{(0)} \leftharpoonup h_{(1)} \otimes f_{(1)}h_{(2)}$. That is, we must see that $\forall p \in H^*$, and $\forall x \in H$,

$$< p, x_{(1)} >< f \leftharpoonup h, x_{(2)} >=< f_{(0)} \leftharpoonup h_{(1)}, x >< p, f_{(1)}h_{(2)} > .$$

Now,

$$\begin{aligned} &< f_{(0)} \leftharpoonup h_{(1)}, x >< p, f_{(1)}h_{(2)} >=< f_{(0)}, x\mathcal{S}(h_{(1)}) >< h_{(2)} \rightharpoonup p, f_{(1)} >= \\ &< h_{(3)} \rightharpoonup p, x_{(1)}\mathcal{S}(h_{(2)}) >< f, x_{(2)}\mathcal{S}(h_{(1)}) >=< p, x_{(1)} < \epsilon, h_{(2)} >>< f, x_{(2)}\mathcal{S}(h_{(1)}) >= \\ &< p, x_{(1)} >< f, x_{(2)}\mathcal{S}(h) >=< p, x_{(1)} >< f \leftharpoonup h, x_{(2)} > . \quad \square \end{aligned}$$

In what follows k will be a field. The next theorem, due to Larson and Sweedler (1969), is a consequence of theorem (2.1) and lemma (2.2).

Theorem 2.3 (Larson - Sweedler, 1969). *Let H be a finite dimensional Hopf algebra over k. Then*

1) $\dim \mathcal{I}_l(H) = \dim \mathcal{I}_r(H) = 1$.

2) The antipode $\mathcal{S}$ is bijective, and $\mathcal{S}(\mathcal{I}_l) = \mathcal{I}_r$.

3) For $0 \neq \lambda \in \mathcal{I}_l(H^*)$, the map $H \to H^*$, given by $h \mapsto h \rightharpoonup \lambda$, is a left linear isomorphism.

Proof. 1) Consider the Hopf module structure on H^* given by lemma (2.2). By theorem (2.1), $(H^*)^{\mathrm{co}\,H} \otimes H \backsimeq H^*$. And, as H is finite dimensional, we get $\dim (H^*)^{\mathrm{co}\,H} = 1$.

It remains to observe that $(H^*)^{\mathrm{co}\,H} = \mathcal{I}_l(H^*)$, which is clear from the definitions. Then replacing H^* by H (again using the finite dimensionality of H), we get $\dim \mathcal{I}_l(H) = 1$. The remaining equality will follow from 2).

2) By theorem (2.1), the map

$$\mathcal{I}_l(H^*) \otimes H \xrightarrow[\lambda \otimes h \mapsto \lambda \leftharpoonup h]{} H^*,$$

is an isomorphism.

Suppose now that $0 \neq \lambda \in \mathcal{I}_l(H^*)$, and let $h \in H$ such that $\mathcal{S}(h) = 0$. Then

$$0 = \mathcal{S}(h) \rightharpoonup \lambda = \lambda \leftharpoonup h.$$

Thus $\lambda \otimes h = 0$, and so $h = 0$.

This shows that $\mathcal{S}$ is injective. Now, as H is finite dimensional, it is bijective.

Finally, using this it is an easy calculation to show that $\mathcal{S}(\mathcal{I}_l) = \mathcal{I}_r$.

3) Again using theorem (2.1), plus the fact that $\dim \mathcal{I}_l(H^*) = 1$, we get that for any $0 \neq \lambda \in \mathcal{I}_l(H^*)$,

$$H^* = \lambda \leftharpoonup H = \mathcal{S}(H) \rightharpoonup \lambda.$$

Now, as $\mathcal{S}$ is bijective, it follows that $H^* = H \rightharpoonup \lambda$, which proves 3). □

From now on we will write $hf := h \rightharpoonup f$ and $fh := f \leftharpoonup h$, for $h \in H$, $f \in H^*$.

In what follows we consider a class of algebras that contains the finite dimensional Hopf algebras.

Frobenius algebras.

Let k denote a field. If A is a k-algebra, the *left* (respectively *right*) *regular representation* of A is the module structure in A given by left (respectively right) multiplication. It is denoted by ${}_AA$ (respectively A_A).

Recall that if M is a right A-module, then the dual space M^* is a left A-module by

$$< a.\phi, m > = < \phi, m.a >,$$

$a \in A$, $\phi \in M^*$, $m \in M$.

In particular, this holds if we take M to be the right regular module for A, ${}_AA$.

Let A be a finite dimensional algebra (say $\dim A = n$), $\phi \in A^*$, and $r_i, l_i \in A$, $1 \leq i \leq n$. Then ϕ is called a *Frobenius homomorphism,* with *dual bases* (r_i, l_i) if one of the following (equivalent) conditions holds:

a) $\forall x \in A$, $x = \sum_i r_i < \phi, l_i x >$.

b) $\forall x \in A$, $x = \sum_i < \phi, x r_i > l_i$.

Proposition 2.4. *Let A be a finite dimensional algebra, and let $f \in A^*$. Then the following statements are equivalent:*

1) The map ${}_AA \to {A_A}^*$, given by $x \mapsto xf$ is an isomorphism of left A-modules.

2) There exist $r_i, l_i \in A$, $1 \leq i \leq n$ ($n = \dim A$), such that f is a Frobenius homomorphism with dual bases (r_i, l_i).

3) The map ${A_A} \to {}_A{A^*}$, given by $x \mapsto fx$ is an isomorphism of right A-modules.

Proof.

1) $\Rightarrow$ 2). Let (l_i) be a k-basis for A, and let (f_i) its dual basis.

By 1), there exist $r_i \in A$, such that $f_i = r_i f$. Then, $\forall x \in A$,

$$x = \sum_i < f_i, x > l_i = \sum_i < r_i f, x > l_i = \sum_i < f, x r_i > l_i.$$

2) $\Rightarrow$ 1). Suppose $fx = 0$ for some $x \in A$. Then $< fx, y >=< f, xy >= 0$, $\forall y \in A$. Hence

$$x = \sum_i < f, x r_i > l_i = 0.$$

So the map $x \mapsto fx$ is injective, and as A is finite dimensional it is bijective.

Similarly one shows that 2) $\Leftrightarrow$ 3), but here using the condition a) in the definition of dual bases for Frobenius homomorphisms. $\square$

Definition. Let A be a finite dimensional k-algebra. If A satisfies any of the equivalent conditions 1) – 3) of the proposition above, then A is called a *Frobenius algebra.*

Remark. By theorem (2.3), we know that if H is a finite dimensional Hopf algebra, then H is a Frobenius algebra.

We have moreover, that if $0 \neq \lambda$ is any left integral in H^*, then the maps ${}_HH \to {H_H}^*$, $h \mapsto h\lambda$, and ${H_H} \to {}_H{H^*}$, $h \mapsto \lambda h$ are isomorphisms of left (respectively right) H-modules.

We may then choose $\Lambda \in H$ such that $\lambda\Lambda = \epsilon$. Such Λ is necessarily a right integral in H as the following argument shows.

If I is a right integral in H, then $\lambda I =< \lambda, I > \epsilon$. And by the injectivity of $h \mapsto \lambda h$, $< \lambda, I >\neq 0$ if $I \neq 0$.

So we can choose I to be such that $< \lambda, I >= 1$, and then $\lambda I = \epsilon$.

Again using the injectivity of $h \mapsto \lambda h$, we find that $\Lambda = I$ is a right integral in H.

We saw also that the condition $\lambda\Lambda = \epsilon$ is equivalent to $< \lambda, \Lambda >= 1$.

§3 Finite Hopf algebras

In what follows, k will denote a field. Let H be a Hopf algebra.

The following are conjectures made by Kaplansky (1975) (see appendix):
1. If R is a Hopf subalgebra of H, then H is a free R-module.
2. If $\dim H$ is finite and H is semisimple, then the square of the antipode is the identity.
3. If $\dim H = p$, p a prime, then H is commutative and cocommutative.

Of these, (1) is known to be false in general [12], though it is true if H is finite dimensional. As to (2) and (3), they are known over fields of characteristic 0.

The main results we treat in this section and the next are partial answers to these questions.

A finite dimensional Hopf algebra H over k will be called *finite.* By the *order* of H we will mean its dimension.

The results in §2 allowed us to assert that H is a Frobenius algebra. Now we treat the connection between this structure and the Hopf algebra structure in H following [13].

Theorem 3.1. *Let $0 \neq \lambda \in H^*$ be a left integral, and let $\Lambda \in H$ be such that $\lambda\Lambda = \epsilon$. Then λ is a Frobenius homomorphism with dual bases $(\mathcal{S}(\Lambda_{(1)}), \Lambda_{(2)})$.*

Proof. Let $x \in H$. Then

$$\mathcal{S}(\Lambda_{(1)})\langle\lambda, \Lambda_{(2)}x\rangle = \mathcal{S}(\Lambda_{(1)})\Lambda_{(2)}x_{(1)}\langle\lambda, \Lambda_{(3)}x_{(2)}\rangle = x_{(1)}\langle\lambda, \Lambda x_{(2)}\rangle = x\langle\lambda, \Lambda\rangle = x. \quad \square$$

In an enterily similar fashion, one can see that if $\gamma \in H^*$ is a nonzero right integral, then there exists a left integral $\Gamma \in H$ such that $\Gamma\gamma = \epsilon$. We also have that γ is a Frobenius homomorphism in H with dual bases $(\Gamma_{(1)}, \mathcal{S}(\Gamma_{(2)}))$.

From now on we fix a nonzero left (respectively right) integral $\lambda \in H^*$ (respectively γ), and call Λ (respectively Γ) the right (respectively left) integral in H such that $< \lambda, \Lambda >= 1$ (respectively $< \gamma, \Gamma >= 1$), without further comment.

Remark. If A is a Frobenius algebra, and $f \in A^*$ is a Frobenius homomorphism with dual bases (r_i, l_i), then in $A \otimes A$ we have the identity

$$\sum_i xr_i \otimes l_i = \sum_i r_i \otimes l_i x.$$

$\forall x \in A$.

Indeed, these have the same image in $\mathrm{End}(A)$ under the map

$$A \otimes A \xrightarrow[a\otimes b \mapsto a \otimes fb]{} A \otimes A^* \backsimeq \mathrm{End}(A).$$

Here, as usual, the linear isomorphism $A \otimes A^* \longrightarrow \mathrm{End}(A)$ is given by $(a \otimes \phi)(x) =< \phi, x > a$.

This remark motivates the following

Definition.
A k algebra A is called *separable* if there exist $r_i, l_i \in A$, $1 \leq i \leq n = \dim A$, such that:
1)$\sum_i r_i l_i = 1$.
2) $\forall x \in A$, $\sum_i xr_i \otimes l_i = \sum_i r_i \otimes l_i x$ in $A \otimes A$.

We say a Hopf algebra H is semisimple if it is semisimple as an algebra, i.e., if every finite dimensional left H-module is completely reducible.

Remark. For a finite dimensional k-algebra A, the condition of being semisimple is equivalent to $\mathrm{rad}(A) = 0$. Where $\mathrm{rad}(A)$ denotes the *radical* of A, which by definition is the sum of all nilpotent left ideals in A. (See [1, §25, p. 163]).

We also have the identity $\mathrm{rad}(A) = \mathcal{J}$, where $\mathcal{J}$ denotes the *Jacobson radical* of A, i.e., $\mathcal{J}$:=intersection of all maximal left ideals of A. In particular, as $\mathcal{J}$ is a nilpotent ideal of A (A being finite dimensional), every element of $\mathcal{J}$ is nilpotent. We will use these facts later on.

Example.
Consider a finite group G, kG its group algebra. Recall the well known Maschke theorem, which asserts that kG is semisimple iff the characteristic of k does not divide the order $|G|$ of G.

Now, $|G| = \sum_{g \in G} < \epsilon, g > =< \epsilon, \sum_{g \in G} g >$.

As $\sum_{g \in G} g$ spans the (one dimensional) space of left integrals in kG, Maschke theorem is equivalent to the statement " kG is semisimple iff $< \epsilon, \mathcal{I}_l(kG) > \neq 0$".

The next theorem generalizes this result.

Theorem 3.2. Maschke Theorem for Hopf algebras.
Let H be a finite dimensional Hopf algebra. Then the following statements are equivalent.
1) H is semisimple.
2) H is separable.
3) $< \epsilon, \mathcal{I}_l(H) > \neq 0$.

Proof.
Observe that as $\mathcal{S}(\mathcal{I}_l(H)) = \mathcal{I}_r(H)$ and $\epsilon \mathcal{S} = \epsilon$, then $< \epsilon, \mathcal{I}_l(H) >= 0 \Leftrightarrow < \epsilon, \mathcal{I}_r(H) >= 0$.

3) $\Rightarrow$ 2).
Take $(r_i, p_i) = (\mathcal{S}(\Lambda_{(1)}), \Lambda_{(2)})$.
We have that

$$\sum_i r_i p_i = \mathcal{S}(\Lambda_{(1)})\Lambda_{(2)} =< \epsilon, \Lambda > 1,$$

by 3), $t =< \epsilon, \Lambda > \neq 0$.

Then changing p_i by $l_i = t^{-1} p_i$, and using theorem (3.1), we find that (r_i, l_i) makes H into a separable algebra.

2) $\Rightarrow$ 1).

Let Y be a finite dimensional H-module, and let X be a submodule of Y.

Let $\pi : Y \to X$ be any k-linear projection, and define $\widehat{\pi} : Y \to Y$ in the form $\widehat{\pi}(y) = \sum_i r_i.\pi(l_i.y)$.

We claim that $\widehat{\pi}$ is an H-linear projection.

As X is an H-submodule, $\widehat{\pi}(Y) \subseteq X$.

By 2), $\sum_i hr_i \otimes l_i = \sum_i r_i \otimes l_i h$ in $H \otimes H$, $\forall h \in H$. This implies that

$$\sum_i hr_i.\pi(l_i.y) = \sum_i r_i \pi(l_i h.y), \quad \forall h \in H, y \in Y.$$

Hence,

$$\widehat{\pi}(h.y) = \sum_i r_i.\pi(l_i h.y) = \sum_i hr_i.\pi(l_i.y) = h.\widehat{\pi}(y),$$

$\forall h \in H$, $y \in Y$. So $\widehat{\pi}$ is H-linear.

Finally,

$$\widehat{\pi}(x) = \sum_i r_i \pi(l_i.x) = \sum_i r_i l_i.x = (\sum_i r_i l_i).x = 1.x = x,$$

$\forall x \in X$. So the claim is proved.

1) $\Rightarrow$ 3).

As H is semisimple, we have that any short exact sequence of left H-modules

$$0 \to U \xrightarrow{\mu} V \xrightarrow{\pi} W \to 0,$$

splits. That is, there exists an H-linear map $\nu : W \to V$, such that $\pi\nu = \mathrm{id}_W$.

Applying this to the short exact sequence

$$0 \to \ker \epsilon \to H \xrightarrow{\epsilon} k \to 0,$$

we get in particular that $< \epsilon, \nu(1) >= 1$.

Now, if $h \in H$, as ν is H-linear

$$h\nu(1) = \nu(< \epsilon, h >) =< \epsilon, h > \nu(1).$$

This shows that $\nu(1)$ is a left integral in H. So $< \epsilon, \mathcal{I}_l(H) >\neq 0$. Then $< \epsilon, \mathcal{I}_r(H) >\neq 0$, and as Λ is a nonzero right integral, being $\dim \mathcal{I}_r(H) = 1$, we must have $< \epsilon, \Lambda >\neq 0$. $\square$

Observation. Replacing H by H^* in theorem (3.2) we get that H^* is semisimple iff $< \lambda, 1 >\neq 0$, for some left integral $\lambda \in H^*$.

Recall that for a finite dimensional vector space V over k, we have a canonical isomorphism $V^* \otimes V \to \mathrm{End}(V)$, given by

$$(\phi \otimes v)(w) =< \phi, w > v, \quad v, w \in V, \phi \in V^*.$$

Via this identification, if $\mathrm{Tr} : \mathrm{End}(V) \to k$ denotes the *trace* map, i.e., $\mathrm{Tr}(F) :=$ trace of F, we find that $\mathrm{Tr}(\phi \otimes v) =< \phi, v >$, for $v \in V$, $\phi \in V^*$.

Lemma 3.3. *Let H be a finite Hopf algebra, and let F be an endomorphism of H. Then the trace of F is given by*

$$\mathrm{Tr}(F) =< \lambda, F(\Lambda_{(2)})\mathcal{S}(\Lambda_{(1)}) > .$$

Proof.

Let $F \in \mathrm{End}(H)$. We know that for all $x \in H$,

$$F(x) =< \lambda, F(x)\mathcal{S}(\Lambda_{(1)}) > \Lambda_{(2)}.$$

So via the identification $H^* \otimes H \backsimeq \mathrm{End}(H)$, F corresponds to

$$< \lambda, F(\_)\mathcal{S}(\Lambda_{(1)}) > \otimes \Lambda_{(2)},$$

then

$$\mathrm{Tr}(F) =< \lambda, F(\Lambda_{(2)})\mathcal{S}(\Lambda_{(1)}) > .$$

□

In a finite Hopf algebra the trace of the square of the antipode plays a very important role, as we will see soon.

For an element $h \in H$, call $L_h \in \mathrm{End}(H)$ the endomorphism of H given by $L_h(x) = hx$, $x \in H$.

This defines a k-linear map $\mathrm{Tr}_H : H \longrightarrow k$, in the form: $\mathrm{Tr}_H(h) = \mathrm{Tr}(L_h)$, $h \in H$.

This map will be of central importance later on. As a consequence of lemma (3.3), we have the next proposition.

Proposition 3.4. *Let H be a finite Hopf algebra, then:*

1) $\mathrm{Tr}(\mathcal{S}^2) =< \epsilon, \Lambda >< \lambda, 1 >$.

2) If $\mathcal{S}^2 = \mathrm{id}$, *then* $\mathrm{Tr}_H =< \epsilon, \Lambda > \lambda$.

Proof.

1) Taking $F = \mathcal{S}^2$ in the lemma above, we get

$$\mathrm{Tr}(\mathcal{S}^2) =< \lambda, \mathcal{S}^2(\Lambda_{(2)})\mathcal{S}(\Lambda_{(1)}) >=< \lambda, \mathcal{S}(\Lambda_{(1)}\mathcal{S}(\Lambda_{(2)})) >=< \epsilon, \Lambda >< \lambda, 1 > .$$

2) As $\mathcal{S}^2 = \mathrm{id}$, we have that $h_{(2)}\mathcal{S}(h_{(1)}) =< \epsilon, h > 1$, $\forall h \in H$.

Now take $F = L_h$, $h \in H$, then

$$\mathrm{Tr}_H(h) = \mathrm{Tr}(L_h) =< \lambda, h\Lambda_{(2)}\mathcal{S}(\Lambda_{(1)}) >=< \epsilon, \Lambda >< \lambda, h > .$$

□

Corollary 3.5.

a) H and H^* are semisimple, if and only if $\mathrm{Tr}(\mathcal{S}^2) \neq 0$.

b) If $\mathcal{S}^2 = \mathrm{id}$ *and* $\mathrm{char}\, k$ *does not divide the order of H, then H and H^* are semisimple.*

Proof. It is immediate. □

Indeed, if the characteristic of k is zero, then the converse of 2) holds.

Remark. [1] Combining Theorem 1.5 c) and Corollary (3.5), we conclude that a cocommutative finite Hopf algebra H is semisimple and cosemisimple, in characteristic 0. Therefore, if k is algebraically closed, H is a group algebra. We recover in this way part of the Fundamental theorem for cocommutative Hopf algebras in characteristic 0.

In what follows, we develop a formula for $\mathcal{S}^4$, that is valid over an arbitrary field k, and that will imply this last assertion.

It will also prove the finiteness of the order of the antipode for finite Hopf algebras.

The order of the antipode. Radford's formula for $\mathcal{S}^4$.

If $0 \neq t \in H$ is a right integral and $h \in H$, then it is clear that ht is again a right integral. Thus, as the space of right integrals is one dimensional, we may find an $\alpha = \alpha(h) \in k$ such that $ht = \alpha(h)t$.

This defines an element $\alpha \in H^*$. We have, moreover, that $\alpha \in \mathrm{Alg}(H, k) = G(H^*)$. For, if $x, y \in H$, then

$$< \alpha, xy > t = xyt =< \alpha, y >< \alpha, x > t,$$

and as $t \neq 0$, it must be $< \alpha, xy >=< \alpha, x >< \alpha, y >$.

In analogous way, given a right integral $0 \neq I \in H^*$, we may find an element $a \in H$ such that $h_{(1)} < I, h_{(2)} >=< I, h > a$, $\forall h \in H$.

Changing the roles of H and H^* in the preceding discussion, it results that $a \in G(H)$ is a grouplike element in H.

It is clear that α and a are independent of the choice of the nonzero right integrals t and I. So they are determined exclusively by H.

Definition. Let $a \in G(H)$ and $\alpha \in \mathrm{Alg}(H, k)$ as above. Then a, α are called the *modular elements* of H.

Observe that as a and α are grouplike elements, then they are units (of H and H^* respectively), and $\mathcal{S}(a) = a^{-1}$, $\mathcal{S}(\alpha) = \alpha^{-1}$.

Remarks.

1) It follows from the definitions that H^* is unimodular iff $a = 1$, and H is unimodular iff $\alpha = \epsilon$.

2) If H is semisimple, then H is unimodular.

To see this, let $0 \neq t$ be a right integral in H. So that $< \epsilon, t > \neq 0$, by the semisimplicity of H.

If $h \in H$, then apply ϵ to the defining equation

$$ht =< \alpha, h > t.$$

Then $\alpha = \epsilon$, and thus H is unimodular.

[1] This application was added by S. Natale.

Let $\gamma \in \mathcal{I}_r(H^*)$ be the Frobenius homomorphism of H considered earlier. Then γ determines an isomorphism $H \to H^*$, $h \mapsto h\gamma$.

Now, for fixed $x \in H$, we can consider the element of H^* defined by $y \mapsto < \gamma, xy >$, $y \in H$.

There exists then $\rho = \rho(x) \in H$ such that $\forall y \in H$

$$< \gamma, xy > = < \rho(x)\gamma, y > = < \gamma, y\rho(x) > .$$

In other words, $\gamma x = \rho(x)\gamma$. The map $\rho : H \to H$ defined this way is an automorphism of H.

Definition. ρ is called the *Nakayama automorphism* of H with respect to the Frobenius homomorphism γ.

The following two propositions will help us to give a conceptual proof of Radford's formula for $\mathcal{S}^4$, which is simpler than the original proof in [10].

Denote by $\overline{\mathcal{S}}$ the (composition) inverse of the antipode of H.

Proposition 3.6. *Let $\gamma \in H^*$ be a nonzero right integral, and let $\Gamma \in H$ be a left integral such that $< \gamma, \Gamma >= 1$. If $t = \mathcal{S}(\Gamma)$, and $\alpha \in \mathrm{Alg}(H, k)$ is the modular function of H, we have:*

1) $(\overline{\mathcal{S}}(t_{(2)}), t_{(1)})$ are dual bases for γ.

2) $\forall h \in H$, $\rho(h) = < \alpha, h_{(1)} > \overline{\mathcal{S}}^2(h_{(2)})$.

Proof.

1) Follows from the fact that $(\Gamma_{(1)}, \mathcal{S}(\Gamma_{(2)}))$ are dual bases for γ. (Or applying theorem (3.1) to the Hopf algebra H^{cop}, which is obtained from H by taking the opposite comultiplication $\Delta^{op} = \tau \circ \Delta$.) In particular, $\langle \gamma, t \rangle = 1$, by applying ϵ to the equation a) in 2.4.

2) Let $h \in H$, then by 1)

$$\rho(h) = \overline{\mathcal{S}}(t_{(2)}) < \gamma, t_{(1)}\rho(h) > = \overline{\mathcal{S}}(t_{(2)}) < \gamma, ht_{(1)} >,$$

the last equality following from the definition of ρ. Applying $\mathcal{S}^2$, and recalling that γ is a right integral in H^*, we get

$$\mathcal{S}^2 \circ \rho(h) = < \gamma, ht_{(1)} > \mathcal{S}(t_{(2)}) = < \gamma, h_{(1)}t_{(1)} > h_{(2)}t_{(2)}\mathcal{S}(t_{(3)}) =$$
$$< \gamma, h_{(1)}t > h_{(2)} = < \gamma, < \alpha h_{(1)} > t > h_{(2)} = < \alpha, h_{(1)} > h_{(2)}.$$

Then

$$\rho(h) = < \alpha, h_{(1)} > \overline{\mathcal{S}}^2(h_{(2)}),$$

as claimed. □

Proposition 3.7. *If $a \in G(H)$ is the modular element of H and t is as in (3.6), we have:*
1) $(\mathcal{S}(t_{(1)})a, t_{(2)})$ are dual bases for γ.
2) $\forall h \in H$, $\rho(h) = a^{-1}(\mathcal{S}^2(h_{(1)}) < \alpha, h_{(2)} >)a$.

Proof.
1) Using the definition of a, we have that $\forall h \in H$,

$$\mathcal{S}(t_{(1)})a < \gamma, t_{(2)}h >= \mathcal{S}(t_{(1)})t_{(2)}h_{(1)} < \gamma, t_{(3)}h_{(2)} >= h_{(1)} < \gamma, th_{(2)} >= h_{(1)} < \epsilon, h_{(2)} >= h.$$

2) By 1), $\forall h \in H$, we may write

$$\rho(h) = \mathcal{S}(t_{(1)})a < \gamma, t_{(2)}\rho(h) > .$$

Then

$$a\overline{\mathcal{S}}^2(\rho(h))a^{-1} = a < \gamma, ht_{(2)} > \overline{\mathcal{S}}(t_{(1)}) = h_{(1)}t_{(2)} < \gamma, h_{(2)}t_{(3)} > \overline{\mathcal{S}}(t_{(1)}) = h_{(1)} < \gamma, h_{(2)}t >= h_{(1)} < \alpha, h_{(2)} > .$$

Hence, conjugating by a^{-1} and applying $\mathcal{S}^2$, we get the result. □

Consider the left and right H^*-module structures on H given by:

$$h^* \rightharpoonup h = h_{(1)} < h^*, h_{(2)} >,$$
$$h \leftharpoonup h^* =< h^*, h_{(1)} > h_{(2)},$$

$\forall h \in H, h^* \in H^*$. We then have:

Theorem 3.8 (Radford, 1976). *Let $a \in G(H)$, $\alpha \in \mathrm{Alg}(H, k)$ be the modular elements of H. Then the following formula holds , $\forall h \in H$:*

$$\mathcal{S}^4(h) = a(\alpha^{-1} \rightharpoonup h \leftharpoonup \alpha)a^{-1} = \alpha^{-1} \rightharpoonup (aha^{-1}) \leftharpoonup \alpha.$$

Proof. We show first that

$$a(\alpha^{-1} \rightharpoonup h \leftharpoonup \alpha)a^{-1} = \alpha^{-1} \rightharpoonup (aha^{-1}) \leftharpoonup \alpha,$$

$\forall h \in H$. For this, we compute

$$a(\alpha^{-1} \rightharpoonup h \leftharpoonup \alpha)a^{-1} =< \alpha, h_{(1)} > ah_{(2)}a^{-1} < \alpha^{-1}, h_{(3)} > .$$

On the other hand, as a is a grouplike element of H,

$$\alpha^{-1} \rightharpoonup (aha^{-1}) \leftharpoonup \alpha =< \alpha, ah_{(1)}a^{-1} > ah_{(2)}a^{-1} < \alpha^{-1}, ah_{(3)}a^{-1} >= < \alpha, h_{(1)} > ah_{(2)}a^{-1} < \alpha^{-1}, h_{(3)} >,$$

the last equality because $\alpha \in \mathrm{Alg}(H, k)$.

Now, by propositions (3.6) and (3.7), we have, $\forall h \in H$,

$$< \alpha, h_{(1)} > \overline{\mathcal{S}}^2(h_{(2)}) = \rho(h) = a^{-1}(\mathcal{S}^2(h_{(1)}) < \alpha, h_{(2)} >)a.$$

Applying $\mathcal{S}^2$ and conjugating by a, we get

$$a < \alpha, h_{(1)} > h_{(2)}a^{-1} = \mathcal{S}^4(h_{(1)}) < \alpha, h_{(2)} > .$$

Multiplying with $< \alpha^{-1}, h_{(3)} >$, we find

$$a(\alpha^{-1} \rightharpoonup h \leftharpoonup \alpha)a^{-1} = a(< \alpha, h_{(1)} > h_{(2)} < \alpha^{-1}, h_{(3)} >)a^{-1} = \mathcal{S}^4(h),$$

which finishes the proof. □

Theorem (3.8) has important consequences:

Corollary 3.9. *The order of the antipode is finite.*

Proof. Since H is finite, and distinct powers of a grouplike element are linearly independent (being themselves grouplikes), every grouplike element in H and also in H^* has finite order. Then, by Radford's formula, $\mathcal{S}^4$ and then $\mathcal{S}$ have finite order. □

Corollary 3.10 (Larson, 1971).
a) If H is unimodular, then $\mathcal{S}^4$ coincides with the inner automorphism of H induced by a grouplike element. In particular the order of the antipode is at most $4 \dim H$.
b) If H and H^* are unimodular, then $\mathcal{S}^4 = \mathrm{id}$. □

We want to show now an important trace formula involving the antipode. For this, we need the following lemmas.

Lemma 3.11. *Let A be a Frobenius algebra with Frobenius homomorphism ϕ and dual bases (r_i, l_i).*
Let $\alpha \in k$, $e \in A$, such that $e^2 = \alpha e$. If $f \in \mathrm{End}(eA)$ is a k-linear endomorphism of eA, then:
i) $\alpha \operatorname{Tr}(f) =< \phi, \sum_i f(el_i)r_i >$.
ii) $\alpha \operatorname{Tr}(f) =< \phi, \sum_i l_i f(er_i) >$.

Proof.
$\forall x \in A$, we have that $ex = \sum_i < \phi, exr_i > l_i$, then $\alpha ex = \sum_i < \phi, exr_i > el_i$. Thus, $\alpha f(ex) = \sum_i < \phi, exr_i > f(el_i)$.
Hence under the canonical isomorphism $(eA)^* \otimes eA \longrightarrow \mathrm{End}(eA)$,

$$\sum_i < \phi, \_r_i > \otimes f(el_i) \longmapsto \alpha f.$$

This proves i).
ii) is shown similarly. □

Definition. Let V be a finite dimensional left H-module, and let $\rho : H \longrightarrow \mathrm{End}(V)$ be the algebra map affording the module structure on V. Then the element $\mathcal{X}_V$ of H^*, defined by $< \mathcal{X}_V, h >= \operatorname{Tr}(\rho(h))$ is called the *character* of V.

Basic Properties. If V and W are finite dimensional H-modules then we have the following relations, whose verifications are left to the reader:
1) $< \mathcal{X}_V, 1 >= \dim V$.
2) $V \backsimeq W \Rightarrow \mathcal{X}_V = \mathcal{X}_W$.
3) $\mathcal{X}_{V \oplus W} = \mathcal{X}_V + \mathcal{X}_W$.
4) $\mathcal{X}_{V \otimes W} = \mathcal{X}_V \mathcal{X}_W$.
5) $\mathcal{X}_{V^*} = \mathcal{X}_V \circ \mathcal{S}$.

Later we will develop a more detailed study of the characters of the modules of a Hopf algebra. In the moment, we have the following lemma.

Lemma 3.12.
1) $\mathcal{X}_H{}^2 = (\dim H)\mathcal{X}_H$.
2) $\mathcal{S}^2(\mathcal{X}_H) = \mathcal{X}_H$ *in* H^*.

Proof.
1) Let V be any finite dimensional H-module. Denote by V_ϵ the trivial H-module structure in the underlying vector space V, i.e., the module structure given by $h.v =< \epsilon, h > v$, $\forall v \in V$, $h \in H$.

Then the map $H \otimes V_\epsilon \longrightarrow H \otimes V$, such that $h \otimes v \mapsto h_{(1)} \otimes h_{(2)}v$, defines an H-linear isomorphism.

This implies that $\mathcal{X}_H \mathcal{X}_{V_\epsilon} = \mathcal{X}_H \mathcal{X}_V$.

But $\mathcal{X}_{V_\epsilon} = (\dim V)\epsilon$. So we proved that $\mathcal{X}_H(\dim V) = \mathcal{X}_H \mathcal{X}_V$.

Specializing V in H, we get 1).

2) Let $h \in H$, then

$$< \mathcal{S}^2(\mathcal{X}_H), h >=< \mathcal{X}_H, \mathcal{S}^2(h) >= \mathrm{Tr}(L_{\mathcal{S}^2(h)}).$$

Now, as $\mathcal{S}^2$ is an algebra automorphism of H, we have that $\forall h \in H$,

$$\mathrm{Tr}(L_{\mathcal{S}^2(h)}) = \mathrm{Tr}(L_h) =< \mathcal{X}_H, h >,$$

and this proves 2). □

We are now in a position to give a short proof of the following important trace formula by Larson and Radford.

Theorem 3.13. *Let* $\gamma \in H^*$ *be a nonzero right integral, and let* $\Gamma \in H$ *be a left integral such that* $< \gamma, \Gamma >= 1$. *Then*

$$\mathrm{Tr}_{H^*}(\mathcal{S}^2) =< \epsilon, \Gamma >< \gamma, 1 >= (\dim H)\,\mathrm{Tr}(\mathcal{S}^2|_{\mathcal{X}_H H^*}).$$

Proof.
Let $\widetilde{\Gamma} \in H^{**}$, be defined by $< \widetilde{\Gamma}, h^* >=< h^*, \Gamma >$, $\forall h^* \in H^*$. Using the fact that γ is a Frobenius homomorphism in H with dual bases $(\Gamma_{(1)}, \mathcal{S}(\Gamma_{(2)}))$, it is easy to see that $\widetilde{\Gamma}$ is a Frobenius homomorphism in H^* with dual bases $(\mathcal{S}(\gamma_{(1)}), \gamma_{(2)})$. Applying lemma (3.11) to $\mathcal{S}^2 \in \mathrm{End}(H^*)$, taking $\alpha = 1$, $e = 1$, we get

$$\mathrm{Tr}(\mathcal{S}^2) =< \widetilde{\Gamma}, \mathcal{S}^2(\gamma_{(2)})\mathcal{S}(\gamma_{(1)}) >=< \widetilde{\Gamma}, < \gamma, 1 > \epsilon >=< \gamma, 1 >< \epsilon, \Gamma > .$$

Observe that this equality also follows from proposition (3.4) applied to $(H^{op})^{cop}$.

Now, by lemma (3.12), $\mathcal{S}^2|_{\mathcal{X}_H H^*}$ is an endomorphism of $\mathcal{X}_H H^*$ to which lemma 3.11 applies (with $\alpha = \dim H$, $e = \mathcal{X}_H$), giving that

$$(*) \quad (\dim H)\,\mathrm{Tr}(\mathcal{S}^2|_{\mathcal{X}_H H^*}) =< \widetilde{\Gamma}, \mathcal{S}^2(\mathcal{X}_H \gamma_{(2)})\mathcal{S}(\gamma_{(1)}) >=$$
$$< \widetilde{\Gamma}, \mathcal{S}^2(\mathcal{X}_H)\mathcal{S}^2(\gamma_{(2)})\mathcal{S}(\gamma_{(1)}) >=< \widetilde{\Gamma}, \mathcal{X}_H \mathcal{S}^2(\gamma_{(2)})\mathcal{S}(\gamma_{(1)}) >=< \gamma, 1 >< \mathcal{X}_H, \Gamma > .$$

Again by lemma 3.11, now taking f to be the left multiplication by Γ in H ($\alpha = 1$, $e = 1$), we have

$$< \mathcal{X}_H, \Gamma >=< \gamma, \mathcal{S}(\Gamma_{(2)})\Gamma\Gamma_{(1)} >=< \gamma, < \epsilon, \Gamma_{(2)} > \Gamma\Gamma_{(1)} >=< \epsilon, \Gamma >< \gamma, \Gamma >=< \epsilon, \Gamma > .$$

(The second equality because Γ is a left integral in H). Then, by $(*)$,

$$(\dim H)\,\mathrm{Tr}(\mathcal{S}^2|_{\mathcal{X}_H H^*}) =< \epsilon, \Gamma >< \gamma, 1 >,$$

which finishes the proof of the theorem. □

Another consequence of the trace formula is the following theorem, due to Larson and Radford (1988), on semisimple Hopf algebras over fields of characteristic zero.

Theorem 3.14 (Larson - Radford, 1988). *Let k be a field of characteristic zero, and let H be a finite Hopf algebra over k, then the following statements are equivalent:*

1) H is semisimple.

2) H^* is semisimple.

3) $\mathcal{S}^2 = \mathrm{id}$.

Proof.

We have proved in (3.5) that 3) implies 1) and 2). For a proof of the part 2) $\Rightarrow$ 1), see [7, Th. (3.3), p. 276].

We show now that 1) and 2) together imply 3).

Suppose that H and H^* are both semisimple. Then they are unimodular, and so $\mathcal{S}^4 = (\mathcal{S}^2)^2 = \mathrm{id}$ by (3.10). Hence, the eigenvalues of $\mathcal{S}^2$ and $\mathcal{S}^2|_{\mathcal{X}_H H^*}$ are all 1 or -1. Call them, respectively, μ_j, η_i, $1 \le j \le n = \dim H$, $1 \le i \le m = \dim \mathcal{X}_H H^*$.

Then

$$\mathrm{Tr}_{H^*}(\mathcal{S}^2) = \sum_{j=1}^{n} \mu_j, \quad \text{and} \quad \mathrm{Tr}_{H^*}(\mathcal{S}^2|_{\mathcal{X}_H H^*}) = \sum_{i=1}^{m} \eta_i.$$

So, by theorem (3.13),

$$\sum_{j=1}^{n} \mu_j = n \sum_{i=1}^{m} \eta_i,$$

implying that

$$n| \sum_{i=1}^{m} \eta_i \,| \le \sum_{j=1}^{n} |\mu_j| = n.$$

As H and H^* are semisimple, $\sum_{i=1}^{m} \eta_i \neq 0$ by (3.5). So, $\sum_{i=1}^{m} \eta_i = \pm 1$, or $\sum_{j=1}^{n} \mu_j = \pm n$.

But, as there is at least one μ_j which equals 1 (since $\mathcal{S}^2(1_{H^*}) = 1_{H^*}$), then all μ_j must equal 1, thus $\mathcal{S}^2 = \mathrm{id}$. □

Example. Let H be the Taft algebra of dimension N^2, $N \geq 2$.

Keeping the notations introduced in §1, we have $\mathcal{S}(g) = g^{-1}$, $\mathcal{S}(x) = -xg^{-1}$. Then

$$\mathcal{S}^2(g) = g, \quad \mathcal{S}^2(x) = gxg^{-1}.$$

So that $\mathcal{S}^2$ is the inner automorphism of H induced by g. Then, as the order of g in the group of units of H is N, the order of $\mathcal{S}^2$ is also N. In particular, $\mathcal{S}^{2N} = \mathrm{id}$.

Now, suppose $\mathcal{S}^r = \mathrm{id}$. Since the only powers of $\mathcal{S}$ that are algebra maps are the even powers ($\mathcal{S}$ being an antialgebra map), it must be $r = 2q$, $q \in \mathbb{N}$. Then N divides q, so $2N$ divides r, and this proves that the order of $\mathcal{S}$ is $2N$.

The Nichols-Zoeller Theorem.

We consider now (in the context of finite Hopf algebras) another Kaplansky's conjecture, namely, whether a Hopf algebra H is free over any Hopf subalgebra. If H is a finite Hopf algebra, then the Nichols-Zoeller theorem gives a positive answer to this question.

If H is a Hopf algebra, then a subalgebra R of H is called a *Hopf subalgebra,* if $\Delta(R) \subseteq R \otimes R$ and $\mathcal{S}(R) \subseteq R$.

Remark. A finite dimensional subbialgebra R of a Hopf algebra H (i.e., a subalgebra R such that $\Delta(R) \subseteq R \otimes R$) is a Hopf subalgebra.

Indeed, we have to show that $\mathrm{id}_R \in \mathrm{End}(R)$ is invertible. But id_R is invertible in $\mathrm{Hom}(H, R)$ (which contains $\mathrm{End}(R)$ via the inclusion $R \to H$), since H has an antipode. Therefore convolution with id_R is injective in $\mathrm{End}(R)$, and hence bijective since $\mathrm{End}(R)$ is finite dimensional. Thus $\mathrm{id}_R \in \mathrm{End}(R)$ is invertible.

Theorem 3.15. (Nichols-Zoeller, 1989). *Let H be a finite Hopf algebra, and let $R \subseteq H$ be a Hopf subalgebra. Then H is a free R-module.*

Corollary 3.16. "Lagrange's Theorem for Hopf algebras". *If $R \subseteq H$ are finite Hopf algebras, then the order of R divides the order of H.* □

In order to prove the theorem, we need a series of lemmas.

Definition. A finite dimensional k-algebra R is called a *quasi-Frobenius algebra,* if the R-modules ${}_RR$ and R_R are injective.

Recall that for an algebra R, a left R-module M is called *faithful,* if its annihilator $\mathrm{Ann}(M) := \{r \in R : rM = 0\}$ equals 0.

Lemma 3.17. *Let R be a finite dimensional quasi-Frobenius algebra, and let M be a finitely generated left R-module. Then M is faithful if and only if there exist a free left R-module $F \neq 0$, and a non faithful left R-module N, such that*

$$M^r \backsimeq F \oplus N,$$

for some integer $r \geq 1$.

Proof. Follows from [1, Th. (59.3), p. 404]. □

Let now H be a Hopf algebra, and let $R \subseteq H$ be a subalgebra such that $\Delta(R) \subseteq H \otimes R$.

If M is a left R-module, and we consider H as a trivial R-module (i.e., $r.h =< \epsilon, r > h$, $\forall r \in R, h \in H$), then $H \otimes_R M$ is a left R-module via

$$R \xrightarrow{\Delta} H \otimes R \to \mathrm{End}(H) \otimes \mathrm{End}(M) \to \mathrm{End}(H \otimes M),$$

that is,

$$r.(h \otimes m) =< \epsilon, r_{(1)} > h \otimes r_{(2)}.m = h \otimes r.m, \tag{1}$$

for $r \in R$, $h \in H$ and $m \in M$. In fact, $H \otimes {}_{\cdot}M \backsimeq M^{\dim H}$ as left R-modules.

Also, if ${}_{\cdot}H$ denotes the left R-module structure on H given by left multiplication, then ${}_{\cdot}H \otimes {}_{\cdot}M$ is a left R-module via

$$r.(h \otimes m) = r_{(1)}h \otimes r_{(2)}.m. \tag{2}$$

Remark. Observe that the R-actions considered on H are both restrictions to R of the analogous H-actions. Thus the fact that $\Delta(R) \subseteq H \otimes R$ allowed us to give $H \otimes {}_{\cdot}M$ and ${}_{\cdot}H \otimes {}_{\cdot}M$ a left R-module structure, as in (1) and (2).

With this in mind, we have:

Lemma 3.18. *Let $R \subseteq H$ be a subalgebra such that $\Delta(R) \subseteq H \otimes R$. Suppose that the antipode, $\mathcal{S}$, of H is bijective. Then, $\forall n \in \mathbb{N}$,*

1) $H \otimes {}_{\cdot}R^n \backsimeq {}_{\cdot}H \otimes {}_{\cdot}R^n$, as left R-modules.

2) $H \otimes {}_{\cdot}H^n \backsimeq {}_{\cdot}H \otimes {}_{\cdot}H^n$, as left H-modules.

Proof.

1) It is enough to show it in the case $n = 1$. For this, define $\phi : H \otimes {}_{\cdot}R \rightarrow {}_{\cdot}H \otimes {}_{\cdot}R$, by $\phi(h \otimes r) = r_{(1)}h \otimes r_{(2)}$.

ϕ is well defined since $\Delta(R) \subseteq H \otimes R$, and it is clear that it is R-linear.

Moreover, the map $\psi : {}_{\cdot}H \otimes {}_{\cdot}R \rightarrow H \otimes {}_{\cdot}R$, given by $\psi(h \otimes r) = \overline{\mathcal{S}}(r_{(1)})h \otimes r_{(2)}$, is inverse to ϕ (where $\overline{\mathcal{S}}$ denotes the composition inverse of the antipode $\mathcal{S}$).

So ϕ is an R-isomorphism, and this proves 1).

2) follows from 1) by taking $R = H$. $\square$

Denote, for any subalgebra R of H, $R^+ := R \bigcap \ker(\epsilon)$. It is immediate that R^+H is an R-submodule of ${}_{\cdot}H$. In particular, the quotient space H/R^+H is a left R-module, we have also that for $r \in R$, $\overline{r} = \overline{\epsilon(r)1}$, where $\overline{r}$ denotes the class of r in H/R^+H.

Lemma 3.19. *Let $R \subseteq H$ be a subalgebra of H as in Lemma 3.18, then*

$$H \otimes_R H \backsimeq {}_{\cdot}H \otimes (H/R^+H),$$

as left H-modules.

Proof.

Define $\phi : H \otimes_R H \rightarrow {}_{\cdot}H \otimes (H/R^+H)$, by $\phi(x \otimes y) = xy_{(1)} \otimes \overline{y_{(2)}}$.

To see that ϕ is well defined, let $r \in R$, then

$$\phi(x \otimes ry) = xr_{(1)}y_{(1)} \otimes \overline{r_{(2)}y_{(2)}} = xr_{(1)}y_{(1)} \otimes < \epsilon, r_{(2)} > \overline{y_{(2)}} = xry_{(1)} \otimes \overline{y_{(2)}} = \phi(xr \otimes y).$$

Clearly ϕ is H-linear. Moreover, the map $\psi : {}_{\cdot}H \otimes (H/R^+H) \rightarrow H \otimes_R H$ given by $\psi(x \otimes \overline{y}) = x\mathcal{S}(y_{(1)}) \otimes y_{(2)}$, is inverse of ϕ (ψ is well-defined because $\Delta(R) \subseteq H \otimes R$). So ϕ is an isomorphism of H-modules, as claimed. $\square$

An *augmented algebra* is a pair (R, ϵ), where R is a finite dimensional k-algebra and $\epsilon : R \longrightarrow k$ is an algebra map. In particular, if H is a Hopf algebra with counit ϵ, (R, ϵ) is an augmented algebra for every subalgebra R of H.

Observe that if (R, ϵ) is augmented, then we may consider $k \in {}_R\mathcal{M}$ via ϵ.

Lemma 3.20. *Let R be a finite dimensional augmented k-algebra, and let M be a finitely generated left R-module such that M^n is free over R for some $n \geq 1$. Then M is free over R.*

Proof.

By hypotheses, $M^n \backsimeq R^m$, for some $m \in \mathbb{N}$. Then

$$(M \otimes_R k)^n \backsimeq (R \otimes_R k)^m \backsimeq k^m.$$

Comparing dimensions, we get that $m = nd$, where $d = \dim(M \otimes_R k)$. Hence,

$$M^n \backsimeq R^m \backsimeq (R^d)^n.$$

Now, by the Krull-Schmidt theorem (see [1, Th. (14.5), p. 83]), $M \backsimeq R^d$ is free over R. $\square$

We finally have:

Proof of the Nichols-Zoeller'Theorem.

If R is a finite dimensional Frobenius algebra, then R is a quasi-Frobenius algebra (see for instance [1, Th. (61.3), p. 414]).

Also, if R is a Hopf subalgebra of H, as R itself is a finite Hopf algebra, it follows from theorem (2.3) that R is a Frobenius algebra. Then we may apply the preceding lemmas.

Consider the left R-module ${}_{.}H$. As ${}_{.}H$ is a faithful R-module, by lemma (3.17), ${}_{.}H^r \backsimeq F \oplus N$, for some $r \geq 1$, where $F \backsimeq R^m$ is a free left R-module, and N is a non faithful left R-module.

Observe that, calling $t := \dim H$,

$$F^t \oplus N^t \backsimeq {}_{.}H^{rt} \backsimeq H \otimes {}_{.}H^r \underset{\text{by lemma 3.18}}{\backsimeq} {}_{.}H \otimes {}_{.}H^r \backsimeq$$
$$({}_{.}H \otimes {}_{.}F) \oplus ({}_{.}H \otimes {}_{.}N) \underset{\text{by lemma 3.18}}{\backsimeq} F^t \oplus ({}_{.}H \otimes {}_{.}N).$$

Then, by the Krull-Schmidt theorem, it follows that $N^t \backsimeq {}_{.}H \otimes {}_{.}N$. Now, we have a surjection of R-modules

$$N^t \backsimeq {}_{.}H \otimes {}_{.}N \xrightarrow{\text{id} \otimes \text{can}} {}_{.}H \otimes {}_{.}(N/R^+N).$$

But, as R acts trivially on (N/R^+N) and ${}_{.}H$ is a faithful R-module, ${}_{.}H \otimes (N/R^+N)$ is faithful. So, as N is not faithful, $N/R^+N = 0$. Hence, we find that

$$(*) \qquad (H/R^+H)^r \backsimeq (R/R^+R)^m \oplus (N/R^+N) \backsimeq (R/R^+R)^m \backsimeq k^m.$$

We have also that

$$H\otimes_R H^r \backsimeq (H\otimes_R F)\oplus(H\otimes_R N)\backsimeq H^m\oplus(H\otimes_R N),$$

and on the other hand,

$$H\otimes_R H^r \backsimeq (H\otimes_R H)^r \underset{\text{by lemma (3.19)}}{\backsimeq} (H\otimes H/R^+H)^r \backsimeq$$
$$H\otimes(H/R^+H)^r \underset{\text{by}(*)}{\backsimeq} H\otimes k^m \backsimeq H^m.$$

So $H\otimes_R N=0$.

But the inclusion $R_R\subseteq H_R$ is R-direct, since R_R is injective. Thus,

$$N\backsimeq R\otimes_R N\hookrightarrow H\otimes_R N=0.$$

Then $N=0$, implying that $H^r\backsimeq F$ is free over R, and by lemma (3.20), that H is free over R. □

Remark. It is possible to show that if R is a subalgebra of R such that $\Delta(R)\subseteq H\otimes R$, the following statements are equivalent:

1) R is a Frobenius algebra.
2) R is a quasi-Frobenius algebra.
3) ${}_RH$ and H_R are R-free.

An open problem is whether a subalgebra R of H satisfying $\Delta(R)\subseteq H\otimes R$ is *always* a Frobenius algebra.

§4 Character Theory for Finite Hopf algebras

We want to develop now a character theory for finite semisimple Hopf algebras, similar to that when $H = kG$, the group algebra of a finite group G (see references [1] or [3] on the subject).

From now on, k will denote an algebraically closed field of characteristic 0, and H will be a finite semisimple Hopf algebra over k. By the theorem of Larson and Radford (3.14) we know that H^* is also semisimple and $\mathcal{S}^2 = \mathrm{id}$.

As H is semisimple, every finite dimensional irreducible H-module is isomorphic to a direct summand of H. Then, there exist only a *finite* number of such modules up to isomorphism (because H is finite). We denote them by them $V_1, \dots, V_n$, $V_1 = k_\epsilon$.

Definition. The *irreducible characters* of H are by definition the characters of the irreducible H-modules $V_1, \dots, V_n$.

We denote by $\mathcal{X}_i := \mathcal{X}_{V_i}$, and by $\mathcal{X}_{\bar{i}} := \mathcal{X}_{V_i{}^*}$.

The *character rings* of H are defined to be the following subrings of H^*:

$$R_{\mathbb{Q}}(H) := \sum_{i=1}^{n} \mathbb{Q}\mathcal{X}_i, \quad \text{and} \quad R_k(H) := \sum_{i=1}^{n} k\mathcal{X}_i.$$

These are in fact subrings by the basic properties of the characters, see the paragraph before Lemma 3.12.

We then have the inclusions

$$R_{\mathbb{Q}}(H) \subseteq R_k(H) \subseteq H^*.$$

Remark. With the above definition, we get that the character of the left regular representation of H may be written in the form

$$\mathcal{X}_H = \sum_{i=1}^{n} n_i \mathcal{X}_i,$$

where n_i are integers, $n_i \geq 1$, and $n_1 = 1$. Observe also that $\mathcal{X}_1 = \epsilon$.

Let V, W be left H-modules. Then H acts on $\mathrm{Hom}(W, V)$, in the form $(h.\phi)(w) = h_{(1)}.\phi(\mathcal{S}(h_{(2)}).w)$.

Lemma 4.1. *Let V, W as above, then $\mathrm{Hom}_H(W, V) = \mathrm{Hom}(W, V)^H$, the isotypic component of trivial type in $\mathrm{Hom}(W, V)$.*

Proof. Let $\phi : W \to V$ be an H-linear map, and let $h \in H$, $w \in W$. Then

$$(h.\phi)(w) = h_{(1)}.\phi(\mathcal{S}(h_{(2)}).w) = h_{(1)}\mathcal{S}(h_{(2)}).\phi(w) =< \epsilon, h > \phi(w).$$

So $\phi \in \mathrm{Hom}(W, V)^H$.

Conversely, suppose $\phi \in \mathrm{Hom}(W, V)^H$, and let $h \in H$, $w \in W$. We have

$$\phi(h.w) =< \epsilon, h_{(1)} > \phi(h_{(2)}.w) = (h_{(1)}.\phi)(h_{(2)}.w) =$$
$$h_{(1)}.\phi(\mathcal{S}(h_{(2)})h_{(3)}.w) = h_{(1)} < \epsilon, h_{(2)} > .\phi(w) = h.\phi(w).$$

So $\phi \in \mathrm{Hom}_H(W, V)$. $\square$

If V, W be finite dimensional H-modules. Then we have a canonical k-isomorphism $V \otimes W^* \backsimeq \mathrm{Hom}(W, V)$, given by $(v \otimes \phi)(w) =< \phi, w > v$.

This defines an H-linear isomorphism. So in particular, $\mathcal{X}_{\mathrm{Hom}(W,V)} = \mathcal{X}_V \mathcal{X}_{W^*}$.

Lemma 4.2. (Schur's lemma). *Let V, W be irreducible H-modules, then $\mathrm{Hom}_H(W, V) = \delta_{V,W} k$. (Here $\delta_{V,W}$ equals 0 if V and W are non isomorphic, and 1 if they are isomorphic).*

Proof.

As V and W are irreducible, any H-linear map $\phi : W \longrightarrow V$ must be zero or an isomorphism. Thus, if V and W are not isomorphic, $\mathrm{Hom}_H(W, V) = 0$.

Now, let $\phi : V \longrightarrow V$ be an H-linear map. As k is algebraically closed, we may choose an eigenvalue of ϕ, $a \in k$. Hence, $\ker(\phi - a\,\mathrm{id}) \neq 0$. And by the irreducibility of V, $\ker(\phi - a\,\mathrm{id}) = V$. So $\phi = a\,\mathrm{id}$.

This defines a map $\mathrm{Hom}_H(W, V) \longrightarrow k$, which is clearly an isomorphism. □

(4.1) and (4.2) imply

Corollary 4.3. *Let $1 \leq i, j \leq n$, then*

$$\mathcal{X}_i \mathcal{X}_{\bar{j}} = \delta_{ij} \mathcal{X}_1 + \sum_{k \geq 2} c_k \mathcal{X}_k,$$

for some non negative integers c_k. □

As H is a semisimple k-algebra, applying Wedderburn's theorem [1, Th. (26.4), p.175], H is isomorphic to a product of full matrix algebras over skew fields of finite degree over k. Now, as k is algebraically closed, every such skew field must coincide with k. Thus

$$(*) \qquad H \backsimeq \prod_{i=1}^{n} M_{n_i}(k).$$

Moreover, we can assume that V_i is the natural representation of $M_{n_i}(k)$ of dimension n_i, then V_i is an irreducible H-module, and we have an H-isomorphism: $M_{n_i}(k) \backsimeq {V_i}^{n_i}$.

Call $E_i \in M_{n_i}(k)$ the $n_i \times n_i$ identity matrix, and let $e_i \in H$ be the element which corresponds to $(0, \ldots, E_i, \ldots, 0)$ via the isomorphism $(*)$.

Then, the e_i form a set of orthogonal idempotents in H, that is,

$$e_i e_j = 0, \quad \text{if } i \neq j,$$
$${e_i}^2 = e_i,$$
$$e_1 + \cdots + e_m = 1.$$

In particular, $H = \bigoplus He_i$.

We have, for $1 \leq i \leq n$, that $He_i \backsimeq M_{n_i}(k)$, hence $He_i \backsimeq {V_i}^{n_i}$.

As a consequence, we get

Proposition 4.4. *Each V_i occurs in the left regular representation of H with multiplicity equals to its k-dimension: $n_i = \mathcal{X}_i(1)$. In terms of characters, we have*

$$\mathcal{X}_H = \sum_{i=1}^{n} n_i \mathcal{X}_i$$

In particular, $\dim H = \sum_{i=1}^{n} {n_i}^2$. □

It is clear also, from $(*)$, that if $Z(H)$ denotes the center of H, then

$$Z(H) = \sum_{i=1}^{n} k e_i.$$

Observe that e_i acts as the identity on V_i and anihilates V_j, $\forall j \neq i$. That is,

$$\mathcal{X}_i(e_i) = n_i, \quad \text{and } \mathcal{X}_j(e_i) = 0, \text{if } j \neq i.$$

Proposition 4.5. *Let $\lambda \in H^*$ be a nonzero integral such that $< \lambda, 1 >= 1$. Then $Z(H)\lambda = R_k(H)$.*

Proof. As $Z(H) = \sum_{i=1}^{n} k e_i$, the claim will be proved if we show that

$$e_i \lambda = (\dim H)^{-1} n_i \mathcal{X}_i.$$

Observe that as $< \lambda, 1 >= 1$, then $\mathcal{X}_H = (\dim H)\lambda$, by (3.4).

Now, if $h \in H$, then

$$< e_i\lambda, h >=< \lambda, he_i >= (\dim H)^{-1} < \mathcal{X}_H, he_i >=$$
$$(\dim H)^{-1} < \mathrm{Tr}_{He_i}, h >= (\dim H)^{-1} < n_i \mathcal{X}_i, h >= (\dim H)^{-1} n_i < \mathcal{X}_i, h > .$$

□

Let $\Lambda \in H$ be an integral such that $< \lambda, \Lambda >= 1$. Then we have, as H and H^* are unimodular, that λ is a Frobenius homomorphism of H with dual bases $(\Lambda_{(1)}, \mathcal{S}(\Lambda_{(2)}))$.

This gives the following

Corollary 4.6. *Let $1 \leq i \leq n$, then*

$$(\dim H/n_i)\ e_i = \Lambda_{(1)} < \mathcal{X}_i, \mathcal{S}(\Lambda_{(2)}) > .$$

Proof. Using the identity $e_i\lambda = (\dim H)^{-1} n_i \mathcal{X}_i$, we compute

$$(\dim H)^{-1} n_i \Lambda_{(1)} < \mathcal{X}_i, \mathcal{S}(\Lambda_{(2)}) >= \Lambda_{(1)} < e_i\lambda, \mathcal{S}(\Lambda_{(2)}) >= \Lambda_{(1)} < \lambda, \mathcal{S}(\Lambda_{(2)})e_i >= e_i.$$ □

Remark. When $H = kG$, the group algebra of a finite group G, then for $\Lambda = \sum_{g\in G} g$, corollary (4.6) says that

$$(|G|/n_i)\ e_i = \sum_{g\in G} g < \mathcal{X}_i, g^{-1} >.$$

Now, as G is a finite group, $\rho_i(g)$ has finite order as an element of $GL(V_i)$, $\forall g \in G$ (where, as usual, ρ_i denotes the representation of $H = kG$ in V_i).

Hence the eigenvalues of $\rho_i(g)$ are roots of unity in k. In particular, they are all contained in a subring R of algebraic integers such that R is finitely generated as $\mathbb{Z}$-module. Any element of the group algebra RG is integral over $\mathbb{Z}$ (since it generates a subring which is finitely generated as $\mathbb{Z}$-module). Hence $(|G|/n_i)\ e_i$ is integral, and $|G|/n_i$ is an algebraic integer.

But $|G|/n_i$ is a rational number, so it must be an integer. Then n_i divides $|G|$.

We have seen then that, for a finite group G, the dimensions of the irreducible representations of G *divide* the order of G.

We want to prove now a theorem on orthogonality of characters due to Larson (1971).

Recall that for $f \in H^*$, $< \mathrm{Tr}_{H^*}, f >= \mathrm{Tr}(L_f)$. Define for $1 \le i, j \le n$, $(\mathcal{X}_i, \mathcal{X}_j) :=< \mathrm{Tr}_{H^*}, \mathcal{X}_i \mathcal{X}_{\bar{j}} >$.

Theorem 4.7 (Orthogonality relations). *Let $1 \le i, j \le n$, then*

$$(\mathcal{X}_i, \mathcal{X}_j) = \delta_{ij} \dim H.$$

Proof.

By corollary (4.6), we have that for $1 \le i, j \le n$, $\mathcal{X}_i \mathcal{X}_{\bar{j}} = \delta_{ij}\mathcal{X}_1 + \sum_{k\ge 2} c_k \mathcal{X}_k$, with $c_k \ge 0$. Then,

$$(\mathcal{X}_i, \mathcal{X}_j) =< \mathrm{Tr}_{H^*}, \mathcal{X}_i \mathcal{X}_{\bar{j}} >= \delta_{ij} \dim H + \sum_{k\ge 2} c_k < \mathrm{Tr}_{H^*}, \mathcal{X}_k >.$$

(Observe that $< \mathrm{Tr}_{H^*}, \mathcal{X}_1 >=< \mathrm{Tr}_{H^*}, \epsilon >= \dim H^* = \dim H$).

We claim that $< \mathrm{Tr}_{H^*}, \mathcal{X}_k >= 0$, for all $k \ge 2$.

From (3.4), we know that if the integrals $\Lambda \in H$, $\lambda \in H^*$ are chosen as above, then $\mathrm{Tr}_{H^*} = (\dim H)\ \widetilde{\Lambda}$, (where $< \widetilde{\Lambda}, h^* >=< h^*, \Lambda >$, $\forall h^* \in H^*$).

Now, as H is semisimple, and thus unimodular, the space of integrals is contained in the center of H.

Let then $k \ge 2$, and let $\rho_k : H \to \mathrm{End}(V_k)$ denote the algebra map affording the H-module structure in V_k. Then the image of the integral is an H-linear map since the integral is central. By Schur's Lemma (4.2) there exists an element $a \in k$ such that $\rho_k(\Lambda) = a\,\mathrm{id}$.

Let $h \in H^+ = \ker(\epsilon)$. We have

$$a\rho_k(h) = \rho_k(\Lambda)\rho_k(h) = \rho_k(\Lambda h) =< \epsilon, h > \rho_k(\Lambda) = 0.$$

Now, as $k \ge 2$, we may find $h \in H^+$ such that $\rho_k(h) \ne 0$, and this implies that $a = 0$. But then $\Lambda.V_k = 0$, so $< \mathrm{Tr}_{H^*}, \mathcal{X}_k >=< \mathcal{X}_k, \Lambda >= 0$, as we claimed. $\square$

Corollary 4.8. *The irreducible characters of H, $\mathcal{X}_1, \dots, \mathcal{X}_n$, are k-linearly independent in H^*, and the map $R_{\mathbb{Q}}(H) \otimes_{\mathbb{Q}} k \to R_k(H)$, $x \otimes 1 \mapsto x$, is an isomorphism of k-algebras.* □

Theorem (4.7) implies, moreover, that $(\dim H)^{-1/2}\mathcal{X}_i$, $1 \le i \le n$, is an orthonormal basis of $R_k(H)$ with respect to the form $(\ ,\ )$.

In particular, if V is a finite dimensional module for H, then its character $\mathcal{X}_V$ is expressible in a unique way as a linear combination

$$\mathcal{X}_V = \sum_i m_i \mathcal{X}_i, \tag{1}$$

where $m_i = (\dim H)^{-1}(\mathcal{X}_V, \mathcal{X}_i)$. So that if V, W are finite dimensional H-modules, $V \backsimeq W$ iff $\mathcal{X}_V = \mathcal{X}_W$.

Remark. As H is semisimple (and thus $\mathcal{S}^2 = \mathrm{id}$), we have that for every finite dimensional H-module V, $V^{**} \backsimeq V$ as H-modules.

Also, if W is a finite dimensional H-module, the canonical isomorphism $(V \otimes W)^* \backsimeq W^* \otimes V^*$ is an H-isomorphism.

Putting these together, we find that the map $x \mapsto \overline{x}$, defined by $\mathcal{X}_i \mapsto \mathcal{X}_{\bar{i}}$, gives an involutory antialgebra map in $R_k(H)$ (and also in $R_{\mathbb{Q}}(H)$).

Corollary (4.8) says that $R_k(H)$ is obtained by $R_{\mathbb{Q}}(H)$ by extension of scalars. Using this fact, we will prove the following result, which is due to Zhu (1994).

Theorem 4.9. *$R_k(H)$ is a semisimple k-algebra.*

Proof. We first show that $R_{\mathbb{Q}}(H)$ is semisimple.

For this, observe that if $0 \ne x \in R_{\mathbb{Q}}(H)$, say $x = \sum_i x_i \mathcal{X}_i$, $x_i \in \mathbb{Q}$, then by (4.3)

$$x\overline{x} = \sum_{i,j} x_i x_j \mathcal{X}_i \mathcal{X}_{\bar{j}} = \sum_{i,j} x_i x_j \ (\delta_{ij}\mathcal{X}_1 + \sum_{k \ge 2} c_{ijk}\mathcal{X}_k) = (\sum_i {x_i}^2)\ \mathcal{X}_1 + \sum_{k \ge 2} b_k \mathcal{X}_k,$$

for some coefficients c_{ijk} and some rational numbers b_k.

And, as $x_i \subset \mathbb{Q}$ are not all zero, $\sum_i {x_i}^2 \ne 0$, so $x\overline{x} \ne 0$.

Suppose now that there exists $0 \ne x \in \mathrm{rad}(R_{\mathbb{Q}}(H))$. Call $y := x\overline{x}$. Then $y \ne 0$ and $y \in \mathrm{rad}(R_{\mathbb{Q}}(H))$. Moreover, $\overline{y} = y$.

So, $y^2 = y\overline{y} \ne 0$, $y^4 = y^2\overline{y^2} \ne 0$, and in general $y^{2^t} = y^{2^{t-1}}\overline{y^{2^{t-1}}} \ne 0$, for all $t \ge 1$.

But this is absurd, since all the elements in $\mathrm{rad}(R_{\mathbb{Q}}(H))$ are nilpotent.

Then x must equal 0, so $\mathrm{rad}(R_{\mathbb{Q}}(H)) = 0$ and $R_{\mathbb{Q}}(H)$ is semisimple.

By the results in [1, §69, p. 459], as $R_{\mathbb{Q}}(H)$ is semisimple, then $R_{\overline{\mathbb{Q}}}$ also is. Then $R_{\overline{\mathbb{Q}}}(H)$ is a direct product

$$R_{\overline{\mathbb{Q}}} = \prod M_{n_i}(\overline{\mathbb{Q}}),$$

of full matrix algebras over $\overline{\mathbb{Q}}$. But as k is algebraically closed and $\mathrm{char}\, k = 0$, $\overline{\mathbb{Q}} \subseteq k$, and we also have

$$M_{n_i}(\overline{\mathbb{Q}}) \otimes_{\overline{\mathbb{Q}}} k \backsimeq M_{n_i}(k).$$

Now, as $R_k(H)$ is the extension by scalars of $R_{\overline{\mathbb{Q}}}(H)$, $R_k(H)$ is semisimple, as we claimed. □

The Class Equation for Hopf algebras.

We state now some results concerning algebraic number theory, that will be needed in the sequel. The reader can find in [1, Ch. III] the proofs of these results.

Definition. An integral domain R is called a *Dedekind domain,* if it satisfies the following conditions:

i) R is a noetherian ring.

ii) Every non-zero prime ideal in R is maximal.

iii) R is integrally closed in its field of quotients, K. (That is, if $a \in K$ is integral over R, then $a \in R$).

If M is a torsion free module over a Dedekind domain R, then the *rank* of M is the dimension of $M \otimes_R K$ over K. If M is finitely generated, then it has finite rank.

Let K be an algebraic number field (i.e., a finite extension of the field $\mathbb{Q}$ of rational numbers), and let R denote the ring of integers of K, $R = \{a \in K : a \text{ is an algebraic integer}\}$. Then R is a Dedekind domain (whose field of quotients is K).

If R is an integral domain, and K is its field of quotients, a finitely generated R-submodule $0 \neq I$ of K, is called a *fractional ideal* of R.

Proposition 4.10. *Let M be a finitely generated, projective module of rank t over a Dedekind domain R. Then there exist $m_1, \ldots, m_t \in M$, and fractional ideals $I_1, \ldots, I_t$ of R such that*

$$M = I_1 m_1 + \cdots + I_t m_t,$$

where the indicated sum is direct. □

Lemma 4.11. *Let K be an algebraic number field, R its ring of integers, and call $\overline{K}$ the algebraic closure of K.*

Suppose A is an R-algebra finitely generated and projective as an R-module, such that $A \otimes_R K$ is semisimple.

Then, there exists an isomorphism of $\overline{K}$-algebras

$$A \otimes_R \overline{K} \to \prod_{\alpha=1}^{s} M_{n_\alpha}(\overline{K}), \quad e_{\alpha_{ij}} \mapsto E_{\alpha_{ij}},$$

for some $s \geq 1$, and natural numbers n_α (where $E_{\alpha_{ij}}$ denotes the s-tuple consisting of all zeros, except for the α-place, where it equals the $n_\alpha \times n_\alpha$ matrix whose entries are $a_{kl} = \delta_{ik}\delta_{jl}$), such that every $a \in A$ may be written in the form

$$a = \sum_{\alpha,i,j} r_{\alpha_{ij}} e_{\alpha_{ij}},$$

with $r_{\alpha_{ij}}$ algebraic integers.

Proof.

(Observe that we are identifying $a \in A$ with $a \otimes 1$ in $A \otimes_R \overline{K}$).

As $A \otimes_R \overline{K} \backsimeq (A \otimes_R K) \otimes_K \overline{K}$, then $A \otimes_R \overline{K}$ is semisimple, and we may assume that

$$A \otimes_R \overline{K} \simeq \prod_{\alpha=1}^{s} \mathrm{End}_{\overline{K}}(V_\alpha),$$

where V_α are irreducible $A \otimes_R \overline{K}$-modules (say, of dimension n_α).

The claim will be proved if we can show that for each irreducible $A \otimes_R \overline{K}$-module, there exists a basis over $\overline{K}$, such that the matrices representing elements of A in that basis, have all entries algebraic integers.

Now, let V be an irreducible $A \otimes_R \overline{K}$-module, with $\overline{K}$-basis $v_1, \ldots, v_t$. The matrices representing elements of A in this basis have all entries in a finite field extension of K (since A is finitely generated over R). Instead of extending K we may assume that all these entries are in K.

Call $U := \sum_i Av_i \subseteq V$. Then U is a finitely generated, projective R-module of rank t, and thus there exist $u_1, \ldots, u_t \in U$, and fractional ideals $I_1, \ldots, I_t$ of R such that

$$U = \sum_i I_i u_i.$$

Also, we may find $K \subseteq K'$, an algebraic number field extension ($R \subseteq R' =$ the ring of integers of K'), such that all fractional ideals in K become principal in K'. (See [1, Th. (20.14), p.130]).

In particular, there exist $s_i \in K'$, such that $R'I_i = R's_i$, for all $i = 1, \ldots, t$. Then

$$R'U = \sum_i R'I_i u_i = \sum_i R's_i u_i = \sum_i R'v_i{}'.$$

where $v_i{}' = s_i u_i$. Now, in the basis $(v_i{}')$, the matrices representing elements of $A \otimes_R R' \subseteq A \otimes_R K'$ have all entries in R', and thus are algebraic integers. It remains to observe the inclusion: $A = A \otimes_R R \subseteq A \otimes_R R'$. $\square$

Definition. Let A be a finite dimensional k-algebra. A k-linear map $t : A \longrightarrow k$, is called a *trace like* function if it satisfies the following conditions:

a) $\forall x, y \in A$, $t(xy) = t(yx)$.

b) If $0 \neq e$ is an idempotent in A, then $0 \neq t(e)$ is a natural number.

c) If e, f are nonzero idempotents in A, such that $eA \underset{A}{\backsimeq} fA$, then $t(e) = t(f)$.

Remark. Note that the usual trace map Tr_A is trace like. But also Tr_A restricted to any subalgebra B of A is trace like. Indeed, a) is clear, and b) follows since $\mathrm{Tr}_A(e) = \dim(eA)$. To prove c), note that $eB \otimes_B A \simeq eA$.

The following lemma is due, independently, to Kac (1971) and Zhu (1994).

A non-zero idempotent e in an algebra R is called *primitive,* if it can not be expressed as the sum of two non-zero orthogonal idempotents.

Lemma 4.12. *In the situation of lemma (4.11), let $t : A\otimes_R\overline{K} \to \overline{K}$ be a trace like function.*

Assume that there exist $0 \neq d \in \mathbb{N}$, and $a_i, b_i \in A$, $1 \leq i \leq n := \dim(A\otimes_R\overline{K})$, such that $t(a_k b_l) = \delta_{kl} d$, $\forall k, l$.

Then, if $0 \neq e \in A\otimes_R\overline{K}$ is a primitive idempotent, $t(e)$ divides d.

Proof. Keeping the notations in lemma (4.11), we may write

$$a_k = \sum_{\alpha,i,j} r_{k,\alpha_{ij}} e_{\alpha_{ij}}, \quad b_l = \sum_{\beta,\mu,\nu} s_{l,\beta_{\mu\nu}} e_{\beta_{\mu\nu}},$$

where $r_{k,\alpha_{ij}}$ and $s_{l,\beta_{\mu\nu}}$ are algebraic integers.

The $t(e_{\alpha_{ii}})$ are natural numbers. Since the $e_{\alpha_{ii}}$ form a complete set of orthogonal primitive idempotents, there is an α_{ii} such that e and $e_{\alpha_{ii}}$ generate isomorphic right ideals. Hence, by property c), $t(e) = t(e_{\alpha_{ii}})$.

In view of the relations

$$e_{\alpha_{ij}} e_{\beta_{\mu\nu}} = \delta_{\alpha,\beta}\delta_{\mu,j} e_{\alpha_{i\nu}}, \quad \forall \alpha, \beta, \mu, \nu, i, j \ ,$$

which, in particular, imply that for $\nu \neq i$

$$t(e_{\alpha_{i\nu}}) = t(e_{\alpha_{ii}} e_{\alpha_{i\nu}} - e_{\alpha_{i\nu}} e_{\alpha_{ii}}) = 0,$$

we get,

$$a_k b_l = \sum r_{k,\alpha_{ij}} s_{l,\beta_{\mu\nu}} e_{\alpha_{ij}} e_{\beta_{\mu\nu}} = \sum_{\alpha,i,j,\nu} r_{k,\alpha_{ij}} s_{l,\alpha_{j\nu}} e_{\alpha_{i\nu}},$$

and then

$$d\delta_{kl} = t(a_k b_l) = \sum_{\alpha,i,j,\nu} r_{k,\alpha_{ij}} s_{l,\alpha_{j\nu}} t(e_{\alpha_{i\nu}}) = \sum_{\alpha,i,j} r_{k,\alpha_{ij}} s_{l,\alpha_{ji}} t(e_{\alpha_{ii}}).$$

Since $n =$ number of all $e_{\alpha_{ij}}$: $1 \leq \alpha \leq s$, $1 \leq i, j \leq n_\alpha$, there is a bijection

$$\{1, \ldots, n\} \to \{\alpha_{ij} : 1 \leq \alpha \leq s \ , \ 1 \leq i, j \leq n_\alpha\}.$$

Define

$$a_{k,\alpha_{ij}} = r_{k,\alpha_{ij}} (t(e_{\alpha_{ii}})/d)^{1/2}, \quad b_{\alpha_{ij},l} = s_{l,\alpha_{ji}} (t(e_{\alpha_{ii}})/d)^{1/2}.$$

By the calculation above, the $n \times n$ matrices $A = (a_{k,\alpha_{ij}})$ and $B = (b_{\alpha_{ji},l})$ verify that $AB = \mathrm{id}$, but this implies that $BA = \mathrm{id}$.

Then $\forall \alpha, i$,

$$\sum_l b_{\alpha_{ii},l} a_{l,\alpha_{ii}} = 1, \quad \text{or} \ \sum_l s_{l,\alpha_{ii}} r_{l,\alpha_{ii}} = dt(e_{\alpha_{ii}})^{-1},$$

which is an algebraic integer. But as it is a rational number, it must be an integer. So $t(e_{\alpha_{ii}})$ divides d. $\square$

The following theorem is due to Kac and Zhu.[2]

Theorem 4.13. "Class Equation". *Let $\lambda \in H^*$ be an integral, such that $< \lambda, 1 >= 1$, and let $\lambda = e_1, e_2, \ldots, e_n$, be a complete set of orthogonal primitive idempotents in $R_k(H)$. Then*

$$\dim H = \sum_{i=1}^{n} \dim(e_i H^*),$$

with $\dim(e_1 H^*) = 1$, *and* $\dim(e_i H^*) \,/ \dim H$, $\forall 1 \leq i \leq n$.

Proof. Since $H^* = \bigoplus_i e_i \; H^*$, $\dim H = \dim H^* = \sum_{i=1}^{n} \dim(e_i H^*)$. It is clear also, as λ is an integral, that $\dim(e_1 H^*) = 1$.

Call $A = R_{\mathbb{Z}}(H) = \sum_i \mathbb{Z} \; \mathcal{X}_i$, which is a free $\mathbb{Z}$-module of finite rank n, and such that $A \otimes_{\mathbb{Z}} \mathbb{Q} = R_{\mathbb{Q}}(H)$ is semisimple.

Let $t = \mathrm{Tr}_{H^*} : R_k(H) \to k$; it is a trace like function by the remark after the definition of such functions.

Now, if we consider $a_i = \mathcal{X}_i$, $b_i = \mathcal{X}_{\bar{i}}$, $1 \leq i \leq n$, $(a_i, b_i \in A)$, then lemma (4.12) applies with $d = \dim H$ by the orthogonality relations (4.7). (Observe that, as k is algebraically closed and $\mathrm{char}\, k = 0$, $A \otimes_{\mathbb{Z}} \overline{\mathbb{Q}} \subseteq R_k(H)$).

On the other hand, as $e_1, \ldots, e_m$ are orthogonal idempotents, $t(e_i) = \dim(e_i H^*)$.

Thus, $t(e_i) = \dim(e_i H^*) \,/ d = \dim H$, which finishes the proof of the theorem. □

As a consequence of theorem (4.13), we show a theorem of Masuoka [9] on semisimple Hopf algebras of dimension p^m, p a prime generalizing previous results of Kac [3] and Zhu [21]. We need the following lemma.

Lemma 4.14. *Let $\lambda \in H^*$ an integral, such that $< \lambda, 1 >= 1$. Then*

1) $\dim(h\lambda \; H^*) = 1$, *$h \in H$, if and only if, there exist $0 \neq \alpha \in k$ and $g \in G(H)$ such that $h = \alpha g$.*

2) If $a \in R_k(H)$ is such that $\dim(aH^*) = 1$, *and aH^* is not the trivial H^*-module, then there exist $0 \neq \alpha \in k$, and $1 \neq g \in G(H) \bigcap Z(H)$, such that $a = \alpha g \lambda$.*

Proof.

1) Let $h \in H$. Then $\dim(h\lambda H^*) = 1$, if and only if there exists $g \in G(H)$, such that $\forall p \in H^*$, $(h\lambda)p = (h\lambda) < p, g >$.

But that is equivalent to the existence of a $g \in G(H)$ such that $\forall x \in H$,

$$< h\lambda, x_{(1)} > x_{(2)} =< h\lambda, x > g, \quad \text{or} \quad < gh\lambda, x_{(1)} g^{-1} > x_{(2)} g^{-1} =< gh\lambda, xg^{-1} > \; 1,$$

if and only if $gh\lambda$ is an integral in H^*. Which is equivalent to the existence of a nonzero $\alpha \in k$ such that $gh\lambda = \alpha\lambda$, i.e., $h = \alpha g^{-1}$.

[2]Added in 1997: In a recent paper by M. Lorenz [M. Lorenz, On the class equation for Hopf algebras, Proc. Amer. Math. Soc. (1997)] a shorter proof of 4.13 is giving using less algebraic number theory.

2) As $a \in R_k(H)$ (and $a \neq 0$), there exists $0 \neq x \in Z(H)$ such that $a = x\lambda$. Then, by 1), there exists $0 \neq \alpha \in k$ and $g \in G(H)$, such that $x = \alpha g$. In particular, $g \in Z(H)$ by (4.6).

Suppose $g = 1$. Then $x\lambda = \alpha\lambda$, and so $aH^* = \lambda H^*$, which is the trivial H^*-module. But this contradicts our assumption on a, so $g \neq 1$. □

Theorem 4.15. *Let H be a semisimple Hopf algebra such that $\dim H = p^m$, with p a prime, and $m \geq 1$. Then H contains a central grouplike $g \neq 1$.*

Proof. By theorem (4.13), we may write

$$p^m = 1 + \sum_i \dim(e_i H^*),$$

with $e_i \neq \lambda$ a primitive idempotent in H^*, and $\dim(e_i H^*) \,/\, \dim H = p^m$, $\forall i$.

Then, there must be a primitive idempotent $e_i \neq \lambda$, such that $\dim(e_i H^*) = 1$.

Now, as $e_i \neq \lambda$, $e_i H^*$ is not the trivial H^*-module, so the previous lemma implies, in particular, that H possesses a central grouplike $g \neq 1$. □

Hopf algebras of prime order. We now apply the previous results to arbitrary, not necessarily semisimple, Hopf algebras of prime order. k will denote an algebraically closed field of characteristic zero.

Let p be a prime, and let $\mathbb{Z}_p$ be the cyclic group of order p. Consider the Hopf algebra $H = k\mathbb{Z}_p$.

Observe that $H^* = k^{\mathbb{Z}_p}$ contains a grouplike G of order p (defined by $G(a) = \omega_p$, where a is a generator of $\mathbb{Z}_p$, and ω_p is a primitive p-th root of unity in k). Then $k^{\mathbb{Z}_p}$ contains the k-linear span of the powers of G, which is isomorphic (as a Hopf algebra) to $k\mathbb{Z}_p$. So, because they have the same finite order, $H^* = k^{\mathbb{Z}_p} \backsimeq k\mathbb{Z}_p = H$.

Theorem 4.16. (Zhu, 1994). *Let H be a Hopf algebra over k of prime order p. Then H is isomorphic to the algebra of functions on the cyclic group $\mathbb{Z}_p$.*

Proof. If $p = 2$, it is easily seen that H must be commutative and cocommutative, and the result follows from the theorem which asserts that every finite dimensional cocommutative Hopf algebra over an algebraically closed field of characteristic zero is isomorphic to a group algebra kG for some finite group G, and it is clear that G must be isomorphic to $\mathbb{Z}_2$.

Assume now $p > 2$. We consider separetaly three cases.

First Case: H or *H^** not unimodular.

Suppose H is not unimodular (the proof is analogous for H^*). Then the modular function $\alpha \in H^*$ (see §3) is a nontrivial grouplike element in H^*. By theorem (3.15), the linear span of the powers of α, $k < \alpha >$ (which is a Hopf subalgebra of H), must coincide with H. So in particular it is isomorphic to $k\mathbb{Z}_p$, and we have

$$H \backsimeq H^{**} = (k < \alpha >)^* \backsimeq k\mathbb{Z}_p{}^* \backsimeq k\mathbb{Z}_p.$$

Second Case: H and H^* unimodular, but H or H^* not semisimple.

By (3.4), we must have $\mathrm{Tr}(\mathcal{S}^2) = 0$. And as H and H^* are unimodular, $\mathcal{S}^4 = \mathrm{id}$. But then, the eigenvalues of $\mathcal{S}^2$ are all 1 or -1, and their sum is 0. This implies that the order of H must be even, which is an absurd. So this case is not possible.

Third Case : H and H^* both semisimple.

By theorem (4.15), H contains a central grouplike $g \neq 1$. Hence, by the Nichols-Zoeller's theorem, $H = k < g > \backsimeq k\mathbb{Z}p$. Note that we did not use "2) $\Longrightarrow$ 1)" of Theorem (3.13). $\square$

Appendix

Here is a complete list of the conjectures made by Kaplansky (except one which is easy).

1. *If C is a Hopf subalgebra of the Hopf algebra B then B is a free left C-module.*

Remark. In general this is false. A counterexample is given in [12]. Some particular cases are known, most notably if B is finite dimensional [11], as seen in the text, but also if C is finite dimensional and either semisimple or normal. The following form of the conjecture is still open: is B is faithfully flat over C? And dually, is a Hopf algebra faithfully coflat over its quotient Hopf algebras?

2. *Call a coalgebra C admissible if it admits an algebra structure making it a Hopf algebra. The conjecture states that C is admissible if and only if every finite subset of C lies in a finite dimensional admissible subcoalgebra.*

3. *A Hopf algebra of characteristic zero has no non-zero central nilpotents.*

4. *If H is a finite dimensional Hopf algebra, such that H or H^* are semisimple, the square of the antipode is the identity.*

Remark. We have seen this is true if the characteristic of the ground field k equals zero.

5. *If H is a (semisimple) Hopf algebra over the algebraically closed field k, then the sizes of the matrices occuring in any full matrix constituent of H divides the dimension of H.*

Remark. This is seen in the text if H is a group algebra.

6. *If H and H^* are semisimple the characteristic of k does not divide the dimension of H.*

Remark. This is a consequence of theorem (3.13) first proved by Larson and Radford.

7. *If the dimension of H is prime (k algebraically closed), then H is commutative and cocommutative.*

Remark. This is the result of Zhu shown in the text (th. 4.16) if the characteristic of k is zero, and is still open if the characteristic is positive.

8. *If the characteristic of k does not divide the dimension of H, the dimension of the radical is the same in H and in H^*.*

Remark. If the $\operatorname{char} k = p$ divides the dimension of H one has the following counterexample: $H = \mathbb{Z}_p$ is not semisimple, but H^* is.

We have seen that in characteristic zero H is semisimple iff H^* is. But the conjecture is false even in characteristic zero (take the Frobenius- Luztig kernel of $sl(2)$)[3].

[3]This counterexample was suggested by N. Andruskiewitsch.

9. *Again under the hipothesis that the characteristic of k does not divide the dimension of H, the conjecture states that there are only a finite number (up to isomorphism) of Hopf algebras of a given dimension.*

Remark. The following result is known (D. Stefan, 1995): The set of types of semisimple and cosemisimple Hopf algebras of a given dimension is finite (in any characteristic).

REFERENCES

[1]. C.W. Curtis and I. Reiner. *Representation Theory of finite groups and associative algebras,* Interscience, New York, 1962.

[2]. N. Jacobson. *Lie Algebras,* Interscience, New York, 1962.

[3]. G. I. Kac. *Certain arithmetic properties of ring groups,* Funct. anal. appl. **6** , (158-160), 1972.

[4]. J. C. Jantzen. *Representations of algebraic groups,* Academic Press, 1987.

[5]. R. G. Larson. *Characters of Hopf algebras,* J. of Algebra **17** , (352-368), 1971.

[6]. R. G. Larson and D. E. Radford. *Semisimple cosemisimple Hopf algebras,* Amer. J. of Math. **110**, (187-195), 1988.

[7]. R. G. Larson and D. E. Radford. *Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple,* J. of Algebra **117** , (267-289), 1988.

[8]. R. G. Larson and M. Sweedler. *An associative orthogonal bilinear form for Hopf algebras,* Amer. J. Math. **91** , (75-93), 1969.

[9]. A. Masuoka. *The p^n-theorem for semisimple hopf algebras,* Proc. Amer. Math. Soc., to appear.

[10]. S. Montgomery. *Hopf algebras and their actions on rings,* CBMS, 1993.

[11]. W. D. Nichols and M. B. Zoeller. *A Hopf algebra freeness theorem,* Amer. J. Math. **111**, (381-385), 1989.

[12]. U. Oberst and H.J. Schneider. *Untergruppen formeller Gruppen von endlichen Index,* J. of Algebra **31**, (10-44), 1974.

[13]. U. Oberst and H.J. Schneider. *Uber untergruppen endlicher algebraischer Gruppen,* Manuscripta Math. **8**, (217-241), 1973.

[14]. D. E. Radford. *The order of the antipode of a finite dimensional Hopf algebra is finite,* Amer. J. Math. **98**, (333-355), 1976.

[15]. J. P. Serre. *Linear Representations of Finite Groups,* Springer-Verlag, New York, 1977.

[16]. M. E. Sweedler. *Hopf Algebras,* Benjamin, New York, 1969.

[17]. M. E. Sweedler, *Integrals for Hopf algebras,* Ann. Math. **89**, (323-335), 1969.

[18]. E. J. Taft. *The order of the antipode of finite dimensional Hopf algebras,* Proc. Nat. Acad. Sci. USA **68**, (2631-2633), 1971.

[19]. E. J. Taft and R. L. Wilson. *There exist finite dimensional Hopf algebras with antipode of arbitrary even order,* J. of Algebra **62**, (283-291), 1980.

[20]. D. Wigner. *An identity in the free Lie algebras,* Proc. Amer. Math. Soc. **106**, (639-640), 1989.

[21]. Y. Zhu. *Hopf algebras of prime dimension,* Inter. Math. Research Not. **1**, (53-59), 1994.

[22]. M. Lorentz. *On the class equation for Hopf algebras,* Inter. Math. Research Not. **1**, (53-59), 1997.

Mathematisches Seminar der Universität München. Theressienstr. 39. (80333) München. Germany

E-mail address: hanssch@rz.mathematik.uni-muenchen.de