# HOPF ALGEBRAS

*by*

Benedikt Stufler

# Contents

# 1. Introduction

The present notes summarize the content of an advanced course on the algebraic foundation of Hopf algebra theory given by the author at the University of Zurich in 2018.

The study of Hopf algebras lies at the interface of representation theory, combinatorial algebra, and mathematical physics. We start with an introduction to the algebraic foundations (coalgebras, bialgebras, Hopf algebras, Hopf modules and comodules, universal enveloping algebras, ...). The highlight of the lecture will be a proof of the Cartier-Kostant theorem for pointed cocommutative Hopf algebras, that describes how a large variety of Hopf algebras are isomorphic to a smash product algebra composed out of the primitive and grouplike elements.

# 2. Basics

**2.1. Tensor products.** — We let $R$ denote a ring (with 1, not necessarily commutative).

DEFINITION 2.1 (UNIVERSAL MIDDLE-LINEAR MAPS). — *Let $X$ be a right $R$-module, $Y$ a left $R$-module, and $T$ an abelian group.*

1) *A map $\tau : X \times Y \to T$ is termed* middle linear, *if for all $x, x' \in X$, $y, y' \in Y$, $r \in R$ it holds that*

$$\tau(x + x', y) = \tau(x, y) + \tau(x', y),$$
$$\tau(x, y + y') = \tau(x, y) + \tau(x, y'),$$
$$\tau(xr, y) = \tau(x, ry).$$

2) *A middle-linear map $\tau : X \times Y \to T$ is* universal, *if for any abelian group $M$ and any middle-linear map $\varphi : X \times Y \to M$ there exists a unique group homomorphism $\bar{\varphi} : T \to M$ such that the diagram*

$$
\begin{array}{ccc}
X \times Y & \xrightarrow{\varphi} & M \\
{\scriptstyle \tau}\downarrow & \nearrow{\scriptstyle \bar{\varphi}} & \\
T & &
\end{array}
$$

*commutes.*

THEOREM 2.2 (TENSOR PRODUCTS). — *Let $X$ be a right $R$-module and $Y$ a left $R$-module.*

1) *If $\tau : X \times Y \to T$ and $\tau' : X \times Y \to T'$ are both universal middle-linear maps, then there is a unique isomorphism $\varphi : T \to T'$ such that the diagram*

$$
\begin{array}{ccc}
X \times Y & \xrightarrow{\ \tau'\ } & T' \\
{\scriptstyle\tau}\downarrow & {\scriptstyle\varphi}\nearrow & \\
T & &
\end{array}
$$

*commutes.*

2) *There is an abelian group $T$ with an universal middle-linear map $\tau : X \times Y \to T$. Notation: $T = X \otimes Y$ and $\tau(x,y) = x \otimes_R y$ for all $x \in X$, $y \in Y$.*

*Proof.* — Let $\mathbb{Z}^{(X \times Y)}$ be the free $\mathbb{Z}$-module with basis $X \times Y$. Let $N$ be the submodule that is generated by all elements of the form

$$
(x + x', y) - (x, y) - (x', y)
$$
$$
(x, y + y') - (x, y) - (x, y')
$$
$$
(xr, y) - (x, ry)
$$

with $x, x' \in X$, $y, y' \in Y$, and $r \in R$. Let $T = \mathbb{Z}^{(X \times Y)}/N$ and define $\tau$ by

$$
\begin{array}{ccc}
\mathbb{Z}^{(X \times Y)} & \xrightarrow{\ \mathrm{can}\ } & T \ . \\
{\scriptstyle\mathrm{can}}\uparrow & {\scriptstyle\tau}\nearrow & \\
X \times Y & &
\end{array}
$$

$\square$

**REMARK 2.3.** —  1) *$(x \otimes y)_{x \in X, y \in Y}$ is a $\mathbb{Z}$-span of $X \otimes_R Y$. We often denote $\mathbb{Z}$-linear maps on the tensor product by stating how they act on this spanning family, but care has to be taken whether such maps actually exist (or are "well-defined").*

2) *$\mathbb{Z}/(n) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ for all $n \geq 1$.*

**DEFINITION 2.4** (BIMODULES). — *Let $R$ and $S$ be rings. Suppose that the set $X$ is equipped both with a left $R$-module structure and an right $S$-module structure.*

1) *We say $X$ is an $(R, S)$-bimodule, if for all $x \in X$, $r \in R$, and $s \in S$ it holds that*

$$
(rx)s = r(xs)
$$

2) *A map $\phi : X \to Y$ between $(R, S)$-bimodules $X$ and $Y$ is $(R, S)$-linear if it is both $R$-linear (from the left) and $S$-linear (from the right).*

**THEOREM 2.5** (MODULE STRUCTURES ON TENSOR PRODUCTS)

*Let $R, S, T, U$ be rings, $X$ an $(R, S)$-bimodule, $Y$ an $(S, T)$-bimodule, and $Z$ an $(T, U)$-bimodule.*

1) The tensor product $X \otimes_S Y$ is an $(R,T)$-bimodule via $r(x \otimes y) = rx \otimes y$ and $(x \otimes y)s = x \otimes ys$.

2) $(X \otimes_S Y) \otimes_T Z \simeq X \otimes_S (Y \otimes_T Z)$ is an $(R,U)$-linear isomorphism that is functorial in $X$, $Y$, and $Z$.

3) $X \otimes_S S \simeq X$ with $x \otimes s \mapsto xs$ is $(R,S)$-linear and functorial in $X$.
$R \otimes_R X \simeq X$ with $r \otimes x \mapsto rx$ is $(R,S)$-linear and functorial in $X$.

4) If $R$ is commutative and $M, N$ are $R$-modules, then

$$M \otimes_R N \simeq N \otimes_R M \quad \text{with} \quad m \otimes n \mapsto n \otimes m$$

is $R$-linear and functorial.

DEFINITION 2.6. — Let $X, X'$ be right $R$-modules, $Y, Y'$ be left $R$-modules, and $f : X \to X'$, $g : Y \to Y'$ be a $R$-linear maps. Then we let

$$f \otimes g : X \otimes_R Y \to X' \otimes_R Y', \quad x \otimes y \mapsto f(x) \otimes g(y).$$

THEOREM 2.7 (COPRODUCTS AND TENSORS). — Let $(X_i)_{i \in I}$ be a family of right $R$-modules, $Y$ a left $R$-module. Then $\phi : \coprod_{i \in I}(X_i \otimes_R Y) \to (\coprod_{i \in I} X_i) \otimes_R Y$ defined via $X_i \otimes_R Y \xrightarrow{\mathrm{can} \otimes \mathrm{id}} (\coprod_{i \in I} X_i) \otimes_R Y$ for all $i \in I$ is a functorial isomorphism.

COROLLARY 2.8 (BASES OF TENSOR PRODUCTS). — 1) Let $X$ be a right $R$-module with basis $(x_i)_{i \in I}$ and let $Y$ be a left $R$-module. Then each element $t \in X \otimes_R Y$ has a unique representation $t = \sum_{i \in I} x_i \otimes y_i$ with $y_i \in Y$ for all $i \in I$ and $y_i = 0$ for almost all (=all but finitely many) $i \in I$.

2) $k$ field, $V, W$ $k$-vector spaces with bases $(v_i)_{i \in I}, (w_j)_{j \in J}$. Then the family $(v_i \otimes w_j)_{i \in I, j \in J}$ is a basis of $V \otimes_k W$.

THEOREM 2.9 ($\otimes$ IS RIGHT EXACT). — Let $A, B, C$ be left $R$-modules and let $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an exact sequence of $R$-linear maps. Then for all right $R$-modules $Y$ it holds that the sequence $Y \otimes_R A \xrightarrow{\mathrm{id} \otimes f} Y \otimes_R B \xrightarrow{\mathrm{id} \otimes g} Y \otimes C \to 0$ is exact too.

*Proof.* — See exercises. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

**2.2. Algebras.** — We let $k$ denote a commutative ring (with 1).

DEFINITION 2.10. — 1) Let $A$ be a ring (with 1) and a $k$-module. We say $A$ is a $k$-algebra if for all $\lambda \in k$ and $x, y \in A$ it holds that $\lambda.(xy) = (\lambda.x)y = x(\lambda.y)$.

2) An algebra homomorphism from a $k$-algebra $A$ to a $k$-algebra $B$ is a $k$-linear ring homomorphism.

3) The center of an algebra $A$ is the subalgebra

$$Z(A) = \{x \in A \mid xy = yx \text{ for all } y \in A\}.$$

REMARK 2.11. —    *1) Let $A$ be a $k$-algebra. The unique ring homomorphism $\eta : k \to A$ satisfies $\mathrm{im}(\eta) \subset Z(A)$.*

*2) Conversely, if $A$ is a ring and $\eta : k \to A$ is a ring homomorphism with $\mathrm{im}(\eta) \subset Z(A)$, then $A$ is a $k$-algebra via $\lambda.x = \eta(\lambda)$ for all $\lambda \in k$, $x \in A$.*

REMARK 2.12. —    *1) Let $A$ be a $k$-algebra. The linear map $\mu : A \otimes_k A \to A$ with $\mu(a \otimes b) = ab$ and the ring homomorphism $\eta : k \to A$ satisfy*

$$
\begin{array}{ccccc}
k \otimes_k A & \xrightarrow{\eta \otimes \mathrm{id}} & A \otimes_k A & \xleftarrow{\mathrm{id} \otimes \eta} & A \otimes_k k \\
& \searrow{\scriptstyle \mathrm{can}} & \downarrow{\scriptstyle \mu} & \swarrow{\scriptstyle \mathrm{can}} & \\
& & A & &
\end{array}
$$

*and*

$$
\begin{array}{ccccc}
A \otimes_k (A \otimes_k A) & \xrightarrow{\mathrm{id} \otimes \mu} & A \otimes_k A & \xrightarrow{\mu} & A \;. \\
\downarrow{\scriptstyle \mathrm{can}} & & & \nearrow{\scriptstyle \mu} & \\
(A \otimes_k A) \otimes_k A & \xrightarrow{\mu \otimes \mathrm{id}} & A \otimes_k A & &
\end{array}
$$

*2) Conversely, let $A$ be a $k$-module. If $\mu : A \otimes_k A \to A$ and $\eta : k \to A$ are $k$-linear maps such that these diagrams commute, then $A$ is a $k$-algebra with $xy = \mu(x \otimes y)$ and $1_A = \eta(1_k)$.*

REMARK 2.13. —    *1) $\mathrm{M}_n(k)$ and $\mathrm{End}_k(V)$ ($V$ a $k$-module) are $k$-algebras.*

*2) If $A$ is a $k$-algebra, then we define the algebra $A^{\mathrm{op}}$ by setting $A^{\mathrm{op}} := A$ as $k$-module and defining $\eta_{A^{\mathrm{op}}} := \eta_A$ and $\mu_{A^{\mathrm{op}}} := \mu_A \circ \tau$ with the linear map $\tau : A \otimes_k A \to A \otimes_k A$, $\tau(x \otimes y) = y \otimes x$.*

*3) If $A$ is a $k$-algebra then*

$$
\begin{aligned}
\delta :& A \to \mathrm{End}_k(A), a \mapsto (x \mapsto ax) \\
\delta' :& A \to \mathrm{End}_k(A)^{\mathrm{op}}, a \mapsto (x \mapsto xa)
\end{aligned}
$$

*are algebra homomorphisms.*

REMARK 2.14. —    *1) If $A$ and $B$ are $k$-algebras, then so is $A \otimes_k B$.*

*2) If $\varphi : A \to A'$ and $\psi : B \to B'$ are algebra homomorphisms then so is $\varphi \otimes \psi : A \otimes_k B \to A' \otimes_k B'$.*

DEFINITION 2.15. — *Let $G$ be a monoid. Then $k[G] := k^{(G)}$ (also denoted by $kG$) is a $k$-algebra with $\mu(g \otimes h) = gh$ (product in $G$). It satisfies the universal property, that for any algebra $A$ and any monoid homomorphism $\varphi : G \to (A, \cdot)$ there is a unique algebra*

*homomorphism $\bar{\varphi} : k[G] \to A$ such that*

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ {\scriptstyle \text{can}} \downarrow & \nearrow & \\ k[G] & {\scriptstyle \bar{\varphi}} & \end{array} \quad .$$

REMARK 2.16. — *1) Let $G = \mathbb{N}_0$ be the additive monoid. Then $k[G] \simeq k[X_1, \dots, X_n]$ polynomial ring in $n$ indeterminates.*

*2) Let $X$ be a set, $<X>$ the free monoid over $X$, then $k<X>$ is called the free algebra over $X$.*

PROPOSITION 2.17. — *Let $A$ be a $k$-algebra and $I \subset A$ a both-sided ideal. Then for any algebra homomorphism $\varphi : A \to B$ with $\varphi(I) = 0$ there is a unique algebra homomorphism $\bar{\varphi} : A/I \to B$ such that*

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \text{can}} \downarrow & \nearrow & \\ A/I & {\scriptstyle \bar{\varphi}} & \end{array} \quad .$$

**2.3. Category theory.** — The language of category theory allows us to express complex relationships in a concise and elegant way. Setting up a rigorous foundation for the set-theoretic background does not lie within the scope of this lecture. We naively define *classes* to be collections of sets which we can define and talk about. Hence we may form the class of all sets, which is a *proper class* as it cannot be a set. We may also consider maps between classes.

DEFINITION 2.18. — *A category $\mathcal{C}$ consists of a class $\mathrm{Ob}(\mathcal{C})$, whose elements are called the objects of the class, with the following additional structures:*

– *For any two objects $X, Y \in \mathrm{Ob}(\mathcal{C})$ we are given a set $\mathcal{C}(X, Y)$ whose elements are called the morphisms from $X$ to $Y$. We require that*

$$\mathcal{C}(X, Y) \cap \mathcal{C}(X', Y') = \emptyset$$

*for all $X, X', Y, Y' \in \mathrm{Ob}(\mathcal{C})$ with $X \neq X'$ or $Y \neq Y'$. Instead of $f \in \mathcal{C}(X, Y)$ we also write $f : X \to Y$ or $X \xrightarrow{f} Y$.*

– *For any $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$ we are given a map*

$$\mathcal{C}(Y, Z) \times \mathcal{C}(X, Y) \to \mathcal{C}(X, Z), (g, f) \mapsto gf = g \circ f.$$

*We require that for all $X \xrightarrow{f} Y$, $Y \xrightarrow{g} Z$ and $Z \xrightarrow{h} U$*

$$h(gf) = (hg)f.$$

− *For any $X \in \mathrm{Ob}(\mathcal{C})$ there is a distinguished element $\mathrm{id}_X \in \mathcal{C}(X, X)$. We require that*

$$f\mathrm{id}_X = f = \mathrm{id}_Y f$$

*for all $X \xrightarrow{f} Y$.*

EXAMPLE 2.19. —    *1) The category $\mathrm{Set}$ of all sets with maps as morphisms.*
  *2) The category $\mathrm{Gr}$ of all groups with group homomorphisms as morphisms.*
  *3) The categories $_R\mathcal{M}$ and $\mathcal{M}_R$ of left R-modules and right R-modules.*

REMARK 2.20. — *A category $\mathcal{C}$ is termed small, if $\mathrm{Ob}(\mathcal{C})$ is a set.*

DEFINITION 2.21. — *Let $\mathcal{C}$ be a category. A morphism $X \xrightarrow{f} Y$ in $\mathcal{C}$ is termed an isomorphism, if there exists a morphism $Y \xrightarrow{g} X$ with $gf = \mathrm{id}_X$ and $fg = \mathrm{id}_Y$. If this is the case then $g$ is uniquely determined and we may write $g = f^{-1}$.*

DEFINITION 2.22. — *Given a category $\mathcal{C}$ we may form the category $\mathcal{C}^{\mathrm{op}}$ with $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$ and $\mathcal{C}^{\mathrm{op}}(X, Y) = \mathcal{C}(Y, X)$ for all objects $X, Y$.*

DEFINITION 2.23. — *Let $\mathcal{C}$ and $\mathcal{D}$ be categories.*

*1) A (covariant) functor $F : \mathcal{C} \to \mathcal{D}$ consists of a map*

$$\mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D}), X \mapsto F(Y)$$

*together with a family of maps*

$$\mathcal{C}(X, Y) \to \mathcal{D}(X, Y), f \mapsto F(f),$$

*for $X, Y \in \mathrm{Ob}(\mathcal{C})$, such that*

$$F(gf) = F(g)F(f) \qquad and \qquad F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$$

*for all $X, Y, Z \in \mathrm{Ob}(\mathcal{C})$, $f \in \mathcal{C}(X, Y)$, and $g \in \mathcal{C}(Y, Z)$.*
*2) A contravariant functor $\mathcal{C} \to \mathcal{D}$ is a functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.*

EXAMPLE 2.24. —    *1) Let $k$ be a commutative ring. $_k\mathcal{M} \to {_k\mathcal{M}}$ defined by*

$$V \mapsto V^* = \mathrm{Hom}_k(V, k) \qquad and \qquad f \mapsto (f^* : g \mapsto gf)$$

*is a contravariant functor.*
*2) Let $R, S$ be rings and $X$ an $(R, X)$-bimodule. Then*

$$X \otimes_S - : {_S\mathcal{M}} \to {_\mathbb{Z}\mathcal{M}}$$

*is a covariant functor.*

*3) Let $R$ be a ring and $X \in {}_R\mathcal{M}$. Then*

$$\mathrm{Hom}_R(X, -) : {}_R\mathcal{M} \to {}_{\mathbb{Z}}\mathcal{M}$$

*is a covariant functor, and*

$$\mathrm{Hom}_R(-, X) : {}_R\mathcal{M} \to {}_{\mathbb{Z}}\mathcal{M}$$

*is a contravariant functor.*

*4) Let $\mathcal{C}$ be a category and $X \in \mathrm{Ob}(\mathcal{C})$. Then*

$$\mathcal{C}(X, -) : \mathcal{C} \to \mathrm{Set}$$

*is a covariant functor, and*

$$\mathcal{C}(-, X) : \mathcal{C} \to \mathrm{Set}$$

*is a contravariant functor.*

REMARK 2.25. — *Any category $\mathcal{C}$ admits the trivial functor $\mathrm{id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$. We may concatenate a functor $F : \mathcal{C} \to \mathcal{D}$ with a functor $G : \mathcal{D} \to \mathcal{E}$ to form a functor $GF : \mathcal{C} \to \mathcal{E}$. This operation is associative and the functors behave like neutral elements.*

DEFINITION 2.26. — *1) Let $\mathcal{C}$, $\mathcal{D}$ be categories and $F, G : \mathcal{C} \to \mathcal{G}$ be functors. A natural transformation $\alpha : F \to G$ is a family $\alpha = (\alpha_C)_{C \in \mathrm{Ob}(\mathcal{C})}$ of morphisms $\alpha_C : F(C) \to G(C)$ such that for all $C, C' \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathcal{C}(C, C')$*

$$
\begin{array}{ccc}
F(C) & \xrightarrow{F(f)} & F(C') \\
\downarrow{\scriptstyle \alpha_C} & & \downarrow{\scriptstyle \alpha_{C'}} \\
G(C) & \xrightarrow{G(f)} & G(C')
\end{array}
\quad .
$$

*2) The natural transformation $\alpha$ is a natural isomorphism, if $\alpha_C$ is an isomorphism for each $C \in \mathrm{Ob}(\mathcal{C})$. We denote the existence of a natural isomorphism between $F$ and $G$ by*

$$F \simeq G.$$

*3) We may think of natural transformation as "morphisms between functors". Any functor $F$ admits the trivial natural isomorphism $\mathrm{id}_F : F \to F$. We may concatenate a natural transformation $\alpha : F \to G$ with a natural transformation $\beta : G \to H$ to form a natural transformation $\beta\alpha : F \to H$. This operation is associative and the trivial natural isomorphisms behave like neutral elements.*

*4) The natural transformation $\alpha : F \to G$ is a natural isomorphism, if and only if there exists a natural transformation $\beta : G \to F$ such that $\beta\alpha = \mathrm{id}_F$ and $\alpha\beta = \mathrm{id}_G$.*

EXAMPLE 2.27. — *1) Suppose that $k$ is a field. For any $k$-vector space $V$ let $\alpha_V : V \to V^{**}, v \mapsto (f \mapsto f(v))$. Then $\alpha = (\alpha_V)_V$ is a natural transformation $\mathrm{id} \to ()^{**}$. $\alpha$ is a natural isomorphism when restricted to finite dimensional vector spaces.*
*2) Let $k$ be commutative ring and let $X$ and $Y$ be $k$-modules. The map $X \otimes_k Y^* \to \mathrm{Hom}(Y, X)$ with $x \otimes f \mapsto (y \mapsto f(y)x$ is functorial in $X$ and $Y$. That is,*

$$- \otimes_k Y^* \to \mathrm{Hom}_k(Y, -)$$

*is a natural transformation of covariant functors, and*

$$X \otimes_k ()^* \to \mathrm{Hom}_k(-, X)$$

*is a natural transformation of contravariant functors.*

DEFINITION 2.28. — *A functor $F : \mathcal{C} \to \mathcal{D}$ is an equivalence of categories if there is a functor $G : \mathcal{D} \to \mathcal{C}$ such that $GF \simeq \mathrm{id}_\mathcal{C}$ and $FG \simeq \mathrm{id}_\mathcal{D}$.*

DEFINITION 2.29. — *A functor $F : \mathcal{C} \to \mathcal{D}$ is termed left adjoint to a functor $G : \mathcal{D} \to \mathcal{C}$, if there is a family of bijections $\varphi_{C,D} = \mathcal{D}(F(C), D) \to \mathcal{C}(C, G(D))$ (with $C \in \mathrm{Ob}(\mathcal{C})$, $D \in \mathrm{Ob}(\mathcal{D})$) that is functorial in $C$ and $D$. In this case there is a canonical natural transformation $\eta : \mathrm{id}_\mathcal{C} \to GF$ with $\eta_C = \varphi_{C,F(C)}(\mathrm{id}_{F(C)})$ for all $C \in \mathrm{Ob}(\mathcal{C})$.*

*Proof.* — Diagram chasing. $\qquad\square$

PROPOSITION 2.30. — *Let $R$, $S$, and $T$ be rings.*
*1) Let $_RX_S$ and $_RY_T$ be bimodules. Then $\mathrm{Hom}_R(_RX_S, _RY_T)$ is an $(S,T)$-bimodule with*

$$(s.f)(x) = f(x.s)$$
$$(f.t)(x) = f(x).t$$

*("Left Hom from $(R,S)$ to $(R,T)$ gives $(S,T)$"; we may use the notation $_S\mathrm{Hom}_R(_RX_S, _RY_T)_T$)*
*2) Let $_RX_S$ and $_TY_S$ be bimodules. Then $\mathrm{Hom}_S(_RX_S, _TY_S)$ is an $(T,R)$-bimodule with*

$$(f.r)(x) = f(rx)$$
$$(t.f)(x) = tf(x)$$

*("Right Hom from $(R,S)$ to $(T,S)$ gives $(T,R)$"; we may use the notation $_T\mathrm{Hom}_S(_RX_S, _TY_S)_R$)*
*3) Let $_RX_S$ be a bimodule. Then*

$$\mathrm{Hom}_R(_RX_S, -) : {_R\mathcal{M}} \to {_S\mathcal{M}}$$
$$\mathrm{Hom}_S(_RX_S, -) : \mathcal{M}_S \to \mathcal{M}_R$$

*are covariant functors, and*

$$\operatorname{Hom}_S(-, {}_RX_S) : \mathcal{M}_S \to {}_R\mathcal{M}$$

$$\operatorname{Hom}_R(-, {}_RX_S) : {}_R\mathcal{M} \to \mathcal{M}_S$$

*are contravariant functors.*

PROPOSITION 2.31. — *1) There is a canonical isomorphism of right $T$-modules:*

$$\operatorname{Hom}_R({}_RX_S \otimes_S {}_SY, {}_RZ_T)_T \simeq \operatorname{Hom}_S({}_SY, \operatorname{Hom}_R({}_RX_S, {}_RZ_T))_T$$

*2) The functor*

$$_RX_S \otimes_S - : {}_S\mathcal{M} \to {}_R\mathcal{M}$$

*is left adjoint to*

$$\operatorname{Hom}_R({}_RX_S, -) : {}_R\mathcal{M} \to {}_S\mathcal{M}.$$

COROLLARY 2.32. — *If $S \subset R$ is a subring, then*

$$_RR_S \otimes_S - : {}_S\mathcal{M} \to {}_R\mathcal{M}$$

*is left-adjoint to*

$$\operatorname{Hom}_R({}_RR_S, -) : {}_R\mathcal{M} \to {}_S\mathcal{M}.$$

## 3. Coalgebras and Hopf algebras

Unless otherwise stated, $k$ always denotes a field and all vector spaces are over $k$. We let $\otimes = \otimes_k$ denote the tensor product over $k$.

### 3.1. Coalgebras. —

DEFINITION 3.1 (COALGEBRAS). — *Let $C$ be a vector space over $k$, and let $\Delta : C \to C \otimes C$ and $\epsilon : C \to k$ be $k$-linear maps. The tupel $(C, \Delta, \epsilon)$ is a coalgebra, if the following diagrams commute:*

$$
k \otimes_k C \xleftarrow{\ \epsilon \otimes \mathrm{id}\ } C \otimes_k C \xrightarrow{\ \mathrm{id} \otimes \epsilon\ } C \otimes_k k
$$

$$
\begin{array}{c} \simeq \quad\quad \uparrow \Delta \quad\quad \simeq \\ C \end{array}
$$

*and*

$$
C \otimes_k (C \otimes_k C) \xleftarrow{\ \mathrm{id} \otimes \Delta\ } C \otimes_k C \xleftarrow{\ \Delta\ } C \ .
$$

$$
\simeq \uparrow \quad\quad\quad\quad\quad\quad\quad\quad \downarrow \Delta
$$

$$
(C \otimes_k C) \otimes_k C \xleftarrow{\ \Delta \otimes \mathrm{id}\ } C \otimes_k C
$$

EXAMPLE 3.2. —      1) *If $G$ is a set, then $k^{(G)}$ is a coalgebra with $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$ for all $g \in G$.*

2) *Let $C$ be a vector space over $k$ with basis $(x_{i,j})_{1 \le i,j \le n}$. $C$ is a coalgebra with $\Delta(x_{i,j}) = \sum_{k=1}^n x_{i,k} \otimes x_{k,j}$, $\epsilon(x_{i,j}) = \delta_{i,j}$.*

*Proof.* — It suffices to verify the axioms on the basis of $C$.

$$
\sum_{k=1}^n \Delta(x_{i,k}) \otimes x_{k,j} = \sum_{1 \le k_1, k_2 \le n} x_{i,k_1} \otimes x_{k_1,k_2} \otimes x_{k_2,j} = \sum_{k=1}^n x_{i,k} \otimes \Delta(x_{k,j})
$$

and

$$
\sum_{k=1}^n \epsilon(x_{i,k}) \otimes x_{k,j} = 1 \otimes x_{i,j}, \qquad \sum_{k=1}^n x_{i,k} \otimes \epsilon(x_{k,j}) = x_{i,j} \otimes 1.
$$

$\square$

3) *$C$ a vector space over $k$ with basis $(x_i)_{i \ge 0}$. $C$ is a coalgebra with $\Delta(x_n) = \sum_{i=0}^n x_i \otimes x_{n-i}$ and $\epsilon(x_n) = \delta_{0,n}$.*

*Proof.* —

$$
\sum_{i=0}^n \Delta(x_i) \otimes x_{n-i} = \sum_{i_1 + i_2 + i_3 = n} x_{i_1} \otimes x_{i_2} \otimes x_{i_3} = \sum_{i=0}^n x_i \otimes \Delta(x_{n-i}).
$$

The rest is clear. $\square$

*4) Let $C$ be a vector space over $k$ with basis $g, h, x$. Then $C$ is a coalgebra with $\Delta(g) = g \otimes g$, $\epsilon(g) = 1$, $\Delta(h) = h \otimes h$, $\epsilon(h) = 1$, $\Delta(x) = g \otimes x + x \otimes h$, $\epsilon(x) = 0$.*

DEFINITION 3.3 (SWEEDLER NOTATION). — *Let $C$ be a coalgebra, $x \in C$. We use the notation*

$$\Delta(x) =: \sum_i x_{1,i} \otimes x_{2,i} =: x_{(1)} \otimes x_{(2)} =: x_1 \otimes x_2,$$

$$\Delta^n(x) =: (\Delta \otimes \mathrm{id})(\Delta^{n-1})(x) =: x_{(1)} \otimes \ldots \otimes x_{(n+1)} =: x_1 \otimes \ldots \otimes x_{n+1}.$$

*For $f : C^n \to X$ multilinear, $\bar{f} : \bigotimes_{1 \leq i \leq n} C \to X$ the induced map, we set*

$$\bar{f}(\Delta^{n-1}(x)) =: f(x_{(1)}, \ldots, x_{(n)}) =: f(x_1, \ldots, x_n).$$

DEFINITION 3.4. — *A $k$-linear map $f : C \to C'$ between coalgebras is called a coalgebra homomorphism if for all $x \in C$ it holds that $\epsilon_{C'}(f(x)) = \epsilon_C(x)$ and $f(x)_1 \otimes f(x)_2 = f(x_1) \otimes f(x_2)$.*

DEFINITION 3.5. — *$A$ an algebra, $C$ a coalgebra, $f, g \in \mathrm{Hom}_k(C, A)$. Then $f * g \in \mathrm{Hom}_k(C, A)$ with $(f * g)(x) = f(x_1)g(x_2)$ is called the convolution of $f$ and $g$. That is:*

$$C \xrightarrow{\ \Delta\ } C \otimes C \xrightarrow{\ f \otimes g\ } A \otimes A \xrightarrow{\ \mu\ } A$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{f * g}$$

THEOREM 3.6. — *Let $A$ be an algebra, $C$ a coalgebra.*

*1) Then $\mathrm{Hom}_k(C, A)$ is an algebra with product $*$ and unit element $\eta\epsilon$.*

   *Proof. —*

| | |
|---|---|
| Associativity: | $((f * g) * h)(x) = f(x_1)g(x_2)h(x_3) = (f * (g * h))(x)$ |
| Unit element: | $(f * (\eta\epsilon))(x) = f(x_1)\epsilon(x_2) = f(x_1\epsilon(x_2)) = f(x)$ |
| | $((\eta\epsilon) * f)(x) = \epsilon(x_1)f(x_2) = f(\epsilon(x_1)x_2) = f(x).$ |

$\square$

*2) We have the following functors:*

$$\mathrm{Hom}_k(C, -) : \mathrm{Algebras}_k \to \mathrm{Algebras}_k$$
$$\mathrm{Hom}_k(-, A) : \mathrm{Coalgebras}_k^{\mathrm{op}} \to \mathrm{Algebras}_k$$

   *Proof. —* Let $\varphi : A \to A'$ be an algebra homomorphism. Then

$$\mathrm{Hom}_k(\mathrm{id}, \varphi) : \mathrm{Hom}_k(C, A) \to \mathrm{Hom}_k(C, A'), f \mapsto \varphi f$$

   is an algebra homomorphism, because

$$(\varphi\eta_A\epsilon)(x) = \varphi(\epsilon(x)1_A) = \epsilon(x)1_{A'} = (\eta_{A'}\epsilon)(x)$$

and

$$(\varphi(f * g))(x) = \varphi(f(x_1)g(x_2)) = \varphi(f(x_1))\varphi(f(x_2)) = ((\varphi f) * (\varphi g))(x).$$

This shows that $\mathrm{Hom}_k(C, -)$ is a functor $\mathrm{Algebras}_k \to \mathrm{Algebras}_k$.

Let $\psi : C \to C'$ be a coalgebra homomorphism. Then

$$\mathrm{Hom}_k(\psi, \mathrm{id}) : \mathrm{Hom}_k(C', A) \to \mathrm{Hom}_k(C, A), f \mapsto f\psi$$

is an algebra homomorphism, because

$$(\eta\epsilon_{C'}\psi)(x) = 1_A\epsilon_{C'}(\psi(x)) = 1_A\epsilon_C(x) = (\eta\epsilon_C)(x)$$

and

$$\begin{aligned}
((f * g)\psi)(x) &= (f \odot g)((\psi(x))_1 \otimes (\psi(x))_2) \\
&= (f \odot g)(\psi(x_1) \otimes \psi(x_2)) \\
&= ((f\psi) * (g\psi))(x).
\end{aligned}$$

$\square$

COROLLARY 3.7. — *If $C$ is a coalgebra, then $C^*$ is an algebra.*

EXAMPLE 3.8. — 1) *If $G$ is a finite set, then the coalgebra $k^G$ from Example 3.2, 1) satisfies $(k^G)^* \simeq k^G$ as algebras.*

2) *The coalgebra $C$ from Example 3.2, 2) satisfies $C^* \simeq M_n(k)$ as k-algebras.*

3) *The coalgebra $C$ from Example 3.2, 3) satisfies $C^* \simeq k[X]$ as k-algebras.*

*Proof.* — See exercises. $\square$

PROPOSITION 3.9. — *Let $X$ and $Y$ be vector spaces over $k$. Then*

$$X^* \otimes Y^* \to (X \otimes Y)^*, \quad f \otimes g \mapsto (f \odot g : x \otimes y \mapsto f(x)g(y)).$$

*If $X$ or $Y$ is finite dimensional, then this linear map is an isomorphism.*

*Proof.* — As the functor $X \otimes -$ is left-adjoint to the functor $Hom(X, -)$, it holds that

$$\mathrm{Hom}(X \otimes Y, k) \simeq \mathrm{Hom}(Y, \mathrm{Hom}(X, k)) = \mathrm{Hom}(Y, X^*).$$

We have seen in the exercises that for all vector spaces $V$ and $W$ it holds that

$$V \otimes W^* \to \mathrm{Hom}(W, V), \quad v \otimes f \mapsto (w \mapsto f(w)v)$$

is an isomorphism if $V$ or $W$ is finite dimensional. In particular,

$$\mathrm{Hom}(Y, X^*) \simeq X^* \otimes Y^*$$

if $X$ or $Y$ is finite dimensional. $\square$

THEOREM 3.10. — *Let $A$ be a finite dimensional algebra. Then $A^*$ is a coalgebra with $\epsilon(f) = f(1)$ and $\Delta(f) = f_1 \otimes f_2$ uniquely determined by $f_1(a)f_2(b) = f(ab)$ for all $a, b \in A$. That is,*

$$A^* \xrightarrow{\eta^*} k^* \xrightarrow{\simeq} k$$
$$\underset{\epsilon}{\searrow\nearrow}$$

*and*

$$A^* \xrightarrow{\mu^*} (A \otimes A)^* \xrightarrow{\simeq} A^* \otimes A^*$$
$$\underset{\Delta}{\searrow\nearrow}$$

*Proof.* — $\epsilon$ is a counit because $\eta$ is a unit, that is

$$(\epsilon(f_1)f_2)(x) = f_1(1)f_2(x) = f(1x) = f(x)$$

and

$$f_1\epsilon(f_2)(x) = f_1(x)f_2(1) = f(x1) = f(x).$$

$\Delta$ is coassociative because $\mu$ is associative, that is for all $a, b, c \in A$

$$f_{11}(a)f_{12}(b)f_2(c) = f_1(ab)f_2(c) = f(abc)$$
$$f_1(a)f_{21}(b)f_{22}(c) = f_1(a)f_2(bc) = f(abc)$$

and hence

$$f_{11} \otimes f_{12} \otimes f_2 = f_1 \otimes f_{21} \otimes f_{22}.$$

$\square$

EXAMPLE 3.11. — *Let $G$ be a finite monoid and $k[G]$ the corresponding monoid algebra. Let $(e_g)_{g \in G}$ be the dual basis of $(g)_{g \in G}$. Then $\epsilon(e_g) = e_g(1_G) = \delta_{g,1_G}$ and $\Delta(e_g) = \sum_{a,b \in G, ab = g} e_a \otimes e_b$ because for $x, y \in G$:*

$$\sum_{ab=g} e_a(x)e_b(y) = \sum_{ab=g} \delta_{a,x}\delta_{b,y} = \delta_{g,xy} = e_g(xy).$$

COROLLARY 3.12. — *We have an equivalence of categories*

$$\{C \mid C \text{ f. d. } k\text{-coalgebra}\}^{\mathrm{op}} \simeq \{A \mid A \text{ f. d. } k\text{-algebra}\}$$

*with $C \mapsto C^*$ and $A \mapsto A^*$.*

*Proof.* — These functors are well-defined: We have already seen that $\mathrm{Hom}_k(-, k) :$ $\mathrm{Coalgebras}_k^{\mathrm{op}} \to \mathrm{Algebras}_k$ is a functor. It is also easy to check that if $\kappa : A \to A'$ is an homomorphism between finite dimensional algebras, then $\kappa^* : (A')^* \to A^*$ is a coalgebra homomorphism.

We already know that $\mathrm{id} \simeq ()^{**}$ for finite dimensional vector spaces. It remains to show that this natural isomorphism restricts to isomorphisms of finite dimensional coalgebras and algebras.

That is, for $A$ a finite dimensional algebra, consider the bijective map

$$\varphi : A \to A^{**}, a \mapsto (f \mapsto f(a)).$$

We have to check that $\varphi$ is an algebra homomorphism. For $F, G \in A^{**}$, $f \in A^*$ we have $(F \cdot G)(f) = F(f_1)G(f_2)$ with $f_1(a)f_2(b) = f(ab)$ for all $a, b \in A$. This implies that

$$\varphi(ab)(f) = f(ab) = f_1(a)f_2(b) = (\varphi(a) \cdot \varphi(b))(f).$$

Also,

$$\varphi(1)(f) = f(1) = 1_{A^{**}}(f).$$

This shows that $A \simeq A^{**}$ as algebras.

Likewise, for $C$ a finite dimensional coalgebra, the linear bijection

$$\psi : C \to C^{**}, x \mapsto (f \mapsto f(x))$$

preserves the coalgebra structures: For $F \in C^{**}$ we have that $\Delta(F) = F_1 \otimes F_2$ is uniquely determined by $F_1(f)F_2(g) = F(f * g)$ for all $f, g \in C^*$. So

$$\psi(x_1)(f)\psi(x_2)(g) = f(x_1)g(x_2) = (f * g)(x) = \psi(x)(f * g)$$

implies that

$$\Delta(\psi(x)) = \psi(x_1) \otimes \psi(x_2).$$

Moreover, $\epsilon_{C^{**}}(F) = F(1_{C^*}) = F(\epsilon_C)$ implies that

$$\epsilon_{C^{**}}(\psi(x)) = \psi(x)(\epsilon_C) = \epsilon_C(x).$$

This shows that $C \simeq C^{**}$ as coalgebras. The isomorphism is easily seen to be functorial.
□

PROPOSITION 3.13. — *Let $C$ and $D$ be $k$-coalgebras. Then so is $C \otimes D$ is a coalgebra with a componentwise structure. That is, $\Delta(x \otimes y) = (x_1 \otimes y_1) \otimes (x_2 \otimes y_2)$ and $\epsilon(x \otimes y) = \epsilon_C(x)\epsilon_D(y)$.*

DEFINITION 3.14. — *Let $C$ be a coalgebra.*

*1) An element $g \in C$ is called grouplike, if $\Delta(g) = g \otimes g$ and $\epsilon(g) = 1$.*
*2) We set $G(C) := \{g \in C \mid g \text{ is grouplike}\}$.*
*3) Let $x \in C$, $g, h \in G(C)$. We say $x$ is $(g, h)$-primitive or skew-primitive, if $\Delta(x) = g \otimes x + x \otimes h$.*

PROPOSITION 3.15. — *Let $C$ be a coalgebra.*

*1) If $g \in C$ satisfies $\Delta(g) = g \otimes g$ and $g \neq 0$ then $\epsilon(g) = 1$.*
*2) If $x \in C$ is skew-primitive, then $\epsilon(x) = 0$.*

PROPOSITION 3.16. — *If $A$ is a finite dimensional algebra, then $G(A^*) = \mathrm{Alg}_k(A, k)$.*

*Proof.* — Let $f \in A^*$. Then $f \in G(A^*)$ if and only if $1 = \epsilon_{A^*}(f) = f(1_A)$ and $f_1 \otimes f_2 = f \otimes f$, which is equivalent to $f(a)f(b) = f(ab)$ for all $a, b \in A$. $\qquad \square$

LEMMA 3.17 (DEDEKIND). — *Let $M$ be a set, $\mu : M \times M \to M$ a map, $k$ a field. Then*

$$X = \{f \in k^M \setminus 0 \mid f(\mu(a, b)) = f(a)f(b) \text{ for all } a, b \in M\}$$

*is a linear independent subset of $k^M$.*

*Proof.* — Suppose that $X$ is not linear independent. Then there are distinct elements $f_1, \ldots, f_n \in X$ that linear dependent such that all proper subsets of $\{f_1, \ldots, f_n\}$ are linear independent. Hence we may write

$$f_1 = \sum_{i \geq 2} \lambda_i f_i.$$

Thus for all $a, b \in M$:

$$\left( \sum_{i \geq 2} \lambda_i f_i(a) \right) \left( \sum_{j \geq 2} \lambda_j f_j(b) \right) = f_1(a) f_2(b)$$
$$= f_1(\mu(a, b))$$
$$= \sum_{i \geq 2} \lambda_i f_i(\mu(a, b))$$
$$= \sum_{i \geq 2} \lambda_i f_i(a) f_i(b).$$

This implies that $f_2, \ldots, f_n$ are linear dependent, contradicting our minimality assumption. $\qquad \square$

THEOREM 3.18. — *If $C$ is a coalgebra, then $G(C) \subset C$ is linear independent.*

*Proof.* — The injective coalgebra homomorphism

$$\psi : C \to C^{**}, \quad x \mapsto (f \to f(x))$$

restricts to an injective linear map

$$G(C) \to G(C^{**}) = \mathrm{Alg}(C^*, k).$$

Since $\mathrm{Alg}(C^*, k) \subset C^{**}$ is linear independent by Dedekind's lemma, it follows that $G(C) \subset C$ is linear independent. $\qquad \square$

DEFINITION 3.19. — *Let $C$ be a coalgebra. A subspace $I \subset C$ is a coideal if $\Delta(I) \subset C \otimes I + I \otimes C$ and $\epsilon(I) = 0$. In this case $C/I$ is a coalgebra as well.*

*Proof.* — The conditions on $I$ are precisely what we require for $\epsilon$ to factor over $C/I$ and for $\Delta$ to factor over $C/I \otimes C/I$. The coalgebra axioms of $C/I$ then follow from the coalgebra axioms of $C$. $\qquad \square$

REMARK 3.20. — *If $X, Y$ are vector spaces and $U \subset X$, $V \subset X$ are subspaces, then $U \otimes V \subset X \otimes Y$ is a subspace. This needs not hold for tensor products over arbitrary rings.*

PROPOSITION 3.21. — *Let $\varphi : C \to C'$ be a coalgebra homomorphism. Then $\ker(\varphi) \subset C$ is a coideal and $\operatorname{im}(\varphi) \subset C'$ is a subcoalgebra. The map $\varphi$ induces a coalgebra isomorphism*

$$\bar{\varphi} : C/\ker(\varphi) \to \operatorname{im}(\varphi), \quad \bar{x} \mapsto \varphi(x).$$

*Proof.* — The homomorphism theorem for modules gives us that $\bar{\varphi}$ is a well-defined $k$-linear map. As $\varphi$ is a coalgebra homomorphism it follows that $\bar{\varphi}$ is aslo a coalgebra homomorphism. □

## 3.2. Hopf algebras. —

DEFINITION 3.22. — *Let $H$ be a $k$-algebra and let $\Delta : H \to H \otimes H$ and $\epsilon : H \to k$ be $k$-linear maps.*

1) *$H$ is a bialgebra, with $(H, \Delta, \epsilon)$ is a coalgebra and $\Delta$ and $\epsilon$ are algebra homomorphisms.*

2) *$H$ is a Hopf algebra if it is a bialgebra and $\operatorname{id} \in \operatorname{Hom}_k(H, H)$ has an $*$-inverse $S$. That is, if there exists a linear map $S : H \to H$ such that*

$$S(x_1)x_2 = \epsilon(x)1_H = x_1 S(x_2)$$

*for all $x \in H$. We way $S$ the antipode of $H$. Note that any bialgebra may have at most one antipode.*

EXAMPLE 3.23. —     *1) If $G$ is a group then $k[G]$ is a Hopf algebra.*

*Proof.* — $\Delta$ and $\epsilon$ are algebra homomorphisms by construction (via the universal property of the monoid algebra). Let $S : k[G] \to k[G]^{\mathrm{op}}$ be the algebra homomorphism with $S(g) = g^{-1}$. Then $S$ satisfies the antipode axioms. □

2) *If $H$ is a Hopf algebra and $g \in G(H)$ then $S(g) = g^{-1}$.*

*Proof.* — $\epsilon(g) = 1$ implies $S(g)g = 1_H = gS(g)$. □

3) *If $H$ is a Hopf algebra, and $x \in H$ is $(g, h)$-primitive, then $S(x) = -g^{-1}xh^{-1}$.*

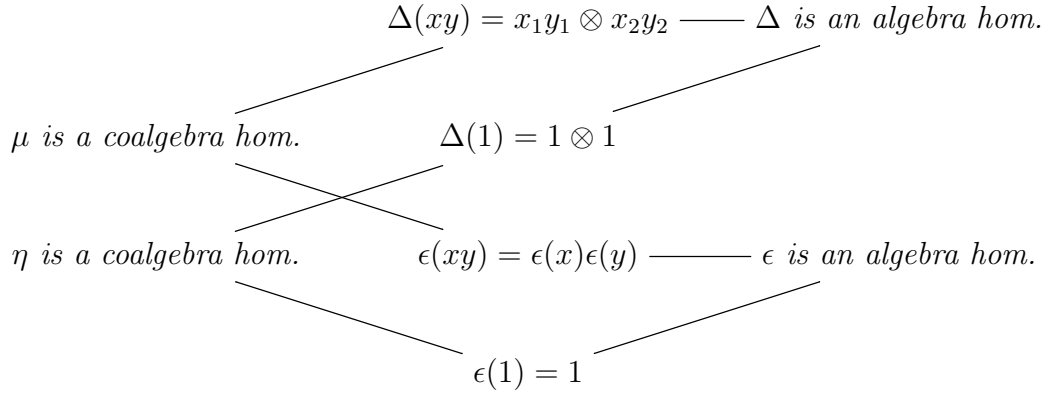*Proof.* — $\Delta(x) = g \otimes x + x \otimes h$ and $\epsilon(x) = 0$ implies

$$0 = S(g)x + S(x)h = g^{-1}x + S(x)h.$$

We know that $h$ is invertible because it is grouplike, hence

$$S(x) = -g^{-1}xh^{-1}.$$

□

PROPOSITION 3.24. — *Let $H$ be an algebra and $(H, \Delta, \epsilon)$ a coalgebra. Then*

$$\Delta(xy) = x_1 y_1 \otimes x_2 y_2 \quad\rule{1cm}{0.4pt}\quad \Delta \text{ is an algebra hom.}$$

$\mu$ *is a coalgebra hom.* $\qquad \Delta(1) = 1 \otimes 1$

$\eta$ *is a coalgebra hom.* $\qquad \epsilon(xy) = \epsilon(x)\epsilon(y) \quad\rule{1cm}{0.4pt}\quad \epsilon \text{ is an algebra hom.}$

$$\epsilon(1) = 1$$

DEFINITION 3.25. —    1) *If $C$ is a coalgebra, we may form the coalgebra $C^{\mathrm{cop}}$ with*
$\Delta_{C^{\mathrm{cop}}}(x) = x_2 \otimes x_1$.

2) *We say a coalgebra $C$ is cocommutative, if $x_1 \otimes x_2 = x_2 \otimes x_1$ for all $x \in C$.*

3) *Let $A, B$ be algebras. An anti-algebra homomorphism $\varphi : A \to B$ is an algebra homomorphism $\varphi : A^{\mathrm{op}} \to B$.*

4) *Let $C, D$ be coalgebras. An anti-coalgebra homomorphism $\psi : C \to D$ is a coalgebra homomorphism $\psi : C^{\mathrm{cop}} \to D$.*

5) *Let $H_1$ and $H_2$ be bialgebras. A linear map $\varphi : H_1 \to H_2$ is a bialgebra homomorphism if $\varphi$ is both an algebra homomorphism and a coalgebra homomorphism.*

6) *Hopfalgebra homomorphisms are bialgebra homomorphisms.*

7) *Subcoalgebras, subbialgebras and sub Hopf algebras are defined in a canonical way.*

THEOREM 3.26. —    1) *Let $H_1$ and $H_2$ be Hopf algebras and $\varphi : H_1 \to H_2$ a bialgebra homomorphism. Then $S_{H_2}\varphi = \varphi S_{H_1}$.*

2) *Let $H_1 \subset H_2$ be a sub Hopf algebra. Then $S_{H_2}(H_1) \subset H_1$ and $S_{H_1} = (S_{H_2})|_{H_1}$.*

*Proof.* — 1) The idea is to show that $S_{H_2}\varphi$ and $\varphi S_{H_1}$ are both $*$-inverse to $\varphi$ in the algebra $\mathrm{Hom}_k(H_1, H_2)$. To this end, note that for all $x \in H_1$

$$S_{H_2}(\varphi(x_1))\varphi(x_2) = S_{H_2}(\varphi(x)_1)\varphi(x)_2 = \epsilon(\varphi(x))1 = \epsilon(x)1$$

and likewise $\varphi(x_1)S_{H_2}(\varphi(x_2)) = \epsilon(x)1$. Thus $S_{H_2}\varphi$ the $*$-inverse of $\varphi$.

It also holds that

$$\varphi(S_{H_1}(x_1))\varphi(x_2) = \varphi(S_{H_1}(x_1)x_2) = \varphi(\epsilon(x)1) = \epsilon(x)1$$

and likewise $\varphi(x_1)\varphi(S_{H_1}(x_2)) = \epsilon(x)1$. This shows that $\varphi S_{H_1}$ is the $*$-inverse of $\varphi$ and hence must be identical to $S_{H_2}\varphi$.

2) Let $\iota : H_1 \subset H_2$ be the inclusion map. By 1) we know that $S_{H_2}\iota = \iota S_{H_1}$, so $S_{H_2}(H_1) \subset H_1$ and $S_{H_1} = (S_{H_2})|_{H_1}$. $\qquad\qquad\square$

PROPOSITION 3.27. —    1) *If $C$ is a coalgebra, then $k^{(G(C))} \subset C$ is a subcoalgebra.*

2) *If $B$ is a bialgebra, then $G(B)$ is a monoid and $k[G(B)] \subset B$ is a subbialgebra.*

3) *If $H$ is a Hopf algebra, then $G(H)$ is a group and $k[G] \subset H$ is a sub Hopf algebra.*

PROPOSITION 3.28. — *Let $H$ be a Hopf algebra with antipode $S$.*

1) *$S$ is an anti-algebra homomorphism.*

*Proof.* — Consider the map

$$\varphi : H \otimes H \to H, \quad x \otimes y \mapsto S(xy)$$

and the map

$$\psi : H \otimes H \to H, \quad x \otimes y \mapsto S(y)S(x).$$

We are going to show $\phi = \psi$ by verifying that both maps are both left $*$-inverse to the multiplication $\mu$.

Indeed

$$\varphi(x_1 \otimes y_1)\mu(x_2 \otimes y_2) = S(x_1 y_1)(x_2 y_2) = S((xy)_1)(xy)_2 = \epsilon(xy)1_H = \epsilon(x)\epsilon(y)1_H$$

implies that $\varphi * \mu = \eta_H \epsilon_{H \otimes H}$. Analogously we may check that $\mu * \varphi = \eta_H \epsilon_{H \otimes H}$. Furthermore

$$\psi(x_1 \otimes y_1)\mu(x_2 \otimes y_2) = S(y_1)S(x_1)x_2 y_2 = \epsilon(x)S(y_1)y_2 = \epsilon(x)\epsilon(y)1_H.$$

Hence $\psi = \mu^{-1} = \varphi$ in $\operatorname{Hom}(H \otimes H, H)$. $\square$

2) *$S$ is an anti-coalgebra homomorphism.*

*Proof.* — Consider

$$\varphi : H \to H \otimes H, \quad x \mapsto S(x_2) \otimes S(x_1)$$

and

$$\psi : H \to H \otimes H \otimes H, \quad x \mapsto S(x)_1 \otimes S(x)_2.$$

We are going to show that $\varphi = \Delta^{-1} = \psi$ in the algebra $\operatorname{Hom}(H, H \otimes H)$.

To this end, note that for all $x \in H$:

$$\begin{aligned}
\Delta(x_1)\varphi(x_2) &= (x_1 \otimes x_2)(S(x_4) \otimes S(x_3)) \\
&= x_1 S(x_4) \otimes x_2 S(x_3) \\
&= x_1 S(x_3) \otimes \epsilon(x_2)1_H \\
&= x_1 S(\epsilon(x_2)x_3) \otimes 1_H \\
&= x_1 S(x_2) \otimes 1_H \\
&= \epsilon(x)1_H \otimes 1_H.
\end{aligned}$$

This shows that $\Delta * \varphi = \eta_{H \otimes H} \epsilon_H$ in $\operatorname{Hom}(H, H \otimes H)$. Analogously, we may check that $\varphi * \Delta = \eta_{H \otimes H} \epsilon_H$.

Furthermore, it holds that

$$\Delta(x_1)\psi(x_2) = \Delta(x_1)\Delta(S(x_2)) = \Delta(x_1 S(x_2)) = \epsilon(x)\Delta(1) = \epsilon(x)1 \otimes H.$$

This show that $\psi = \Delta^{-1}$ in $\mathrm{Hom}(H, H \otimes H)$.                           □

*3) The following three conditions are equivalent:*
  *a) $S^2 = \mathrm{id}$*
  *b) $x_2 S(x_1) = \epsilon(x)1_H$ for all $x \in H$*
  *c) $S(x_2)x_1 = \epsilon(x)1_H$ for all $x \in H$*

*Proof.* — $a) \Rightarrow b)$: Suppose that $a)$ holds. Then $S$ is bijective and

$$S(x_2 S(x_1)) = S^2(x_1)S(x_2) = x_1 S(x_2) = \epsilon(x)1 = S(\epsilon(x)1).$$

hence $x_2 S(x_1) = \epsilon(x)$.
  $b) \Rightarrow a)$: Suppose that $b)$ holds. Then

$$\epsilon(x)1_H = S^2(x_1)S(x_2).$$

Hence $S^2$ is left-$*$-inverse to $S$, yielding $S^2 = \mathrm{id}$.
  The equivalence $a) \Leftrightarrow c)$ may be proven analogously.                           □

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

COROLLARY 3.29. — *Let $H$ be an algebra and $M \subset H$ an algebra generating system.*

  *1) Suppose that $\Delta : H \to H \otimes H$, and $\epsilon : H \to k$ are algebra homomorphisms. Then $H$ is a bialgebra if the axioms are satisfied on $M$.*
  *2) Suppose that $H$ a bialgebra, $S : H \to H$ an anti-algebrahomomorphism. Then $H$ is a Hopf algebra if the axioms are satisfied on $M$.*

COROLLARY 3.30. — *1) Let $H$ be a bialgebra, $A$ a commutative algebra. Then $\mathrm{Alg}_k(H, A)$ is a monoid. If $H$ is a Hopf algebra, then it is a group.*

*Proof.* — For $\varphi, \psi \in \mathrm{Alg}_k(H, A)$ the commutativity of $A$ implies that

$$\begin{aligned}
(\varphi * \psi)(xy) &= \varphi(x_1 y_1)\psi(x_2 y_2) \\
&= \varphi(x_1)\psi(x_2)\varphi(y_1)\psi(y_2) \\
&= (\varphi * \psi)(x)(\varphi * \psi)(y)
\end{aligned}$$

As $(\varphi * \psi)(1) = \varphi(1)\psi(1) = 1$ this implies that $\mathrm{Alg}_k(H, A)$ is a monoid.
  Suppose that $H$ is a Hopf algebra. As $A$ is commutative it follows that $\varphi S$ is an algebra homomorphism. We are going to check that $\varphi S$ is the inverse of $\varphi$. To this end:

$$\varphi(S(x_1))\varphi(x_2) = \varphi(S(x_1)x_2) = \epsilon_H(x)1$$

and

$$\varphi(x_1)\varphi(S(x_2)) = \varphi(x_1 S(x_2)) = \epsilon_H(x)1.$$

$\square$

*2) Let $H$ be a bialgebra, $C$ a cocommutative coalgebra. Then $\mathrm{Coalg}_k(C, H)$ is a monoid. If $H$ is a Hopf algebra, then it is a group.*

*Proof.* — Let $\varphi, \psi \in \mathrm{Coalg}_k(C, H)$. Then the cocommutativity of $C$ implies that

$$\begin{aligned}
\Delta_H((\varphi * \psi)(x)) &= \Delta_H(\varphi(x_1))\Delta_H(\psi(x_2)) \\
&= (\varphi(x_1) \otimes \varphi(x_2))(\psi(x_3) \otimes \psi(x_4)) \\
&= \varphi(x_1)\psi(x_3) \otimes \varphi(x_2)\psi(x_4) \\
&= \varphi(x_1)\psi(x_2) \otimes \varphi(x_3)\psi(x_4) \\
&= (\varphi * \psi)(x_1) \otimes (\varphi * \psi)(x_2).
\end{aligned}$$

Moreover,

$$\epsilon_H((\varphi * \psi)(x)) = \epsilon_H(\varphi(x_1))\epsilon_H(\psi(x_2)) = \epsilon_C(x_1)\epsilon_C(x_2) = \epsilon_C(\epsilon_C(x_1)x_2) = \epsilon_C(x).$$

This shows that $\mathrm{Coalg}_k(C, H)$ is a monoid.

Suppose that $H$ is a Hopf algebra. We are going to show that $S\varphi$ is the $*$-inverse of $\varphi$. Indeed:

$$(S\varphi)(x_1)\varphi(x_2) = S(\varphi(x_1))\varphi(x_2) = S(\varphi(x)_1)\varphi(x)_2 = \epsilon_H(\varphi(x))1_H = \epsilon_C(x)1_H.$$

That is, $S\varphi * \varphi = \eta_H\epsilon_C$. Likewise, we may check that $\varphi * S\varphi = \eta_H\epsilon_C$. $\square$

THEOREM 3.31. — *We have an equivalence of categories*

$$\{B \mid B \text{ f. d. } k\text{-bialgebra}\}^{\mathrm{op}} \simeq \{B \mid B \text{ f. d. } k\text{-bialgebra}\}$$

*with $B \mapsto B^*$. It restricts to*

$$\{H \mid H \text{ f. d. Hopf algebra over } k\}^{\mathrm{op}} \simeq \{H \mid H \text{ f. d. Hopf algebra over } k\}$$

*Proof.* — We know that if $B$ if a finite dimensional $k$-bialgebra then $B^*$ is both an algebra and a coalgebra. In order to check that it is a bialgebra, we have to verify that $\Delta_{B^*}$ and $\epsilon_{B^*}$ are algebra homomorphisms.

Recall that

$$B^* \xrightarrow{\mu_B^*} (B \otimes B)^* \xrightarrow{\simeq} B^* \otimes B^*.$$
$$\underbrace{\qquad\qquad\qquad}_{\Delta_{B^*}}$$

The map

$$B^* \xrightarrow{\mu_B^*} (B \otimes B)^*, \quad f \mapsto (x \otimes y \mapsto f(xy))$$

is an algebra homomorphism (since $\mu_B : B \otimes B \to B$ is a coalgebra homomorphism), and the isomorphism

$$B^* \otimes B^* \simeq (B \otimes B)^*, \quad (f \otimes g) \mapsto (x \otimes y \mapsto f(x)g(y))$$

is an algebra homomorphism as well. This shows that $\Delta_{B^*}$ is an algebra homomorphism.

Recall that

$$B^* \xrightarrow{\eta_B^*} k^* \xrightarrow{\simeq} k \ .$$
$$\underset{\epsilon_{B^*}}{\searrow \nearrow}$$

The map $\epsilon_{B^*}$ is an algebra homomorphism: The map

$$B^* \xrightarrow{\eta_B^*} k^*, \quad f \mapsto (\lambda \mapsto \lambda f(1))$$

preserves the algebra structure (as $\eta : k \to B$ is a coalgebra homomorphism) and the map

$$k^* \simeq k, \quad g \mapsto g(1)$$

is an algebra isomorphism. Here $k^*$ becomes an algebra via the coalgebra structure $\Delta_k(\lambda) = \lambda 1_k \otimes 1_k$ and $\epsilon_k(\lambda) = \lambda$ for $\lambda \in k$.

The functorial vector space isomorphism

$$\varphi : B \to B^{**}, \quad b \mapsto (f \mapsto f(b))$$

preserves both the algebra and coalgebra structures, and is hence a bialgebra isomorphism. This proves the first equivalence of categories.

In order to prove the second equivalence, it remains to show that if $H$ is a finite dimensional Hopf algebra, then $H^*$ is a Hopfalgebra with antipode $S_{H^*} = S_H^*$, that is $S_{H^*}(f) = fS$ for all $f \in H^*$.

Indeed, it holds that

$$f_1 * f_2(S) = \epsilon_{H^*}(f) 1_{H^*}$$

because for all $x \in H$

$$f_1(x_1)f_2(S(x_2)) = f(x_1 S(x_2)) = f(\epsilon(x)1_H) = \epsilon(x)f(1_H) = 1_{H^*}(x)\epsilon_{H^*}(f).$$

Likewise we may verify that

$$f_1(S) * f_2 = \epsilon_{H^*}(f) 1_{H^*}.$$

$\square$

DEFINITION 3.32. — *1) $H$ a bialgebra, $I \subset H$ a subspace. We say $I$ is a biideal, if it is both an ideal an a coideal. In this case $H/I$ is a bialgebra.*

*2) If $\phi : H \to H'$ is a bialgebra homomorphism then $\ker \phi \subset H$ is a biideal. The usual homorphism theorems hold.*

*3) If $H$ and $H'$ are bialgebras then so is $H \otimes H'$.*

DEFINITION 3.33. — *1) $H$ a Hopf algebra. A biideal $I \subset H$ is a Hopf ideal if $S(I) \subset I$. In this case $S/I$ is a Hopf algebra.*

*2) If $\phi : H \to H'$ is a Hopf algebra homomorphism then $\ker \phi \subset H$ is a Hopf ideal.*

*3) If $H$ and $H'$ are Hopf algebras, then so is $H \otimes H'$.*

PROPOSITION 3.34. — *Let $H$ be a bialgebra, $G \subset G(H)$ a subset. Then $I =< g-1 \mid g \in G >$ (the ideal generated by all elements $g-1$) is a biideal of $H$. If $H$ is Hopf algebra, then it is a Hopf ideal.*

*Proof.* — $I$ is an ideal be definition. It is a coideal because for all $g \in G$ it holds that $\epsilon(g-1) = 0$ and

$$\Delta(g-1) = g \otimes g - 1 \otimes 1 = g \otimes (g-1) + (g-1) \otimes 1 \in H \otimes I + I \otimes H.$$

Moreover, if $H$ is a Hopf algebra then $I$ is an Hopf ideal, since $S(g-1) = S(g) - 1 = g^{-1} - 1 = -g^{-1}(g-1) \in HI \subset I$. □

**3.3. Examples.** — In the previous section we saw that when $H$ is a Hopf algebra, then $\mathrm{Alg}(H, -)$ is a functor from the category of commutative algebras to the category of groups. The following are few examples of Hopf algebras for which we may determine this functor explicitly.

EXAMPLE 3.35. — *1) The polynomial algebra $k[T]$ is a Hopf algebra with $T$ primitive. It holds that*

$$\Delta(T^n) = \sum_{i=0}^{n} \binom{n}{i} T^i \otimes T^{n-i}$$

*for all $n \geq 0$. If $A$ is a commutative algebra then*

$$\mathrm{Alg}_k(k[T], A) \to (A, +), \quad \varphi \mapsto \varphi(T)$$

*is a group isomorphism.*

*Proof.* — For $\varphi, \psi \in \mathrm{Alg}_k(k[T], A)$ it holds that

$$(\varphi * \psi)(T) = \varphi(T)\psi(1) + \varphi(1)\psi(T) = \varphi(T) + \psi(T).$$

□

*2) If $\mathrm{char}(k) = p$ then $(T^p) \subset k[T]$ is a Hopf-ideal and $k[T]/(T^p)$ is a quotient Hopf algebra. For any commutative algebra $A$ set $\alpha_p(A) = \{a \in A \mid a^p = 0\}$. Then*

$$\mathrm{Alg}_k(k[T]/(T^p), A) \to \alpha_p(A), \quad \varphi \mapsto \varphi(\bar{T})$$

*is a group isomorphism that is functorial in $A$.*

EXAMPLE 3.36. — *The polynomial ring $B = k[T_{i,j} \mid 1 \le i,j \le n]$ is a bialgebra with $\Delta(T_{i,j}) = \sum_{1 \le \ell \le n} T_{i,\ell} \otimes T_{\ell,j}$ and $\epsilon(T_{i,j}) = \delta_{i,j}$. Consider the matrix $M = (T_{i,j})_{i,j} \in M_n(B)$ and set $d = \det(M)$. Then $d$ is a group-like element, because*

$$\Delta(d) = \det(\sum_{1 \le \ell \le n} T_{i,\ell} \otimes T_{\ell,j})_{i,j}$$
$$= (\det(T_{i,j} \otimes 1)_{i,j})(\det(1 \otimes T_{i,j})_{i,j})$$
$$= (d \otimes 1)(1 \otimes d)$$
$$= d \otimes d.$$

*Hence $(d - 1) \subset B$ is a biideal and $H = B/(d - 1)$ is a bialgebra.*

*By Cramer's rule there is a matrix $N = (t_{i,j})_{i,j} \in M_n(B)$ with*

$$MN = NM = dI.$$

*Note that this implies $\det(N) = d^{n-1}$ since $B$ is an integral domain. Let $S : B \to H$ be the algebra homomorphism with $S(T_{i,j}) = \bar{t}_{i,j}$. Then*

$$S(d - 1) = \det(\bar{t}_{i,j})_{i,j} - 1 = 0.$$

*Hence $S$ induces an algebra homomorphism $\bar{S} : H \to H$ with*

$$\bar{S}(\bar{T}_{i,j}) = \bar{t}_{i,j}.$$

*We may verify that $\bar{S}$ is an antipode of $H$, making $H$ a Hopf algebra:*

$$(\Delta(T_{i,j}))_{i,j} = (T_{i,j} \otimes 1)_{i,j}(1 \otimes T_{i,j})_{i,j}$$

*and hence*

$$((\bar{T}_{i,j})_1 \bar{S}((\bar{T}_{i,j})_2))_{i,j} = (S((\bar{T}_{i,j})_1)(\bar{T}_{i,j})_2)_{i,j} = I = (\bar{\epsilon}(\bar{T}_{i,j})1)_{i,j}.$$

*If $A$ is a commutative algebra, then*

$$\mathrm{Alg}(k[T_{i,j}]/(d-1), A) \to \mathrm{SL}_n(A), \quad \varphi \mapsto (\varphi(\bar{T}_{i,j}))_{i,j}$$

*is a group isomorphism that is functorial in $A$.*

DEFINITION 3.37. — *Let $v$ be an indeterminate. In the field $\mathbb{Q}(v)$ we define for $0 \le i \le n$*

(3.1) $$(n)_v = \frac{v^n - 1}{v - 1} = 1 + \ldots + v^{n-1} \in \mathbb{Z}[v]$$

(3.2) $$(n)_v! = (1)_v \cdot \ldots \cdot (n)_v \in \mathbb{Z}[v]$$

(3.3) $$\binom{n}{i}_v = \frac{(n)_v!}{(i)_v!(n-i)_v!} \in \mathbb{Z}[v].$$

*For $i < 0$ or $i > n$ we set $\binom{n}{i}_v = 0$.*

LEMMA 3.38. — *For $0 < i < n$ it holds that*

$$\binom{n}{i}_v = \binom{n-1}{i-1}_v + v^i \binom{n-1}{i}_v.$$

*Proof.* —

$$\binom{n-1}{i-1}_v + v^i \binom{n-1}{i}_v = \frac{(n-1)_v!}{(i-1)_v!(n-i)_v!} + \frac{v^i(n-1)_v!}{(i)_v!(n-i-1)_v!}$$

$$= \frac{(n-1)_v!((i)_v + v^i(n-i)_v)}{(i)_v!(n-i)_v!}$$

Since

$$(i)_v + v^i(n-i)_v = 1 + \ldots + v^i + v^i(1 + \ldots v^{n-i}) = (n)_v$$

it follows that this expression is equal to $\binom{n}{i}_v$. □

DEFINITION 3.39. — *Given $q \in k$ there is a ring homomorphism $\mathbb{Z}[v] \to k$ with $v \mapsto q$. We let $(n)_q$, $(n)_q!$, and $\binom{n}{i}_q$ denote the images of $(n)_v$, $(n)_v!$, and $\binom{n}{i}_v$ under this homomorphism.*

COROLLARY 3.40. — *Let $A$ be an algebra, $a, b \in A$, $ba = qab$ for some $q \in k$.*
  1) $(a+b)^n = \sum_{i=0}^n \binom{n}{i}_q a^i b^{n-i}$
  2) *If $q$ is a primitive $n$th root of unity then $\binom{n}{i}_q = 0$ for $1 \leq i \leq n-1$ and hence $(a+b)^n = a^n + b^n$.*

*Proof.* — 1) By induction on $n$. If $(a+b)^n = \sum_{i=0}^n \binom{n}{i}_q a^i b^{n-i}$ then

$$(a+b)(a+b)^n = \sum_{i=0}^n \binom{n}{i}_q a^{i+1} b^{n-i} + q^i \sum_{i=0}^n \binom{n}{i}_q a^i b^{n+1-i}$$

$$= a^n + b^n + \sum_{k=1}^n \left(\binom{n}{k-1}_q + q^k \binom{n}{k}_q\right) a^k b^{n+1-k}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}.$$

2) Suppose that $n \geq 2$. Since

$$(q-1)(i)_q = q^i - 1$$

it follows that $(i)_q \neq 0$ for $0 \leq i < n$ and $(n)_q = 0$. Hence for $0 < i < n$ it follows that

$$(i)_q!(n-i)_q! \binom{n}{i}_q = (n)_q! = 0,$$

and hence $\binom{n}{i}_q = 0$. □

EXAMPLE 3.41. —    *1) For $q \in k^\times$ the bialgebra*

$$H = k < g, x \mid gx = qxg >= k < g, x > /(gx - qxg)$$

*with $g$ group-like and $x$ $(g, 1)$-primitive is called the quantum plane.*

*Proof.* — We may define a bialgebra structure on $k < g, x >$ with $g$ group-like and $x$ $(g, 1)$-primitive. The ideal $(gx - qxg)$ is a biideal, since

$$\Delta(gx - qxg) = g^2 \otimes gx + gx \otimes g - qg^2 \otimes xg - qxg \otimes g$$
$$= g^2 \otimes (gx - qxg) + (gx - qxg) \otimes g$$

This makes $H = k < g, x \mid gx = qxg >$ a bialgebra.                    □

*2) For $q \in k^\times$ the Hopf algebra*

$$H =< g, h, x \mid gh = 1 = hg, gx = qxg >$$

*with $g, h$ group-like, $x$ $(g, 1)$-primitive has an antipode with $S(x) = q^{-1}x$.*

*Proof.* — It is clear that $H$ is a bialgebra. Let $\hat{S} : k[G, H, X] \to H$ be the anti-algebra homomorphism with $\hat{S}(G) = h$, $\hat{S}(H) = g$, and $\hat{S}(x) = -hx$. Then $\hat{S}$ factorizes over $H$, since

$$\hat{S}(GH) = \hat{S}(hg) = 1$$

and

$$\hat{S}(GX - qXG) = -hxh + qh^2x = 0.$$

It is clear that the induced map $S$ satisfies the antipode axioms. Moreover, $S^2(x) = S(-hx) = hxg = q^{-1}hgx = q^{-1}x$.                    □

*3) Let $q \in k^\times$ be a primitive $n$th root of unity. Then*

$$H = k < g, x \mid g^n = 1, x^n = 0, gx = qxg >$$

*with $g$ group-like and $x$ $(g, 1)$-primitive is called the Taft Hopf algebra. Its antipode satisfies $S^2(x) = q^{-1}x$.*

*Proof.* — Consider $B = k < G, X >$ as a bialgebra with $G$-grouplike and $X$ $(G, 1)$-primitive. Then $I = (G^n - 1, X^n - 0, GX - qXG)$ is a biideal: We know that

$$\Delta(G^n - 1) \in I \otimes B + B \otimes I$$

because $G$ is group-like. We already made the calculations to verify

$$\Delta(GX - qXG) \in I \otimes B + B \otimes I.$$

Since $q$ is a primitive $n$th root of unity it follows by the $q$-binomial formula that

$$\Delta(X)^n = (g \otimes x + x \otimes 1)^n = g^n \otimes x^n + x^n \otimes 1 = 0.$$

Hence $H$ is a bialgebra. It is easy to check that $H$ is a Hopfalgebra with antipode $S(g) = g^{-1}$ and $S(x) = g^{-1}x$. □

## 4. $H$-module algebras and smash products

REMARK 4.1. — *1) Let $M$ be an abelian group, $R$ a ring. Then*

$$\{\mu : R \times M \to M \mid \mu \ R\text{-module structure}\} \simeq \mathrm{Alg}_{\mathbb{Z}}(R, \mathrm{End}_{\mathbb{Z}}(M))$$

$$\mu \mapsto (\lambda \mapsto (m \mapsto \mu(\lambda, m)))$$

$$((\lambda, m) \mapsto \delta(\lambda)(m)) \leftarrow\!\shortmid \delta$$

*is a bijection.*

*2) Let $V$ be a $k$-vector space, $A$ a $k$-algebra. Let us call an $A$-module structure on $V$ "extending", if the $k$-module structure on $V$ induced by $\eta : k \to A$ is identical to the vector space structure that is already present on $V$. (That is, $\lambda.v = (\lambda 1_A).v$ for $\lambda \in k$, $v \in V$.) Then the above bijection induces a vector space isomorphism*

$$\{\mu : A \times V \to V \mid \mu \ \text{extending } A\text{-module struct.}\} \simeq \mathrm{Alg}_k(A, \mathrm{End}_k(V)).$$

DEFINITION 4.2. — *Let $A$ be an algebra and let $S : A^{\mathrm{op}} \to A$, $\Delta : A \to A \otimes A$, $\epsilon : A \to k$ be algebra homomorphisms. Then for all $V, W \in {}_A\mathcal{M}$:*

$$k \in {}_A\mathcal{M} \ via \ \epsilon, \quad that \ is \ a.\lambda = \epsilon(a)\lambda$$

$$V \otimes_k W \in {}_A\mathcal{M} \ via \ \Delta, \quad that \ is \ a.(v \otimes w) = a_1 v \otimes a_2 w$$

$$\mathrm{Hom}_k(V, W) \in {}_A\mathcal{M} \ via \ \Delta, S, \quad that \ is \ (a.f)(v) = a_1 f(S(a_2)v)$$

$$V^* \in {}_A\mathcal{M} \ via \ S, \quad that \ is \ (a.f)(v) = f(S(a).v)$$

*Note that the module structure on $V^*$ needs not be a special case of the module structure on $\mathrm{Hom}_k(V, k)$ (with $(a.f)(v) = f(S(\epsilon(a_1)a_2).v)$), but it is if $\epsilon$ satisfies the counit axioms. In this setting:*

*1) The $k$-linear isomorphism $(U \otimes V) \otimes W \simeq U \otimes (V \otimes W)$ is $A$-linear for all $U, V, W \in {}_A\mathcal{M}$, if and only if $\Delta$ is coassociative.*

*2) The $k$-linear isomorphism $V \otimes k \simeq V \simeq k \otimes V$ is $A$-linear for all $V \in {}_A\mathcal{M}$, if and only if $\Delta, \epsilon$ satisfy the counit axioms.*

*3) The evaluation map $V^* \otimes V \to k$ is $A$-linear for all $V \in {}_A\mathcal{M}$, if and only if $S(a_1)a_2 = \epsilon(a)1_A$ for all $a \in A$.*

*4) The map $k \to \mathrm{End}_k(V)$ is $A$-linear for all $V \in {}_A\mathcal{M}$, if and only if $a_1 S(a_2) = \epsilon(a)1_A$ for all $a \in A$.*

*Proof.* — 1) It holds that

$$a.((u \otimes v) \otimes w) = a_{11}u \otimes a_{12}v \otimes a_2 w$$

and

$$a.(u \otimes (v \otimes w)) = a_1 u \otimes a_{21} v \otimes a_{22} w.$$

If $\Delta$ is coassociative then these two expressions are identical. Conversely, taking $U = V = A$ and $u = v = w = 1_A$ would yield coassociativity.

2) It holds that

$$a.(v \otimes \lambda) = a_1 v \otimes \epsilon(a_2)\lambda = \lambda(\epsilon(a_2)a_1)v \otimes 1.$$

and

$$a(\lambda v) = \lambda(av).$$

If $\epsilon$ is a counit, then the first expression corresponds to the second under the canonical isomorphism. Conversely, taking $V = A$, $v = 1_A$ and $\lambda = 1_k$ would yield the counit axiom.

3) It holds that

$$a.(f \otimes v) = a_1.f \otimes a_2 v = f(S(a_1) \cdot -) \otimes a_2 v$$

gets mapped to

$$f(S(a_1)a_2 v).$$

If $S(a_1)a_2 = \epsilon(a)$ then this is equal to $\epsilon(a)f(v) = a.f(v)$. Conversely, if the evaluation map is always $A$-linear, then taking $V = A$, $v = 1_A$ yields $f(S(a_1)a_2) = f(\epsilon(a)1_A)$ for all $f \in A^*$ which implies $S(a_1)a_2 = \epsilon(a)1_A$.

4) The element $a.\lambda = \epsilon(a)\lambda$ gets mapped to

$$v \mapsto \epsilon(a)\lambda v.$$

This is equal to

$$a.(v \mapsto \lambda v) = (v \mapsto a_1 S(a_2)v)$$

if $S$ satisfies the second antipode axiom. Conversely, taking $V = A$, $v = 1_A$ yields the second antipode axiom if $k \to \mathrm{End}_k(A)$ is $A$-linear.

□

DEFINITION 4.3. — *Let $H$ be a bialgebra, $A$ an algebra.*

*1) Let $H$ be an $A$-left-module such that $H \to \mathrm{End}_k(A)$ is an algebra homomorphism. We say $A$ is an $H$ left module algebra if for all $a, b \in A$ and $x \in H$*

$$x.(ab) = (x_1.a)(x_2.b) \qquad and \qquad x.1_A = \epsilon(x)1_A.$$

*That is, we require that $\mu_A$ and $\eta_A$ are $H$-linear. It suffices to verify these axioms on an algebra generating set of $H$.*

*2) Let $\sigma, \tau \in \mathrm{Alg}_k(A, A)$, $\delta \in \mathrm{Hom}_k(A, A)$. We say $\delta$ is a $(\sigma, \tau)$-derivation, if*

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)\tau(b).$$

*This is equivalent to requiring that*

$$A \to M_2(A), \quad a \mapsto \begin{pmatrix} \sigma(a) & \delta(a) \\ 0 & \tau(a) \end{pmatrix}$$

*is an algebra homomorphism.*

PROPOSITION 4.4. — *Let $H$ be a bialgebra, $A$ a $H$ left module algebra, $g, h \in G(H)$, and $x \in H$ $(g, h)$-primitive. Then the element $g \in B$ operates on $A$ as an algebra homomorphism. That is, $A \to A, a \mapsto g.a$ is an algebra homomorphism. The element $x$ operates on $A$ as a $(g.-, h.-)$-derivation.*

*Proof.* — It holds that

$$g.(ab) = (g_1.a)(g_2.b) = (g.a)(g.b)$$

and

$$g.(1_A) = \epsilon(g)1_A = 1_A.$$

Moreover,

$$x.(ab) = (g.a)(x.b) + (x.a)(h.b).$$

$\square$

DEFINITION 4.5. — *Let $H$ be a bialgebra, $A$ an $H$ left module algebra. The algebra $A\#H := A \otimes H$ as vector space, with $a\#h = a \otimes h$ and*

$$(a\#g)(b\#h) = ag_1.b\#g_2.h$$

*for all $a, b \in A$, $g, h \in H$ is called the smash product algebra of $A$ and $H$. We use the notation*

$$a = a\#1 \in A\#H, \quad g = 1\#g \in A\#H.$$

*Thus $a\#g = (a\#1)(1\#g) = ag$ and*

$$ga = g_1.a\#g_2 = g_1.ag_2.$$

DEFINITION 4.6. — *Let $A$ be a $k$-algebra, $\sigma \in \mathrm{Alg}_k(A, A)$, $\delta : A \to A$ a $(\sigma, \mathrm{id})$-derivation. We define the algebra extension $A \subset A[x, \sigma, \delta]$ as follows. Let $H = k < g, x >$ be the bialgebra with $g$ group-like and $x$ $(g, 1)$-primitive. The algebra $A$ becomes an $H$ left module algebra via $g.a = \sigma(a)$ and $x.a = \delta(a)$ for all $a \in A$. We define the sub algebra*

$$A[x, \sigma, \delta] := A \otimes k[x] \subset A\#H.$$

*This is well-defined since $\Delta(k[x]) \subset H \otimes k[x]$. The extension $A \subset A[x, \sigma, \delta]$ is termed Ore extension. Every element $y \in A[x, \sigma, \delta]$ has a unique representation $y = \sum_{i \geq 0} a_i x^i$ (with but finitely many coefficients equal to zero). For $a \in A$ it holds that*

$$xa = g.a\#x + x.a\#1 = \sigma(a)x + \delta(a).$$

EXAMPLE 4.7. — *1) Weyl algebra: $k < x, t \mid xt = tx + 1 > \simeq k[T][X, \mathrm{id}, \frac{\mathrm{d}}{\mathrm{d}T}]$. Hence $(t^i x^j)_{i,j \geq 0}$ is a $k$-basis of the Weyl algebra.*

*2) Quantum plane: $k < g, x \mid gx = qxg > \simeq k[X] \# k[G]$, $q \in k^\times$, with $G$ group-like and $G.X = qX$. Hence $(x^i g^j)_{i,j \geq 0}$ is a $k$-basis of the quantum plane.*

*3) $k < g, h, x \mid gh = 1 = hg, gx = qxg > \simeq k[X] \# k(G)$, $q \in k^\times$ with $G$ group-like and $G.X = qX$. Hence $(x^i g^j)_{i \geq 0, j \in \mathbb{Z}}$ is a $k$-basis.*

*4) Taft Hopf algebra: For $q \in k^\times$ a primitive $n$-th root of unity*

$$k < g, x \mid g^n = 1, x^n = 0, gx = qxg > \simeq k[X]/(X^n) \# k[G]/(G^n - 1)$$

*with $G$ group-like, $G.X = qX$. Hence the Taft Hopf algebra has dimension $n^2$ and $(x^i g^j)_{0 \leq i,j < n}$ is basis.*

REMARK 4.8. — *For the Taft Hopf algebra $B$ we are in the situation*

$$
\begin{array}{ccc}
k[g] & \hookrightarrow & B \\
{\scriptstyle =}\downarrow & \swarrow & \\
k[g] & &
\end{array}
$$

*with the arrows denoting Hopf algebra homomorphisms. This is analogous to the semi-direct product: If $M$ and $H$ are groups with*

$$
\begin{array}{ccc}
H & \overset{\iota}{\hookrightarrow} & M \\
{\scriptstyle =}\downarrow & \swarrow {\scriptstyle \pi} & \\
H & &
\end{array}
$$

*then $M \simeq G \rtimes H$ with $G = \ker \pi$.*

EXAMPLE 4.9 (QUANTUM ENVELOPING ALGEBRA OF $\mathfrak{sl}_2$). — *Let $q \in k \setminus \{0, \pm 1\}$. Then the algebra $U_q(\mathfrak{sl}_2)$ generated by indeterminates $E, F, K, K^{-1}$ subject to the relations*

$$KK^{-1} = 1 = K^{-1}K$$

$$KEK^{-1} = q^2 E$$

$$KFK^{-1} = q^{-2} F$$

$$EF - FE = \frac{K - K^{-1}}{q - q^{-1}}$$

*is a Hopf algebra with $K$ group-like, $E$ $(K, 1)$-primitive, $F$ $(1, K^{-1})$-primitive. It holds that*

$$U_q(\mathfrak{sl}_2) \simeq A[E, \sigma, \delta]$$

*with*

$$A = k < F, K, K^{-1} \mid KK^{-1} = 1 = K^{-1}K, KF = q^{-2}FK >,$$

*and $\sigma \in \mathrm{Alg}_k(A, A)$ the algebra endomorphism with $\sigma(K) = q^{-2}K$ and $\sigma(F) = F$, and $\delta : A \to A$ the $(\sigma, \mathrm{id})$-derivation given by $\delta(K) = 0 = \delta(K^{-1})$ and $\delta(F) = (K - K^{-1})(q - q^{-1})$. In particular, $(F^i K^j E^\ell)_{i \in \mathbb{N}_0, j \in \mathbb{Z}, \ell \in \mathbb{N}_0}$ is a $k$-basis of $U_q(\mathfrak{sl}_2)$.*

*Proof.* — Checking that $U_q(\mathfrak{sl}_2)$ is a Hopf algebra will be an exercise. We are going to verify that $U_q(\mathfrak{sl}_2) \simeq A[E, \sigma, \delta]$.

To this end, let us first check that $A[E, \sigma, \delta]$ is well-defined. It is clear that $\sigma$ is a well-defined algebra homomorphism. As for $\delta$, we need to show that the algebra homomorphism $\varphi : A \to M_2(A)$ with

$$\varphi(F) = \begin{pmatrix} F & \frac{K - K^{-1}}{q - q^{-1}} \\ 0 & F \end{pmatrix}$$

$$\varphi(K) = \begin{pmatrix} q^{-2}K & 0 \\ 0 & K \end{pmatrix}$$

$$\varphi(K^{-1}) = \begin{pmatrix} q^2 K^{-1} & 0 \\ 0 & K^{-1} \end{pmatrix}$$

is well-defined. Indeed,

$$\varphi(K)\varphi(K^{-1}) = I = \varphi(K^{-1})\varphi(K),$$

and

$$\varphi(K)\varphi(F) = \begin{pmatrix} q^{-2}K & 0 \\ 0 & K \end{pmatrix} \begin{pmatrix} F & \frac{K - K^{-1}}{q - q^{-1}} \\ 0 & F \end{pmatrix} = \begin{pmatrix} q^{-2}KF & q^{-2}K\frac{K - K^{-1}}{q - q^{-1}} \\ 0 & KF \end{pmatrix},$$

and

$$\varphi(F)\varphi(K) = \begin{pmatrix} F & \frac{K - K^{-1}}{q - q^{-1}} \\ 0 & F \end{pmatrix} \begin{pmatrix} q^{-2}K & 0 \\ 0 & K \end{pmatrix}$$

$$= \begin{pmatrix} q^{-2}FK & \frac{K - K^{-1}}{q - q^{-1}}K \\ 0 & FK \end{pmatrix}$$

$$= \begin{pmatrix} KF & K\frac{K - K^{-1}}{q - q^{-1}} \\ 0 & q^2 KF \end{pmatrix}.$$

The relations of the $U_q(\mathfrak{sl}_2)$ hold in the Ore extension $A[E, \sigma, \delta]$. It is clear that

$$KK^{-1} = 1 = K^{-1}K \qquad \text{and} \qquad KF = q^{-2}FK$$

holds in $A[E, \sigma, \delta]$. Moreover,

$$EK = \sigma(K)E + \delta(K) = q^{-2}KE$$

and

$$EF = \sigma(F)E + \delta(F) = FE + \frac{K - K^{-2}}{q - q^{-1}}.$$

This yields well-defined algebra homomorphism

$$\psi : U_q(\mathfrak{sl}_2) \to A[E, \sigma, \delta].$$

By our previous examples we know that $A$ has a $k$-basis $(F^i K^j)_{i \geq 0, j \in \mathbb{Z}}$. Hence $A[E, \sigma, \delta]$ has a $k$-basis $(F^i K^j E^\ell)_{i \geq 0, j \in \mathbb{Z}, \ell \geq 0}$. The algebra homomorphism $\varphi$ maps the vector space generating family $(F^i K^j E^\ell)_{i \geq 0, j \in \mathbb{Z}, \ell \geq 0}$ of $U_q(\mathfrak{sl}_2)$ to the $k$-basis $(F^i K^j E^\ell)_{i \geq 0, j \in \mathbb{Z}, \ell \geq 0}$ of $A[E, \sigma, \delta]$. Hence it is an isomorphism. □

REMARK 4.10. — $\mathfrak{sl}_2 = \{A \in M_2(k) \mid \operatorname{tr}(A) = 0\}$ *has a $k$-basis given by*

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$\mathfrak{sl}_2$ *is a Lie algebra with Lie bracket given by* $[A, B] = AB - BA$. *Thus*

$$[h, e] = 2e, \quad [h, f] = -2f, \quad [e, f] = h.$$

*Its universal enveloping algebra*

$$U(\mathfrak{sl}_2) = k < e, f, h \mid he - eh = 2e, hf - fh = -2f, ef - fe = h >$$

*is a cocommutative Hopf algebra with* $e, f, h$ *primitive.*

## 5. Comodules and comodule algebras

DEFINITION 5.1. — *Let $C$ be a coalgebra.*

1) *Let $V$ be a vector space and $\delta : V \to V \otimes C$ a k-linear map that we denote by $\delta(v) = v_0 \otimes v_1$. We say $(V, \delta)$ is a right $C$ comodule if*

$$\delta(v_0) \otimes v_1 = v_0 \otimes \Delta(v_1)$$

$$v = v_0 \epsilon(v_1)$$

*for all $v \in V$. That is:*

$$
\begin{array}{ccccc}
V \otimes_k (C \otimes_k C) & \xleftarrow{\mathrm{id} \otimes \Delta} & V \otimes_k C & \xleftarrow{\delta} & V \\
\simeq \uparrow & & & \searrow \delta & \\
(V \otimes_k C) \otimes_k C & \xleftarrow{\delta \otimes \mathrm{id}} & V \otimes_k C &
\end{array}
$$

*and*

$$
\begin{array}{ccc}
V \otimes_k C & \xrightarrow{\mathrm{id} \otimes \epsilon} & V \otimes_k k \\
\delta \uparrow & \nearrow \simeq & \\
V & &
\end{array}
$$

2) *Let $(V, \delta_V)$ and $(W, \delta_W)$ be $C$ right comodules. A k-linear map $f : V \to W$ is a termed $C$-colinear or $C$ comodule homomorphism if*

$$\delta_W(f(v)) = f(v_0) \otimes v_1$$

*for all $v \in V$.*

3) *Left comodules are defined analogously. We let $\mathcal{M}^C$ and $^C\mathcal{M}$ denote the categories of $C$ right comodules and $C$ left comodules.*

4) *A subspace $V' \subset V$ of a $C$ right comodule $V$ is a subcomodule if $\delta(V') \subset V' \otimes C$.*

REMARK 5.2. — 1) *A coalgebra homomorphism $\varphi : C \to D$ induces a functor $\mathcal{M}^C \to \mathcal{M}^D$ with $(V, \delta) \mapsto (V, (\mathrm{id} \otimes \varphi)\delta)$.*

2) *Let $H$ be a bialgebra, $V, W \in \mathcal{M}^H$. Then $V \otimes_k W \in \mathcal{M}^H$ via $\delta(v \otimes w) = v_0 \otimes w_0 \otimes v_1 w_1$. Also $k \in \mathcal{M}^H$ via $k \to k \otimes H$, $1 \mapsto 1 \otimes 1$.*

*Proof.* — It holds that

$$v_0 \otimes w_0 \otimes \Delta(v_1 w_1) = v_0 \otimes w_0 \otimes v_1 w_1 \otimes v_2 w_2 = \delta(v_0 \otimes w_0) \otimes v_1 w_1$$

and

$$(v_0 \otimes w_0)\epsilon(v_1 w_1) = v \otimes w.$$

$\square$

LEMMA 5.3. — *$C$ a coalgebra, $V$ a finite dimensional vector space with basis $v_1, \ldots, v_n$.*

1) *Let $\delta : V \to V \otimes C$ be a $k$-linear with $\delta(v_j) = \sum_{i=1}^n v_i \otimes c_{i,j}$. The map $\delta$ is a $C$ right comodule structure if and only if $\Delta(c_{i,j}) = \sum_\ell c_{i,\ell} \otimes c_{\ell,j}$ and $\epsilon(c_{i,j}) = \delta_{i,j}$.*

*Proof.* — It holds that

$$\sum_{i=1}^n \delta(v_i) \otimes c_{i,j} = \sum_{h=1}^n \sum_{i=1}^n v_h \otimes c_{h,i} \otimes c_{i,j}.$$

$\square$

2) *Let $(e_{i,j})_{i,j}$ be the standard basis of $M_n(k)$ and $(x_{i,j})_{i,j}$ the corresponding dual basis of $M_n(k)^*$. Then*

$$\{\delta : V \to V \otimes C \mid \delta \text{ right comodule structure}\} \simeq \mathrm{Coalg}(M_n(k)^*, C)$$

$$\delta \mapsto \left( x_{i,j} \mapsto c_{i,j} \text{ with } \delta(v_j) = \sum_{i=1}^n v_i \otimes c_{i,j} \right)$$

*Proof.* — It holds that $\Delta(x_{i,j}) = \sum_{\ell=1}^n x_{i,\ell} \otimes x_{\ell,j}$ because

$$\sum_\ell x_{i,\ell}(A) x_{\ell,j}(B) = \sum_\ell a_{i,\ell} b_{\ell,j} = x_{i,j}(AB)$$

for all $A = (a_{i,j}) \in M_n(k)$, $B = (b_{i,j})_{i,j} \in M_n(k)$. Also

$$\epsilon(x_{i,j}) = x_{i,j}(I) = \delta_{i,j}.$$

$\square$

THEOREM 5.4. — *Let $C$ be a coalgebra, $V \in \mathcal{M}^C$.*

  *1) $V$ is the union of all its finite dimensional $C$ subcomodules.*
  *2) $C$ is the union of all its finite dimensional subcoalgebras.*

*Proof.* — It suffices to verify 1). Let $0 \neq v \in V$. We need to show that $v$ is contained in some finite dimensional subcomodule. Let $(c_i)_{i \in I}$ be a basis of $C$. Let $(v_i)_i \in V$ be the unique elements with

$$\delta(v) = \sum_i v_i \otimes c_i.$$

Here all but finitely many $v_i = 0$. It clearly holds that

$$v = v_0 \epsilon(v_1) \in V' := \sum_i k v_i.$$

Moreover,

$$\sum_i \delta(v_i) \otimes c_i = \sum_i v_i \otimes \Delta(c_i) \in V' \otimes C \otimes C.$$

As $C = \bigoplus_i k c_i$ we have $V \otimes C \otimes C \simeq \bigoplus_i V \otimes C \otimes k c_i$. Applying the projection to the $i$th component to $\sum_i \delta(v_i) \otimes c_i$ yields

$$\delta(v_i) \in V' \otimes C$$

for all $i$.                                                                                                   □

DEFINITION 5.5. — *Let $H$ be a bialgebra, $A$ an algebra, $\delta : A \to A \otimes H$ an $H$ right comodule structure. We say $(A, \delta)$ is a right comodule algebra if $\delta$ is an algebra homomorphism.*

*This is equivalent to requiring that $\mu$ and $\eta$ are colinear.*

*Proof.* — It holds that

$$(\mu \otimes \mathrm{id})\delta_{A \otimes A}(a \otimes b) = a_0 b_0 \otimes a_1 b_1$$

and

$$\delta(\mu(a \otimes b)) = (ab)_0 \otimes (ab)_1.$$

That is, $\mu$ is colinear if and only if $\delta(ab) = \delta(a)\delta(b)$ for all $a, b$. Likewise $\delta(1) = 1_A \otimes 1_H$ if and only if $\eta$ is colinear, since

$$(\eta \otimes \mathrm{id})\delta_k(\lambda) = \lambda 1_A \otimes 1_H$$

and

$$\delta(\eta(\lambda)) = \lambda \delta(1_A).$$

□

REMARK 5.6. —    *1) Let $A$ be an algebra, $H$ a bialgebra. $A$ is an $H$ left module algebra, if it is an algebra in $_H\mathcal{M}$ with respect to $\otimes_k$. (That is, if $\mu$ and $\eta$ are $H$-linear.) $A$ is an $H$ right comodule algebra if it is in algebra in $\mathcal{M}^H$ with respect to $\otimes_k$. (That is, if $\mu$ and $\eta$ are $H$-colinear.)*

*2) Let $A$ be an algebra, $H$ a bialgebra, $\delta : A \to A \otimes H$ an algebra homomorphism. Then $\delta$ is a right comodule algebra structure if the axioms are satisfied on some algebra generating set of $A$.*

*3) A bialagebra homomorphism $\varphi : H \to H'$ induces a functor from the category of $H$ right comodule algebras to $H'$ right comodule algebras.*

EXAMPLE 5.7. —    *1) If $H$ is a bialgebra, $A$ an $H$ left module algebra. Then $A\#H$ is an $H$ right comodule algebra via $\mathrm{id} \otimes \Delta$.*

*2) $G$ a group, $N \lhd G$ a normal subgroup. Then $k[G]$ is a $k[G/N]$ right comodule algebra via $\delta(g) = g \otimes \bar{g}$.*

*3) If $\varphi : H \to H'$ is a bialgebra homomorphism, then $H$ is a $H'$ right comodule algebra via $(\mathrm{id} \otimes \varphi)\Delta$.*

*4) $k[X_1, \ldots, X_n]$ is a $k[X_{i,j} \mid 1 \le i, j \le n]$ right comodule algebra via $\delta(x_n) = \sum_{\ell=1}^n x_\ell \otimes x_{\ell,i}$. (Recall $\Delta(X_{i,j}) = \sum_{\ell=1}^n X_{i,\ell} \otimes X_{\ell,j}$ and $\epsilon(X_{i,j}) = \delta_{i,j}$.)*

LEMMA 5.8. — *Let $X, Y, Z$ be vector spaces such that $Z$ is finite dimensional. Then*

$$\mathrm{Hom}(X, Y \otimes Z) \simeq \mathrm{Hom}(Z^* \otimes X, Y), \quad \delta \mapsto (f \otimes x \mapsto x_0 f(x_1)).$$

*Proof.* — The tensor product is left-adjoint to the Hom functor, hence

$$\mathrm{Hom}(Z^* \otimes X, Y) \simeq \mathrm{Hom}(X, \mathrm{Hom}(Z^*, Y)).$$

As $Z$ is finite dimensional we have $Z \simeq Z^{**}$ and

$$\mathrm{Hom}(Z^*, Y) \simeq Y \otimes Z^{**} \simeq Y \otimes Z.$$

Here $y \otimes z$ corresponds to $Z^* \to Y, f \mapsto f(z)y$. So a linear map $\delta : X \to Y \otimes Z$ corresponds to $x \mapsto (f \mapsto x_0 f(x_1))$. And this map in turn corresponds to $Z^* \otimes X \to Y, f \otimes x \mapsto x_0 f(x_1)$. $\qquad\square$

DEFINITION 5.9. — *Let $C$ be a coalgebra , $V$ a vector space, $\delta : V \to V \otimes C$ k-linear. Then $(V, \delta)$ is a $C$ right comodule structure if and only if the corresponding map*

$$\mu : C^* \otimes V \to V, \quad f \otimes v \mapsto v_0 f(v_1)$$

*is a module structure (that extends the k-vector space structure on $V$). We say the $C^*$-module structure $\mu$ is adjungated to $\delta$. If $\varphi : V \to W$ is a linear map with $V, W \in \mathcal{M}^C$ then $\varphi$ is a $C$ comodule homomorphism if and only if it is $C^*$-linear.*

*Proof.* — Consider the map

$$\kappa : C^* \to \mathrm{End}_k(V), \quad f \mapsto (v \mapsto v_0 f(v_1)).$$

Then

$$\kappa(f * g)(v) = v_0(f \odot g)(\Delta(v_1))$$

and

$$\kappa(f)\kappa(g)(v) = \kappa(f)(v_0 g(v_1)) = v_{00} f(v_{01}) g(v_1).$$

The two expressions are equal for all $f, g \in C^*$ if and only if

$$\delta(v_0)v_1 = v_0 \Delta(v_1).$$

Moreover, $\kappa(1_{C^*})(v) = \kappa(\epsilon)(v) = v_0 \epsilon(v_1)$ is equal to $\mathrm{id}(v) = v$ if and only if $v_0 \epsilon(v_1) = v$. This shows that $\delta$ is a comodule structure if and only if $\mu$ is an extending module structure.

For $f \in C^*$, $v \in V$ it holds that

$$\varphi(f.v) = \varphi(v_0 f(v_1)) = \varphi(v_0) f(v_1)$$

and

$$f.(\varphi(v)) = \varphi(v)_0 f(\varphi(v)_1).$$

The two expressions are equal for all $f \in C^*$ if and only if

$$\varphi(v_0) \otimes v_1 = \varphi(v)_0 \otimes \varphi(v)_1.$$

$\qquad\square$

THEOREM 5.10. — *1) Let $C$ be a finite dimensional coalgebra, $V$ a vector space. Then the $C$ right comodule structures on $V$ correspond bijectively to the extending $C^*$ left module structures.*

*2) Let $H$ be a finite dimensional algebra, $A$ an algebra. Then the $H$ right comodule algebra structures on $A$ correspond bijectively to the extending $H^*$ left module algebra structures.*

*3) $\mathcal{M}^C \simeq {}_{C^*}\mathcal{M}$ and likewise for the categories of $H$ right comodule algebras and $H^*$ left module algebra structures.*

*Proof.* — We already verified 1). In order to check 2), let the comodule structure $\delta : A \to A \otimes H$ correspond to the module structure $\mu : H^* \otimes A \to A$.

Then $\delta$ is a comodule algebra structure if and only if $\mu_A : A \otimes A \to A$ and $\eta_A : k \to A$ are $H$ colinear with respect to the comodule structures on $A \otimes A$ and $k$.

We know that $\mu$ is a module algebra structure if and only if $\mu_A$ and $\eta_A$ are $H^*$-linear with respect to the $H^*$ module structures on $A \otimes A$ and $k$.

We also now that $H$ colinearity is equivalent to $H^*$ linearity on the adjungated $H^*$ module structure. Hence it suffices to show that $H^*$ module structures on $A \otimes A$ and $k$ induced by $\Delta_{H^*}$ and $\epsilon_{H^*}$ are the adjungated structures to the $H$ comodule structures on $A \otimes A$ and $k$.

Indeed, for all $a, b \in A$ and $f \in H^*$

$$
\begin{aligned}
f.(a \otimes b) &= f_1.a \otimes f_2.b \\
&= a_0 f_1(a_1) \otimes b_0 f_2(b_1) \\
&= (a_0 \otimes b_0) f_1(a_1) f_2(b_1) \\
&= (a_0 \otimes b_0) f(a_1 b_1).
\end{aligned}
$$

This verifies that $A \otimes A$ carries the $H^*$ module structure that is adjungated to the $H$ module structure.

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

$$
f.1_k = \epsilon_{H^*}(f) = f(1_H) = (\mathrm{id} \odot f)(1_k \otimes 1_H).
$$

Hence $k$ carries the $H^*$ module structure that is adjungated to its $H$ comodule structure.

Part 3) follows from parts 1) and 2). $\qquad \square$

## 6. Affine groups

### 6.1. Affine schemes, monoids, and groups. —

DEFINITION 6.1. — *Let $\mathcal{C}$ be a category. A functor $F : \mathcal{C} \to \mathrm{Set}$ is representable if there is an object $C \in \mathcal{C}$ such that $F \simeq \mathcal{C}(C, -)$.*

LEMMA 6.2 (YONEDA). — *1) Let $F : \mathcal{C} \to \mathrm{Set}$ be a functor and $C \in \mathcal{C}$ an object. Then*

$$\mathrm{Mor}(\mathcal{C}(C, -), F) \simeq F(C)$$

$$(\alpha_E)_E \mapsto \alpha_C(\mathrm{id}_C)$$

$$(\alpha_E : \mathcal{C}(C, E) \to F(E), \quad f \mapsto F(f)(x))_E \hookleftarrow x$$

*2) For $C, D \in \mathcal{C}$:*

$$\mathrm{Mor}(\mathcal{C}(C, -), \mathcal{C}(D, -)) \simeq \mathcal{C}(D, C)$$

$$(\alpha_E)_E \mapsto \alpha_C(\mathit{id})$$

$$\mathcal{C}(g, -) \hookleftarrow g$$

*Proof.* — It is clear that 2) follows from 1). Let us first check that the two maps are well-defined. If $(\alpha_E)_E$ is a natural transformation from $\mathcal{C}(C, -)$ to $F$ then $\alpha_C : \mathcal{C}(C, C) \to F(C)$ and consequently $\alpha_C(\mathrm{id}_C) \in F(C)$. Conversely, if $x \in F(C)$ then the maps

$$\alpha_E : \mathcal{C}(C, E) \to F(E), \quad f \mapsto F(f)(x), \qquad E \in \mathcal{C}$$

are well-defined and functorial in $E$. Indeed, if $g : E \to E'$ is a morphism in $\mathcal{C}$, then

$$
\begin{array}{ccc}
\mathcal{C}(C, E) & \xrightarrow{\mathcal{C}(\mathrm{id}, g)} & \mathcal{C}(C, E') \\
\downarrow{\scriptstyle \alpha_E} & & \downarrow{\scriptstyle \alpha_{E'}} \\
F(E) & \xrightarrow{F(g)} & F(E')
\end{array}
$$

because

$$(F(g)\alpha_E)(f) = F(g)F(f)(x) = F(gf)(x) = \alpha_{E'}(gf) = (\alpha_{E'}\mathcal{C}(\mathrm{id}, g))(f).$$

To see that the two constructions are inverse to each other, note that for $x \in F(C)$ it holds that

$$F(\mathrm{id}_C)(x) = x.$$

Conversely, if $(\alpha_E)_E$ is a natural transformation from $\mathcal{C}(C, -)$ to $F$, then for each $f \in \mathcal{C}(C, E)$ it holds that

$$
\begin{array}{ccc}
\mathcal{C}(C, C) & \xrightarrow{\mathcal{C}(\mathrm{id}, f)} & \mathcal{C}(C, E) \\
\downarrow{\scriptstyle \alpha_C} & & \downarrow{\scriptstyle \alpha_E} \\
F(C) & \xrightarrow{F(f)} & F(E)
\end{array}
$$

and hence

$$F(f)(\alpha_C(\mathrm{id}_C)) = \alpha_E(\mathcal{C}(\mathrm{id}, f)(\mathrm{id}_C)) = \alpha_E(f).$$

$\square$

REMARK 6.3. — *We are sweeping some set-theoretic aspects under the table, since our naive definition that classes are just collections of sets does not work for the collection* $\mathrm{Mor}(\mathcal{C}(C, -), F)$.

REMARK 6.4. — *Let* $F : \mathcal{C} \to \mathcal{D}$ *be a functor.*

1) *$F$ is called faithful, if for each $X, Y \in \mathcal{C}$ the map*

$$\mathcal{C}(X, Y) \to \mathcal{D}(X, Y), \quad f \mapsto F(f)$$

*is injective. We say $F$ is full, if this map is surjective, and fully faithful if it is bijective.*

2) *We say $F$ is essentially surjective, if for each $D \in \mathcal{D}$ there is an object $C \in \mathcal{C}$ such that $F(C) \simeq D$.*

3) *The functor $F$ is an equivalence of categories, if and only if it is fully faithful and essentially surjective.*

*Proof.* — Suppose that $F$ is fully faithful and for each $D \in \mathcal{D}$ there is an object $G(D) \in \mathcal{C}$ with an isomorphism $\beta_D : F(G(D)) \simeq D$. This defines a map $G$ from the objects of $\mathcal{D}$ to the objects of $\mathcal{C}$ (using a suitable axiom of choice). Since $F$ is fully faithful it holds that for any morphism $D \xrightarrow{g} D'$ in $\mathcal{D}$ there is a unique morphism $G(D) \xrightarrow{f} G(D')$ with $F(f) = \beta_{D'}^{-1} g \beta_D$. We set $G(g) = f$, hence

$$
\begin{array}{ccc}
FG(D) & \xrightarrow{\beta_D} & D \\
\downarrow{\scriptstyle FG(g)} & & \downarrow{\scriptstyle g} \\
FG(D') & \xrightarrow{\beta_{D'}} & D'
\end{array}
$$

Since $F$ is a functor it follows that $FG$ is a functor too, and $(\beta_D)_D$ is natural isomorphism from $FG$ to $\mathrm{id}_{\mathcal{D}}$. As $F$ is faithful, this implies that $G$ is also a functor. It remains to verify that $GF \simeq \mathrm{id}_{\mathcal{C}}$. To this end, note that

$$F(GF) = (FG)F \simeq (\mathrm{id}_{\mathcal{D}})F \simeq F.$$

In other words, for all $C \xrightarrow{h} C'$

$$
\begin{array}{ccc}
FGF(C) & \xrightarrow{\simeq} & F(C) \\
\downarrow{\scriptstyle FGF(h)} & & \downarrow{\scriptstyle F(h)} \\
FGF(C') & \xrightarrow{\simeq} & F(C').
\end{array}
$$

Since $F$ is fully faithful, it follows that

$$
\begin{array}{ccc}
GF(C) & \xrightarrow{\simeq} & C \\
\downarrow{\scriptstyle GF(h)} & & \downarrow{\scriptstyle h} \\
GF(C') & \xrightarrow{\simeq} & C'.
\end{array}
$$

$\square$

REMARK 6.5. — *Let $\mathcal{C}$ and $\mathcal{D}$ denote categories.*

1) *A functor $F : \mathcal{C} \to \mathrm{Set}$ is representable, if there is an object $C \in \mathcal{C}$ such that $F \simeq \mathcal{C}(C, -)$. We may from the category $\mathcal{E}$ of representable functors from $\mathcal{C} \to \mathrm{Set}$ with natural transformations as sets.*

2) *The functor*

$$
\mathcal{C}^{\mathrm{op}} \to \mathcal{E}, \quad C \mapsto \mathcal{C}(C, -)
$$

*is fully faithful by the Yoneda lemma and hence an equivalence of categories.*

DEFINITION 6.6. — *Let $\mathcal{A}_k$ denote the category of commutative $k$-algebras. We let $\mathrm{Mon}$ denote the category of monoids and $\mathrm{Gr}$ the category of groups. The forgetful functors from these categories to the category $\mathrm{Set}$ of sets will be denoted by $\mathrm{Fo}$.*

1) *A representable functor $F : \mathcal{A}_k \to \mathrm{Set}$ is called an affine scheme. We let $\mathrm{Sch}_k$ denote the category of affine schemes.*

2) *A representable functor $F : \mathcal{A}_k \to \mathrm{Mon}$ is called an affine monoid. We let $\mathrm{Mon}_k$ denote the category of affine monoids.*

3) *A representable functor $F : \mathcal{A}_k \to \mathrm{Gr}$ is called an affine group. We let $\mathrm{Gr}_k$ denote the category of affine groups.*

4) *For each algebra $A \in \mathcal{A}_k$ the affine scheme $\mathrm{Sp}(A) := \mathrm{Alg}_k(A, -)$ is called the spectrum of $A$. Thus*

$$
\mathrm{Sp} : \mathcal{A}_k^{\mathrm{op}} \simeq \mathrm{Sch}_k.
$$

EXAMPLE 6.7. —   *1) $\mathbb{A}_n : \mathcal{A}_k \to \mathrm{Gr}, \quad A \mapsto (A^n, +)$ is an affine group with*

$$
\mathbb{A}_n \simeq \mathrm{Sp}(k[T_1, \ldots, T_n]).
$$

2) *$GL_n : \mathcal{A}_k \to \mathrm{Gr}, \quad A \mapsto GL_n(A)$ is an affine group with*

$$
GL_n \simeq \mathrm{Sp}(k[(T_{i,j})_{1 \le i,j \le n}, d^{-1} \mid d^{-1}\det(T_{i,j})_{i,j} = 1].
$$

3) *If $\mathrm{char}\, k = p > 0$ then $\alpha_p : \mathcal{A}_k \to \mathrm{Gr}, \quad A \mapsto (\{a \in A \mid a^p = 0\}, +)$ is an affine group with*

$$
\alpha_p \simeq \mathrm{Alg}_k(k[T]/(T^p), -).
$$

## 6.2. Groups in the category of affine schemes. —

THEOREM 6.8. — *1) If $H$ is a commutative bialgebra, then $\mathrm{Sp}(H)$ is an affine monoid with respect to the $*$-product. For a bialgebra homomorphism $\varphi : H \to H'$ the natural transformation $\mathrm{Sp}(\varphi) : \mathrm{Sp}(H') \to \mathrm{Sp}(H)$ is a morphism of monoids. Hence we obtain a functor*

$$\mathrm{Sp} : \{com.\ k\text{-}bialgebras\}^{\mathrm{op}} \to \mathrm{Mon}_k$$

*This functor is fully faithful. In $\mathrm{Sp}(H)(H \otimes H)$ it holds that $\Delta = i_1 * i_2$ if $i_1(x) = x \otimes 1$ and $i_2(x) = 1 \otimes x$. In $\mathrm{Sp}(H)(k)$ it holds that $\epsilon$ is the unit element.*

*Proof.* — Let $H$ and $H'$ be bialgebra. Then

$$
\begin{array}{ccc}
\mathrm{Alg}_k(H', H) & \xrightarrow{\ \mathrm{Sp}\ } & \mathrm{Sch}_k(\mathrm{Sp}(H), \mathrm{Sp}(H')) \\
\uparrow & & \uparrow \\
\mathrm{BiAlg}_k(H', H) & \xrightarrow{\ \mathrm{Sp}\ } & \mathrm{Mon}_k(\mathrm{Sp}(H), \mathrm{Sp}(H'))
\end{array}
$$

and the first row is a bijection. This readily yields that $\mathrm{Sp}$ is full. What is left to show is that if $\varphi : H' \to H$ is an algebra homomorphism such that $\mathrm{Sp}(\varphi)$ respects the monoid structures on $\mathrm{Sp}(H)$ and $\mathrm{Sp}(H')$ then $\varphi$ is already a bialgebra homomorphism. Indeed, since

$$\mathrm{Alg}_k(H, A) \to \mathrm{Alg}_k(H', A), \quad \psi \mapsto \psi\varphi$$

is a monoid homomorphism for all commutative $k$-algebras $A$, the special case $A = H \otimes H$ and $\psi = \Delta_H = i_1 * i_2$ yields

$$\Delta_H \varphi = (i_1 \varphi) * (i_2 \varphi),$$

that is

$$\varphi(x)_1 \otimes \varphi(x)_2 = \varphi(x_1) \otimes \psi(x_2).$$

Likewise, for $A = k$ and $\psi = \epsilon_H$ the unit element in $\mathrm{Alg}_k(H, k)$ it follows that

$$\epsilon_{H'} = \epsilon_H \varphi.$$

$\square$

*2) If $H$ is a commutative Hopf algebra, then $\mathrm{Sp}(H)$ is an affine group. Hence we obtain a fully faithful functor*

$$\mathrm{Sp} : \{com.\ k\text{-}Hopf\ algebras\}^{\mathrm{op}} \to \mathrm{Gr}_k$$

*In $\mathrm{Sp}(H)(H)$ it holds that $S = \mathrm{id}^{-1}$.*

*3) If A and B are commutative k-algebras / bialgebras / Hopf algebras, then*

$$\mathrm{Sp}(A \otimes B) \simeq \mathrm{Sp}(A) \times \mathrm{Sp}(B).$$

*as affine schemes / monoids / groups.*

*4) If G is an affine monoid / group, then there is a commutative bialgebra / Hopf algeba H with $G \simeq \mathrm{Sp}(H)$ as affine monoids / groups. In particular,*

$$\mathrm{Sp} : \{com.\ k\text{-bialgebras}\}^{\mathrm{op}} \simeq \mathrm{Mon}_k$$

$$\mathrm{Sp} : \{com.\ k\text{-Hopf algebras}\}^{\mathrm{op}} \simeq \mathrm{Gr}_k.$$

*Proof.* — Without loss of generality we may assume that there is a commutative algebra $H$ with $G(A) = \mathrm{Sp}(H)(A)$ for all commutative algebras $A$. We are going to show that there is a bialgebra structure / Hopf algebra structure $(H, \Delta, \epsilon)$ such that the monoid structure / group structure on $G(A)$ is the $*$-multiplication monoid / group structure on $\mathrm{Sp}(H)(A)$ for all commutative algebras $A$.

Consider the multiplication of $\mathrm{Sp}(H)$ as a functor

$$\mu : \mathrm{Sp}(H) \times \mathrm{Sp}(H) \to \mathrm{Sp}(H)$$

and the unit element as a functor

$$\eta : 1 \mapsto \mathrm{Sp}(H).$$

Since Sp is fully faithful, there is an algebra homomorphism $\Delta : H \to H \otimes H$ such that

$$\mathrm{Sp}(H \otimes H \otimes H) \xrightarrow{\quad\mathrm{Sp}(\mathrm{id}\otimes\Delta)\quad} \mathrm{Sp}(H \otimes H) .$$



Since Sp is faithful, this implies that

$$H \otimes H \otimes H \xleftarrow{\ \mathrm{id}\otimes\Delta\ } H \otimes H$$

$$\Delta\otimes\mathrm{id} \uparrow \qquad\qquad \uparrow \Delta$$

$$H \otimes H \xleftarrow{\quad\Delta\quad} H.$$

The rest of the proof works analogously.                                           $\square$

5) *From an abstract point of view, what happened in the last proof is that the equivalence* $\mathrm{Sp} : \mathcal{A}_k^{\mathrm{op}} \simeq \mathrm{Sch}_k$ *induces equivalences*

$$\mathrm{Mon}_k \simeq \{\textit{monoids in } \mathrm{Sch}_k \textit{ with respect to } \times\}$$
$$\simeq \{\textit{monoids in } \mathcal{A}_k^{\mathrm{op}} \textit{ with respect to } \otimes\}$$
$$\simeq \{\textit{commutative } k\text{-}\textit{bialgebras}\}^{\mathrm{op}}$$

*and*

$$\mathrm{Gr}_k \simeq \{\textit{groups in } \mathrm{Sch}_k \textit{ with respect to } \times\}$$
$$\simeq \{\textit{groups in } \mathcal{A}_k^{\mathrm{op}} \textit{ with respect to } \otimes\}$$
$$\simeq \{\textit{commutative } k\text{-}\textit{Hopf algebras}\}^{\mathrm{op}}.$$

THEOREM 6.9. — *Let $V$ be a vector space of dimension $n$, $H$ a commutative Hopf algebra, $G \simeq \mathrm{Sp}(H)$ an affine group. Then*

$$\{\delta : V \to V \otimes H \mid \delta \text{ } H\text{-comodule structure}\} \simeq \mathrm{Gr}_k(G, GL_n).$$

*Proof.* — Since $H$ is a Hopf algebra and

$$d := \det(T_{i,j})_{i,j} \in k[(T_{i,j})_{i,j}]$$

is group-like, it follows that any bialgebra homomorphism from $k[(T_{i,j})_{i,j}]$ to $H$ factors through the localization

$$k[(T_{i,j})_{i,j}, d^{-1} \mid dd^{-1} = 1].$$

Hence the injection

$$\mathrm{BiAlg}_k(k[(T_{i,j})_{1 \leq i,j \leq n}, d^{-1}], H) \hookrightarrow \mathrm{BiAlg}_k(k[(T_{i,j})_{1 \leq i,j \leq n}], H)$$

induced by the epismorphism

$$k[(T_{i,j})_{i,j}] \longrightarrow\!\!\!\!\!\to k[(T_{i,j})_{i,j}, d^{-1} \mid dd^{-1} = 1]$$

is actually a bijection. Using that $k[(T_{i,j})_{i,j}, d^{-1}]$ is a Hopf algebra and that we established that $\mathrm{Sp} : \{\text{commutative Hopfalgebras}\}^{\mathrm{op}} \to \mathrm{Gr}_k$ is an equivalence

$$\{\delta : V \to V \otimes H \mid \delta \text{ } H\text{-comodule structure}\} \simeq \mathrm{BiAlg}_k(k[(T_{i,j})_{1 \leq i,j \leq n}], H)$$
$$\simeq \mathrm{BiAlg}_k(k[(T_{i,j})_{1 \leq i,j \leq n}, d^{-1}], H)$$
$$\simeq \mathrm{Gr}_k(\mathrm{Sp}(H), \mathrm{Sp}(k[(T_{i,j})_{1 \leq i,j \leq n}, d^{-1}]))$$
$$\simeq \mathrm{Gr}_k(\mathrm{Sp}(H), GL_n).$$

$\square$

DEFINITION 6.10. —     *1) An affine scheme $X$ is algebraic if $X \simeq \mathrm{Sp}(A)$ for an algebra $A$ that is finitely generated as algebra.*

2) *A morphism $X \xrightarrow{\alpha} Y$ of affine schemes is a closed embedding, if the algebra homomorphism $\varphi : B \to A$ with $X \simeq \mathrm{Sp}(A)$, $Y \simeq \mathrm{Sp}(B)$ and*

$$
\begin{array}{ccc}
X & \xrightarrow{\ \alpha\ } & Y \\
\simeq \Big| & & \Big| \simeq \\
\mathrm{Sp}(A) & \xrightarrow{\ \mathrm{Sp}(\varphi)\ } & \mathrm{Sp}(B)
\end{array}
$$

*is surjective.*

REMARK 6.11. — *1) If $X \xrightarrow{\alpha} Y$ is a closed embedding, then $X(R) \xrightarrow{\alpha_R} Y(R)$ is injective for all $R \in \mathcal{A}_k$.*

*2) The inverse needs not hold. For example, $k[T] \subset k(T)$ is not surjective, but $\mathrm{Sp}(k(T))(R) \to \mathrm{Sp}(k[T])(R)$ is injective for all $R \in \mathcal{A}_k$.*

THEOREM 6.12. — *If $G$ is an affine algebraic group, then there is a closed embedding $G \mapsto GL_n$.*

*Proof.* — Let $H$ be a commutative Hopf algebra with $G \simeq \mathrm{Sp}(H)$. Let $x_1, \ldots, x_m$ be an algebra generating set of $H$ that is linear independent. Then there is a finite dimensional subcomodule $V \subset H$ with $x_1, \ldots, x_m \in V$. We may extend $(x_i)_i$ to a basis $x_1, \ldots, x_n$ of $V$. The corresponding algebra homomorphism

$$
k[(T_{i,j})_{i,j} d^{-1}] \to H, \qquad T_{i,j} \mapsto x_{i,j}
$$

with $\Delta(x_j) = \sum_i x_i \otimes x_{i,j}$ is surjective, because $x_j = \sum_\ell \epsilon(x_\ell) x_{\ell,j}$. $\qquad\square$

DEFINITION 6.13. — *$X$ an affine scheme, $G$ an affine group, $\mu : X \times G \to X$ a morphism. We say $(X, \mu)$ is a $G$-scheme and $\mu$ is an operation of $G$ on $X$ if for all $R \in \mathcal{A}_k$*

$$
\mu_R : X(R) \times G(R) \to X(R)
$$

*is an operation of the group $G(R)$ on the set $X(R)$.*

EXAMPLE 6.14. — *$\mathbb{A}^n \times SL_n \to \mathbb{A}^n$ is an operation.*

THEOREM 6.15. — *Let $G \simeq \mathrm{Sp}(H)$ be an affine group, $X \simeq \mathrm{Sp}(A)$ an affine scheme. Then*

$$
\{\mu : X \times G \to X \text{ operation}\} \simeq \{\delta : A \to A \otimes H \text{ right comodule algebra struct}\}
$$

*Proof.* — Suppose that $\mu : X \times G \to X$ is an operation. Then

$$
\begin{array}{ccc}
\mathrm{Sp}(A \otimes H \otimes H) & \xrightarrow{\ \mathrm{Sp}(\mathrm{id} \otimes \Delta)\ } & \mathrm{Sp}(A \otimes H)\ .
\end{array}
$$

$$
X \times G \times G \xrightarrow{\ \mathrm{id} \times \mu\ } X \times G
$$

$$
\mathrm{Sp}(\delta \otimes \mathrm{id}) \qquad \mu \times \mathrm{id} \qquad \mu \qquad \mathrm{Sp}(\Delta)
$$

$$
X \times G \xrightarrow{\ \mu\ } X
$$

$$
\mathrm{Sp}(A \otimes H) \dashrightarrow_{\mathrm{Sp}(\delta)} \mathrm{Sp}(A)
$$

Since Sp is faithful, this implies that

$$
\begin{array}{ccc}
A \otimes H \otimes H & \xleftarrow{\ \mathrm{id} \otimes \Delta\ } & A \otimes H \\
\uparrow{\scriptstyle \delta \otimes \mathrm{id}} & & \uparrow{\scriptstyle \delta} \\
A \otimes H & \xleftarrow{\ \delta\ } & A.
\end{array}
$$

$\square$

## 7. Lie algebras and their universal enveloping algebras

### 7.1. Lie algebras. —

DEFINITION 7.1. — *Let $\mathfrak{g}$ be a k-vector space and $[-, -] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ a k-bilinear map. We say $\mathfrak{g}$ is a Lie algebra if*

$$[x, x] = 0 \qquad and \qquad [[x, y], z] + [[y, z], x] + [[z, x], y] = 0$$

*for all $x, y, z \in \mathfrak{g}$.*

REMARK 7.2. — *1) If $\mathfrak{g}$ is a Lie algebra then $[x, y] = -[y, x]$.*

*Proof. —* It holds that $0 = [x - y, x - y] = 0 - [x, y] - [y, x] + 0$. $\qquad\qquad\square$

*2) Any vector space $V$ is a lie algebra with $[v, v] = 0$ for all $v \in V$.*
*3) If $A$ is an associative algebra then $A^-$ with $A^- := A$ and $[x, y] := xy - yx$ is a Lie algebra.*

DEFINITION 7.3. — *1) A linear map $f : \mathfrak{g} \to \mathfrak{g}'$ between Lie algebras is a Lie algebra homomorphism, if $f([x, y]) = [f(x), f(y)]$ for all $x, y \in \mathfrak{g}$.*
*2) A subspace $\mathfrak{a} \subset \mathfrak{g}$ is a sub Lie algebra if $[x, y] \in \mathfrak{a}$ for all $x, y \in \mathfrak{a}$.*
*3) A subspace $\mathfrak{a} \subset \mathfrak{g}$ is an ideal if $[x, y] \in \mathfrak{a}$ for all $x \in \mathfrak{a}$ and $y \in \mathfrak{g}$. Notation: $\mathfrak{a} \lhd \mathfrak{g}$. In this case $\mathfrak{g}/\mathfrak{a}$ is a Lie algebra.*
*4) If $f : \mathfrak{g} \to \mathfrak{g}'$ is a Lie algebra homomorphism, then $\ker f \lhd \mathfrak{g}$, $\mathrm{im} f \subset \mathfrak{g}$ is a sub Lie algebra, and*

$$\mathrm{im} f \simeq \mathfrak{g}/ \ker f.$$

DEFINITION 7.4. — *1) Let $A$ be a k-vector spaces and $\mu : A \times A \to A$ a k-bilinear map. We say a linear map $d : A \to A$ is a derivation, if $d(\mu(a, b)) = \mu(d(a), b) + \mu(a, d(b))$ holds for all $a, b \in A$. The set $\mathrm{Der}(A, A) \subset \mathrm{End}_k(A)^-$ of all derivations is a sub Lie algebra. If $(A, \mu)$ has a unit element then $d(1) = 0$.*
*2) If $\mathfrak{g}$ is a Lie algebra, then for all $x \in \mathfrak{g}$ the map $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}, y \mapsto [x, y]$ is a derivation. The map*

$$\mathrm{ad} : \mathfrak{g} \to \mathrm{Der}(\mathfrak{g}, \mathfrak{g})$$

*is a Lie algebra homomorphism.*

*Proof. —* It holds that

$$\mathrm{ad}_x([y, z]) = [x, [y, z]] = [[x, y], z] + [y, [x, z]] = [\mathrm{ad}_x(y), z] - [y, \mathrm{ad}_x(z)]$$

and

$$\mathrm{ad}_{[x,y]}(z) = [[x, y], z] = [x, [y, z]] - [y, [x, z]] = (\mathrm{ad}_x \mathrm{ad}_y - \mathrm{ad}_y \mathrm{ad}_x)(z).$$

$\qquad\qquad\square$

*3) Let $H$ be a bialgebra. Then $P(H) = \{x \mid \Delta(x) = x \otimes 1 + 1 \otimes x\} \subset H^-$ is a subliealgebra. If* char$k = p > 0$ *then* $x \in P(H)$ *implies* $x^p \in P(H)$.

*Proof.* — For $x, y \in P(H)$ it holds that $\Delta(xy - yx)$ is given by

$$(x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x)$$
$$= xy \otimes 1 + x \otimes y + y \otimes x + 1 \otimes xy - (yx \otimes 1 + y \otimes x + y \otimes x + 1 \otimes yx)$$
$$= (xy - yx) \otimes 1 + 1 \otimes (xy - yx).$$

<div align="right">□</div>

*4) Let $H$ be a bialgebra. Then* $\mathrm{Der}_\epsilon(H, k)$ *denotes the set of all $\epsilon$-derivations from $H$ to $k$, that is linear maps $d : H \to k$ with $d(ab) = d(a)\epsilon(b) + \epsilon(a)d(b)$ for all $a, b \in H$. It holds that* $\mathrm{Der}_\epsilon(H, k) \subset (H^*)^-$ *is a sub lie algebra.*

*Proof.* — For $d, d' \in \mathrm{Der}_\epsilon(H, k)$ it holds that $d * d' - d' * d \in \mathrm{Der}_\epsilon(H, k)$ because for all $a, b \in H$

$$(d * d' - d' * d)(ab) = d(a_1 b_1)d'(a_2 b_2) - d'(a_1 b_1)d'(a_2 b_2)$$
$$= (d(a_1)\epsilon(b_1) + \epsilon(a_1)d(b_1))(d'(a_2)\epsilon(b_2) + \epsilon(a_2)d'(b_2))$$
$$- (d'(a_1)\epsilon(b_1) + \epsilon(a_1)d'(b_1))(d(a_2)\epsilon(b_2) + \epsilon(a_2)d(b_2))$$
$$= (d * d' - d' * d)(a)\epsilon(b) + \epsilon(a)(d * d' - d' * d)(b).$$

<div align="right">□</div>

*5) $H \mapsto \mathrm{Der}_\epsilon(H, k)$ is a functor from the category of Hopf algebras over $k$ to the category of Lie algebras over $k$.*

EXAMPLE 7.5. —    *1)* $\mathfrak{sl}_n = \{A \in M_n(k) \mid \mathrm{tr}(A) = 0\} \subset M_n(k)^-$ *is a sub Lie algebra.*
*2) For $Q \in M_n(k)$ it holds that* $\mathfrak{o}(Q) = \{X \in M_n(k) \mid QX + X^\mathsf{T}Q = 0\} \subset M_n(k)^-$ *is a sub Lie algebra.*

REMARK 7.6. — *We saw in the exercises that if $B$ is a bialgebra, then for each $x \in B^+ = \ker(\epsilon)$ it holds that*

$$\Delta(x) \in 1 \otimes x + x \otimes 1 + B^+ \otimes B^+.$$

THEOREM 7.7. — *Let $A$ be a commutative Hopf algebra, $G = \mathrm{Sp}(A)$ an affine group, $A^+ = \ker(\epsilon_A)$ the augmentation ideal.*

*1) It holds that*

$$\mathrm{Der}_\epsilon(A, k) \simeq \left(A^+/(A^+)^2\right)^*$$
$$d \mapsto (\bar{a} \mapsto d(a))$$
$$(a \mapsto f(\overline{a - \epsilon(a)1_A})) \leftarrow\!\!\!\shortmid f$$

*Proof.* — The ideal $(A^+)^2$ is generated by terms of the form $ab$ with $a, b \in A^+$, and for each such term and each $d \in \mathrm{Der}_\epsilon(A, k)$ it holds that

$$d(ab) = d(a)\epsilon(b) + \epsilon(a)d(b) = 0.$$

This shows that the map $\mathrm{Der}_\epsilon(A, k) \to (A^+/(A^+)^2)^*$ is well-defined. Conversely, given $f \in (A^+/(A^+)^2)^*$ it follows that the map

$$d_f : A \to k, \qquad a \mapsto f(\overline{a - \epsilon(a)1_A})$$

is an $\epsilon$-derivation. To see this, note that for all $a, b \in A$

$$d_f(a)\epsilon(b) + \epsilon(a)d_f(b) = f(\overline{a\epsilon(b) - \epsilon(a)\epsilon(b)1_A + \epsilon(a)b - \epsilon(a)\epsilon(b)1_A})$$

and

$$
\begin{aligned}
a\epsilon(b) &- 2\epsilon(a)\epsilon(b)1_A + \epsilon(a)b - (ab - \epsilon(ab)1_A) \\
&= -ab + a\epsilon(b) + \epsilon(a)b - \epsilon(ab)1_A \\
&= (a - \epsilon(a)1_A)(\epsilon(b)1_A - b) \\
&\in (A^+)^2.
\end{aligned}
$$

It is clear that the two constructions are inverse to each other, yielding $\mathrm{Der}_\epsilon(A, k) \simeq (A^+/(A^+)^2)^*$. $\qquad\square$

2) *The quotient algebra $k[T]/(T^2)$ is generated by $\tau = \bar{T}$. Let $\pi : k[\tau] \to k$ be the algebra homomorphism with $\pi(\tau) = 0$. We set*

$$\mathrm{Lie}(G) := \ker(G(\pi) : G(k[\tau]) \to G(k))$$
$$= \{\varphi \in \mathrm{Alg}_k(A, k[\tau]) \mid \pi\varphi = \epsilon\}$$

*Then*

$$\mathrm{Der}_\epsilon(A, k) \simeq \mathrm{Lie}(G)$$
$$d \mapsto (a \mapsto \epsilon(a) + d(a)\tau)$$

*is a bijection.*

*Proof.* — Let $d \in \mathrm{Der}_\epsilon(A, k)$ and $\varphi_d : A \to k[\tau], a \mapsto \epsilon(a) + d(a)\tau$. Then $\varphi_d$ is an algebra homomorphism, because $d(1) = 0$ and for all $a, b \in A$

$$
\begin{aligned}
\varphi_d(a)\varphi_d(b) &= (\epsilon(a) + d(a)\tau)(\epsilon(b) + d(b)\tau) \\
&= \epsilon(ab) + (d(a)\epsilon(b) + \epsilon(a)d(b))\tau \\
&= \epsilon(ab) + d(ab)\tau.
\end{aligned}
$$

Conversely, any element $\varphi \in \mathrm{Lie}(G)$ is of the form $\varphi_d$ for some $d \in A^*$, and using that $1, \tau$ is a basis a similar calculation yields that this already implies that $d \in \mathrm{Der}_\epsilon(A, k)$. $\qquad\square$

*3) The isomorphism*

$$\mathrm{Der}_\epsilon(A, k) \simeq \mathrm{Lie}(G)$$

*is an isomorphism of Lie algebras. We define the a vector space structure and Lie algebra structure on* $\mathrm{Lie}(G)$ *as follows. Let* $\Delta, i_1, i_2 \in \mathrm{Alg}_k(k[\tau], k[\tau] \otimes k[\tau])$ *be the algebra homomorphisms with*

$$\Delta(\tau) = \tau \otimes \tau$$
$$i_1(\tau) = \tau \otimes 1$$
$$i_2(\tau) = 1 \otimes \tau.$$

*For each* $\lambda \in k$ *we let* $f_\lambda \in \mathrm{Alg}_k(k[\tau], k[\tau])$ *be the algebra homomorphism with* $f_\lambda(\tau) = \lambda\tau$. *For* $\varphi, \varphi' \in \mathrm{Lie}(G)$, $\varphi = \epsilon + d\tau$, $\varphi' = \epsilon + d'\tau$, $d, d' \in \mathrm{Der}_\epsilon(A, k)$ *we set*

$$\varphi + \varphi' := \varphi * \varphi' = \epsilon + (d + d')\tau$$

*and*

$$\lambda.\varphi = G(f_\lambda)(\varphi) = f_\lambda\varphi = \epsilon + (\lambda d)\tau.$$

*We define* $[\varphi, \varphi']$ *by*

$$G(\Delta)([\varphi, \varphi']) = [G(i_1)(\varphi), G(i_2)(\varphi')] = ghg^{-1}h^{-1}$$

*with* $g = G(i_1)(\varphi)$, $h = G(i_2)(\varphi')$. *That is*

$$[\varphi, \varphi'] = \epsilon + [d, d']\tau.$$

*4) It holds that*

$$(A \mapsto \mathrm{Lie}(\mathrm{Sp}(A))) \simeq (A \mapsto \mathrm{Der}_\epsilon(A, k))$$

*functors from commutative Hopf algebras over* $k$ *to Lie algebras over the field* $k$.

COROLLARY 7.8. — *1) If* $G \subset G'$ *is an affine closed subgroup, then* $\mathrm{Lie}(G) \to \mathrm{Lie}(G')$ *is a sub Lie algebra.*

*Proof.* — Without loss of generality $G = \mathrm{Sp}(H)$ and $G' = \mathrm{Sp}(H')$. Let the closed embedding $G \to G'$ be given by $\mathrm{Sp}(\varphi)$ with $\varphi : H' \to H$ a surjective Hopf algebra homomorphism. Then

$$\mathrm{Der}_\epsilon(H, k) \to \mathrm{Der}_\epsilon(H', k), \quad d \mapsto d\varphi$$

is injective and an Lie algebra homomorphism. $\qquad\square$

*2) It holds that* $\mathrm{Lie}(GL_n) \simeq M_n(k)^-$

*Proof.* — We have

$$\text{Lie}(GL_n) = \ker(GL_n(k[\tau]) \overset{GL_n(\pi)}{\longrightarrow} GL_n(k)) = \{E + \tau A \mid A \in M_n(k)\}.$$

because any element of the form $E + \tau A$ is invertible with inverse $E - \tau A$ (since $\tau^2 = 0$).

The sum of $X = E + A\tau \in \text{Lie}(GL_n)$ and $Y = E + A'\tau \in \text{Lie}(GL_n)$ is given by

$$X + Y = (E + A\tau)(E + A'\tau) = E + (A + A')\tau$$

and for $\lambda \in k$ the scalar product of $\lambda$ and $E + A\tau$ in $\text{Lie}(GL_n)$ is given by

$$\lambda . X = E + \lambda A.$$

The Lie bracket of $X$ and $Y$ is defined by

$$[X, Y] = E + \tau C$$

with

$$E + \tau \otimes \tau C = (E + \tau \otimes 1A)(E + 1 \otimes \tau A')(E - \tau \otimes 1A)(E - 1 \otimes \tau A')$$
$$= E + \tau \otimes \tau(AA' - A'A).$$

$\square$

3) *In particular, for any affine algebraic group $G$ it holds that $\text{Lie}(G) \hookrightarrow M_n(k)^-$ is a sub Lie algebra for some $n$.*

## 7.2. The universal enveloping algebra. —

DEFINITION 7.9. — *Let $V$ be a vector space. Then*

$$T(V) := \coprod_{n \geq 0} V^{\otimes n}$$

*is an algebra with multiplication given by*

$$V^{\otimes m} \times V^{\otimes n} \to V^{\otimes m+n}, \quad (a, b) \mapsto a \otimes b.$$

*We call $T(V)$ the tensor algebra of $V$. If $(v_i)_{i \in I}$ is a basis of $V$ then*

$$T(V) \simeq k < x_i, i \in I >$$

*as algebras. For any algebra $A$ and any $k$-linear map $f : V \to A$ there is a unique algebra homomorphism $\varphi : T(V) \to A$ such that the diagram*

$$
\begin{array}{ccc}
V & \overset{f}{\longrightarrow} & A \\
{\scriptstyle \text{can}} \downarrow & \nearrow & \\
T(V) & {\scriptstyle \varphi} &
\end{array}
$$

*commutes. That is,*

$$\mathrm{Hom}_k(V, A) \simeq \mathrm{Alg}_k(T(V), A).$$

DEFINITION 7.10. — *Let $\mathfrak{g}$ be a Lie algebra. The factor algebra*

$$U(\mathfrak{g}) = T(\mathfrak{g})/ < x \otimes y - y \otimes x - [x, y] \mid x, y \in \mathfrak{g} >$$

*is called the universal enveloping algebra of $\mathfrak{g}$. We let $\sigma$ denote the canonical map $\mathfrak{g} \to U(\mathfrak{g}), x \mapsto \bar{x}$. For any algebra $A$ and any Lie algebra homomorphism $f : \mathfrak{g} \to A^-$ there is a unique algebra homomorphism $\varphi : U(\mathfrak{g}) \to A$ such that the diagram*

$$\begin{array}{ccc} \mathfrak{g} & \xrightarrow{\ f\ } & A \\ {\scriptstyle \sigma}\downarrow & {\nearrow}^{\varphi} & \\ U(\mathfrak{g}) & & \end{array}$$

*commutes. That is,*

$$\mathrm{LieAlg}_k(\mathfrak{g}, A^-) \simeq \mathrm{Alg}_k(U(\mathfrak{g}), A).$$

REMARK 7.11. — *1) If $\mathfrak{g}$ is a Lie algebra with basis $(x_i)_{i \in I}$ and $[x_i, x_j] = \sum_{\ell \in I} a_{i,j}^\ell x_\ell$ for all $i, j$ then*

$$U(\mathfrak{g}) \simeq k < (x_i)_{i \in I} \mid x_i x_j - x_j x_i = \sum_{\ell \in I} a_{i,j}^\ell x_\ell \text{ for all } i, j > .$$

*2) This yields the representation of the enveloping algebra $U(\mathfrak{sl}_2)$ of Remark 4.10.*

COROLLARY 7.12. — *1) $U(\mathfrak{g})$ is a Hopf algebra with $\sigma(x)$ primitive for all $x \in \mathfrak{g}$.*

*Proof.* — The maps

$$\tilde{\Delta} : \mathfrak{g} \to (U(\mathfrak{g}) \otimes U(\mathfrak{g}))^-, \quad x \mapsto \sigma(x) \otimes 1 + 1 \otimes \sigma(x)$$
$$\tilde{\epsilon} : \mathfrak{g} \to k^-, \quad x \mapsto 0$$
$$\tilde{S} : \mathfrak{g} \to (U(\mathfrak{g})^{\mathrm{op}})^-, \quad x \mapsto -x.$$

are Lie algebra homomorphisms. Hence they induce algebra homomorphisms $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$, $\epsilon : U(\mathfrak{g}) \to k$ and $S : U(\mathfrak{g}) \to U(\mathfrak{g})^{\mathrm{op}}$ that satisfy the Hopf algebra axioms on the algebra generating set $\sigma(\mathfrak{g}) \subset U(\mathfrak{g})$. $\qquad\square$

*2) For any bialgebra $H$ and any Lie algebra homomorphism $f : \mathfrak{g} \to P(H)$ there is a unique bialgebra homomorphism $\varphi : U(\mathfrak{g}) \to H$ such that the diagram*

$$\begin{array}{ccccc} \mathfrak{g} & \xrightarrow{\ f\ } & P(H) & \hookrightarrow & H \\ {\scriptstyle \sigma}\downarrow & & {\nearrow}^{\varphi} & & \\ U(\mathfrak{g}) & & & & \end{array}$$

*commutes. That is,*

$$\mathrm{LieAlg}_k(\mathfrak{g}, P(H)) \simeq \mathrm{BiAlg}_k(U(\mathfrak{g}), H).$$

DEFINITION 7.13. — *Let $\mathfrak{g}$ be a Lie algebra, $V$ a vector space, and $\mu : \mathfrak{g} \times V \to V$ a bilinear map that we denote by $\mu(x, v) = x.v$ for all $x \in \mathfrak{g}, v \in V$. The pair $(V, \mu)$ is called a $\mathfrak{g}$-module if for all $x, y \in \mathfrak{g}$, $v \in V$ it holds that*

$$[x, y].v = x.(y.v) - y.(x.v).$$

DEFINITION 7.14. — *Let $V, W$ be $\mathfrak{g}$-modules. A linear map $f : V \to W$ is called $\mathfrak{g}$-linear, if for all $x \in \mathfrak{g}$ and $v \in V$ it holds that $f(x.v) = x.f(v)$.*

REMARK 7.15. — *1) Let $V$ be a vector space, $\mathfrak{g}$ a Lie algebra. Then*

$$\{\mu : \mathfrak{g} \times V \to V \ \mathfrak{g} \ module \ structure\}$$
$$\simeq \mathrm{LieAlg}_k(\mathfrak{g}, \mathrm{End}_k(V)^-)$$
$$\simeq \mathrm{Alg}_k(U(\mathfrak{g}), \mathrm{End}_k(V))$$
$$\simeq \{\mu : U(\mathfrak{g}) \times V \to V \ U(\mathfrak{g}) \ module \ structure\}.$$

*A linear map $f : V \to W$ is $\mathfrak{g}$-linear with respect to $\mathfrak{g}$-module structures on $V$ and $W$ if and only if it is $U(\mathfrak{g})$-linear with the corresponding $U(\mathfrak{g})$-module structures.*
*2) $_{U(\mathfrak{g})}\mathcal{M} \simeq \{\mathfrak{g} \ modules\}$ is an equivalence of categories.*

## 7.3. Hopf algebra filtrations. —

DEFINITION 7.16. — *1) $(A, (A_n)_{n \geq 0})$ filtered algebra: $A$ algebra,*

$$A_0 \subset A_1 \subset \ldots \subset A, \qquad A = \bigcup_{n \geq 0} A_n$$

*sub vector spaces, $1 \in A_0$, $A_n A_m \subset A_{n+m}$ for all $n, m \geq 0$.*
*2) $(C, (C_n)_{n \geq 0})$ filtered coalgebra: $C$ coalgebra,*

$$C_0 \subset C_1 \subset \ldots \subset C, \qquad C = \bigcup_{n \geq 0} C_n$$

*sub vector spaces, $\Delta(C_n) \subset \sum_{i=0}^{n} C_i \otimes C_{n-i}$ for all $n \geq 0$.*
*3) $(H, (H_n)_{n \geq 0})$ filtered bialgebra: $H$ bialgebra and $(H_n)_{n \geq 0}$ is both an algebra and coalgebra filtration.*
*4) $(H, (H_n)_{n \geq 0})$ filtered Hopf algebra: $H$ Hopf algebra, $(H_n)_{n \geq 0}$ bialgebra filtration, $S(H_n) \subset H_n$ for all $n \geq 0$.*

DEFINITION 7.17. — *Let $(A, (A_n)_{n \geq 0})$ be a filtered algebra.*

*1) The algebra*

$$\mathrm{gr}(A) = \coprod_{n \geq 0} A_n/A_{n-1}, \qquad A_{-1} = 0$$

*with multiplication*

$$A_m/A_{m-1} \times A_n/A_{n-1} \to A_{m+n}/A_{m+n-1}, \quad (\bar{a}, \bar{b}) \mapsto \bar{a}\bar{b}$$

*is the graded algebra associated to $A$.*

*2) $(M, (M_n)_{n \geq 0})$ filtered $A$ right module: $M$ $A$ right module, $M_m A_n \subset M_{m+n}$ for all $m, n \geq 0$.*

$$\mathrm{gr}(M) = \coprod_{n \geq 0} M_n/M_{n-1}, \qquad M_{-1} = 0$$

*is a $\mathrm{gr}(A)$ right-module via*

$$M_m/M_{m-1} \times A_n/A_{n-1} \to M_{m+n}/M_{m+n-1}, \quad (\bar{m}, \bar{a}) \mapsto \bar{m}\bar{a}.$$

REMARK 7.18. — *A left/right module is noetherian if any ascending sequence of left/right modules stabilizes. Equivalently, all left/right submodules are finitely generated.*

*A ring is left/right noetherian if it is left/right noetherian as left/right module over itself.*

LEMMA 7.19. — *Let $(A, (A_n)_{n \geq 0})$ be a filtered algebra.*

*1) If $\mathrm{gr}(A)$ is an integral domain, then so is $A$.*

*Proof. —* Suppose that there are $m, n \geq 0$ with $m + n$ minimal such that there exist $0 \neq x \in A_m$ and $0 \neq y \in A_n$ with $xy = 0$. Then $\bar{x}\bar{y} = 0$ in $\mathrm{gr}(A)$ with $\bar{x} \in A_n/A_{n-1}$, $\bar{y} \in A_m/A_{m-1}$. We assumed that $\mathrm{gr}(A)$ is an integral domain, hence it follows that $x \in A_{n-1}$ or $y \in A_{m-1}$. This contradicts the minimality assumption on $m + n$. □

*2) If $\mathrm{gr}(A)$ is right- or left-noetherian, then so is $A$.*

*Proof. —* Suppose that $\mathrm{gr}(A)$ is right-noetherian. Let $I \subset \mathrm{gr}(A)$ be a right-ideal. Then $(I, (I \cap A_n)_{n \geq 0})$ is a filtered $A$ right module, $\mathrm{gr}(I) \subset \mathrm{gr}(A)$ with

$$(I \cap A_n)/(I \cap A_{n-1}) \hookrightarrow A_n/A_{n-1}$$

is a right ideal of $\mathrm{gr}(A)$. We assumed that $\mathrm{gr}(A)$ is right noetherian, hence $\mathrm{gr}(I)$ is finitely generated. That is, there are elements $\bar{a}_1, \ldots, \bar{a}_N \in \mathrm{gr}(I)$, $\bar{a}_i \in (I \cap A_{n_i})/(I \cap A_{n_i-1})$ for all $i$, with

$$\mathrm{gr}(I) = \sum_{i=1}^{N} \bar{a}_i \mathrm{gr}(A).$$

We are going to show by induction that $I \cap A_n \subset \sum_{i=1}^{N} a_i A$ for all $n$. For $n = 0$ this is trivial. Suppose that $n \geq 1$ and let $x \in I \cap A_n$. Then $\bar{x} \in \text{gr}(I)$ with $\bar{x} \in (I \cap A_n)/(I \cap A_{n-1})$. Hence

$$\bar{x} \in \sum_{i=1}^{N} \bar{a}_i \text{gr}(A).$$

In fact, it even holds that

$$\bar{x} \in \sum_{i, n_i \leq n} \bar{a}_i \left( A_{n-n_i}/A_{n-n_i-1} \right).$$

That is, there are $\lambda_i \in I_n \cap A_{n_i}$ (with $n_i \leq n$ such that

$$\bar{x} = \sum_{i, n_i \leq n} \overline{a_i \lambda_i} = \overline{\sum_{i, n_i \leq n} a_i \lambda_i}$$

This implies that

$$x - \sum_{i, n_i \leq n} a_i \lambda_i \in I \cap A_{n-1}.$$

By induction hypothesis it holds that $I \cap A_{n-1} \subset \sum_{i=1}^{N} a_i A$. Thus

$$x \in \sum_{i=1}^{N} a_i A.$$

$\square$

PROPOSITION 7.20. — *Let $A$ be an algebra and $(x_i)_{i \in I}$ an algebra generating set. Then $(A_n)_{n \geq 0}$ with $A_n$ the $k$-span of all $x_{i_1} \cdots x_{i_m}$ with $m \leq n$, $i_1, \ldots, i_m \in I$ is the natural filtration of $A$.*

### 7.4. The Poincaré-Birkhoff-Witt theorem. —

DEFINITION 7.21. — *Let $\mathfrak{g}$ be a Lie algebra with basis $(x_i)_{i \in I}$. We let $(U_n(\mathfrak{g}))_{n \geq 0}$ denote the natural filtration of $U(\mathfrak{g})$ with respect to $(\sigma(x_i))_{i \in I}$ and let $\text{gr}(U(\mathfrak{g}))$ denote the corresponding graded algebra.*

LEMMA 7.22. — *Let $\mathfrak{g}$ be a Lie algebra with basis $(x_i)_{i \in I}$. Let $\leq$ be a total order on $I$.*

*1) $\text{gr}(U(\mathfrak{g}))$ is commutative.*

*Proof.* — $\text{gr}(U(\mathfrak{g}))$ is generated as an algebra by $(\overline{\sigma(x_i)})_{i \in I}$ with $\overline{(\sigma(x_i))} \in U_1(\mathfrak{g})/U_0(\mathfrak{g})$. For all $i, j \in I$ it holds that

$$\sigma(x_i)\sigma(x_j) - \sigma(x_j)\sigma(x_i) = \sigma([x_i, x_j]) \in U_1(\mathfrak{g})$$

and hence

$$\overline{\sigma(x_i)\sigma(x_j)} = \overline{\sigma(x_j)\sigma(x_i)}$$

in $U_2(\mathfrak{g})/U_1(\mathfrak{g})$.

$\square$

2) $U_n(\mathfrak{g})$ is already generated (as vector space) by all $\sigma(x_{i_1}) \cdots \sigma(x_{i_m})$ with $m \le n$ and $i_1 \le \ldots \le i_m$.

*Proof.* — Follows from 1) and induction on $n$. □

LEMMA 7.23. — *Let $\mathfrak{g}$ be a Lie algebra with basis $(x_i)_{i \in I}$ and suppose that $I$ is equipped with a total order. Let $\mathfrak{M} = \{(i_1, \ldots, i_n) \mid n \ge 0, i_1 \le \ldots \le i_n$ elements of $I\}$. For each $M = (i_1, \ldots, i_n) \in \mathfrak{M}$ set*

$$v_M = \sigma(x_{i_1}) \cdots \sigma(x_{i_n}).$$

*For each $i \in I$ we set*

$$i\#M = (i_1, \ldots, i_\ell, i, i_{\ell+1}, \ldots, i_n)$$

*with $i_\ell \le i \le i_{\ell+1}$. We write $i \le M$ if $i \le i_1$ and in this case we set $iM := i\#M$.*

1) *$(v_M)_{M \in \mathfrak{M}}$ is a $k$-linear generating set of $U(\mathfrak{g})$.*
2) *$U(\mathfrak{g})$ is a $\mathfrak{g}$-module via $\mathfrak{g} \xrightarrow{can} U(\mathfrak{g})^- \longrightarrow \mathrm{End}_k(U(\mathfrak{g}))^-$. That is, $x.v = \sigma(x)v$ for all $x \in \mathfrak{g}$ and $v \in U(\mathfrak{g})$. Recall that $M = (i_1, \ldots, i_n)$.*
    a) *For all $i \in I$ with $i \le M$ it holds that $x_i.v_M = v_{iM}$.*
    b) *$[x_i, x_j].v_M = x_i.(x_j.v_M) - x_j.(x_i.v_M)$*
    c) *For all $i \in I$ it holds that $x_i.v_M = v_{i\#M} \mod U_n(\mathfrak{g})$*
3) *If there is a $\mathfrak{g}$-module $V$ with basis $(u_M)_{M \in \mathfrak{M}}$ such that a), b), and c) hold analogously in $V$, then $(v_M)_{M \in \mathfrak{g}}$ is a basis of $U(\mathfrak{g})$. (Here we have to replace $U_n(\mathfrak{g})$ by the span of all $u_M$, $M \in \mathfrak{M}$ with length at most $n$.*

*Proof.* — If $\sum_M \lambda_M v_M = 0$, then it follows that $0 = \sum_M \lambda_M v_M u_\emptyset = \sum_{\lambda_M} u_M$ and hence $\lambda_M = 0$ for all $M$. □

4) *Suppose that $V$ is a vector space with basis $(u_M)_{M \in \mathfrak{M}}$ and $\mu : \mathfrak{g} \times V \to V$ is a $k$-bilinear map such that a), c) hold and b) holds for all $i, j$ with $j < i$ and $j \le M$. Then b) holds and $V$ is a $\mathfrak{g}$-module.*
5) *A pair $(V, \mu)$ as in 4) exists.*

THEOREM 7.24 (POINCARÉ–BIRKOHOFF–WITT). — *Let $\mathfrak{g}$ be a Lie algebra with basis $(x_i)_{i \in I}$ and suppose that $I$ is equipped with a total order. Then $(v_M)_{M \in \mathfrak{M}}$ is a $k$-linear basis of $U(\mathfrak{g})$.*

COROLLARY 7.25. —     1) *If $\mathfrak{g}$ is a Lie algebra, then $(U(\mathfrak{g}), (U_n(\mathfrak{g}))_{n \ge 0})$ is a filtered Hopf algebra.*
2) *If $\mathfrak{g}$ is finite dimensional then $U(\mathfrak{g})$ is left- and right-noetherian.*
3) *$U(\mathfrak{g})$ is an integral domain.*

LEMMA 7.26. — *Let $A$ be an algebra and $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$, $a_i b_j = b_j a_i$ for all $i, j$. Then*

$$(a_1 + b_1) \cdots (a_n + b_n) = \sum_{v=0}^{n} \sum_{\substack{\sigma \in S_n \\ \sigma(1) < \ldots < \sigma(v) \\ \sigma(v+1) < \ldots < \sigma(n)}} a_{\sigma(1)} \cdots a_{\sigma(v)} b_{\sigma(v+1)} \cdots b_{\sigma(n)}$$

LEMMA 7.27. —   *1) The canonical map $\sigma : \mathfrak{g} \to U(\mathfrak{g})$ is injective.*
  *2) The map*

$$k[T_i \mid i \in I] \to \mathrm{gr}(U(\mathfrak{g})), \quad T_i \mapsto \overline{\sigma(x_i)} \in U_1(\mathfrak{g})/U_0(\mathfrak{g})$$

*is an algebra isomorphism.*

## 8. Selected classical algebraic results

**8.1. The Jacobson radical of noncommutative rings.** — In this section $R$ denotes a ring and $M$ denotes an $R$ left-module (or right-module).

DEFINITION 8.1. —
1) $M$ is called simple if $M \neq 0$ and if $0$ and $M$ are the only submodules of $M$.
2) For any subset $X \subset M$ we set
$$\mathrm{Ann}(X) = \{r \in R \mid rX = 0\}.$$

PROPOSITION 8.2. — For $N \subsetneq M$ a submodule it holds that $M/N$ is simple if and only if $N \neq M$ is a maximal submodule.

PROPOSITION 8.3. — For all $m \in M$ it holds that $R/\mathrm{Ann}(m) \simeq Rm$.

PROPOSITION 8.4. — Suppose that $M \neq 0$. Then the following statements are equivalent.
1) $M$ is simple
2) There is a maximal left-ideal $I \lhd R$ such that $M \simeq R/L$ as left-modules.
3) For any $0 \neq m \in M$ it holds that $M = Rm$.

PROPOSITION 8.5. —
1) The Jacobson radical $\mathrm{Ra}(M)$ is defined as the intersection of all maximal submodules $U \subsetneq M$. (If no such submodules exist then we set $\mathrm{Ra}(M) = M$.)
2) It holds that $\mathrm{Ra}(M/\mathrm{Ra}(M)) = 0$.
3) If $M$ is finitely generated then $\mathrm{Ra}(M) \subsetneq M$.

LEMMA 8.6. — Let $R$ be a ring and $a, b \in R$.
1) Then $1 - ab$ has a left-inverse (right-inverse) if and only if $1 - ba$ has a left-inverse (right-inverse).
2) More precisely, If $x$ is a left-inverse (right-inverse) of $1 - ab$ then $1 + bxa$ is a left-inverse (right-inverse) of $1 - ba$.
3) The set
$$I = \{r \in R \mid 1 - rx \text{ has a left-inverse for all } x \in R\}$$
is a two-sided ideal of $R$.

LEMMA 8.7. — Let $R$ be a ring and $r \in R$. Then the following statements are equivalent:
1) $r \in \mathrm{Ra}(_R R)$
2) $r \in \mathrm{Ra}(R_R)$
3) For any $x \in R$ it holds that $1 - xr$ has a left-inverse
4) For any $x \in R$ it holds that $1 - rx$ has a right-inverse
5) For all $x, y \in R$ it holds that $1 - xry \in R^\times$
6) For any simple left $R$-module $M$ it holds that $rM = 0$

*7) For any simple right $R$-module $M$ it holds that $Mr = 0$*

COROLLARY 8.8. — *For any ring $R$ it holds that $\mathrm{Ra}(R) := \mathrm{Ra}(_R R) = \mathrm{Ra}(R_R) \lhd R$ is an ideal.*

PROPOSITION 8.9. — *If $M$ is simple then any ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)$ factorizes over $R/\mathrm{Ra}(R)$. The two ring $R$ and $R/\mathrm{Ra}(R)$ have the same simple left-modules and right-modules.*

PROPOSITION 8.10. — *For any any $r \in R$ it holds that $r \in R^{\times}$ if and only if $\bar{r} \in (R/\mathrm{Ra}(R))^{\times}$.*

PROPOSITION 8.11. — *It holds that $\mathrm{Ra}(R)\,_R M \subset \mathrm{Ra}(_R M)$.*

LEMMA 8.12 (NAKAYAMA). — *Suppose that $0 \neq M$ is finitely generated. Let $U \subset M$ be a submodule with $M = \mathrm{Ra}(R)M + U$. Then it follows that $M = U$.*

PROPOSITION 8.13. — *A left-ideal $I \subset R$ is called nil if each element $x \in I$ is nilpotent. If this is the case then $I \subset \mathrm{Ra}(R)$.*

*Proof.* — Let $x \in I$. Then for all $r \in R$ it holds that $rx \in I$, yielding that $rx$ is nilpotent. This means that $1 + rx$ is invertible. As this holds for all $r \in R$ it follows that $x \in \mathrm{Ra}(R)$. $\qquad\square$

DEFINITION 8.14. — *We say $M$ is artinian if any non-empty set of submodules has a minimal element. This is equivalent to requiring that any descending chaing of submodules stabilizes.*

PROPOSITION 8.15. — *Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence. Then $M$ is artinian if and only if $M'$, $M''$ are artinian.*

PROPOSITION 8.16. — *If $M_1, \ldots, M_n$ are artinian then so is $M_1 \otimes \ldots \otimes M_n$.*

*Proof.* — The sequence $0 \to M_1 \to M_1 \times M_2 \to M_2 \to 0$ is exact. $\qquad\square$

PROPOSITION 8.17. — *If $_R R$ is artinian and $M$ is finitely generated then $M$ is artinian.*

DEFINITION 8.18. — *An ideal $I$ is called nilpotent if $I^n = 0$ for some $n \geq 1$.*

PROPOSITION 8.19. — *If $_R R$ or $R_R$ is artinian, then $\mathrm{Ra}(R) \lhd R$ is the largest nilpotent ideal of $R$.*

*Proof.* — Suppose that $_R R$ is artinian. Set $I = \mathrm{Ra}(R)$. Then there is an $n \geq 1$ with $I^n = I^{2n}$. Suppose that $I^n \neq 0$. Then there is a left-ideal $0 \neq L \lhd R$ that is minimal with $I^n L = L$. Hence there is an element $0 \neq x \in L$ with $0 \neq I^n x \subset L$. It holds that $I^n(I^n x) = I^{2n}x = I^n x$. By minimality of $L$ it follows that $L = I^n x$. Since $x \in L$ it follows that there is an element $y \in I^n$ with $yx = x$. This implies $(y-1)x = 0$. But $y \in \mathrm{Ra}(R)$

implies that $y - 1 \in R^\times$ and hence $x = 0$. This contradicts our assumption. It follows that $I^n = 0$.                                                                                              $\square$

PROPOSITION 8.20. — *$R$ is a skew field if and only if $_R R$ is simple (equivalently, if $R_R$ is simple).*

DEFINITION 8.21. — *We say a ring $R$ is local if any of the following equivalent conditions is satisfied.*

  *1) $R$ has a unique maximal left ideal*
  *2) $R$ has a unique maximal right ideal*
  *3) $R/\mathrm{Ra}(R)$ is a skew field*
  *4) $\mathrm{Ra}(R) = R \setminus R^\times$*
  *5) $R \setminus R^\times$ is closed under addition*
  *6) $R \setminus R^\times$ is an ideal of $R$*

*Proof.* — The first three equivalences are clear. For any $r \in R$ it holds that $r \in R^\times$ if and only if $\bar{r} \in (R/\mathrm{Ra}(R))^\times$. Hence $R/\mathrm{Ra}(R)$ is a skew field if and only if $\mathrm{Ra}(R) = R \setminus R^\times$. Suppose that $R \setminus R^\times$ is closed under addition. Let $x \in R \setminus \mathrm{Ra}(R)$. Then there is a maximal ideal $I \lhd R$ with $x \notin I$. Hence $R = I + Rx$. That is, there is an $y \in I, r \in R$ with $1 = y + rx$. Since $y$ is not invertible and we assumed that $R \setminus R^\times$ is closed under addition it follows that $rx$ is invertible. In particular, $x$ has a left-inverse. As this holds for all $x \in R \setminus \mathrm{Ra}(R)$ it follows that $N := R/\mathrm{Ra}(R)$ is simple as a left $R$ module. Consequently, $N$ is also simple as an $R/\mathrm{Ra}(R)$ left module. Hence $R/\mathrm{Ra}(R)$ is a skew field.          $\square$

PROPOSITION 8.22. — *If $R$ is local then any element $e \in R$ with $e^2 = e$ satisfies $e = 1$ or $e = 0$.*

*Proof.* — If $e \in R^\times$ then it follows that $e = 1$. If $e \notin R^\times$ then it follows that $1 - e$ is invertible and hence $e = 0$.                                                                      $\square$

PROPOSITION 8.23. — *Let $R$ be a ring and suppose that each element $r \in R \setminus R^\times$ is nilpotent. Then $R$ is local.*

*Proof.* — Suppose that $R$ is not local. Then there are $x, y \in R \setminus R^\times$ with $x + y \in R^\times$. We may assume that $x + y = 1$. But this implies that $y = 1 - x$ is invertible since $x$ is nilpotent.                                                                                                    $\square$

**8.2. The Krull–Schmidt theorem.** — In this section $R$ denotes a ring and $M$ a left $R$-module.

PROPOSITION 8.24. — *There is a bijection between the collection of families $(M_i)_{i \in I}$ of submodules of $M$ with $M = \bigoplus_{i \in I} M_i$ and the collection of families $(e_i)_{i \in I}$ of endomorphisms of $M$ that satisfy $e_i e_j = \delta_{i,j} e_i$ for all $i, j$ and $\mathrm{id} = \sum_{i \in I} e_i$.*

*Here such a family* $(e_i)_{i \in I}$ *of endomorphisms gets mapped to the family* $(e_i(M))_{i \in I}$ *of submodules. Conversely, a family* $(M_i)_{i \in I}$ *of submodules with* $M = \bigoplus_{i \in I} M_i$ *gets mapped to the family* $(\pi_i \iota_i)_{i \in I}$ *of endomorphisms with* $\iota_i : M_i \subset M$ *the subset embedding and* $\pi_i : M \to M_i$ *the projection.*

PROPOSITION 8.25. — *Let* $f \in \operatorname{End}(M)$.

1) *If* $M$ *is artinian and* $f$ *a monomorphism, then* $f$ *is an isomorphism.*
2) *If* $M$ *is noetherian and* $f$ *an epimorphism, then* $f$ *is an isomorphism.*
3) *If* $M$ *is artinian and noetherian then there exists an integer* $N$ *such that for all* $n \geq N$ *it holds that* $M = \operatorname{im} f^n \oplus \ker f^n$.

*Proof.* — 1) Suppose that $M$ is artinian. The descending chain $\operatorname{im} f \subset \operatorname{im} f^2 \subset \ldots$ stabilizes after a finite number $n$ of steps. Then for any $x \in M$ there is an element $y \in M$ with $f^{2n}(y) = f^n(x)$. This implies $x - f^n(y) \in \ker f^n$. Since this holds for all $x$ it follows that $M = \operatorname{im} f^n + \ker f^n$. In particular, if $f$ is injective it follows that $f$ is also surjective.

2) Suppose that $M$ is noetherian. Then the ascending chain $\ker f \subset \ker f^2 \subset \ldots$ stabilizes after a finite number $n$ of steps. This implies $\operatorname{im} f^n \cap \ker f^n = 0$. If $f$ is surjective then this implies that is also injective.

3) If $M$ is artinian and noetherian then we obtain $M = \operatorname{im} f^n \oplus \ker f^n$. $\qquad \square$

DEFINITION 8.26. — *We say* $M$ *is indecomposable if* $M \neq 0$ *and for any submodules* $X, Y \subset M$ *with* $M = X \oplus Y$ *it holds that* $X = 0$ *or* $X = M$.

PROPOSITION 8.27. — *Let* $M \neq 0$.

1) $M$ *is indecomposable if and only if* $\operatorname{End}(M)$ *has no idempotent elements besides* $0$ *and* id.
2) *If* $\operatorname{End}(M)$ *is local then* $M$ *is indecomposable.*

PROPOSITION 8.28. — *Let* $M \neq 0$ *be artinian and noetherian. Then* $M$ *is indecomposable if and only if* $\operatorname{End}(M)$ *is local.*

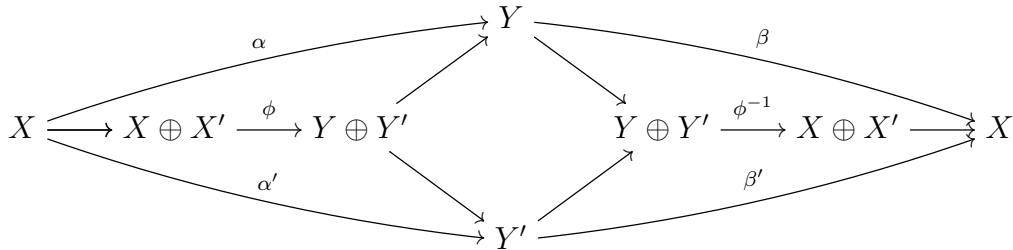LEMMA 8.29. — *Suppose that the following diagram has exact diagonals:*
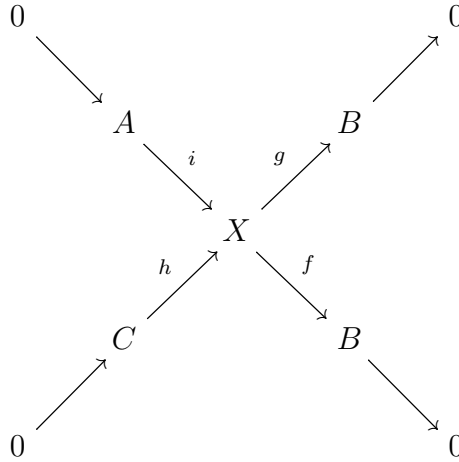


*The $gi$ is an isomorphism if and only if $fh$ is an isomorphism.*

*Proof.* — Suppose that $gi$ is an isomorphism. Then

$$X = \operatorname{im}i \oplus \ker g = \operatorname{im}h \oplus \ker f.$$

Thus $fh$ is an isomorphism.       □

PROPOSITION 8.30. — *Let $X, X', Y, Y'$ be modules and $\phi : X \oplus X' \to Y \oplus Y'$ an isomorphism. Let $\alpha, \alpha', \beta, \beta'$ be the morphism with*



*Then it holds that*

$$\operatorname{id} = \beta\alpha + \beta'\alpha'.$$

    *1) If $\beta\alpha$ is an isomorphism then $X' \simeq \ker\beta \oplus Y'$.*
    *2) If $\beta'\alpha'$ is an isomorphism then $X' \simeq Y \oplus \ker\beta'$.*

LEMMA 8.31. — *Let $X, X', Y, Y'$ be modules, $X \oplus X' \simeq Y \oplus Y'$, $X \simeq Y$, $\operatorname{End}(X)$ local. Then it follows that $X' \simeq Y'$.*

LEMMA 8.32. — *Let $Y, Y', X_1, \ldots, X_n$ be modules such that $\bigoplus_{i=1}^{n} X_i \simeq Y \oplus Y'$, $\operatorname{End}(X_i)$ local for all $i$, and $Y \neq 0$. Then there is an index $i$ such that the composition $X_i \to Y \to X_i$ is an automorphism of $X_i$.*

THEOREM 8.33 (KRULL–SCHMIDT). — *Let $X_1, \ldots, X_n, Y_1, \ldots, Y_m$ be indecomposable (and hence nonzero) modules. Suppose that $\mathrm{End}(X_i)$ is local for all $i$ and*

$$\bigoplus_{i=1}^{n} X_i \simeq \bigoplus_{j=1}^{m} Y_j.$$

*Then $m = n$ and there is a permutation $\sigma \in S_n$ with*

$$X_i \simeq Y_{\sigma(i)}$$

*for all $1 \le i \le n$.*

THEOREM 8.34. — *Let $M \ne 0$ be artinian and noetherian. Then there are up to reordering unique indecomposable submodules $M_1, \ldots, M_n \subset M$ with*

$$M = \bigoplus_{i=1}^{n} M_i.$$

DEFINITION 8.35. — *We sy $M$ is projective if for all modules $X, Y$, any epimorphism $f : X \to Y$ and any morphism $g : M \to Y$ there is a morphism $h : M \to X$ wiwth $g = fh$.*

PROPOSITION 8.36. — *The module $M$ is projective if and only if there is a free module $F$ with submodules $P, P' \subset F$ such that $F = P \oplus P'$ and $M \simeq P$.*

PROPOSITION 8.37. — *Suppose that $M$ is finitely generated. Then $M$ is projective if there is an integer $n \ge 1$ and submodules $P, P \subset R^n$ such that $R^n = P \oplus P'$ and $M \simeq P$.*

PROPOSITION 8.38. — *If $R$ is local then any finitely generated projective $R$ module is free.*

*Proof.* — Let $P \ne 0$ be a finitely generated projective $R$ module. Then there is an integer $n \ge 1$ and a module $P'$ with

$$R^n \simeq P \oplus P'.$$

The endomorphism ring $\mathrm{End}_R(R) \simeq R$ is local. It follows that one of the compositions $R \to P \to R$ is an automorphism of $R$. This yields $P \simeq P_1 \oplus R$ and hence

$$R^n \simeq P_1 \oplus R \oplus P'.$$

Using again that $\mathrm{End}_R(R)$ is local it follows that we may cancel the summand $R$ from the direct sum, yielding

$$R^{n-1} \simeq P_1 \oplus P'.$$

If $P_1 = 0$ we are done. Otherwise we may iterate. $\qquad\square$

## 8.3. The Wedderburn–Artin theorem. —

DEFINITION 8.39. —    *1) We say $R$ is simple if $R \neq 0$ and $0$ and $R$ are the only two-sided ideals of $R$.*

  *2) We say $R$ is semi-simple if $\mathrm{Ra}(R) = 0$ and $R$ is left-artinian or right-artinian.*

THEOREM 8.40 (WEDDERBURN–ARTIN). — *Let $R$ be a semisimple (left- or right-artinian) ring. Then*

$$R \simeq M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r)$$

*for some skew fields $D_1, \ldots, D_r$ and integers $r, n_1, \ldots, n_r \geq 1$. The pairs $(D_i, n_i)$ are unique up to reordering.*

LEMMA 8.41. — *Suppose that $k$ is an algebraically closed field and $D$ is a finite dimensional $k$-algebra. If $D$ is a skew field then $D = k$.*

*Proof.* — Let $x \in D$. Then there is a minimal integer $n \geq 1$ such that $1, x, \ldots, x^n$ are linear independent. This implies that there is a monic polynomial $f \in k[x]$ with degree $n$ such that $f(x)$. Since $k$ is algebraically closed it follows that $f$ has a zero $\zeta \in k$. Hence we may write $f = (X - \zeta)g$ for some monic polynomial $g$. Since $n$ is minimal it follows that $g(x) \neq 0$ and $0 = (x - \zeta)g(x)$. Hence $x = \zeta \in k$.                         $\square$

COROLLARY 8.42. — *Suppose that $k$ is an algebraically closed field and $A$ is a finite dimensional semi-simple $k$-algebra. Then there is a unique integer $r \geq 1$ and up to reordering unique integers $n_1, \ldots, n_r$ such that*

$$A \simeq M_{n_1}(k) \times \ldots \times M_{n_t}(k).$$

*For each integer $n \geq 1$ it holds that $M_n(k)$ is simple. In particular, $A$ is simple if and only if $A \simeq M_n(k)$ for some $n \geq 1$.*

## 9. Cocommutative Hopf algebras in characteristic $0$

**9.1. Irreducible and pointed coalgebras. —**

DEFINITION 9.1. — *Let $C$ be a coalgebra.*

1) *$C$ is called simple, if $C \neq 0$ and $0$ and $C$ are the only subcolagebras of $C$.*

2) *The subcoalgebra*

$$C_0 = \sum_{D \subset C \ simple} D$$

*is called the coradical of $C$.*

3) *We say $C$ is pointed if every simple subcoalgebra $\neq 0$ of $C$ has dimension $1$.*

4) *We say $C$ is irreducible if $C$ has precisely one simple subcoalgebra.*

PROPOSITION 9.2. —     1) *A coalgebra $C$ is cocommutative if and only if $C^*$ is commutative.*

*Proof.* — If $C$ is cocommuative then $C^*$ is commutative. Conversely, suppose that $C^*$ is commutative. Let $(x_i)_i$ be a basis of $C$ and $(e_i)_i$ the corresponding dual basis. For $x \in C$ write $\Delta(x) = \sum_{i,j} \lambda_{i,j} x_i \otimes x_j$. Then for all $k, \ell$ it holds that

$$\lambda_{k,\ell} = (e_k * e_\ell)(x) = (e_\ell * e_k)(x) = \lambda_{\ell,k}.$$

$\square$

2) *Let $D \subset C$ be a one-dimensional subcoalgebra. Then $D$ is simple and there is a group-like element $g \in C$ with $D = kg$.*

*Proof.* — Let $D \subset C$ be a one-dimensional subcoalgebra, $0 \neq x \in D$. It must hold that $\Delta(x) \neq 0$ because otherwise $x = x_1 \epsilon(x_2) = 0$. Hence there is $\lambda \in k^\times$ with $\Delta(x) = \lambda x \otimes x$. Hence $g = \lambda x$ satisfies $g \neq 0$ and $\Delta(g) = g \otimes g$. Hence $g$ is grouplike and $D = kg$. $\square$

3) *If $C$ is a simple coalgebra then $C$ is finite dimensional and $C^*$ is a simple algebra. If additionally $k$ is algebraically closed then there is a unique integer $n \geq 1$ with $C \simeq M_n(k)^*$.*

*Proof.* — $C$ is finite dimensional since it is the union of its finite dimensional subcoalgebras. Let $I \lhd C^*$ be an ideal. Then $C^* \to C^*/I$ is a surjective algebra homomorphism. Consequently, $(C^*/I)^* \to C^{**}$ is an injective coalgebra homomorphism. Since $C^{**} \simeq C$ is simple it follows that $\dim_k(C^*/I)^* \in \{0, \dim_k(C)\}$. That is, $I = 0$ or $I = C^*$.

   If $k$ is algebraically closed, then the Wedderburn–Artin theorem yields that $C^* \simeq M_n(k)$ for a unique integer $n \geq 1$. $\square$

4) *If $C$ is a cocommutative coalgebra and $k$ is algebraically closed then $C$ is pointed.*

*Proof.* — Let $D \subset C$ be a simple subcoalgebra. Then $D$ is finite dimensional and $D \simeq M_n(k)^*$ as coalgebra for a unique $n$. Since $D$ is cocommutative it follows that $n = 1$, that is $D$ is one-dimensional. $\qquad\square$

LEMMA 9.3. — *Let $0 \neq C$ be a coalgebra. Then there is a subcoalgebra $0 \neq D \subset C$ that is simple.*

*Proof.* — Any coalgebra is the union of its finite dimensional subcoalgebras. $\qquad\square$

DEFINITION 9.4. — *Let $V$ be a vector space, $X \subset V$ and $Y \subset V^*$ linear subspaces. We set*

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

PROPOSITION 9.5. — *Let $C$ be a coalgebra (not necessarily finite dimensional).*

*1) For $I \subset C^*$ it holds that $I$ is a two-sided ideal if and only if $I^\perp \subset C$ is a subcoalgebra.*

*2) For $D \subset C$ it holds that $D$ is a subcolagebra if and only of $D^\perp$ is an ideal.*

PROPOSITION 9.6. — *Let $C$ be a finite dimensional coalgebra. Then $X \mapsto X^\perp$ and $Y \mapsto Y^\perp$ yield inclusion inverting bijections:*

$$
\begin{array}{ccc}
\{X \subset C \mid X \text{ linear subspace}\} & \xrightarrow{\ \simeq\ } & \{Y \subset C^* \mid Y \text{ linear subspace}\} \\
\uparrow & & \uparrow \\
\{D \subset C \mid D \text{ subcoalgebra}\} & \xrightarrow{\ \simeq\ } & \{I \lhd C^* \mid I \text{ two-sided ideal}\} \\
\uparrow & & \uparrow \\
\{D \subset C \mid D \text{ simple subcoalgebra}\} & \xrightarrow{\ \simeq\ } & \{I \lhd C^* \mid I \text{ maximal two-sided ideal}\}
\end{array}
$$

*In particular it holds that $\mathrm{Ra}(C^*) = C_0^\perp$ with $C_0$ the coradical of $C$. $C$ is a simple coalgebra if and only if $C^*$ is a simple algebra.*

*Proof.* — It holds that

$$C_0^\perp = \left( \sum_{D \subset C \text{ simple}} D \right)^\perp = \bigcap_{D \subset C \text{ simple}} D^\perp = \bigcap_{I \lhd C^* \text{ maximal ideal}} I = \mathrm{Ra}(C^*).$$

$\qquad\square$

THEOREM 9.7. — *Let $(C, (\tilde{C}_n)_{n \geq 0})$ be a filtered coalgebra. Then $C_0 \subset \tilde{C}_0$. In particular, if $\tilde{C}_0$ is one-dimensional then $C$ is pointed and irreducible.*

*Proof.* — Suppose that there is a simple coalgebra $D \subset C$ that is not a subset of $\tilde{C}_0$. Then there is an integer $n \geq 1$ with $D \subset \tilde{C}_n$ and $D \cap \tilde{C}_{n-1} = 0$. In particular $D \cap \tilde{C}_0 = 0$. Hence there is an $f \in C^*$ with $f(C_0) = 0$ and $f|_D = \epsilon|_D$. This yields for all $d \in D$

$$d = d_1 f(d_2) \in \sum_{i=0}^{n} \tilde{C}_i f(\tilde{C}_{n-i}) = \sum_{i=0}^{n-1} \tilde{C}_i f(\tilde{C}_{n-i}) \in \tilde{C}_{n-1}.$$

$\square$

COROLLARY 9.8. — *If $\mathfrak{g}$ is a Lie algebra then $U(\mathfrak{g})$ is pointed and irreducible.*

THEOREM 9.9. — *Suppose that $k$ is characteristic $0$. Let $\mathfrak{g}$ be a Lie algebra with basis $(x_i)_{i \in I}$. Let $\simeq$ be a total order on $I$. For any $m = (m_i)_i \in \mathbb{N}_0^{(I)}$ we set*

$$e_m = \frac{\prod_{i \in I} x_i^{m_i}}{\prod_{i \in I} m_i!}.$$

1) $(e_m)_{m \in \mathbb{N}_0^{(I)}}$ *is a $k$-basis of $U(\mathfrak{g})$.*
2) *For all $m \in \mathbb{N}_0^{(I)}$ it holds that $\Delta(e_m) = \sum_{a+b=m} e_a \otimes e_b$.*
3) *For any bialgebra $H$ and any injective Lie algebra homomorphism*

$$\mathfrak{g} \hookrightarrow P(H)^-$$

   *it holds that the induced bialgebra homomorphism*

$$U(\mathfrak{g}) \hookrightarrow H$$

   *is injective.*
4) $U(\mathfrak{g})^* \simeq k[[T_i \mid i \in I]], \quad f \mapsto \sum_{m \in \mathbb{N}_0^{(I)}} f(e_m) T^m.$
5) $P(U(\mathfrak{g})) = \mathfrak{g}$

## 9.2. The coradical filtration. —

DEFINITION 9.10. — *Let $C$ be a coalgebra. For any two linear subspaces $X, Y \subset C$ we define the wedge product of $X$ and $Y$ as the preimage*

$$X \wedge Y = \Delta^{-1}(X \otimes C + C \otimes Y).$$

*We also set $\wedge^0 X = 0$ and*

$$\wedge^n X = (\wedge^{n-1} X) \wedge X = \Delta^{-1}((\wedge^{n-1} X) \otimes C + C \otimes X).$$

LEMMA 9.11. — *Let $C$ be a coalgebra and $X, X', Y, Y', Z \subset C$ linear subspaces.*

1) $X \wedge Y = (X^{\perp} Y^{\perp})^{\perp}$
2) $(X \wedge Y) \wedge Z = X \wedge (Y \wedge Z)$
3) *If $X$ and $Y$ are subcoalgebras then so is $X \wedge Y$*
4) *If $X \subset X'$ and $Y \subset Y'$ then $X \wedge Y \subset X' \wedge Y'$*

*Proof.* — *1)* It holds that

$$(X^\perp Y^\perp)^\perp = \left\{ \sum_i f_i * g_i \mid f_i \in X^\perp, g_i \in Y^\perp \text{ for all i} \right\}^\perp$$

$$= \{ c \in C \mid (f * g)(c) = 0 \text{ for all } f \in X^\perp, g \in Y^\perp \}$$

$$= X \otimes C + C \otimes Y.$$

*2)* It follows that

$$(X \wedge Y) \wedge Z = ((X \wedge Y)^\perp Z^\perp)^\perp = (X^\perp Y^\perp Z^\perp)^\perp = X \wedge (Y \wedge Z).$$

*3)* If $X$ and $Y$ are subcoalgebras, then $X^\perp$ and $Y^\perp$ are ideals. Hence $X^\perp Y^\perp$ is an ideal and consequently $X \wedge Y = (X^\perp Y^\perp)^\perp$ is a subcoalgebra. (There is no problem with $C$ not being finite dimensional.)

*4)* This is clear.                                                                                      □

DEFINITION 9.12. — *Let $C$ be a coalgebra and $C_0$ its coradical. For all $n \geq 1$ set*

$$C_n = \wedge^{n+1} C_0.$$

*Then*

$$C_0 \subset C_1 \subset C_2 \subset \dots$$

*is a coalgebra filtration. We call $(C_i)_{i \geq 0}$ the coradical filtration of $C$.*

*Proof.* —     1) We show that $C_n \subset C_{n+1}$ for all $n \geq 0$ by induction. $C_0$ is a subcoalgebra and consequently it holds that $C_0 \subset C_1$. If $C_{n-1} \subset C_n$ then it follows that

$$C_n = \Delta^{-1}(C_{n-1} \otimes C + C \otimes C_0)$$

$$\subset \Delta^{-1}(C_n \otimes C + C \otimes C_0)$$

$$= C_{n+1}.$$

2) We show that $\Delta(C_n) \subset \sum_{i=0}^{n} C_i \otimes C_n$ for all $n$. This is clear for $n = 0$. For $n \geq 1$ it holds for all $0 \leq i \leq n+1$ that

$$C_n = (\wedge^i C_0) \wedge (\wedge^{n+1-i} C_0).$$

Setting $C_{-1} = 0$ this may be expressed by

$$C_n = C_{i-1} \wedge C_{n-i}.$$

It also holds that $\Delta(C_n) \subset C_n \otimes C_n$ since the wedge product of subcoalgebras is a subcoalgebra. Hence Hence

$$\Delta(C_n) \subset \bigcap_{i=0}^{n+1} (C_{i-1} \otimes C_n + C_n \otimes C_{n-i})$$

Choose any supplementary subspace $D_i$ of $C_{i-1}$ inside $C_i$. Then

$$C_i = D_0 \oplus \ldots \oplus D_i$$

for all $i \geq 0$. This implies

$$\bigcap_{i=0}^{n+1} (C_{i-1} \otimes C_n + C_n \otimes C_{n-i}) = \bigcap_{i=0}^{n+1} \bigoplus_{r \leq i-1 \text{ or } s \leq n-i} D_r \otimes D_s$$

$$= \bigoplus_{r+s \leq n} D_r \otimes D_s$$

$$= \sum_{i=0}^{n} C_i \otimes C_{n-i}.$$

3) We show that $\bigcup_{i \geq 0} C_i = C$. If $D \subset C$ is a subcoalgebra then the corresponding coradical filtration $(D_i)_{i \geq 0}$ satisfies $D_i \subset C_i$ for all $i$. Hence without loss of generality we assume that $C$ is finite dimensional. Then $C_0^{\perp} = \mathrm{Ra}(C^*)$ is nilpotent, that is

$$0 = (C_0^{\perp})^n$$

for some $n \geq 1$. Applying $\perp$ to both sides yields

$$C = ((C_0^{\perp})^n)^{\perp} = \wedge^n C_0.$$

$\square$

COROLLARY 9.13. — *If $f : C \to D$ is a surjective coalgebra homomorphism, then $D_0 \subset f(C_0)$.*

*Proof.* — It holds that

$$f(C_0) \subset f(C_1) \subset \ldots$$

is a coalgebra filtration. Consequently, $D_0 \subset f(C_0)$.                      $\square$

## 9.3. Irreducible cocommutative Hopf algebras in characteristic $0$. —

THEOREM 9.14. — *Suppose that $k$ has characteristic $0$. Then*

$$\{\mathfrak{g} \mid \mathfrak{g} \text{ Lie alg.}\} \simeq \{H \mid H \text{ irred. cocom. Hopf alg.}\}$$

$$\mathfrak{g} \mapsto U(\mathfrak{g})$$

$$P(H) \hookleftarrow H.$$

*Proof.* — The functors are well-defined and we already showed that $P(U(\mathfrak{g})) \simeq \mathfrak{g}$. We also know that the Hopf algebra morphism $U(P(H)) \to H$ that we obtain from the universal property of the enveloping algebra is injective (since $k$ has characteristic $0$). It remains to check that is also surjective. We will do this at the end of this section.     $\square$

DEFINITION 9.15. —     *1) We let $\mathcal{C}_k$ denote the category of cocommutative coalgebras.*

2) We let $\mathcal{E}_k$ denote the category of cocommutative coalgebras.

3) For any $C \in \mathcal{C}_k$ we let

$$\mathrm{Cosp}(C) : \mathcal{E}_k^{\mathrm{op}} \to \mathrm{Set}, \quad E \mapsto \mathrm{Coalg}(E, C)$$

denote the cospectrum functor.

PROPOSITION 9.16. —     1) Let $C \in \mathcal{C}_k$ and let $R$ be a commutative finite dimensional algebra. Then $R \otimes_k C$ is an $R$-coalgebra with comultiplication and counit given by

$$R \otimes_k C \xrightarrow{\mathrm{id} \otimes \Delta_C} R \otimes_k C \otimes_k C \xrightarrow{\simeq} (R \otimes_k C) \otimes_R (R \otimes_k C)$$

with $\Delta$ labeling the composite,

and

$$\epsilon : R \otimes_k C \to R, \quad r \otimes c \mapsto r\epsilon(c).$$

We have a functorial bijection of sets

$$G(R \otimes_k C) \simeq \mathrm{Coalg}(R^*, C) = \mathrm{Cosp}(C)(R^*)$$

$$t \mapsto (f \mapsto (f \odot \mathrm{id})(t)).$$

If $C = H$ is a cocommutative Hopf algebra then $R \otimes_k H$ is a Hopf algebra over $R$ and this is a natural isomorphism of groups.

*Proof.* — Let

$$x = \sum_i r_i \otimes c_i \in R \otimes C$$

and let

$$\varphi : R^* \to C, \quad f \mapsto \sum_i f(r_i) c_i$$

be the corresponding map under the isomorphism

$$R \otimes_k C \simeq \mathrm{Hom}_k(R^*, C)$$

$$r \otimes c \mapsto (f \mapsto f(r)c).$$

Then

$$\Delta(\varphi(f)) = \varphi(f_1) \otimes \varphi(f_2) \qquad \text{for all } f \in R^*$$

$$\Leftrightarrow \sum_i f(r_i)\Delta(c_i) = \sum_{s,t} f_1(r_s)f_2(r_t)c_s \otimes c_t \qquad \text{for all } f \in R^*$$

$$\Leftrightarrow \sum_i r_i \Delta(c_i) = \sum_{s,t} \underbrace{f_1(r_s)f_2(r_t)}_{f(r_s r_t)} c_s \otimes c_t \qquad \text{for all } f \in R^*$$

$$\Leftrightarrow \Delta(x) = x \otimes x.$$

and

$$\epsilon(x) = 1 \Leftrightarrow \sum_i r_i \epsilon(c_i) = 1 \Leftrightarrow \underbrace{\sum_i f(r_i)\epsilon(c_i)}_{\epsilon(\varphi(f))} = \underbrace{f(1)}_{\epsilon(f)} \qquad \text{for all } f \in R^*.$$

Now suppose that $C = H$ is cocommutative Hopf algebra. It remains to check that

$$\phi : G(R \otimes H) \simeq \mathrm{Coalg}(R^*, H)$$

is a group homomorphism. To this end, let $x = \sum_i r_i \otimes c_i$ and $y = \sum_j s_j \otimes d_j$ be elements of $G(R \otimes H)$. It holds for all $f \in R^*$ that

$$\begin{aligned}
(\phi(x) * \phi(y))(f) &= \phi(x)(f_1)\phi(y)(f_2) \\
&= \sum_i f_1(r_i)c_i \sum_j f_2(r_j)d_j \\
&= \sum_{i,j} f(r_i r_j)c_i d_j \\
&= \phi(xy)(f)
\end{aligned}$$

and

$$\phi(1 \otimes 1)(f) = f(1)1_H.$$

$\square$

2) *For any $C \in \mathcal{C}_k$ and any two finite dimensional commutative algebras $R$ and $S$ it holds that*

$$G((R \times S) \otimes C) \simeq G(R \otimes C) \times G(S \otimes C).$$

*Proof. —*

$$\begin{aligned}
G((R \times S) \otimes C) &\simeq \mathrm{Coalg}((R \times S)^*, C) \\
&\simeq \mathrm{Coalg}(R^*, C) \times \mathrm{Coalg}(S^*, C) \\
&\simeq G(R \otimes C) \times G(S \otimes C).
\end{aligned}$$

$\square$

3) *Let $C \xrightarrow{f} D$ be a morphism in $\mathcal{C}_k$ such that for any finite dimensional commutative algebra $R$ it holds that the map $G(R \otimes C) \xrightarrow{\mathrm{id} \otimes f} G(R \otimes D)$ is bijective. Then $f$ is an isomorphism.*

*Proof. —* For any finite dimensional commutative algebra $R$ it holds that

$$\begin{CD}
G(R \otimes C) @>{\mathrm{id} \otimes f}>> G(R \otimes D) \\
@V{\simeq}VV @VV{\simeq}V \\
\mathrm{Coalg}(R^*, C) @>{\mathcal{C}_k(\mathrm{id}, f)}>> \mathrm{Coalg}(R^*, D).
\end{CD}$$

That is, for any $E \in \mathcal{E}_k$ it holds that

$$\mathrm{Coalg}(E, C) \overset{\mathcal{C}_k(\mathrm{id}, f)}{\longrightarrow} \mathrm{Coalg}(E, D)$$

is bijective. This means that under the Yoneda bijection

$$\mathcal{C}_k(C, D) \to \mathrm{Mor}(\mathrm{Cosp}(C), \mathrm{Cosp}(D))$$
$$g \mapsto \mathcal{C}_k(\mathrm{id}, g)$$

the map $f$ gets mapped to a natural isomorphism. Since

$$\mathcal{C}_k \simeq \{F : \mathcal{E}_k^{\mathrm{op}} \to \mathrm{Set} \mid F \simeq \mathrm{Cosp}(C) \text{ for some } C \in \mathcal{C}_k\}$$

is an equivalence of categories this implies that $f$ is a bijection.  $\square$

LEMMA 9.17. — *Let $C$ be a coalgebra over $k$ and $k \subset K$ a field extension. Then $(K \otimes C)_0 \subset K \otimes C_0$. In particular, if $C$ is pointed and irreducible then so is $K \otimes C$.*

*Proof.* — Let $C_0 \subset C_1 \subset \ldots$ be the coradical filtration of $C$. Then $K \otimes C_0 \subset K \otimes C_1 \subset \ldots$ is a coalgebra filtration of $K \otimes C$ and consequently

$$(K \otimes C)_0 \subset K \otimes C_0.$$

$\square$

THEOREM 9.18. — *Let $H$ be an irreducible, cocommutative Hopf algebra and $R$ a finite dimensional commutative algebra. Then*

$$G(R \otimes H) = \{g \in 1 \otimes 1 + \mathrm{Ra}(R) \otimes H \mid \Delta(g) = g \otimes g\}.$$

*Proof.* — Since $R$ is finite dimensional the collection $\mathrm{Max}(R)$ of maximal ideals is finite by the Chinese remainder theorem. With $\mathrm{Max}(R) = \{I_1, \ldots, I_n\}$, $K_i = R/I_i$, $k \subset K_i$ finite field extension it holds that

$$G(R/\mathrm{Ra}(R) \otimes H) \simeq G((K_1 \times \ldots \times K_t) \otimes H)$$
$$\simeq G(K_1 \otimes H) \times \ldots \times G(K_t \otimes H).$$

Since $H$ is pointed and irreducible it follows that $K_i \otimes H$ is pointed and irreducible for all $i$. In particular the unit element of $K_i \otimes H$ is its only group-like element. It follows that

$$|G(R/\mathrm{Ra}(R)) \otimes H| = 1.$$

That is,

$$G(R \otimes H) = \ker(G(R \otimes H) \to G(R/\mathrm{Ra}(R) \otimes H)).$$

This implies

$$G(R \otimes H) - 1 \otimes 1 \in \ker(R \otimes H \to R/\mathrm{Ra}(R) \otimes H) = \mathrm{Ra}(R) \otimes H.$$

For each $g \in 1 \otimes 1 + \mathrm{Ra}(R) \otimes H$ it holds that

$$\epsilon(g) \in 1 + \mathrm{Ra}(R) \subset R^{\times}$$

since each element of $\mathrm{Ra}(R)$ is nilpotent. Hence $g$ is group-like if and only if $\Delta(g) = g \otimes g$. $\qquad \square$

THEOREM 9.19. — *Let $H$ be an irreducible cocommutative Hopf algebra and* $\mathrm{char}(k) = 0$. *Then for each finite dimensional commutative algebra $R$ it holds that*

$$\mathrm{Ra}(R) \otimes P(H) \xrightarrow{\exp} G(R \otimes H), \quad x \mapsto \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

*is bijective and functorial in $R$ and $H$.*

*Proof.* — $\mathrm{Ra}(R)$ is nilpotent, so exp yields a functorial bijection

$$\mathrm{Ra}(R) \otimes H \simeq 1 \otimes 1 + \mathrm{Ra}(R) \otimes H$$

with inverse given by log. The sequence

$$0 \to P(H) \subset H \xrightarrow{\Delta - f} H \otimes H$$

is exact with $f(x) = x \otimes 1 + 1 \otimes x$ for all $x \in H$. Since $\otimes_k$ is exact it follows that

$$0 \to \mathrm{Ra}(R) \otimes P(H) \to \mathrm{Ra}(R) \otimes H \to \mathrm{Ra}(R) \otimes H \otimes H$$

is exact. Here $r \otimes y \in \mathrm{Ra}(R) \otimes P(H)$ gets mapped to

$$r \otimes y_1 \otimes y_2 - r \otimes y \otimes 1 - r \otimes 1 \otimes y.$$

Applying the canonical bijection $R \otimes H \otimes H \simeq (R \otimes H) \otimes_R (R \otimes H)$ yields that

$$\mathrm{Ra}(R) \otimes P(H) = \{x \in \mathrm{Ra}(R) \otimes H \mid \Delta(x) = x \otimes 1 + 1 \otimes x\}.$$

For any $x \in \mathrm{Ra}(R) \otimes H$ it holds that $\Delta(x) = 1 \otimes x + x \otimes 1$ if and only if $\Delta(\exp(x)) = \exp(x) \otimes \exp(x)$. This follows from

$$\exp(\Delta(x)) = \Delta(x)$$

and

$$\exp(1 \otimes x + x \otimes 1) = (1 \otimes \exp(x))(\exp(x) \otimes 1) = \exp(x) \otimes \exp(x).$$

$\qquad \square$

*Remaining proof of Theorem 9.14.* — In order to finalize the proof of Theorem 9.14 it remains to show that the monomorphism $U(P(H)) \to H$ is surjective. We know that

$$\psi : P(U(P(H))) = P(H).$$

Hence for any commutative algebra $R$ it holds with $\tilde{H} = U(P(H))$ that

$$
\begin{array}{ccc}
\mathrm{Ra}(R) \otimes P(\tilde{H}) & \xrightarrow{\;\simeq\;} & G(R \otimes \tilde{H}) \\
\Big\downarrow{\scriptstyle \mathrm{id}\otimes\psi} & & \Big\downarrow{\scriptstyle \mathrm{id}\otimes\psi} \\
\mathrm{Ra}(R) \otimes P(H) & \xrightarrow{\;\simeq\;} & G(R \otimes H).
\end{array}
$$

$\square$

## 9.4. Cocommutative Hopf algebras in characteristic $0$. —

REMARK 9.20. — *Let $H$ be a Hopf algebra, $G$ a group, $H$ a $k[G]$ left module algebra such that for each $g \in G$ it holds that*

$$
\hat{g} : H \to H, \quad x \mapsto g.x
$$

*is a coalgebra homomorphism. That is, we assume that the left module algebra structure is induced by a group homomorphism*

$$
\rho : G \to \mathrm{BiAlg}(H, H).
$$

*Then $H \# k[G]$ is a Hopf algebra with smash product algebra structure and*

$$
\begin{aligned}
\Delta(x \# g) &= x_1 \# g \otimes x_2 \# g \\
\epsilon(x \# g) &= \epsilon(x) \\
S(x \# g) &= (1 \# g^{-1})(S(x) \# 1)
\end{aligned}
$$

*for all $x \in H$, $g \in G$.*

*Proof.* — For any $x, y \in H$ and $g \in G$ we have

$$
g.(xy) = (g_1.x)(g_2.x) = (g.x)(g.x) \qquad \text{and} \qquad g.1 = \epsilon(g)1 = 1.
$$

That is, $k[G]$ left module algebra structures correspond to algebra homomorphisms $k[G] \to \mathrm{Alg}(H, H)$, that is a group homomorphism

$$
G \to \mathrm{Alg}(H, H), \quad g \mapsto \hat{g}.
$$

Hence requiring that $\hat{g}$ is a coalgebra homomorphism is equivalent to requiring that this group homomorphism is actually a morphism

$$
G \to \mathrm{BiAlg}(H, H).
$$

It's easy to see that $\Delta, \epsilon$ satisfy the coalgebra axioms. Let's check that they are algebra homomorphisms. It holds that

$$
\begin{aligned}
\Delta((x\#g)(y\#h)) &= \Delta(x(g.y)\#gh) \\
&= x_1(g.y)_1\#gh \otimes x_2(g.y)_2\#gh \\
&= x_1(g.y_1)\#gh \otimes x_2(g.y_2)\#gh \\
&= (x_1\#g \otimes x_2\#g)(y_1\#h \otimes y_2\#h) \\
&= \Delta(x\#g)\Delta(y\#h).
\end{aligned}
$$

and

$$
\begin{aligned}
\epsilon((x\#g)(y\#h)) &= \epsilon(xg.y\#gh) \\
&= \epsilon(x)\epsilon(g.y) \\
&= \epsilon(x)\epsilon(y) \\
&= \epsilon(x\#g)\epsilon(y\#h).
\end{aligned}
$$

As for the antipode axioms:

$$
\begin{aligned}
S(x_1\#g)x_2\#g &= (1\#g^{-1})(S(x_1)\#1)(x_2\#g) \\
&= (1\#g^{-1})(S(x_1)x_2\#g) \\
&= \epsilon(x)(g^{-1}.1\#g^{-1}g) \\
&= \epsilon(x)1\#1.
\end{aligned}
$$

The rest is clear. $\hfill\square$

LEMMA 9.21. — *Let $C$ be a coalgebra, $C_i \subset C$ a subcoalgebra for each $i \in I$, and $E \subset \sum_{i\in I} C_i$ a simple subcoalgebra. Then there is an index $i \in I$ with $E \subset C_i$.*

*Proof.* — Since $E$ is finite dimensional we may assume that $I$ is finite. By induction it suffices to show that if $E \subset C_i + C_j$ and $E \not\subseteq C_i$ then $E \subset C_j$. In this case it holds that $E \cap C_i = 0$ since $E$ is simple. Hence there is a functional $f \in C^*$ with $f\mid_E = \epsilon$ and $f\mid_{C_i} = 0$. Let $x \in E$. Then there are $a \in C_i$ and $b \in C_j$ with $x = a + b$. Hence

$$
x = x_1\epsilon(x_2) = x_1 f(x_2) = b_1 f(b_2) \in C_j.
$$

$\hfill\square$

REMARK 9.22. — *Recall: If $A$ is a finite dimensional algebra, then $A$ is artinian and noetherian as $A$-module. By the Krull–Schhmidt theorem it follows that $A = \bigoplus_{i=1}^{n} A_i$ for some indecomposable $A$-submodules $A_i \subset A$. In particular, $\mathrm{End}_A(A_i)$ is a local ring for all*

*i. Writing $1 = \sum_{i=1}^{n} e_i$ with $e_i \in A_i$ it follows that $e_i e_j = \delta_{i,j} e_i$ for all $i, j$ and $A_i = Ae_i$. Moreover,*

$$\mathrm{End}_A(Ae_i)^{\mathrm{op}} \simeq e_i A e_i$$
$$\varphi \mapsto \varphi(e_i) = \varphi(e_i^2) = e_i \varphi(e_i)$$
$$(x \mapsto xy) \leftmapsto y.$$

*If $A$ is commutative, this implies that $A_i \simeq \mathrm{End}_A(A_i)^{\mathrm{op}}$ is a local ring with unit element $e_i$. In particular,*

$$A = \bigoplus_{i=1}^{n} A_i \simeq \prod_{i=1}^{n} A_i$$

*is the product of local subrings.*

DEFINITION 9.23. — *A subcoalgebra $D$ of a coalgebra $C$ is an irreducible component if $D$ is a maximal irreducible subcoalgebra.*

THEOREM 9.24. — *Let $C$ be a coalgebra.*

1) *Every sum of pairwise distinct simple subcoalgebras is direct.*

*Proof.* — If $E_i \subset C$ is simple for all $i \in I$ and the sum $\sum_i E_i$ is not direct, then there is an index $i \in I$ with $E_i \cap \bigcap_{j \neq i} E_j \neq 0$. But this would entail $E_i \subset E_j$ for some $j \neq i$. □

2) *Every irreducible subcoalgebra of $C$ is contained in a unique irreducible component of $C$.*

*Proof.* — Let $D \subset C$ be a simple subcoalgebra. It suffices that the sum of all irreducible subcoalgebras $C'_i$, $i \in I$ that contain $D$ is irreducible. Indeed, if $E \subset \sum_i C'_i$ is a simple coalgebra then it follows that $E \subset C'_i$ for some $i$. Since $C'_i$ is irreducible and $D \subset C'_i$ it follows that $E = D$. □

3) *The sum of all irreducible components of $C$ is direct.*

*Proof.* — Let $C_i \subset C$, $i \in I$ be the irreducible components. If the sum is not direct, then there is an index $i \in I$ such that $C_i \cap \sum_{j \neq i} C_j \neq 0$. Let $E \subset C_i$ be the unique simple subcoalgebra. Since $C_i \cap \sum_{j \neq i} C_j$ is a non-trivial subcoalgebra of $C_i$ that contains a simple coalgebra it follows that $E \subset C_i \cap \sum_{j \neq i} C_j$. Hence there is an index $j \neq i$ with $E \subset C_j$. But this would imply $C_i = C_j$.x □

4) *If $C$ is cocommutative, then $C = \bigoplus_{D \subset C \text{ irred. comp.}} D$.*

*Proof.* — It suffices to show that $C$ is the sum of irreducible subcoalgebras. Without loss of generality we assume that $C$ is finite dimensional. Then $C^*$ is a finite dimensional commutative algebra, yielding

$$C^* \simeq \prod_{i=1}^{n} A_i$$

for some local subalgebras $A_i \subset C^*$. This implies that $A_i^*$ is an irreducible coalgebra for all $i$ and

$$C \simeq \bigoplus_{i=1}^{n} A_i^*.$$

$\square$

PROPOSITION 9.25. — *Let $C, D$ be coalgebras. Then $(C \otimes D)_0 \subset C_0 \otimes D_0$. In particular, if $C$ and $D$ are pointed then so is $C \otimes D$.*

*Proof.* — Without loss of generality we assume that $C$ and $D$ are finite dimensional. We define the ideal

$$I := C_0^{\perp} \otimes D^* + C^* \otimes D_0^{\perp} \lhd C^* \otimes D^* = (C \otimes D)^*.$$

Our aim is to show that

$$(C \otimes D)_0 \subset I^{\perp} \subset C_0 \otimes D_0.$$

As for the first inclusion, note that

$$C_0^{\perp} = \mathrm{Ra}(C^*)$$

is nilpotent since $C^*$ is finite dimensional (and hence artinian). Likewise it holds that $D_0^{\perp}$ is nilpotent. This implies that $I$ is nilpotent. Since $\mathrm{Ra}((C \otimes D)^*)$ is the largest nilpotent ideal of $(C \otimes D)^*$ it follows that

$$I \subset \mathrm{Ra}((C \otimes D)^*) = (C \otimes D)_0^{\perp}.$$

That is, $(C \otimes D)_0 \subset I^{\perp}.+$

As for the second inclusion, let $x = \sum_i c_i \otimes d_i \in I^{\perp}$ with $(d_i)_i$ linear independent. Then for all $f \in C_0^{\perp}$ and $g \in D^*$ it follows that

$$0 = \sum_i f(c_i)g(d_i) = g(\sum_i f(c_i)d_i).$$

Hence

$$\sum_I f(c_i)d_i = 0$$

and consequently

$$f(c_i) = 0$$

for all $i$. That is, $c_i \in C_0^{\perp\perp} = C_0$ for all $i$ and consequently

$$I^\perp \subset C_0 \otimes D.$$

Analogously, it follows that

$$I^\perp \subset C \otimes D_0$$

and hence

$$I^\perp \subset C_0 \otimes D_0.$$

□

THEOREM 9.26 (CARTIER–KOSTANT). — *Let $H$ be a Hopfalgebra, $G = G(H)$. For each $g \in G$ let $H^g$ be the irreducible component that contains $g$. We set*

$$H' = \bigoplus_{g \in G} H^g.$$

1) *The map*

$$\rho : G \to \mathrm{HopfAut}(H^1), \quad \rho(g)(x) = gxg^{-1}$$

*is a well-defined group homomorphism. It holds that*

$$H^1 \# k[G] \simeq H', \quad x\#g \mapsto xg$$

*is an isomorphism of Hopf algebras.*
2) *If $H$ is pointed and cocommutative, then*

$$H^1 \# k[G] \simeq H.$$

*Proof. —* 2) follows from 1), because if $H$ is pointed and cocommutative then $H$ is the sum of its irreducible components and all irreducible components are of the form $H^g$, $g \in G(H)$. It remains to verify 1). We proceed in small steps.

a) For all $g \in G$ it holds that $H^g = gH^1 = H^1g$.

   The map $H \to H, x \mapsto gx$ is a coalgebra isomorphism because $g$ is group-like. Hence $gH^1 \subset H$ is an irreducible component. Since $g \in gH^1$ it follows that $g.H^1 = H^g$. Likewise it follows that $H^1g = H^g$.

b) For all $g \in G$ it holds that $S(H^g) \subset H^{g^{-1}}$.

   $S : H^{\mathrm{cop}} \to H$ is a coalgebra homomorphism and $\tilde{H} := H^g \subset H^{\mathrm{cop}}$ is a subcoalgebra. This entails that $S(\tilde{H}) \subset H$ is a subcoalgebra and $g^{-1} \in S(\tilde{H})$. So $S(\tilde{H})_0 \subset S(\tilde{H}_0) = kg^{-1}x$. Hence $S(\tilde{H})$ is irreducible, yielding $S(H^g) \subset H^{g^{-1}}$.

c) $(H^1)^2 = H^1$ and $H^1 \subset H$ is a sub Hopf algebra.

   $H^1$ is pointed and irreducible, and hence so is $H^1 \otimes H^1$. Hence $(H^1)^2 = \mathrm{im}(H^1 \otimes H^1 \to H^1)$ is also pointed and irreducible. This yields $(H^1)^2 \subset H^1$. Conversely, $H^1 = H^1 1 \subset (H^1)^2$.

d) $H'$ is a sub Hopf algebra.

For any $g, h \in G$ it holds by a) that

$$H^g H^h = H^1 g h H^1 = H^1 H^{gh} = H^1 H^1 gh = H^1 gh = H^{gh}.$$

Hence $H'$ is a subalgebra. It is a subcoalgebra because all irreducible components are subcoalgebras. It is a sub Hopf algebra by b).

e) $\rho$ is well-defined and hence $H^1 \# k[G]$ is a Hopf algebra

For all $g, h \in G$ it holds by a) that $g H^h g^{-1} = H^{ghg^{-1}}$.

f) $H^1 \# k[G] \simeq H^g$ as Hopf algebras

For any $g \in G$ it holds that the multiplication $H^1 \# kg \to H^g$ is an isomorphism of vector spaces, yielding a linear isomorphism

$$\varphi : H^1 \# k[G] \to H', \quad x \# g \mapsto xg.$$

This is already a Hopf algebra isomorphism, since

$$\varphi((x \# g)(y \# h)) = \varphi(x g y g^{-1} \# gh) = x g y h = \varphi(x \# g)\varphi(y \# h)$$

and

$$(\varphi \otimes \varphi)(x_1 \# g \otimes x_2 \# g) = x_1 g \otimes x_2 g = \Delta(xg).$$

$\square$

THEOREM 9.27 (CARTIER–KOSTANT). — *Suppose that $k$ is characteristic $0$ and is algebraically closed. Let $H$ be a cocommutative Hopf algebra and set $G = G(H)$, $\mathfrak{g} = P(H)^-$. Define*

$$\rho : G \to \mathrm{LieAut}(\mathfrak{g}), \quad g \mapsto (x \mapsto gxg^{-1}).$$

*Then*

$$U(\mathfrak{g}) \# k[G] \simeq H, \quad x \# g \mapsto xg$$

*is an isomorphism of Hopf algebras with $U(\mathfrak{g}) \# k[g]$ a Hopf algebra via $\rho$.*

*Proof.* — It holds that $\mathrm{LieAut}(\mathfrak{g}) \simeq \mathrm{HopfAut}(U(\mathfrak{g}))$, so $\rho$ yields a group isomorphism from $G$ to $\mathrm{HopfAut}(U(\mathfrak{g}))$ that sends an element $g \in G$ to the corresponding conjugation map.

$H$ is pointed since it is cocommutative and $k$ is algebraically closed (recall that we deduced this from the Artin–Wederburn theorem, since the dual of a simple sub coalgebra must be of the form $M_n(k)^*$ because $k$ is algebraically closed, and $n = 1$ follows from cocommutativity). It follows that

$$H^1 \# k[G] \simeq H$$

as Hopf algebras.

It holds that (using that $k$ is characteristic $0$)

$$H^1 \simeq U(P(H^1)) \subset U(P(H)) \subset H.$$

As the monomorphic image of $U(P(H))$ in $H$ is irreducible and contains $H^1$ it follows that $H^1 = \operatorname{im}(U(P(H)) \subset H)$.                                                                  □

COROLLARY 9.28. — *If $H$ is finite dimensional cocommutative Hopf algebra over an algebraically closed field of characteristic $0$ then $H \simeq k[G(H)]$ is a group algebra.*

*Proof.* — We have $U(P(H)) \subset H$ and hence $P(H) = 0$ since $H$ is finite dimensional.   □

## References

[1] E. ABE, *Hopf algebras*, vol. 74 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge-New York, 1980. Translated from the Japanese by Hisae Kinoshita and Hiroko Tanaka.

[2] D. GRINBERG AND V. REINER, *Hopf Algebras in Combinatorics*, ArXiv e-prints, (2014).

[3] J. C. JANTZEN, *Lectures on quantum groups*, vol. 6 of Graduate Studies in Mathematics, American Mathematical Society, Providence, RI, 1996.

[4] C. KASSEL, *Quantum groups*, vol. 155 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1995.

[5] S. MAC LANE, *Categories for the working mathematician*, vol. 5 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1998.

[6] S. MONTGOMERY, *Hopf algebras and their actions on rings*, vol. 82 of CBMS Regional Conference Series in Mathematics, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1993.

[7] H.-J. SCHNEIDER, *Hopfalgebren und Quantengruppen*, Lecture at the University of Munich, (2008).

[8] M. E. SWEEDLER, *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969.

[9] R. G. UNDERWOOD, *Fundamentals of Hopf algebras*, Universitext, Springer, Cham, 2015.

BENEDIKT STUFLER