SOME THEOREMS ON STRUCTURE OF HOPF ALGEBRAS

PHÙNG HÔ HAI

ABSTRACT. After introducing the concepts of algebra, coalgebra, bialgebras and their (co)-modules we discuss the comodule theory of a coalgebra. This will help us to show the fundamental theorem of coalgebras, that each coalgebra is the union of its finite dimensional coalgebras. Given this we introduce the notion of simple and irreducible coalgebras.

The main tool for studying structure of coalgebras is the coradical filtration, which is introduced in section 2.

The aim of section 3 is to examine the structure of co-commutative Hopf algebras over an algebraically closed field of characteristic zero. The upshot is Cartier theorem 3.6.

LECTURE AT INTERNATIONAL SCHOOL ON HOPF ALGEBRAS AND APPLICATIONS, HANOI, OCTOBER 23 - NOVEMBER 3, 2023.

Contents

Version of October 27, 2023.

1. Algebraic structures

1.1. **Algebras and modules.** We fix a field k and consider vector spaces over k. All linear structures are defined over k.

Axioms for algebras. Let A be a vector space. An algebra structure on A consists of the following:

(i) A bilinear map $m : A \times A \longrightarrow A$ call the multiplication, or the product;
(ii) An element $1 \in A$ called the unit element; subject to the associativity and the unity:
(iii) For all $a, b, c \in A$ the following equations hold

$$m(m(a,b),c) = m(a, m(b,c)); \quad m(1,a) = m(a,1) = a.$$

We shall usually shorten $m(a,b)$ as $a \cdot b$.

Axioms for a Lie algebra. Let L be a vector space. A Lie algebra structure on L consists of the following:

(i) A bilinear map $[-,-] : A \times A \longrightarrow A$ called Lie product; subject to the anti-commutativity and Leibniz rule:
(ii) For all $x, y, z \in L$ the following equations hold

$$[x,y] = -[y,z]; \quad [x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0.$$

Structure constants. Choose a basis $\{e_i\}$ of A, then the multiplication rule on A can be given in terms of the structure constants $c_{i,j}k$:

$$e_i \cdot e_j = \sum_k c_{i,j}^k e_k.$$

This is most useful when A is finite dimensional.

Example. Let $A = \mathrm{End}(V)$ – the set of linear endomorphism of a vector space V. This is an algebra with respect to the composition. If V is finite dimensional then so is A. Choose a basis of A in terms of a basis $\{e_i\}$ of V as follows: take the maps

$$e_{ij} : e_k \mapsto \delta_k^j e_i,$$

that is e_{ij} sends e_k to 0 unless $k = j$, in which case, it sends e_k to e_i. Then the multiplication on A is given by

$$e_{ij} \cdot e_{kl} = \delta_k^j e_{il}.$$

Example. A Lie algebra can be obtained from any associative algebra by taking the commutator as Lie product

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

This Lie algebra will usually be denoted A^L.

Exercise. Find the structure constant for $\mathrm{End}(V)^L$.

The tensor product. For two vector space V, W, their tensor product satisfies the following universal property for all vector space U:

$$\begin{tikzcd} V \times W \arrow[rr, "\otimes-\text{bilinear}"] \arrow[dr, "\forall\varphi", "\text{bilinear}"'] & & V \otimes W \arrow[dl, "\exists!\psi"', "\text{linear}"] \\ & U & \end{tikzcd},$$

where $\otimes$ is the canonical map, sending (v, w) to $v \otimes w$.

A tensor (i.e. an element of $V \otimes W$) of the form $v \otimes w$ is called indecomposable. A general tensor is a linear combination of indecomposable tensors. Notice that "tensor product over k" means

$$(\lambda v) \otimes w = v \otimes (\lambda w).$$

The rank of a tensor $z \in U \otimes V$ is defined to be the shortest length of the presentations of z as sum of indecomposable tensors. We shall see the meaning of this notion later.

The algebra structure can be given in terms of the tensor product as follows.

(i) A linear map $m : A \otimes A \longrightarrow A$ called the multiplication, or the product;
(ii) A linear map $u : k \longrightarrow A$ called the unit map; subject to the associativity and the unity:
(iii) The following equations hold

$$m(m \otimes \mathrm{id}) = m(\mathrm{id} \otimes m) : A \otimes A \otimes A \longrightarrow A;$$

$$m(u \otimes \mathrm{id}) = m(\mathrm{id} \otimes u) = \mathrm{id} : A \longrightarrow A.$$

We can express these equality in terms of diagrams as follows:

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "m\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes m"'] & A \otimes A \arrow[d, "m"] \\ A \otimes A \arrow[r, "m"'] & A \end{tikzcd} \qquad \begin{tikzcd} k \otimes A = A \otimes k \arrow[r, "\mathrm{id}\otimes u"] \arrow[d, "u\otimes\mathrm{id}"'] \arrow[dr, "\mathrm{id}"] & A \otimes A \arrow[d, "m"] \\ A \otimes A \arrow[r, "m"'] & A. \end{tikzcd}$$

Modules are tool to study an algebra. In this lecture we shall usually study left modules. There is also a notion of right modules, the study is similar.

Axioms for modules. A module over an algebra A is a vector space M equipped with a linear map

$$\mu : A \otimes M \longrightarrow M$$

satisfying the following axioms:

(i) associativity: $\mu(\mathrm{id} \otimes \mu) = \mu(m \otimes \mathrm{id})$

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

(ii) unity: $\mu(u \otimes \mathrm{id}) = \mathrm{id}$

$$\begin{tikzcd} k \otimes M \arrow[r, "u\otimes \mathrm{id}"] \arrow[dr, "\mathrm{id}"'] & A \otimes M \arrow[d, "m"] \\ & M. \end{tikzcd}$$

There are other (equivalent) definitions of modules, for instance, using a bilinear map $A \times M \longrightarrow M$ or using an algebra map $A \longrightarrow \mathrm{End}(M)$. Details are left to the reader.

Axioms for modules over a Lie algebra. The notion of modules over a Lie algebra can be given in several ways. The simplest way is perhaps the following.

First notice the canonical isomorphism

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W)),$$

which sends a map $\varphi : U \otimes V \longrightarrow W$ to the map

$$\overline{\varphi} : u \longmapsto \overline{\varphi}_u, \quad \overline{\varphi}_u(v) = \varphi(u \otimes v).$$

Let L be a Lie algebra. A (left) L-module is a vector space V equipped with a linear map $\mu : L \otimes M \longrightarrow M$ such that the induced map

$$L \longrightarrow \mathrm{End}(V)^L$$

is a Lie algebra homomorphism.

1.2. **Coalgebras and Comodules.** Axioms for coalgebras and their comodules are "dual" (in the sense of categories – meaning reversing all morphisms) to those of algebras and their modules. The crucial difference here is the finiteness of the tensor product. To explain this phenomena let's take the space

$$\mathrm{End}(V)$$

of linear endomorphisms of a vector space V. If V is finite dimensional, there is a canonical isomorphism

$$\mathrm{End}(V) \cong V \otimes V^*,$$

here V^* stands for $\mathrm{Hom}(V, k)$. Indeed, there is a natural map from the right hand side to the left hand side:

$$z = \sum_i v_i \otimes \varphi_i \longmapsto \varphi_z : \varphi_z(v) = \sum_i \varphi_i(v) v_i.$$

This map is bijective if and only if V has finite dimension. If V is not finite dimensional, the image of $V^* \otimes V$ in $\mathrm{End}(V)$ consists of those endomorphisms which have finite dimensional image.

Exercise. Show that

(i) The natural map $V \otimes U^* \longrightarrow \mathrm{Hom}(U, V)$

$$z = \sum_i v_i \otimes \varphi_i \longmapsto \varphi_z : \varphi_z(u) = \sum_i \varphi_i(u) v_i$$

is injective with image being the set of maps $U \longrightarrow V$ with finite dimensional image.

(ii) Show that rank of z (that is, the length of the shortest expression of z) is equal to rank of φ_z.

Axioms for coalgebras. A coalgebra structure on a vector space C consists of:

(i) A linear map $\Delta : A \longrightarrow A \otimes A$ call the co-multiplication, or the co-product;

(ii) A linear map $\varepsilon : A \longrightarrow k$ called the co-unit map;

(iii) Subject to the co-associativity and co-unity:

$$(\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta : A \longrightarrow A \otimes A \otimes A;$$
$$(\varepsilon \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \varepsilon)\Delta = \mathrm{id} : A \longrightarrow A.$$

We can express these equations in terms of diagrams, which are mirrored images of those for algebras (all arrows are reversed):

$$\begin{tikzcd}
A \otimes A \otimes A & A \otimes A \arrow[l, "\Delta\otimes\mathrm{id}"'] \\
A \otimes A \arrow[u, "\mathrm{id}\otimes\Delta"] & A \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}
\qquad
\begin{tikzcd}
k \otimes A = A \otimes k & A \otimes A \arrow[l, "\mathrm{id}\otimes\varepsilon"'] \\
A \otimes A \arrow[u, "\varepsilon\otimes\mathrm{id}"] & A. \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \arrow[ul, "\mathrm{id}"']
\end{tikzcd}$$

The axioms for comodules over a coalgebra are constructed in the same manner - reversing all arrows in the diagrams for modules over an algebra. We shall mainly study right comodules to match with left modules.

A comodule over a coalgebra C is a vector space M equipped with a linear map

$$\rho : M \longrightarrow M \otimes C$$

satisfying the following axioms:

(i) associativity: $(\rho \otimes \mathrm{id})\rho = (\mathrm{id} \otimes \Delta)\rho$

$$\begin{tikzcd}
A \otimes A \otimes M & A \otimes M \arrow[l, "\mathrm{id}\otimes\mu"'] \\
A \otimes M \arrow[u, "m\otimes\mathrm{id}"] & A; \arrow[l, "\mu"] \arrow[u, "\mu"']
\end{tikzcd}$$

(ii) unity: $\mu(u \otimes \mathrm{id}) = \mathrm{id}$

$$\begin{tikzcd}
k \otimes M & A \otimes M \arrow[l, "u\otimes\mathrm{id}"'] \\
 & M. \arrow[ul, "\mathrm{id}"] \arrow[u, "m"']
\end{tikzcd}$$

Example. The simplest examples of coalgebras are those obtained by dualizing finite dimensional algebras. If (A, m, u) is an algebra with A finite dimensional, then $(A^*, \Delta = m^*, \varepsilon = u^*)$ is a coalgebra. This is due to the isomorphy between $(V \otimes V)^*$ and $V^* \otimes V^*$. Notice that there are more than one isomorphism between these two spaces and we shall fix the following canonical way:

$$\varphi \otimes \psi \mapsto \xi : u \otimes v \mapsto \varphi(u)\psi(v).$$

Thus, the coproduct on A^* is determined by the following condition:

$$\Delta(\varphi)(a \otimes b) = \varphi(a \cdot b).$$

If M is a (left) A-module then it is a right A^*-comodule with the action $\rho : M \longrightarrow M \otimes A^*$ satisfying the condition

$$\rho(m)(a) = a \cdot m, \quad m \in M, a \in A.$$

Vice-verse, if M is a right A^*-comodule then it is a left A-module by the action given by the above condition (read from the right to the left).

Subcoalgebras and coideals. A coalgebra map is a linear map between coalgebras that is compatible with the coalgebra structures in the natural way. The reader is asked to draw the relevant diagrams.

A subcoalgebra is by definition a subset which is closed under the coproduct. For instance, the image of a colagebra map is a subcoalgebra.

The two-sided coideals should imitate kernels of coalgebra maps. Thus is it defined as a subspace $D \subset C$ satisfying two conditions

(i) $\Delta(D) \subset C \otimes D + D \otimes C \subset C \otimes C$;
(ii) $\varepsilon(D) = 0$,

where Δ, ε are structure map on the coalgebra C. It is straightforward to check that the quotient space by a two-sided coideal is a coalgebra.

There is also notions of left (resp. right) coideals, which are special case of subcomodules (of C considered as left (resp. right) comodule on itself.

Notice that two-side coideals are not "left and right coideals". In fact the latter does not exist, except for the zero ideal.

Exercise. Show that if at subspace $I \subset C$ is at the same time a left and a right coideal in C, then it is a subcoalgebra. The set of two-sided coideals and that of subcoalgebras intersect only in the zero space.

Commutativity and co-commutativity. An algebra is commutative if $ab = ba$ for all $a, b \in A$. In terms of the maps we have the equality

$$m\sigma_{A\otimes A} = m.$$

The notion of co-commuativity for coalgebras is similar, it reads:

$$\sigma_{C\otimes C}\Delta = \Delta.$$

In an algebra we can say that two elements commute, while in a coalgebra we can say that the coproduct is co-commutative in some element if the relevant equation above holds for that elements.

1.3. **Duality.** There is a full duality between finite dimensional algebras and coalgebras. This is due to the fact that the natural inclusion

$$V \longrightarrow V^{**}$$

of a finite dimensional vector space into its double dual is a canonical isomorphism and the natural inclusion

$$V^* \otimes V^* \longrightarrow (V \otimes V)^*$$

is also an isomorphism. Thus the data of an algebra (A, m, u) are in one-one correspondence with the data of a coalgebra (A^*, m^*, u^*).

The situation is more subtle when dealing with infinite dimensional vector spaces: the two maps mentioned above are merely injective but far from surjective. Due to this, only the dual of a coalgebra is an algebra. In this way, coalgebras can be seen as dual of pro-finite algebras (this fact will be proven later, see section 2.

The best known way to attain full duality is to introduce the weak topology on the dual.

From coalgebra to algebra. The duality for coalgebras is not just a formal duality theory, but serves as an important too for the comodule study of coalgebra as well as the structure theory of coalgebras themselves. See sections 2.2

If C is a coalgebra, then its dual space C^* is an algebra, the product on C^* is the restriction of the dual map $m^* : (C \otimes C)^* \longrightarrow C^*$ to the subspace

$$C^* \otimes C \subset (C \otimes C)^*.$$

This product on C^* is called the convolution product:

$$\varphi * \psi : c \longleftarrow (\varphi \otimes \psi)\Delta(c).$$

The co-unit map ε of C is the unit element in C^*.

Correspondence between ideals and coideals. Recall that for a subspace $L \subset C$, it orthogonal complement is

$$L^\perp := \{\varphi \in C^* | \varphi|_L = 0\}.$$

We define the orthogonal complement to a subspace $\Phi \subset C^*$ in the similar manner. We have

$$(L^\perp)^\perp = V$$

for any $L \subset C$. The similar statement for subspaces of C^* is not true. For example, take a basis $\{e_\alpha, \alpha \in S\}$ of C and let ξ^i to be the linear functional $\xi^i(e_j) = \delta^i_j$. Then the complement to the subspace in C^*, spanned by these linear functional is zero, but this subspace is different form C^*. The set $\{\xi^i\}$ is called a pseudo-basis of C^*.

There is a one-one correspondence between ideals, coideals, etc as follows.

Proposition 1.1. *Let C be a coalgebra. The correspondence between right coideals in C and ideals in C^* is as follows (the same holds for left (co-)ideals):*

(i) *If $J \subset C$ is a right coideal then $J^\perp \subset C^*$ is a right ideal.*
(ii) *If $I \subset C^*$ is a right ideal then $I^\perp \subset C$ is a right coideal.*
(iii) *Consequently $J \subset C$ is a left (right) if and only if $J^\perp \subset C^*$ is a left (right ideal).*

The correspondence between two-sided coideals in C and subalgebras in C^* is as follows:

(i) *If $J \subset C$ is a two-sided coideal then $J^\perp \subset C^*$ is a subalgebra.*
(ii) *If $I \subset C^*$ is a subalgebra then $I^\perp \subset C$ is a two-sided coideal.*
(iii) *Consequently $J \subset C$ is a two-sided coideal if and only if $J^\perp \subset C^*$ is a subalgebra.*

Proof. See [Sw69, Prop. 1.4.4–1.4.6]. ☐

The similar statement for subspaces of C^* is not true. To get correct statements one needs to introduce a topology on C^* (the week topology) and restrict to closed ideals in C^*. We shall not discuss further on this topic, the interested reader may consult [Di73].

1.4. **Sweedler's notation.** Let (C, Δ, ε) be a coalgebra. For an element $c \in C$,
$$\Delta(c) \in C \otimes C.$$
Unlike a map $f : C \longrightarrow C$ which can be defined free of basis, there is not canonical way to describe elements of $C \otimes C$ base-free. Thus, usually one write
$$\Delta(c) = \sum_i c_i \otimes c'_i$$
for some (finite) set of elements c_i, c'_i of C. Now the co-associativity of Δ says:
$$\sum_i \Delta(c_i) \otimes c'_i = \sum_i c_i \otimes \Delta(c'_i).$$
It would be tedious to expand $\Delta(c_i)$ and $\Delta(c'_i)$ again and to express their equality.

M. Sweedler introduces the following clever way to express $\Delta(c)$:
$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}.$$
Then the co-associativity would mean
$$\Delta^{(2)}(c) = (\Delta \otimes \mathrm{id})\Delta(c) = (\mathrm{id}\Delta\otimes)\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$
The co-unity amounts to the following:
$$\sum_{(a)} \varepsilon(a_{(1)}) \otimes a_{(2)} = \sum_{(a)} a_{(1)} \otimes \varepsilon(a_{(2)}) = a.$$

1.5. **Rational modules.** The duality functor $V \longrightarrow V^*$ yields a full equivalence between the category of finite dimensional algebras and the category of finite dimensional coalgebras. Further, for a given (co)algebra, it induces an equivalence between the category of its (co)modules and the category of (modules) comodules over its dual:
$$\mathrm{comod}_C \cong \mathrm{mod}_{C^*}, \qquad \mathrm{mod}_A \cong \mathrm{comod}_{A^*}.$$

If A is a infinite dimensional algebra, A^* is generally *not* a coalgebra in the canonical way, since the map $m^* : A^* \longrightarrow (A \otimes A)^*$ may not land in the subspace $A^* \otimes A^* \subset (A \otimes A)^*$.

On the other hand, if C is an arbitrary coalgebra, then C^* is an algebra, as the dual map $\Delta^* : (C \otimes C)^* \longrightarrow C$ restricts to a map
$$m : C^* \otimes C^* \longrightarrow C^*.$$
Explicitly, we define an algebra structure on C^* by the formula:
$$(\phi \cdot \psi)(c) = \sum_{(c)} \phi(c_1)\psi(c_2).$$
This product is usually called the *convolution* product. The unit element in C^* is precisely the counit ε of C.

There is a natural functor $\mathrm{comod}_C \longrightarrow \mathrm{mod}_{C^*}$: if M is a (right) C-comodule given by the coaction ρ, define the action of C^* on M as follows (σ denotes the flip on tensor products):
$$\mu : C^* \otimes M \longrightarrow C^* \otimes M \otimes C \stackrel{\mathrm{id}\otimes\sigma}{\longrightarrow} C^* \otimes C \otimes M \longrightarrow M;$$

$$\varphi \cdot m = \sum_{(m)} \varphi(c_1)c_0.$$

Let rat denote this functor (which is identical on morphisms).

This functor is generally not an equivalence.

Let $\mu : C^* \otimes M \longrightarrow M$ be a module structure. By means for the canonical isomorphism

$$\mathrm{Hom}(C^* \otimes M, M) \cong \mathrm{Hom}(M, \mathrm{Hom}(C^*, M)),$$

μ induces a map

$$\rho : M \longrightarrow \mathrm{Hom}(C^*, M).$$

There is a natural inclusion $M \otimes C \longrightarrow \mathrm{Hom}(C^*, M)$, which sends a tensor $z \in M \otimes C$ to the map

$$\xi \longmapsto (\mathrm{id} \otimes \xi)z.$$

In terms of the bases $\{e_i\}$ and $\{\xi^i\}$ above, it maps $m \otimes e_i$ to the map that maps ξ^j to $\delta_i^j m$.

Lemma 1.2. *If the image of ρ is in $M \otimes C$ then ρ is a coaction of C on M and μ is the induced action from ρ. Conversely, if μ is induced from a coalgebra action of C on M then that action is ρ.*

Proof. (i) We have a more general claim: if μ is induced from a linear map $\tilde{\mu} : M \longrightarrow M \otimes C$ then this map must be ρ. Indeed, the map $\tilde{\mu}$ send an element $m \in M$ to a map $\tilde{\mu}(m) : C^* \longrightarrow M$, given by

$$\tilde{\mu}(m)(\xi) = \mu(\xi \otimes m).$$

If μ is induced from ρ, that is:

$$\mu(\xi \otimes m) = (\mathrm{id} \otimes \xi)\rho(m),$$

Then $\tilde{\mu}(m)(\xi) = (\mathrm{id} \otimes \xi)\rho(m)$, which means

$$\mathrm{im}\tilde{\mu} = \rho(m) \in M \otimes C.$$

(ii) Assume now that the image of ρ is in $M \otimes C$. We need to check its coassociativity and counity. This is obvious due to the equality:

$$\xi \cdot m = (\mathrm{id} \otimes \xi)\rho,$$

and the associativity and unity of C^*. Indeed, to see that

$$(\rho \otimes \mathrm{id})\rho = (\mathrm{id} \otimes \Delta)\rho,$$

we apply $\mathrm{id} \otimes \varphi \otimes \psi$ on both sides and obtain $\varphi \cdot (\psi \cdot m)$ on the left hand side and $(\varphi \cdot \psi) \cdot m$ on the right hand side. □

Definition 1.3. A module of C^* is called rational if it is in the image of rat.

Theorem 1.4. *The functor* rat *satisfies the following properties:*

(i) *The functor* rat *is bijective on hom-sets (i.e. fully faithful).*
(ii) *The functor* rat *is closed under taking subquotient (i.e. a sub- and a quotient module of a rational module is again rational).*
(iii) *Every C^*-module contains a maximal rational submodule, which is the sum of all its rational submodules.*

Proof. □

Corollary 1.5. *Every cyclic submodule of a rational module is finite dimensional. (This is equivalent to the fundamental theorem of comodules).*

1.6. **Bialgebras and Hopf algebras.** There is a notion of tensor product of algebras. If A and B are algebras, a canonical algebra structure on $A \otimes B$ is defined as follows:

$$m_{A\otimes B} := (m_A \otimes m_B)(\mathrm{id} \otimes \sigma_{B\otimes A} \otimes \mathrm{id}) : (A \otimes B) \otimes (A \otimes B) \longrightarrow A \otimes B,$$

where $\sigma_{B\otimes A}$ is the symmetry map $B \otimes A \longrightarrow A \otimes B$, and

$$u_{A\otimes b} := u_A \otimes u_B.$$

In diagram:

$$\begin{tikzcd}
(A \otimes B) \otimes (A \otimes B) \arrow[r, "\mathrm{id}\otimes\sigma_{B\otimes A}\otimes\mathrm{id}"] \arrow[dr, "m_{A\otimes B}"'] & A \otimes A \otimes B \otimes B \arrow[d, "m_A\otimes m_B"] \\
 & A \otimes B.
\end{tikzcd}$$

Similarly, there is a notion of tensor product of coalgebras. If C and D are coalgebras, the canonical coalgebra structure on $C \otimes D$ is defined as follows:

$$\Delta_{C\otimes D} = (\mathrm{id} \otimes \sigma_{C\otimes D} \otimes \mathrm{id})(\Delta_C \otimes \Delta_D),$$

$$\varepsilon_{C\otimes D} = \varepsilon_C \otimes \varepsilon_D.$$

In diagram:

$$\begin{tikzcd}
(C \otimes D) \otimes (C \otimes D) & C \otimes C \otimes D \otimes D \arrow[l, "\mathrm{id}\otimes\sigma_{C\otimes D}\otimes\mathrm{id}"'] \\
 & C \otimes D. \arrow[u, "\Delta_C\otimes\Delta_D"'] \arrow[ul, "\Delta_{C\otimes D}"]
\end{tikzcd}$$

Bialgebras. A bialgebra is defined as a coalgebra in the category of algebras, that is, an algebra H, equipped with algebra maps:

$$\Delta : H \longrightarrow H \otimes H; \quad \varepsilon : H \longrightarrow k,$$

making it a coalgebra, or, equivalently, as an algebra in the category of coalgebra, that is, a coalgebra H, equipped with coalgebra maps:

$$m : H \otimes H \longrightarrow H, u : k \longrightarrow H,$$

making it an algebra.

All in all, we have four maps $m, u, \Delta, \varepsilon$ defining algebra and coalgebra structures on H and satisfying the following compatibility axioms: either Δ, ε are an algebra maps or, equivalently, m, u are a coalgebra maps.

(i)
$$\begin{tikzcd}
H \otimes H \arrow[r, "m"] \arrow[d, "\Delta\otimes\Delta"'] & H \arrow[r, "\Delta"] & H \otimes H \\
H \otimes H \otimes H \otimes H \arrow[rr, "\mathrm{id}\otimes\sigma_{H\otimes H}\otimes\mathrm{id}"] & & H \otimes H \otimes H \otimes H, \arrow[u, "m\otimes m"']
\end{tikzcd}$$

(ii)
$$\begin{tikzcd}
k \arrow[r, "u"] \arrow[d] & H \arrow[d, "\Delta"] \\
k \otimes k \arrow[r, "u\otimes u"'] & H \otimes H,
\end{tikzcd}$$

(iii)
$$\begin{tikzcd}
H \otimes H \arrow[r, "\varepsilon\otimes\varepsilon"] \arrow[d, "m"'] & k \otimes k \arrow[d] \\
H \arrow[r, "\varepsilon"'] & k,
\end{tikzcd}$$

(iv)
$$\begin{tikzcd}
k \arrow[r, "\mathrm{id}"] \arrow[d, "u"'] & k \arrow[d, "\mathrm{id}"] \\
H \arrow[r, "\varepsilon"'] & k
\end{tikzcd}$$

Remark. Δ is an algebra map amounts to (i) and (ii), ε is an algebra map amounts to (iii) and (iv);

m is a coalgebra map amounts to (i) and (iii), u is a coagebra map amounts to (ii) and (iv).

Hopf algebra. A bialgebra H is called a Hopf algebra if there exists a linear endomorphism

$$S : H \longrightarrow H$$

satisfying the following relation

$$m(S \otimes \mathrm{id})\Delta = m(\mathrm{id} \otimes S)\Delta = u\varepsilon.$$

S can be seen as the inverse to the identity map in the algebra $\mathrm{End}(H)$ where the product is the convolution:

$$f * g := m(f \otimes g)\Delta.$$

Notice that the unit with respect to the convolution product is the map $u\varepsilon$ (and certainly not the identity map). In Sweedler's notation it reads:

$$\sum_{(a)} S(a_1)a_2 = \sum_{(a)} a_1 S(a_2) = \varepsilon(a) \cdot 1.$$

Proposition 1.6. *The antipode is an anti-algebra and anti-coalgebra map. That is*

$$S(ab) = S(b)S(a), \quad \Delta(S(a)) = \sum_{(a)} S(a_2) \otimes S_{a_1}, \quad S(1) = 1, \varepsilon S = \varepsilon.$$

Proof. See [Sw69, Proposition 4.0.1]. □

Tensor product of modules and comodules. The coproduct on a bialgebra H allows one to define a natural action of H on the tensor product of its modules:

$$\mu_{V\otimes W} := (\mu_V \otimes \mu_W)(\mathrm{id} \otimes \sigma_{H\otimes V} \otimes \mathrm{id})(\Delta \otimes \mathrm{id} \otimes \mathrm{id}),$$

or, in Sweedler's notation:

$$h \cdot (v \otimes w) = \sum_{(h)} h_1 \cdot v \otimes h_2 \cdot w.$$

Dually, the product on H allows one to define a coaction of H on the tensor product of its comodules:

$$\rho_{V\otimes W} := (\mathrm{id} \otimes \mathrm{id} \otimes m)(\mathrm{id} \otimes \sigma_{H\otimes W} \otimes \mathrm{id})(\rho_V \otimes \rho_W),$$

or, in Sweedler's notation:

$$\rho(v \otimes w) = \sum_{(v),(w)} v_0 \otimes w_0 \otimes v_1 w_1.$$

Dual modules and comodules. If H is a Hopf algebra, the antipode induces an action of H on any of its module, by the following equation:

$$h \cdot \varphi(v) := \varphi(S(v)), \quad v \in V, \varphi \in V^*.$$

The case of coaction is more limited, one has to assume that the comodule is finite dimensional. In this case, the coaction of V^* is defined by the following equation

$$\rho(\varphi)(v) = \sum_{(v)} \varphi(S(v_1))v_0, \quad v \in V, \varphi \in V^*.$$

The last equation is generally not solvable if V has infinite dimension.

Example. Let Γ be a group. The group ring $k[\Gamma]$ has a basis indexed by elements of Γ: $\{e_\gamma\}$. The algebra structure is given by the group multiplication:

$$e_\gamma \cdot e_\kappa = e_{\gamma\kappa}.$$

The unit element is thus e_1 where $1 \in \Gamma$ is the unit element of Γ.

The co-algebra structure is given by

$$\Delta(e_\gamma) = e_\gamma \otimes e_\gamma, \quad \varepsilon(e_\gamma) = 1,$$

and the antipode is

$$S(e_\gamma) = e_{\gamma^{-1}}.$$

Affine group schemes. Let G be an affine group scheme over k. That is $G = \mathrm{Spec}(A)$, where A is a commutative algebra over k, and G is equipped with group structure given by algebraic morphisms (the multiplication and the inverse element):

$$m : G \times G \longrightarrow G, \iota : G \longrightarrow G,$$

and a k-point playing the role of the unit element. In terms of algebra maps we thus have maps

$$\Delta : A \longrightarrow A \otimes A, \quad S : A \longrightarrow A, \quad \text{and } \varepsilon : A \longrightarrow k,$$

making A a Hopf algebra.

Example. The group scheme $\mathbb{G}_m$ is represented by the algebra $k[\mathbb{G}_m] := k[x, x^{-1}] = k[x, y]/(xy - 1)$. The Hopf algebra structure is

$$\Delta(x) = x \otimes x, \quad S(x) = x^{-1}, \quad \varepsilon(x) = 1.$$

Example. The group scheme μ_n over k is represented by the Hopf algebra

$$k[\mu_n] := k[x]/(x^n - 1).$$

The coalgebra structure is given by:

$$\Delta(x) = x \otimes x, \quad S(x) = x^{-1}, \quad \varepsilon(x) = 1.$$

There is a natural map of Hopf algebras

$$k[\mathbb{G}_m] \longrightarrow k[\mu_n],$$

which, in geometric language, tell us that μ_n is subgroup scheme of $\mathbb{G}_m$.

Example. The group scheme $\mathbb{G}_a$ is represented by the algebra $k[\mathbb{G}_a] := k[x]$. The Hopf algebra structure is

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \quad S(x) = -x, \quad \varepsilon(x) = 0.$$

$\mathbb{G}_a$ has no subgroups unless the field k has positive characteristic.

Example. If the field k has characteristic $p > 0$ there is a Hopf algebra structure on the algebra $k[x]/(x^p)$:

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \quad \varepsilon(x) = 0.$$

Δ is an algebra map as we are in characteristic p and

$$\Delta(x^p) = (x \otimes 1 + 1 \otimes x)^p = x^p \otimes 1 + 1 \otimes x^p = 0.$$

The associated group scheme is denoted by α_p. α_p is a finite subgroup of $\mathbb{G}_a$.

Example. Every finite group, say Γ can be made into a (finite) group scheme $G := \widehat{\Gamma}$ over k. Its affine ring is spanned as a vector space by $\{x_\gamma, \gamma \in \Gamma\}$, each are idempontents. That is as an algebra it decomposes into direct product:

$$k[G] = \prod_{\gamma \in \Gamma} k_\gamma,$$

where each k_γ is a copy of k. The coproduct should reflect the group multiplication by the rule

$$\Delta(f)(\gamma, \eta) = f(\gamma\eta),$$

here Δ is seen as the map $k[G] \longrightarrow k[G \times G]$. Therefore we have

$$\Delta(x_\gamma) = \sum_{\alpha\beta = \gamma} x_\alpha \otimes x_\beta.$$

From here we conclude

$$\varepsilon(x_\gamma) = \delta^1_\gamma.$$

This construction does not extend to arbitrary groups as the co-multiplication doesn't.

Exercise.

(i) Show that, the Hopf algebra $k[\mu_n]$ and the Hopf algebra $k[\widehat{\mathbb{Z}/n\mathbb{Z}}]$ are dual to each other.

(ii) In general, if Γ is a finite commutative group. Then the group ring $k[\Gamma]$ and the affine algebra $k[\widehat{\Gamma}]$ are dual to each other.

(iii) If k has characteristic p, the Hopf algebra $k[\alpha_p]$ is self-dual.

The tensor algebra. For a vector space V, the tensor algebra on V is

$$\mathbf{T}(V) := \bigoplus_{i=0}^{\infty} V^{\otimes i}.$$

The product is given by the identification

$$V^{\otimes i} \otimes V^{\otimes j} = V^{\otimes i+j}.$$

We shall omit the tensor product when write the product on $\mathbb{T}(V)$. Thus elements of this algebra are just linear combinations of non-commutative monomials

$$v_1 v_2 \dots v_i, \quad i \geq 0, v_j \in V.$$

Fix a basis $\{e_j\}$ of V, we can identify $\mathbf{T}(V)$ with the ring of non-commutative polynomials in the variables e_js.

There is a natural coalgebra structure on $\mathbf{T}(V)$ given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \quad \varepsilon(x) = 0, \quad x \in V,$$

making $\mathbf{T}(V)$ a bialgebra. This $\mathbf{T}(V)$ cocomutative.

In fact, a Hopf algebra with the antipode $S : x \mapsto -x, x \in V$.

The symmetric tensor algebra. Let $\mathbf{S}(V)$ denote the symmetric tensor algebra, that is, the quotient of $\mathbf{T}(V)$ by the ideal generated by

$$xy - yx, \quad x, y \in V.$$

$\mathbf{S}(V)$ is isomorphic to the algebra of polynomials in the variables e_js. This relation is compatible with the coproduct, that is, the ideal is also a (two-sided) coideal, hence $\mathbb{S}(V)$ inherits the coproduct, antipode and co-unit of $\mathbf{T}(V)$. Thus $\mathbf{S}(V)$ is also a Hopf algebra.

The algebra of symmetric tensors. If the characteristic p of k is positive, there is a big difference between the symmetric power (a quotient of the tensor power) and the symmetric tensors (a subspace of the tensor power). We shall denote by $\mathbf{TS}^i(V)$ the subspace of symmetric tensors in $V^{\otimes i}$ – that is, the set of tensors invariant under the action of the symmetric group $\mathfrak{S}_i$. The subspace

$$\mathbf{TS}(V) := \bigoplus_i \mathbf{TS}^i(V)$$

is a subalgebra of $\mathbf{T}(V)$. Moreover, as the coproduct on $\mathbf{T}(V)$ is commutative, is restricts to $\mathbf{TS}(V)$ making it a Hopf algebra too.

To see the difference between $\mathbf{TS}(V)$ and $\mathbf{T}(V)$, consider the composed map

$$F : \mathbf{TS}^p(V) \longrightarrow V^{\otimes p} \longrightarrow \mathbf{S}^p(V).$$

Excercise. Show that the image of F is spanned by the p-powers of a basis of V (it is certainly independent of the choice of basis) and therefore has dimension equal to the dimension of V.

2. Elementary structure theory of coalgebras

2.1. **Playing with the tensor product.** It this known that the tensor product over a field defines an exact functor. That is, given an exact sequence of vector spaces

$$0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0$$

then for any vector space W, the induced sequence

$$0 \longrightarrow V' \otimes W \longrightarrow V \otimes W \longrightarrow V'' \otimes W \longrightarrow 0$$

is also exact. As a consequence we have the following properties:

Lemma 2.1. *Let $V_1, V_2 \subset V$ and $W_1 \subset W$ be vector subspaces then the following relations hold:*

(i) $V_1 \otimes W \cap V_2 \otimes W = (V_1 \cap V_2) \otimes W$;
(ii) $V_1 \otimes W \cap V \otimes W_2 = V_1 \otimes W_1$,

as vector subspaces of $V \otimes W$.

Proof. The first claim is proved by tensoring W with the exact sequence

$$0 \longrightarrow V_1 \cap V_2 \longrightarrow V_1 \oplus V_2 \longrightarrow V_1 + V_2 \longrightarrow 0,$$

where the left inclusion is the diagonal map $v \longmapsto v \oplus v$ and the right projection is the map $v \oplus w \longmapsto v - w$.

The second claim is proved by tensoring the exact sequence $0 \longrightarrow V_1 \longrightarrow V \longrightarrow V/V_1 \longrightarrow 0$ with that for W_1, W, and chasing the diagram. $\square$

As a consequence we have

Corollary 2.2. *For subspaces $V_1, V_2 \subset V$ and $W \neq 0$, $V_1 \otimes W \subset V_2 \otimes W$ if and only if $V_1 \subset V_2$.*

Proof. "Only if": by Lemma above, $V_1 \otimes W \subset V_2 \otimes W$ implies $V_1 \otimes W = (V_1 \cap V_2) \otimes W$, hence $V_1 = V_1 \cap V_2$, that is $V_1 \subset V_2$. $\square$

Lemma 2.3. *For each element $x \in V \otimes W$, there exists the smallest vector subspace $V_1 \subset V$ such that $x \in V_1 \otimes W$ and hence there exists the smallest $W_1 \subset W$ such that $x \in V_1 \otimes W_1$.*

Proof. One can utilize the lemma above right a way. But there exists a more explicit proof as follow. There exists a shortest expression

$$x = \sum_{i=1}^{r} v_i \otimes v_i',$$

which implies that the v_i's (resp. v_i''s) are linearly independent. Let V_1 be the linear span of the v_i's. Without loss of generality we can assume that V and W are finite dimensional. Then $V \otimes W \cong \mathrm{Hom}(W^\vee, V)$. Under this isomorphism, x corresponds to a linear map $f_x : W^\vee \longrightarrow V$. Then r is the rank of this map and V_1 is the image of it. This shows that V_1 is the smallest vector subspace such that $V_1 \otimes W$ contains x. $\square$

2.2. **Local finiteness of comodules.**

Lemma 2.4. *Let M be a right comodule over a coalgebra C. For any $m \in M$, there exists a finite subcomodule $N \subset M$ that contains m. Consequently, any finite subspace of M is contained in a finite subcomodule.*

Proof. There exists the smallest subspace $N \subset M$ such that $\rho(m) \in N \otimes C$. Notice that ρ and hence $\rho \otimes \mathrm{id}$ is an injective map. Therefore, $\rho(N) \subset M \otimes C$ is the smallest subspace such that $\rho(N) \otimes C$ contains $(\rho \otimes \mathrm{id})\rho(m)$.

Now the coassociativity

$$(\mathrm{id} \otimes \Delta)\rho = (\rho \otimes \mathrm{id})\rho$$

implies that $N \otimes C \otimes C$ is contains $\rho(N) \otimes C$ and hence $\rho(N) \subset N \otimes C$.

The following trick, due to Serre, allows one to generalized the proposition to the case of flat coalgebras over a noetherian ring. Let N' be any finite subspace of M such that $\rho(m) \in N' \otimes C$ and let N be preimage of $N' \otimes C$ in M. Thus

$$\rho(N) \subset N' \otimes C.$$

Using the counit map we have $N \subset N'$, hence is finite dimensional. We claim $\rho(N) \subset N \otimes C$. We have $N \otimes C$ is the preimage of $N' \otimes C \otimes C$ under the map

$$\rho \otimes \mathrm{id} : M \otimes C \longrightarrow M \otimes C \otimes C.$$

Thus is suffices to show that

$$(\rho \otimes \mathrm{id})\rho(N) \subset N' \otimes C \otimes C.$$

But this is obvious due to the coassociativity of ρ. □

Theorem 2.5 (Fundamental theorem of comodules)**.** *Each comodule is the union of its finite dimensional comodules.*

Theorem 2.6 (Fundamental theorem of coalgebras)**.** *Let C be a coalgebra, $x \in C$. Then there exist a finite dimensional subcoalgebra C_0, containing x. Consequently, C is the union of its finite dimensional subcoalgebras.*

Proof. Consider C as a right comodule on ifself by the coproduct. Then there exists a finite subcomodule $M \subset C$ that contains x. Let $\{e_i\}$ be a basis of M. Then there exists unique elements c_i^j such that

$$\Delta(e_i) = \sum_j e_j \otimes c_i^j.$$

The coassociativity implies

$$\Delta(c_i^j) = \sum_k c_k^j \otimes c_i^k, \quad \text{and} \quad \varepsilon(c_i^j) = \delta_i^j.$$

Therefore the subspace C_0 spanned by $\{c_i^j\}$ is a coalgebra. On the other hand, the counity of Δ implies $M \subset C_0$:

$$e_i = \sum_j \varepsilon(e_j) c_i^j.$$

□

If $D, E \subset C$ are subcoalgebras. Then $D \cap E$ is also a subcoalgebra, this is due to the fact that

$$D \otimes D \cap E \otimes E = (D \cap E) \otimes (D \cap E).$$

Hence there exists the smallest coalgebra that contains a given element $x \in C$. This subcoalgebra is called **the subcoalgebra generated** by x.

2.3. **Irreducible coalgebras.** Let C be a coalgebra. From the previous section we know that C is the union of its finite dimensional subcoalgebra. For finite dimensional coalgebras their structure can be deduced from the structure of their duals.

Simple coalgebras. C is said to be simple if it has no proper subcoalgebras. This forces C to be finite dimensional and hence C^* is simple as an algebra. In particular, if k is algebraically closed and C is co-commutative then C is simple iff C is one dimensional.

Exercise. An one dimensional coalgebra is always spanned by an element g such that $\Delta(g) = g \otimes g$. Such an element is called group-like.

Irreducible coalgbras. C is said to be irreducible if any two non-zero subcoagebras have non-zero intersection.

Lemma 2.7. *C is irreducible if and only if it contains a unique simple subcoalgebra and this subcoalgebra is contained in any subcoalgebra.*

Proof. The intersection of subcoalgebras is again a subcoalgebra. If D and E are simple, their intersection has to be zero or they are equal. □

Theorem 2.8. *Let C be a coalgebra.*

(i) *Any irreducible subcoalgebra is contained in a maximal irreducible subcoalgebra.*
(ii) *If C is co-commutative then C is the direct sum of its maximal irreducible subcoalgebras.*
(iii) *Assume $f : C \longrightarrow D$ be a surjective map of co-commutative coalgebras. If C is irreducible then so is D.*

Proof. (i) is due to the fact that the sum of subcoalgebras is again a subcoalgebra.

(ii) Let C_α be a family of maximal irreducible subcoalgebra. We show the sum

$$\sum_\alpha C_\alpha$$

is direct. In fact, if the intersection of C_α with $\sum_{\alpha' \neq \alpha} C_{\alpha'}$ is non-zero, it has to contain the simple subcoalgebra of C_α, a contradiction.

Now, as C is co-commutative, for any $x \in C$, the dual of the subcoalgebra $C(x)$ generated by x is a finite dimensional commutative algebra, hence is a direct sum of local subalgebras. Each term in this decomposition is the dual of an irreducible subcoalgebra of $C(x)$. Thus $C(x)$, and hence x, is in the (direct) sum of irreducible maximal subcoalgebras of C.

(iii) The claim is "local" so we can assume that C and D are finite dimensional. Thus f is dual to the map

$$0 \longrightarrow D^* \xrightarrow{f^*} C^*,$$

where C^* is a local artinial ring. Hence so is D^*. $\square$

2.4. **The coradical filtration.** A coalgebra is called pointed if any simple subcoalgebra is one-dimensional (thus is spanned by a group-like element). For example, any co-commutative coalgebra over an algebraically closed field is pointed. We identify k with the one-dimensional subcoalgebra of C.

Let $\mathfrak{m} \subset C^*$ be orthogonal complement to the subcoalgebra $k \subset C$, it is the maximal ideal in C^*. For each $n \in \mathbb{N}$, set

$$C_n := (\mathfrak{m}^{n+1})^{\perp}$$

the orthogonal complement in C to $(\mathfrak{m}^{n+1})^{\perp}$. We have $C_0 = k$,

$$C_0 \subseteq C_1 \subseteq \dots$$

Lemma 2.9. (i) *C_i's are subcoalgebras in C.*
(ii) *$\varphi \cdot C_n \subset C_{n-1}$ for any $\varphi \in \mathfrak{m}$.*
(iii) *C_n is the set of elements $c \in C$ such that $\Delta(c)$ has rank at most $n+1$.*
(iv) *As as consequence we have*

$$C = \bigcup_i C_i.$$

Proof. (i) For any $\xi \in C^*$, $\varphi \in \mathfrak{m}^{n+1}$ and $c \in C_n$, we have

$$0 = (\xi \cdot \varphi)(c) = \sum_{(c)} \xi(c_{(1)})\varphi(c_{(2)}) = 0.$$

Hence $\Delta(c) \in C \otimes C_n$. Similarly, we have $\Delta(c) \in C_n \otimes C$. Thus

$$\Delta(C_n) \subset C_n \otimes C_n.$$

(ii) for $\varphi_1, \dots, \varphi_n \in \mathfrak{m}$, $c \in C_n$, we have

$$(\varphi_1 \cdot \ldots \cdot \varphi_n)(\varphi \cdot c) = (\varphi_1 \cdot \ldots \cdot \varphi_n \cdot \varphi)(c) = 0.$$

Thus $\varphi \cdot c \in C_{n-1}$.

As a consequence C_n is annihilated by $\mathfrak{m}^{n+1}$. Vice-verse, as

$$\varepsilon(\varphi \cdot c) = \varepsilon(c)$$

we conclude that C_n is the set of elements in C killed by $\mathfrak{m}^{n+1}$ through the dot-action.

(iii) This is true for $n = 0$ by assumption: if $\Delta(c) = a \otimes b$ then

$$c = \varepsilon(a)b = a\varepsilon(b).$$

Hence, after normalization we conclude that c is a group-like element.

Let c be such that $\Delta(c)$ has rank 2. Then $\Delta(c) - c \otimes 1$ has rank 1. Indeed, apply the form $\mathrm{id} \otimes \varepsilon$ on this tensor we get 0. Thus

$$\Delta(c) = a \otimes b + c \otimes 1.$$

We have the following equality for any $\varphi \in C^*$:

$$\Delta(\varphi \cdot c) = \Delta(\sum_{(c)} c_{(1)}\varphi(c_{(2)}) = \sum_{(c)} c_{(1)} \otimes c_{(2)}\varphi(c_{(3)}) = \sum_{(c)} c_{(1)} \otimes \varphi \cdot c_{(2)}. \tag{1}$$

For any $\varphi \in \mathfrak{m}$, we have $\varphi \cdot 1 = 0$, hence

$$\Delta(\varphi \cdot c) = a \otimes \varphi \cdot b.$$

Thus $\varphi \cdot c$ is a group-like element, whence $c \in C_2$.

The general induction step is similar. Assume $\Delta(c)$ has rank $n+1$. Then $\Delta(c) - c \otimes 1$ has rank n. Therefore, for any $\varphi \in \mathfrak{m}$, Equation (1) shows that $\varphi \cdot c$ has rank n. □

Lemma 2.10. *We have*

$$\Delta(C_n) \subset \sum_{i=0}^{n} C_i \otimes C_{n-i}.$$

Proof. Let $c \in C_n$, then $\varphi(c) = 0$ for any $\varphi \in \mathfrak{m}^{n+1}$. Thus, for each $i = 0, 1, \ldots, n+1$ and each pair $\xi \in \mathfrak{m}^i$, $d \in \mathfrak{m}^{n+1-i}$

$$0 = (\xi \cdot d)(c) = (\xi \otimes d)\Delta(c).$$

Thus

$$\Delta(C_n) \subset \left(\mathfrak{m}^i \otimes \mathfrak{m}^{n+1-i}\right)^{\perp} = C_{i-1} \otimes C + C \otimes C_{n-i}.$$

Now we use the following equality [Sw, 9.1.5] (note the shift on indices, $C_{-1} := 0$)

$$\bigcap_{i=-1}^{n} (C_i \otimes C + C \otimes C_{n-1-i}) = \sum_{i=0}^{n} C_i \otimes C_{n-i}$$

to conclude. □

3. Structure of co-commutative Hopf algebras

3.1. **The universal enveloping algebra of a Lie algebra.** Let L be a Lie algebra and let $\mathfrak{U}(L)$ be its universal enveloping algebra. Recall that $\mathfrak{U}(L)$ is an associative algebra equipped with a Lie algebra map $\iota : L \longrightarrow \mathfrak{U}(L)^L$ which satisfies the following universal property:

$$\begin{tikzcd} L \arrow[rr, "\iota"] \arrow[dr, "\forall\varphi \text{ Lie map}"'] & & \mathfrak{U}(L) \arrow[dl, "\exists! \psi \text{ algebra map}"] \\ & A & \end{tikzcd}$$

Or, formulated in terms of adjoin functors, $L \longmapsto \mathfrak{U}(L)$ is left adjoin to the functor $A \longmapsto A^L$ from the category of associative algebras to the category of Lie algebras:

$$\mathrm{Hom}_{\mathrm{Lie}}(L, A^L) \cong \mathrm{Hom}_{\mathrm{Alg}}(\mathfrak{U}(L), A).$$

There exists an explicit construction of $\mathfrak{U}(L)$:

$$\mathfrak{U}(L) = \mathbf{T}(L)/I,$$

where $\mathbf{T}(L)$ is the tensor algebra over L,

$$\mathbf{T}(L) = \bigoplus_{i=0}^{\infty} L^{\otimes i},$$

and I is the two-sided ideal generated by elements of the form

$$x \cdot y - y \cdot x - [x, y],$$

where $\cdot$ denotes the product on $\mathbf{T}(L)$ and $[-,-]$ denotes the Lie product on L. The canonical map $\iota : L \longrightarrow \mathfrak{U}(L)$ is given by $x \longmapsto x$.

As a vector space, $\mathfrak{U}(L)$ has a basis determined in terms of a basis L as follows.

Theorem 3.1 (Poincaré-Birkhoff-Witt)**.** *Fix an ordered basis $\{e_j, j \in J\}$ of L. Then monomials*

$$e_1^{r_1} e_2^{r_2} \dots e_k^{r_k}, \quad k, r_j \in \{\mathbb{N}, 0\}$$

form a k-basis for $\mathfrak{U}(L)$. In particular, the canonical map $\iota : L \longrightarrow \mathfrak{U}(L)$ is injective.

Proposition 3.2. *If L and L' are Lie algebras, there exists a natural component-wise Lie algebra structure on $L \oplus L'$. We have*

$$\mathfrak{U}(L \oplus L') \cong \mathfrak{U}(L) \otimes \mathfrak{U}(L').$$

Proof. This follows from the universal property of the enveloping algebra. We check that $\mathfrak{U}(L) \otimes \mathfrak{U}(L')$ is the universal enveloping of $L \oplus L'$ with the canonical map given by

$$(x, x') \mapsto x \otimes 1 + 1 \otimes x'.$$

□

Consider now the Lie map $L \longrightarrow L \oplus L$, $x \mapsto (x, x)$ (the diagonal map. It yields, by the universal property an algebra map

$$\Delta : \mathfrak{U}(L) \longrightarrow \mathfrak{U}(L) \otimes \mathfrak{U}(L'), \quad x \longmapsto x \otimes 1 + 1 \otimes x, \quad x \in L.$$

Then $\mathfrak{U}(L)$, equipped with Δ and the co-unit map $\varepsilon : \mathfrak{U}(L) \longrightarrow k$, $x \mapsto 0, x \in L$, is a bialgebra. It is indeed a Hopf algebra with the antipode given by

$$S(x) = -x, \quad x \in L.$$

Remark. The coalgebra structure on $\mathfrak{U}(L)$ does not depend on the Lie algebra structure on L. Further, the PBW theorem implies that, as coalgebra, $\mathfrak{U}(L)$ depends only on the vector space L.

3.2. **Structure of co-commutative Hopf algebras.** Recall that a coalgebra is pointed if its simple subcoalgebras are one-dimensional. Each such subalgebra is spanned by a group-like element.

Let now H be a Hopf algebra which is pointed co-commutative as a coalgebra. Denote the set of group-like elements in H by $\mathcal{G}(H)$. Then $\mathcal{G}(H)$ is a group. The associated group ring $k[\mathcal{G}(H)]$ is therefore a Hopf subalgebra of H.

On the other hand we have the decomposition of H into direct sum of maximal irreducible subcoalgebras, each contains a unique group-like element:

$$H = \bigoplus_{g\in\mathcal{G}(H)} H_g, \quad H_g \ni g. \tag{2}$$

Theorem 3.3. *Let H be a pointed co-commutative Hopf algebras. Then H is a semi-direct product of its Hopf subalgebra $k[\mathcal{G}(H)]$ and the Hopf subalgebra H_1 – the maximal irreducible subcoalgebra of H containing the unit element.*

Proof. (1) We first show that H_1 is a Hopf algebra. By definition it is a subcoalgebra. Consider the decompostion of $H \otimes H$:

$$H\otimes H = \bigoplus_{g,h\in\mathcal{G}(H)} H_g \otimes H_h.$$

As $m : H \otimes H \longrightarrow H$ is a coalgebra, by means of Theorem 2.8 (iii), the image of $H_1 \otimes H_1$ is in H_1. That is H_1 is a subalgebra.

As H is co-commutative, the antipode is a coalgebra map, by the same argument we conclude that $S(H_1) \subset H_1$. Thus H_1 is a Hopf subalgebra.

(2) We have, for a group-like element g and any element x

$$\Delta(gx) = \sum_{(x)} gx_{(1)} \otimes gx_{(2)}.$$

Therefore we have

$$gH_h \subset H_{gh}.$$

Thus $\mathcal{G}(H)$ acts on the components of the decomposition (2) by conjugation. □

In the next step we proceed to show that the Hopf algebra H_1 above, in the case $\mathrm{char}(k) = 0$, is the universal enveloping algebra of the Lie algebra of its primitive elements. We follow the proof of [Sw69, Chapt. XII], which is due to B. Kostant [AS09].

Proposition 3.4. *There exists for each vector space U a pointed irreducible co-commutative coalgebra $\mathcal{B}(U)$ together with canonical map $\pi : \mathcal{B}(U) \longrightarrow U$, such that, for any pointed irreducible co-commutative coalgebra, the natural map*

$$\begin{array}{ccc} \mathrm{Hom}_{coalg}(C, \mathcal{B}(U)) & \xrightarrow{\cong} & \mathrm{Hom}_k(C^+, U) \\ f & \longmapsto & \pi f \end{array}$$

is an isomorphism.

Proof. Indeed $\mathcal{B}(U)$ is a commutative, co-commutative graded bialgebra. If $U = U_1 \oplus U_2$ then $\mathcal{B}(U) \cong \mathcal{B}(U_1) \otimes \mathcal{B}(U_2)$ as graded bialgebras. Define $\mathcal{B}(U)$ to be the graded dual of the symmetric tensor algebra on U. In particular, the n-th coradical term of $\mathcal{B}(U)$ is

$$\mathcal{B}(U)_n \cong \left(\mathbf{S}(U^*)/U^{*\otimes n+1}\right)^*.$$

It is enough to check the universal property for finite dimensional coalgebras C. Then any map $C \longrightarrow \mathcal{B}(U)$ has image a finite subcoalgebra $\mathcal{B}(U)_n$. Now we have

$$\begin{aligned}
\mathrm{Hom}_{\mathrm{coalg}}(C, \mathcal{B}(U)) &\cong \varinjlim_n \mathrm{Hom}_{\mathrm{coalg}}(C, \mathcal{B}(U)_n) \\
&\cong \varinjlim_n \mathrm{Hom}_{\mathrm{alg}}\left(\left(\mathbf{S}(U^*)/U^{*\otimes n+1}\right)^*, C^*\right) \\
&\cong \mathrm{Hom}_{\mathrm{alg}}(\varprojlim_n \mathbf{S}(U^*)/U^{*\otimes n+1}, C^*) \\
&\cong \mathrm{Hom}_k(U^*, C^{+*}) \\
&\cong \mathrm{Hom}_k(C^+, U).
\end{aligned}$$

□

Remark. Let $\{f_i\}$ be a basis of U^*. Then $\mathbf{S}(U)$ has a basis

$$\left\{\mathbf{f}^{\mathbf{a}} := \prod f_i^{a_i}\right\}.$$

We denote by $\{\mathbf{e}_{\mathbf{a}}\}$ the dual basis to this basis in $\mathcal{B}(U)$. Then we have the coproduct on $\mathcal{B}(U)$ given as follows:

$$\Delta \mathbf{e}_{\mathbf{a}} = \sum_{\mathbf{b}+\mathbf{c}=\mathbf{a}} \mathbf{e}_{\mathbf{b}} \otimes \mathbf{e}_{\mathbf{c}},$$

and the product on $\mathcal{B}(U)$ is given by

$$\mathbf{e}_{\mathbf{a}} \cdot \mathbf{e}_{\mathbf{b}} = \binom{\mathbf{a}+\mathbf{b}}{\mathbf{a}} \mathbf{e}_{\mathbf{a}+\mathbf{b}}. \tag{3}$$

Proposition 3.5. *Let C be a pointed irreducible co-commutative coalgebra. Let $F : \mathcal{B}(U) \longrightarrow C$ be a coalgebra map. Then F is injective (resp. surjective) iff $F : U \longrightarrow \mathcal{P}(C)$ is injective (resp. surjective).*

Proof. (i) Assume that the restriction of F to U is injective. We show it is injective by induction on the coradical filtration. Let $x \in \mathcal{B}(U)^+_{n+1} := \mathcal{B}(U)_{n+1} \cap \mathcal{B}(U)^+$. We have

$$\Delta(x) - 1 \otimes x - x \otimes 1 \in (\mathcal{B}(U)_n \otimes \mathcal{B}(U)_n) \bigcap \left(\mathcal{B}(U)^+ \otimes \mathcal{B}(U)^+\right).$$

Thus

$$\Delta(x) - g \otimes x - x \otimes g = y \in \mathcal{B}(U)^+_n \otimes \mathcal{B}(U)^+_n.$$

Thus, if $F(x) = 0$ then $(F \otimes F)(y) = 0$, by induction this implies $y = 0$. This means $x \in \mathcal{B}(U)^+_1 = U$, thus $x = 0$.

Assume that $F : U \longrightarrow \mathcal{P}(C)$ is surjective. Let $G : \mathcal{P}(C) \longrightarrow U$ be a section to F. It induces a map, also denoted by G from $C \longrightarrow \mathcal{B}(U)$ which is injective by the above discussion. Consider the diagram

$$\begin{tikzcd} U \arrow[r, "F"] \arrow[d] & \mathcal{P}(C) \arrow[r, "G"] \arrow[d] & U \arrow[d] \\ \mathcal{U}(U) \arrow[r, "F"'] & C \arrow[r, "G"'] & \mathcal{B}(U). \end{tikzcd}$$

By assumption, $GF : U \longrightarrow U$ is the identity map, hence it is the identity map on $\mathcal{B}(U)$. A G is injective, this forces F surjective. $\square$

In this subsection k is a field of characteristic 0.

Theorem 3.6 (Cartier (cf. [Sw69, Theorem 13.0.1], [Ca, 3.8])). *Let H be a pointed irreducible co-commutative Hopf algebra. Assume that k has characteristic 0. Then H is isomorphic as as Hopf algebra to the universal enveloping of the Lie algebra of its primitive elements:*

$$\mathfrak{U}(\mathcal{P}(H)) \cong H.$$

Proof. Let denote $L := \mathcal{P}(H)$. We shall exhibit isomorphisms of coalgebras from $\mathcal{B}(L)$ to H and to $\mathfrak{U}(L)$ which are compatible with the canonical map $\mathfrak{U}(\mathfrak{P}(H)) \longrightarrow H$.

Fix a basis $\{e_i\}$ of L. According to the product rule on $\mathcal{B}(H)$ given in (3) define the map $e_H : \mathcal{B}(L) \longrightarrow H$ sending $\mathbf{e_a}$ to $\mathbf{e^a}/\mathbf{a}!$. One checks that it is bialgebra map, hence an isomorphism as it is bijective on the subspace L. The same applies to a similar map $e_{\mathfrak{U}} : \mathcal{B}(L) \longrightarrow \mathfrak{U}(L)$. But it is obvious that these to maps agree with the canonical map $\mathfrak{U}(\mathfrak{P}(H)) \longrightarrow H$. Hence the latter is an isomorphism. $\square$

References

[AS09] N. Andruskiewitsch, W. Ferrer Santos, *The beginnings of the theory of Hopf algebras*, Acta Appl. Math. 108 (2009), no. 1, 3–17.

[Ca] P. Cartier, *A primer of Hopf Algebras.*

[Di73] J. Dieudonné, *Introduction to the theory of formal groups*, Pure Appl. Math., 20, Marcel Dekker, Inc., New York, 1973, xii+265 pp.

[MM65] J.W. Milnor and J.C. Moore, *On the structure of Hopf algebras*, Ann. of Math. 81 (1965), 211-264.

[Hu75] J. Humphreys, *Linear algebraic groups*, Springer 21, 1975.

[Sw69] M. Sweedler, *Hopf algebras*, Benjamin 1969.

[Wa79] W.C. Waterhouse, Introduction to Affine Group Schemes, Lecture Notes in Mathematics,

E-mail address: phung@math.ac.vn

Institute of Mathematics