POLYNOMIAL IDENTITIES OF HOPF ALGEBRAS

MIKHAIL V. KOTCHETOV

Your file Votre référence
ISBN: 0-612-84066-2
Our file Notre référence
ISBN: 0-612-84066-2

Polynomial Identities of Hopf Algebras

by

© Mikhail V. Kotchetov

A thesis submitted to the School of Graduate Studies in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Department of Mathematics and Statistics
Memorial University of Newfoundland

September 2002

St.John's Newfoundland Canada

Abstract

In this dissertation we consider Hopf algebras that satisfy a polynomial identity as algebras or coalgebras. The notion of a polynomial identity for an algebra is classical. The dual notion of an identity for a coalgebra is new.

In Chapter 0 we give basic definitions and facts that are used throughout the rest of this work.

Chapter 1 is devoted to coalgebras with a polynomial identity. First we introduce the notion of identity of a coalgebra and discuss its general properties. Then we study what classes of coalgebras are varieties, i.e. can be defined by a set of identities. In the case of algebras, varieties are characterized by the classical Theorem of Birkhoff. Somewhat unexpectedly, the dual statement for coalgebras does not hold. Further, we give two realizations of a relatively (co)free coalgebra of a variety: one via the so called finite dual of a relatively free algebra and the other a direct construction using some kind of symmetric functions.

In Chapter 2 we give necessary and sufficient conditions for a cocommutative Hopf algebra (with additional restrictions in the case of prime characteristic) to satisfy a polynomial identity as an algebra. These results generalize the well-known Passman's Theorem on group algebras with a polynomial identity and Bahturin-Latyšev's Theorem on universal enveloping algebras with a polynomial identity. The proofs for the case of prime characteristic are given in Chapter 4.

In Chapter 3 we dualize the results of Chapter 2 to obtain some criteria for a commutative Hopf algebra (assumed reduced in the case of prime characteristic) to satisfy an identity as a coalgebra. We also extend our result in charecteristic zero to a certain class of nearly commutative Hopf algebras (pseudoinvolutive Hopf algebras of Etingof-Gelaki).

Finally, in Chapter 4 we use the interpretation of cocommutative Hopf algebras as formal groups to prove the results of Chapter 2. Our method also demonstrates that Bahturin-Latyšev's Theorem in characteristic zero is in fact a corollary of Passman's Theorem.

For the most part, this dissertation is based on my papers [19], [20], and [21].

Acknowledgements

First of all, I would like to thank my supervisor Prof. Yuri A. Bahturin for his guidance during my studies at both Moscow State University and Memorial University of Newfoundland. Without his advice, encouragement, and financial support this dissertation would not have been written. I am grateful to the Faculty of Mechanics and Mathematics of Moscow State University for my mathematical education. I also thank the Department of Mathematics and Statistics of Memorial University for providing a friendly atmosphere and facilities for my Ph.D. programme. In particular, I would like to thank Drs. E. Goodaire and H. Gaskill for their kind concern about my life and career. I am also grateful to Dr. V. Petrogradsky for useful discussions. I acknowledge the financial support of the School of Graduate Studies during my years at Memorial University. Finally, I thank my parents and friends for their invaluable moral support.

Contents

Definitions and Basic Facts

Throughout $\Bbbk$ will denote the ground field. All vector spaces, algebras, tensor products, etc. will be considered over $\Bbbk$ unless stated otherwise. $\bar{\Bbbk}$ will denote the algebraic closure of $\Bbbk$.

All algebras will be assumed associative and unital, and algebra maps $A_1 \to A_2$ will be required to send the unit element of A_1 to the unit element of A_2. In particular, a subalgebra of A must contain the unit element of A.

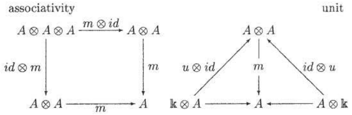
$\mathbb{Z}$ will denote the set of integers and $\mathbb{N}$ the set of positive integers.

0.1 Coalgebras and Comodules

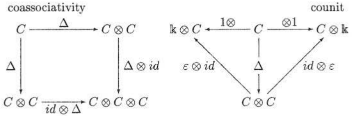
In this and the following section we refer to the excellent monograph of S.Montgomery [25] for the basic properties of coalgebras and Hopf algebras. See the bibliography of [25] for the references to original papers.

The notion of a coalgebra is the dual of the notion of an algebra. We first express the associativity and unit axioms via commutative diagrams so that we can dualize them.

Definition 0.1.1. A $\Bbbk$-*algebra* is a $\Bbbk$-vector space A together with two $\Bbbk$-linear maps, multiplication $m : A \otimes A \to A$ and unit $u : \Bbbk \to A$, such that the following diagrams are commutative:



Definition 0.1.2. A $\Bbbk$-*coalgebra* is a $\Bbbk$-vector space C together with two $\Bbbk$-linear maps, comultiplication $\Delta : C \to C \otimes C$ and counit $\varepsilon : C \to \Bbbk$, such that the following diagrams are commutative:



We say C is *cocommutative* if Δc is a symmetric tensor for any $c \in C$. A subspace $D \subset C$ is a *subcoalgebra* if $\Delta D \subset D \otimes D$.

Definition 0.1.3. Let C and D be coalgebras, with comultiplications Δ_C and Δ_D, and counits ε_C and ε_D, respectively. A linear map $f : C \to D$ is a *homomorphism of coalgebras* if $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$ and $\varepsilon_C = \varepsilon_D \circ f$. A subspace $I \subset C$ is a *coideal* if $\Delta I \subset I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.

It is easy to check that if I is a coideal, then the space C/I is a coalgebra with comultiplication induced from Δ, and conversely.

We will now see that there is a very close relationship between algebras and coalgebras, by looking at their dual spaces. If V is a vector space, we will often use the symmetric notation $\langle f, v\rangle$ instead of $f(v)$, for $v \in V$ and $f \in V^*$.

If C is a coalgebra, then C^* is an algebra, with multiplication $m = \Delta^*$ and unit $u = \varepsilon^*$. If C is cocommutative, then C^* is commutative.

However, if we begin with an algebra A, then difficulties arise. For, if A is not finite-dimensional, the image of $m^* : A^* \to (A \otimes A)^*$ does not have to be a subspace of $A^* \otimes A^*$. The largest subspace of A^* whose image lies in $A^* \otimes A^*$, is the so called *finite dual*:

$$A^\circ = \{f \in A^* \mid f(I) = 0 \text{ for some ideal } I \triangleleft A,\ \dim A/I < \infty\}.$$

A° is a coalgebra with comultiplication $\Delta = m^*$ and counit $\varepsilon = u^*$ (restricted to A°). If A is commutative, then A° is cocommutative.

Moreover, the functor $(\ )^\circ$ is the right adjoint of $(\ )^*$, i.e. for any algebra A and coalgebra C, the sets of homomorphisms $\mathrm{Alg}(A, C^*)$ and $\mathrm{Coalg}(C, A^\circ)$ are in a one-to-one correspondence (see Lemma 1.3.12).

Unfortunately, A° may happen to be too small (even zero). The following condition on A is precisely what we need to guarantee that A° is big enough to separate the elements of A (in other words, A° is dense in A^* in the sense of Definition 0.4.1).

Definition 0.1.4. An algebra A is called *residually finite-dimensional* if its ideals of finite codimension (i.e. $I \triangleleft A$ with $\dim A/I < \infty$) intersect to 0 or, equivalently, for any $0 \neq a \in A$, there exists a finite-dimensional representation φ of A such that $\varphi(a) \neq 0$.

The relationship between subcoalgebras, coideals, ideals, and subalgebras is the following.

Lemma 0.1.5. *1) Let C be a coalgebra.*

(a) A subspace $D \subset C$ is a subcoalgebra iff $D^{\perp} = \{f \in C^* \mid \langle f, D\rangle = 0\}$ is an ideal of C^*.

(b) A subspace $I \subset C$ is a coideal iff $I^{\perp} = \{f \in C^* \mid \langle f, I\rangle = 0\}$ is a subalgebra of C^*.

2) Let A be an algebra.

(a) If $B \subset A$ is a subalgebra, then $B^{\perp} = \{f \in A^{\circ} \mid \langle f, B\rangle = 0\}$ is a coideal of A°.

(b) If $I \subset A$ is an ideal, then $I^{\perp} = \{f \in A^{\circ} \mid \langle f, I\rangle = 0\}$ is a subcoalgebra of A°. ■

Now we introduce the so called *sigma notation* as follows. Let C be any coalgebra with comultiplication $\Delta : C \to C \otimes C$. For any $c \in C$, we write:

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

The subscripts (1) and (2) are symbolic, and do not indicate particular elements of C.

In sigma notation, the coassociativity means that

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

so we simply write $\sum c_{(1)} \otimes c_{(2)} \otimes c_{(3)} = \Delta_3 c$. Iterating this procedure gives, for any $n \geq 2$,

$$\Delta_n c = \sum c_{(1)} \otimes \ldots \otimes c_{(n)},$$

where $\Delta_2 = \Delta$. We will sometimes use the convention that $\Delta_1 = id_C$ and $\Delta_0 = \varepsilon$.

Now we dualize the notion of a (unital) module by first writing its definition in terms of commutative diagrams.

Definition 0.1.6. For a $\Bbbk$-algebra A, a (left) *A-module* is a $\Bbbk$-space M with a $\Bbbk$-linear map $\gamma : A \otimes M \to M$ such that the following diagrams commute:

$$\begin{array}{ccc} A \otimes A \otimes M & \xrightarrow{m \otimes id} & A \otimes M \\ {\scriptstyle id \otimes \gamma}\downarrow & & \downarrow{\scriptstyle \gamma} \\ A \otimes M & \xrightarrow[\gamma]{} & M \end{array} \qquad \begin{array}{ccc} \Bbbk \otimes M & \xrightarrow{u \otimes id} & A \otimes M \\ & \searrow^{\text{scalar mult.}} & \downarrow{\scriptstyle \gamma} \\ & & M \end{array}$$

Definition 0.1.7. For a $\Bbbk$-coalgebra C, a (right) *C-comodule* is a $\Bbbk$-space M with a $\Bbbk$-linear map $\rho : M \to M \otimes C$ such that the following diagrams commute:

$$\begin{array}{ccc} M & \xrightarrow{\rho} & M \otimes C \\ {\scriptstyle \rho}\downarrow & & \downarrow{\scriptstyle id \otimes \Delta} \\ M \otimes C & \xrightarrow[\rho \otimes id]{} & M \otimes C \otimes C \end{array} \qquad \begin{array}{ccc} M & \xrightarrow{\rho} & M \otimes C \\ & \searrow^{\otimes 1} & \downarrow{\scriptstyle id \otimes \varepsilon} \\ & & M \otimes \Bbbk \end{array}$$

A linear map $f : M \to N$ is a *homomorphism of (right) comodules* if it preserves ρ:

$$\rho_N(f(m)) = (f \otimes id)\rho_M(m), \qquad \forall m \in M.$$

A subspace $N \subset M$ is a *subcomodule* if $\rho(N) \subset N \otimes C$.

There is also sigma notation for right comodules: we write

$$\rho(m) = \sum m_{(0)} \otimes m_{(1)} \in M \otimes C.$$

Analogously, one has left comodules, via a map $\rho' : M \to C \otimes M$, and we use the notation

$$\rho'(m) = \sum m_{(-1)} \otimes m_{(0)} \in C \otimes M,$$

so that for both right and left comodules we have $m_0 \in M$ and $m_{(i)} \in C$ for $i \neq 0$.

The following Finiteness Theorem [25, Theorem 5.1.1] points out the main feature that distinguishes coalgebras and comodules from algebras and modules.

Theorem 0.1.8. *Let C be a coalgebra.*

1) Any C-comodule M is locally finite in the sense that any finite subset of M is contained in a finite-dimensional subcomodule.

2) Any finite subset of C is contained in a finite-dimensional subcoalgebra.

∎

A nonzero coalgebra is called *simple* if it does not have proper nonzero subcoalgebras. The theorem above implies that all simple coalgebras are *finite-dimensional*. It also implies that any nonzero coalgebra has a simple subcoalgebra.

Definition 0.1.9. Let C be a coalgebra.

1) The *coradical* corad$C$ of C is the sum of all simple subcoalgebras of C.

2) C is *cosemisimple* if corad$C = C$.

3) C is *irreducible* if corad$C$ is simple or, equivalently, if C contains only one simple subcoalgebra. Any maximal irreducible subcoalgebra of C is called an *irreducible component.*

4) C is *pointed* if every simple subcoalgebra is one-dimensional.

5) C is *connected* if corad$C$ is one-dimensional.

If D is a simple cocommutative coalgebra, then D^* is a simple (finite-dimensional) commutative algebra. It follows that any cocommutative coalgebra C over an algebraically closed field is pointed. A one-dimensional subcoalgebra $D \subset C$ is necessarily of the form $\Bbbk g$, where $g \in C$ is *group-like*: $g \neq 0$ and $\Delta g = g \otimes g$. Distinct group-like elements of C are linearly independent, the set of all group-like elements is denoted $G(C)$.

Let us now quote for future reference the basic properties of irreducible components [25, Lemma 5.6.2 and Theorem 5.6.3].

Lemma 0.1.10. *Let C be a coalgebra.*

1) Any irreducible subcoalgebra of C is contained in a unique irreducible component.

2) A sum of distinct irreducible components is direct.

3) If C is cocommutative, then C is the direct sum of its irreducible components. ■

In fact, the coradical corad$C$ is the bottom piece of the so called *coradical filtration* of C. We set $C_0 = $ corad$C$ and for each integer $n > 0$ define inductively:

$$C_n = \Delta^{-1}(C \otimes C_{n-1} + C_0 \otimes C).$$

Then it turns out (see [25, Theorem 5.2.2]) that $\{C_n\}$ is a *coalgebra filtration* in the following sense:

$$\Delta C_n \subset \sum_{k=0}^{n} C_k \otimes C_{n-k},$$
$$C_n \subset C_{n+1}, \text{ and } C = \bigcup_{n\geq 0} C_n.$$

The conditions above guarantee that the space $C^{\mathrm{gr}} = \bigoplus_{n\geq 0} C_n/C_{n-1}$ (with C_{-1}=0) has a natural coalgebra structure.

Example 0.1.11. If C is a connected coalgebra, then C_0 is one-dimensional. It is spanned by a group-like element that we will denote by 1 (although there is no multiplication yet). Let $P(C)$ be the set of all *primitive* elements of C: $x \in C$ such that $\Delta x = x \otimes 1 + 1 \otimes x$. Then $P(C)$ is a subspace and $C_1 = \Bbbk 1 \oplus P(C)$ [25, Lemma 5.3.2].

The following lemma [25, Lemma 5.3.4] shows that $\mathrm{corad} C$ is the smallest piece a coalgebra filtration can start with.

Lemma 0.1.12. *Let C be any colagebra and $\{B_n\}_{n\geq 0}$ a coalgebra filtration of C. Then $B_0 \supset \mathrm{corad} C$.* ■

Corollary 0.1.13. *If $f : C \to D$ is a surjective coalgebra map, then $f(\mathrm{corad} C) \supset \mathrm{corad} D$.* ■

We conclude this section with another fundamental property of the coradical filtration [25, Theorem 5.3.1].

Theorem 0.1.14. *Let C and D be coalgebras and $f : C \to D$ a coalgebra map. If $f|_{C_1}$ is injective, then f is injective.* ■

Corollary 0.1.15. *If C is connected and $f : C \to D$ is a coalgebra map such that $f|_{P(C)}$ is injective, then f is injective.* ■

0.2 Bialgebras and Hopf Algebras

We now combine the notions of algebra and coalgebra.

Definition 0.2.1. A $\Bbbk$-space B is a *bialgebra* if (B, m, u) is an algebra, (B, Δ, ε) is a coalgebra, and either of the following equivalent conditions holds: Δ and ε are algebra morphisms or m and u are coalgebra morphisms.

Naturally, a *bialgebra homomorphism* is a map which is both an algebra and a coalgebra homomorphism, and a subspace $D \subset B$ is a *subbialgebra* if it is both a subalgebra and a subcoalgebra. Similarly, a subspace $I \subset B$ is a *biideal* if it is both an ideal and a coideal. The quotient B/I is a bialgebra precisely when I is a biideal of B.

The last ingredient we need to define Hopf algebras is the *convolution product.* Namely, if C is a coalgebra and A is an algebra, then $\mathrm{Hom}_{\Bbbk}(C, A)$ becomes an (associative) algebra under the convolution:

$$(f * g)(c) = (m_A \circ (f \otimes g) \circ \Delta_C)c = \sum f(c_{(1)})g(c_{(2)}),$$

for all $f, g \in \mathrm{Hom}_{\Bbbk}(C, A)$, $c \in C$. The unit element of $\mathrm{Hom}_{\Bbbk}(C, A)$ is $u_A \circ \varepsilon_C$.

Remark 0.2.2. Note that the multiplication on C^* defined earlier is the same as the convolution product on $\mathrm{Hom}_{\Bbbk}(C, \Bbbk) = C^*$.

Definition 0.2.3. Let $(H, m, u, \Delta, \varepsilon)$ be a bialgebra. Then H is a *Hopf algebra* if there exists an element $S \in \mathrm{Hom}(H, H)$ which is an inverse to id_H

under convolution, i.e.

$$\sum S(h_{(1)})h_{(2)} = \varepsilon(h)1_H = \sum h_{(1)}S(h_{(2)}), \qquad \forall h \in H.$$

Obviously, if such S exists, it is unique. S is called the *antipode* of H.

Naturally, a linear map $f : H \to K$ of Hopf algebras is a *Hopf homomorphism* if it is a bialgebra homomorphism and $f(S_H h) = S_K f(h)$, for all $h \in H$. A subspace $D \subset H$ is a *subHopfalgebra* if it is a subbialgebra and $SD \subset D$. From the uniqueness of S it follows that if $D \subset H$ is a subbialgebra that has its own antipode S_D, then D is in fact a subHopfalgebra and $S_D = S|_D$. A subspace $I \subset H$ is a *Hopf ideal* if it is a biideal and $SI \subset I$, in this situation H/I is a Hopf algebra with the structure induced from H. The largest Hopf ideal is the *augmentation ideal* $H^+ = \operatorname{Ker}\varepsilon$.

Let us note that the antipode is necessarily an anti-algebra morphism, i.e.

$$\begin{aligned} S(1) &= 1, \\ S(gh) &= S(h)S(g), \qquad \forall g, h \in H, \end{aligned}$$

and anti-coalgebra morphism, i.e.

$$\begin{aligned} \varepsilon(Sh) &= \varepsilon(h), \\ \sum (Sh)_{(1)} \otimes (Sh)_{(2)} &= \sum S(h_{(2)}) \otimes S(h_{(1)}), \qquad \forall h \in H. \end{aligned}$$

If H is commutative or cocommutative, then $S^2 = id$. In general, S does not even have to be injective or surjective.

The basic examples of Hopf algebras are the following.

1) The group algebra $\Bbbk G$ of any group G, with $\Delta g = g \otimes g$, $\varepsilon(g) = 1$, $Sg = g^{-1}$ for all $g \in G$.

2) The universal enveloping algebra $U(L)$ of any Lie algebra L, with $\Delta x = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$, $Sx = -x$, for all $x \in L$.

3) The algebra of regular functions $\mathcal{O}(G)$ on any affine algebraic group G, with $\Delta : \mathcal{O}(G) \to \mathcal{O}(G \times G) = \mathcal{O}(G) \otimes \mathcal{O}(G)$ corresponding to the group multiplication $G \times G \to G$: $(\Delta f)(x, y) = f(xy)$, $\varepsilon(f) = f(e)$, $(Sf)(x) = f(x^{-1})$, for all $f \in \mathcal{O}(G)$, $x, y \in G$.

The former two Hopf algebras are cocommutative, the latter is commutative. For any Hopf algebra H, the set $G(H)$ of all group-like elements is in fact a group (under the multiplication of H), so H contains the group algebra $\Bbbk G(H)$ (of course, $G(H)$ may consist only of the unit element). The set $P(H)$ of all primitive elements of H forms a Lie algebra under the commutator $[x, y] = xy - yx$.

The axioms of a bialgebra (or Hopf algebra) are self-dual. So it is not surprising that if $(H, m, u, \Delta, \varepsilon)$ is a bialgebra, then $(H^\circ, \Delta^*, \varepsilon^*, m^*, u^*)$ is also a bialgebra, and if H is a Hopf algebra with antipode S, then H° is a Hopf algebra with antipode S^* [25, Theorem 9.1.3]. We have to use the finite dual H° here rather than the whole H^*, because comultiplication is not defined on H^*.

Given a bialgebra H and a vector space V, we can turn V into a "trivial" (left) H-module by setting for all $h \in H$, $v \in V$,

$$h \cdot v = \varepsilon(h)v. \tag{0.2.1}$$

We can also turn V into a "trivial" (right) H-comodule by setting for all $v \in V$,

$$\rho(v) = v \otimes 1. \tag{0.2.2}$$

Now if V is any left H-module, the elements $v \in V$ that satisfy (0.2.1), for all $h \in H$, are called *invariants*. Of course, a similar definition can be given for right modules. The set of all invariants is denoted by ${}^{H}V$ for a left module V and V^H for a right module.

If V is a right H-comodule, the elements $v \in V$ that satisfy (0.2.2) are called *coinvariants*. The set of all coinvariants is denoted by V^{coH} for right comodules and ${}^{coH}V$ for left comodules.

For any Hopf algebra H, the following actions and coactions of H on itself are defined:

1) The left adjoint action: $(ad_l h)(k) = \sum h_{(1)} k (S h_{(2)})$, for all $h, k \in H$,

2) The right adjoint action: $(ad_r h)(k) = \sum (S h_{(1)}) k h_{(2)}$, for all $h, k \in H$,

3) The left adjoint coaction: $\rho_l : H \to H \otimes H : h \to \sum h_{(1)} S h_{(3)} \otimes h_{(2)}$,

4) The right adjoint coaction: $\rho_r : H \to H \otimes H : h \to \sum h_{(2)} \otimes (S h_{(1)}) h_{(3)}$.

Definition 0.2.4. A subHopfalgebra $K \subset H$ is called *normal* if

$$(ad_l H)K \subset K \text{ and } (ad_r H)K \subset K.$$

A Hopf ideal $I \subset H$ is called *normal* if

$$\rho_l(I) \subset H \otimes I \text{ and } \rho_r(I) \subset I \otimes H.$$

Obviously, all subHopfalgebras are normal for a commutative H, and all Hopf ideals are normal for a cocommutative H.

There is a natural correspondence between normal subHopfalgebras and normal Hopf ideals of H as follows. If $K \subset H$ is a normal subHopfalgebra, then $HK^+ = K^+H$ is a normal Hopf ideal. Conversely, if $I \subset H$ is a Hopf ideal, then we can consider H as a right H/I-comodule via

$$H \to H \otimes H/I : h \to \sum h_{(1)} \otimes (h_{(2)} + I),$$

and similarly on the left. Thus we can define the spaces of right and left H/I-coinvariants in H: $H^{coH/I}$ and ${}^{coH/I}H$. If I is a normal Hopf ideal, then ${}^{coH/I}H = H^{coH/I}$ is a normal subHopfalgebra. It is known that these two mappings are inverse bijections in the case when H is finite-dimensional or commutative or with cocommutative coradical (see [25, Section 3.4]).

Definition 0.2.5. Let A be an algebra and H a Hopf algebra.

1) A is a (left) *H-module algebra* if it is a (left) H-module such that

$$\begin{aligned} h \cdot 1 &= \varepsilon(h)1 \qquad \text{and} \\ h \cdot (ab) &= \sum (h_{(1)} \cdot a)(h_{(2)} \cdot b), \qquad \forall h \in H,\ a, b \in A. \end{aligned}$$

2) A is a (right) *H-comodule algebra* if it is a (right) H-comodule via $\rho : A \to A \otimes H$ such that

$$\begin{aligned} \rho(1) &= 1 \otimes 1 \qquad \text{and} \\ \rho(ab) &= \sum a_{(0)}b_{(0)} \otimes a_{(1)}b_{(1)}, \qquad \forall a, b \in A. \end{aligned}$$

It is straightforward to verify that the adjoint action and coaction of H on itself satisfy the above conditions.

We will need one more concept from general Hopf algebra theory, namely that of a crossed product.

Definition 0.2.6. Let H be a Hopf algebra and A an algebra. Assume that H *measures* A, i.e. there is a linear map $H \otimes A \to A : h \otimes a \to h \cdot a$ such that $h \cdot 1 = \varepsilon(h)1$ and $h \cdot (ab) = \sum(h_{(1)} \cdot a)(h_{(2)} \cdot b)$, for all $h \in H$, $a, b \in A$. Assume also that $\sigma : H \otimes H \to A$ is a convolution-invertible map. The *crossed product* $A\#_\sigma H$ is $A \otimes H$ as a vector space, with multiplication

$$(a\#h)(b\#k) = \sum a(h_{(1)} \cdot b)\sigma(h_{(2)}, k_{(1)})\#h_{(3)}k_{(2)},$$

for all $h, k \in H$, $a, b \in A$, and we have written $a\#h$ for the tensor $a \otimes h$.

It is straightforward to derive the conditions on $\cdot$ and σ so that $A\#_\sigma H$ will be an associative algebra with the unit $1\#1$ [25, Section 7.1]:

1) A is a twisted H-module, i.e. $1 \cdot a = a$ and

$$h \cdot (k \cdot a) = \sum \sigma(h_{(1)}, k_{(1)})[(h_{(2)}k_{(2)}) \cdot a]\sigma(h_{(3)}, k_{(3)}),$$

for all $h, k \in H$, $a \in A$,

2) σ is a (left) 2-cocycle, i.e. $\sigma(h, 1) = \sigma(1, h) = \varepsilon(h)1$ and

$$\sum[h_1 \cdot \sigma(k_{(1)}, m_{(1)})]\sigma(h_{(2)}, k_{(2)}m_{(2)}) = \sum \sigma(h_{(1)}, k_{(1)})\sigma(h_{(2)}k_{(2)}, m), \tag{0.2.3}$$

for all $h, k, m \in H$.

Note that if H is cocommutative and A commutative (or σ has values in the centre of A), then A is simply an H-module algebra. Another special case arises if we assume σ trivial: $\sigma(h, k) = \varepsilon(h)\varepsilon(k)1$, for all $h, k \in H$. Then again A is an H-module algebra, and the crossed product $A\#_\sigma H$ with such a σ is called the *smash product* and denoted simply $A\#H$.

The following decomposition theorem for cocommutative pointed Hopf algebras is due to Kostant, Cartier, Gabriel, et al. and can be found in [25, Section 5.6].

Theorem 0.2.7. *Let H be a pointed cocommutative Hopf algebra over $\Bbbk$. Let $G = G(H)$ be the group of group-like elements of H and H_1 the irreducible component of the simple subcoalgebra $\Bbbk 1$. Then G acts on H_1 by conjugation (which is the left adjoint action in this case) and H is isomorphic to the smash product $H_1 \# \Bbbk G$ via $h \# g \to hg$. Moreover, if $\operatorname{char} \Bbbk = 0$, then $H_1 \cong U(L)$, where $L = P(H)$ is the Lie algebra of primitive elements.* ■

Thus any pointed cocommutative Hopf algebra can be represented as a smash product of a connected Hopf algebra and a group algebra, the former being just the universal envelope of a Lie algebra in the case of characteristic 0.

Remark 0.2.8. The proof of the first statement of Theorem 0.2.7 given in [25, Section 5.6] does not require that H be cocommutative. It is sufficient to assume that H is the sum of its irreducible components (this condition is satisfied by any cocommutative Hopf algebra by Lemma 0.1.10).

We conclude this section by demonstrating the structure of H-comodules in the case $H = \Bbbk G$ for some group G. It is easy to see that, for any (right) $\Bbbk G$-comodule V, we have

$$V = \bigoplus_{g \in G} V_g, \text{ where } V_g = \{v \in V \mid \rho(v) = v \otimes g\},$$

so V is a G-graded space. Conversely, any G-graded vector space can be turned into a $\Bbbk G$-comodule by setting $\rho(v) = v \otimes g$ for any homogeneous

v of degree g. Moreover, $\Bbbk G$-comodule algebras are equivalent to G-graded algebras in this way.

0.3 Polynomial Identities

Definition 0.3.1. Let A be an algebra over a field $\Bbbk$ (although most of the definitions and results of this section are still valid if $\Bbbk$ is a commutative ring with 1). Let $F(X_1, \ldots, X_n)$ be a polynomial in n noncommuting variables with coefficients in $\Bbbk$. We say that A satisfies the identity $F = 0$ (or just F) if

$$F(a_1, \ldots, a_n) = 0, \qquad \forall a_1, \ldots, a_n \in A.$$

An algebra A is called PI if it satisfies the identity $F = 0$ for some nonzero polynomial F.

Because of the following theorem, multihomogeneous (i.e. homogeneous in each variable), and especially multilinear (i.e. linear in each variable), identities play a prominent role in the theory of polynomial identities. The proof of 1) is an easy exercise with Vandermonde's determinant, for 2) see e.g. [18, Section 1.3].

Theorem 0.3.2. *Let A be an algebra over a field $\Bbbk$ and F a polynomial in noncommuting variables that is an identity for A.*

1) *If $\Bbbk$ is infinite, then every multihomogeneous component of F is an identity for A.*

2) *The algebra A satisfies a multilinear identity of degree $\leq \deg F$. Moreover, if $\Bbbk$ is a field of characteristic 0, then F is equivalent to a (finite)*

system $\{F_i\}$ of multilinear identities, i.e. any algebra that satisfies F must also satisfy all F_i and vice versa. ■

Corollary 0.3.3. *If an algebra A with 1 over an infinite field satisfies an identity that does not follow from the commutativity $X_1X_2 - X_2X_1$, then $A = 0$.* ■

The *standard polynomial* of degree n is defined by

$$s_n(X_1, \ldots, X_n) = \sum_{\pi \in S_n} (-1)^\pi X_{\pi(1)} \ldots X_{\pi(n)},$$

where S_n is the group of permutations and $(-1)^\pi$ is the sign of π. In particular, $s_2 = X_1X_2 - X_2X_1$.

Since s_n is multilinear and alternating (i.e. vanishes upon any substitution $X_i = X_j$ for $i \neq j$), any finite-dimensional algebra A will satisfy the *standard identity* $s_n = 0$, for any $n > \dim A$. For example, the algebra $M_n(\Bbbk)$ of $n \times n$ matrices satisfies s_{n^2+1}. This can be improved, as stated by the following classical Theorem of Amitsur-Kaplansky-Levitzki.

Theorem 0.3.4. *The matrix algebra $M_n(\Bbbk)$ satisfies the standard identity $s_{2n} = 0$. It does not satisfy any nontrivial identity of degree $< 2n$.* ■

Finally, it is obvious that if an algebra A satisfies a multihomogeneous identity F, and B is any commutative algebra, then $A \otimes B$ satisfies F. In particular, $M_n(B)$ satisfies s_{2n}, for any commutative algebra B. It also follows that if A is PI and B is commutative, then $A \otimes B$ is PI. The classical Theorem of A.Regev generalizes this simple observation: if A and B are PI, then $A \otimes B$ is PI (see e.g. [1]).

0.4 Some Topological Notions

Since we want to work over an arbitrary field $\Bbbk$, we take $\Bbbk$ with the *discrete topology*, i.e. all subsets of $\Bbbk$ are open. By a *topological vector space* we will mean a $\Bbbk$-vector space endowed with a Hausdorff topology, with a fundamental system of neighbourhoods of 0 consisting of *subspaces*, such that the addition of vectors is continuous. This is not the most general kind of a topological vector space, but it will be sufficient for our purposes. In particular, our definition forces any finite-dimensional vector space to have the discrete topology. By a *topological algebra* we will mean a topological vector space that is also a $\Bbbk$-algebra such that the multiplication is continuous.

Recall that a partially ordered set I is called *directed* if for any $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. A family $\{z_i\}_{i\in I}$ of elements of a topological space Z is called a *net* if I is a directed set. A net $\{z_i\}_{i\in I}$ *converges* to the point z if for any neighbourhood U of z there exists $k \in I$ such that $z_i \in U$ for all $i \geq k$. A net $\{v_i\}_{i\in I}$ in a topological vector space V is called a *Cauchy net* if for any neighbourhood U of 0 there exists $k \in I$ such that $v_i - v_j \in U$ as soon as $i, j \geq k$. A topological vector space V is *complete* if any Cauchy net converges to an element of V.

Recall also the definitions of the direct and inverse limits. If I is a directed set and $\{Z_i\}_{i\in I}$ is a family of sets endowed with a system of maps $\psi_{ij} : Z_i \to Z_j$, for any $i \leq j$, such that $\psi_{ii} = id_{Z_i}$ and $\psi_{jk} \circ \psi_{ij} = \psi_{ik}$, then the *direct limit* is defined by

$$\varinjlim Z_i = \coprod_{i\in I} Z_i / \sim,$$

the quotient set of the disjoint union of Z_i by the following equivalence relation: $x \sim y$ if $x \in Z_i$, $y \in Z_j$, and $\psi_{ik}(x) = \psi_{jk}(y)$ for some $i, j \leq k$. The inclusions $Z_j \subset \coprod_{i\in I} Z_i$ induce the canonical maps $\psi_j : Z_j \to \varinjlim Z_i$. Clearly, we have $\psi_j \circ \psi_{ij} = \psi_i$, and $\varinjlim Z_i$, together with the maps ψ_i, is universal with respect to this property. If the sets Z_i have the structure of vector spaces, algebras, coalgebras, etc. that is preserved by the maps ψ_{ij}, then this structure is inherited by $\varinjlim Z_i$.

Dually, if I is a directed set and $\{Z_i\}_{i\in I}$ is a family of sets endowed with a system of maps $\varphi_{ij} : Z_j \to Z_i$, for any $i \leq j$, such that $\varphi_{ii} = id_{Z_i}$ and $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$, then the *inverse limit*

$$\varprojlim Z_i \subset \prod_{i\in I} Z_i$$

consists of all families $\{z_i\}_{i\in I} \in \prod_{i\in I} Z_i$ such that $\varphi_{ij}(z_j) = z_i$ for all $i \leq j$. The projections $\prod_{i\in I} Z_i \to Z_j$ define the canonical maps $\varphi_j : \varprojlim Z_i \to Z_j$. We have $\varphi_{ij} \circ \varphi_j = \varphi_i$, and $\varprojlim Z_i$, with the maps φ_i, is universal with respect to this property. If the sets Z_i have the structure of vector spaces, algebras, etc. that is preserved by φ_{ij} , then $\varprojlim Z_i$ inherits this structure. Note that in general, the coalgebra structure is *not* inherited because comultiplication is not defined for an infinite direct product of coalgebras. If Z_i are topological spaces, then $\varprojlim Z_i$ has a natural topology as a subset of $\prod_{i\in I} Z_i$.

Let V be a topological vector space and suppose the subspaces U_i, $i \in I$, form a fundamental system of neighbourhoods of 0. We write $i \leq j$ iff $U_i \supset U_j$. Then I is a directed set and the inverse limit $\varprojlim V/U_i$ of the discrete spaces V/U_i contains V as a topological subspace. Moreover, V is dense in $\varprojlim V/U_i$ and $\varprojlim V/U_i$ is complete, so $\hat{V} = \varprojlim V/U_i$ is the *completion* of V.

Definition 0.4.1. Let V be a vector space (without topology), then the dual vector space V^* can be given the "$*$-weak" topology $\sigma(V^*, V)$, i.e. the topology with a fundamental system of neighbourhoods of 0 of the form

$$U_{v_1,\dots,v_m} = \{f \in V^* | \, \langle f, v_k \rangle = 0, \ \forall k = 1, \dots, m\},$$

where $v_1, \dots, v_m \in V$, $m \in \mathbb{N}$.

We immediately observe that all the sets $U_{v_1,\dots,v_m}$ are subspaces of finite codimension, and V^* is complete, thus V^* is a *pro-finite* vector space, i.e. an inverse limit of finite-dimensional vector spaces. Conversely, every pro-finite topological vector space W has the form V^*, where V is the space of *continuous* linear functions on W. Moreover, if $\varphi : V \to W$ is a linear map, then $\varphi^* : W^* \to V^*$ is a continuous linear map, and every continuous linear map $W^* \to V^*$ has the form φ^* for some $\varphi : V \to W$ (see e.g. [14, Section 1.2]).

If V and W are complete topological vector spaces, then $V \otimes W$ can be endowed with a *tensor product topology* defined by a fundamental system of neighbourhoods of 0 of the form $U_1 \otimes W + V \otimes U_2$, where $U_1 \subset V$ and $U_2 \subset W$ are open subspaces. Hence we can define the *completed tensor product*

$$V \hat{\otimes} W = \varprojlim \left((V/U_i) \otimes (W/U_j)\right),$$

where $\{U_i\}$ and $\{U_j\}$ are fundamental systems of neighbourhoods of 0 in V and W, respectively.

If $\varphi : V \to V'$ and $\psi : W \to W'$ are continuous linear maps, we will denote by $\varphi \hat{\otimes} \psi : V \hat{\otimes} W \to V' \hat{\otimes} W'$ the extension of $\varphi \otimes \psi : V \otimes W \to V' \otimes W'$.

Now if V and W are vector spaces (without topology), and V^* and W^* are endowed with $*$-weak topology, then $V^* \otimes W^*$ is a dense topological subspace of the complete space $(V \otimes W)^*$. Therefore, $(V \otimes W)^* = V^* \hat{\otimes} W^*$.

To conclude this section, let us introduce our main example of a topological algebra — the algebra of formal power series (in any number of variables). But first we need to define the multiindex notation.

Definition 0.4.2. Let I be a set. A *multiindex* on I is a map $\alpha : I \to \{0, 1, \ldots\}$ such that

$$\operatorname{supp} \alpha = \{i \in I \mid \alpha(i) \neq 0\}$$

is finite, in other words, $\alpha \in \mathbb{Z}_+^{(I)}$, the direct sum of $|I|$ copies of $\mathbb{Z}_+$. For any such α we set

$$|\alpha| = \sum_{i \in \operatorname{supp} \alpha} \alpha(i).$$

For $\alpha, \beta \in \mathbb{Z}_+^{(I)}$, we write $\alpha \leq \beta$ if $\alpha(i) \leq \beta(i)$ for all $i \in I$.

For two multiindices α, β, we define the combination number:

$$\binom{\alpha}{\beta} = \prod_{i \in \operatorname{supp} \alpha} \binom{\alpha(i)}{\beta(i)}$$

if $\beta \leq \alpha$ and 0 otherwise. We also denote by ε_i the multiindex whose only nonzero component is $\varepsilon_i(i) = 1$.

Definition 0.4.3. The *algebra of formal power series* $\mathbb{k}[[t_i | i \in I]]$ is the topological vector space $\prod_{\alpha \in \mathbb{Z}_+^{(I)}} \mathbb{k}$ (direct product of copies of $\mathbb{k}$, with direct product topology), whose elements will be written as formal sums

$$\sum_\alpha \lambda_\alpha \mathbf{t}^\alpha,$$

with multiplication defined by the Cauchy rule:

$$\left(\sum_{\alpha}\lambda_\alpha \mathbf{t}^\alpha\right)\left(\sum_{\beta}\mu_\beta \mathbf{t}^\beta\right)=\sum_{\gamma}\left(\sum_{\alpha+\beta=\gamma}\lambda_\alpha\mu_\beta\right)\mathbf{t}^\gamma.$$

Note that the definition above makes sense because the sum over $\alpha+\beta=\gamma$ is finite for any fixed $\gamma\in\mathbb{Z}_+^{(I)}$. Moreover, if we set $t_i=\mathbf{t}^{\varepsilon_i}$, then, for any $\alpha\in\mathbb{Z}_+^{(I)}$,

$$\mathbf{t}^\alpha=\prod_{i\in\operatorname{supp}\alpha}t_i^{\alpha(i)},$$

so $\Bbbk[[t_i|i\in I]]$ contains the algebra of polynomials $\Bbbk[t_i|i\in I]$ as a dense subalgebra.

Finally, $\Bbbk[[t_i|i\in I]]$ is a pro-finite topological algebra with a fundamental system of neighbourhoods of 0 consisting of the ideals

$$U_\alpha=\operatorname{ideal}\langle t_i^{\alpha(i)+1}\mid i\in I\rangle,\qquad \alpha\in\mathbb{Z}_+^{(I)}.$$

In general, any pro-finite topological algebra has a fundamental system of neighbourhoods of 0 consisting of *ideals* [14, Section 1.2.7].

0.5 One Fact from Descent Theory

We will need the following standard descent theory lemma (see e.g [36, Chapter 17]). Recall that if $L/\Bbbk$ is a (possibly infinite) Galois field extension, then we can define the *Krull topology* on the Galois group $\Sigma=\operatorname{Gal}(L/\Bbbk)$ by taking as a fundamental system of neighbourhoods of 1 all the centralizer subgroups of finite subextensions. Then Σ becomes a compact Hausdorff topological group and we recover in the general case the classical bijection between subgroups and subfields (that holds for finite $L/\Bbbk$) if we restrict our attention only to *closed* subgroups (see e.g. [22]). Moreover, any open subgroup of Σ is of finite index, so Σ is a pro-finite group.

Lemma 0.5.1. *Let $L/\Bbbk$ be a Galois field extension, $\Sigma = \mathrm{Gal}(L/\Bbbk)$. Let V be a vector space over L endowed with a continuous semilinear Σ-action, i.e.*

$$s(v+w) = s(v) + s(w),\ s(\lambda v) = s(\lambda)s(v), \qquad \forall s \in \Sigma,\ v, w \in V,\ \lambda \in L,$$

and the centralizer of any vector in V is an open subgroup of Σ. Then

$$V = V^{\Sigma} \otimes_{\Bbbk} L,$$

where $V^{\Sigma} \subset V$ is the set of Σ-invariants. Moreover, V^{Σ} inherits any algebraic structure defined on V by Σ-invariant L-multilinear maps. ■

Chapter 1

Identities of Coalgebras

1.1 Coalgebras with a Polynomial Identity

It seems natural to define a polynomial identity for coalgebras using their duality with algebras, for which this notion is quite well-known (see Section 0.3). The following definition was introduced by the author in [19].

Definition 1.1.1. Let C be a coalgebra over a field $\Bbbk$, $F(X_1, \ldots, X_n)$ a polynomial in n noncommuting variables with coefficients in $\Bbbk$. We say that $F = 0$ (or just F) is an identity for the coalgebra C, if it is an identity for the dual algebra C^*.

Using duality, we immediately observe that if a coalgebra C satisfies some identity, then any subcoalgebra and any factorcoalgebra of C satisfies this identity. If a family of coalgebras satisfies some identity, then their direct sum satisfies this identity.

Since any coalgebra C is the sum of its finite-dimensional subcoalgebras (see Theorem 0.1.8), in order to prove that $F = 0$ holds for C, it is sufficient to verify this identity on finite-dimensional subcoalgebras of C. We will use this observation later.

Now we want to give an intrinsic definition when a coalgebra satisfies an identity, i.e. a definition that would not use the dual algebra. Unfortunately, it works well only for multilinear identities (which is sufficient in the case of $\operatorname{char} \Bbbk = 0$ because of Theorem 0.3.2).

A multilinear polynomial of degree n has the form:

$$F(X_1, \ldots, X_n) = \sum_{\pi \in S_n} \lambda_\pi X_{\pi(1)} \ldots X_{\pi(n)},$$

where S_n is the group of permutations and $\lambda_\pi \in \Bbbk$. It will be convenient to identify F with the element $\sum_{\pi \in S_n} \lambda_\pi \pi$ of the group algebra $\Bbbk S_n$.

For any vector space V, there are natural right and left actions of S_n on $V^{\otimes n}$:

$$\begin{aligned}(v_1 \otimes \ldots \otimes v_n) \cdot \pi &= v_{\pi(1)} \otimes \ldots \otimes v_{\pi(n)}, \\ \pi \cdot (v_1 \otimes \ldots \otimes v_n) &= v_{\pi^{-1}(1)} \otimes \ldots \otimes v_{\pi^{-1}(n)}.\end{aligned}$$

Then the fact that an algebra A satisfies a multilinear identity $F = 0$ can be written as follows:

$$m_n(A^{\otimes n} \cdot F) = 0,$$

where $m_n : A^{\otimes n} \to A$ is the multiplication of A. The following dual definition for coalgebras is due to Yu.Bahturin.

Definition 1.1.2. Let C be a coalgebra, $F = \sum_{\pi \in S_n} \lambda_\pi X_{\pi(1)} \ldots X_{\pi(n)}$ a multilinear polynomial. We say that C satisfies the identity $F = 0$ if

$$F \cdot (\Delta_n C) = 0,$$

where $\Delta_n : C \to C^{\otimes n}$ is the comultiplication of C.

So a multilinear identity of degree n can be viewed as a sort of symmetry condition on the tensors $\Delta_n c$, for all $c \in C$.

Proposition 1.1.3. *Definitions 1.1.1 and 1.1.2 are equivalent for multilinear identities.*

Proof. Using the sigma notation $\Delta_n c = \sum c_{(1)} \otimes \ldots \otimes c_{(n)}$, $c \in C$, we have:

$$F \cdot (\Delta_n c) = \sum_{\pi \in S_n} \lambda_\pi \sum c_{(\pi^{-1}(1))} \otimes \ldots \otimes c_{(\pi^{-1}(n))},$$

hence, for all $\varphi_1, \ldots, \varphi_n \in C^*$,

$$\begin{aligned} \langle \varphi_1 \otimes \ldots \otimes \varphi_n, F \cdot (\Delta_n c) \rangle &= \sum_{\pi \in S_n} \lambda_\pi \sum \langle \varphi_1, c_{(\pi^{-1}(1))} \rangle \ldots \langle \varphi_n, c_{(\sigma^{-1}(n))} \rangle \\ &= \sum_{\pi \in S_n} \lambda_\pi \sum \langle \varphi_{\pi(1)}, c_{(1)} \rangle \ldots \langle \varphi_{\pi(n)}, c_{(n)} \rangle \\ &= \sum_{\pi \in S_n} \lambda_\pi \langle \varphi_{\pi(1)} \ldots \varphi_{\pi(n)}, c \rangle \\ &= \langle F(\varphi_1, \ldots, \varphi_n), c \rangle. \end{aligned}$$

Therefore, $F \cdot (\Delta_n C) = 0$ iff the identity $F(\varphi_1, \ldots, \varphi_n) = 0$ holds for all $\varphi_1, \ldots, \varphi_n \in C^*$. ■

Using the sigma notation as in the proof, the fact that a coalgebra C satisfies a multilinear identity can be written as follows:

$$\sum_{\pi \in S_n} \lambda_\pi \sum x_{(\pi^{-1}(1))} \otimes \ldots \otimes x_{(\pi^{-1}(n))} = 0, \qquad \forall x \in C.$$

For example, cocommutativity can be expressed like this:

$$\sum x_{(1)} \otimes x_{(2)} - \sum x_{(2)} \otimes x_{(1)} = 0.$$

By Definition 1.1.1, any finite-dimensional coalgebra C satisfies the standard identity

$$\sum_{\pi \in S_n} (-1)^\pi \sum x_{(\pi^{-1}(1))} \otimes \ldots \otimes x_{(\pi^{-1}(n))} = 0,$$

for any $n > \dim C$.

The following proposition provides a way of constructing infinite-dimensional PI-coalgebras (i.e. coalgebras with a nontrivial identity).

Proposition 1.1.4. *If an algebra A satisfies the identity $F = 0$, then so does the coalgebra A°. The converse holds if A is residually finite-dimensional.*

Proof. For the first assertion, it suffices to prove that $F = 0$ is an identity for any finite-dimensional subcoalgebra $D \subset A^\circ$. Set $I = D^\perp$. This is an ideal of finite codimension in A. Since D is finite-dimensional, $I^\perp = D$, and so we have $D \cong (A/I)^\circ = (A/I)^*$, hence $D^* \cong A/I$ satisfies $F = 0$.

Conversely, if A is residually finite-dimensional, i.e. the intersection of the ideals of finite codimension in A is 0, then $A \subset A^{\circ *}$. But the algebra $A^{\circ *}$ satisfies $F = 0$ since so does the coalgebra A°. ∎

1.2 Free Coalgebras

A polynomial identity $F(X_1, \ldots, X_n)$ of an (associative) algebra may be considered as an element of the free (associative) algebra with n generators, i.e. the tensor algebra $T(V)$, where $V = \langle X_1, \ldots, X_n \rangle$ (recall that we assume that algebras have the unit element).

In order to make a link between identities of coalgebras and free coalgebras, we first need to define the latter. Free coalgebras (which more precisely should be called "cofree coalgebras") were introduced by M.Sweedler in [32]. They are defined by the following universal property, which is dual to the universal property of tensor algebras.

Definition 1.2.1. Let V be a vector space, C a coalgebra, $\theta : C \to V$ a linear map. The pair (C, θ) is called a *free coalgebra of* V if, for any coalgebra D and a linear map $\varphi : D \to V$, there exists a unique coalgebra map $\Phi : D \to C$ completing the commutative diagram:

$$\begin{array}{ccc} D & \overset{\Phi}{\dashrightarrow} & C \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\theta} & \\ & V & \end{array}$$

By a standard argument, if a free coalgebra of V exists, it is unique up to a uniquely defined isomorphism. We will denote it by $cT(V)$. It is shown in [32] that $cT(V)$ exists for any V, but we will follow a more explicit construction of R.Block and P.Leroux [10]. First we introduce the generalized finite dual.

Definition 1.2.2. Let $A = \bigoplus_{n \geq 0} A_n$ be a graded algebra, V a vector space. Let $\mathrm{Hom}(A, T(V))$ denote the space of all graded linear functions of degree 0 from A to the tensor algebra $T(V) = \bigoplus_{n \geq 0} T^n(V)$, i.e. all linear functions $f : A \to T(V)$ such that if $a \in A_n$, then $f(a)$ is a tensor of degree n. We will call $f \in \mathrm{Hom}(A, T(V))$ *representative* if there exists a finite family $\{g_i, h_i\}$ of elements of $\mathrm{Hom}(A, T(V))$ such that

$$f(ab) = \sum_i g_i(a) h_i(b), \qquad \forall a, b \in A, \tag{1.2.1}$$

where the multiplication on the right-hand side is the tensor product in $T(V)$. Since we will later consider elements of $T(V) \otimes T(V)$, we reserve the symbol $\otimes$ for the "outer" tensor product and simply write $v_1 \ldots v_n$ for the element

$v_1 \otimes \ldots \otimes v_n \in T(V)$. The set of all representative functions $A \to T(V)$ will be denoted by A_V°.

It follows that if $f \in A_V^\circ$, then the tensor $\sum_i g_i \otimes h_i$ is uniquely determined by (1.2.1). We define $\Delta f = \sum_i g_i \otimes h_i$, and it turns out that $\Delta f \in A_V^\circ \otimes A_V^\circ$ and (A_V°, Δ) is a coalgebra with counit $\varepsilon(f) = f(1)$ [10, Lemma 1 and Theorem 1]. If $V = \Bbbk$, we recover the usual finite dual coalgebra A° of the (underlying ungraded) algebra A.

If we now specify $A = T(W)$ (graded by degree), for some vector space W, then there is a natural linear map $\theta : T(W)_V^\circ \to \mathrm{Hom}(W, V)$ which sends $f \in T(W)_V^\circ$ to its restriction to $W = T^1(W)$.

Theorem 1.2.3 (Theorem 2′ in [10]). *Let V and W be vector spaces. Then $(T(W)_V^\circ, \theta)$ defined above is (a realization of) the free coalgebra of the space $\mathrm{Hom}(W, V)$. Moreover, if D is a coalgebra and $\varphi : D \to \mathrm{Hom}(W, V)$ is a linear map, then the lifting of φ to a coalgebra map $\Phi : D \to T(W)_V^\circ$ is given by*

$$\begin{aligned}
\Phi(d)1 &= \varepsilon(d), \\
\Phi(d)w &= \varphi(d)w, \qquad \forall w \in W = T^1(W), \text{ and} \\
\Phi(d)z &= \left(\sum \varphi(d_{(1)}) \otimes \ldots \otimes \varphi(d_{(n)})\right) z, \qquad \forall z \in T^n(W), \text{ if } n > 1.
\end{aligned}$$

■

In particular, if we set $V = \Bbbk$, we see that $T(W)^\circ$ is the free coalgebra of W^*. This is a result of M.Sweedler originally used to prove the existence of free coalgebras. It also sheds light on the nature of identities of a coalgebra. Let $F(X_1, \ldots, X_n)$ be an associative polynomial in n variables, set

$W = \langle X_1 \ldots, X_n \rangle$, so $F \in T(W)$. Then the free coalgebra $cT(W^*) = T(W)^\circ$ is a subspace of $T(W)^*$ containing $T(W^*)$ (see Remark 1.2.4 below). Moreover, $T(W)^*$ has a natural topology of a dual space (see Definition 0.4.1), and $T(W)$ can be recovered as the space of all continuous linear functions on $T(W)^*$. Since $T(W^*)$ is dense in $T(W)^*$, so is $cT(W^*)$ and hence the spaces of continuous linear functions on $T(W)^*$ and on $cT(W^*)$ (with topology inherited from $T(W)^*$) are in one-to-one correspondence. Thus we conclude that $T(W)$ is the space of continuous linear functions on $cT(W^*)$ and so polynomial identities in $X_1, \ldots, X_n$ can be viewed as continuous linear functions on the free coalgebra of the space $\langle X_1, \ldots, X_n \rangle^*$.

On the other hand, if we set $W = \Bbbk$ in Theorem 1.2.3, we obtain that $\Bbbk[t]^\circ_V$ is the free coalgebra of V. This gives a rather explicit construction of $cT(V)$ as follows. Denote $\hat{T}(V)$ the completion of the tensor algebra $T(V)$, i.e. the algebra of all infinite formal sums $z = z_0 + z_1 + \ldots$, where $z_i \in T^i(V)$. The topology on $\hat{T}(V)$ is defined by a fundamental system of neighbourhoods of 0 consisting of the sets

$$F^n\hat{T}(V) = \{z \in \hat{T}(V) \mid z_i = 0 \ \forall i < n\}.$$

Then an element $f \in \mathrm{Hom}(\Bbbk[t], T(V))$ can be identified with the formal sum $f_0 + f_1 + \ldots$, where $f_i = f(t^i) \in T^i(V)$, and so $cT(V)$ becomes a subspace of $\hat{T}(V)$. Upon this identification, the canonical map $\theta : cT(V) \to V$ just sends the sum $f_0 + f_1 + \ldots$ to its degree 1 component $f_1 \in T^1(V) = V$, and the formulas of Theorem 1.2.3 for the lifting of a linear map $\varphi : D \to V$ to a coalgebra map $\Phi : D \to cT(V)$ become:

$$\begin{aligned}\Phi(d)_0 &= \varepsilon(d),\\ \Phi(d)_1 &= \varphi(d), \text{ and}\\ \Phi(d)_n &= \sum \varphi(d_{(1)}) \otimes \ldots \otimes \varphi(d_{(n)}) \text{ if } n > 1.\end{aligned}$$

Moreover, an explicit formula for the comultiplication of $cT(V)$ can be obtained as follows (see [9, Sections 1 and 2]). Let $\mathcal{D}$ denote the continuous linear function from $\hat{T}(V)$ to $\hat{T}(V)\hat{\otimes}\hat{T}(V)$ defined by its action on the monomials:

$$\mathcal{D}(v_1 \ldots v_n) = \sum_{i=0}^{n} v_1 \ldots v_i \otimes v_{i+1} \ldots v_n, \qquad \forall v_1, \ldots, v_n \in V,\ n = 0, 1, \ldots \tag{1.2.2}$$

Then an element $f \in \hat{T}(V)$ belongs to $cT(V)$ iff $\mathcal{D}f$ lies in the subspace $\hat{T}(V) \otimes \hat{T}(V) \subset \hat{T}(V)\hat{\otimes}\hat{T}(V)$, in which case $\Delta f = \mathcal{D}f$, i.e. the comultiplication of $cT(V)$ is just the restriction of $\mathcal{D}$ on $cT(V)$. We also see from here that $T(V) \subset cT(V)$. In particular, this implies that the canonical map θ is surjective. The counit of $cT(V)$ just sends the sum $f_0 + f_1 + \ldots$ to its degree 0 component $f_0 \in T^0(V) = \Bbbk$.

Remark 1.2.4. Assuming the space V finite-dimensional, set $W = V^*$. Then the above construction of $cT(V) \subset \hat{T}(V)$ agrees with the construction of M.Sweedler which realizes $cT(W^*)$ as the subspace $T(W)^\circ$ of $T(W)^* = \hat{T}(V)$. In particular, $T(W)^\circ$ contains $T(W^*)$.

Remark 1.2.5. R.Block also proves in [9] a number of interesting properties of $cT(V)$ which we will not use here. But one thing should be mentioned, since it illustrates the duality with algebras. Namely, there is a natural multiplication $\star : cT(V) \otimes cT(V) \to cT(V)$ which is the lifting of the linear map $\theta \otimes \varepsilon + \varepsilon \otimes \theta : cT(V) \otimes cT(V) \to V$, so $cT(V)$ has a structure of a commutative Hopf algebra, with the antipode induced by $-\theta : T(V) \to V$ — dually to the fact the free algebra $T(V)$ has a natural structure of a cocommutative Hopf algebra defined by $V \to T(V) \otimes T(V) : v \to v \otimes 1 + 1 \otimes v$, with antipode induced by $V \to T(V) : v \to -v$ (this is the same Hopf algebra structure as the one coming from the fact that $T(V)$ is the universal envelope of the free Lie algebra generated by the space V). We will return to the multiplication $\star$ in Section 1.5, where we will see that it is in fact the so called "shuffle product".

To conclude this section, let us introduce the notion of a cogenerating map for coalgebras, which is the dual of a generating set (or, more precisely, space) for algebras. Let A be an algebra, V a vector space. Suppose we have a linear map $\varphi : V \to A$, then the image $\varphi(V)$ generates A as an algebra iff

$$\sum_{n \geq 0} \left(m_n \circ \varphi^{\otimes n}\right) V^{\otimes n} = A,$$

where $m_n : A^{\otimes n} \to A$ is the multiplication of A (with $m_1 = id_A$ and $m_0 = u$, the unit map). The formal dual of this statement is the following:

Definition 1.2.6. Let C be a coalgebra, V a vector space. We will call a linear map $\varphi : C \to V$ *cogenerating* if

$$\bigcap_{n \geq 0} \operatorname{Ker}\left(\varphi^{\otimes n} \circ \Delta_n\right) = 0.$$

A generating set in an algebra A allows us to represent A as a factor of a free algebra. Dually, cogenerating maps for a coalgebra C correspond to the imbeddings of C into free coalgebras.

Proposition 1.2.7. *Let C be a coalgebra, V a vector space, $\varphi : C \to V$ a linear map. Then the induced coalgebra map $\Phi : C \to cT(V)$ is injective iff φ is cogenerating.*

Proof. Recall from the explicit construction of $cT(V)$ that $\Phi(d)_n = \sum \varphi(d_{(1)}) \otimes \ldots \otimes \varphi(d_{(n)})$, $d \in C$ (with the convention that the right-hand side means $\varphi(d)$ for $n = 1$ and $\varepsilon(d)$ for $n = 0$). In other words, $\Phi(d)_n = (\varphi^{\otimes n} \circ \Delta_n)d$, hence $d \in \operatorname{Ker}\Phi$ iff $(\varphi^{\otimes n} \circ \Delta_n)d = 0$, for all n. ∎

In particular, any coalgebra can be imbedded into a free coalgebra (take $V = C$, then $id : C \to V$ is obviously a cogenerating map).

1.3 Varieties of Coalgebras and Theorem of Birkhoff

In this section we assume the field $\Bbbk$ infinite.

First we briefly recall the situation that we have for algebras. Let $\mathcal{F}$ denote the free algebra in countably many generators, i.e. $\mathcal{F} = T(V)$, where $V = \langle X_1, X_2, \ldots \rangle$. Then any polynomial identity, no matter in how many variables, can be viewed as an element of $\mathcal{F}$.

Let A be an algebra, then the set $\mathcal{I}(A)$ of all identities satisfied by A is an ideal of $\mathcal{F}$, invariant under any endomorphism of $\mathcal{F}$.

Definition 1.3.1. An ideal J of $\mathcal{F}$ is called a *T-ideal* if $\alpha(J) \subset J$, for any endomorphism α of $\mathcal{F}$, or, equivalently, if $\beta(J) = 0$, for any algebra map $\beta : \mathcal{F} \to \mathcal{F}/J$ (the equivalence follows from the universal property of $\mathcal{F}$).

Definition 1.3.2. Let S be a subset of $\mathcal{F}$. The *variety of algebras* defined by S is the class $\mathrm{Var}(S)$ of all algebras that satisfy each identity from the set S.

Then varieties of algebras are in one-to-one correspondence with T-ideals as follows. If $\mathfrak{A}$ is a variety defined by some $S \subset \mathcal{F}$, then the set $\mathcal{I}(\mathfrak{A})$ of all identities satisfied by each algebra from $\mathfrak{A}$ is the T-ideal generated by S (i.e. the smallest T-ideal containing S). In other words, the T-ideal generated by S consists of all possible consequences of the identities from S. Therefore, if $J \subset \mathcal{F}$ is already a T-ideal, then for the variety of algebras $\mathfrak{A} = \mathrm{Var}(J)$ we have $\mathcal{I}(\mathfrak{A}) = J$. Conversely, if $\mathfrak{A}$ is a variety, then clearly $\mathfrak{A} = \mathrm{Var}(\mathcal{I}(\mathfrak{A}))$.

Varieties of algebras can be characterized by the following theorem [8].

Theorem 1.3.3 (Birkhoff). *Let $\mathfrak{A}$ be a nonempty class of algebras. Then $\mathfrak{A}$ is a variety (i.e. is defined by identities) iff $\mathfrak{A}$ is closed under isomorphisms, subalgebras, factoralgebras, and direct products.* ■

Now we turn our attention to coalgebras. By analogy with algebras, it is natural to give the following definition.

Definition 1.3.4. Let S be a subset of $\mathcal{F}$. The *variety of coalgebras* defined by S is the class $\mathrm{cVar}(S)$ of all coalgebras that satisfy each identity from S.

Here we also have a one-to-one correspondence between varieties and T-ideals. Since by definition the set $\mathcal{I}(C)$ of identities of a coalgebra C is the same as the set of identities of the algebra C^*, $\mathcal{I}(C)$ is a T-ideal. Consequently, if $\mathfrak{C} = \mathrm{cVar}(S)$, then the set $\mathcal{I}(\mathfrak{C})$ of all identities satisfied by $\mathfrak{C}$ is a T-ideal containing S. It is not immediately obvious why $\mathcal{I}(\mathfrak{C})$ should be the smallest such T-ideal, but we will prove this in a moment (and we will need the assumption that $\Bbbk$ is infinite). With this fact at hand, the maps $\mathcal{I}$ and cVar establish the desired one-to-one correspondence as in the case of algebras.

Proposition 1.3.5. *Let $\mathfrak{C}$ be the variety of coalgebras defined by a set of identities S. Then the T-ideal $\mathcal{I}(\mathfrak{C})$ of identities of $\mathfrak{C}$ is generated by S as a T-ideal. In other words, the consequences of the system of identities S are the same for coalgebras as they are for algebras.*

Proof. First of all, since the base field $\Bbbk$ is infinite, any T-ideal J is graded (see Theorem 0.3.2). It follows that the algebra $\mathcal{F}/J$ is residually finite-dimensional. Indeed, for any $F(X_1, \ldots, X_n) \notin J$, we need to find an ideal of finite codimension $J' \supset J$ such that $F \notin J'$. Since J is graded, we can set J' equal to the ideal generated by J,$X_{n+1}, X_{n+2}, \ldots$ and by all monomials in $X_1, \ldots, X_n$ of degree $d+1$, where d is the maximum degree of monomials occuring in F.

Now let J be an arbitrary T-ideal containing our set S. By Proposition 1.1.4, the coalgebra $D = (\mathcal{F}/J)^\circ$ satisfies the same identities as the algebra $\mathcal{F}/J$, so $\mathcal{I}(D) = J$. Since $S \subset J$, D is in the variety $\mathfrak{C}$, hence $J = \mathcal{I}(D) \supset \mathcal{I}(\mathfrak{C})$. Therefore, $\mathcal{I}(\mathfrak{C})$ is the smallest T-ideal containing S. ■

Surprisingly enough, the analog of Theorem 1.3.3 does not hold for coalgebras. Obviously, any variety of coalgebras is closed under isomorphisms, subcoalgebras, factorcoalgebras, and direct sums. However, not every such class is a variety.

Example 1.3.6. The class *Grp* of all coalgebras spanned by group-like elements is closed under the four operations just listed, but it is not a variety.

Proof. First, if a coalgebra C is represented as a direct sum of coalgebras: $C = \bigoplus_i C_i$, then any subcoalgebra $D \subset C$ has the form $D = \bigoplus_i D_i$, where $D_i = D \cap C_i$. This is the fact dual to the following statement for algebras: if $A = \prod_i A_i$, then any ideal $J \subset A$ has the form $J = \prod_i J_i$, where J_i is the projection of J to A_i. It follows that if C is spanned by group-like elements (which are necessarily linearly independent), then any subcoalgebra of C is just a span of a subset of these group-like elements. Second, if C is spanned by group-like elements, then any homomorphic image of C is spanned by the images of these elements, which are either group-like or zero. Obviously, the class *Grp* is also closed under isomorphisms and direct sums.

Grp is not a variety, because it is properly contained in the variety *Cocomm* of all cocommutative algebras, which does not have any proper subvarieties other than $\{0\}$. The latter is the case since any T-ideal containing the identity $X_1X_2 - X_2X_1$ is either generated by it or is the whole $\mathcal{F}$ by Corollary 0.3.3. ∎

Example 1.3.7. The class *Pnt* of all pointed coalgebras is closed under the four operations listed above, but it is not a variety.

Proof. Recall that a coalgebra is called pointed if all its simple subcoalgebras are one-dimensional or, equivalently, its coradical is spanned by group-like elements. Thus *Pnt* is obviously closed under isomorphisms and subcoalgebras. Further, by Corollary 0.1.13, a homomorphic image of a pointed coalgebra is pointed. Finally, [25, Lemma 5.6.2(1)] says that if $C = \sum_i C_i$, where $C_i \subset C$ are subcoalgebras, then any simple subcoalgebra of C lies in one of the C_i, hence a sum of pointed coalgebras is pointed.

Example 1.5.1 in Section 1.5 (discussing Taft's algebras) implies that *Pnt* does not satisfy any nontrivial identity. Hence Pnt is a proper subclass of the variety $Coalg$ of all coalgebras, which is not contained in any proper subvariety. ■

Definition 1.3.8. We will use the term *pseudo-variety* for any nonempty class of coalgebras closed under isomorphisms, subcoalgebras, factorcoalgebras, and direct sums.

Thus Grp and Pnt are pseudo-varieties which are not varieties. We have shown that varieties of coalgebras are in one-to-one correspondence with T-ideals in the free algebra $\mathcal{F}$ in countably many generators $X_1, X_2, \ldots$ To characterize pseudo-varieties in a similar manner, we will need the objects dual to T-ideals. Let $c\mathcal{F} = cT(V)$, where $V = \langle X_1, X_2, \ldots \rangle$. Loosely speaking, $c\mathcal{F}$ is the free coalgebra "in countably many cogenerators".

Definition 1.3.9. A subcoalgebra $L \subset c\mathcal{F}$ is called a *T-subcoalgebra* if $\alpha(L) \subset L$, for any endomorphism α of $c\mathcal{F}$, or, equivalently, if $\beta(L) \subset L$, for any coalgebra map $\beta : L \to c\mathcal{F}$ (the equivalence follows from the universal property of $c\mathcal{F}$).

Then pseudo-varieties of coalgebras are in a one-to-one correspondence with T-subcoalgebras as follows. We associate with a pseudo-variety $\mathfrak{C}$ the largest subcoalgebra $L \subset c\mathcal{F}$ belonging to $\mathfrak{C}$ (the sum of all such subcoalgebras, which belongs to $\mathfrak{C}$ because $\mathfrak{C}$ is closed under direct sums and factors). Since $\mathfrak{C}$ is closed under homomorphic images, L will be a T-subcoalgebra.

Conversely, we associate with a T-subcoalgebra $L \subset c\mathcal{F}$ the class $\mathfrak{C}$ consisting of all coalgebras D such that, for any coalgebra map $\gamma : D \to c\mathcal{F}$, $\gamma(D) \subset L$. Obviously, $\mathfrak{C}$ is closed under isomorphisms, factors and direct sums. It is also closed under subcoalgebras, because coalgebra maps to $c\mathcal{F}$ can always be extended from subcoalgebras by the universal property of $c\mathcal{F}$. Two more checks are necessary.

Firstly, let L be a T-subcoalgebra, $\mathfrak{C}$ the pseudo-variety associated with L, and L' the T-subcoalgebra associated with $\mathfrak{C}$. Since L' belongs to $\mathfrak{C}$, then considering the inclusion map $L' \hookrightarrow \mathcal{F}$, we see that $L' \subset L$ by the construction of $\mathfrak{C}$. Conversely, using the definition of a T-coalgebra, we conclude that L also belongs to $\mathfrak{C}$, but then $L \subset L'$ since L' is the largest subcoalgebra with this property. So $L = L'$.

Secondly, let $\mathfrak{C}$ be a pseudo-variety, L the T-subcoalgebra associated with $\mathfrak{C}$, and $\mathfrak{C}'$ the pseudo-variety associated with L. If a coalgebra D belongs to $\mathfrak{C}$, then for any coalgebra map $\gamma : D \to c\mathcal{F}$, $\gamma(D) \subset L$ since $\mathfrak{C}$ is closed under homomorphic images and L is the largest subcoalgebra of $c\mathcal{F}$ belonging to $\mathfrak{C}$. Therefore, D is in $\mathfrak{C}'$ and we proved that $\mathfrak{C} \subset \mathfrak{C}'$. Conversely, if a coalgebra D belongs to $\mathfrak{C}'$, we want to prove that D must be in $\mathfrak{C}$ and so $\mathfrak{C}' \subset \mathfrak{C}$. To this end, observe that it suffices to prove that any finite-dimensional subcoalgebra of D lies in $\mathfrak{C}$, because D is a sum of such subcoalgebras and $\mathfrak{C}$ is closed under sums. So we may assume D finite-dimensional. Then there is an injective linear map $\varphi : D \to V = \langle X_1, X_2, \ldots \rangle$, which can be lifted to a coalgebra map $\Phi : D \to c\mathcal{F}$, necessarily also injective. Since $\Phi(D) \subset L$ by the definition of the class $\mathfrak{C}'$, we conclude that D is isomorphic to a subcoalgebra of L, hence D is in $\mathfrak{C}$. This completes the proof of the desired one-to-one correspondence.

To conclude this section, we will give a characterization of varieties of coalgebras among pseudo-varieties. The following replacement of Birkhoff's theorem says that a pseudo-variety is a variety iff it is closed under some sort of "completion".

Theorem 1.3.10. *A nonempty class of coalgebras $\mathfrak{C}$ is a variety iff it is closed under isomorphisms, subcoalgebras, factorcoalgebras, and direct sums, and in addition, for any coalgebra C from $\mathfrak{C}$ and any subalgebra $A \subset C^*$, A° belongs to $\mathfrak{C}$.*

Remark 1.3.11. In the theorem above, it suffices to consider only subalgebras $A \subset C^*$ that are dense in the topology of the dual space. In this case, C imbeds into A°, so the latter can be regarded, loosely speaking, as "completions" of C (not in the topological sense: C has no topology).

Before we can prove Theorem 1.3.10, we will need the following useful characterization of the T-ideal $\mathcal{I}(C)$ of identities of a coalgebra C. This lemma is a dualization of the statement: the T-ideal $\mathcal{I}(A)$ of identities of an algebra A is equal to the intersection of the kernels of all algebra maps $\mathcal{F} \to A$. Recall the notation of Lemma 0.1.5.

Lemma 1.3.12. *Let C be a coalgebra. Denote by L the sum of the images of all coalgebra maps $C \to \mathcal{F}^\circ$. Then $\mathcal{I}(C) = L^\perp$.*

Proof. Recall from Section 0.1 that the functor $(\ )^\circ$ is the right adjoint of $(\ )^*$, i.e. for any algebra A and coalgebra C, the sets of homomorphisms $\mathrm{Alg}(A, C^*)$ and $\mathrm{Coalg}(C, A^\circ)$ are in a one-to-one correspondence. Namely, the following are the inverse bijections constructed by M.Sweedler [32]:

$\Phi : \mathrm{Alg}(A, C^*) \to \mathrm{Coalg}(C, A^\circ)$ sending β to the composite $C \hookrightarrow C^{*\circ} \xrightarrow{\beta^*} A^\circ$,

and

$\Psi : \mathrm{Coalg}(C, A^\circ) \to \mathrm{Alg}(A, C^*)$ sending α to the composite $A \to A^{\circ *} \xrightarrow{\alpha^*} C^*$.

We apply this result to $A = \mathcal{F}$ and our C. Let $\alpha : C \to \mathcal{F}^\circ$ be a coalgebra map, then $\alpha = \Phi(\beta)$ for the algebra map $\beta = \Psi(\alpha) : \mathcal{F} \to C^*$, so we have:

$$\begin{aligned}
(\mathrm{Im}\alpha)^\perp &= \{F \in \mathcal{F} \,|\, \forall c \in C \ \langle F, \alpha(c)\rangle = 0\} \\
&= \{F \in \mathcal{F} \,|\, \forall c \in C \ \langle F, \beta^*(c)\rangle = 0\} \\
&= \{F \in \mathcal{F} \,|\, \forall c \in C \ \langle \beta(F), c\rangle = 0\} \\
&= \{F \in \mathcal{F} \,|\, \beta(F) = 0\} = \mathrm{Ker}\beta.
\end{aligned}$$

Since by definition the identities of C are the same as the identitiies of C^*, we can compute:

$$\mathcal{I}(C) = \mathcal{I}(C^*) = \bigcap_\beta \mathrm{Ker}\beta = \bigcap_\alpha (\mathrm{Im}\alpha)^\perp = \left(\sum_\alpha \mathrm{Im}\alpha\right)^\perp = L^\perp.$$

■

Proof of Theorem 1.3.10. The necessity of the last condition follows from Proposition 1.1.4. Let us prove the sufficiency.

Suppose a class $\mathfrak{C}$ satisfies the conditions of the theorem. Set $J = \mathcal{I}(\mathfrak{C})$, the T-ideal of identities satisfied by each coalgebra of $\mathfrak{C}$. We claim that $\mathfrak{C}$ coincides with the variety of coalgebras $\mathrm{cVar}(J)$ defined by J. Obviously, $\mathfrak{C}$ is contained in $\mathrm{cVar}(J)$.

Conversely, let D be a coalgebra satisfying all identities from J. We want to prove that D is in $\mathfrak{C}$. Without loss of generality, we assume D finite-dimensional. Choose some imbedding of vector spaces $D \hookrightarrow V^*$, where $V = \langle X_1, X_2, \ldots\rangle$. By the universal property of $\mathcal{F}^\circ = cT(V^*)$, we obtain an imbedding of coalgebras $D \hookrightarrow \mathcal{F}^\circ$. Since D satisfies all identities from J, Lemma 1.3.12 implies that $D^\perp \supset J$.

Let L be the largest subcoalgebra of $\mathcal{F}^\circ$ belonging to $\mathfrak{C}$. Applying Lemma 1.3.12 again, we conclude that $L^\perp = J$. Therefore, $\mathcal{F}/J$ can be identified with a subalgebra of L^*. By the last condition on the class $\mathfrak{C}$, this implies that the coalgebra $(\mathcal{F}/J)^\circ$ is in $\mathfrak{C}$. But $(\mathcal{F}/J)^\circ \cong J^\perp$, so $J^\perp$ is in $\mathfrak{C}$. Hence $J^\perp \subset L$ by the definition of L (obviously, $L \subset L^{\perp\perp} = J^\perp$, so in fact $L = J^\perp$). We have proved that $D^\perp \supset J$, therefore, $D \subset D^{\perp\perp} \subset J^\perp \subset L$, hence D is in $\mathfrak{C}$. ∎

1.4 Relatively Free Coalgebras

In this section we assume the field $\Bbbk$ infinite.

We start by briefly recalling the notion of a relatively free algebra. Fix some system of polynomial identities S. Let $\mathbf{X} = \{X_i \,|\, i \in I\}$ be a set of varables indexed by a set I of any cardinality. Then the relatively free algebra $\mathcal{F}_{\mathfrak{A}}(\mathbf{X})$ of the variety $\mathfrak{A} = \mathrm{Var}(S)$ generated by $\mathbf{X}$ is defined by the same universal property as the (absolutely) free algebra, but we restrict our attention only to the algebras from $\mathfrak{A}$. Namely, $\mathcal{F}_{\mathfrak{A}}(\mathbf{X})$ must belong to $\mathfrak{A}$, and for any algebra $A \in \mathfrak{A}$ and any family $\{a_i\}_{i\in I}$ of elements of A, there must exist a unique algebra map $\Phi : \mathcal{F}_{\mathfrak{A}}(\mathbf{X}) \to A$ such that $\Phi(X_i) = a_i$, for all $i \in I$. The idea here is that we impose on the generators X_i, $i \in I$, only the relations that follow from the system of identities S (hence the term "relatively free").

To make a transition to coalgebras, we first need to replace the set $\mathbf{X}$ by the linear space $V = \langle \mathbf{X} \rangle$. Then the relatively free algebra $\mathcal{F}_{\mathfrak{A}}(\mathbf{X})$, which will be denoted $T_{\mathfrak{A}}(V)$ in this context, has the same universal property as the tensor algebra $T(V) = \mathcal{F}(\mathbf{X})$, but restricted to algebras from $\mathfrak{A}$ only: $T_{\mathfrak{A}}(V)$ must itself belong to $\mathfrak{A}$, and for any algebra $A \in \mathfrak{A}$ and any linear map $\varphi : V \to A$, there must exist a unique algebra map $\Phi : T_{\mathfrak{A}}(V) \to A$ extending φ, i.e. making the following diagram commute:

$$\begin{array}{ccc} T_{\mathfrak{A}}(V) & \overset{\Phi}{\dashrightarrow} & A \\ {\scriptstyle\varphi}\nwarrow & & \nearrow{\scriptstyle\eta} \\ & V & \end{array}$$

where η is the inclusion map. Dualizing this universal property gives the following relative version of Definition 1.2.1.

Definition 1.4.1. Let $\mathfrak{C}$ be a pseudo-variety of coalgebras. Let V be a vector space, C a coalgebra, $\theta : C \to V$ a linear map. The pair (C, θ) is called a *$\mathfrak{C}$-free coalgebra of V* if C belongs to $\mathfrak{C}$ and, for any coalgebra $D \in \mathfrak{C}$ and a linear map $\varphi : D \to V$, there exists a unique coalgebra map $\Phi : D \to C$ completing the commutative diagram:

$$\begin{array}{ccc} D & \overset{\Phi}{\dashrightarrow} & C \\ {\scriptstyle\varphi}\searrow & & \swarrow{\scriptstyle\theta} \\ & V & \end{array}$$

Such a $\mathfrak{C}$-free coalgebra is automatically unique, and we will denote it by $cT_{\mathfrak{C}}(V)$. The existence is also immediate: the largest subcoalgebra of the (absolutely) free coalgebra $cT(V)$ that belongs to $\mathfrak{C}$ obviously satisfies the universal property of $cT_{\mathfrak{C}}(V)$. Any coalgebra of the pseudo-variety $\mathfrak{C}$ can be imbedded in a suitable $\mathfrak{C}$-free coalgebra (just take any imbedding into an absolutely free coalgebra, the image will automatically lie in the corresponding $\mathfrak{C}$-free coalgebra).

From now on, we assume that $\mathfrak{C}$ is in fact a variety. We will give two realizations of $\mathfrak{C}$-free coalgebras: the first is an extension of M.Sweedler's result that $cT(V^*) = T(V)^\circ$, and the second is a more explicit construction inspired by the ideas of R.Block and P.Leroux.

Theorem 1.4.2. *Let $\mathfrak{C}$ be a variety of coalgebras and $\mathfrak{A}$ a variety of algebras defined by the same set of identities S. Then for any vector space V, the $\mathfrak{C}$-free coalgebra $cT_{\mathfrak{C}}(V^*)$ of V^* is naturally isomorphic to $T_{\mathfrak{A}}(V)^\circ$, where $T_{\mathfrak{A}}(V)$ is the relatively free algebra of the variety $\mathfrak{A}$ generated by a basis of V.*

Proof. As we observed, $cT_{\mathfrak{C}}(V^*)$ can be identified with the largest subcoalgebra $L \subset cT(V^*) = T(V)^\circ$ belonging to the class $\mathfrak{C}$. The calculation similar to the one in Lemma 1.3.12 shows that $L^\perp \subset T(V)$ coincides with the intersection J of the kernels of all algebra maps $\alpha : T(V) \to L^*$. Since L^* belongs to the variety $\mathfrak{A}$, the ideal J contains the intersection J' of the kernels of all algebra maps $\alpha : T(V) \to A$, for all $A \in \mathfrak{A}$.

Clearly, $T(V)/J'$ is nothing else but (a realization of) the $\mathfrak{A}$-free algebra $T_{\mathfrak{A}}(V)$. Now by Proposition 1.1.4, the coalgebra $(T(V))/J')^\circ$ belongs to $\mathfrak{C}$, but it is naturally isomorphic to the subcoalgebra $(J')^\perp \subset T(V)^\circ$, hence $(J')^\perp \subset L$ (since L is the largest). Therefore, $J = L^\perp \subset (J')^{\perp\perp}$. But since $T(V)/J'$ is residually finite-dimensional (by the same argument as in the proof of Proposition 1.3.5) and $(T(V)/J')^\circ = (J')^\perp$, we see that $(J')^{\perp\perp} = J'$. Hence $J \subset J'$, and we have already shown that $J \supset J'$, so $J = J'$.

Finally, since $J = L^\perp$, $L \subset L^{\perp\perp} = J^\perp$, but $J^\perp = (J')^\perp \subset L$, so we conclude that $L = J^\perp$ and thus L is naturally isomorphic to $(T(V)/J)^\circ = (T(V)/J')^\circ = (T_{\mathfrak{A}}(V))^\circ$. It remains to recall that L is (a realization of) $cT_{\mathfrak{A}}(V^*)$. ∎

For the second construction, recall that, for any graded algebra

$$A = \bigoplus_{n \geq 0} A_n$$

and a vector space V, we defined the generalized finite dual coalgebra A_V° (Definition 1.2.2). We will need the following criterion [10, Corollary 4] for a subspace of A_V° to be a subcoalgebra. First we introduce some notation.

Fix $b \in A_n$, then, for any graded linear map $f : A \to T(V)$ of degree 0, we can define the right translate $R_b f : A \to T(V)$ by $(R_b f)a = f(ab)$, for all $a \in A$. Similarly, the left translate $L_b f : A \to T(V)$ is defined by $(L_b f)a = f(ba)$, for all $a \in A$. Obviously, $R_b f$ and $L_b f$ are graded linear maps of degree n.

Now, fix a multilinear map $\varphi : V \times \ldots \times V \to \Bbbk$ in n variables. We can also view it as a linear map $\varphi : T^n(V) \to \Bbbk$, i.e. an element of $T^n(V)^*$. Using φ, we can "truncate" tensors from $T(V)$ in the following way. Define $Rtrunc_\varphi : T(V) \to T(V)$ by

$$Rtrunc_\varphi(v_1 \ldots v_m) = \begin{cases} 0 & \text{if } m < n, \\ v_1 \ldots v_{m-n}\varphi(v_{m-n+1}, \ldots, v_m) & \text{if } m \geq n. \end{cases}$$

Similarly,

$$Ltrunc_\varphi(v_1 \ldots v_m) = \begin{cases} 0 & \text{if } m < n, \\ \varphi(v_1, \ldots, v_n)v_{n+1} \ldots v_m & \text{if } m \geq n. \end{cases}$$

Clearly, $Rtrunc_\varphi$ and $Ltrunc_\varphi$ are graded linear maps of degree $-n$.

Definition 1.4.3. Fix $b \in A_n$ and $\varphi \in T^n(V)^*$. Then, for any graded linear map $f : A \to T(V)$ of degree 0, the composite maps $Rtrunc_\varphi \circ R_b f$ and

$Ltrunc_\varphi \circ L_b f$ are again graded of degree 0. We will call them the *right* and *left truncated translates of* f, respectively, and denote $R(b,\varphi)f$ and $L(b,\varphi)f$.

Recall from Definition 1.2.2 that the coalgebra A_V° consists of all graded linear functions $A \to T(V)$ of degree 0 that are representative.

Lemma 1.4.4. *Suppose $D \subset A_V^\circ$ is a subspace. Then D is a subcoalgebra iff $R(b,\varphi)D \subset D$ and $L(b,\varphi)D \subset D$, for all $b \in A_n$, $\varphi \in T^n(V)^*$, and $n \geq 0$.* ■

We are now ready for our construction. Recall $\mathcal{F} = T\langle X_1, X_2, \ldots\rangle$. We will denote by P_n the space of all multilinear polynomials in the first n variables, i.e.

$$P_n = \langle X_{\pi(1)} \ldots X_{\pi(n)} \mid \pi \in S_n \rangle.$$

As before, we can view $F \in P_n$ as an element of $\Bbbk S_n$, so $F = \sum_{\pi \in S_n} \lambda_\pi \pi$ acts on the tensors from $T^n(V)$ by the formula:

$$F \cdot (v_1 \ldots v_n) = \sum_{\pi \in S_n} \lambda_\pi v_{\pi^{-1}(1)} \ldots v_{\pi^{-1}(n)}.$$

Definition 1.4.5. Let $J \subset \mathcal{F}$ be a T-ideal generated by multilinear identities. Let A be a graded algebra and V a vector space. We will denote by $A_V^\circ(J)$ the space of all representative functions $f : A \to T(V)$ that satisfy, for all $n \geq 0$ and $a \in A_n$,

$$F \cdot f(a) = 0, \qquad \forall F \in J \cap P_n. \tag{1.4.1}$$

Specifying $J = 0$, we recover the whole A_V°. If J is generated by the identity $X_1X_2 - X_2X_1$, then a representative function $f : A \to T(V)$ belongs to

$A_V^\circ(J)$ iff $f(a)$ is a symmetric tensor, for all $a \in A_n$, $n \geq 0$ (such "symmetric-valued" representative functions were used in [10] to construct free cocommutative coalgebras). Note also that by Theorem 0.3.2, if $\operatorname{char} \Bbbk = 0$, then any T-ideal J is generated by multilinear identities.

Theorem 1.4.6. *Let J be a T-ideal generated by multilinear identities and V a vector space. Then $A_V^\circ(J)$ is a subcoalgebra of A_V°. Moreover, if A is commutative (in the ordinary, non-graded sense), then $A_V^\circ(J)$ satisfies all the identities from J.*

Proof. By Lemma 1.4.4, we have to prove that if $f \in A_V^\circ(J)$, $b \in A_m$, $\varphi \in T^m(V)^*$ $(m \geq 0)$, then $R(b,\varphi)f$, $L(b,\varphi)f \in A_V^\circ(J)$. For the right truncated translate, we have to show that, for any $n \geq 0$ and $a \in A_n$, $(R(b,\varphi)f)a$ satisfies (1.4.1), i.e. $F \cdot Rtrunc_\varphi(f(ab)) = 0$, for all $F \in J \cap P_n$. Fix $F = \sum_{\pi \in S_n} \lambda_\pi \pi \in J \cap P_n$.

Set $z = f(ab)$, it is a tensor of degree $n + m$, so we can write:

$$z = \sum_{(i)} \mu_{i_1,\ldots,i_{n+m}} v_{i_1} \cdots v_{i_{n+m}},$$

where $\{v_i\}$ is a basis of V. Thus we can compute:

$$Rtrunc_\varphi(z) = \sum_{(i)} \mu_{i_1,\ldots,i_{n+m}} v_{i_1} \cdots v_{i_n} \varphi(v_{i_{n+1}}, \ldots, v_{i_{n+m}}),$$

hence

$$\begin{aligned}
&F \cdot Rtrunc_\varphi(z) \\
&= \sum_{\pi\in S_n}\sum_{(i)} \lambda_\pi \mu_{i_1,\ldots,i_{n+m}} v_{i_{\pi^{-1}(1)}} \cdots v_{i_{\pi^{-1}(n)}} \varphi(v_{i_{n+1}},\ldots,v_{i_{n+m}}) \\
&= Rtrunc_\varphi\left(\sum_{\pi\in S_n}\sum_{(i)} \lambda_\pi \mu_{i_1,\ldots,i_{n+m}} v_{i_{\pi^{-1}(1)}} \cdots v_{i_{\pi^{-1}(n)}} v_{i_{n+1}} \cdots v_{i_{n+m}}\right) \\
&= Rtrunc_\varphi(\tilde{F} \cdot z),
\end{aligned}$$

where $\tilde{F} = \sum_{\pi\in S_n} \lambda_\pi \tilde{\pi}$ and $\tilde{\pi}$ is the permutation of $1,\ldots n+m$ that acts as π on $1,\ldots,n$ and leaves $n+1,\ldots,m$ intact.

Clearly, the identity $\sum_{\pi\in S_n} \lambda_\pi X_{\pi(1)}\ldots X_{\pi(n)} X_{n+1}\ldots X_{n+m} = 0$, corresponding to $\tilde{F}$, is a corollary of the identity $\sum_{\pi\in S_n} \lambda_\pi X_{\pi(1)}\ldots X_{\pi(n)} = 0$, corresponding to F. Therefore, $\tilde{F} \in J$. But since $f \in A_V^\circ(J)$, $z = f(ab)$ must satisfy $G \cdot f(ab) = 0$, for all $G \in J \cap P_{n+m}$, hence $\tilde{F} \cdot z = 0$, and we have proved that $R(b,\varphi)f$ is in $A_V^\circ(J)$. The proof for the left truncated translate is similar. Therefore, $A_V^\circ(J)$ is a subcoalgebra.

Now assume that A is commutative. We want to prove that $A_V^\circ(J)$ satisfies all the identities from J. Since J is generated by multilinear identities, it suffices to show that $A_V^\circ(J)$ satisfies all $F \in J \cap P_n$, for all n. Fix $F = \sum_{\pi\in S_n} \lambda_\pi \pi \in J \cap P_n$.

Recalling Definition 1.1.2, we have to prove that, for all $f \in A_V^\circ(J)$,

$$F \cdot \sum f_{(1)} \otimes \ldots \otimes f_{(n)} = 0. \tag{1.4.2}$$

Since $f_{(1)},\ldots,f_{(n)}$ are linear functions from A to $T(V)$, the left-hand side of (1.4.2) can be viewed as a linear function from $A^{\otimes n}$ to $T(V)^{\otimes n}$. Therefore, (1.4.2) is equivalent to the following:

$$\left\langle F \cdot \sum f_{(1)} \otimes \ldots \otimes f_{(n)}, a_1 \otimes \ldots \otimes a_n \right\rangle = 0, \qquad \forall a_1, \ldots, a_n \in A. \quad (1.4.3)$$

Clearly, it suffices to verify (1.4.3) only for homogeneous $a_1, \ldots, a_n$, say, of degrees $m_1, \ldots, m_n$, respectively. Then the left-hand side of (1.4.3) is an element of the space $T^{m_1}(V) \otimes \ldots \otimes T^{m_n}(V)$, which is naturally imbedded in $T^m(V)$, where $m = m_1 + \ldots + m_n$. Hence we can write, omitting, by our convention, the symbol $\otimes$ in the monomials from $T(V)$:

$$\begin{aligned} LHS &= \sum_{\pi \in S_n} \lambda_\pi \left\langle \sum f_{(\pi^{-1}(1))} \otimes \ldots \otimes f_{(\pi^{-1}(n))}, a_1 \otimes \ldots \otimes a_n \right\rangle \\ &= \sum_{\pi \in S_n} \lambda_\pi \sum \langle f_{(\pi^{-1}(1))}, a_1 \rangle \ldots \langle f_{(\pi^{-1}(n))}, a_n \rangle. \qquad (1.4.4) \end{aligned}$$

Now, for any permutation π of $1, \ldots, n$, we define a permutation $\tilde{\pi}$ of $1, \ldots, m$ in the following way:

$$\begin{array}{lclclcl} \tilde{\pi}(1) &=& M_{\pi(1)-1} + 1, & \ldots, & \tilde{\pi}(m - m'_n + 1) &=& M_{\pi(n)-1} + 1, \\ \tilde{\pi}(2) &=& M_{\pi(1)-1} + 2, & \ldots, & \tilde{\pi}(m - m'_n + 2) &=& M_{\pi(n)-1} + 2, \\ \ldots, & & & \ldots, & & & \ldots, \\ \tilde{\pi}(m'_1) &=& M_{\pi(1)-1} + m'_1, & \ldots, & \tilde{\pi}(m) &=& M_{\pi(n)-1} + m'_n, \end{array}$$

where $m'_i = m_{\pi(i)}$ and $M_i = m_1 + \ldots + m_i$, for $i = 1, \ldots, n$. Loosely speaking, $\tilde{\pi}$ permutes the blocks of sizes $m_1, \ldots, m_n$ according to the action of π on $1, \ldots, n$. Then we can continue with (1.4.4) as follows:

$$LHS = \sum_{\pi \in S_n} \lambda_\pi \sum \tilde{\pi} \cdot \left(\langle f_{(1)}, a_{\pi(1)} \rangle \ldots \langle f_{(n)}, a_{\pi(n)} \rangle \right). \qquad (1.4.5)$$

By the iterated (1.2.1), we have:

$$\langle f, b_1 \ldots b_n \rangle = \sum \langle f_{(1)}, b_1 \rangle \ldots \langle f_{(n)}, b_n \rangle,$$

hence (1.4.5) gives, with $b_i = a_{\pi(i)}$:

$$LHS = \sum_{\pi \in S_n} \lambda_\pi \tilde{\pi} \cdot \langle f, a_{\pi(1)} \dots a_{\pi(n)} \rangle = \sum_{\pi \in S_n} \lambda_\pi \tilde{\pi} \cdot \langle f, a_1 \dots a_n \rangle \qquad (1.4.6)$$

by commutativity of A. Thus we have rewritten the left-hand side of (1.4.2) as $\tilde{F} \cdot f(a_1 \dots a_n)$, where $\tilde{F} = \sum_{\pi \in S_n} \lambda_\pi \tilde{\pi} \in \Bbbk S_m$.

It remains to observe that the identity $\sum_{\pi \in S_n} \lambda_\pi X_{\tilde{\pi}(1)} \dots X_{\tilde{\pi}(n)} = 0$, corresponding to $\tilde{F}$, follows from the identity $\sum_{\pi \in S_n} \lambda_\pi X_{\pi(1)} \dots X_{\pi(n)} = 0$, corresponding to F, by substitution of $X_1 \dots X_{m_1}$ for X_1, and so on, $X_{m-m_n+1} \dots X_m$ for X_n (here we substitute 1 for X_i in the case $m_i = 0$). Hence $\tilde{F} \in J$ and $\tilde{F} \cdot f(a_1 \dots a_n) = 0$ since $f \in A_V^\circ(J)$. ∎

Corollary 1.4.7. *Let J be a T-ideal generated by multilinear identities and V a vector space. Then $\Bbbk[t]_V^\circ(J)$ is the* cVar(J)*-free coalgebra of V.*

Proof. By Theorem 1.4.6, $\Bbbk[t]_V^\circ(J)$ is a subcoalgebra of $\Bbbk[t]_V^\circ$, which belongs to cVar(J). It is the largest such subcoalgebra since if $f \in \Bbbk[t]_V^\circ$ satisfies

$$F \cdot \sum f_{(1)} \otimes \dots \otimes f_{(n)} = 0, \qquad (1.4.7)$$

for some $F \in P_n$, then we have:

$$F \cdot f(t^n) = F \cdot \left(\sum f_{(1)}(t) \dots f_{(n)}(t) \right) = 0,$$

whence if f satisfies (1.4.7), for all $n \geq 0$ and $F \in J \cap P_n$, then f is in $\Bbbk[t]_V^\circ(J)$. It remains to recall that $\Bbbk[t]_V^\circ$ is the (absolutely) free coalgebra of V. ∎

Using the natural imbedding of the absolutely free coalgebra $cT(V) = \Bbbk[t]_V^\circ$ into $\hat{T}(V)$, we obtain a realization of the cVar(J)-free coalgebra

$$cT_{\mathrm{cVar}(J)}(V) = \Bbbk[t]_V^\circ(J) \subset \hat{T}_J(V),$$

where $\hat{T}_J(V)$ consists of all formal sums $f_0 + f_1 + \ldots$ such that $f_n \in T^n(V)$ satisfies the "symmetry conditions" $F \cdot f_n = 0$, for all $F \in J \cap P_n$.

1.5 Some Examples

When we study a bialgebra (in particular, a Hopf algebra), it will be convenient to use the term *coidentities* for the identities of the underlying coalgebra, and simply *identities* for the identities of the underlying algebra.

Example 1.5.1. Consider the family of Hopf algebras $H(n, \xi)$ constructed by Taft [35]. Let n be a natural number and $\xi \in \Bbbk$ a primitive n-th root of unity (hence $\operatorname{char} \Bbbk \nmid n$). As an algebra,

$$H(n, \xi) = alg\langle x, g \mid x^n = 0, g^n = 1, gx = \xi xg\rangle.$$

The coalgebra structure is defined by

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

i.e., g is group-like, x is $(g, 1)$-primitive. Then the T-ideal of identities of $H(n, \xi)$ coincides with the T-ideal of coidentities and is generated by the identity

$$(X_1X_2 - X_2X_1)\ldots(X_{2n-1}X_{2n} - X_{2n}X_{2n-1}) = 0. \qquad (1.5.1)$$

In particular, $H(n, \xi)$ does not satisfy any identities or coidentities of degree $< 2n$.

Proof. It can be shown that the comultiplication of $H(n, \xi)$ is well-defined, and $H(n, \xi)$ is in fact a Hopf algebra with counit $\varepsilon(x) = 0$, $\varepsilon(g) = 1$ and antipode $S(x) = -xg^{-1}$, $S(g) = g^{-1}$ (see e.g. [31]). Furthermore,

$$\{x^i g^j \mid 0 \leq i, j < n\}$$

is a basis of $H(n, \xi)$ over $\Bbbk$, and so $\dim H(n, \xi) = n^2$. The Taft's algebras $H(n, \xi)$ are pointed and also self-dual, i.e. $H(n, \xi)^* \cong H(n, \xi)$ (see [31]). Thus we have to prove only that (1.5.1) is a basis of identities for $H(n, \xi)$ as an algebra, i.e. all identities follow from (1.5.1).

Since any commutator of elements of $H(n, \xi)$ is either 0 or has a factor x, and $x^n = 0$, the algebra $H(n, \xi)$ satisfies the identity (1.5.1). It is a well-known fact that (1.5.1) is a basis of identities for the algebra $UT(n)$ of upper triangular $n \times n$ matrices (see e.g. [24]). We will prove that the algebra $UT(n)$ can be imbedded into $H(n, \xi)$, which gives the desired result.

Set $E_{ij} = x^{j-i} e_j$, $0 \leq i \leq j < n$, where $e_j = \frac{1}{n} \sum_{s=0}^{n-1} (\xi^j g)^s$ are the orthogonal idempotents of the group algebra of the cyclic group $\langle g \rangle_n$. From the form of the basis of $H(n, \xi)$ mentioned above, it follows that E_{ij} are linearly independent.

Since $e_j x^l = x^l e_{j+l \pmod n}$, $0 \leq j, l < n$, we can compute:

$$E_{ij} E_{pq} = x^{j-i} e_j x^{q-p} e_q = x^{j+q-i-p} e_{j+q-p \pmod n} e_q = \delta_{jp} x^{q-i} e_q = \delta_{jp} E_{iq},$$

where $0 \leq i \leq j < n, 0 \leq p \leq q < n$, and δ_{jp} is the Kronecker symbol.

Therefore, the span of E_{ij}, $0 \leq i \leq j < n$, is a subalgebra of $H(n, \xi)$ isomorphic to $UT(n)$. ■

Now we will look at a few simple examples of relatively free coalgebras that can be explicitly computed. Recall from Remark 1.2.5 that the (absolutely) free coalgebra $cT(V)$ has a natural structure of a commutative Hopf algebra. In our realization of $cT(V)$ as a subspace of $\hat{T}(V)$, the multiplication of $cT(V)$ is the restriction of the *shuffle product* on $\hat{T}(V)$, which we denote by $\star$ to avoid confusion with the tensor product (that *does not* respect comultiplication in the sense of Definition 0.2.1). The shuffle product on $\hat{T}(V)$ is defined by extending the following formula for monomials by linearity and continuity:

$$v_1 \dots v_m \star v_{m+1} \dots v_n = \sum_{\pi \in Sh(m,n-m)} \pi \cdot (v_1 \dots v_n) \qquad (1.5.2)$$
$$\forall v_1, \dots, v_n \in V,\ n \geq 0,\ 0 \leq m \leq n,$$

where $Sh(m, n-m)$ is the set of all $(m, n-m)$-shuffles, i.e. permutations of $1, \dots, n$ preserving the order of $1, \dots m$ and $m+1, \dots, n$: $\pi(1) < \dots < \pi(m)$ and $\pi(m+1) < \dots < \pi(n)$. The antipode is defined by

$$S(v_1 \dots v_n) = (-1)^n v_n \dots v_1, \qquad \forall v_1, \dots v_n \in V,\ n \geq 0.$$

Example 1.5.2. Recall the pseudo-variety Grp of Example 1.3.6. The relatively free coalgebra $cT_{Grp}(V)$ is spanned by the set $G(cT(V))$ of all group-like elements of $cT(V)$, which is in one-to-one correspondence with V by virtue of the map

$$e : V \to cT(V) : v \to e(v) = 1 + v + v^2 + v^3 + \dots,$$

where v^2 is the monomial $v \otimes v$, etc.

Proof. Using (1.2.2), we immediately see that $e(v)$ is indeed group-like, for any $v \in V$. Conversely, if $g \in G(cT(V))$, then by the iterated (1.2.1), the degree n component $g_n = g(t^n) = \sum g_{(1)}(t) \dots g_{(n)}(t) = (g(t))^n = (g_1)^n$, hence $g = e(v)$ for $v = g_1$. ∎

Moreover, the map $e : V \to G(cT(V))$ above is an isomorphism of the underlying additive group of V and the group (under $\star$) of group-like elements of $cT(V)$ (see [9, Section 2]). It is also proved in [9] that the irreducible component of $1 = 1 + 0 + 0 + \dots$ in $cT(V)$ is equal to $T(V)$. It is obviously a subHopfalgebra of $cT(V)$.

Recall from Example 1.3.7 that the class Pnt of all pointed coalgebras is a pseudo-variety, and so there exists the largest pointed subcoalgebra of $cT(V)$, which is (a realization of) the relatively free coalgebra $cT_{Pnt}(V)$. Since the explicit computation of $cT_{Pnt}(V)$ seems to be difficult, we will look at the following pseudo-variety which is contained in Pnt. The class $Conn$ of all connected coalgebras is closed under isomorphisms, subcoalgebras and factors (the proof as in Example 1.3.7 for pointed coalgebras). Clearly, it is not closed under direct sums, so we introduce the class $\Sigma Conn$ of all coalgebras that are sums of their connected subcoalgebras.

Example 1.5.3. The class $\Sigma Conn$ introduced above is a pseudo-variety, whose relatively free coalgebra $cT_{\Sigma Conn}(V)$ is a subHopfalgebra of $cT(V)$ isomorphic to $T(V) \otimes \Bbbk(V, +)$ via $z \otimes v \to z \star e(v)$.

Proof. By Lemma 0.1.10, if a coalgebra C is a sum of connected subcoalgebras, it is a direct sum of maximal connected subcoalgebras: $C = \bigoplus_i C_i$, hence any subcoalgebra $D \subset C$ is the direct sum of connected coalgebras $D \cap C_i$ (cf. proof of Example 1.3.6). All other properties necessary to make $\Sigma Conn$ a pseudo-variety are obvious.

By Remark 0.2.8, we obtain that the sum of all connected subcoalgebras of $cT(V)$ is a subHopfalgebra isomorphic to $cT(V)_1 \# \Bbbk G(cT(V))$ via $z \# g \to z \star g$, where $cT(V)_1$ is the irreducible component of 1. It remains to recall the structure of $G(cT(V))$ and $cT(V)_1$ and the fact that $\star$ is commutative. ■

Finally, let us describe the free cocommutative coalgebra $cT_{Cocomm}(V)$, which we will denote by $cT_{sym}(V)$, because it consists of all elements of $cT(V)$ $f = f_0 + f_1 + \ldots$ such that all f_n are symmetric tensors. We denote the space of symmetric tensors of degree n by $T^n_{sym}(V)$. The following description is given in [9, Section 4] (where it is partly attributed to M.Sweedler).

Since the irreducible component of 1 in $cT(V)$ is $T(V)$, the irreducible component of 1 in $cT_{sym}(V)$ is $cT_{sym}(V) \cap T(V) = T_{sym}(V)$, where

$$T_{sym}(V) = \bigoplus_{n \geq 0} T^n_{sym}(V).$$

Choose a basis $\{x_i \mid i \in I\}$ of the space V, indexed by a set I and fix some linear order on I. Consider multiindices $\alpha \in \mathbb{Z}_+^{(I)}$ as defined in Section 0.4, then $T(V)$ has a basis of monomials $\mathbf{x}^\alpha = \prod_{i \in I} x^{\alpha(i)}$ (meaning tensor product performed according to the order of I). To construct a basis for $T_{sym}(V)$, consider the orbit $Orb_{S_{|\alpha|}}(\mathbf{x}^\alpha)$ of $\mathbf{x}^\alpha$ under the usual action of $S_{|\alpha|}$ on $T^{|\alpha|}(V)$ and set

$$z^{(\alpha)} = \sum_{z \in Orb_{S_{|\alpha|}}(\mathbf{x}^\alpha)} z.$$

Clearly, $\{z^{(\alpha)} \mid \alpha \in \mathbb{Z}_+^{(I)}\}$ is a basis for $T_{sym}(V)$.

Now the formula (1.2.2) for comultiplication of $cT(V)$ implies that

$$\Delta z^{(\alpha)} = \sum_{\beta + \gamma = \alpha} z^{(\beta)} \otimes z^{(\gamma)}, \qquad \forall \alpha \in \mathbb{Z}_+^{(I)}. \tag{1.5.3}$$

The counit of $T_{sym}(V)$ is given by $\varepsilon(z^{(\alpha)}) = 0$ if $\alpha \neq 0$ and $\varepsilon(z^{(0)}) = 1$.

As to multiplication, (1.5.2) gives

$$z^{(\alpha)} \star z^{(\beta)} = \binom{\alpha + \beta}{\alpha} z^{(\alpha+\beta)}, \qquad \forall \alpha, \beta \in \mathbb{Z}_+^{(I)}. \tag{1.5.4}$$

The unit of $T_{sym}(V)$ is $z^{(0)}$, and the antipode is given by

$$Sz^{(\alpha)} = (-1)^{|\alpha|}z^{(\alpha)}, \qquad \forall \alpha \in \mathbb{Z}_+^{(I)}.$$

Definition 1.5.4. Let I be a set. The Hopf algebra $D(I)$ with a basis $\{z^{(\alpha)}\}$ indexed by $\alpha \in \mathbb{Z}_+^{(I)}$ and comultiplication and multiplication defined by (1.5.3) and (1.5.4), respectively, is called the *divided power algebra* with index set I.

Hence we obtained that the irreducible component $cT_{sym}(V)_1 = T_{sym}(V)$ is isomorphic to the divided power algebra $D(I)$, where $V = \langle x_i \mid i \in I \rangle$.

Now we put all facts together and apply Theorem 0.2.7:

Example 1.5.5. Let V be a vector space with a basis indexed by a set I (i.e. $\dim V = |I|$). The relatively free coalgebra $cT_{\mathfrak{C}}(V)$ of the pseudo-variety $\mathfrak{C} = Cocomm \cap Pnt$ is a subHopfalgebra of $cT(V)$ isomorphic to $D(I) \otimes \Bbbk(V, +)$ via $z \otimes v \to z \star e(v)$.

In particular, if $\Bbbk$ is algebraically closed, then $\mathfrak{C} = Cocomm$ and we obtain an explicit description of the free cocommutative coalgebra $cT_{sym}(V)$. We will return to divided power algebras in Chapters 2 and 4.

Chapter 2

Cocommutative Hopf Algebras with a Polynomial Identity

2.1 Overview of Known Results

In this section we summarize known results giving necessary and sufficient conditions for certain kinds of algebras, which are in fact examples of cocommutative Hopf algebras, to be PI, i.e. to satisfy a nontrivial polynomial identity. The following sections will be devoted to the question of determining when a general cocommutative Hopf algebra is PI (as an algebra). We will give the complete answer in the case of zero characteristic and some partial results in prime characteristic.

The simplest example of a cocommutative Hopf algebra is the group algebra $\Bbbk G$ of a group G (see Section 0.2). The problem of determining when $\Bbbk G$ is PI was attempted by a number of authors (see references in [26]). In 1972, D.Passman published the following final result [26]. In the statement of this theorem a group A is called *p-Abelian* if the commutator subgroup A' is a finite p-group (where p is a prime).

Theorem 2.1.1. *Let G be a group, $\Bbbk$ a field. Then the group algebra $\Bbbk G$ is PI iff there exists a subgroup $A \subset G$ of finite index such that A is Abelian in the case* $\operatorname{char} \Bbbk = 0$ *and p-Abelian in the case* $\operatorname{char} \Bbbk = p$. *Moreover, the subgroup A can be chosen characteristic (i.e. invariant under all automorphisms of G).* ∎

Remark 2.1.2. As V.Petrogradsky pointed out to me, in the theorem above we can also assume A' Abelian (just replace A by the centralizer $C_A(A')$). This observation makes Theorem 2.1.4 below look completely analogous to Theorem 2.1.1.

The next example of a cocommutative Hopf algebra that we gave in Section 0.2 was the universal envelope $U(L)$ of a Lie algebra L. For finite-dimensional L and characteristic 0, the answer to when $U(L)$ is *PI* was given by V.Latyšev [23] in 1963, and then Yu.Bahturin [2] in 1974 extended that result to arbitrary L and also gave the answer in prime characteristic. Here we will only need universal envelopes in the case of characteristic 0, since in the context of Hopf algebras, it is more natural to consider restricted envelopes in prime characteristic (see Remark 2.1.8 below).

Theorem 2.1.3. *Let L be a Lie algebra over a field $\Bbbk$,* $\operatorname{char} \Bbbk = 0$. *Then the universal enveloping algebra $U(L)$ is PI iff L is Abelian.* ∎

Recall that a Lie algebra L over a field $\Bbbk$ of characteristic p with an additional operation $[p] : L \to L : x \to x^{[p]}$ is called a *p-Lie algebra* if

1) $(\lambda x)^{[p]} = \lambda^p x^{[p]}$, $\lambda \in \Bbbk$, $x \in L$;

2) $\mathrm{ad} x^{[p]} = (\mathrm{ad} x)^p$, $x \in L$;

3) $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{k=1}^{p-1} s_k(x,y)$, $x, y \in L$, where $ks_k(x,y)$ is the coefficient of t^{k-1} in the polynomial $(\mathrm{ad}(tx+y))^{p-1}(x) \in L[t]$.

If L is a p-Lie algebra, then the *restricted enveloping algebra* $u(L)$ is defined in the same way as $U(L)$, but the following additional relations are imposed: $x^p = x^{[p]}$, for all $x \in L$. There is a version of Poincaré-Birkhoff-Witt Theorem for restricted envelopes (see e.g. [1]). Given a linearly ordered basis $\{x_i \mid i \in I\}$ of L, the ordered monomials with powers $< p$ (hence the name "restricted"):

$$x_{i_1}^{n_1} \dots x_{i_k}^{n_k},\ i_1 < \dots i_k,\ 0 \le n_1, \dots, n_k < p,\ k = 0, 1, \dots,$$

form a basis of $u(L)$. From now on, we will simply write x^p for $x^{[p]}$, $x \in L$, since they define the same element of $u(L)$. The restricted envelope $u(L)$ can be endowed with a Hopf algebra structure in the same way as $U(L)$, i.e. by defining $\Delta x = x \otimes 1 + 1 \otimes x$ for all $x \in L$.

The following criterion was proved independently by V.Petrogradsky [29] and D.Passman [27].

Theorem 2.1.4. *Let L be a p-Lie algebra over a field $\Bbbk$, $\operatorname{char} \Bbbk = p$. Then the restricted enveloping algebra $u(L)$ is PI iff there exist p-ideals $Q \subset B \subset L$ such that*

1) $\dim L/B < \infty$, $\dim Q < \infty$,

2) B/Q is Abelian,

3) Q is Abelian with nilpotent operation $[p]$.

∎

Remark 2.1.5. As shown in [6], the ideals Q and B can also be chosen invariant under all automorphisms of L.

Now recall the Decomposition Theorem 0.2.7 for pointed cocommutative Hopf algebras. Since the condition of pointedness is automatically satisfied if $\Bbbk$ is algebraically closed, this theorem represents any cocommutative Hopf algebra H over such a field as the smash product of a connected cocommutative Hopf algebra H_1 and the group algebra $\Bbbk G$, where the group $G = G(H)$ acts on H_1 by Hopf algebra automorphisms.

Definition 2.1.6. For brevity, and following P.Cartier [12], we will use the term *hyperalgebra* for any connected cocommutative bialgebra. The existence of the antipode for such bialgebras is automatic (see e.g. [14, 2.2.8]), so they are in fact Hopf algebras.

In characteristic 0, we know that any hyperalgebra is just a universal enveloping algebra. Namely, H_1 is isomorphic to the universal envelope $U(L)$ of the Lie algebra $L = P(H)(= P(H_1))$ of primitive elements (Theorem 0.2.7 again). Thus over an algebraically closed field of characteristic 0, our question of determining when a cocommutative Hopf algebra is PI reduces to the same question for the smash product $U(L)\#\Bbbk G$ of a universal enveloping algebra $U(L)$ and a group algebra $\Bbbk G$, where G acts on L by automorphisms. This smash product is nothing else but the skew group ring of G with coefficients in $U(L)$. Since $U(L)$ is a prime ring (even an integral domain), many results on skew group rings can be applied to derive the following criterion when $U(L)\#\Bbbk G$ is PI. For the most general results of this nature see e.g. [28, Section 5.23], where the ring of coefficients is just G-semiprime and the multiplication of elements of G may be "twisted" by a cocycle.

Theorem 2.1.7. *Let L be a Lie algebra over $\Bbbk$, $\operatorname{char}\Bbbk = 0$. Let G be a group acting on L by automorphisms. Then the smash product $U(L)\#\Bbbk G$ is PI iff*

1) *L is Abelian, and*

2) *there exists a normal Abelian subgroup $A \subset G$ of finite index such that A acts trivially on L.*

■

We will prove this criterion in Section 2.2, using an elegant result from [16]. An elementary proof was given by the author in [19]. In Section 2.2, we will also show how we can get rid of the hypothesis that $\Bbbk$ is algebraically closed.

Now we pass to the case of prime characteristic p. Here the space of primitive elements $P(H)$ of a Hopf algebra H is closed not only under the commutator, but also under the p-th power, so $L = P(H)$ is a p-Lie algebra. By the universal property of $u(L)$, we can extend the inclusion $L \hookrightarrow H$ to an algebra map $\varphi : u(L) \to H$, which will be in fact a Hopf algebra map since $\Delta\varphi(x) = x \otimes 1 + 1 \otimes x = (\varphi \otimes \varphi)\Delta x$ and $S\varphi(x) = -x = \varphi(Sx)$, for all $x \in L$, and L generates $u(L)$ as an algebra. Moreover, by [25, Proposition 5.5.3], $u(L)$ is connected and $P(u(L)) = L$. Thus by Corollary 0.1.15, φ is injective since so is its restriction to L.

Remark 2.1.8. For $H = U(L)$, we have $P(H) = L$ only if $\operatorname{char} \Bbbk = 0$. If $\operatorname{char} \Bbbk = p > 0$, $P(H)$ is the p-hull

$$\langle L \rangle_p = \langle x^{p^n} \mid x \in L,\, n \geq 0 \rangle$$

of L (see [25, Proposition 5.5.3] again). This explains why it is more convenient to work with restricted envelopes rather than with universal envelopes when we study Hopf algebras. Universal envelopes are also included this way, because $U(L) = u(\langle L \rangle_p)$.

We have just shown that $u(L) \hookrightarrow H$. Since $u(L)$ is connected, it is in fact contained in the connected component H_1. Unlike the case of characteristic 0, where for any cocommutative Hopf algebra H, we have $H_1 = U(L)$, here the hyperalgebra H_1 does not have to be equal to $u(L)$. Since $u(L)$ is generated by L, H_1 equals $u(L)$ iff it is *primitively generated*, i.e. generated, as an algebra, by primitive elements. Divided power algebras $D(I)$ introduced in Chapter 1 (see Definition 1.5.4) provide examples of hyperalgebras which are not primitively generated. Taking for simplicity a one-element set I, we get $D = \langle z^{(n)} \mid n \geq 0 \rangle$, with comultiplication

$$\Delta z^{(n)} = \sum_{k=0}^{n} z^{(k)} \otimes z^{(n-k)}$$

and multiplication

$$z^{(k)} z^{(l)} = \binom{k+l}{k} z^{(k+l)}.$$

Hence $P(D)$ is the one-dimensional subspace spanned by $z^{(1)}$, but $(z^{(1)})^p = 0$, so $P(D)$ generates only the subHopfalgebra

$$\langle 1 = z^{(0)}, z^{(1)}, \ldots, z^{(p-1)} \rangle.$$

The answer in the case of primitively generated H_1 (i.e. H_0 of *coheight 0*, according to Definition 2.3.2) was given by Yu.Bahturin and V.Petrogradsky [6, Theorem 3.1].

Theorem 2.1.9. *Suppose that a group G acts by automorphisms on a p-Lie algebra L. Then $u(L)\#\Bbbk G$ is PI iff*

1) there exist G-invariant p-subalgebras $Q \subset B \subset L$ with

  (a) $\dim L/B < \infty$, $\dim Q < \infty$,

  (b) $[B, B] \subset Q$,

  (c) Q is Abelian with nilpotent operation $[p]$;

2) there exists a subgroup $A \subset G$ with

  (a) $(G : A) < \infty$,

  (b) A' is a finite Abelian p-group;

3) A acts trivially on B/Q.

■

Remark 2.1.10. Note that the ring of coefficients $u(L)$ of the skew group ring $u(L)\#\Bbbk G$ need not be semiprime, so the results of [28] on PI skew group rings cannot be applied.

In the present work, we will look at the case, which is, in a sense, opposite to the primitively generated case, namely, when H_1 is *coreduced* (see Definition 2.3.3) and thus has *infinite coheight*. It turns out that such hyperalgebras are similar to universal enveloping algebras of characteristic 0.

We will obtain, in passing, a new proof of Theorem 2.1.3 that presents it as a corollary of Theorem 2.1.1.

To conclude this introductory section, we obtain a somewhat unexpected corollary of Theorems 2.1.3 and 2.1.4 (cf. the examples at the end of Chapter 1).

Proposition 2.1.11. *Let $\mathcal{F}$ be the free algebra (associative with 1) in countably many variables $X_1, X_2, \ldots$ over an infinite field $\Bbbk$. Then $\mathcal{F}$ has a natural structure of a cocommutative Hopf algebra defined by $\Delta X_i = X_i \otimes 1 + 1 \otimes X_i$, for all i (as in Remark 1.2.5). Suppose J is a T-ideal of $\mathcal{F}$. Then J is a Hopf ideal iff $J = 0$ or $J = \mathcal{F}$ or J is generated by $X_1X_2 - X_2X_1$ as a T-ideal.*

Proof. The nontrivial part is to prove that if a T-ideal $J \neq 0$ is a Hopf ideal, then J contains $[X_1, X_2]$, because then either J is generated by $[X_1, X_2]$ as a T-ideal or $J = \mathcal{F}$ by Corollary 0.3.3.

First assume that $\operatorname{char} \Bbbk = 0$. We represent $\mathcal{F} = U(\mathcal{L})$, where $\mathcal{L}$ is the free Lie algebra generated by $X_1, X_2, \ldots$ Let $\pi : \mathcal{F} \to \mathcal{F}/J$ be the factorization map. Then the connected Hopf algebra $\mathcal{F}/J$ is generated as an algebra by the Lie subalgebra $\pi(\mathcal{L})$ of $P(\mathcal{F}/J)$. Since $\mathcal{F}/J = U(P(\mathcal{F}/J))$, we see that $\pi(\mathcal{L})$ must be equal to $P(\mathcal{F}/J)$, and so $\mathcal{F}/J = U(\pi(\mathcal{L}))$. Since $J \neq 0$, the algebra $\mathcal{F}/J$ is PI, hence by Theorem 2.1.3, $\pi(\mathcal{L})$ is Abelian, which implies that J contains $[X_1, X_2]$.

If $\operatorname{char} \Bbbk = p > 0$, we represent $\mathcal{F} = u(\mathcal{L})$, where $\mathcal{L}$ is now the free p-Lie algebra generated by $X_1, X_2, \ldots$ By a similar argument, we obtain that $\mathcal{F}/J = u(\mathcal{L}/I)$, where $I = J \cap \mathcal{L}$ is a p-Lie ideal of $\mathcal{L}$. By Theorem 2.1.4, we can find p-Lie ideals $Q \subset B \subset \mathcal{L}$ containing I such that $\dim \mathcal{L}/B < \infty$, B/Q is Abelian, and Q/I is finite-dimensional Abelian with nilpotent operation $[p]$.

Moreover, we may assume B and Q invariant under all automorphisms of $\mathcal{L}$ that preserve I. In particular, B and Q are invariant under a linear change of variables, because any such change preserves I: $I = J \cap \mathcal{L}$ and J is a T-ideal. Since $\dim \mathcal{L}/B < \infty$, B must contain a nontrivial linear combination of the variables $X_1, X_2, \dots$ Performing an appropriate linear change, we conclude that B contains X_1 and similarly, all other variables. Since B/Q is Abelian, we obtain that $[X_i, X_j] \in Q$, for all i, j. But recall that $\dim Q/I < \infty$, hence I must contain a nontrivial linear combination of $[X_i, X_j]$. Therefore, the T-ideal J contains a nontrivial polynomial identity of degree 2, hence by Theorem 0.3.2, a nontrivial multilinear identity of degree 2. Any such identity, written in the variables X_1 and X_2, has the form $\lambda X_1 X_2 + \mu X_2 X_1$, for some $\lambda, \mu \in \Bbbk$ not simultaneously 0. Upon substitution $X_1 = X_2 = 1$, it follows that either $J = \mathcal{F}$ or $\lambda + \mu = 0$ and thus J contains $[X_1, X_2]$. ■

2.2 The Case of Zero Characteristic

The goal of this section is to generalize Passman's criterion for group algebras (Theorem 2.1.1) to cocommutative Hopf algebras in the case of characteristic 0 (see the equivalence of 1) and 2) in Theorem 2.2.9). First we obtain Theorem 2.1.7 that immediately gives the desired result if a cocommutative Hopf algebra H is decomposed to a smash product as in Theorem 0.2.7, e.g. over an algebraically closed field. Then we extend our criterion to arbitrary fields of characteristic 0 and also give it a form that does not explicitly involve the decomposition to a smash product.

Definition 2.2.1. Let R be a prime ring. Then the ring $Q_s = Q_s(R)$ is called the *symmetric Martindale ring of quotients* if

1) $Q_s(R) \supset R$ with the same 1,

2) if $q \in Q_s$, then there exist $0 \neq I, J \lhd R$ with $Iq, qJ \subset R$,

3) if $q \in Q_s$ and $0 \neq I \lhd R$, then either of $Iq = 0$ or $qI = 0$ implies $q = 0$,

4) let $f : {}_RI \to {}_RR$ and $g : J_R \to R_R$ be given with $0 \neq I, J \lhd R$ and suppose that for all $a \in I$ and $b \in J$, we have $(af)b = a(gb)$ (where we write left module maps on the right and vice versa), then there exists $q \in Q_s(R)$ with $af = aq$ and $gb = qb$, for all $a \in I$, $b \in J$.

The ring $Q_s(R)$ exists and is uniquely defined by the properties listed above (see e.g. [28, Chapter 3]). If R is a PI ring, then the Theorem of Posner, Rowen et al. (see e.g. [18, Section 1.11]) implies that Q_s coincides with the ring of central quotients of R(=the left classical ring of quotients=the right classical ring of quotients).

Definition 2.2.2. Let σ be an automorphism of a prime ring R. Then σ is said to be *X-inner* if there exists an invertible element $q \in Q_s(R)$ such that σ is the restriction to R of the inner automorphism $x \to qxq^{-1}$ of $Q_s(R)$.

We can now state the following result due to D.Handelman, J.Lawrence and W.Schelter [16, Theorem 2.3] (these authors use the term "inner" for the automorphisms of a prime PI ring that we now call "X-inner").

Theorem 2.2.3. *Let R be a prime PI ring. Suppose a group G acts on R by automorphisms. Then the skew group ring RG is PI iff there exists a* *subgroup $A \subset G$ of finite index such that A acts on R by X-inner automorphisms and A is Abelian in the case* $\operatorname{char} R = 0$ *and p-Abelian in the case* $\operatorname{char} R = p > 0$. ■

Proof of Theorem 2.1.7. Apply the theorem above with $R = U(L)$, which is always a domain, and recall that $U(L)$ is PI iff L is Abelian (Theorem 2.1.3), in which case $Q_s(U(L))$ is just a field of rational functions that has no nontrivial inner automorphisms. ■

We will need a version of Theorem 0.2.7 that does not require pointedness (which is not automatic over a non algebraically closed field). But first we prove two lemmas.

Lemma 2.2.4. *Let $L/\Bbbk$ be a separable field extension, C a coalgebra over $\Bbbk$. Then* $\operatorname{corad}(C \otimes L) = (\operatorname{corad} C) \otimes L$.

Proof. The inclusion $\operatorname{corad}(C \otimes L) \subset (\operatorname{corad} C) \otimes L$ holds for any field extension and can be deduced e.g. from Lemma 0.1.12. Assuming L/k separable, since $\operatorname{corad} C$ is a sum of simple subcoalgebras, then so is $(\operatorname{corad} C) \otimes L$, because any simple coalgebra is finite-dimensional (due to Theorem 0.1.8) and hence dual to a finite-dimensional simple algebra, that remains simple upon tensoring with L. But this implies $(\operatorname{corad} C) \otimes L \subset \operatorname{corad}(C \otimes L)$. ■

Lemma 2.2.5. *Let C be a coalgebra over $\Bbbk$, $D \subset C$ a simple subcoalgebra. Denote* $\operatorname{Irr} D$ *the irreducible component of D. Let $L/\Bbbk$ be a Galois field extension and assume $D \otimes L$ simple. Then* $\operatorname{Irr}(D \otimes L) = (\operatorname{Irr} D) \otimes L$.

Proof. By definition, $\operatorname{corad}(\operatorname{Irr} D) = D$, then by Lemma 2.2.4 we get

$$\operatorname{corad}((\operatorname{Irr} D) \otimes L) = D \otimes L.$$

Since $D \otimes L$ is simple, $(\mathrm{Irr}\, D) \otimes L$ is irreducible and thus

$$(\mathrm{Irr}\, D) \otimes L \subset \mathrm{Irr}\,(D \otimes L) \tag{2.2.1}$$

by maximality. Let $\Sigma = \mathrm{Gal}(L/\mathbb{k})$, then we have a natural continuous action of Σ on $C \otimes L$ by semilinear coalgebra automorphisms. Since $D \otimes L$ is Σ-invariant, so is $\mathrm{Irr}\,(D \otimes L)$. Then by Lemma 0.5.1,

$$\mathrm{Irr}\,(D \otimes L) = D' \otimes L, \tag{2.2.2}$$

where $D' = \mathrm{Irr}\,(D \otimes L)^{\Sigma}$. By (2.2.1), $\mathrm{Irr}\, D \subset D'$. If $\mathrm{Irr}\, D \neq D'$, then by maximality D' is not irreducible, but then $D' \otimes L$ cannot be irreducible, which contradicts (2.2.2). Therefore, $D' = \mathrm{Irr}\, D$ and we are done. ∎

Theorem 2.2.6. *Let H be a cocommutative Hopf algebra over a perfect field $\mathbb{k}$. Let $H_0 = \mathrm{corad}H$ be the coradical and H_1 the irreducible component of the simple subcoalgebra $\mathbb{k}1$. Then H_1 is an H_0-module algebra under the (left) adjoint action and H is isomorphic to the smash product $H_1 \# H_0$ via $a\#b \to ab$.*

Proof. Set $\bar{H} = H \otimes \bar{\mathbb{k}}$, then by Theorem 0.2.7 we have $\bar{H} \cong \bar{H}_1 \# \bar{\mathbb{k}}G$, where $\bar{H}_1$ is the irreducible component of $\bar{\mathbb{k}}1$, $G = G(\bar{H})$, and the smash product is taken over $\bar{\mathbb{k}}$. Since $\mathrm{corad}\bar{H} = \bar{\mathbb{k}}G$, we have precisely the statement of our theorem for $\bar{H}$, so we only need to descend to H. By Lemma 2.2.4, $\mathrm{corad}\bar{H} = (\mathrm{corad}H) \otimes \bar{\mathbb{k}}$, and by Lemma 2.2.5, $\bar{H}_1 = H_1 \otimes \bar{\mathbb{k}}$. Since $\bar{H}_1$ is a $\mathrm{corad}\bar{H}$-module algebra under the adjoint action, then H_1 is a $\mathrm{corad}H$-module algebra. Hence $H \cong H_1 \# (\mathrm{corad}H)$ as desired. ∎

If $\mathrm{char}\,\mathbb{k} = 0$, as we assume from now on, then we again have $H_1 \cong U(P(H))$, a universal enveloping algebra. In fact, the cosemisimple factor

H_0 is not too far from a group algebra. Namely, it is what is sometimes called a "twisted form" of a group algebra in the following sense. We have a natural action of $\Sigma = \mathrm{Gal}(\bar{\Bbbk}/\Bbbk)$ on $H_0 \otimes \bar{\Bbbk} = \bar{\Bbbk}G$, where $G = G(H_0 \otimes \bar{\Bbbk})$ and so Σ acts by automorphisms of G in such a way that the stabilizer of any element of G is an open subgroup of Σ. This situation is described by saying that G is a "Galois module". Conversely, given any Galois module G, we can extend the Σ action to $\bar{\Bbbk}G$ and define $H_0 = \bar{\Bbbk}G^{\Sigma}$. Then by Lemmas 0.5.1 and 2.2.4, H_0 is a cosemisimple Hopf algebra with $H_0 \otimes \bar{\Bbbk} = \bar{\Bbbk}G$. Obviously, if the action of Σ on G is trivial, we simply get $H_0 = \Bbbk G$, an ordinary group algebra.

Definition 2.2.7. Let H be a "twisted form" of a group algebra, $K \subset H$ a normal subHopfalgebra. Following the group terminology, we will call $\dim H/HK^+$ the *index* of K in H.

Remark 2.2.8. If H is a "twisted form" of a group algebra, $K \subset H$ a normal subHopfalgebra of finite index, then H is finitely generated as a left or right K-module. Indeed, passing to $\bar{\Bbbk}$ we get $H \otimes \bar{\Bbbk} = \bar{\Bbbk}G$, $K \otimes \bar{\Bbbk} = \bar{\Bbbk}N$, for some group G and its normal subgroup N of finite index, thus $H \otimes \bar{\Bbbk}$ is generated as a $K \otimes \bar{\Bbbk}$-module by coset representatives and then H is generated as a K-module by H-components of these representatives. This remark would have been trivial if H were always a *free* module over a normal subHopfalgebra K (then we could choose $\dim H/HK^+$ free generators), but freeness may fail even if H is a "twisted form" of the group algebra of the infinite cyclic group (see [25, Example 3.5.2]). However, any commutative or cocommutative Hopf algebra H is *faithfully flat* over any subHopfalgebra [25, Section 3.4]. A ring extension $R \subset S$ is called left faithfully flat if for any right R-module map

$f : M \to N$, f is injective $\Leftrightarrow f \otimes id : M \otimes_R S \to N \otimes_R S$ is injective. If S is a free (left) R-module, then $R \subset S$ is (left) faithfully flat. For many applications, faithful flatness is as good as freeness: e.g. if $R \subset S$ is left faithfully flat, then for any right ideal $J \subset B$ we have $R \cap JS = J$.

We are now ready to prove the main result of this section (given by the author in [21]).

Theorem 2.2.9. *Let H be a cocommutative Hopf algebra over a field $\Bbbk$ of characteristic 0. Then the following conditions are equivalent:*

1) H is PI as an algebra,

2) There exists a normal commutative subHopfalgebra $A \subset H$ such that H/HA^+ is finite-dimensional,

3) There exists a normal commutative subHopfalgebra $B \subset H$ such that H is a finitely generated left B-module,

4) The Lie algebra $L = P(H)$ of primitive elements is Abelian and there exists a normal subHopfalgebra $C \subset \operatorname{corad} H$ of finite index such that C is commutative and the adjoint action of C on L is trivial.

Proof. 4) $\Rightarrow$ 3) : According to Theorem 2.2.6, we have $H \cong H_1 \# H_0$. Moreover, since the characteristic is 0, $H_1 \cong U(L)$ and therefore $C \subset H_0$ acts trivially on H_1 and thus $H_1 \# C \cong H_1 \otimes C$ is a normal commutative subHopfalgebra of H. By Remark 2.2.8, H_0 is a finitely generated left C-module, hence $H \cong H_1 \# H_0$ is a finitely generated left $H_1 \# C$-module. Set $B = H_1 \# C$.

3) $\Rightarrow$ 2) : Given a normal subHopfalgebra $B \subset H$ such that H is generated by $h_1, \ldots, h_l$ as a left B-module, then H/B^+H is spanned by $h_1 + B^+H, \ldots, h_l + B^+H$ as a $\Bbbk$-space, thus we can set $A = B$ (note that $HA^+ = A^+H$ by normality).

2) $\Rightarrow$ 1) : Without loss of generality, we can assume the field $\Bbbk$ algebraically closed. Indeed, if H satisfies 2), then so does $\bar{H} = H \otimes \bar{\Bbbk}$ (and with the same dimension of the factor). Suppose we know that this impies that $\bar{H}$ satisfies an identity over $\bar{\Bbbk}$. Then expressing the coefficients of this identity through some basis of $\bar{\Bbbk}$ over $\Bbbk$, we obtain an identity for H over $\Bbbk$ (of the same or lower degree).

So let $\Bbbk$ be algebraically closed. Then $\tilde{H} = H/HA^+$, being a finite-dimensional cocommutative Hopf algebra over an algebraically closed field of characteristic 0, is necessarily a group algebra: $\tilde{H} \cong \Bbbk G$, for some finite group G. This follows, for example, from Theorem 0.2.7, since in characteristic 0 the connected part is either trivial or infinite-dimensional. According to the one-to-one correspondence between normal subHopfalgebras and Hopf ideals in the cocommutative case, $A = H^{co\tilde{H}}$, the subalgebra of coinvariants of the (right) $\tilde{H}$-comodule algebra H. Since $\tilde{H} \cong \Bbbk G$, we can interpret this fact by saying that A is the identity component of H under the G-grading corresponding to the $\tilde{H}$-comodule structure. We can now apply the theorem of Bergen and Cohen [7], saying that if the identity component B_1 of an algebra B graded by a finite group is PI, then the whole algebra B is PI (moreover, by [4] — see also [5] for generalizations — the degree of a polynomial identity in B depends only on the degree of the identity in B_1 and the order of the group). Hence H is a PI algebra.

1) $\Rightarrow$ 4) : Let $\Sigma = \mathrm{Gal}(\bar{\Bbbk}/\Bbbk)$. Set $\bar{H} = H \otimes \bar{\Bbbk}$, then Σ acts on $\bar{H}$ by semilinear Hopf algebra automorphisms. Now we can decompose over $\bar{\Bbbk}$:

$$\bar{H} = U(\bar{L})\#\bar{\Bbbk}G,$$

where $\bar{L} = P(\bar{H}) = P(H) \otimes \bar{\Bbbk} = L \otimes \bar{\Bbbk}$ and $G = G(\bar{H})$.

Since $\bar{H}$ is PI, we see that $\bar{L}$ is Abelian, and there exists a *characteristic* Abelian subgroup $G_1 \subset G$ of finite index, and the kernel $G_0 \subset G$ of the action of G on $\bar{L}$ also has a finite index by Theorem 2.1.7. Clearly, $\bar{L}$ and G are Σ-invariant. It follows that G_1 is also Σ-invariant. Moreover, since the action of G on $\bar{L}$ is given by

$$g \cdot l = glg^{-1}, \, g \in G, \, l \in \bar{L},$$

the kernel G_0 of the action is Σ-invariant as well. Therefore, according to Lemma 0.5.1 we conclude that

$$\bar{\Bbbk}(G_0 \cap G_1) = C \otimes \bar{\Bbbk},$$

where C is the set of all elements of $\bar{\Bbbk}(G_0 \cap G_1)$ fixed by Σ. Since $\bar{\Bbbk}(G_0 \cap G_1)$ is a subHopfalgebra of $\bar{H}$, C is a subHopfalgebra of H. Moreover, by Lemma 2.2.4, $(\mathrm{corad} H) \otimes \bar{\Bbbk} = \mathrm{corad}(H \otimes \bar{\Bbbk}) = \bar{\Bbbk}G$, so in fact C is in $H_0 = \mathrm{corad} H$. Finally, C is commutative and acts trivially on L by construction, and

$$\dim H_0/H_0C^+ = \dim(H_0 \otimes \bar{\Bbbk})/(H_0 \otimes \bar{\Bbbk})(C \otimes \bar{\Bbbk})^+ = (G : G_0 \cap G_1)$$

is finite. ■

Remark 2.2.10. It follows from the estimate of $(G : G_1)$ found in [26] and the estimate of $(G_1 : G_0 \cap G_1)$ found in [19] that $(\mathrm{corad} H : C)$ in 4) and therefore, $\dim H/HA^+$ in 2) (by taking $A = H_1\#C$) can be bounded by a function that depends only on the degree of the identity satisfied by H. Unfortunately, we do not have an estimate of the number of generators in 3) unless $\bar{\Bbbk}/\Bbbk$ is finite.

Conversely, the estimate for the theorem of Bergen and Cohen found in [4] implies that H satisfies an identity of degree bounded by a function of $\dim H/HA^+$ in 2). Moreover, since in 3) H is a finitely generated left B-module and B is commutative, H in fact satisfies the standard identity of degree $2l$, where l is the number of generators, because H can then be realized as a factor of a subalgebra of $l \times l$ matrices over B. By similar argument, H satisfies the standard identity of degree $2(\mathrm{corad}H : C)$ in 4).

Remark 2.2.11. If H happens to be pointed (e.g. if $\bar{\Bbbk} = \Bbbk$), we can do better in part 3): H is isomorphic to the crossed product $B\#_\sigma D$, with the tensor product coalgebra structure, where B is a commutative Hopf algebra and D is a finite-dimensional one. Indeed, according to Theorem 0.2.7, we have $H \cong U(L)\#\Bbbk G$, with the tensor product coalgebra structure. By part 4), we have a normal Abelian subgroup $N \subset G$ of finite index that acts trivially on $U(L)$ and thus $U(L)\#\Bbbk N$ is commutative and the action of G on $U(L)$ gives rise to an action of G/N. Set $B = U(L)\#\Bbbk N$, $D = \Bbbk(G/N)$. By a classical argument, $\Bbbk G$ can be represented as the crossed product $\Bbbk N\#_\tau D$, with the tensor product coalgebra structure, for some twisted action of D on $\Bbbk N$ and a 2-cocycle $\tau : D \otimes D \to \Bbbk N$. So we finally obtain:

$$H \cong U(L)\#\Bbbk G \cong U(L)\#(\Bbbk N\#_\tau D) \cong (U(L)\#\Bbbk N)\#_\sigma D, \tag{2.2.3}$$

where D acts on $U(L)\#\Bbbk N$ by the rule:

$$d \cdot (x\#y) = \sum (d_{(1)} \cdot x)\#(d_{(2)} \cdot y), \qquad \forall d \in D,\ x \in U(L),\ y \in \Bbbk N,$$

and the cocycle $\sigma : D \otimes D \to U(L)\#\Bbbk N$ is given by

$$\sigma(c, d) = 1\#\tau(c, d), \qquad \forall c, d \in D.$$

The last isomorphism in (2.2.3) is simply $x\#(y\#d) \to (x\#y)\#d$.

2.3 The Case of Prime Characteristic: Coreduced Hyperalgebras

The case of prime characteristic appears to be much more complicated, in particular because of the structure of the irreducible component H_1 of $\Bbbk 1$, which need not be an enveloping algebra. We restrict our attention mainly to the case when H_1 is coreduced (see the definition below). We extend Theorem 2.1.3 to coreduced hyperalgebras and also give some partial results for the smash products $H_1\#\Bbbk G$ with H_1 coreduced. The proofs will be postponed until Chapter 4.

Until the end of this section, we assume the field $\Bbbk$ perfect of characteristic $p > 0$, unless stated otherwise.

First we quote some definitions and results from [14, Sections 2.2.6, 2.2.7, 2.2.9].

Definition 2.3.1. Let V and W be vector spaces, n an integer. A map $\varphi : V \to W$ is called p^n-linear if it is additive and

$$\varphi(\lambda v) = \lambda^{p^n} \varphi(v), \qquad \forall v \in V,\ \lambda \in \Bbbk.$$

Let H be a hyperalgebra, then H^* is a commutative algebra and so we can define a p-linear algebra map $F : H^* \to H^* : f \to f^p$, called the *Frobenius homomorphism*. Then there exists a unique $1/p$-linear Hopf algebra map $V : H \to H$, called *Verschiebung*, such that F is the transpose of V:

$$\langle f, V(h)\rangle = \sqrt[p]{\langle F(f), h\rangle}, \qquad \forall h \in H,\ f \in H^*. \tag{2.3.1}$$

Definition 2.3.2. We will say that H is of *coheight* r, $r \in \mathbb{Z}_+ = \{0, 1, \ldots\}$, if $V^{r+1}(H^+) = 0$ and $V^r(H^+) \neq 0$. If no such r exists, H is said to be of *infinite coheight*.

Let $L = P(H)$ and $L_r = L \cap V^r(H)$, then we have $L = L_0 \supset L_1 \supset \ldots$ and each L_r is in fact a p-Lie subalgebra.

Definition 2.3.3. If the chain $L = L_0 \supset L_1 \supset \ldots$ stabilizes, i.e. we have $L_{r_0} = L_{r_0+1} = \ldots$ for some r_0, then H is called *stable*. If $L_0 = L_1 = \ldots$, i.e. $r_0 = 0$, then H is called *coreduced* (in particular, it means that H is of infinite coheight).

Remark 2.3.4. All hyperalgebras that are of finite type ($\dim P(H) < \infty$), of finite coheight, or coreduced satisfy the stability condition. Stability is necessary for the PBW-type structure theorem below.

Remark 2.3.5. It can be seen from [14] that H is coreduced iff $V : H \to H$ is surjective iff $F : H^* \to H^*$ is injective, which is equivalent to saying that H^* has no nilpotent elements, i.e. H^* is *reduced* in the sense of commutative algebra (Definition 3.1.1). This observation justifies the term "coreduced".

The following structure theorem is due to Cartier, Demazure, Gabriel et al. Recall the multi-index notation from Section 0.4.

Theorem 2.3.6. *Let H be a hyperalgebra over a perfect field $\mathbb{k}$ of characteristic p. Let $L = P(H)$ and $L_r = L \cap V^r(H)$, $r = 0, 1, \ldots$, where V is the Verschiebung operator. Assume H is stable, i.e. $L = L_0 \supset L_1 \supset \ldots \supset L_{r_0} = L_{r_0+1} = \ldots$, for some r_0. Choose a chain of sets $I = I_0 \supset I_1 \supset \ldots \supset I_{r_0} = I_{r_0+1} = \ldots$ and a family $\{x_{i0} | i \in I\}$ of elements of L such that x_{i0}, $i \in I_r$, form a basis of L_r, for any r. Then there exists a basis $\{z^{(\alpha)}\}$ of H, indexed by $\alpha \in \mathbb{Z}_+^{(I)}$ with $\alpha(i) < p^{r+1}$ for $i \in I_r \setminus I_{r+1}$, such that*

1) $z^{(\varepsilon_i)} = x_{i0}$, *for all* $i \in I$, *and* $z^{(0)} = 1$,

2) $\Delta z^{(\alpha)} = \sum_{\beta+\gamma=\alpha} z^{(\beta)} \otimes z^{(\gamma)}$, *for all* α.

We will refer to any basis satisfying 2) above as a basis of "divided powers" (cf. Definition 1.5.4). For any such basis of H, we have

$$z^{(\alpha)} z^{(\beta)} = \binom{\alpha+\beta}{\alpha} z^{(\alpha+\beta)} \quad (\text{mod span}\{z^{(\gamma)} | \, |\gamma| < |\alpha| + |\beta|\}).$$

■

Remark 2.3.7. Note that the components $\alpha(i)$ with $i \in I_{r_0} = I_{r_0+1} = \ldots$ are not restricted. It can be verified that

$$H_{red} = V^{r_0}(H) = \text{span}\{z^{(\alpha)} | \, \text{supp}\, \alpha \subset I_{r_0}\}$$

is the largest coreduced subbialgebra (hence a subHopfalgebra by connectedness) of H.

Remark 2.3.8. It immediately follows from (2.3.1) that $V(z^{(\alpha)}) = z^{(\alpha/p)}$ if each component of α is divisible by p, and 0 otherwise.

Remark 2.3.9. In characteristic 0, we have $H = U(L)$. So if we choose any ordered basis $\{x_{i0} | i \in I\}$ of L and set

$$z^{(\alpha)} = \prod_{i \in \operatorname{supp} \alpha} \frac{1}{\alpha(i)!} x_{i0}^{\alpha(i)},$$

then $\{z^{(\alpha)} | \alpha \in \mathbb{Z}_+^{(I)}\}$ will be a basis for H satisfying the conditions of Theorem 2.3.6 (whence the term "divided powers"). Because of this observation, our proof of Theorem 2.3.11 will also apply to the case of zero characteristic, thereby giving a new proof of Theorem 2.1.3.

As a consequence, one can also obtain a PBW-type basis for H.

Corollary 2.3.10. *Using the notation of the theorem above, set $x_{ik} = z^{(p^k \varepsilon_i)}$, where the pairs (i, k) are such that $0 \le k \le r$ if $i \in I_r \setminus I_{r+1}$, and fix a linear order on the set of such pairs. Then the ordered monomials of the form $\prod_{(i,k)} x_{ik}^{n_{ik}}$, $0 \le n_{ik} < p$ with only a finite number of $n_{ik} \neq 0$, constitute a basis of H.* ∎

Now we state our main result on PI coreduced hyperalgebras (given by the author in [20]).

Theorem 2.3.11. *Let H be a hyperalgebra (i.e. connected cocommutative Hopf algebra) over a perfect field $\Bbbk$. In the case* $\operatorname{char} \Bbbk = p > 0$, *assume also that H is coreduced. Then H is a PI algebra iff H is commutative.*[1]

Proof. See Section 4.2. ∎

We will also prove the dual analog of this theorem for commutative Hopf algebras in the next section — see Corollary 3.2.7.

[1]This result was obtained in collaboration with Yu.Bahturin

Corollary 2.3.12. *Let H be a hyperalgebra of finite type (i.e.* $\dim P(H) < \infty$*) over a perfect field* $\Bbbk$*. Then H is a PI algebra iff the maximal coreduced subbialgebra of H is commutative.*

Proof. As we observed, H contains a (unique) maximal coreduced subbialgebra H_{red} (see Remark 2.3.7). Moreover, using Corollary 2.3.10, we see that H is a free finitely generated left module over H_{red}. This proves the sufficiency of our condition, because H is realized (by virtue of right multiplication) as a subalgebra of a matrix ring over the commutative algebra H_{red}. The necessity follows from Theorem 2.3.11. ∎

Corollary 2.3.13. *Let $\mathfrak{A}$ be a variety of algebras (associative with 1). Let $\mathcal{F}_{\mathfrak{A}}$ be the relatively free algebra of $\mathfrak{A}$ in countably many variables $X_1, X_2, \dots$ over an infinite perfect field $\Bbbk$. Then $\mathcal{F}_{\mathfrak{A}}$ admits a structure of a coreduced hyperalgebra iff $\mathfrak{A}$ is $\{0\}$ or the variety Alg of all algebras or the variety Comm of all commutative algebras (cf. Proposition 2.1.11).*

Proof. By Theorem 2.3.11, if $\mathcal{F}_{\mathfrak{A}}$ admits a structure of a coreduced hyperalgebra and satisfies a polynomial identity, then $\mathcal{F}_{\mathfrak{A}}$ is commutative. This proves the necessity. The sufficiency follows from the examples below. ∎

Example 2.3.14. Let $\mathcal{F}$ be the free algebra (associative with 1) in $X_1, X_2, \dots$ Set $X_0 = 1$. Then

$$\Delta X_n = \sum_{k=0}^{n} X_k \otimes X_{n-k}, \; n = 0, 1, \dots \tag{2.3.2}$$

defines a structure of a reduced hyperalgebra on $\mathcal{F}$ [17, Sections 36.3.8 and 38.1.10].

Example 2.3.15. Let $\mathcal{F}_{Comm} = \Bbbk[X_1, X_2, \ldots]$, the free commutative algebra (with 1) in $X_1, X_2, \ldots$ Then (2.3.2) defines a structure of a reduced hyperalgebra on $\mathcal{F}_{Comm}$ [17, Section 36.3.8].

Remark 2.3.16. It should be pointed out that the comultiplication on $\mathcal{F}$ defined above is *not* the same as the comultiplication that we had before (e.g. in Proposition 2.1.11).

As we have seen, Theorem 2.1.3 can be extended from universal envelopes of characteristic 0 to coreduced hyperalgebras of characteristic p. It is natural to expect that the same can be done with Theorem 2.1.7.

Conjecture 2.3.17. Let H be a hyperalgebra over a perfect field $\Bbbk$. In the case $\operatorname{char} \Bbbk > 0$, assume also that H is coreduced. Let G be a group acting on H by bialgebra automorphisms(=Hopf algebra automorphisms). Then the smash product $H \# \Bbbk G$ is *PI* iff

1) H is commutative,

2) there exists a subgroups $A \subset G$ of finite index such that A is Abelian in the case $\operatorname{char} \Bbbk = 0$ and p-Abelian in the case $\operatorname{char} \Bbbk = p > 0$, and

3) A acts trivially on H.

It is easy to see that these conditions are sufficient. The necessity of the first two conditions follows from Theorems 2.1.1 and 2.3.11. Presently, I cannot prove the necessity of the third condition, but Theorems 2.3.18 and 2.3.19 below (given by the author in [20]) present some positive evidence that it should be true. This conjecture is also the formal dual of Theorem 3.2.5.

Recall from Section 0.1 that any Hopf algebra H has a fundamental *coradical filtration* $H = \cup_{m=0}^{\infty} H_m$. It is always a coalgebra filtration, and it is a Hopf algebra filtration iff $H_0 = \mathrm{corad} H$ is a subalgebra of H, invariant under antipode [25, Lemma 5.2.8]. This is the case, for instance, if H is pointed, so we can define the associated graded Hopf algebra H^{gr} for any pointed Hopf algebra H. Note also that any bialgebra automorphism of H preserves the coradical filtration and therefore induces an automorphism of H^{gr}.

Theorem 2.3.18. *Let a group G act by bialgebra automorphisms on a coreduced hyperalgebra H. If $H\#\Bbbk G$ is PI, then there exists a subgroup of finite index in G that acts trivially on H^{gr}.*

Proof. Let us fix a basis of "divided powers" $\{z^{(\alpha)} | \alpha \in \mathbb{Z}_+^{(I)}\}$ in H. Then

$$H_m = \mathrm{span}\{z^{(\alpha)} |\ |\alpha| \leq m\}.$$

Denote $\mathrm{gr} z^{(\alpha)} = z^{(\alpha)} + H_{|\alpha|-1} \in H^{\mathrm{gr}}$, then $\{\mathrm{gr} z^{(\alpha)} | \alpha \in \mathbb{Z}_+^{(I)}\}$ is a basis of H^{gr} and Theorem 2.3.6 implies that

$$\mathrm{gr} z^{(\alpha)} \cdot \mathrm{gr} z^{(\beta)} = \binom{\alpha+\beta}{\alpha} \mathrm{gr} z^{(\alpha+\beta)}.$$

In other words, H^{gr} is isomorphic to the divided power algebra $D(I)$ introduced in Chapter 1 (Definition 1.5.4).

Note that since all H_m are G-invariant, we can extend the filtration to $H\#\Bbbk G$ by setting $(H\#\Bbbk G)_m = H_m\#\Bbbk G$. Then we obtain $H^{\mathrm{gr}}\#\Bbbk G \cong (H\#\Bbbk G)^{\mathrm{gr}}$, and the latter is PI since so is $H\#\Bbbk G$. The theorem now follows from Theorem 2.3.19 below applied to $H^{\mathrm{gr}}\#\Bbbk G$. ∎

Theorem 2.3.19. *Let I be a set and $H = D(I)$, the divided power algebra, i.e. H has a basis $\{z^\alpha \mid \alpha \in \mathbb{Z}_+^{(I)}\}$, with multiplication*

$$z^{(\alpha)} \cdot z^{(\beta)} = \binom{\alpha+\beta}{\alpha} z^{(\alpha+\beta)}, \tag{2.3.3}$$

and comultiplication

$$\Delta z^{(\alpha)} = \sum_{\beta+\gamma=\alpha} z^{(\beta)} \otimes z^{(\gamma)}.$$

Suppose a group G acts on H by bialgebra automorphisms. Then the smash product $H\#\Bbbk G$ is PI iff there exists a subgroup $A \subset G$ of finite index such that A is Abelian in the case $\operatorname{char} \Bbbk = 0$ and p-Abelian in the case $\operatorname{char} \Bbbk = p > 0$, and A acts trivially on H.

Proof. See Section 4.3. ■

Chapter 3

Commutative Hopf Algebras with a Coidentity

3.1 Preliminaries

In this chapter, we will prove necessary and sufficient conditions for a reduced commutative Hopf algebra over a perfect field to be cPI, i.e. to satisfy a nontrivial polynomial identity as a coalgebra – see Theorems 3.2.2 and 3.2.5 (given by the author in [21]) in the next section. The equivalence of 1) and 2) in Theorem 3.2.2 is the formal dual of the generalized Passman theorem obtained in Chapter 2 for the case of zero characteristic (Theorem 2.2.9). Theorem 3.2.5 is dual to Conjecture 2.3.17 in prime characteristic (assuming the field algebraically closed).

Definition 3.1.1. Let A be a commutative algebra, then the set of all nilpotent elements is an ideal in A, called the *nilradical* of A. We will denote it $\mathrm{rad}A$. The algebra A is called *reduced* if $\mathrm{rad}A = 0$. An ideal $J \triangleleft A$ is said to be *radical* if A/J is reduced.

The following is an old result of P.Cartier (see e.g. [25, Corollary 9.2.11]).

Theorem 3.1.2. *Let H be a commutative Hopf algebra over a field $\Bbbk$ of characteristic* 0. *Then H is reduced.* ■

In the case of prime characteristic, a commutative Hopf algebra H does not have to be reduced. However, if $\Bbbk$ is *perfect*, as we will assume from now on (unless stated otherwise), rad$H$ is a Hopf ideal [36, Chapter 6, Exercise 3] and thus $H/\text{rad}H$ is a reduced Hopf algebra (cf. Remark 2.3.7).

We will extensively use the geometric interpretation of commutative Hopf algebras – affine group schemes. But since we will concentrate on the reduced case, we can restrict ourselves to (affine) algebraic groups in the "naïve" sense, i.e. an algebraic group G defined over $\Bbbk$ will be a subset of a finite-dimensional affine space over $\bar{\Bbbk}$ determined by polynomial equations with coefficients in $\Bbbk$ and endowed with a group structure by polynomial functions with coefficients in $\Bbbk$. As is well-known, such algebraic groups are in one-to-one correspondence with commutative Hopf algebras H that are finitely generated (as algebras) and such that $H \otimes \bar{\Bbbk}$ is reduced. In the geometric literature, algebraic groups of this kind as well as their Hopf algebras are called "smooth"; over a perfect field this is the same as reduced. The correspondence is set up as follows. Given an algebraic group G, we can construct its Hopf algebra $H = \mathcal{O}(G)$ of regular (=polynomial) functions with coefficients in $\Bbbk$, from which the group G can be recovered as the group $\text{Alg}(H, \bar{\Bbbk})$ of all algebra maps $H \to \bar{\Bbbk}$ (under the convolution product). The comultiplication of H is induced by the multiplication in G and vice versa (see Section 0.2).

Recall that the *Zarissky topology* of the d-dimensional affine space $\bar{\mathbb{k}}^d$ is defined by taking the sets of zeros of families of polynomials in d variables with coefficients in $\bar{\mathbb{k}}$ for the system of closed sets. If H is a commutative Hopf algebra generated by d elements, then the group $G = \mathrm{Alg}(H, \bar{\mathbb{k}})$ can be identified with a closed subset of $\bar{\mathbb{k}}^d$ and thus inherits the Zarissky topology. Moreover, closed subgroups of G are in one-to-one correspondence with the Hopf ideals of $\bar{H} = H \otimes \bar{\mathbb{k}}$ that are radical. Namely, if Q is a closed subgroup, the corresponding ideal J is the set of all elements from $\bar{H}$ that vanish on Q. By Lemma 0.5.1, Q is defined over $\mathbb{k}$, i.e. J comes from an ideal in H, iff J is invariant under $\Sigma = \mathrm{Gal}(\bar{\mathbb{k}}/\mathbb{k})$. The latter happens iff Q is invariant under Σ, which acts on $G = \mathrm{Alg}(H, \bar{\mathbb{k}})$ by virtue of its action on $\bar{\mathbb{k}}$.

If $Q \subset G$ is a closed normal subgroup, then the factorgroup G/Q can again be viewed as an algebraic group (see e.g. [36, Chapter 16]). If G and Q are defined over $\mathbb{k}$, then so is G/Q. The Hopf algebra $\mathcal{O}(G/Q)$ of regular functions on G/Q is the subHopfalgebra of $H = \mathcal{O}(G)$ obtained from the ideal J of Q by the correspondence between subHopfalgebras and normal Hopf ideals discussed in Section 0.2. Let us now show that this correspondence agrees with taking the dual (we will use this fact later).

Lemma 3.1.3. *Let H be a Hopf algebra, $K \subset H$ a normal subHopfalgebra. Consider $J = K^{\perp} = \{f \in H^{\circ} \mid \langle f, K\rangle = 0\}$. Then J is a normal Hopf ideal of H° and $(H^{\circ})^{co(H^{\circ}/J)} = (HK^{+})^{\perp}$.*

Proof. By Lemma 0.1.5, J is a biideal. Since K is invariant under the antipode S of H, $J = K^{\perp}$ will be invariant under S^*. But S^* is the antipode of H°, hence J is a Hopf ideal.

Now consider the right adjoint coaction $\rho_r : H^{\circ} \to H^{\circ} \otimes H^{\circ}$. For $f \in H^{\circ}$

and $k, h \in H$, we compute:

$$\begin{aligned}
\langle \rho_r f, k \otimes h \rangle &= \langle \sum f_{(2)} \otimes (Sf_{(1)})f_{(3)}, k \otimes h \rangle \\
&= \sum \langle f_{(2)}, k \rangle \langle (Sf_{(1)})f_{(3)}, h \rangle \\
&= \sum \langle f_{(2)}, k \rangle \langle Sf_{(1)}, h_{(1)} \rangle \langle f_{(3)}, h_{(2)} \rangle \\
&= \sum \langle f_{(1)}, Sh_{(1)} \rangle \langle f_{(2)}, k \rangle \langle f_{(3)}, h_{(2)} \rangle \\
&= \sum \langle f, (Sh_{(1)})kh_{(2)} \rangle = \langle f, (\mathrm{ad}_r h)(k) \rangle.
\end{aligned}$$

Since K is $\mathrm{ad}_r H$-invariant, it follows that $\rho_r f$ will annihilate $K \otimes H$ as long as f annihilates K. In other words, $\rho_r J \subset (K \otimes H)^\perp = J \otimes H^\circ$. Similarly, we also have $\rho_l J \subset H^\circ \otimes J$ and thus J is normal.

Finally,

$$\begin{aligned}
(H^\circ)^{co(H^\circ/J)} &= \{f \in H^\circ \mid \Delta f - f \otimes 1 \in H^\circ \otimes J\} \\
&= \{f \in H^\circ \mid \langle \Delta f - f \otimes 1, H \otimes K \rangle = 0\} \text{ (since } J = K^\perp) \\
&= \{f \in H^\circ \mid \forall h \in H, \forall k \in K \ \langle f, hk \rangle - \langle f, h \rangle \langle 1, k \rangle = 0\} \\
&= \{f \in H^\circ \mid \forall h \in H, \forall k \in K \ \langle f, h(k - \varepsilon(k)1) \rangle = 0\} \\
&= (HK^+)^\perp.
\end{aligned}$$

■

Now we want to assign a group to a commutative Hopf algebra that is not necessarily finitely generated. The local finiteness of coalgebras (Theorem 0.1.8) implies that any Hopf algebra H is the union of its subHopfalgebras that are finitely generated (as algebras). We will denote these subHopfalgebras by H_i, $i \in I$, where I is an indexing set and we write $i \leq j$ iff $H_i \subset H_j$. Then I is a directed set and we obtain:

$$H = \varinjlim H_i, \ i \in I.$$

Therefore, we can assign to H a "pro-algebraic group" (i.e. an inverse limit of algebraic groups)

$$G = \mathrm{Alg}(H, \bar{\Bbbk}) = \varprojlim G_i,$$

where $G_i = \mathrm{Alg}(H_i, \bar{\Bbbk})$. If we assume H commutative and smooth(=reduced if $\Bbbk$ is perfect), then, thanks to Lemma 3.1.4 below, H can be recovered from G as $\mathcal{O}(G)$. The latter is defined as the set of functions $G \to \bar{\Bbbk}$ that can be written as a composition of the canonical map $G \to G_i$ and a function from $\mathcal{O}(G_i)$, for some $i \in I$.

Lemma 3.1.4. *Let H be a commutative Hopf algebra over an algebraically closed field $\Bbbk$ of any characteristic. If $K \subset H$ is a subHopfalgebra, then the restriction map $\mathrm{Alg}(H, \Bbbk) \to \mathrm{Alg}(K, \Bbbk)$ is surjective. Consequently, the intersection of all kernels of algebra maps $H \to \Bbbk$ is the nilradical of H.*

Proof. The proof follows from the faithful flatness over subHopfalgebras and the Hilbert Nullstellensatz (see [36, Chapter 15, Exercise 3]). ∎

3.2 The Dual Passman Theorem

A group G is called Abelian-by-finite if it contains an Abelian subgroup A of finite index (without loss of generality, A can be assumed normal and even characteristic). Then the result of D.Passman (Theorem 2.1.1) says that the Hopf algebra $\Bbbk G$ over a field of characteristic 0 is PI iff G is Abelian-by-finite. In Section 2.2, we have generalized this result to arbitrary cocommutative Hopf algebras. Now we obtain a dualization of this theorem. First we need a version of "Abelian-by-finiteness" suitable for pro-algebraic groups.

Definition 3.2.1. Let G be a pro-algebraic group: $G = \varprojlim G_i$, $i \in I$, I a directed set, G_i algebraic groups defined over $\Bbbk$. We will call G Abelian-by-finite if there exists a compatible family of normal Abelian algebraic subgroups $A_i \subset G_i$, $i \in I$, defined over $\Bbbk$, such that $(G_i : A_i)$ are bounded. By "compatibility" we mean that $\varphi_{ij}(A_j) \subset A_i$, for any $i < j$ in I, where $\varphi_{ij} : G_j \to G_i$ are the structure maps of the inverse limit system.

Theorem 3.2.2. *Let H be a commutative Hopf algebra over a field $\Bbbk$ of characteristic 0. Then the following conditions are equivalent:*

1) H is PI as a coalgebra,

2) There exists a finite-dimensional subHopfalgebra $K \subset H$ such that H/HK^+ is cocommutative,

3) $H = \mathcal{O}(G)$, where G is an Abelian-by-finite pro-algebraic group (in the sense of the above definition),

4) The (abstract) group $G = \mathrm{Alg}(H, \bar{\Bbbk})$ is Abelian-by-finite, i.e. there exists an Abelian subgroup $A \subset G$ of finite index.

Proof. 1) $\Rightarrow$ 4) : Set $\bar{H} = H \otimes \bar{\Bbbk}$ and

$$G = \mathrm{Alg}(H, \bar{\Bbbk}) = \mathrm{Alg}(\bar{H}, \bar{\Bbbk}) = G(\bar{H}^\circ).$$

Since the elements of G are linearly independent over $\bar{\Bbbk}$, we have $\bar{\Bbbk}G \subset \bar{H}^\circ$. Now $\bar{H}^\circ$ is a PI algebra by Proposition 1.1.4, hence by Theorem 2.1.1, there exists an Abelian subgroup $A \subset G$ of finite index.

4) $\Rightarrow$ 3) : As we know, $H = \varinjlim H_i$, $i \in I$, I a directed set, where H_i are finitely generated subHopfalgebras. Set $G_i = \mathrm{Alg}(H_i, \bar{\Bbbk})$, the algebraic

group corresponding to H_i. Then $G = \varprojlim G_i$. Moreover, by Lemma 3.1.4, the canonical maps $\varphi_i : G \to G_i$ are surjective (being the restriction maps induced by the inclusions $H_i \subset H$).

Without loss of generality, we can assume $A \subset G$ *characteristic*. Set $A_i = \overline{\varphi_i(A)}$, the Zarissky closure of $\varphi_i(A)$, then $A_i \subset G_i$, $i \in I$, is a compatible family of closed normal Abelian subgroups, which are invariant under all continuous automorphisms of G_i liftable to automorphisms of G. In particular, A_i are invariant under $\mathrm{Gal}(\bar{\Bbbk}/\Bbbk)$ that acts on $G = \mathrm{Alg}(H, \bar{\Bbbk})$ and $G_i = \mathrm{Alg}(H_i, \bar{\Bbbk})$ in a natural way. Thus all A_i are defined over $\Bbbk$. Clearly, $(G_i : A_i) \leq (G : A)$.

3) $\Rightarrow$ 2) : Let $H_i = \mathcal{O}(G_i)$, then $H = \varinjlim H_i$, where the maps

$$\psi_{ij} : H_i \to H_j,\ i < j,$$

of the direct limit system are induced by the morphisms

$$\varphi_{ij} : G_j \to G_i.$$

Set $K_i = \mathcal{O}(G_i/A_i)$, then K_i is a subHopfalgebra of H_i and

$$\mathcal{O}(A_i) = H_i/H_iK_i^+.$$

Moreover, since $\varphi_{ij}(A_j) \subset A_i$, we have $\psi_{ij}(K_i) \subset K_j$, for all $i < j$, so we can set $K = \varinjlim K_i$. Then K is a subHopfalgebra of H and

$$H/HK^+ = \varinjlim H_i/H_iK_i^+.$$

Since $\dim K_i = (G_i : A_i)$ are bounded, K is finite-dimensional. Finally, since $H_i/H_iK_i^+ = \mathcal{O}(A_i)$ are cocommutative, so is H/HK^+.

2) $\Rightarrow$ 1) : By the argument similar to the 2) $\Rightarrow$ 1) part of the proof of Theorem 2.2.9, we can assume $\Bbbk$ algebraically closed. From Lemma 3.1.4 it follows that $H^\circ \supset \mathrm{Alg}(H, \Bbbk)$ separates the elements of H (H has zero nilradical since $\mathrm{char}\,\Bbbk = 0$ by Theorem 3.1.2). Hence H imbeds into $H^{\circ\circ}$ in a natural way. So it suffices to prove that the cocommutative Hopf algebra H° is PI as an algebra. To show this, consider

$$J = K^\perp = \{f \in H^\circ \mid \langle f, K\rangle = 0\}.$$

Since K is a subHopfalgebra, J is a Hopf ideal of H° and H°/J naturally imbeds into K°, so it is finite-dimensional. According to the one-to-one correspondence between normal subHopfalgebras and Hopf ideals, $I = H^\circ A^+$, where $A = (H^\circ)^{co(H^\circ/J)}$ is a normal subHopfalgebra of H°. By Lemma 3.1.3, $A = (HK^+)^\perp = (H/HK^+)^\circ$. Since H/HK^+ is cocommutative, A is commutative and Theorem 2.2.9 applies to H°. ■

Remark 3.2.3. Similarly to the dual situation, it follows from [26] that the index of A in $\mathrm{Alg}(H, \bar{\Bbbk})$ in 4) and, therefore, $(G_i : A_i)$ in the inverse limit in 3) (see Definition 3.2.1) and $\dim K$ in 2) can be bounded by a function that depends only on the degree of the coidentity satisfied by H. Conversely, Remark 2.2.10 implies that H satisfies an identity of degree bounded by a function of $\dim K$ in 2) or the bound of $(G_i : A_i)$ in the inverse limit in 3) or $(G : A)$ in 4). Moreover, H in fact satisfies a standard identity as a coalgebra since so does H° as an algebra.

Now we pass to the case of prime characteristic p. In this case, Theorem 2.1.1 says that $\Bbbk G$ is PI iff G is p-Abelian-by-finite, i.e. there exists a p-Abelian subgroup $A \subset G$ of finite index. We need a version of this notion for pro-algebraic groups.

Definition 3.2.4. Let G be a pro-algebraic group: $G = \varprojlim G_i$, $i \in I$, I a directed set, G_i algebraic groups defined over $\Bbbk$, $\operatorname{char} \Bbbk = p$. We will say that G is p-Abelian-by-finite if there exists a compatible family of normal algebraic subgroups $A_i \subset G_i$, $i \in I$, defined over $\Bbbk$, such that $(G_i : A_i)$ are bounded and $(A_i' : 1)$ are bounded powers of p.

Theorem 3.2.5. *Let H be a reduced commutative Hopf algebra over a perfect field $\Bbbk$ of characteristic p. Then the following conditions are equivalent:*

1) H is PI as a coalgebra,

2) There exist subHopfalgebras $K \subset L \subset H$ such that K is finite-dimensional semisimple, L/LK^+ is cocommutative, and H/HL^+ is finite-dimensional semisimple with dimension equal to a power of p,

3) $H = \mathcal{O}(G)$, where G is a p-Abelian-by-finite pro-algebraic group (in the sense of the above definition),

4) The (abstract) group $G = \operatorname{Alg}(H, \bar{\Bbbk})$ is p-Abelian-by-finite, i.e. there exists a subgroup A such that $(G : A)$ is finite and $(A' : 1)$ is a power of p.

Proof. The demonstration of 1) $\Rightarrow$ 4) $\Rightarrow$ 3) proceeds in a way quite similar to the proof of Theorem 3.2.2, replacing "Abelian" by "p-Abelian".

3) $\Rightarrow$ 2) : Let $H_i = \mathcal{O}(G_i)$, then $H = \varinjlim H_i$, where the maps

$$\psi_{ij} : H_i \to H_j,\ i < j,$$

of the direct limit system are induced by the morphisms

$$\varphi_{ij} : G_j \to G_i.$$

Set $K_i = \mathcal{O}(G_i/A_i)$, $L_i = \mathcal{O}(G_i/A_i')$, then $K_i \subset L_i$ are subHopfalgebras of H_i and we have

$$\mathcal{O}(A_i/A_i') = L_i/L_iK_i^+ \text{ and } \mathcal{O}(A_i') = H_i/H_iL_i^+.$$

Hence $L_i/L_iK_i^+$ are cocommutative, K_i and $H_i/H_iL_i^+$ are semisimple of bounded dimension, the latter having dimension equal to a power of p. Moreover, since $\varphi_{ij}(A_j) \subset A_i$, we have $\varphi_{ij}(A_j') \subset A_i'$ and so $\psi_{ij}(K_i) \subset K_j$, $\psi_{ij}(L_i) \subset L_j$, for all $i < j$. Thus we can set $K = \varinjlim K_i$, $L = \varinjlim L_i$, which clearly satisfy all the desired conditions.

2) $\Rightarrow$ 1) : Without loss of generality, $\Bbbk$ is algebraically closed. From Lemma 3.1.4 it follows that $H^\circ \supset \mathrm{Alg}(H, \Bbbk)$ separates the elements of H (H has zero nilradical by assumption). Hence H imbeds into $H^{\circ\circ}$ and it suffices to prove that the cocommutative Hopf algebra H° is PI as an algebra. To show this, consider the Hopf ideal $J = K^\perp \subset H^\circ$. Since H°/J naturally imbeds into K°, it is finite-dimensional cosemisimple, hence a group algebra of a finite group.

According to the one-to-one correspondence between normal subHopfalgebras and Hopf ideals, $J = H^\circ A^+$, where $A = (H^\circ)^{co(H^\circ/J)}$ is a normal subHopfalgebra of H°. As in the proof of Theorem 2.2.9, A is the identity component of H° under the grading corresponding to the H°/J-coaction. Hence it suffices to prove that A is PI.

By Lemma 3.1.3, $A = (HK^+)^\perp = (H/HK^+)^\circ$. Set $\tilde{H} = H/HK^+$. Then $\tilde{L} = L/(L \cap HK^+)$ is a subHopfalgebra of $\tilde{H}$. By faithful flatness (see Remark

2.2.8),

$$L \cap HK^+ = LK^+,$$

so $\tilde{L} = L/LK^+$ and thus $\tilde{L}$ is cocommutative.

Now consider the Hopf ideal $N = \tilde{L}^\perp$ of $\tilde{H}^\circ$. Again by the one-to-one correspondence, $N = \tilde{H}^\circ B^+$ for some normal subHopfalgebra $B \subset \tilde{H}^\circ$. By Lemma 3.1.3, $B = (\tilde{H}/\tilde{H}\tilde{L}^+)^\circ = (H/HL^+)^\circ$, so B is cosemisimple with dimension equal to a power of p, i.e. a group algebra of a finite p-group. Hence B^+ is nilpotent and so is $N = \tilde{H}^\circ B^+ = B^+\tilde{H}^\circ$. Finally, $\tilde{H}^\circ/N$ imbeds into $\tilde{L}^\circ$ and thus is commutative. It follows that $A = \tilde{H}^\circ$ is PI. ∎

Remark 3.2.6. It follows from [26] that $(G : A)(A' : 1)$ in condition 4) and therefore, $(G_i : A_i)(A'_i : 1)$ in the inverse limit in 3) (see Definition 3.2.4) and $\dim(K)\dim(H/HL^+)$ in condition 2) can be bounded by a function that depends only on the degree of the coidentity satisfied by H. Conversely, it can be deduced from the proof 2) $\Rightarrow$ 1) above that H satisfies an identity of degree bounded by a function of $\dim K$ and $\dim H/HL^+$ in 2), etc.

These results can be sharpened in a remarkable way if we assume that H is an integral domain.

Corollary 3.2.7. *Let H be a commutative Hopf algebra over any field $\Bbbk$. Assume further that H is an integral domain. Then H is PI as a coalgebra iff H is cocommutative.*

Proof. The nontrivial part is to show that if H is cPI, then H is cocommutative. Since H is a domain, so is $\bar{H}/\text{rad}\bar{H}$, where $\bar{H} = H \otimes \bar{\Bbbk}$. This follows from the fact that the condition "$H/\text{rad}H$ is a domain" is invariant under any field extension [36, Section 6.6] (this condition is equivalent to the connectedness of the affine group scheme associated with H). But then H imbeds into the domain $\bar{H}/\mathrm{rad}\bar{H}$, which is a Hopf algebra over $\bar{\Bbbk}$ and satisfies the same coidentity as H. Thus we have reduced the proof to the case of algebraically closed $\Bbbk$.

Since H is cPI, then by part 3) of Theorems 3.2.2 and 3.2.5, the group $G = \mathrm{Alg}(H, \Bbbk)$ is an inverse limit of algebraic groups G_i, each of which has a closed (p-)Abelian subgroup A_i of finite index. In terms of H we have: $H = \varinjlim \mathcal{O}(G_i)$, and without loss of generality, the canonical maps

$$\psi_i : \mathcal{O}(G_i) \to H$$

are injective (otherwise we can replace $\mathcal{O}(G_i)$ by $\mathcal{O}(G_i)/\mathrm{Ker}\psi_i$ and G_i by $\mathrm{Im}\varphi_i$, where $\varphi_i : G \to G_i$ are the canonical maps). But then all $\mathcal{O}(G_i)$ are integral domains, so G_i are connected and therefore, A_i must be equal to G_i and further A_i' must be trivial. Thus all G_i are Abelian and so $H = \varinjlim \mathcal{O}(G_i)$ is cocommutative. ■

3.3 Pseudoinvolutive Hopf Algebras

We can now extend our scope to include Hopf algebras that are not commutative, but can be twisted in a certain way to become commutative. These are the "pseudoinvolutive" Hopf algebras introduced in [15].

Definition 3.3.1. Let H be a Hopf algebra, $\beta : H \otimes H \to \Bbbk$ a linear map. The pair (H, β) is called a *cotriangular Hopf algebra* if β is a *skew-symmetric* *bicharacter*, i.e. for all $h, k, l \in H$ we have

$$\begin{aligned} \sum \beta(h_{(1)}, k)\beta(h_{(2)}, l), &= \beta(h, kl) && (3.3.1) \\ \sum \beta(h, l_{(2)})\beta(k, l_{(1)}), &= \beta(hk, l) && (3.3.2) \\ \sum \beta(h_{(1)}, k_{(1)})\beta(k_{(2)}, h_{(2)}) &= \varepsilon(hk), && (3.3.3) \end{aligned}$$

and H is *almost commutative* by virtue of β, i.e. for all $h, k \in H$,

$$\sum \beta(h_{(1)}, k_{(1)})k_{(2)}h_{(2)} = \sum h_{(1)}k_{(1)}\beta(h_{(2)}, k_{(2)}).$$

Note that (3.3.3) above says that $\beta(k, h)$ is the inverse of $\beta(h, k)$ under the convolution product $*$ (hence the term "skew-symmetric"). Clearly, (3.3.1) and (3.3.2) follow from each other in the presence of (3.3.3).

If (H, β) is a cotriangular Hopf algebra, then the square of the antipode S^2 is known to have the form (see e.g. [25, Proposition 10.2.12]):

$$S^2(h) = \sum u(h_{(1)})h_{(2)}u^{-1}(h_{(3)}),$$

where $u : H \to \mathbb{k}$ is the Drinfeld element ($u \in G(H^\circ)$) given by

$$u(h) = \sum \beta(h_{(2)}, Sh_{(1)}).$$

Therefore, S^2 preserves any subcoalgebra $C \subset H$.

From now on, $\mathbb{k}$ is algebraically closed of characteristic 0.

Definition 3.3.2. A cotriangular Hopf algebra (H, β) is called *pseudoinvolutive* if $\mathrm{tr}(S^2|_C) = \dim C$, for any finite-dimensional subcoalgebra $C \subset H$.

Suppose we have a Hopf algebra H and a left 2-cocycle $\sigma : H \otimes H \to \mathbb{k}$, where $\mathbb{k}$ is viewed as a trivial H-module so (0.2.3) becomes:

$$\sum \sigma(k_{(1)}, m_{(1)})\sigma(h, k_{(2)}m_{(2)}) = \sum \sigma(h_{(1)}, k_{(1)})\sigma(h_{(2)}k_{(2)}, m),$$

for all $h, k, m \in H$. Then we can define a new Hopf algebra H^σ in the following way: $H^\sigma = H$ as a vector space, with the multiplication given by

$$h \cdot_\sigma k = \sum \sigma(h_{(1)}, k_{(1)}) h_{(2)} k_{(2)} \sigma^{-1}(h_{(3)}, k_{(3)}), \qquad \forall h, k \in H,$$

the comultiplication the same as in H and the antipode

$$S^\sigma(h) = \sum \sigma(h_{(1)}, Sh_{(2)}) Sh_{(3)} \sigma^{-1}(Sh_{(4)}, h_{(5)}), \qquad \forall h \in H.$$

Remark 3.3.3. If σ is a left 2-cocycle on H, then its convolution inverse σ^{-1} is a right 2-cocycle on H and a left 2-cocycle on H^σ (see [3]). Clearly, $(H^\sigma)^{\sigma^{-1}} = H$, so our "cocycle twist" of a Hopf algebra is an invertible operation.

P.Etingof and S.Gelaki [15] proved the following result describing pseudoinvolutive cotriangular Hopf algebras.

Theorem 3.3.4. *Let (H, β) be a cotriangular Hopf algebra. Then (H, β) is pseudoinvolutive iff $H = \mathcal{O}(G)^\sigma$, for some pro-algebraic group G and a left 2-cocycle $\sigma : \mathcal{O}(G) \otimes \mathcal{O}(G) \to \Bbbk$, and*

$$\beta = (\sigma \circ \tau) * \beta_c * \sigma^{-1},$$

where τ is the "flip" $h \otimes k \to k \otimes h$ and $\beta_c = \frac{1}{2}(\varepsilon \otimes \varepsilon + \varepsilon \otimes c + c \otimes \varepsilon - c \otimes c)$, for some central element $c \in G$ of order ≤ 2. ∎

Combining this theorem with our Theorem 3.2.2 and using the fact that H and H^σ have the same comultiplication and the same subHopfalgebras, we get the following

Corollary 3.3.5. *Let H be a pseudoinvolutive cotriangular Hopf algebra. Then the following conditions are equivalent:*

1) H is PI as a coalgebra,

2) There exists a finite-dimensional subHopfalgebra $K \subset H$ and a left 2-cocycle $\sigma' : H \otimes H \to \mathbb{k}$ such that $H^{\sigma'}$ is commutative and $H/H \cdot_{\sigma'} K^+$ is cocommutative,

3) $H = \mathcal{O}(G)^{\sigma}$, where G is an Abelian-by-finite pro-algebraic group and $\sigma : \mathcal{O}(G) \otimes \mathcal{O}(G) \to \mathbb{k}$ is a left 2-cocycle.

■

Chapter 4

Divided Power Algebras and Power Series

4.1 Hyperalgebras and Formal Groups

In this section we will show, following J.Dieudonné [14, Section 1.2], how the dual topological algebra H^* for a Hopf algebra H can be constructed. If H is a coreduced hyperalgebra in the sense of Chapter 2, then H^* turns out to be an algebra of power series, with some additional structure which is equivalent to a "formal group law" (see below). Then in Section 4.2 we will use this formal group law to construct a certain group, and then apply Passman's criterion together with some topological ideas (suggested by the proof of Corollary 3.2.7) in order to prove Theorem 2.3.11. Section 4.3 is devoted to the proof of Theorem 2.3.19 and also uses the dual topological algebra.

Recall that in Section 0.4 we have established a duality between the category of vector spaces (without topology) and the category of pro-finite topological vector spaces. If C is a coalgebra, then $\Delta : C \to C \otimes C$ induces a map $\Delta^* : (C \otimes C)^* \to C^*$ that we used in Section 0.1 to define the multiplication on the dual space C^*. Now we consider C^* not just as a vector space, but as a topological vector space (with the $*$-weak topology). Thus C^* becomes a pro-finite topological algebra. Conversely, suppose A is a pro-finite topological algebra with multiplication $m : A \otimes A \to A$. We know that $A = C^*$ as a topological vector space, where C is the space of continuous linear functions on A. Furthermore, we can extend m by continuity to the completed tensor product $A \hat{\otimes} A$, which is naturally isomorphic to $(C \otimes C)^*$, hence we obtain a continuous linear map $\hat{m} : (C \otimes C)^* \to C^*$. But then there exists $\Delta : C \to C \otimes C$ such that $\hat{m} = \Delta^*$, so C becomes a coalgebra. Thus we have established a duality between the category of coalgebras and the category of pro-finite topological algebras.

Now if H is a Hopf algebra, then H^* is a (pro-finite) topological algebra, and the multiplication and unit of H induce the continuous algebra maps $\mathcal{D} : H^* \to H^* \hat{\otimes} H^*$ and $\varepsilon : H^* \to \Bbbk$ such that the following two diagrams are commutative:

$$\begin{array}{ccc} H^* & \xrightarrow{\mathcal{D}} & H^* \hat{\otimes} H^* \\ \Big\downarrow{\scriptstyle \mathcal{D}} & & \Big\downarrow{\scriptstyle \mathcal{D} \hat{\otimes} id} \\ H^* \hat{\otimes} H^* & \xrightarrow[id \hat{\otimes} \mathcal{D}]{} & H^* \hat{\otimes} H^* \hat{\otimes} H^* \end{array} \tag{4.1.1}$$

so we can denote the diagonal map above by $\mathcal{D}_3 : H^* \to (H^*)^{\hat{\otimes} 3}$ and define by induction $\mathcal{D}_n : H^* \to (H^*)^{\hat{\otimes} n}$, and

$$\begin{array}{ccccc} H^*\hat{\otimes}H^* & \xleftarrow{\mathcal{D}} & H^* & \xrightarrow{\mathcal{D}} & H^*\hat{\otimes}H^* \\ & \searrow^{id\hat{\otimes}\varepsilon} & \downarrow{\scriptstyle id} & \swarrow_{\varepsilon\hat{\otimes}id} & \\ & & H^* & & \end{array} \tag{4.1.2}$$

The antipode of H, in its turn, induces a continuous anti-algebra map $\mathcal{S} : H^* \to H^*$ such that the following diagram commutes:

$$\begin{array}{ccccc} H^*\hat{\otimes}H^* & \xleftarrow{\mathcal{D}} & H^* & \xrightarrow{\mathcal{D}} & H^*\hat{\otimes}H^* \\ & \searrow^{m\circ(id\hat{\otimes}\mathcal{S})} & \downarrow{\scriptstyle \varepsilon} & \swarrow_{m\circ(\mathcal{S}\hat{\otimes}id)} & \\ & & H^* & & \end{array} \tag{4.1.3}$$

where $m : H^*\hat{\otimes}H^* \to H^*$ is the (extended) multiplication map.

We can summarize the above diagrams by saying that H^* is a "topological Hopf algebra" (but of course it is *not* a Hopf algebra in the usual sense). Conversely, any such pro-finite "topological Hopf algebra" has the form H^* for some (ordinary) Hopf algebra H. This is a version of *Cartier duality* [13].

Remark 4.1.1. An affine group scheme over $\Bbbk$ (that generalizes the "naïve" notion of algebraic group used in Chapter 3) is defined as a representable functor G from the category of commutative $\Bbbk$-algebras to the category of groups, i.e. to any commutative algebra A we assign a group $G(A)$ and there exists a commutative algebra H such that $G(A) = \mathrm{Alg}(H, A)$ as sets, for any A. It turns out that defining the group multiplication on all the sets $G(A)$ in a natural way is equivalent to defining a Hopf algebra structure on H (see [36]). Similarly, a formal group scheme over $\Bbbk$ can be defined as a representable functor G from the category of pro-finite commutative topological $\Bbbk$-algebras to the category of groups: $G(A) = \mathrm{Alg}_c(Z, A)$, the set of continuous algebra maps $Z \to A$, where Z is a pro-finite commutative topological algebra. Then Z turns out to be a "topological Hopf algebra" as defined above, so $Z = H^*$ for some (usual) cocommutative Hopf algebra H. In this context, the cocommutative Hopf algebra H is referred to as the *covariant algebra* of the formal group scheme G, whereas the commutative "topological Hopf algebra" H^* is referred to as the *contravariant algebra* of G (see [14]).

From now on, the field $\Bbbk$ is *perfect*. Let H be a coreduced hyperalgebra if $\operatorname{char}\Bbbk = p$ (recall that Definition 2.3.3 of a coreduced hyperalgebra was given only over a perfect field), or any hyperalgebra if $\operatorname{char}\Bbbk = 0$. Then by Theorem 2.3.6 (with $r_0 = 0$) and Remark 2.3.9, we can choose a basis of "divided powers" $\{z^{(\alpha)} | \alpha \in \mathbb{Z}_+^{(I)}\}$ in H. Defining $t_i \in H^*$ by $\langle t_i, z^{(\alpha)} \rangle = 1$ if $\alpha = \varepsilon_i$ and 0 otherwise, and setting $\mathbf{t}^\alpha = \prod_{i \in \operatorname{supp}\alpha} t_i^{\alpha(i)}$, we see that the formula for the iterated comultiplication

$$\Delta_n z^{(\beta)} = \sum_{\beta_1 + \dots + \beta_n = \beta} z^{(\beta_1)} \otimes \dots \otimes z^{(\beta_n)}$$

implies:

$$\langle \mathbf{t}^\alpha, z^{(\beta)} \rangle = \begin{cases} 1, & \text{if } \alpha = \beta, \\ 0, & \text{if } \alpha \neq \beta. \end{cases} \tag{4.1.4}$$

It now follows that the algebra H^*, with the $*$-weak topology, is isomorphic to the topological algebra of formal power series $\Bbbk[[t_i | i \in I]]$, which we will often abbreviate as $\Bbbk[[\mathbf{t}]]$. In terms of $\Bbbk[[\mathbf{t}]]$, the map $\varepsilon : H^* \to \Bbbk$ sends each power series to its constant term. Further, $H^* \hat{\otimes} H^*$ is clearly isomorphic to the topological algebra $\Bbbk[[u_i, v_i | i \in I]]$ of power series in the double set of variables (similarly $(H^*)^{\hat{\otimes}3}$, etc.). Then (4.1.1), (4.1.2), and (4.1.3) take the form of the following diagrams:

$$\begin{array}{ccc} \Bbbk[[\mathbf{t}]] & \xrightarrow{\mathcal{D}} & \Bbbk[[\mathbf{u},\mathbf{v}]] \\ {\scriptstyle\mathcal{D}}\downarrow & & \downarrow{\scriptstyle\mathcal{D}_{\mathbf{u}}} \\ \Bbbk[[\mathbf{u},\mathbf{v}]] & \xrightarrow[\mathcal{D}_{\mathbf{v}}]{} & \Bbbk[[\mathbf{u},\mathbf{v},\mathbf{w}]] \end{array} \tag{4.1.5}$$

where $\mathcal{D}_{\mathbf{u}}$ sends the series $\sum_{\alpha,\beta} \lambda_{\alpha,\beta}\mathbf{u}^\alpha\mathbf{v}^\beta$ to $\sum_{\beta} \mathcal{D}\left(\sum_{\alpha} \lambda_{\alpha,\beta}\mathbf{u}^\alpha\right)\mathbf{w}^\beta$, etc.,

$$\begin{array}{ccccc} \Bbbk[[\mathbf{u},\mathbf{v}]] & \xleftarrow{\mathcal{D}} & \Bbbk[[\mathbf{t}]] & \xrightarrow{\mathcal{D}} & \Bbbk[[\mathbf{u},\mathbf{v}]] \\ & {\scriptstyle\varepsilon_{\mathbf{v}}}\searrow & \downarrow{\scriptstyle id} & \swarrow{\scriptstyle\varepsilon_{\mathbf{u}}} & \\ & & \Bbbk[[\mathbf{t}]] & & \end{array} \tag{4.1.6}$$

where $\varepsilon_{\mathbf{u}}$ sends $\sum_{\alpha,\beta} \lambda_{\alpha,\beta}\mathbf{u}^\alpha\mathbf{v}^\beta$ to $\sum_{\beta} \lambda_{0,\beta}\mathbf{t}^\beta$, etc., and

$$\begin{array}{ccccc} \Bbbk[[\mathbf{u},\mathbf{v}]] & \xleftarrow{\mathcal{D}} & \Bbbk[[\mathbf{t}]] & \xrightarrow{\mathcal{D}} & \Bbbk[[\mathbf{u},\mathbf{v}]] \\ & {\scriptstyle\mathcal{S}_{\mathbf{v}}}\searrow & \downarrow{\scriptstyle\varepsilon} & \swarrow{\scriptstyle\mathcal{S}_{\mathbf{u}}} & \\ & & \Bbbk[[\mathbf{t}]] & & \end{array} \tag{4.1.7}$$

where $\mathcal{S}_{\mathbf{u}}$ sends $\sum_{\alpha,\beta} \lambda_{\alpha,\beta}\mathbf{u}^\alpha\mathbf{v}^\beta$ to $\sum_{\beta} \mathcal{S}\left(\sum_{\alpha} \lambda_{\alpha,\beta}\mathbf{t}^\alpha\right)\mathbf{t}^\beta$, etc.

Conversely, any pro-finite commutative "topological Hopf algebra" that is isomorphic to $\Bbbk[[\mathbf{t}]]$ as a topological algebra, gives rise to a hyperalgebra which is coreduced if $\operatorname{char}\Bbbk = p$.

Definition 4.1.2. A *formal group law* with (possibly infinite) index set I

over $\Bbbk$ is a family $\mathbf{f} = \{f_i\}_{i \in I}$ of elements of $\Bbbk[[\mathbf{u}, \mathbf{v}]] = \Bbbk[[u_i, v_i | i \in I]]$:

$$f_i(\mathbf{u}, \mathbf{v}) = \sum_{\alpha, \beta} \lambda_{\alpha,\beta}(i) \mathbf{u}^\alpha \mathbf{v}^\beta \tag{4.1.8}$$

such that the following conditions are satisfied:

1) $f_i(\mathbf{u}, \mathbf{v}) = u_i + v_i \pmod{\text{degree } 2}$, for all $i \in I$;

2) for any fixed $\alpha, \beta \in \mathbb{Z}_+^{(I)}$ there are only finitely many $i \in I$ such that $\lambda_{\alpha,\beta}(i) \neq 0$;

3) $\mathbf{f}(\mathbf{f}(\mathbf{u}, \mathbf{v}), \mathbf{w}) = \mathbf{f}(\mathbf{u}, \mathbf{f}(\mathbf{v}, \mathbf{w}))$ — this condition makes sense, because 2) above guarantees that computing the coefficients of the composite power series involves only finite sums (see [17, 9.6]).

It is well-known that for any formal group law $\mathbf{f} = \{f_i(\mathbf{u}, \mathbf{v})\}$ there exists a unique "inverse", i.e. a family of power series $\mathbf{g} = \{g_i(\mathbf{t})\}$ such that

$$f_i(\mathbf{t}, \mathbf{g}(\mathbf{t})) = f_i(\mathbf{g}(\mathbf{t}), \mathbf{t}) = 0, \qquad \forall i \in I. \tag{4.1.9}$$

Now any continuous algebra map $\mathcal{D} : \Bbbk[[\mathbf{t}]] \to \Bbbk[[\mathbf{u}, \mathbf{v}]]$ is uniquely determined by the images of the variables t_i. Moreover, the family $f_i = \mathcal{D}(t_i)$, $i \in I$, will satisfy the condition 2) of Definition 4.1.2. Indeed, let α, β be fixed, then the set U of all power series $\sum_{\alpha', \beta'} \lambda_{\alpha',\beta'} \mathbf{u}^{\alpha'} \mathbf{v}^{\beta'}$ with $\lambda_{\alpha,\beta} = 0$ is a neighbourhood of 0 in $\Bbbk[[\mathbf{u}, \mathbf{v}]]$, hence there must be a neighbourhood U' of 0 in $\Bbbk[[\mathbf{t}]]$ such that $\mathcal{D}(U') \subset U$, but all t_i except a finite number will lie in U', hence the condition 2) for $f_i = \mathcal{D}(t_i)$. Conversely, for any family $\{f_i\}$ satisfying 2) we can construct a continuous algebra map $\mathcal{D} : \Bbbk[[\mathbf{t}]] \to \Bbbk[[\mathbf{u}, \mathbf{v}]]$ such that $\mathcal{D}(t_i) = f_i$, for all $i \in I$, by setting $\mathcal{D}(h(\mathbf{t})) = h(\mathbf{f}(\mathbf{u}, \mathbf{v}))$, all $h \in \Bbbk[[\mathbf{t}]]$.

Further, the axioms (4.1.5) and (4.1.6) are equivalent to the conditions 3) and 1) of Definition 4.1.2, respectively, and (4.1.7) is equivalent to (4.1.9) for $g_i = \mathcal{S}(t_i)$. Therefore, coreduced hyperalgebras in prime characteristic are precisely those hyperalgebras that arise from formal group laws (and in zero characteristic, all hyperalgebras arise from formal group laws). Recall here that the existence of antipode is automatic for hyperalgebras — this proves the existence of the "inverse" $\{g_i\}$ above.

Tracing back our two steps, we can even obtain the explicit structure of the hyperalgebra H correponding to the formal group law $\mathbf{f}(\mathbf{u},\mathbf{v})$ given by (4.1.8). H has a basis of "divided powers" $z^{(\alpha)}$, $\alpha \in \mathbb{Z}_+^{(I)}$, that satisfies (4.1.4). Let us express the product $z^{(\beta)}z^{(\gamma)}$ through the basis $\{z^{(\alpha)}\}$:

$$z^{(\beta)}z^{(\gamma)} = \sum_{\alpha} \mu_\alpha^{\beta,\gamma} z^{(\alpha)}.$$

Then applying $\mathbf{t}^\alpha \in H^*$ to both sides, we compute:

$$\mu_\alpha^{\beta,\gamma} = \langle \mathbf{t}^\alpha, z^{(\beta)}z^{(\gamma)} \rangle = \langle \mathcal{D}(\mathbf{t}^\alpha), z^{(\beta)} \otimes z^{(\gamma)} \rangle,$$

and recalling that $\mathcal{D}(\mathbf{t}^\alpha) = (\mathbf{f}(\mathbf{u},\mathbf{v}))^\alpha$, we see that $\mu_\alpha^{\beta,\gamma}$ is equal to the coefficient of $\mathbf{u}^\beta \mathbf{v}^\gamma$ in the power series

$$\prod_{i \in \operatorname{supp} \alpha} \left(\sum_{\beta',\gamma'} \lambda_{\beta',\gamma'}(i) \mathbf{u}^{\beta'} \mathbf{v}^{\gamma'} \right)^{\alpha(i)}.$$

Remark 4.1.3. If $\operatorname{char} \mathbb{k} = 0$, then the hyperalgebra that corresponds to the formal group law $\mathbf{f}$ is the universal envelope $U(L)$, where L is the Lie algebra of $\mathbf{f}$ (see [30]). In this sense, the hyperalgebra of a formal group law in prime characteristic is a replacement of $U(L)$ in zero characteristic.

Example 4.1.4. The simplest example of a formal group law with index set I is the "additive law":

$$f_i(\mathbf{u}, \mathbf{v}) = u_i + v_i, \qquad \forall i \in I.$$

The hyperalgebra corresponding to this formal group law is nothing else but the divided power algebra $D(I)$ introduced in Chapter 1 (Definition 1.5.4). If $\operatorname{char} \Bbbk = 0$, then $D(I) \cong \Bbbk[x_i | i \in I]$, which is also the universal envelope of the Abelian Lie algebra of dimension $|I|$.

In what follows, it will be necessary to extend the ring of scalars. Let A be a commutative complete topological algebra (in a moment we will assume that the topology of A is induced by a discrete valuation – see below). Obviously, $H^* = \Bbbk[[t_i | i \in I]]$, with the topology of the direct product of copies of $\Bbbk$, is a subspace of $A[[t_i | i \in I]]$, with the topology of the direct product of copies of A (hence complete). The A-submodule generated by $\Bbbk[[\mathbf{t}]]$ is dense in $A[[\mathbf{t}]]$ and isomorphic to $A \otimes \Bbbk[[\mathbf{t}]]$, so in fact $A[[\mathbf{t}]] \cong A \hat{\otimes} H^*$, the completion of $A \otimes \Bbbk[[\mathbf{t}]]$. Thus we can uniquely extend $\mathcal{D}$, ε, and $\mathcal{S}$ to continuous A-algebra maps $A[[\mathbf{t}]] \to A[[\mathbf{u}, \mathbf{v}]]$, $A[[\mathbf{t}]] \to A$, and $A[[\mathbf{t}]] \to A[[\mathbf{t}]]$, respectively, and (4.1.5), (4.1.6), and (4.1.7) continue to hold for the extended maps, which we will denote from now on by the same letters $\mathcal{D}$, ε, and $\mathcal{S}$.

Lemma 4.1.5. *Let $\varphi, \psi : A[[\mathbf{t}]] \to A$ be continuous A-module maps. Then there is a unique continuous A-module map $(\varphi, \psi) : A[[\mathbf{u}, \mathbf{v}]] \to A$ that sends $\mathbf{u}^\alpha \mathbf{v}^\beta$ to $\varphi(\mathbf{t}^\alpha)\psi(\mathbf{t}^\beta)$. Moreover, if φ, ψ are algebra maps, then so is (φ, ψ).*

Proof. The composition of the map

$$\sum_{\alpha,\beta} b_{\alpha,\beta} \mathbf{u}^\alpha \mathbf{v}^\beta \to \sum_{\alpha} \psi \left(\sum_{\beta} b_{\alpha,\beta} \mathbf{t}^\beta \right) \mathbf{t}^\alpha$$

with φ is clearly a continuous A-module map satisfying the desired property of (φ, ψ). The uniqueness follows from the fact that the monomials $\mathbf{u}^\alpha \mathbf{v}^\beta$ generate a dense A-submodule in $A[[\mathbf{u}, \mathbf{v}]]$. As to the last assertion, it suffices to check it only for the monomials and this is obvious. ■

Now the maps $\mathcal{D}$, ε, and $\mathcal{S}$ allow us to define a group structure on the set of all continuous A-algebra maps $\mathrm{Alg_c}(A[[\mathbf{t}]], A)$.

First we make the set $\mathrm{Hom_c}(A[[\mathbf{t}]], A)$ of all continuous A-module maps an A-algebra by virtue of (a topological version of) the convolution product: for any $\varphi, \psi \in \mathrm{Hom_c}(A[[\mathbf{t}]], A)$, we define

$$\varphi * \psi = (\varphi, \psi) \circ \mathcal{D}, \tag{4.1.10}$$

where $(\varphi, \psi) : A[[\mathbf{u}, \mathbf{v}]] \to A$ is as in Lemma 4.1.5 above.

Lemma 4.1.6. *The product on* $\mathrm{Hom_c}(A[[\mathbf{t}]], A)$ *thus defined is A-bilinear, associative and has a unit* ε.

Proof. Obviously, $*$ is A-bilinear, associativity and the unit axiom follow directly from (4.1.5) and (4.1.6). ■

If φ, ψ are algebra maps, then $\varphi * \psi$ is also an algebra map (as a composition of such). Moreover, from (4.1.7) it follows that the algebra map $\varphi \circ \mathcal{S}$ is the inverse of φ. Therefore, the subset $\mathrm{Alg_c}(A[[\mathbf{t}]], A)) \subset \mathrm{Hom_c}(A[[\mathbf{t}]], A)$ becomes a group under $*$.

From now to the end of this section, we will assume the indexing set I finite or countable, and A will be a fixed commutative $\Bbbk$-algebra with the discrete valuation $\nu : A \to \mathbb{Z}_+ \cup \{\infty\}$ satisfying

$$\nu(a) = \infty \text{ iff } a = 0,$$
$$\nu(\lambda) = 0 \text{ for any } 0 \neq \lambda \in \Bbbk,$$
$$\nu(ab) = \nu(a) + \nu(b) \text{ for any } a, b \in A,$$
$$\nu(a + b) \geq \min(\nu(a), \nu(b)) \text{ for any } a, b \in A.$$

Note in particular that $\Bbbk \subset A$ is discrete and A has no zero divisors. We will further assume that ν is nontrivial (i.e. there exists $a \in A$ with $\nu(a)$ other than 0 and ∞, which in particular implies that A is infinite), and A is complete with respect to ν. The latter is equivalent to saying that

$$\text{“a series } \sum_{n=0}^{\infty} a_n \text{ converges in } A \text{ iff } \lim_{n \to \infty} \nu(a_n) = \infty\text{”.} \tag{4.1.11}$$

Remark 4.1.7. If I is finite or countable, then the topology of $\Bbbk[[t_i|i \in I]]$ can be induced by a discrete valuation as follows. Let us fix some total order on I so that I can be identified with $\mathbb{N}$ or with its subset $\{1, \ldots, N\}$. For any $\alpha \in \mathbb{Z}_+^{(I)}$, define

$$\|\alpha\| = \sum_{i \in \operatorname{supp} \alpha} i\alpha(i).$$

Then for a power series f, we set $\nu(f)$ to be the lowest $\|\alpha\|$ such that $\mathbf{t}^\alpha$ occurs in f. It can be immediately verified that the topology induced by ν coincides with the topology of $\Bbbk[[t_i|i \in I]]$ defined earlier, in particular, ν is complete.

Lemma 4.1.8. *Suppose I is finite or countable. Then the set of all continuous A-algebra maps $\operatorname{Alg}_c(A[[t_i|i \in I]], A)$ is in one-to-one correspondence* *with the set of all families $\{a_i\}_{i\in I}$ of elements of A that satisfy $\nu(a_i) > 0$, for any $i \in I$, and, if I is infinite, $\lim_{i\to\infty} \nu(a_i) = \infty$.*

Proof. We will use the notation introduced in the remark above.

If $\varphi \in \mathrm{Alg}_c(A[[t_i|i \in I]], A)$, set $a_i = \varphi(t_i)$. Clearly, φ is uniquely determined by the family $\{a_i\}_{i\in I}$, and we must have $\nu(a_i) > 0$, since $\lim_{n\to\infty} t_i^n = 0$ in $A[[\mathbf{t}]]$, and $\lim_{i\to\infty} \nu(a_i) = \infty$ (in the case I is infinite), since $\lim_{i\to\infty} t_i = 0$ in $A[[\mathbf{t}]]$.

On the other hand, let $\{a_i\}_{i\in I}$ be a family satisfying the conditions of the lemma. If $I = \{1, \dots, N\}$, we set for convenience $a_i = 0$, for all $i > N$, so we can assume $I = \mathbb{N}$.

Fix a power series $f = \sum_\alpha b_\alpha \mathbf{t}^\alpha \in A[[\mathbf{t}]]$. For any $n \geq 0$, let us define

$$c_n = \sum_{\|\alpha\|=n} b_\alpha \prod_{i\in\operatorname{supp}\alpha} a_i^{\alpha(i)}.$$

Note that the sum above is finite and $\nu(c_n) \geq d(n)$, where

$$d(n) = \min_{\|\alpha\|=n} \sum_{i\in\operatorname{supp}\alpha} \nu(a_i)\alpha(i).$$

We will show that $\lim_{n\to\infty} d(n) = \infty$. Indeed, let $m \in \mathbb{N}$ be fixed. Since $\lim_{i\to\infty} \nu(a_i) = \infty$, there is $M \in \mathbb{N}$ such that $\nu(a_i) \geq m$ as soon as $i > M/m$. Suppose $n > M$ and $\|\alpha\| = n$. Then either there is $j \in \operatorname{supp}\alpha$ such that $j > n/m$, whence

$$\sum_{i\in\operatorname{supp}\alpha} \nu(a_i)\alpha(i) \geq \nu(a_j) \geq m$$

by the choice of M, or else $n = \|\alpha\| \leq \frac{n}{m} \sum_{i\in\operatorname{supp}\alpha} \alpha(i)$, whence

$$\sum_{i\in\operatorname{supp}\alpha} \nu(a_i)\alpha(i) \geq \sum_{i\in\operatorname{supp}\alpha} \alpha(i) \geq m.$$

In either case we obtained $\sum_{i\in\operatorname{supp}\alpha}\nu(a_i)\alpha(i)\geq m$, so $d(n)\geq m$, which proves our assertion.

Now by (4.1.11), we see that the series $\sum_{n=0}^{\infty}c_n$ is convergent in A and we define $\varphi(f)$ to be the sum of this series.

It is a standard computation with (absolutely) convergent series to show that φ thus defined is an algebra map. Finally, the set U of all the series $f=\sum_\alpha b_\alpha\mathbf{t}^\alpha\in A[[\mathbf{t}]]$ such that $\nu(b_\alpha)\geq d(n)$, for all α with $\|\alpha\|<n$, is an open set in $A[[\mathbf{t}]]$, and we have $\nu(\varphi(f))\geq d(n)$, for any $f\in U$, which proves that φ is continuous. ∎

Lemma 4.1.9. $\operatorname{Alg}_c(A[[\mathbf{t}]],A)$ *separates the elements of* $A[[\mathbf{t}]]$.

Proof. Let $0\neq f=\sum_\alpha b_\alpha\mathbf{t}^\alpha\in A[[\mathbf{t}]]$. Then we can write

$$f=\sum_{n=0}^{\infty}f_n,\text{ where } f_n=\sum_{\|\alpha\|=n}b_\alpha\mathbf{t}^\alpha$$

is the n-th homogeneous component with respect to $\deg(\mathbf{t}^\alpha)=\|\alpha\|$. Notice that all f_n are in fact polynomials.

Let n_0 be the minimal n with $f_n\neq 0$. Since ν is nontrivial, we can find $0\neq e\in A$ with $\nu(e)>0$. Since A is infinite and has no zero divisors, we conclude that there is a family $(c_i)_{i\in I}$ in A such that $f_{n_0}(\mathbf{c})\neq 0$. Let us set $a_i=e^{mi}c_i$, $i\in I$, where m will be chosen later.

According to Lemma 4.1.8, we can construct $\varphi\in\operatorname{Alg}_c(A[[\mathbf{t}]],A)$ with $\varphi(t_i)=a_i$, $i\in I$. Then we have

$$\varphi(f)=f_{n_0}(\mathbf{a})+\sum_{n=n_0+1}^{\infty}f_n(\mathbf{a}).$$

By definition of f_n, we have $f_n(\mathbf{a})=e^{mn}f_n(\mathbf{c})$. Therefore,

$$\nu(f_{n_0}(\mathbf{a}))=\nu(f_{n_0}(\mathbf{c}))+mn_0\nu(e)$$

and

$$\nu(f_n(\mathbf{a})) \geq mn\nu(e) \geq m\nu(e) + mn_0\nu(e),$$

for $n > n_0$. If we choose m such that $m\nu(e) > \nu(f_{n_0}(\mathbf{c}))$ (which is possible since $\nu(e) > 0$ and $\nu(f_{n_0}(\mathbf{c})) < \infty$), we will get $\varphi(f) \neq 0$. ■

4.2 PI Coreduced Hyperalgerbas Are Commutative

Our main goal in this section will be the proof of Theorem 2.3.11 which says that if a coreduced hyperalgebra over a perfect field of prime characteristic, or any hyperalgebra over a field of zero characterstic, is PI, then it is commutative. For brevity, we will simply say "coreduced hyperalgebra" when we mean a hyperalgebra of either of these two kinds.

So let H be a coreduced hyperalgebra. As we have just seen in Section 4.1, the dual algebra H^* is isomorphic to the algebra $\Bbbk[[t_i|i \in I]]$ of formal power series, for some set I. Moreover, if A is a commutative complete topological $\Bbbk$-algebra, the multiplication, unit, and antipode of H induce continuous algebra maps $\mathcal{D} : A[[\mathbf{t}]] \to A[[\mathbf{u}, \mathbf{v}]]$, $\varepsilon : A[[\mathbf{t}]] \to A$, and $\mathcal{S} : A[[\mathbf{t}]] \to A[[\mathbf{t}]]$. Using $\mathcal{D}$, ε, and $\mathcal{S}$, we have defined a group structure on the set $\mathrm{Alg_c}(A[[\mathbf{t}]], A)$ of continuous A-algebra maps. The idea of the proof will be to show that if H is PI, then so is the group algebra $\Bbbk\mathrm{Alg_c}(A[[\mathbf{t}]], A)$, and therefore Theorem 2.1.1 claims that the group $\mathrm{Alg_c}(A[[\mathbf{t}]], A)$ has a very specific form, which will further imply, by use of a Zariski-type topology, that the group must in fact be Abelian. Then by suitably specifying A, we will show that $\mathcal{D}$ is symmetric, which means that H is commutative.

To carry out this program, we will need some rather standard results for our Zarissky-type topology, which we shall prove nonetheless, for the sake of completeness and because our topology is not the classical Zarissky topology, as in Chapter 2: we use power series, possibly in infinitely many variables, instead of polynomials.

In what follows until the beginning of the proof of the main theorem, we will assume the indexing set I finite or countable, and the topology of A will be induced by a discrete valuation $\nu : A \to \mathbb{Z}_+ \cup \{\infty\}$, so our lemmas from Section 4.1 apply.

First we define a topology on $X = \mathrm{Alg}_c(A[[\mathbf{t}]], A)$. The closed sets will be all sets of the form

$$F(T) = \{\varphi \in X | \varphi(T) = 0\},$$

where $T \subset A[[\mathbf{t}]]$ is any subset.

Since $F(\{0\}) = X$, $F(\{1\}) = \emptyset$, $\cap F(T_\gamma) = F(\cup T_\gamma)$, and

$$F(T_1) \cup F(T_2) = F(T_1 T_2)$$

(the latter uses that A has no zero divizors), we see that we have indeed a topology on X.

Lemma 4.2.1. *Every point of X forms a closed subset.*

Proof. Let $\varphi \in X$, define $a_i = \varphi(t_i)$, $i \in I$, as in Lemma 4.1.8. Then $\{\varphi\} = F(\{a_i - t_i | i \in I\})$ and therefore $\{\varphi\}$ is closed. ∎

Lemma 4.2.2. *X is connected.*

Proof. We will prove a stronger property, namely that X is an irreducible topological space, i.e. for any closed subsets $F_1, F_2 \subset X$, $X = F_1 \cup F_2$ implies $X = F_1$ or $X = F_2$.

Assume that X is reducible, i.e. there exist proper closed subsets

$$F_1, F_2 \subset X \text{ with } F_1 \cup F_2 = X.$$

Since F_1, F_2 are closed, we can write $F_1 = F(T_1)$, $F_2 = F(T_2)$, for some $T_1, T_2 \subset A[[\mathbf{t}]]$. Since F_1, F_2 are proper, we can find $0 \neq f_1 \in T_1$ and $0 \neq f_2 \in T_2$. Then clearly $f_1 f_2 \neq 0$ and it is annihilated by $F_1 \cup F_2 = X$, which contradicts Lemma 4.1.9. ∎

Now let $X = \mathrm{Alg_c}(R, A)$, $X' = \mathrm{Alg_c}(R', A)$, where $R = A[[t_i | i \in I]]$, $R' = A[[v_j | j \in I']]$ (I and I' are finite or countable). Then any continuous A-algebra map $\Phi : R \to R'$ induces $\hat{\Phi} : X' \to X : \varphi \to \phi \circ \Phi$.

Lemma 4.2.3. *For any continuous A-algebra map $\Phi : R \to R'$, the corresponding map $\hat{\Phi} : X' \to X$ is continuous.*

Proof. For any closed subset $F(T) \in X$ we have $\hat{\Phi}^{-1}(F(T)) = F(\Phi(T))$, which is closed in X'. ∎

According to Lemma 4.1.8, we can identify the set

$$\mathrm{Alg_c}(A[[t_i, v_j | i \in I,\ j \in I']], A)$$

with the direct product $X \times X'$. We will always assume that $X \times X'$ is endowed with the Zarissky-type topology coming from this identification (and *not* the topology of direct product).

Lemma 4.2.4. *For any fixed $\varphi \in X$ and $\varphi' \in X'$, the imbeddings*

$$X \to X \times X' : \psi \to (\psi, \varphi') \text{ and } X' \to X \times X' : \psi' \to (\varphi, \psi')$$

are continuous. The "diagonal" imbedding $\delta : X \to X \times X : \psi \to (\psi, \psi)$ is also continuous.

Proof. By Lemma 4.2.3, it suffices to notice that each of the imbeddings is induced by a suitable continuous A-algebra map.

The imbedding $X \to X \times X' : \psi \to (\psi, \varphi')$ clearly corresponds to $\Phi' : A[[\mathbf{t}, \mathbf{v}]] \to A[[\mathbf{t}]]$, where

$$\Phi'\left(\sum_{\alpha,\beta} b_{\alpha,\beta}\mathbf{t}^\alpha \mathbf{v}^\beta\right) = \sum_\alpha \varphi'\left(\sum_\beta b_{\alpha,\beta}\mathbf{v}^\beta\right)\mathbf{t}^\alpha$$

is a continuous A-algebra map (since so is φ').

The imbedding $X' \to X \times X' : \psi' \to (\varphi, \psi')$ is similar.

As to $\delta : X \to X \times X : \psi \to (\psi, \psi)$, it is induced by the map $A[[\mathbf{t}, \mathbf{v}]] \to A[[\mathbf{t}]]$ given by

$$\sum_{\alpha,\beta} b_{\alpha,\beta}\mathbf{t}^\alpha \mathbf{v}^\beta \to \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} b_{\alpha,\beta}\right)\mathbf{t}^\gamma,$$

which is a continuous A-algebra map, since the inner sum on the right hand side is finite, for any γ. ∎

Now we recall that $\mathcal{D}$, ε and $\mathcal{S}$ turn $\mathrm{Alg_c}(A[[\mathbf{t}]], A)$ into a group, which we will denote by G. Let us now check that the group structure on G is compatible with the topology.

Lemma 4.2.5. *The maps*

$$\begin{aligned} \mu :&\quad G \times G \to G : (\varphi, \psi) \to \varphi * \psi, \\ \iota :&\quad G \to G : \varphi \to \varphi^{-1}, \text{ and} \\ [,] :&\quad G \times G \to G : (\varphi, \psi) \to \varphi\psi\varphi^{-1}\psi^{-1} \end{aligned}$$

are continuous.

Proof. Using the notation of Lemma 4.2.3, $\mu = \hat{\mathcal{D}}$, $\iota = \hat{\mathcal{S}}$, so they are continuous. As to $[,]$, we can write:

$$[,] = \mu \circ (\mu \times \mu) \circ (id \times id \times \iota \times \iota) \circ (id \times \tau \times id) \circ (\delta \times \delta),$$

where τ is the flip, and all these maps are continuous by Lemmas 4.2.3 and 4.2.4. ■

Remark 4.2.6. Since we use for $G \times G$ a topology different from the topology of direct product, G will *not* be a topological group in the usual sense. It should be mentioned that the classical algebraic groups with Zarissky topology are not topological groups because of the same reason.

We can now put all our topological facts together and prove the following

Proposition 4.2.7. *Let H be a coreduced hyperalgebra over $\Bbbk$ such that $\dim P(H)$ is finite or countable. Let A be a commutative $\Bbbk$-algebra with a nontrivial discrete valuation ν such that A is complete with respect to ν. If the $\Bbbk$-subalgebra spanned by the group $\mathrm{Alg_c}(A\hat{\otimes}H^*, A)$ in $\mathrm{Hom_c}(A\hat{\otimes}H^*, A)$ satisfies a nontrivial polynomial identity, then the group $\mathrm{Alg_c}(A\hat{\otimes}H^*, A)$ is Abelian.*

Proof. Denote $G = \mathrm{Alg_c}(A\hat{\otimes}H^*, A)$. According to a classical lemma due to Artin (see [22], Section 8.4), distinct elements of G will be Q-linearly independent, where Q is the field of quotients of A (recall that A has no zero divisors). Since $\Bbbk \subset Q$, it follows that the $\Bbbk$-subalgebra spanned by G is isomorphic to the group algebra $\Bbbk G$, hence the latter is PI, so by Theorem 2.1.1, there exist normal subgroups $G_0 \subset G_1$ in G such that G_0 and G/G_1

are finite and G_1/G_0 is Abelian (where in fact G_0 is a p-group if char $\Bbbk = p$ and G_0 is trivial if char $\Bbbk = 0$).

Now from Lemmas 4.2.5 and 4.2.4 it follows that the maps

$$G \to G : \varphi \to [\varphi, \psi_0] \text{ and } \psi \to [\varphi_0, \psi] \qquad (4.2.1)$$

are continuous, for any fixed $\varphi_0, \psi_0 \in G$. Since $[G_1, G_1] \subset G_0$ and G_0 is closed (according to Lemma 4.2.1), we conclude that $[\overline{G}_1, \overline{G}_1] \subset G_0$, where $\overline{G}_1$ is the closure of G_1.

Notice that $\overline{G}_1$ is a subgroup, because of the fact $G_1 * G_1 \subset G_1 \subset \overline{G}_1$ and the continuity of the maps $\varphi \to \phi * \psi_0$ and $\psi \to \phi_0 * \psi$, for any fixed $\varphi_0, \psi_0 \in G$ (Lemmas 4.2.5 and 4.2.4 again). Clearly, $\overline{G}_1 \supset G_1$ is of finite index in G, so G is a disjoint union of a finite number of $\overline{G}_1$-cosets, which are all closed. Now Lemma 4.2.2 implies that $\overline{G}_1 = G$.

Thus we have proved that $[G, G] \subset G_0$. From the continuity of the maps (4.2.1) and Lemmas 4.2.2 and 4.2.1 it follows that $[G, G]$ is trivial. ■

Now we are ready to prove the main result.

Proof of Theorem 2.3.11.

We need to show that if H is PI, then H is commutative.

We start by choosing a basis of "divided powers" in H as in Theorem 2.3.6 (with $r_0 = 0$):

$$H = \text{span}\{z^{(\gamma)} | \gamma \in \mathbb{Z}_+^{(I)}\},$$

so we can identify H^* with the algebra of formal power series $\Bbbk[[t_i | i \in I]]$.

Suppose H satisfies a nontrivial multilinear identity of degree n over $\Bbbk$:

$$\sum_{\pi \in S_n} \lambda_\pi X_{\pi(1)} \dots X_{\pi(n)} = 0, \tag{4.2.2}$$

for all $X_1, \dots, X_n \in H$.

Let A be a commutative complete topological $\Bbbk$-algebra. On $A \hat{\otimes} H^* \cong A[[\mathbf{t}]]$, we have defined a map $\mathcal{D} : A[[\mathbf{t}]] \to A[[\mathbf{u}, \mathbf{v}]]$. Taking into account (4.1.5), we can iterate $\mathcal{D}$ to obtain a well-defined map

$$\mathcal{D}_n : A[[\mathbf{t}]] \to A[[\mathbf{t}_1, \dots, \mathbf{t}_n]].$$

We are going to show that $A \hat{\otimes} H^*$ satisfies a "coidentity" of the form (cf. Definition 1.1.2, but H^* is not a coalgebra in the usual sense):

$$\sum_{\pi \in S_n} \lambda_\pi \pi \mathcal{D}_n f = 0, \text{ for any } f \in A[[\mathbf{t}]], \tag{4.2.3}$$

where a permutation $\pi \in S_n$ acts on $A[[\mathbf{t}_1, \dots, \mathbf{t}_n]]$ by sending $\mathbf{t}_k$ to $\mathbf{t}_{\pi(k)}$, $k = 1, \dots n$.

Since H^* spans a dense A-submodule in $A \hat{\otimes} H^*$ and the left-hand side of (4.2.3) is a continuous A-module map, it suffices to check (4.2.3) only for $f \in H^* = \Bbbk[[\mathbf{t}]]$. But then $\mathcal{D}_n f \in (H^*)^{\hat{\otimes} n} = (H^{\otimes n})^* = \Bbbk[[\mathbf{t}_1, \dots, \mathbf{t}_n]]$. Let us denote

$$\mathcal{D}_n f = \sum_{\alpha_1, \dots, \alpha_n} \mu_{\alpha_1, \dots, \alpha_n} \mathbf{t}_1^{\alpha_1} \dots \mathbf{t}_n^{\alpha_n}.$$

In order to prove that the left-hand side of (4.2.3) is 0, we must show that it vanishes on every $h_1 \otimes \dots \otimes h_n \in H^{\otimes n}$. Indeed,

$$\begin{aligned}
&\langle \sum_{\pi\in S_n} \lambda_\pi \pi \mathcal{D}_n f, h_1\otimes\ldots\otimes h_n\rangle \\
&= \sum_{\pi\in S_n} \lambda_\pi \langle \sum_{\alpha_1,\ldots,\alpha_n} \mu_{\alpha_1,\ldots,\alpha_n} \mathbf{t}_1^{\alpha_{\pi^{-1}(1)}}\ldots \mathbf{t}_n^{\alpha_{\pi^{-1}(n)}}, h_1\otimes\ldots\otimes h_n\rangle \\
&= \sum_{\pi\in S_n} \lambda_\pi \sum_{\alpha_1,\ldots,\alpha_n} \mu_{\alpha_1,\ldots,\alpha_n} \langle \mathbf{t}_1^{\alpha_{\pi^{-1}(1)}}, h_1\rangle\ldots\langle \mathbf{t}_n^{\alpha_{\pi^{-1}(n)}}, h_n\rangle \\
&= \sum_{\pi\in S_n} \lambda_\pi \langle \sum_{\alpha_1,\ldots,\alpha_n} \mu_{\alpha_1,\ldots,\alpha_n} \mathbf{t}_1^{\alpha_1}\ldots \mathbf{t}_n^{\alpha_n}, h_{\pi(1)}\otimes\ldots\otimes h_{\pi(n)}\rangle \\
&= \langle \mathcal{D}_n f, \sum_{\pi\in S_n} \lambda_\pi h_{\pi(1)}\ldots h_{\pi(n)}\rangle = 0,
\end{aligned}$$

since H satisfies (4.2.2).

Recall that the set $\mathrm{Hom}_c(A\hat{\otimes}H^*, A)$ of all continuous A-module maps is an algebra under convolution product. Let us show that (4.2.3) implies that $\mathrm{Hom}_c(A\hat{\otimes}H^*, A)$ satisfies the identity (4.2.2).

To this end, let $\varphi_1,\ldots,\varphi_n \in \mathrm{Hom}_c(A\hat{\otimes}H^*, A)$ and $f\in A\hat{\otimes}H^* \cong A[[\mathbf{t}]]$, then

$$\mathcal{D}_n f = \sum_{\alpha_1,\ldots,\alpha_n} a_{\alpha_1,\ldots,\alpha_n} \mathbf{t}_1^{\alpha_1}\ldots\mathbf{t}_n^{\alpha_n} \in A[[\mathbf{t}_1,\ldots,\mathbf{t}_n]],$$

and we can compute according to (4.1.10):

$$\begin{aligned}
&\left(\sum_{\pi\in S_n}\lambda_\pi\varphi_{\pi(1)}*\ldots*\varphi_{\pi(n)}\right)f\\
&=\sum_{\pi\in S_n}\lambda_\pi\sum_{\alpha_1,\ldots,\alpha_n}a_{\alpha_1,\ldots,\alpha_n}\varphi_{\pi(1)}(\mathbf{t}^{\alpha_1})\ldots\varphi_{\pi(n)}(\mathbf{t}^{\alpha_n})\\
&=\sum_{\pi\in S_n}\lambda_\pi\sum_{\alpha_1,\ldots,\alpha_n}a_{\alpha_1,\ldots,\alpha_n}\varphi_1(\mathbf{t}^{\alpha_{\pi^{-1}(1)}})\ldots\varphi_n(\mathbf{t}^{\alpha_{\pi^{-1}(n)}})\\
&=\sum_{\pi\in S_n}\lambda_\pi(\varphi_1,\ldots,\varphi_n)(\pi\mathcal{D}_nf)\\
&=(\varphi_1,\ldots,\varphi_n)\left(\sum_{\pi\in S_n}\lambda_\pi\pi\mathcal{D}_nf\right)=0,
\end{aligned}$$

where $(\varphi_1,\ldots,\varphi_n)$ denotes the element of $\mathrm{Hom}_c(A[[\mathbf{t}_1,\ldots,\mathbf{t}_n]],A)$ as defined (for $n=2$) in Lemma 4.1.5.

Now we will reduce the proof that H is commutative to the case when $\dim P(H)$ is finite or countable so that we can apply Proposition 4.2.7.

Recall $H=\mathrm{span}\{z^{(\gamma)}|\gamma\in\mathbb{Z}_+^{(I)}\}$. It suffices to show that

$$z^{(\alpha)}z^{(\beta)}=z^{(\beta)}z^{(\alpha)},$$

for any $\alpha,\beta\in\mathbb{Z}_+^{(I)}$. Let us fix α,β and define $I_0=\mathrm{supp}\,\alpha\cup\mathrm{supp}\,\beta$. Then I_0 is finite, so $H_0=\mathrm{span}\{z^{(\gamma)}|\,\mathrm{supp}\,\gamma\subset I_0\}$ is a subcoalgebra of countable dimension. Now, for any α_0,β_0 such that $\mathrm{supp}\,\alpha_0,\mathrm{supp}\,\beta_0\subset I_0$, we have

$$z^{(\alpha_0)}z^{(\beta_0)}=\sum\lambda_\gamma^{\alpha_0,\beta_0}z^\gamma, \tag{4.2.4}$$

where the sum is finite.

In general, for $z^{(\gamma)}$ occuring in the sum above, $\mathrm{supp}\,\gamma$ does not have to lie in I_0. Let us define $I_1=\cup\,\mathrm{supp}\,\gamma$, where the union is over all multiindices γ

occuring in (4.2.4) for various α_0, β_0 with $\operatorname{supp}\alpha_0, \operatorname{supp}\beta_0 \subset I_0$. Then I_1 is clearly finite or countable.

We can continue by induction and define the chain of subsets

$$I_0 \subset I_1 \subset I_2 \subset \dots$$

such that $H_n H_n \subset H_{n+1}$, where

$$H_n = \operatorname{span}\{z^{(\gamma)} | \operatorname{supp}\gamma \subset I_n\}$$

is a subcoalgebra, for any integer n.

Now setting $I_\omega = \cup_n I_n$ and

$$H_\omega = \cup_n H_n = \operatorname{span}\{z^{(\gamma)} | \operatorname{supp}\gamma \subset I_\omega\},$$

we see that H_ω is a subbialgebra. Moreover, the $z^{(\gamma)}$ above form a basis of "divided powers" for H_ω, therefore H_ω is coreduced. Finally, $P(H_\omega)$ has the cardinality of I_ω, which is finite or countable.

Since H_ω satisfies the same identity as H, then H_ω is commutative, assuming we established our result for the finite or countable case. But $z^{(\alpha)}, z^{(\beta)} \in H_\omega$, so they commute. Since α, β were arbitrary multiindices, we conclude that H is commutative.

So without loss of generality we may assume $\dim P(H)$ finite or countable. Then from Proposition 4.2.7 it follows that the group $G = \operatorname{Alg}_c(A\hat{\otimes}H^*, A)$ is Abelian, for any $\Bbbk$-algebra A with a nontrivial discrete valuation ν, complete with respect to ν. Let us set $A = \Bbbk[[\mathbf{u}, \mathbf{v}]]$, with ν being as in Remark 4.1.7.

Finally, let us choose "a pair of independent generic points" $\varphi, \psi \in G$, defined by $\varphi(t_i) = u_i$ and $\psi(t_i) = v_i$, for all $i \in I$. We know that φ and ψ

must commute. Then for any element $f \in H^*$, with $\mathcal{D}f = \sum_{\alpha,\beta} \lambda_{\alpha,\beta} \mathbf{u}^\alpha \mathbf{v}^\beta$, we obtain:

$$
\begin{aligned}
(\varphi * \psi)(f) &= \sum_{\alpha,\beta} \lambda_{\alpha,\beta} \varphi(\mathbf{t}^\alpha)\psi(\mathbf{t}^\beta) = \sum_{\alpha,\beta} \lambda_{\alpha,\beta} \mathbf{u}^\alpha \mathbf{v}^\beta, \\
(\psi * \varphi)(f) &= \sum_{\alpha,\beta} \lambda_{\alpha,\beta} \psi(\mathbf{t}^\alpha)\varphi(\mathbf{t}^\beta) = \sum_{\alpha,\beta} \lambda_{\beta,\alpha} \mathbf{u}^\alpha \mathbf{v}^\beta.
\end{aligned}
$$

So we have proved that $\mathcal{D}f$ is symmetric, for any $f \in H^*$, which in its turn implies that H is commutative, since $\mathcal{D} = m^*$, where m is the multiplication of H. ∎

4.3 Smash Products with Divided Power Algebra

The goal of this section is to prove Theorem 2.3.19. The case of zero characteristic is covered by Theorem 2.1.7, so from now on, $\operatorname{char} \mathbb{k} = p > 0$.

Let $H = D(I)$, the divided power algebra with index set I. Recall from Section 4.1 that

$$H^* \cong \mathbb{k}[[t_i | i \in I]]$$

as a topological algebra. Moreover, Example 4.1.4 (with $u_i = t_i \hat{\otimes} 1$ and $v_i = 1 \hat{\otimes} t_i$) gives that the map $\mathcal{D} : H^* \to H^* \hat{\otimes} H^*$ is defined by

$$\mathcal{D}t_i = t_i \hat{\otimes} 1 + 1 \hat{\otimes} t_i. \tag{4.3.1}$$

Using the dual algebra H^*, we now want to describe the bialgebra(=Hopf algebra) endomorphisms of H.

Lemma 4.3.1. *Let $H = D(I)$ and set $Q = \overline{\text{span}}\{t_i^{p^k} | i \in I, k \in \mathbb{Z}_+\} \subset H^*$, where $\overline{\text{span}}$ means the closed subspace generated by a given set. Then the set* End$H$ *of bialgebra endomorphisms of H is in one-to-one correspondence with the families of power series $\{q_i\}_{i\in I}$ in Q such that any given monomial occurs only in a finite number of q_i. Moreover, $\Phi^*(Q) \subset Q$, for any $\Phi \in$* End$H$.

Proof. Let $\Phi \in \text{End}H$, then Φ^* is a continuous endomorphism of H^* commuting with $\mathcal{D}$. Set $q_i = \Phi^*(t_i)$, $i \in I$. Then Φ^* (and therefore Φ) is uniquely defined by the family $\{q_i\}_{i\in I}$. Moreover, this family has the property that any fixed monomial occurs only in a finite number of q_i (this follows from the continuity of Φ^* — see the discussion after Definition 4.1.2). Moreover, (4.3.1) implies

$$\mathcal{D}q_i = q_i\hat{\otimes}1 + 1\hat{\otimes}q_i. \tag{4.3.2}$$

Let us determine which power series $f \in H^*$ satisfy the above equation, i.e. $\mathcal{D}f = f\hat{\otimes}1 + 1\hat{\otimes}f$. If $f = \sum_\alpha \mu_\alpha \mathbf{t}^\alpha$, then we can compute:

$$\mathcal{D}f = \sum_\alpha \mu_\alpha(\mathbf{t}\hat{\otimes}1 + 1\hat{\otimes}\mathbf{t})^\alpha = f\hat{\otimes}1 + 1\hat{\otimes}f = \sum_\alpha \mu_\alpha(\mathbf{t}^\alpha\hat{\otimes}1 + 1\hat{\otimes}\mathbf{t}^\alpha).$$

Therefore, if $\mu_\alpha \neq 0$, then the binomial coefficients $\binom{\alpha}{\beta}$ must be 0, for all $\beta \neq 0$ or α, which is only possible if $\alpha = p^k\varepsilon_i$, for some $k \in \mathbb{Z}_+$ and $i \in I$, as one can see from the following well-known lemma (sometimes called Lucas' Theorem — see e.g. [11]).

Lemma 4.3.2. *Let $0 \leq k \leq n$ be integers, p a prime. If $n = n_0 + pn_1 + \ldots + p^N n_N$ and $k = k_0 + pk_1 + \ldots + p^N k_N$ with $0 \leq k_l, n_l < p$, $l = 0, \ldots, N$, then*

$$\binom{n}{k} = \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_N}{k_N} \pmod p,$$

where by convention, $\binom{n_l}{k_l} = 0$ if $k_l > n_l$. ■

Thus we proved that any $f \in H^*$ with $\mathcal{D}f = f\hat{\otimes}1 + 1\hat{\otimes}f$ must have the form:

$$f = \sum_{i \in I} \sum_{k \in \mathbb{Z}_+} \mu_{i,k} t_i^{p^k},$$

i.e. $f \in Q$. Hence $q_i = \Phi^*(t_i) \in Q$, for all $i \in I$. It immediately follows that $\Phi^*(Q) \subset Q$.

Conversely, given a family of power series $\{q_i\}_{i \in I}$ satisfying the conditions of the lemma, we can construct a continuous endomorphism Ψ of the algebra H^* such that $\Psi(t_i) = q_i$, $i \in I$ (see the discussion after Definition 4.1.2 again). Moreover, since q_i satisfy (4.3.2), Ψ will commute with $\mathcal{D}$. Finally, using the continuity of Ψ, we can find an endomorphism Φ of H with $\Phi^* = \Psi$, which will preserve the bialgebra structure of H since Ψ preserves the structure of H^*. ■

Let us look more closely at the algebra structure of H. Set $x_{i,k} = z^{(p^k \varepsilon_i)}$, $i \in I$, $k \in \mathbb{Z}_+$, then

$$H \cong \Bbbk[x_{i,k} | i \in I, k \in \mathbb{Z}_+]/(x_{i,k}^p = 0),$$

the truncated polynomial algebra. To establish this isomorphism, we notice firstly, that indeed $x_{i,k}^p = 0$ and secondly, that every multiindex α can be uniquely written in the form $\alpha = \alpha_0 + p\alpha_1 + \ldots + p^N\alpha_N$ with $\alpha_k(i) < p$, for all $i \in I$, $k = 0, \ldots, N$, and then

$$z^{(\alpha)} = \prod_{i \in \operatorname{supp} \alpha} \prod_{k=0}^{N} \frac{1}{\alpha_k(i)!} (x_{i,k})^{\alpha_k(i)}.$$

In other words, $H \cong u(L)$, the restricted enveloping algebra of

$$L = \operatorname{span}\{x_{i,k} | i \in I, k \in \mathbb{Z}_+\}$$

with zero bracket and zero operation $[p]$.

We want to use certain results of Yu.Bahturin and V.Petrogradsky [6] on smash products of the form $u(L)\#\mathbb{k}G$, where a group G acts on $u(L)$ by automorphisms of L. However, if G acts on H by bialgebra automorphisms, it does not have to preserve L, so the results of [6] may not be applicable to a given action $\cdot$ of G on H. We are going to modify the action $\cdot$ in the following way. Using the fact that H is isomorphic to a truncated polynomial algebra, $H \cong \mathbb{k}[x_{i,k}]/(x_{i,k}^p = 0)$, we can define a grading on H. Let pr_m denote the projection on the m-th homogeneous component. Then, for $g \in G$, $l \in L$, we set

$$g * l = \mathrm{pr}_1(g \cdot L).$$

Obviously, $g * L \subset L$, for any $g \in G$.

Lemma 4.3.3. *L is a G-module under $*$.*

Proof. We want to prove that $g * (g' * l) = (gg') * l$, for any $l \in L$, $g, g' \in G$. Let $Q \subset H^*$ be as in Lemma 4.3.1 and $l_g : H \to H$ denote the bialgebra automorphism sending h to $g \cdot h$. By Lemma 4.3.1, $l_g^*(Q) \subset Q$, hence $l_g(Q^\perp) \subset Q^\perp$, i.e. $g \cdot Q^\perp \subset Q^\perp$. Notice that $Q^\perp$ is the set of all $h \in H$ with $\mathrm{pr}_1(h) = 0$, so we have $\mathrm{pr}_1(g \cdot h) = 0$ if $\mathrm{pr}_1(h) = 0$. Hence $\mathrm{pr}_1(g \cdot h) = pr_1(g \cdot \mathrm{pr}_1(h))$, for any $h \in H$, so we can compute:

$$g * (g' * l) = \mathrm{pr}_1(g \cdot \mathrm{pr}_1(g' \cdot l)) = \mathrm{pr}_1(g \cdot (g' \cdot l)) = \mathrm{pr}_1((gg') \cdot l) = (gg') * l.$$

■

As usual, we can extend $*$ to the action of G on $H = u(L)$ by algebra automorphisms. Now we are going to show that $*$ satisfies some kind of identity. The following general observation is due to Yu.Bahturin (a special case is proved in [6, Lemma 4.2]).

Proposition 4.3.4. *Let H be a Hopf algebra over $\Bbbk$, A a left H-module algebra via $H \otimes A \to A : h \otimes a \to h \cdot a$. If the smash product $R = A\#H$ is PI, then the action $\cdot$ satisfies a nontrivial "weak identity" of the form:*

$$\sum_{\pi \in S_n} \lambda_\pi (h_1 \cdot X_{\pi(1)}) \dots (h_n \cdot X_{\pi(n)}) = 0,$$

for all $h_1, \dots, h_n \in H$, $X_1, \dots, X_n \in A$.

Proof. Since R is PI, it satisfies a nontrivial identity of the form [6, Lemma 4.1]:

$$\sum_{\pi \in S_n} \lambda_\pi Y_0 X_{\pi(1)} Y_1 \dots Y_{n-1} X_{\pi(n)} Y_n \equiv 0, \tag{4.3.3}$$

for some $n \in \mathbb{N}$ and $\lambda_\pi \in \Bbbk$.

Now let us fix $X_1, \dots X_n \in A$ and $h_1, \dots h_n \in H$. Consider the coproduct $\Delta h_1 \in H$. We can write: $\Delta h_1 = u_1 \otimes v_1 + \dots + u_m \otimes v_m$, for some $m \in \mathbb{N}$ and $u_i, v_i \in H$, $i = 1, \dots, m$. For each i, we substitute in (4.3.3) $Y_0 = u_i$, $Y_1 = Sv_i Y_1'$, where Y_1' is an auxiliary variable, thus obtaining:

$$\sum_{\pi \in S_n} \lambda_\pi (u_i X_{\pi(1)} Sv_i) Y_1' X_{\pi(2)} Y_2 \dots Y_{n-1} X_{\pi(n)} Y_n \equiv 0. \tag{4.3.4}$$

Then summation over $i = 1, \dots m$ gives:

$$\sum_{\pi \in S_n} \lambda_\pi (h_1 \cdot X_{\pi(1)}) Y_1' X_{\pi(2)} Y_2 \dots Y_{n-1} X_{\pi(n)} Y_n \equiv 0, \tag{4.3.5}$$

where we took into account that $\sum_i u_i X_{\pi(1)} Sv_i = h_1 \cdot X_{\pi(1)}$ by definition of the smash product.

Then we can write: $\Delta h_2 = u_1{}' \otimes v_1' + \ldots + u_{m'}' \otimes v_{m'}'$ and proceed in the same way by substituting $Y_1' = u_i'$ and $Y_2 = Sv_i'Y_2'$, etc. At the end we will obtain the desired equality. ∎

We are now ready to prove the main result.

Proof of Theorem 2.3.19.

Suppose a group G acts on $D(I)$ by bialgebra automorphisms and consider the smash product $R = D(I)\#\Bbbk G$. If there exists a subgroup $A \subset G$ that is (p-)Abelian and acts trivially on $D(I)$, then the subalgebra

$$R_0 = D(I)\#\Bbbk A \subset R$$

is isomorphic to $D(I) \otimes \Bbbk A$, hence PI. Moreover, R is a finitely generated free R_0-module, so R imbeds into a matrix algebra over R_0. But a matrix algebra over a PI algebra is PI (e.g. by Regev Theorem — see Section 0.3), therefore R is PI.

Let us now prove the converse. So suppose that $D(I)\#\Bbbk G$ is PI. Applying Proposition 4.3.4 to the smash product $D(I)\#\Bbbk G$, we obtain a nontrivial "weak identity" for the given action $\cdot$ of G on $H = D(I)$:

$$\sum_{\pi \in S_n} \lambda_\pi (g_1 \cdot X_{\pi(1)}) \ldots (g_n \cdot X_{\pi(n)}) = 0, \tag{4.3.6}$$

for all $g_1, \ldots, g_n \in G$, $X_1, \ldots, X_n \in H$.

Without loss of generality, (4.3.6) is proper, i.e. it trivializes upon substitution of 1 for one of the variables $X_1, \ldots, X_n$ (if this is not the case, we obtain a nontrivial identity of lower degree). We claim that the modified action $*$ satisfies the same "weak identity" as $\cdot$, i.e.

$$\sum_{\pi \in S_n} \lambda_\pi (g_1 * X_{\pi(1)}) \ldots (g_n * X_{\pi(n)}) = 0, \tag{4.3.7}$$

for all $g_1, \ldots, g_n \in G$, $X_1, \ldots, X_n \in H$.

Since the identity is multilinear in $X_1, \ldots, X_n$ and proper, it suffices to prove (4.3.7) only when $X_1, \ldots, X_n$ are monomials in $x_{i,k}$. If $g \in G$ and $X = u_1 \ldots u_s$, where each of $u_1, \ldots, u_s$ is one of the $x_{i,k}$, then

$$\begin{aligned} g * X &= (g * u_1) \ldots (g * u_s) = \mathrm{pr}_1(g \cdot u_1) \ldots \mathrm{pr}_1(g \cdot u_s) \\ &= \mathrm{pr}_s((g \cdot u_1) \ldots (g \cdot u_s)) = \mathrm{pr}_s(g \cdot X), \end{aligned}$$

where we used the fact that $g \cdot H^+ \subset H^+$ and so $g \cdot u_1, \ldots, g \cdot u_s$ have zero constant terms.

Now we can rewrite each term on the left-hand side of (4.3.7) as follows:

$$\begin{aligned} &(g_1 * X_{\pi(1)}) \ldots (g_n * X_{\pi(n)}) \\ &= \mathrm{pr}_{s_{\pi(1)}}(g_1 \cdot X_{\pi(1)}) \ldots \mathrm{pr}_{s_{\pi(n)}}(g_n \cdot X_{\pi(n)}) \\ &= \mathrm{pr}_m((g_1 \cdot X_{\pi(1)}) \ldots (g_n \cdot X_{\pi(n)})), \end{aligned}$$

where $s_1 = \deg X_1, \ldots, s_n = \deg X_n$, $m = s_1 + \ldots + s_n$.

Finally,

$$\begin{aligned} &\sum_{\pi \in S_n} \lambda_\pi (g_1 * X_{\pi(1)}) \ldots (g_n * X_{\pi(n)}) \\ &= \mathrm{pr}_m \left(\sum_{\pi \in S_n} \lambda_\pi (g_1 \cdot X_{\pi(1)}) \ldots (g_n \cdot X_{\pi(n)}) \right) = 0. \end{aligned}$$

Let us now quote a slightly extended version of Theorem 6.1 in [6] (the proof does not need to be changed).

Theorem 4.3.5. *Suppose a group G acts by automorphisms on $H = u(L)$, the restricted envelope of some p-Lie algebra L. Assume that L is G-invariant* *and the action $*$ of G on H satisfies a "weak identity" (4.3.7) of degree n. Then there exists a subgroup $G_0 \subset G$ such that $(G : G_0) < n$ and*

$$\dim(g-1) * L \leq n^3 4^n,$$

for any $g \in G_0$. ■

Applying this result to our case, we can find a subgroup $G_0 \subset G$ of finite index such that $\dim(g-1) * L < \infty$, for any $g \in G_0$. Now we want to go back to our original action $\cdot$ of G on $H = u(L)$. Fix $g \in G_0$ and set $W = (g-1) * L$, so W is a finite-dimensional subspace of L. Denote by $l_g : H \to H$ the bialgebra automorphism sending h to $g \cdot h$, then $W = (\mathrm{pr}_1 \circ l_g - id)L = (\mathrm{pr}_1 \circ l_g - id)\mathrm{pr}_1 H$, so

$$W = \mathrm{Im}(\mathrm{pr}_1 \circ l_g \circ \mathrm{pr}_1 - \mathrm{pr}_1).$$

Therefore,

$$W^{\perp} = \mathrm{Ker}(\mathrm{pr}_1^* \circ l_g^* \circ \mathrm{pr}_1^* - \mathrm{pr}_1^*). \tag{4.3.8}$$

Since pr_1 is the projection of H on L with kernel $Q^{\perp}$, where Q is as in Lemma 4.3.1, then pr_1^* is the projection of H^* on Q, hence (4.3.8) implies that

$$(\mathrm{pr}_1^* \circ l_g^* - id)(Q \cap W^{\perp}) = 0. \tag{4.3.9}$$

Now recall that W is a finite dimensional subspace of H, so $W^{\perp} \subset H^*$ is defined by a finite number of linear equations each of which involves only a finite number of coefficients of the series. Hence there exists $N \in \mathbb{N}$ such that, for any $k > N$ and $i \in I$, we have $t_i^{p^k} \in W^{\perp}$, so by (4.3.9),

$$\mathrm{pr}_1^*(l_g^* t_i^{p^k}) = t_i^{p^k}.$$

Fix $i \in I$, $k > N$. By Lemma 4.3.1, $l_g^* t_i^{p^k} \in Q$, thus the above equation gives $l_g^* t_i^{p^k} = t_i^{p^k}$. Finally, if

$$l_g^* t_i = \sum_{j \in I} \sum_{l \in \mathbb{Z}_+} \mu_{j,l} t_j^{p^l},$$

then

$$t_i^{p^k} = l_g^* t_i^{p^k} = \sum_{j \in I} \sum_{l \in \mathbb{Z}_+} \mu_{j,l}^{p^k} t_j^{p^{k+l}}.$$

Therefore, all $\mu_{j,l} = 0$ except $\mu_{i,0} = 1$, which means that $l_g^* t_i = t_i$. Since $i \in I$ was arbitrary, we see that $l_g^* = id$, hence $l_g = id$, i.e. g acts trivially on H. Since g was an arbitrary element of G_0, G_0 acts trivially on H. By Passman's criterion, there exists a p-Abelian subgroup $G_1 \subset G$ of finite index. Setting $A = G_0 \cap G_1$ completes the proof of Theorem 2.3.19. ■

Bibliography

[1] Yu.Bahturin, Identical relations in Lie algebras, VNU Science Press, Utrecht, 1987

[2] Yu.Bahturin, Identities in the universal envelopes of Lie algebras, J. Austral. Math. Soc., 18 (1974), pp.10–21

[3] Yu.Bahturin, D.Fischman, and S.Montgomery, Bicharacters, twistings, and Scheunert's theorem for Hopf algebras, J. Algebra, 236(2001), pp.246–276

[4] Yu.Bahturin, A.Giambruno, and D.Riley, Group-graded algebras with polynomial identity, Israel J. of Math., 104(1998), pp.145–155

[5] Yu.Bahturin and V.Linchenko, Identities of algebras with actions of Hopf algebras, J. Algebra 202(1998), 634 - 654

[6] Yu.Bahturin and V.Petrogradsky, Polynomial identities in smash products, J. of Lie Theory, 12(2002), 2, pp.369–395

[7] J.Bergen and M.Cohen, Actions of commutative Hopf algebras, Bull. of London Math. Society, 18(1986), pp.159–164

[8] G.Birkhoff, On the structure of abstract algebras, Proc. Cambridge Phil. Soc., 31(1935), pp. 433–454

[9] R.Block, Commutative Hopf algebras, Lie coalgebras, and divided powers, J. Algebra, 96 (1985), pp.275–306

[10] R.Block and P.Leroux, Generalized dual coalgebras of algebras, with applications to cofree coalgebras, J. Pure and Applied Algebra, 36(1985), pp.15–21

[11] P.Cameron, Combinatorics: topics, techniques, algorithms, Cambridge University Press, 1994

[12] P.Cartier, Hyperalgèbres et groupes de Lie formels, Séminaire "Sophus Lie", 2e année, Paris, 1957

[13] P.Cartier, Arithmétique des groupes algébriques, Colloque sur la théorie des groupes algébriques, Bruxelles, 1962

[14] J.Dieudonné, Introduction to the theory of formal groups, Pure and Applied Mathematics, 20(1973), Marcel Dekker, New York

[15] P.Etingof and S.Gelaki, On cotriangular Hopf algebras, Amer. J. Math., 123(2001), 4, pp.699–713

[16] D.Handelman, J.Lawrence and W.Schelter, Skew group rings, Houston J. of Math., 4(1978), 2, pp.175–197

[17] M.Hazewinkel, Formal groups and applications, Pure and Applied Mathematics, 78(1978), Academic Press

[18] N.Jacobson, PI-algebras — An introduction,
Lecture Notes in Mathematics, 441(1975), Springer-Verlag, Berlin

[19] M.Kochetov, On identities for coalgebras and Hopf algebras,
Comm. Algebra, 28(2000), 3, pp.1211–1221

[20] M.Kochetov, PI Hopf algebras of prime characteristic,
to appear in J. Algebra

[21] M.Kochetov, Polynomial identities in Hopf algebras: Passman's theorem and its dual, to appear in Proceedings of International Workshop on Groups, Rings, Lie and Hopf Algebras, held in St.John's, May 2001

[22] S.Lang, Algebra, Addison-Wesley Pub., 1984

[23] V.N.Latyšev, Two remarks on PI algebras (Russian),
Sibirsk. Mat. Ž., 4(1963), pp.1120–1121

[24] J.Lewin, A matrix representation for associative algebras, I,
Trans. Am. Math. Soc., 188(1974), 2, p.293–308

[25] S.Montgomery, Hopf algebras and their actions on rings,
CMBS Regional Conference Series in Mathematics, 82(1993)

[26] D.Passman, Group rings satisfying a polynomial identity,
J. Algebra, 20(1972), pp.103–117

[27] D.Passman, Enveloping algebras satisfying a polynomial identity,
J. Algebra, 134(1990), 2, pp.469–490

[28] D.Passman, Infinite crossed products,
Pure and Applied Mathematics, 135(1989), Academic Press

[29] V.Petrogradsky, The existence of an identity in a restricted envelope, Mat. Zametki, 49(1991), 1, pp.84–93; translation in Math. Notes, 49(1991), 1-2, pp.60–66

[30] J.-P.Serre, Lie algebras and Lie groups (lectures given at Harvard University in 1964), Second edition,
Lecture Notes in Mathematics, 1500(1992), Springer-Verlag, Berlin

[31] H.J.Schneider, Lectures on Hopf algebras,
Universidad de Cordoba, Argentina, 1995

[32] M.Sweedler, Hopf algebras, Benjamin, New York, 1969

[33] M.Sweedler, Hopf algebras with one grouplike element,
Trans. Amer. Math. Soc., 127(1967), pp.515 - 526

[34] M.Sweedler, Weakening theorem on divided powers,
Trans. Amer. Math. Soc., 154(1971), pp.427 - 428

[35] E.Taft, The order of the antipode of a finite-dimensional Hopf algebra,
Proc. Nat. Acad. Sci. USA 68(1971), pp.2631–2633

[36] W.Waterhouse, Introduction to affine group schemes,
Graduate Texts in Mathematics, 66(1979), Springer–Verlag, New York