Classification of connected Hopf algebras up to prime-cube dimension

Xingting Wang

A dissertation submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2014

Reading Committee:

James Zhang, Chair

John Palmieri

Ralph Greenberg

Program Authorized to Offer Degree:
UW Department of Mathematics

ACKNOWLEDGMENTS

The author wishes to express sincere gratitude to his advisor Professor James Zhang, whose constant and extensive help makes this paper possible. The author would also like to thank Ralph Greenberg, John Palmieri for their careful reading of the paper. Finally, thanks are due to Yanhong Bao, Jiwei He, Jiafeng Lü, Cris Negron, Xuefeng Mao, Van C. Nguyen, Linhong Wang and Guangbin Zhuang for sharing their valuable ideas and insights.

DEDICATION

to my dear parents

University of Washington

Abstract

Classification of connected Hopf algebras up to prime-cube dimension

Xingting Wang

Chair of the Supervisory Committee:
Professor James Zhang
Department of Mathematics

We classify all connected Hopf algebras up to p^3 dimension over an algebraically closed field of characteristic $p > 0$ under the mild restriction such that in dimension p^3, we only work over odd primes p when the primitive space of these Hopf algebras is a two-dimensional abelian restricted Lie algebra. In a conclusion for any odd prime p, we have two isomorphism classes for the p-dimensional, eight isomorphism classes for the p^2-dimensional and fifty-five isomorphism classes, two finite and nine infinite parametric families for the p^3-dimensional.

TABLE OF CONTENTS

Page

Chapter 0

INTRODUCTION

Part of this thesis has been published as follows:

1 X. Wang, Connected Hopf algebras of dimension p^2, *J. Algebra*, 391 (2013), 93-113.

2 X. Wang, Local criteria for cocommutative Hopf algebras, *Comm. Algebra*, 42 (2014), no.12, 5180-5191.

3 L. Wang and X. Wang, Classification of pointed Hopf algebras of dimension p^2 over any algebraically closed field, *Algebr. Represent. Theory*, 17 (2014), no.4, 1267-1276.

4 V. Nguyen. L. Wang and X. Wang, Classification of connected Hopf algebras of dimension p^3 I, preprint, arXiv:1309.0286.

The phrase "Hopf algebra" was given by Borel in 1953, honoring the foundational work of Heinz Hopf in algebraic topology. Nowadays, progresses obtained in understanding the structure of Hopf algebras and their representations have been entwined with the development of different areas of mathematics such as knot theory, topology, conformal field theory, algebraic geometry, ring theory, category theory, combinatorics and etc.

Over the decades, there has been an ongoing project of classifying finite-dimensional Hopf algebras over the complex number. The classification has been done for certain dimensions; see [1, 7, 8, 9, 16]. Let p be a prime number. The following are the classification results of Hopf algebras of dimension p, p^2 and p^3 over the complex number.

- In 1994, Zhu [61] proved the Kaplansky's conjecture, that is, any p-dimensional Hopf algebra is isomorphic to the group algebra $\mathbb{C}[C_p]$.

- In 1996, Masuoka [33] proved that any semisimple p^2-dimensional Hopf algebra must be isomorphic to the group algebras $\mathbb{C}[C_{p^2}]$ or $\mathbb{C}[C_p \times C_p]$.

- In 1998, pointed Hopf algebras of dimension p^3 are classified independently by Andruskiewitsch and Schneider [4], Caenepeel and Dascalescu[14], Ştefan and Van Oystaeyen [44].

- In 2002, using results from [3] and [43], Ng [38] gave an affirmative answer to the question raised by Susan Montgomery asking whether the Taft algebras are the only non-semisimple Hopf algebras of dimension p^2.

The project of classifying all pointed Hopf algebras of dimension p, p^2 and p^3 over an algebraic closed field of characteristic $p > 0$ is a natural extension of the original work done over the complex number. And the most difficult part of this project is to classify all connected Hopf algebras of dimension up to p^3, which only appear over fields of positive characteristic. The only relate reference known to the author is Henderson's work [26], where all graded, co-commutative, connected Hopf algebras of dimension p^2 and p^3 are classified by using Singer's theory [42] of extensions of connected Hopf algebras. We use the theories of restricted Lie algebras and Hochschild cohomology of coalgebras for restricted universal enveloping algebras, which are studied in Chapter 2. One of the sources of finite-dimensional connected Hopf algebras comes from the dual Hopf algebras of the group algebra of any p-group. They turn out be the only semisimple ones in the sense of connectedness. We give an alternative proof of this fact in Chapter 3 due to Masuoka [34]. One consequence of our classification is that all the connected Hopf algebras of dimension $\leq p^2$ are co-commmutative. These finite-dimensional co-commutative Hopf algebra are also studied in Chapter 3.

Chapter 1

CLASSIFICATION RESULTS

Convention 1. Throughout we will use the following conventions:

- Throughout, we assume that the base field $\mathbf{k}$ is algebraically closed of characteristic $p > 0$.

- We use the expression $\boldsymbol{\omega}(t) = \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} t^i \otimes t^{p-i}$ for any variable t, where $\frac{(p-1)!}{i!(p-i)!} \in \mathbf{k}$ for each $1 \le i \le p-1$.

- A parametric family of Hopf algebras $H(\lambda)$ is said to be parametrized by $\mathbf{k}/\sqrt[n]{1}$ for some integer $n > 0$ such that $H(\lambda_1) \cong H(\lambda_2)$ if and only if $\lambda_1 = \gamma\lambda_2$ for some n-th root of unity γ.

- We use the standard notation $(H, m, u, \Delta, \epsilon, S)$ to denote a Hopf algebra and the primitive space of H is denoted by $\mathrm{P}(H)$.

- The augmentation ideal of H is denoted by H^+ and for two elements $x, y \in H$, we denote $\mathrm{ad}(x)y = [x, y]$ and $y(\mathrm{ad}x) = [y, x]$.

The classification starts in Chapter 4, where p and p^2-dimensional connected Hopf algebras are completely classified.

Theorem 1.0.1. *Let H be a connected Hopf algebra of dimension p. There are 2 isomorphism classes:*

(1) $\mathbf{k}[x]/(x^p)$*,*

(2) $\mathbf{k}[x]/(x^p - x)$*,*

where x is primitive.

Theorem 1.0.2. *Let H be a connected Hopf algebra of dimension p^2. When $\dim \mathrm{P}(H) = 2$, there are 5 isomorphism classes:*

(1) $\mathbf{k}\,[x, y] \,/\, (x^p, y^p)$,

(2) $\mathbf{k}\,[x, y] \,/\, (x^p - x, y^p)$,

(3) $\mathbf{k}\,[x, y] \,/\, (x^p - y, y^p)$,

(4) $\mathbf{k}\,[x, y] \,/\, (x^p - x, y^p - y)$,

(5) $\mathbf{k}\langle x, y\rangle / \,([x, y] - y, x^p - x, y^p)$,

where x, y are primitive. When $\dim \mathrm{P}(H) = 1$, there are three isomorphism classes:

(6) $\mathbf{k}\,[x, y] \,/(x^p, y^p)$,

(7) $\mathbf{k}\,[x, y] \,/(x^p, y^p - x)$,

(8) $\mathbf{k}\,[x, y] \,/(x^p - x, y^p - y)$,

where $\Delta\,(x) = x \otimes 1 + 1 \otimes x$ and $\Delta\,(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)$.

Regarding p^3-dimensional connected Hopf algebras, the classification is divided into two cases. In Chapter 5, we classify all p^3-dimensional connected Hopf algebras, except the case when the primitive space of the Hopf algebra is two-dimensional and abelian.

Theorem 1.0.3. *Let H be a connected Hopf algebra of dimension p^3 and suppose that $\dim \mathrm{P}(H) = 1$. If $p = 2$ then there are 5 isomorphism classes. Otherwise, there are four isomorphism classes and 1 infinite family.*

(1) $\mathbf{k}[x, y, z]/(x^p - x, y^p - y, z^p - z)$,

where x is primitive and

$$\Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x),$$
$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)[y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)]^{p-1} + \boldsymbol{\omega}(y),$$

and

(2) $\mathbf{k}[x,y,z]/(x^p, y^p - x, z^p - y)$,

(3) $\mathbf{k}[x,y,z]/(x^p, y^p, z^p)$,

(4) $\mathbf{k}[x,y,z]/(x^p, y^p, z^p - x)$,

(A5)

$p = 2$, $\mathbf{k}\langle x,y,z\rangle/(x^2, y^2, [x,y], [x,z], [y,z] - x, z^2 + xy)$,

$p > 2$, $A(\lambda) := \mathbf{k}\langle x,y,z\rangle/(x^p, y^p, [x,y], [x,z], [y,z] - x, z^p + x^{p-1}y - \lambda x)$,

where x is primitive and

$$\Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x),$$
$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \boldsymbol{\omega}(y).$$

Remark 1. When $p > 2$, $A(\lambda)$ is parametrized by $\mathbf{k}/\sqrt[p^2+p-1]{1}$.

Theorem 1.0.4. *Let H be a connected Hopf algebra of dimension p^3. When* $\dim \mathrm{P}(H) = 2$ *and it is nonabelian, there are 3 isomorphism classes:*

(1) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z], x^p - x, y^p, z^p)$, *where*

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(y),$$

(2) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z] - yf(x), x^p - x, y^p, z^p - z)$, *where* $f(x) = \sum_{i=1}^{p-1}(-1)^{i-1}(p-i)^{-1}x^i$ *and*

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x),$$

(3) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z] - z, [y,z] - y^2, x^p - x, y^p, z^p)$, *where $p > 2$ and*

$$\Delta(z) = z \otimes 1 + 1 \otimes z - 2x \otimes y.$$

In all the cases, x, y are primitive.

Theorem 1.0.5. *Let H be a connected Hopf algebra of dimension* p^3*. When* $\dim \mathrm{P}(H) = 3$*, there are* 15 *isomorphism classes and* 1 *finite parametric family:*

(1) $\mathbf{k}[x,y,z]/(x^p - x, y^p - y, z^p - z)$,

(2) $\mathbf{k}[x,y,z]/(x^p - y, y^p - z, z^p)$,

(3) $\mathbf{k}[x,y,z]/(x^p, y^p - z, z^p)$,

(4) $\mathbf{k}[x,y,z]/(x^p, y^p, z^p)$,

(5) $\mathbf{k}\langle x,y,z\rangle/([x,y] - z, [x,z], [y,z], x^p, y^p, z^p)$,

(6) $\mathbf{k}\langle x,y,z\rangle/([x,y] - z, [x,z], [y,z], x^p - z, y^p, z^p)$, *for* $p > 2$,

(7) $\mathbf{k}[x,y,z]/(x^p, y^p, z^p - z)$,

(8) $\mathbf{k}[x,y,z]/(x^p - y, y^p, z^p - z)$,

(9) $\mathbf{k}[x,y,z]/(x^p, y^p - y, z^p - z)$,

(10) $\mathbf{k}\langle x,y,z\rangle/([x,y] - z, [x,z], [y,z], x^p, y^p, z^p - z)$,

(11) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z], x^p - x, y^p, z^p)$,

(12) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z], x^p - x, y^p - z, z^p)$,

(13) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z], x^p - x, y^p, z^p - z)$,

(14) $\mathbf{k}\langle x,y,z\rangle/([x,y] - y, [x,z], [y,z], x^p - x, y^p - z, z^p - z)$.

(15) $\mathbf{k}\langle x,y,z\rangle/([x,y] - z, [x,z] - x, [y,z] + y, x^p, y^p, z^p - z)$, *for* $p > 2$,

(16) The parametric family

$$B(\lambda,\delta) := \mathbf{k}\langle x,y,z\rangle/([x,y],[x,z]-\lambda x,[y,z]-\lambda^{-1}y,x^p,y^p,z^p-\delta z),$$

for some $\lambda \in \mathbf{k}^\times$ *such that* $\delta := \lambda^{p-1} = \pm 1$.

In all the cases, x, y *are primitive.*

Remark 2. Two Hopf algebras $B(\lambda_1,\delta_1)$ and $B(\lambda_2,\delta_2)$ are isomorphic if and only if $\delta_1 = \delta_2$ and $\lambda_1 = \lambda_2$ or $\lambda_1 \cdot \lambda_2 = 1$. When $P = 2$, there is 1 isomorphism class in (16). When $p > 3$, (16) has p isomorphism classes.

In Chapter 6, we give a structure theorem for connected Hopf algebras with large abelian primitive space and classify such Hopf algebras by some cohomological type group. In Chapter 7, we apply our results to the p^3-dimensional connected Hopf algebras whose primitive space is two-dimensional and abelian.

Let $\mathfrak{g}$ be a two-dimensional restricted Lie algebra with fixed basis x, y, and $\mathfrak{h}$ be a one-dimensional restricted Lie algebra with fixed basis z. For constructing a type T, we have an algebraic representation ρ from $\mathfrak{h}$ to $\mathrm{End}_{\mathbf{k}}(\mathfrak{g})$. Then any Hopf algebra H satisfying the description above can be viewed as certain deformation of the restricted universal enveloping algebra of the semi-product $\mathfrak{g} \rtimes \mathfrak{h}$. Indeed, H can be presented as the quotient algebra $\mathbf{k}\langle x,y,z\rangle/\mathcal{I}$. The relation $\mathcal{I}$ is generated by

$$x^p - x^{[p]},\ y - y^{[p]},\ z^p - z^{[p]} + \Theta,\ [z,x] - \rho_z(x),\ [y,z] - \rho_z(y),$$

where $x^{[p]}, y^{[p]}, z^{[p]}$ denote the restricted maps in $\mathfrak{g}, \mathfrak{h}$ and

$$\Delta(x) = x\otimes 1 + 1\otimes x,\ \Delta(y) = y\otimes 1 + 1\otimes y,\ \Delta(z) = z\otimes 1 + 1\otimes z + \chi.$$

Our classification is complete by providing the compatible data (T, z, χ, Θ) in all isomorphism classes.

Theorem 1.0.6. *Let H be a connected Hopf algebra of dimension p^3. Suppose* char $\mathbf{k} = p > 2$ *and* $\dim \mathrm{P}(H) = 2$ *and abelian. For type (T1) given by* $x^p = 0, y^p = 0, z^p = 0, \rho = 0$, *there are* 8 *isomorphism classes:*

(1) $\chi = x \otimes y, \Theta = 0,$

(2) $\chi = x \otimes y, \Theta = x,$

(3) $\chi = \boldsymbol{\omega}(x), \Theta = 0,$

(4) $\chi = \boldsymbol{\omega}(x), \Theta = x,$

(5) $\chi = \boldsymbol{\omega}(x), \Theta = y,$

(6) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = 0,$

(7) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = x,$

(8) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = y,$

For type (T2) given by $x^p = 0, y^p = 0, z^p = 0, \rho_z(x) = y, \rho_z(y) = 0,$ *there are* 6 *isomorphism classes and* 2 *infinite parametric families:*

(9) $\chi = x \otimes y, \Theta = 0,$

(10) $\chi = x \otimes y, \Theta = y,$

(11) $\chi = \boldsymbol{\omega}(x), \Theta = xy^{p-1},$

(12) $\chi = \boldsymbol{\omega}(x), \Theta = xy^{p-1} + y,$

(13) $\chi = \boldsymbol{\omega}(y), \Theta = 0,$

(14) $\chi = \boldsymbol{\omega}(y), \Theta = y,$

(15) $C(\lambda) : \chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = xy^{p-1} + \lambda y,$

(16) $D(\lambda) : \chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda y.$

For type (T4) given by $x^p = 0, y^p = 0, z^p = z, \rho_z(x) = x, \rho_z(y) = \lambda y$ *for* $\lambda \in \mathbb{F}_p \setminus \{-1\}$, *there is* 1 *isomorphism class:*

(17) $\chi = x \otimes y, \Theta = 0$.

For type (T5) given by $x^p = x, y^p = 0, z^p = 0, \rho = 0$, *there are* 4 *isomorphism classes and* 1 *infinite parametric family:*

(18) $\chi = x \otimes y, \Theta = 0$,

(19) $\chi = x \otimes y, \Theta = y$,

(20) $\chi = \boldsymbol{\omega}(y), \Theta = 0$,

(21) $\chi = \boldsymbol{\omega}(y), \Theta = y$,

(22) $E(\lambda) : \chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda y$.

For type (T6) given by $x^p = x, y^p = 0, z^p = 0, \rho_z(x) = 0, \rho_z(y) = x$, *there is* 1 *isomorphism class and* 1 *infinite parametric family:*

(23) $\chi = x \otimes y, \Theta = 0$,

(24) $F(\lambda) : \chi = \lambda x \otimes y + \boldsymbol{\omega}(y), \Theta = (x^{p-1} - 1)y$.

For type (T7) given by $x^p = x, y^p = 0, z^p = z, \rho = 0$, *there is* 1 *isomorphism class:*

(25) $\chi = \boldsymbol{\omega}(x), \Theta = 0$.

For type (T8) given by $x^p = x, y^p = 0, z^p = z, \rho_z(x) = 0, \rho_z(y) = y$, *there are* 3 *isomorphism classes:*

(26) $\chi = x \otimes y, \Theta = 0$,

(27) $\chi = \boldsymbol{\omega}(x), \Theta = 0$,

(28) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = 0.$

For type (T9) given by $x^p = x, y^p = 0, z^p = z, \rho_z(x) = 0, \rho_z(y) = x + y$*, there are* 2 *infinite parametric families:*

(29) $G(\lambda) : \chi = \lambda x \otimes y, \Theta = -\frac{\lambda}{2}x^2,$

(30) $H(\lambda) : \chi = \lambda x \otimes y + \boldsymbol{\omega}(x), \Theta = -\frac{\lambda}{2}x^2.$

For type (T10) given by $x^p = y, y^p = 0, z^p = 0, \rho = 0$*, there are* 4 *isomorphism classes and* 1 *infinite parametric family:*

(31) $\chi = x \otimes y, \Theta = 0,$

(32) $\chi = x \otimes y, \Theta = x,$

(33) $\chi = \boldsymbol{\omega}(y), \Theta = 0,$

(34) $\chi = \boldsymbol{\omega}(y), \Theta = x,$

(35) $I(\lambda) : \chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda x.$

For type (T11) given by $x^p = y, y^p = 0, z^p = 0, \rho_z(x) = y, \rho_z(y) = 0$*, there is* 1 *isomorphism class and* 1 *infinite parametric family:*

(36) $\chi = x \otimes y, \Theta = 0,$

(37) $J(\lambda) : \chi = \lambda x \otimes y + \boldsymbol{\omega}(y), \Theta = 0.$

For type (T13) given by $x^p = y, y^p = 0, z^p = z, \rho_z(x) = x, \rho_z(x) = 0$*, there is* 1 *isomorphism class:*

(38) $\chi = x \otimes y, \Theta = 0.$

For type (T14) given by $x^p = y, y^p = 0, z^p = z, \rho_z(x) = x + y, \rho_z(y) = 0$*, there is* 1 *isomorphism class:*

(39) $\chi = x \otimes y, \Theta = -\frac{1}{2}y^2$.

For type (T16) given by $x^p = x, y^p = x, z^p = z, \rho = 0$, there are 3 isomorphism classes:

(40) $\chi = x \otimes y, \Theta = 0$,

(41) $\chi = \boldsymbol{\omega}(x), \Theta = 0$,

(42) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = 0$.

Remark 3. There are $\frac{p+1}{2}$ isomorphism classes in (T4).

Remark 4. The 8 infinite families of p^3-dimensional Hopf algebras are parametrized as follows: $C(\lambda)$ is parametrized by $\mathbf{k}/\{\pm 1\}$; $D(\lambda)$ is parametrized by $\mathbf{k}$; $E(\lambda)$ is parametrized by $\mathbf{k}/\sqrt[\frac{p-1}{2}]{1}$; $F(\lambda)$ is parametrized by $\mathbf{k}/\sqrt[\frac{p^2-1}{2}]{1}$; $G(\lambda)$ is parametrized by $\mathbf{k}/(\mathbb{F}_p^\times)^2$; $H(\lambda)$ is parametrized by $\mathbf{k}$; $I(\lambda)$ is parametrized by $\mathbf{k}/\sqrt[p^2-p-1]{1}$; $J(\lambda)$ is parametrized by $\mathbf{k}/\sqrt[p^2-p+1]{1}$.

Chapter 2

PRELIMINARY RESULTS

2.1 *Basic definitions and facts*

Throughout, $\mathbf{k}$ denotes a base field, algebraically closed of characteristic $p > 0$. All vector spaces, algebras, coalgebras, and tensor products are taken over $\mathbf{k}$ unless otherwise stated. Also, V^* denotes the vector space dual of any vector space V. We first give the definitions of algebras, coalgebras and Hopf algebras. A $\mathbf{k}$-algebra (with unit) is basically a $\mathbf{k}$-vector space satisfying associative and unit laws, which can be expressed via the following commutative diagrams.

Definition 1. A $\mathbf{k}$-algebra (with unit) is a $\mathbf{k}$-vector space A together with two $\mathbf{k}$-linear maps, *multipication* $m : A \otimes A \to A$ and *unit* $u : \mathbf{k} \to A$, such that the following diagrams are commutative:

(a) associativity

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

(b) unit

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

Coalgebras have structures dual to algebras. Hence we may dualize the notion of algebras by reversing all the arrows in the above diagrams.

Definition 2. A $\mathbf{k}$-coalgebra (with counit) is a $\mathbf{k}$-vector space C together with two $\mathbf{k}$-linear maps, *comultipication* $\Delta : C \to C \otimes C$ and *counit* $\epsilon : C \to \mathbf{k}$, such that the following diagrams are commutative:

(a) coassociativity

$$\begin{array}{ccc} C & \xrightarrow{\Delta} & C \otimes C \\ {\scriptstyle\Delta}\downarrow & & \downarrow{\scriptstyle\Delta\otimes id} \\ C \otimes C & \xrightarrow{id\otimes\Delta} & C \otimes C \otimes C \end{array}$$

(b) counit

$$\begin{array}{ccccc} k \otimes C & \xleftarrow{1\otimes id} & C & \xrightarrow{id\otimes 1} & C \otimes k \\ {\scriptstyle =}\downarrow & & \downarrow{\scriptstyle\Delta} & & \downarrow{\scriptstyle =} \\ k \otimes C & \xleftarrow{\epsilon\otimes id} & C \otimes C & \xrightarrow{id\otimes\epsilon} & C \otimes k \end{array}$$

Definition 3. A $\mathbf{k}$-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:

(a) Δ and ϵ are algebra morphisms,

(b) m and u are coalgebra morphisms.

To introduce the notion of Hopf algebras, we still need the following definition.

Definition 4. Let C be a coalgebra and A an algebra. Then $\mathrm{Hom}_{\mathbf{k}}(C, A)$ becomes an algebra under the *convolution product*

$$(f * g)(c) = m \circ (f \otimes g)(\Delta c)$$

for any $f, g \in \mathrm{Hom}_k(C, A)$ and $c \in C$. The unit element in $\mathrm{Hom}_{\mathbf{k}}(C, A)$ is $u\epsilon$.

Definition 5. Let $(H, m, u, \Delta, \epsilon)$ be a bialgebra. Then H is a *Hopf algebra* if there exists an element $S \in \mathrm{Hom}_{\mathbf{k}}(H, H)$ which is an inverse to id_H under convolution $*$. The element S is called an *antipode* for H.

By standard notations, we use $(H, m, u, \Delta, \epsilon, S)$ to denote a Hopf algebra. When H is finite-dimensional, we denote by H^* the *dual Hopf algebra* of H. Sweedler's notation is used to write the comultiplication of H, i.e., $\Delta(h) = \sum h_1 \otimes h_2$, for any $h \in H$. In the following, we recall more basic definitions and facts regarding H.

Definition 6. [35, Definitions 5.1.5, 5.2.1] The *coradical* H_0 of H is the sum of all simple subcoalgebras of H. The Hopf algebra H is *pointed* if every simple subcoalgebra is one-dimensional of the form $\mathbf{k}g$ where g is a group-like element, and H is *connected* if H_0 is one-dimensional. For each $n \geq 1$, set

$$H_n = \Delta^{-1}(H \otimes H_{n-1} + H_0 \otimes H).$$

The chain of subcoalgebras $H_0 \subseteq H_1 \subseteq \ldots \subseteq H_{n-1} \subseteq H_n \subseteq \ldots$ is said to be the *coradical filtration* of H.

Following the terminology in [6, Definition 1.13], we recall the definition of graded Hopf algebras.

Definition 7. Let H be a Hopf algebra with antipode S. If

(1) $H = \bigoplus_{n=0}^{\infty} H(n)$ is a graded algebra,

(2) $H = \bigoplus_{n=0}^{\infty} H(n)$ is a graded coalgebra,

(3) $S(H(n)) \subseteq H(n)$ for any $n \geq 0$,

then H is called a *graded Hopf algebra*. If in addition,

(4) $H = \bigoplus_{n=0}^{\infty} H(n)$ is a coradically graded coalgebra,

then H is called a *coradically graded Hopf algebra*. Also, the *associated graded Hopf algebra* of H is defined by $\mathrm{gr} H = \bigoplus_{n \geq 0} H_n / H_{n-1}$ $(H_{-1} = 0)$ with respect to its coradical filtration.

Theorem 2.1.1. *Let $H = \bigoplus_{n=0}^{\infty} H(n)$ be a finite-dimensional connected coradically graded Hopf algebra. Then H is isomorphic to $\mathbf{k}\left[x_1, x_2, \cdots, x_d\right] / \left(x_1^p, x_2^p, \cdots, x_d^p\right)$ for some $d \geq 0$ as algebras.*

Proof. Denote by $K = \bigoplus_{n=0}^{\infty} H(n)^*$ the graded dual of H. It is a graded Hopf algebra and connected for $K_0 \subseteq K(0) = H(0)^* = \mathbf{k}$ by [35, Lemma 5.3.4]. Moreover since H is coradically graded, by [5, Lemma 5.5], K is generated in degree one and hence cocommutative.

Therefore by duality H is commutative and local. Then according to [59, Theorem 14.4], H is isomorphic to $\mathbf{k}[x_1, x_2, \cdots, x_d]/(x_1^{p^{n_1}}, x_2^{p^{n_2}}, \cdots, x_d^{p^{n_d}})$ for some $d \geq 0$ as an algebra. Thus it suffices to prove inductively that for any homogeneous element $x \in H(n)$, we have $x^p = 0$ for all $n \geq 1$. Since H is coradically graded, $\mathrm{P}(H) = H(1)$. Then for any $x \in H(1)$, we have $x^p \in (H(1))^p \bigcap H(1) \subseteq H(p) \bigcap H(1) = 0$. Assume the assertion holds for $n \leq m-1$. Let $x \in H(m)$. By the definition of graded Hopf algebras we have:

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \sum_{i=1}^{m-1} y_i \otimes z_{m-i},$$

where $y_i, z_i \in H(i)$ for all $1 \leq i \leq m-1$. Therefore $\Delta(x^p) = x^p \otimes 1 + 1 \otimes x^p + \sum_{i=1}^{m-1} y_i^p \otimes z_{m-i}^p = x^p \otimes 1 + 1 \otimes x^p$ by induction. Thus $x^p \in (H(m))^p \bigcap H(1) \subseteq H(pm) \bigcap H(1) = 0$. ■

Corollary 2.1.2. *The associated graded Hopf algebra of a finite-dimensional connected Hopf algebra is isomorphic to* $\mathbf{k}[x_1, x_2, \cdots, x_d] / \left(x_1^p, x_2^p, \cdots, x_d^p\right)$ *for some* $d \geq 0$ *as algebras.*

Proof. The associated graded space $\mathrm{gr}H = \bigoplus_{n \geq 0} H_n/H_{n-1}$ is a graded Hopf algebra by [35, P. 62]. Also mentioned in [6, Definition 1.13], $\mathrm{gr}H$ is coradically graded. Therefore $\mathrm{gr}H$ is a coradically graded Hopf algebra, which is clearly connected because H is connected. Hence $\mathrm{gr}H$ satisfies all the conditions in Theorem 2.1.1 and the result follows. ■

As a consequence of the commutativity of the associated graded Hopf algebra for any finite-dimensional connected Hopf algebra we conclude that:

Corollary 2.1.3. *Let* H *be a finite-dimensional connected Hopf algebra. Then* $[H_n, H_m] \subseteq H_{n+m-1}$ *for all integers* n, m.

There are some basic properties of finite-dimensional Hopf algebras, which we use frequently.

Proposition 2.1.4. *Let* H *be a finite-dimensional Hopf algebra.*

(1) H *is local if and only if* H^* *is connected.*

(2) If H *is local, then any quotient or Hopf subalgebra of* H *is local.*

Furthermore assume that H is connected. Denote by $u\,(\mathrm{P}(H))$ the restricted universal enveloping algebra of $\mathrm{P}(H)$.

(3) Any quotient or Hopf subalgebra of H is connected.

(4) $\dim \mathrm{P}(H) = \dim J/J^2$, where J is the Jacobson radical of H^*.

(5) H is primitively generated if and only if $H \cong u\,(\mathrm{P}(H))$.

(6) $\dim u\,(\mathrm{P}(H)) = p^{\dim \mathrm{P}(H)}$.

(7) $\dim H = p^n$ for some integer n.

Proof. (1) and (4) are derived from [35, Proposition 5.2.9].

For (3) assume H is connected, H/I is connected by [35, Corollary 5.3.5], where I is any Hopf ideal of H. And for any Hopf subalgebra K of H, by [35, Lemma 5.2.12], $K_0 = K \bigcap H_0$. Since H_0 is one-dimensional, so is K_0. Thus K is connected.

(2) is the dual version of (3) by (1).

(5) is a standard result from [46, Proposition 13.2.3] and (6) comes from [35, P. 23].

(7) is true because the associated graded ring $\mathrm{gr}_J(H^*)$ with respect to its J-adic filtration is connected and primitively generated. Hence $\dim H = \dim H^* = \dim \mathrm{gr}_J(H^*) = p^n$, where $n = \dim \mathrm{P}(\mathrm{gr}_J(H^*))$ by (6). ■

Definition 8. [35, Definitions 3.4.1, 3.4.5] A Hopf subalgebra K of H is *normal* if both

$$\sum (Sh_1)kh_2 \subseteq K \text{ and } \sum h_1k(Sh_2) \subseteq K,$$

for all $k \in K, h \in H$. A Hopf ideal I of H is *normal* if both

$$\sum h_1Sh_3 \otimes h_2 \subseteq H \otimes I \text{ and } \sum h_2 \otimes (Sh_1)h_3 \subseteq I \otimes H,$$

for all $h \in I$.

Definition 9. Consider an inclusion of finite-dimensional connected Hopf algebras $K \subseteq H$.

(1) If $\dim K = p^m$ and $\dim H = p^n$, then the *p-index* of K in H is defined to be $n - m$.

(2) The *first order* of the inclusion is defined to be the minimal integer n such that $K_n \subsetneq H_n$. And we say it is infinity if $K = H$.

(3) The inclusion is said to be *level-one* if H is generated by H_n as an algebra, where n is the first order of the inclustion.

(4) The inclusion is said to be *normal* if K is a normal Hopf subalgebra of H.

Remark 5. By [35, Lemma 5.2.12], if D is a subcoalgebra of C, we have $D_n = D \bigcap C_n \subseteq C_n$. Also the coradical filtration is exhaustive for any coalgebra by [35, Theorem 5.2.2]. As a result of [35, Lemma 5.2.10], a connected bialgebra is automatically a connected Hopf algebra. Furthermore, it is well known that any sub-bialgebra of a connected Hopf algebra is a Hopf subalgebra. Let H be a connected Hopf algebra. Then the algebra generated by each term of the coradical filtration H_n is a connected Hopf subalgebra of H. Because each term of the coradical filtration H_n is a subcoalgebra and the algebra generated by it is certainly a sub-bialgebra.

2.2 Finite-dimensional connected Hopf algebras with Hopf subalgebras

In this section, we always assume $K \subseteq H$ is an inclusion of finite-dimensional connected Hopf algebras.

Lemma 2.2.1. *Suppose the inclusion $K \subseteq H$ has first order n. Then the p-index of K in H is greater or equal to* $\dim(H_n/K_n)$.

Proof. By Remark 5, the inclusion $K \hookrightarrow H$ induces an injection $K_i/K_{i-1} \hookrightarrow H_i/H_{i-1}$ for all $i \geq 1$. Thus $\mathrm{gr}K = \bigoplus_{i\geq 0} K(i) \hookrightarrow \mathrm{gr}H = \bigoplus_{i\geq 0} H(i)$ and $K(i) = H(i)$ for all $0 \leq i \leq n-1$ since n is the first order of the inclusion. Moreover by [6, Definition 1.13], $(\mathrm{gr}H)_m = \bigoplus_{0\leq i\leq m} H(m)$ for all $m \geq 0$ and the same is true for $\mathrm{gr}K$. Therefore it is enough to prove the result in the associated graded Hopf algebras inclusion $\mathrm{gr}K \subseteq \mathrm{gr}H$.

For simplicity, we write K for $\mathrm{gr}K$, H for $\mathrm{gr}H$ and use $\mathrm{d}(H/K)$ to denote the p-index of K in H. We will prove the result by induction on $\dim(H_n/K_n)$. When $\dim(H_n/K_n) = 1$, it is trivial. Now suppose that $\dim(H_n/K_n) > 1$ and choose any $x \in H(n) \setminus K(n)$. Because H is a graded coalgebra,

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \sum_{i=1}^{n-1} y_i \otimes z_{n-i},$$

where $y_i, z_i \in H(i) = K(i)$ for all $1 \leq i \leq n-1$. Hence K and x generate a Hopf subalgebra of H by Remark 5, which we denote as L. Now according to Theorem 2.1.1, we have $x^p = 0$. Thus $K \subseteq L$ has p-index one and first order n. Because H is a graded algebra, it is clear that L_n is spanned by K_n and x. Hence $\dim(L_n/K_n) = 1$ and $\dim(H_n/L_n) = \dim(H_n/K_n) - 1$. Therefore by induction we have

$$\begin{aligned} \dim(H_n/K_n) &= \dim(H_n/L_n) + \dim(L_n/K_n) = \dim(H_n/L_n) + 1 \\ &\leq \mathrm{d}(H/L) + 1 = \mathrm{d}(H/L) + \mathrm{d}(L/K) = \mathrm{d}(H/K). \end{aligned}$$

■

Lemma 2.2.2. *Let $K \subseteq H$ be a level-one inclusion with first order n. Then K is normal in H if and only if $[K, H_n] \subseteq K$.*

Proof. First suppose that K is normal in H. By [35, Lemma 5.3.2] for any $x \in H_n$, $\Delta(x) - x \otimes 1 - 1 \otimes x \in H_{n-1} \otimes H_{n-1} = K_{n-1} \otimes K_{n-1} \subseteq K \otimes K$. Thus we can write $\Delta(x) = x \otimes 1 + 1 \otimes x + \sum a_i \otimes b_i$ where $a_i, b_i \in K$. Apply the antipode S to get

$$S(x) = \epsilon(x) - x - \sum a_i S(b_i).$$

By the definition of normal Hopf subalgebras [35, Definition 3.4.1], for any $y \in K$

$$\sum x_1 y S(x_2) = xy + yS(x) + \sum a_i y S(b_i) = u \in K.$$

Therefore

$$[y, x] = yx - xy = y\left(\epsilon(x) - \sum a_i S(b_i)\right) + \sum a_i y S(b_i) - u \subseteq K,$$

which shows that $[K, H_n] \subseteq K$. Conversely suppose that $[K, H_n] \subseteq K$. Then it is clear that $K^+ H_n \subseteq H_n K^+ + K^+ \subseteq HK^+$ since $[K^+, H_n] \subseteq K^+$. We claim that $K^+(H_n)^i \subseteq HK^+$ for all $i \geq 0$ by induction. Suppose the inclusion holds for i and then for $i+1$:

$$K^+ (H_n)^{i+1} = K^+ (H_n)^i H_n \subseteq \left(HK^+\right) H_n \subseteq H\left(HK^+\right) \subseteq HK^+.$$

Therefore $K^+H = \bigcup K^+(H_n)^i \subseteq HK^+$ and by symmetry $K^+H = HK^+$. According to [35, Corollary 3.4.4], K is normal. ■

Lemma 2.2.3. *If $x \in H$ satisfies $[K, x] \subseteq K$ and $\Delta(x) - x \otimes 1 - 1 \otimes x \in K \otimes K$, then $\Delta\left(x^{p^n}\right) - x^{p^n} \otimes 1 - 1 \otimes x^{p^n} \in K \otimes K$ for all $n \geq 0$.*

Proof. First, we prove $\Delta\left(x^p\right) - x^p \otimes 1 - 1 \otimes x^p \in K \otimes K$. Denote $\Delta(x) = x \otimes 1 + 1 \otimes x + u$, where $u \in K \otimes K$. By Lemma 2.3.1, we have:

$$\Delta\left(x^p\right) = (x \otimes 1 + 1 \otimes x + u)^p = x^p \otimes 1 + 1 \otimes x^p + u^p + \sum_{i=1}^{p-1} S_i$$

where iS_i is the coefficient of λ^{i-1} in $u\left(\mathrm{ad}\left(\lambda u + x \otimes 1 + 1 \otimes x\right)\right)^{p-1}$. Hence it suffices to show inductively that

$$u\left(\mathrm{ad}\left(\lambda u + x \otimes 1 + 1 \otimes x\right)\right)^n \in (K \otimes K)\left[\lambda\right]$$

for all $n \geq 0$. Notice that when $n = 0$, it is just the assumption. Suppose it's true for $n - 1$ then for n

$$\begin{aligned} u\left(\mathrm{ad}\left(\lambda u + x \otimes 1 + 1 \otimes x\right)\right)^n &\in [(K \otimes K)\left[\lambda\right], \lambda u + x \otimes 1 + 1 \otimes x] \\ &\subseteq \{[K \otimes K, u] + [K, x] \otimes K + K \otimes [K, x]\}\left[\lambda\right] \\ &\subseteq (K \otimes K)\left[\lambda\right]. \end{aligned}$$

Now replace x with $x^{p^{n-1}}$ and we have $[K, x^{p^{n-1}}] = K\left(\mathrm{ad}(x)\right)^{p^{n-1}} \subseteq K$ by Lemma 2.3.1. Then the other cases can be proved in the similar way. ■

Lemma 2.2.4. *If $x \in H$ satisfies $\Delta(x) - x \otimes 1 - 1 \otimes x \in K \otimes K$ and $[K, x] \subseteq \sum_{0 \leq i \leq 1} Kx^i$. For each $n \geq 0$, set $L_n = \sum_{i \leq n} Kx^i$. Then we have the following*

(1) $[K, x^n] \subseteq L_n$ and L_n is a K-bimodule via the multiplication in H.

(2) $\Delta(x^n) - x^n \otimes 1 - 1 \otimes x^n \in L_{n-1} \otimes L_{n-1}$.

(3) L_n is a subcoalgebra of H.

(4) If H is generated by K and x as an algebra, then $H = \bigcup_{n\geq 0} L_n$.

Proof. (1) Since $xL_n \subseteq L_{n+1}$, we have $x^n L_1 \subseteq L_{n+1}$ for all $n \geq 0$. By assumption, it holds that $[K, x] \subseteq L_1$. Suppose $[K, x^{n-1}] \subseteq L_{n-1}$. For any $a \in K$, it follows that

$$x^n a \in x^{n-1}(ax + L_1) \subseteq \left(ax^{n-1} + L_{n-1}\right)x + x^{n-1}L_1 \subseteq ax^n + L_n.$$

Hence $[K, x^n] \subseteq L_n$ for each $n \geq 0$. Moreover, we have $L_n K \subseteq L_n$ for each $n \geq 0$, the left K-module L_n now becomes K-bimodule.

(2) Denote $\Delta(x) = x \otimes 1 + 1 \otimes x + u$, where $u \in K \otimes K$. We still prove by induction. When $n = 1$, it is just the assumption. Suppose it's true for $n - 1$. Write $\Delta(x^{n-1}) = x^{n-1} \otimes 1 + 1 \otimes x^{n-1} + \sum a_i \otimes b_i$, where $a_i, b_i \in L_{n-2}$. Therefore

$$\begin{aligned} & \Delta(x^n) - x^n \otimes 1 - 1 \otimes x^n \\ = \; & (x \otimes 1 + 1 \otimes x + u)\left(x^{n-1} \otimes 1 + 1 \otimes x^{n-1} + \sum a_i \otimes b_i\right) - x^n \otimes 1 - 1 \otimes x^n \\ \in \; & x \otimes x^{n-1} + x^{n-1} \otimes x + xL_{n-2} \otimes L_{n-2} + L_{n-2} \otimes xL_{n-2} + L_{n-2} \otimes L_{n-2} \\ \subseteq \; & L_{n-1} \otimes L_{n-1}. \end{aligned}$$

(3) Now because of (1) and (2), it is enough to check that L_n is a coalgebra by induction.

(4) Furthermore if H is generated by K and x as an algebra, it is easy to see $H = \bigcup_{n\geq 0} L_n$. ■

Theorem 2.2.5. *Let H be a finite-dimensional connected Hopf algebra with Hopf subalgebra K. Suppose the p-index of K in H is d and H is generated by K and some $x \in H$ as an algebra. Also assume that $\Delta(x) = x \otimes 1 + 1 \otimes x + u$, where $u \in K \otimes K$ and $[K, x] \subseteq \sum_{0\leq i\leq 1} Kx^i$. Then H is a free left K-module such that $H = \bigoplus_{i=0}^{p^d-1} Kx^i$. Furthermore if K is normal in H, then x satisfies a polynomial equation as follows:*

$$x^{p^d} + \sum_{i=0}^{d-1} a_i x^{p^i} + b = 0$$

for some $a_i \in \mathbf{k}$ and $b \in K$.

Proof. Denote $L_n = \sum_{0\le i\le n} Kx^i$ for all $n \ge 0$. By the Lemma 2.2.4(3), L_n is a subcoalgebra. Also H is a left K-module with generators $\{x^i | i \ge 0\}$ for $H = \sum Kx^i$. Because H is finite-dimensional, there exist some nontrivial relations between the generators such as

$$d_m x^m + d_{m-1}x^{m-1} + \cdots + d_1 x + d_0 = 0,$$

where $d_i \in K$ and $d_m \ne 0$, among which we choose the lowest degree in terms of x, say degree m. Furthermore denote $D = K$, $L = L_{m-1}$, $F = x^m$ and $V = \{a \in D | aF \in L\}$. As a result of Lemma 2.2.4(2), we know $\Delta(F) - x^m \otimes 1 - 1 \otimes x^m \in L \otimes L$. Then D, L, F satisfy all the conditions listed in [50, Lemma 1.1]. Hence $V = D$ for $0 \ne d_m \in V$. Thus $x^m \in \bigoplus_{i<m} Kx^i$ and consequently H is a free left K-module with the free basis $\{x^i | 0 \le i \le m-1\}$. Since $\dim H = m \dim K$, it is easy to see $m = p^d$ by definition.

Now assume that K is normal. Follow the proof in Lemma 2.2.2, we can show that $[K, x] \subseteq K$. From pervious discussion there exists a general equation for x:

$$x^{p^d} + \sum_{i=0}^{p^d-1} a_i x^i = 0, \tag{2.2.1}$$

where all $a_i \in K$. According to Lemma 2.2.3, we can write $\Delta\left(x^{p^n}\right) = x^{p^n} \otimes 1 + 1 \otimes x^{p^n} + u_n$, where $u_n \in K \otimes K$ for all $n \ge 0$. Now apply the comultiplication Δ to the above identity (2.2.1) to get

$$x^{p^d} \otimes 1 + 1 \otimes x^{p^d} + u_d + \sum_{i=0}^{p^d-1} \Delta(a_i)(x \otimes 1 + 1 \otimes x + u)^i = 0.$$

Replacing x^{p^d} with $\left(-\sum_{i=0}^{p^d-1} a_i x^i\right)$, the following equation is straightforward:

$$\left(-\sum_{i=0}^{p^d-1} a_i x^i\right) \otimes 1 + 1 \otimes \left(-\sum_{i=0}^{p^d-1} a_i x^i\right) \tag{2.2.2}$$

$$+\sum_{i=0}^{d-1} \Delta\left(a_{p^i}\right)\left(x^{p^i} \otimes 1 + 1 \otimes x^{p^i} + u_i\right) + \sum_{i\in S} \Delta\left(a_i\right)\left(x \otimes 1 + 1 \otimes x + u\right)^i + \Delta(a_0) + u_d = 0$$

with the p-index set $S = \{1, 2, \cdots, p^d\} \setminus \{1, p, p^2, \cdots, p^d\}$.

We first prove that $a_i = 0$ for all $i \in S$ by contradiction. If not, suppose $n \in S$ is the largest integer such that $a_n \ne 0$. The free K-module structure for H implies that the $K \otimes K$-module $H \otimes H$ has a free basis $\left\{x^i \otimes x^j | 0 \le i, j < p^d\right\}$. Thus the term $Kx^{n-i} \otimes Kx^i$ would only come from $\Delta(a_n)(x\otimes 1+1\otimes x+u)^n$ for all $1\le i\le n-1$. Moreover it exactly comes from $\Delta(a_n)(x\otimes 1+1\otimes x)^n$ by the choice of n. Therefore $\binom{n}{i}\Delta(a_n)\left(x^{n-i}\otimes x^i\right)=0$ for all $1\le i\le n-1$. Suppose $n=p^\alpha m$ where $m>1$ and $m\not\equiv 0 \pmod p$. Choose $i=p^\alpha$. Hence by [29, Lemma 5.1], $\binom{n}{p^\alpha}\equiv m \pmod p$. Then $\Delta(a_n)=0$, which implies that $a_n=0$, a contradiction. Therefore from equation (2.2.2), we deduce that $\Delta(a_{p^i})(x^{p^i}\otimes 1)=a_{p^i}x^{p^i}\otimes 1$ for all $0\le i\le d-1$. Thus $\Delta(a_{p^i})=a_{p^i}\otimes 1$. Then since H is counital, all of a_{p^i} are coefficients in the base field $\mathbf{k}$. ■

2.3 Restricted Lie algebras

We state the following technical lemma which is the key to our classification of finite-dimensional connected Hopf algebras.

Lemma 2.3.1. *[30, P. 186-187] For any associative* $\mathbf{k}$*-algebra* A*, we have*

$$(x+y)^p=x^p+y^p+\sum_{i=1}^{p-1}s_i(x,y)$$

where $is_i(x,y)$ *is the coefficient of* λ^{i-1} *in* $x\,(\mathrm{ad}(\lambda x+y))^{p-1}$ *and*

$$[x^p,y]=(\mathrm{ad}\ x)^p\,(y)$$

for any $x,y\in A$.

Definition 10. [30, Chapter V Def. 4] A *restricted Lie algebra* $\mathfrak{g}$ over $\mathbf{k}$ is a Lie algebra in which there is defined a map $\mathfrak{g}\to\mathfrak{g}$, i.e., $x\mapsto x^{[p]}$ such that

(1) $(\alpha x)^{[p]}=\alpha^p x^{[p]}$,

(2) $(x+y)^{[p]}=x^{[p]}+y^{[p]}+\sum_{i=1}^{p-1}s_i(x,y)$, where $is_i(x,y)$ is the coefficient of λ^{i-1} in $x\,(\mathrm{ad}(\lambda x+y))^{p-1}$,

(3) $\left[x,y^{[p]}\right]=x\,(\mathrm{ad}\ y)^p$,

for all $x,y\in\mathfrak{g}$ and $\alpha\in\mathbf{k}$.

Definition 11. Let $\mathfrak{g}$ be a restricted Lie algebra. Denote $\mathcal{U}(\mathfrak{g})$ as the usual universal enveloping algebra of $\mathfrak{g}$ and let B be the ideal in $\mathcal{U}(\mathfrak{g})$ generated by all $x^p - x^{[p]}, x \in \mathfrak{g}$, and define $u(\mathfrak{g}) = \mathcal{U}(\mathfrak{g})/B$. Then $u(\mathfrak{g})$ is called the *restricted universal enveloping algebra* of $\mathfrak{g}$.

A version of the PBW theorem holds for $u(\mathfrak{g})$: given a basis for $\mathfrak{g}$, the ordered monomials in this basis, where the exponent of each basis element is bounded by $p-1$, form a basis for $u(\mathfrak{g})$. Consequently if $\dim \mathfrak{g} = n$, then $\dim u(\mathfrak{g}) = p^n$.

Remark 6. In positive characteristic, the primitive space $\mathfrak{g} := \mathrm{P}(H)$ of a Hopf algebra H is a restricted Lie algebra, where the Lie bracket is given by the commutator and the restricted map is given by the p-th power map in H. Suppose K is the Hopf subalgebra of H generated by $\mathfrak{g}$. By [46, Proposition 13.2.3], we have $K \cong u(\mathfrak{g})$.

Let $\mathfrak{g}$ be a two-dimensional Lie algebra with basis $\{x, y\}$. There is, up to isomorphism, a unique two-dimensional non-abelian Lie algebra, and we can assume $[x, y] = y$ without loss of generality. The following result about two-dimensional restricted Lie algebras probably is well-known, see, e.g., [30, Chapter V §8].

Proposition 2.3.2. *Let $\mathfrak{g}$ be a two-dimensional restricted Lie algebra with basis $\{x, y\}$. Then the restricted maps can be classified as follows: When $\mathfrak{g}$ is abelian:*

(1) $x^{[p]} = 0, y^{[p]} = 0,$

(2) $x^{[p]} = x, y^{[p]} = 0,$

(3) $x^{[p]} = y, y^{[p]} = 0,$

(4) $x^{[p]} = x, y^{[p]} = y.$

When $\mathfrak{g}$ is non-abelian such that $[x, y] = y$:

(5) $x^{[p]} = x, y^{[p]} = 0.$

Proof. First suppose $\mathfrak{g}$ is abelian. Then by [30, Ex. 19], $\mathfrak{g}$ can be decomposed into a direct sum $\mathfrak{g} = \mathfrak{g}_0 \oplus \mathfrak{g}_1$, where $\mathfrak{g}_0^{p^n} = 0$ for sufficient large n and $\mathfrak{g}_1^p = \mathfrak{g}_1$. Define the non-commutative polynomial ring $\Phi = \{\alpha_0 + \alpha_1 t + \cdots \alpha_n t^n | \alpha_i \in \mathbf{k}\}$, where t is an indeterminate such that $t\alpha = \alpha^p t$. By comments [30, P. 192], $\mathfrak{g}_0$ can be viewed as a module over Φ with t acts on $\mathfrak{g}_0$ by the restricted map. Hence $\mathfrak{g}_0$ is annihilated by t^n for $n >> 0$. Notice that Φ is a PID. Thus

$$\mathfrak{g}_0 \cong \bigoplus_i \Phi/(t^{n_i})$$

as Φ-modules. Suppose $\dim \mathfrak{g}_1 = 0$. Then $\mathfrak{g}_0$ is either isomorphic to the cyclic module of dimension two over Φ, or isomorphic to the direct sum of two copies of the one-dimensional cyclic module over Φ. By applying [30, Chapter V §8 Thm. 13] to $\mathfrak{g}_1$, it is easy to see that the first one gives case (3) and the second one gives case (1). If $\dim \mathfrak{g}_1 = 1$, we have case (2). If $\dim \mathfrak{g}_1 = 2$, it is case (4). Moreover, they are all non-isomorphic because of the different decompositions and module structures over Φ. When $\mathfrak{g}$ is non-abelian, by the condition (3) of Definition 10, we have $[x, x^{[p]}] = [y, y^{[p]}] = [x, y^{[p]}] = 0$ and $[x^{[p]}, y] = y$. Since $[x, y] = y$, we have $x^{[p]} = x, y^{[p]} = 0$. ■

The following result about finite-dimensional abelian restricted Lie algebras can be easily derived from the discussion in [30, Chapter V, §8].

Proposition 2.3.3. *[30, Chapter V, §8] Let $\mathfrak{g}$ be an abelian restricted Lie algebra of dimension $m < \infty$. Then there exists a set of elements $\{x_1, \ldots, x_d, y_1, \ldots, y_s\} \subset \mathfrak{g}$, such that*

$$\mathfrak{g} = \Big(\oplus_{i=1}^d (\mathbf{k}x_i \oplus \mathbf{k}x_i^p \oplus \ldots \oplus \mathbf{k}x_i^{p^{n_i-1}}) \Big) \oplus \Big(\oplus_{j=1}^s \mathbf{k}y_j \Big)$$

where $0 \le d,\ s \le m$ are integers, $x_i^{p^{n_i}} = 0$, $y_j^p = y_j$, for all i and j, and $\sum_{i=1}^d n_i + s = m$.

Proof. Following [30, P.192], we consider the noncommutative polynomial ring

$$\Phi = \{\alpha_0 + \alpha_1 t + \cdots + \alpha_n t^n \mid \alpha_i \in \mathbf{k}\}.$$

The indeterminate t satisfies $t\alpha = \alpha^p t$ for any $\alpha \in \mathbf{k}$, and so t can be viewed as the restricted p-map on $\mathfrak{g}$. Note that Φ is a principal ideal domain. By [30, Ex. 19], $\mathfrak{g}$ has a p-invariant decomposition $\mathfrak{g} = \mathfrak{n} \oplus \mathfrak{s}$, where $\mathfrak{s}^p = \mathfrak{s}$ and $\mathfrak{n}^{p^n} = 0$ for some integer n sufficiently large.

When $\mathfrak{n} \neq 0$, as a module over Φ, it is a direct sum of torsion cyclic modules. That is, $\mathfrak{n} \cong \oplus_i \Phi/(t^{n_i})$ with $\sum n_i = \dim \mathfrak{n}$. For each $1 \le i \le d$, let x_i be the image of the generator of $\Phi/(t^{n_i})$ in $\mathfrak{n}$. Then

$$\bigcup_{i=1}^{d}\left\{x_i, x_i^p, \ldots, x_i^{p^{n_i-1}} \mid x_i^{p^{n_i}} = 0\right\}$$

is a basis for $\mathfrak{n}$. When $\mathfrak{s} \neq 0$, let $s = \dim \mathfrak{s}$. By [30, Chapter V, §8, Theorem 13], a basis for $\mathfrak{s}$ is $y_1, y_2, \ldots, y_s$ with $y_i^p = y_i$. The proof is completed by combining the bases of $\mathfrak{s}$ and $\mathfrak{n}$ together. ■

Remark 7. By [35, Theorem 2.3.3], $u(\mathfrak{s})$ is semisimple. Then, by [35, Corollary 2.3.5] and the fact that $\mathbf{k}$ is algebraically closed, we have

$$u(\mathfrak{s}) \cong (\mathbf{k}(\mathbb{Z}_p)^s)^* \cong \mathbf{k}[y]/(y^{p^s} - y),$$

where $s = \dim \mathfrak{s}$. Denote the image of y in $\mathfrak{s}$ by x. Then $\{x,\, x^p,\, \ldots,\, x^{p^{s-1}}\}$ with $x^{p^s} = x$ is another basis of $\mathfrak{s}$.

Now the classification of finite-dimensional primitively generated commutative Hopf algebras follows immediately.

Corollary 2.3.4. *Any p^m-dimensional primitively generated commutative Hopf algebra over $\mathbf{k}$ is isomorphic to a Hopf algebra in the form of*

$$\mathbf{k}[x_1, \ldots, x_d, y_1, \ldots, y_s]/(x_1^{p^{n_1}}, \ldots, x_d^{p^{n_d}},\, y_1^p - y_1, \ldots, y_s^p - y_s),$$

where all x_i's and y_j's are primitive elements, n_i's, d, and s are integers such that $\sum_i^d n_i + s = m$. In particular, such a Hopf algebra is semisimple if and only if $s = m$.

Remark 8. From Proposition 2.3.3 and Corollary 2.3.4, we see that the number $N(m)$ of isomorphism classes of m-dimensional abelian restricted Lie algebra (*resp.*, p^m-dimensional primitively generated commutative Hopf algebras) is just the partial sums of partition functions of positive integers, that is, $N(m) = \sum_{n=0}^{m} P(n)$, where $P(n)$ is the number of ways to write n as a sum of non-negative integers, regardless the order of summands.

2.4 Hochschild cohomology of restricted universal enveloping algebras

Suppose H is a Hopf algebra. Denote by $\mathbf{k}$ the trivial H-bicomodule. The Hochschild cohomology $\mathrm{H}^\bullet(\mathbf{k}, H)$ of H with coefficients in $\mathbf{k}$ can be computed as the homology of the differential graded algebra ΩH defined as follows [44, Lemma 1.1]:

- As a graded algebra, ΩH is the tensor algebra $T(H)$,

- The differential in ΩH is given by $d^0 = 0$ and for $n \geq 1$

$$d^n = 1 \otimes I_n + \sum_{i=0}^{n-1} (-1)^{i+1} I_i \otimes \Delta \otimes I_{n-i-1} + (-1)^{n+1} I_n \otimes 1.$$

This DG algebra is usually called the *cobar construction* of H. See [23, §19] for the basic properties of cobar constructions. Throughout, we will use $\mathrm{H}^\bullet(\mathbf{k}, H)$ to denote the homology of the DG algebra $(\Omega H, d)$.

Remark 9. We can also define the cobar construction on H by using its augmentation ideal H^+. The differentials of $T(H^+)$ are given by

$$d^n = \sum_{i=0}^{n-1} (-1)^{i+1}\ 1^i \otimes \overline{\Delta} \otimes 1^{n-i-1}, \text{ where } \overline{\Delta}(a) = \Delta(a) - a \otimes 1 - 1 \otimes a \text{ for any } a \in H^+. \tag{2.4.1}$$

In particular, we have $d^1(a) = -\overline{\Delta}(a)$ and $d^2(a \otimes b) = -\overline{\Delta}(a) \otimes b + a \otimes \overline{\Delta}(b)$ for any $a, b \in H^+$. It is well known that the complex $T(H^+)$ is quasi-isomorphic to $T(H)$. The alternative definition will be used in Chapter 6.

Lemma 2.4.1. *Let H be a finite-dimensional Hopf algebra. Thus*

$$\mathrm{H}^n(\mathbf{k}, H) \cong \mathrm{H}^n(H^*, \mathbf{k}) \cong \mathrm{Ext}^n_{H^*}(\mathbf{k}, \mathbf{k}),$$

for all $n \geq 0$.

Proof. We still denote by $\mathbf{k}$ the trivial H-bimodule. Then the first isomorphism comes from [44, Proposition 1.4]. Let M be a H-bimodule with the trivial right structure. We define the right structure of M^{ad} by $m.h = S(h)m$ using the antipode S of H for any $m \in M, h \in H$. Then it is easy to see $\mathbf{k}^{\mathrm{ad}} \cong \mathbf{k}$ as trivial right H-modules. Hence the second isomorphism is derived from [44, Theorem 1.5]. ■

Let $\mathfrak{g}$ be a restricted Lie algebra. We denote by $u(\mathfrak{g})$ the restricted universal enveloping algebra of $\mathfrak{g}$. Analogue to ordinary Lie algebras, restricted $\mathfrak{g}$-modules are in one-to-one correspondence with $u(\mathfrak{g})$-modules, i.e., a vector space M is a restricted $\mathfrak{g}$-module if there exists an algebra map $T : \mathfrak{u}(\mathfrak{g}) \to \mathrm{End}_{\mathbf{k}}(M)$.

Proposition 2.4.2. *Let $\mathfrak{g}$ be a restricted Lie algebra with basis $\{x_1, x_2, \cdots, x_n\}$. Then the image of*

$$\{\boldsymbol{\omega}(x_i),\ x_j \otimes x_k \mid 1 \leq i \leq n, 1 \leq j < k \leq n\}$$

is a basis in $\mathrm{H}^2(\mathbf{k}, u(\mathfrak{g}))$.

Proof. Denote $K = u(\mathfrak{g})$ and let C_p^n be the elementary abelian p-group of rank n. It is clear that K^* is isomorphic to $\mathbf{k}[C_p^n]$ as algebras. Then it follows from, e.g., [39, P. 558 (4.1)] that $\dim \mathrm{H}^2(K^*, \mathbf{k}) = \dim \mathrm{H}^2(C_p^n, \mathbf{k}) = n(n+1)/2$. Thus by Lemma 2.4.1, $\dim \mathrm{H}^2(\mathbf{k}, K) = n(n+1)/2$. First, it is direct to check that all $\boldsymbol{\omega}(x_i)$ and $x_j \otimes x_k$ are cocycles in $\boldsymbol{\omega}K$. We only check for $x_j \otimes x_k$ here. Notice that $d^2 = 1 \otimes I \otimes I - \Delta \otimes I + I \otimes \Delta - I \otimes I \otimes 1$. Thus

$$\begin{aligned} d^2(x_j \otimes x_k) &= 1 \otimes x_j \otimes x_k - \Delta(x_j) \otimes x_k + x_j \otimes \Delta(x_k) - x_j \otimes x_k \otimes 1 \\ &= 1 \otimes x_j \otimes x_k - (x_j \otimes 1 + 1 \otimes x_j) \otimes x_k + x_j \otimes (x_k \otimes 1 + 1 \otimes x_k) - x_j \otimes x_k \otimes 1 \\ &= 0. \end{aligned}$$

Secondly, we need to show they are linearly independent in $\mathrm{H}^2(\mathbf{k}, K) = \mathrm{Ker}\ d^2/\mathrm{Im}\ d^1$. We only deal with the case when $p \geq 3$. The remaining case of $p = 2$ is similar. By the PBW Theorem, K has a basis formed by

$$\{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid 0 \leq i_1, i_2, \cdots, i_n \leq p-1\}.$$

Because the differential $d^1 = 1 \otimes I - \Delta + I \otimes 1$ in ΩK only uses the comultiplication, without loss of generality, we can assume $\mathfrak{g}$ to be abelian. Suppose each variable x_i of K has degree one. Assign the usual total degree to any monomial in K. Also the total degree of a tensor product $A \otimes B$ in $K \otimes K$ is the sum of the degrees of A and B in K. Therefore d^1 preserves the degree from K to $K \otimes K$ for any monomial. Notice that $\boldsymbol{\omega}(x_i)$ has degree p and $x_j \otimes x_k$ has degree two. We can treat them separately. Suppose that $\sum_i \alpha_i \boldsymbol{\omega}(x_i) \in \mathrm{Im} d^1$. First, we consider the ideal $I = (x_2, \cdots, x_n)$ in K. By passing to the quotient K/I, we have $\alpha_1 \boldsymbol{\omega}(\overline{x_1}) \in \mathrm{Im}\ \overline{d^1}$, where $\overline{d^1} : K/I \to K/I \otimes K/I$. But every monomial in K/I, which is generated by x_1, has degree less than p. This forces that $\alpha_1 = 0$. The same argument works for all the coefficients. Now suppose $\sum_{j<k} \alpha_{jk} x_j \otimes x_k \in \operatorname{Im} d^1$. Therefore there exists $\sum_{j\leq k} \lambda_{jk} x_j x_k \in K$ such that

$$\begin{aligned}\sum_{j<k} \alpha_{jk}\ x_j \otimes x_k &= d^1 \left(\sum_{j\leq k} \lambda_{jk}\ x_j x_k \right) \\ &= \sum_{j\leq k} \lambda_{jk} \left(1 \otimes x_j x_k - \Delta(x_j x_k) + x_j x_k \otimes 1\right) \\ &= -\sum_{j\leq k} \lambda_{jk} \left(x_j \otimes x_k + x_k \otimes x_j\right).\end{aligned}$$

By applying the PBW Theorem to $K \otimes K$, we have all the coefficients equal zero. This completes the proof. ■

Lemma 2.4.3. *Let $\mathfrak{g}$ be a restricted Lie algebra. Then the cocycle*

$$\sum_{i=1}^{n} \alpha_i^p\ \boldsymbol{\omega}\left(x_i\right) - \boldsymbol{\omega}\left(\sum_{i=1}^{n} \alpha_i\ x_i \right)$$

is zero in $\mathrm{H}^2\left(\mathbf{k}, u(\mathfrak{g})\right)$, *where* $x_i \in \mathfrak{g}$ *and* $\alpha_i \in \mathbf{k}$ *for all* $1 \leq i \leq n$.

Proof. Denote by K the restricted universal enveloping algebra of $\mathfrak{g}$. First, it is direct to check that $\boldsymbol{\omega}(x)$ is a cocycle in $(\Omega K, d)$ for any $x \in \mathfrak{g}$. Hence the expression in the statement is also a cocycle in $(\Omega K, d)$. We only need to show that it lies in the coboundary $\operatorname{Im} d^1$. Without loss of generality, we can assume $\mathfrak{g}$ to be finite-dimensional. Note that $\mathbf{k}$ is algebraically closed of characteristic p. We can consider the p-adic Witt vectors $\mathcal{W}$ over $\mathbf{k}$, which is a discrete valuation ring with parameter p whose residue field is $\mathbf{k}$ [25, Theorem 6.19]. Then we can view $\mathfrak{g}$ as a free module over $\mathcal{W}$ with a Lie bracket [,], representing all the relations between a chosen basis for $\mathfrak{g}$. Denote by $A = \mathcal{U}(\mathfrak{g})$ the universal enveloping algebra of $\mathfrak{g}$ over $\mathcal{W}$, which is a Hopf algebra as usual. There is a quotient map $\pi : A \to A/(p) = K$. Therefore it suffices to prove that for any $x, y \in \mathfrak{g}$, there exists some $\Theta \in A$ such that

$$\boldsymbol{\omega}(x) + \boldsymbol{\omega}(y) - \boldsymbol{\omega}(x+y) = 1 \otimes \Theta - \Delta(\Theta) + \Theta \otimes 1. \tag{2.4.2}$$

The general result will follow by applying the quotient map π to (2.4.2), and the induction on the number of variables appearing in the expression. By Lemma 2.3.1, in $A \otimes_{\mathcal{W}} \mathcal{W}/(p) =$

$A/(p) = K$, there exists some $z \in \mathfrak{g}$ such that

$$(x+y)^p = x^p + y^p + z.$$

So back in A, we have some $\Theta \in A$ such that

$$(x+y)^p = x^p + y^p + z + p\ \Theta.$$

Thus in A, we can calculate $\Delta(x+y)^p$ in two different ways:

$$\begin{aligned}\Delta(x+y)^p &= (\Delta(x+y))^p \qquad \text{(I)}\\ &= ((x+y)\otimes 1 + 1\otimes (x+y))^p\\ &= (x+y)^p \otimes 1 + 1 \otimes (x+y)^p + p\ \boldsymbol{\omega}(x+y)\\ &= (x^p+y^p+z)\otimes 1 + 1\otimes (x^p+y^p+z) + p\ \Theta\otimes 1 + 1\otimes p\ \Theta + p\ \boldsymbol{\omega}(x+y).\end{aligned}$$

On the other hand,

$$\begin{aligned}\Delta(x+y)^p &= \Delta\left(x^p+y^p+z+p\ \Theta\right) \qquad \text{(II)}\\ &= x^p\otimes 1 + 1\otimes x^p + p\ \boldsymbol{\omega}(x) + y^p\otimes 1 + 1\otimes y^p + p\ \boldsymbol{\omega}(y) + z\otimes 1 + 1\otimes z + p\ \Delta(\Theta)\\ &= (x^p+y^p+z)\otimes 1 + 1\otimes (x^p+y^p+z) + p\ \boldsymbol{\omega}(x) + p\ \boldsymbol{\omega}(y) + p\ \Delta(\Theta).\end{aligned}$$

Therefore we have the following identity in $A \otimes A$.

$$p\ \{\boldsymbol{\omega}(x) + \boldsymbol{\omega}(y) - \boldsymbol{\omega}(x+y)\} = p\ \{1\otimes\Theta - \Delta(\Theta) + \Theta\otimes 1\}.$$

Since A is a domain, we can cancel p from both sides. This completes the proof. ■

Definition 12. Let H be a Hopf algebra. For any $x \in H$, define the adjoint map T_x on ΩH by

$$T_x^n = \sum_{i=0}^{n-1} I_i \otimes \mathrm{ad}(x) \otimes I_{n-i-1},$$

where $\mathrm{ad}(x)(H) = [x, H]$.

Lemma 2.4.4. *If H is any Hopf algebra, then T_x is a degree zero cochain map from ΩH to itself for all $x \in \mathrm{P}(H)$. Moreover, $\mathrm{P}(H) = \mathrm{H}^1(\mathbf{k}, H)$ and $\bigoplus_{n\geq 0} \mathrm{H}^n(\mathbf{k}, H)$ is a graded restricted $\mathrm{P}(H)$-module via the adjoint map.*

Proof. First, for simplicity write $T = T_x$ for some $x \in \mathrm{P}(H)$. We prove $d^n T^n = T^{n+1} d^n$ inductively for all $n \geq 0$. It is easy to check that it holds for $n = 0, 1$. Notice that

$$d^n = d^{n-1} \otimes I + (-1)^{n-1} I_{n-1} \otimes d^1,$$

for all $n \geq 2$. Thus

$$\begin{aligned}
&d^n T^n \\
&= \left(d^{n-1} \otimes I + (-1)^{n-1} I_{n-1} \otimes d^1\right) \left(T^{n-1} \otimes I + I_{n-1} \otimes T^1\right) \\
&= d^{n-1} T^{n-1} \otimes I + d^{n-1} \otimes T^1 + (-1)^{n-1} T^{n-1} \otimes d^1 + (-1)^{n-1} I_{n-1} \otimes d^1 T^1 \\
&= T^n d^{n-1} \otimes I + d^{n-1} \otimes T^1 + (-1)^{n-1} T^{n-1} \otimes d^1 + (-1)^{n-1} I_{n-1} \otimes T^2 d^1 \\
&= T^n d^{n-1} \otimes I + d^{n-1} \otimes T^1 + (-1)^{n-1} \left(T^{n-1} \otimes I_2 + I_{n-1} \otimes T^1 \otimes I\right) \left(I_{n-1} \otimes d^1\right) \\
&\quad + (-1)^{n-1} I_{n-1} \otimes (I \otimes T^1) d^1 \\
&= T^n d^{n-1} \otimes I + d^{n-1} \otimes T^1 + (-1)^{n-1} \left(T^n \otimes I\right) \left(I_{n-1} \otimes d^1\right) + (-1)^{n-1} I_{n-1} \otimes \left(I \otimes T^1\right) d^1 \\
&= \left(T^n \otimes I + I_n \otimes T^1\right) \left(d^{n-1} \otimes I + (-1)^{n-1} I_{n-1} \otimes d^1\right) \\
&= T^{n+1} d^n
\end{aligned}$$

Therefore T induces an action of $\mathrm{P}(H)$ on $\mathrm{H}^n(\mathbf{k}, H)$ for each n. Moreover, we know $\mathrm{P}(H)$ is a restricted Lie algebra via the p-th power map in H. It is clear that $[T_x, T_y] = T_{[x,y]}$ and $T_x^p = T_{x^p}$ for any $x, y \in \mathrm{P}(H)$. Hence $\bigoplus_{n \geq 0} \mathrm{H}^n(\mathbf{k}, H)$ becomes a graded restricted $\mathrm{P}(H)$-module via T. Finally, $\mathrm{P}(H) \cong \mathrm{H}^1(\mathbf{k}, H)$ by definition. ■

Theorem 2.4.5. *Let $K \subseteq H$ be an inclusion of connected Hopf algebras with first order $n \geq 2$. Then the differential d^1 induces an injective restricted $\mathfrak{g}$-module map*

$$H_n/K_n \hookrightarrow \mathrm{H}^2(\mathbf{k}, K),$$

where $\mathfrak{g} = \mathrm{P}(H)$.

Proof. By Corollary 2.1.3, H_n becomes a restricted $\mathfrak{g}$-module via the adjoint action since $[\mathrm{P}(H), H_n] \subseteq [H_1, H_n] \subseteq H_n$. We know $\mathfrak{g} = \mathrm{P}(H) = \mathrm{P}(K)$ for the inclusion has first order $n \geq 2$. Hence the $\mathfrak{g}$-action factors through H_n/K_n. Choose any $x \in H_n$. We know $d^1(x) = 1 \otimes x - \Delta(x) + x \otimes 1 \in H_{n-1} \otimes H_{n-1} = K_{n-1} \otimes K_{n-1} \subseteq K \otimes K$ by [35, Lemma 5.3.2]. Furthermore, we can view $(\Omega K, d_K)$ as a subcomplex of $(\Omega H, d_H)$. Then $d_K^2 d_H^1(x) = d_H^2 d_H^1(x) = 0$. Hence $d^1(x)$ is a cocycle in $\boldsymbol{\omega} K$ and d^1 maps H_n into $\mathrm{H}^2(\mathbf{k}, K)$. The map d^1 factors through H_n/K_n for $d^2 d^1(K_n) = 0$. To show the induced map is injective, suppose $d^1(x) \in \mathrm{Im}\ d_K^1$. Then there exists some $y \in K$ such that $d^1(x) = d^1(y)$, which implies that $d^1(x-y) = 0$. By definition, we have $x - y \in \mathrm{P}(H) = \mathrm{P}(K)$. Hence $x \in K \bigcap H_n = K_n$ by Remark 5. Finally, d^1 is compatible with the $\mathfrak{g}$-action on $\mathrm{H}^2(\mathbf{k}, K)$ by Lemma 2.4.4. ■

Theorem 2.4.6. *Let $\mathfrak{g}$ be a restricted Lie algebra with basis $\{x_1, x_2, \cdots, x_n\}$. Suppose $u(\mathfrak{g}) \subsetneq H$ is an inclusion of connected Hopf algebras. Then there exists some $x \in H \setminus u(\mathfrak{g})$ such that*

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \boldsymbol{\omega}\left(\sum_i \alpha_i x_i\right) + \sum_{j<k} \alpha_{jk} x_j \otimes x_k$$

with coefficients $\alpha_i, \alpha_{jk} \in \mathbf{k}$. Moreover, the first order for the inclusion can only be 1, 2 or p.

Proof. Denote by d the first order for the inclusion. By definition, $d = 1$ implies that $\mathfrak{g} \subsetneq \mathrm{P}(H)$. Then we can find some primitive element $x \in \mathrm{P}(H) \setminus \mathfrak{g} \subseteq H \setminus u(\mathfrak{g})$ such that $\Delta(x) = x \otimes 1 + 1 \otimes x$. In the following, we may assume $d \geq 2$. By Theorem 2.4.5 and Proposition 2.4.2, there exists $x \in H_d \setminus u(\mathfrak{g})$ such that

$$1 \otimes x - \Delta(x) + x \otimes 1 = d^1(x) = -\sum_i \alpha_i^p\ \boldsymbol{\omega}(x_i) - \sum_{j<k} \alpha_{jk}\ x_j \otimes x_k. \tag{I}$$

By the choice of x, we know the coefficients are not all zero. By Lemma 2.4.3, there exists some $y \in u(\mathfrak{g})$ such that

$$1 \otimes y - \Delta(y) + y \otimes 1 = d^1(y) = \sum_i \alpha_i^p\ \boldsymbol{\omega}(x_i) - \boldsymbol{\omega}\left(\sum_i \alpha_i\ x_i\right). \tag{II}$$

If we add (I) to (II), then we have

$$(x+y)\otimes 1-\Delta(x+y)+1\otimes(x+y)=-\boldsymbol{\omega}\left(\sum_i \alpha_i\ x_i\right)-\sum_{j<k}\alpha_{jk}\ x_j\otimes x_k.$$

This implies that

$$\Delta(x+y)=(x+y)\otimes 1+1\otimes(x+y)+\boldsymbol{\omega}\left(\sum_i \alpha_i\ x_i\right)+\sum_{j<k}\alpha_{jk}\ x_j\otimes x_k.$$

It is clear that $x+y\in H\setminus u(\mathfrak{g})$. Finally, because the associated graded Hopf algebra gr$H$ is coradically graded as mentioned in [6, Def. 1.13], it is easy to see that if all $\alpha_i=0$ then $d=2$. Otherwise $d=p$. Hence the first order d can only be 1, 2 or p. This completes the proof. ■

2.5 Algebraic representations of restricted Lie algebras

For simplicity, we write H^n for the n-fold tensor product $H^{\otimes n}$ and 1 for the identity map on H.

Definition 13. A Hopf algebra A is an *H-module Hopf algebra* if A is a (left) H-module satisfying that

(i) $h\cdot(ab)=\sum(h_1\cdot a)(h_2\cdot b)$,

(ii) $h\cdot 1_A=\epsilon(h)1_A$,

(iii) $\Delta(h\cdot a)=\sum(h_1\cdot a_1)\otimes(h_2\cdot a_2)$,

(iv) $\epsilon(h\cdot a)=\epsilon(h)\epsilon(a)$,

(v) $S(h\cdot a)=h\cdot S(a)$,

for all $h\in H$ and $a,b\in A$. Note that any algebra A, which is a (left) H-module satisfying (i) and (ii) is said to be a H-module algebra [35, Definition 4.1.1].

Definition 14. Let $\mathfrak{g}$ and $\mathfrak{h}$ be two restricted Lie algebras. An *algebraic representation* of $\mathfrak{g}$ on $\mathfrak{h}$ is a linear map $\rho:\mathfrak{g}\to \mathrm{End}_k(\mathfrak{h})$ such that

(i) $\rho_{[x,y]} = \rho_x\rho_y - \rho_y\rho_x$,

(ii) $\rho_{(x^p)} = (\rho_x)^p$,

(iii) $\rho_x([a,b]) = [\rho_x(a), b] + [a, \rho_x(b)]$,

(iv) $\rho_x(a^p) = \rho_x(a)\,(\text{ad } a)^{p-1}$,

for any $x, y \in \mathfrak{g}$ and $a, b \in \mathfrak{h}$.

Note that (i) and (ii) makes $\mathfrak{h}$ into a restricted $\mathfrak{g}$-module via ρ. The representation is said to be *abelian* if $\mathfrak{h}$ is an abelian restricted Lie algebra, where we have an extension of restricted Lie algebras [60, 7.4.9]

$$0 \longrightarrow \mathfrak{h} \longrightarrow \mathfrak{h} \rtimes \mathfrak{g} \longrightarrow \mathfrak{g} \longrightarrow 0.$$

We use $\mathscr{T}$ to denote the collection of all abelian algebraic representations for finite-dimensional restricted Lie algebras. To be more precise, we define the category $\mathscr{T}$, whose objects consist of all triples $(\mathfrak{h}, \mathfrak{g}, \rho)$ containing two finite-dimensional restricted Lie algebras $\mathfrak{h}, \mathfrak{g}$ provided $\mathfrak{h}$ is abelian, and an algebraic representation ρ of $\mathfrak{g}$ on $\mathfrak{h}$. The morphisms between two objects $(\mathfrak{h}, \mathfrak{g}, \rho)$ and $(\mathfrak{h}', \mathfrak{g}', \rho')$ are pairs (ϕ, ψ) of restricted Lie algebra maps, where $\phi : \mathfrak{h} \to \mathfrak{h}'$ and $\psi : \mathfrak{g} \to \mathfrak{g}'$ satisfy the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{g} \otimes \mathfrak{h} & \xrightarrow{\rho} & \mathfrak{h} \\ \downarrow{\scriptstyle \psi\otimes\phi} & & \downarrow{\scriptstyle \phi} \\ \mathfrak{g}' \otimes \mathfrak{h}' & \xrightarrow{\rho'} & \mathfrak{h}'. \end{array} \tag{2.5.1}$$

The automorphism group $\text{Aut}(T)$, for any object $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ in $\mathscr{T}$, consists of pairs (ϕ, ψ) of automorphisms of $\mathfrak{h}$ and $\mathfrak{g}$ respectively, which is compatible with ρ as described by the above commutative diagram. The group multiplication in $\text{Aut}(T)$ is composition of maps. Moreover, we say T is a *type* in $\mathscr{T}$ if $\dim \mathfrak{g} = 1$.

We will investigate the basic facts regarding the three concepts above. Firstly, let $\mathfrak{h}$ and $\mathfrak{g}$ be two restricted Lie algebras. In characteristic $p > 0$, it is clear that all the derivations on $u(\mathfrak{h})$ form a restricted Lie algebra through the commutator and the p-th power map in $\mathrm{End}_k(u(\mathfrak{h}))$. For any $\delta \in \mathrm{Der}(u(\mathfrak{h}))$ and $a, b \in u(\mathfrak{h})$, direct computation shows that

$$\delta[a,b] = [\delta(a), b] + [a, \delta(b)], \quad \delta(a^p) = \delta(a)(\mathrm{ad}\ a)^{p-1}. \tag{2.5.2}$$

Now, consider an algebraic representation ρ of $\mathfrak{g}$ on $\mathfrak{h}$. By Definition 14 and Relation (2.5.2), we see ρ induces a restricted Lie algebra map from $\mathfrak{g}$ to $\mathrm{Der}(u(\mathfrak{h}))$. It is straight forward to check that this makes $u(\mathfrak{h})$ into a $u(\mathfrak{g})$-module Hopf algebra according to Definition 13. Moreover, we have the following bijection between algebraic representations and module Hopf algebras for their restricted enveloping algebras.

Proposition 2.5.1. *Algebraic representations of $\mathfrak{g}$ on $\mathfrak{h}$ are in* 1-1 *correspondence with $u(\mathfrak{g})$-module Hopf algebra structures on $u(\mathfrak{h})$.*

Proof. Here, we only prove one direction. Suppose $u(\mathfrak{h})$ is a $u(\mathfrak{g})$-module Hopf algebra via the action $\rightharpoonup$. We define the representation ρ by $\rho_x(a) = x \rightharpoonup a$ for any $x \in \mathfrak{g}$ and $a \in \mathfrak{h}$. By Definition 13(iii), we have

$$\begin{aligned}
\Delta(\rho_x(a)) &= \sum (x_1 \rightharpoonup a_1) \otimes (x_2 \rightharpoonup a_2) \\
&= (x \rightharpoonup a) \otimes (1 \rightharpoonup 1) + (x \rightharpoonup 1) \otimes (1 \rightharpoonup a) + (1 \rightharpoonup a) \otimes (x \rightharpoonup 1) + (1 \rightharpoonup 1) \otimes (x \rightharpoonup a) \\
&= (x \rightharpoonup a) \otimes 1 + 1 \otimes (x \rightharpoonup a).
\end{aligned}$$

The last equality follows from Definition 13(ii). Hence, we have $\rho : \mathfrak{g} \to \mathrm{End}_k(\mathfrak{h})$. Moreover, since $\mathfrak{g}$ is the primitive space of $u(\mathfrak{g})$, we see

$$\rho_x(ab) = x \rightharpoonup (ab) = (x \rightharpoonup a)(1 \rightharpoonup b) + (1 \rightharpoonup a)(x \rightharpoonup b) = \rho_x(a)b + a\rho_x(b),$$

for any $a, b \in u(\mathfrak{h})$. It follows that $\rho : \mathfrak{g} \to \mathrm{Der}(u(\mathfrak{h}))$. Therefore, in Definition 14, it is easy to see that (iii) and (iv) come from Relation (2.5.2). And it is direct to check for (i) and (ii) by the construction of $u(\mathfrak{g})$. Then, we show that ρ is an algebraic representation. Finally, the bijection comes from the explicit construction. This completes the proof. ∎

Secondly, suppose we have an H-module Hopf algebra A. We use the cobar construction on A in Remark 9. Note that the cobar construction ΩA is the tensor algebra $T(A^+)$ and

A^+ is invariant under the H-action by Definition 13(iv). Hence, we can consider ΩA as an H-module algebra via the comultiplication of H. In details,

$$h \cdot 1_{\Omega A} = \epsilon(h) 1_{\Omega A},$$
$$h \cdot (a_1 \otimes a_2 \otimes \cdots \otimes a_n) = \sum (h_1 \cdot a_1) \otimes (h_2 \cdot a_2) \otimes \cdots \otimes (h_n \cdot a_n),$$

for any $h \in H$ and $a_i \in A^+$. Moreover, we can pass the H-module algebra structure on to the cohomology ring of ΩA.

Proposition 2.5.2. *The H-action commutes with the differentials of ΩA. Thus, the cohomology ring $\mathrm{H}^\bullet(\Omega A)$ becomes an H-module algebra.*

Proof. Observe that the cobar construction ΩA is a differential graded algebra, which is generated in degree one. Thus, it suffices to show that the H-action commutes with d^1. Suppose $a \in A^+$ and $h \in H$. We have

$$\begin{aligned} h[d^1(a)] &= h[1 \otimes a - \Delta(a) + a \otimes 1] \\ &= \sum h_1 1 \otimes h_2 a - \sum h_1 a_1 \otimes h_2 a_2 + \sum h_1 a \otimes h_2 1 \\ &= 1 \otimes ha - \sum (ha)_1 \otimes (ha)_2 + ha \otimes 1 \\ &= d^1(ha). \end{aligned}$$

This completes the proof. ■

In a conclusion, we have the following result about algebraic representations of $\mathfrak{g}$ on $\mathfrak{h}$ and the corresponding $u(\mathfrak{g})$-module algebra structures on $\mathrm{H}^\bullet(\Omega u(\mathfrak{h}))$.

Proposition 2.5.3. *, Let ρ be an algebraic representation of $\mathfrak{g}$ on $\mathfrak{h}$. Then $\mathrm{H}^\bullet(\Omega u(\mathfrak{h}))$ becomes a $u(\mathfrak{g})$-module algebra via the representation ρ.*

Proof. Combine Proposition 2.5.1 and Proposition 2.5.2. ■

Chapter 3

SOME SPECIAL CONNECTED HOPF ALGEBRAS

3.1 Finite-dimensional cocommutative connected Hopf algebras

Notice that the following lemma holds over any arbitrary base field. In the remaining of this section, we still assume $\mathbf{k}$ to be algebraically closed of characteristic $p > 0$.

Lemma 3.1.1. *Let H be a finite-dimensional Hopf algebra with normal Hopf subalgebras $K \subseteq L \subseteq H$. Then there exists a natural isomorphism:*

$$\left(H/K^+H\right)^* \Big/ \left(H/L^+H\right)^{*+} \left(H/K^+H\right)^* \cong \left(L/K^+L\right)^*.$$

Proof. By [35, Theorem 2.1.3], L is Frobenius. Hence the injective left L-module map $L \hookrightarrow H$ splits since L is self-injective. Therefore we can write $H = L \bigoplus M$ as a direct sum of two left L-modules. Because $K \subseteq L$, we have $L \bigcap K^+H = L \bigcap K^+ (L \bigoplus M) = L \bigcap (K^+L \bigoplus K^+M) = K^+L$. Then the inclusion map $L \hookrightarrow H$ induces an injective Hopf algebra map $L/K^+L \hookrightarrow H/K^+H$, since K^+L and K^+H are Hopf ideals of L and H by [35, Lemma 3.4.2].

It is clear that the composition map $L/K^+L \hookrightarrow H/K^+L \twoheadrightarrow H/L^+H$ factors through $\mathbf{k}$ by the counit. Thus the dualized map restricted on $(H/L^+H)^{*+} = (H/L^+H)^* \bigcap \mathrm{Ker}\ u^* \to (L/K^+L)^*$ is the zero map, where u is the unit map in H.

Therefore the natural surjective map $(H/K^+H)^* \twoheadrightarrow (L/K^+L)^*$, which is induced by the inclusion $L/K^+L \hookrightarrow H/K^+H$, factors through $\left(H/K^+H\right)^* \Big/ \left(H/L^+H\right)^{*+} \left(H/K^+H\right)^*$. In order to show that it is an isomorphism, it is enough to prove that both sides have the same dimension. By [35, Theorem 3.3.1], we have

$$\begin{aligned}
\dim \left(H/K^+H\right)^* \Big/ \left(H/L^+H\right)^{*+} \left(H/K^+H\right)^* &= \dim \left(H/K^+H\right)^* \Big/ \dim(H/L^+H)^* \\
&= (\dim H/\dim K)\Big/(\dim H/\dim L) \\
&= \dim L/\dim K \\
&= \dim(L/K^+L)^*.
\end{aligned}$$

■

Let σ be any nontrivial automorphism of $\mathbf{k}$, and A be a Hopf algebra. Then $A \otimes_\sigma \mathbf{k}$ is a **base change** of A via $ak \otimes 1 = a \otimes \sigma(k)$ in $A \otimes \mathbf{k}$ for any $a \in A$ and $k \in \mathbf{k}$. In the proof of [35, Corollary 2.2.2], we know that any base change of A is still a $\mathbf{k}$-Hopf algebra. Let H be another Hopf algebra, and ϕ be a set map from H to A. If $\phi \otimes 1 : H \to A \otimes_\sigma \mathbf{k}$ is a Hopf algebra map (i.e. preserves both algebra and coalgebra structures), then we say that ϕ is a **semi-linear Hopf algebra map**. Note that ϕ preserves all algebra and coalgebra structures except $\mathbf{k}$-linearity. Any quotient or dual of a semi-linear Hopf algebra map is still semi-linear. The composition of two semi-linear Hopf algebra maps is also semi-linear.

Proposition 3.1.2. *Let H be a finite-dimensional cocommutative connected Hopf algebra. Then H has an increasing sequence of normal Hopf subalgebras: $\mathbf{k} = N_0 \subset N_1 \subset \cdots \subset N_n = H$ satisfying the following properties:*

(1) Denote by J the Jacobson radical of H^*. Then the length n is the minimal integer such that $x^{p^n} = 0$ for all $x \in J$.

(2) N_1 is the Hopf subalgebra of H generated by all primitive elements.

(3) There are semi-linear injective Hopf algebra maps:

$$N_n/N_{n-1}^+N_n \hookrightarrow N_{n-1}/N_{n-2}^+N_{n-1} \hookrightarrow \cdots \hookrightarrow N_1/N_0^+N_1 = N_1.$$

(4) $0 = \dim \mathrm{P}\left(H/N_n^+H\right) \leq \dim \mathrm{P}\left(H/N_{n-1}^+H\right) \leq \cdots \leq \dim \mathrm{P}\left(H/N_0^+H\right) = \dim \mathrm{P}(H)$*.*

Proof. (1) By duality, H^* is a finite-dimensional commutative local Hopf algebra. Therefore by [**?**, Theorem 14.4] we can write:

$$H^* = \mathbf{k}\left[x_1, x_2, \cdots, x_d\right] \Big/ \left(x_1^{p^{n_1}}, x_2^{p^{n_2}}, \cdots, x_d^{p^{n_d}}\right)$$

for some $d \geq 0$, in which we can define a decreasing sequence of normal Hopf ideals [35, Def. 3.4.5]

$$\left(J_m = (x_1^{p^m}, x_2^{p^m}, \cdots, x_d^{p^m})\right)_{m \geq 0}.$$

By [35, P. 36], in the dual vector space H we have an increasing sequence of normal Hopf subalgebras: $\mathbf{k} = N_0 \subset N_1 \subset \cdots \subset N_m \subseteq \cdots \subseteq H$, where $N_m = (H^*/J_m)^*$ for all $m \geq 0$. For the length of this sequence, notice that $N_m = H \Leftrightarrow J_m = 0 \Leftrightarrow x_i^{p^m} = 0$ for all $1 \leq i \leq d \Leftrightarrow x^{p^m} = 0$ for all $x \in J_0 = J$.

(2) Denote by L the Hopf subalgebra of H generated by $\mathrm{P}(H)$. By [35, Prop. 5.2.9], $\mathbf{k} \bigoplus \mathrm{P}(H) = \{h \in H | \langle J^2, h \rangle = 0\}$. Hence under the natural identification, $\mathrm{P}(H) \subset (H^*/J^2)^* \subseteq (H^*/J_1)^* = N_1$. Because L is generated by $\mathrm{P}(H)$ as an algebra, we have $L \subseteq N_1$. Moreover we know $\dim L = p^{\dim \mathrm{P}(H)} = p^{\dim J/J^2} = p^d$ by Proposition 2.1.4(4). On the other side, $\dim N_1 = \dim H^*/J_1 = p^d$, which implies that $L = N_1$.

(3) Define a decreasing sequence of normal Hopf subalgebras of H^* by

$$A_m = \{h^{p^m} | h \in H^*\} = \mathbf{k}\left[x_1^{p^m}, x_2^{p^m}, \cdots, x_d^{p^m}\right].$$

Notice that $A_m^+ H^* = J_m$ for all $m \geq 0$. By Lemma 3.1.1, we have

$$\begin{aligned} \left(A_m/A_{m+1}^+ A_m\right)^* &\cong \left(H^*/A_{m+1}^+ H^*\right)^* \Big/ \left(H^*/A_m^+ H\right)^{*+} \left(H^*/A_{m+1}^+ H^*\right)^* \qquad (3.1.1) \\ &= N_{m+1} \Big/ {N_m}^+ N_{m+1}. \end{aligned}$$

Take σ to be the Frobenius map of $\mathbf{k}$ (i.e., the p-th power map). For each A_m, we can formulate $A_m \otimes_{\sigma^{-1}} \mathbf{k}$ such that $ak \otimes 1 = a \otimes \sigma^{-1}(k)$ for any $a \in A_m$ and $k \in \mathbf{k}$. Hence it is easy to see that there exists a series of semi-linear surjective p-th power Hopf algebra maps $\phi_m : A_m \twoheadrightarrow A_{m+1}$ such that $\phi_m(x) = x^p$ for all $x \in A_m$. Therefore ϕ_m induces a series of semi-linear surjective maps on the quotients $A_m/A_{m+1}^+ A_m \twoheadrightarrow A_{m+1}/A_{m+2}^+ A_{m+1}$ for all $m \geq 0$. By daulizing all the maps and the above natural isomorphism (3.1.1), we have a series of semi-linear injective Hopf algebra maps:

$$N_n/N_{n-1}^+ N_n \hookrightarrow N_{n-1}/N_{n-2}^+ N_{n-1} \hookrightarrow \cdots \hookrightarrow N_1/N_0^+ N_1 = N_1.$$

(4) In Lemma 3.1.1, let $K = \mathbf{k}$ and $L = A_m$. Then we have the special isomorphism:

$$A_m^* \cong H \Big/ N_m^+ H.$$

Therefore, by Proposition 2.1.4(4),

$$\dim \mathrm{P}(H/N_m^+ H) = \dim J(A_m)/J(A_m)^2 = \# \left\{\{x_1^{p^m}, x_2^{p^m}, \cdots, x_d^{p^m}\} \setminus \{0\}\right\},$$

which is the number of generators among $\{x_1, x_2, \cdots, x_d\}$, whose p^m-th power does not vanish. Thus the inequalities follow. ■

Corollary 3.1.3. *Let H be a finite-dimensional connected Hopf algebra with* $\dim \mathrm{P}(H) = 1$. *Then H has an increasing sequence of normal Hopf subalgebras:*

$$\mathbf{k} = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = H,$$

where N_1 is generated by $\mathrm{P}(H)$ *and each N_i has p-index one in N_{i+1}.*

Proof. Denote by H^* the dual Hopf algebra of H. By duality, H^* is local. Set $J = J(H^*)$, the Jacobson radical of H^*. Since $\dim \mathrm{P}(H) = 1$, by Proposition 2.1.4(4), $\dim J/J^2 = 1$. Suppose that $\dim H = p^n$ by Proposition 2.1.4(7). It is clear that $H^* \cong \mathbf{k}[x]/(x^{p^n})$ as algebras and $J = (x)$. Hence H is cocommutative and it has an increasing sequence of normal Hopf subalgebras $\mathbf{k} = N_0 \subset N_1 \subset \cdots \subset N_n = H$ such that N_1 is generated by $\mathrm{P}(H)$ and $\dim N_m = p^m$ for all $0 \le m \le n$ by Proposition 3.1.2. ■

Theorem 3.1.4. *Let H be finite-dimensional cocommutative connected Hopf algebra. Denote by K the Hopf subalgebra generated by* $\mathrm{P}(H)$. *Then the following are equivalent:*

(1) H is local.

(2) K is local.

(3) All the primitive elements of H are nilpotent.

Proof. (1) ⇒ (2) is from Proposition 2.1.4(2) and (2) ⇒ (3) is clear since K contains $\mathrm{P}(H)$ and its augmentation ideal is nilpotent.

In order to show that (3) ⇒ (2), denote $\mathfrak{g} = \mathrm{P}(H)$, which is a restricted Lie algebra. Then (3) is equivalent to the statement that $\mathfrak{g}^{p^n} = 0$ for sufficient larger n. Therefore $(\mathrm{ad}x)^{p^n} = \mathrm{ad}(x^{p^n}) = 0$ for all $x \in \mathfrak{g}$. By Engel's Theorem [28, I §3.2], $\mathfrak{g}$ is nilpotent. Any representation of $K \cong u(\mathfrak{g})$ is a restricted representation of $\mathfrak{g}$. Therefore any irreducible representation of K is one-dimensional with trivial action of the augmentation ideal of K. Hence the augmentation ideal of K is nilpotent and K is local.

Finally, we need to show (2) $\Rightarrow$ (1). It suffices to show the augmentation ideal $I = H^+$ of H is nilpotent. We do induction on the dimension of H. When $\dim H = p$, the result is clear since $H = K$. If $\dim H > p$ and $K \neq H$, by Proposition 3.1.2(3), there exists some proper normal Hopf subalgebra $L \supsetneq K$ and there is a semi-linear Hopf algebra injection $H/L^+H \hookrightarrow K$. Therefore it implies that H/L^+H is a Hopf subalgeba of $K \otimes \mathbf{k}$ for some base change. Hence by Proposition 2.1.4(2), H/L^+H is local since any base change preserves the locality of K. Therefore there exists some integer l such that $(I)^l \subseteq L^+H$. By induction, L is local. Then there is another integer s such that $(L^+)^s = 0$. Thus $(I)^{ls} \subseteq (L^+H)^s = (L^+)^s H = 0$. Here we use the fact that $L^+H = HL^+$ in the case that L is normal by [35, Corollary 3.4.4]. This completes the proof. ■

Remark 10. Let G be a connected affine algebraic group scheme over $\mathbf{k}$, and G_1 be the first Frobenius kernel of G. By [18, Prop. 4.3.1 Exp. XVII], we know that G is unipotent if and only if $\mathrm{Lie}\,(G)$ is unipotent, i.e., for any $x \in \mathrm{Lie}(G_1)$, there exists integer $n > 0$, such that $x^{p^n} = 0$. Moreover, $\mathrm{Lie}\,(G) = \mathrm{Lie}\,(G_1)$. Hence G is unipotent if and only if G_1 is unipotent. Denote the coordinate ring $A = \mathbf{k}[G]$. Then $\mathbf{k}[G_1] = A/A^{+(p)}A$, where $A^{(p)} = \{a^p \mid a \in A\}$. We can state the above assertion in another way: A is connected if and only if $A/A^{+(p)}A$ is connected. If A is finite-dimensional, as shown in Proposition 3.1.2(2), $\left(A/A^{+(p)}A\right)^*$ is the Hopf subalgebra of A^* generated by its primitive elements. This provides an alternative proof for Theorem 3.1.4 and shows that the locality criterion in Theorem 3.1.4 for finite-dimensional cocommutative connected Hopf algebras parallel the criteria for unipotency of finite connected group schemes over $\mathbf{k}$.

3.2 Semisimple connected Hopf algebras

In this section, let H be a finite-dimensional connected Hopf algebra and denote by K the Hopf subalgebra of H generated by $\mathrm{P}(H)$.

Definition 15. Let L be a proper Hopf subalebra of H. Then $L \subsetneq H$ is called a *weakly essential extension* if there is no proper Hopf subalgebra between them. If moreover $K \subseteq L$, we say it is an *essential extension.*

Definition 16. [35, Definitions 4.1.1, 7.1.1] A Hopf algebra H *measures* an algebra A if there is a linear map $H \otimes A \to A$, given by $h \otimes a \to h \cdot a$, such that $h \cdot 1 = \epsilon(h)1$ and $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b)$, for all $h \in H, a, b \in A$. Moreover, assume that σ is an invertible map in $\mathrm{Hom}_k(H \otimes H, A)$. The *crossed product* $A \#_\sigma H$ of A with H is the set $A \otimes H$ as a vector space, with multiplication

$$(a\#h)(b\#k) = \sum a(h_1 \cdot b)\sigma(h_2, k_1)\#h_3k_2,$$

for all $h, k \in H$ and $a, b \in A$.

Lemma 3.2.1. *Let $L \subsetneq H$ be an extension of connected Hopf algebras. If there exists some $x \in H \setminus L$ satisfying $\Delta(x) = x \otimes 1 + 1 \otimes x + u$, where $u \in L \otimes L$. Then the subalgebra generated by L and x is a Hopf subalgebra of H. Moreover if the extension is weakly essential, then L is equal to H.*

Proof. First of all, the subalgebra generated by L and x is a sub-bialgebra of H, which is connected by [35, Lemma 5.2.12]. Therefore it is a Hopf subalgebra because of [35, Lemma 2.10]. Moreover if the extension is weakly essential, then by definition it is equal to H. ■

Lemma 3.2.2. *If K is semisimple, then $K \subseteq Z(H)$.*

Proof. By Remark 6 and Hochschild's result [35, Theorem 2.3.3], the restricted Lie algebra $\mathfrak{g}$ is abelian with $\mathfrak{g} = k\mathfrak{g}^p$. Fix a basis $\{x_i | 1 \leq i \leq d\}$ for it. Denote $\mathbf{x} = (x_1, x_2, \cdots, x_d)^T$ and $\mathbf{x}^p = (x_1^p, x_2^p, \cdots, x_d^p)^T$. We can write the restricted map for $\mathfrak{g}$ in a matrix form:

$$\mathbf{x}^p = R\mathbf{x},$$

for some $R \in GL_d(k)$. It suffices to prove inductively that $[H_n, \mathfrak{g}] = 0$ for all $n \geq 0$. Obviously, it is true for H_0 and H_1. In the following, suppose that $[H_n, \mathfrak{g}] = 0$ for some $n \geq 1$. By [35, Lemma 5.3.2(2)], for any $z \in H_{n+1}$, we have $\Delta(z) = z \otimes 1 + 1 \otimes z + u$, where $u \in H_n \otimes H_n$. Therefore by induction

$$\begin{aligned} \Delta([z, x_i]) &= [\Delta(z), \Delta(x_i)] \\ &= [z \otimes 1 + 1 \otimes z + u, x_i \otimes 1 + 1 \otimes x_i] \\ &= [z, x_i] \otimes 1 + 1 \otimes [z, x_i], \end{aligned}$$

which yields that $[z, x_i]$ is primitive for all $1 \leq i \leq d$. Therefore we can write these relations in a matrix form as follows:

$$(\mathrm{ad}z)\mathbf{x} = A\mathbf{x},$$

where $A \in M_d(k)$. Hence a simple calculation shows that:

$$(\mathrm{ad}z)\mathbf{x}^p = R(\mathrm{ad}z)\mathbf{x} = RA\mathbf{x}.$$

By the definition of restricted Lie algebras, on the other hand, $[z, x_i^p] = z(\mathrm{ad}x_i)^p = 0$ for all $1 \leq i \leq d$. Hence $RA = 0$ which implies that $A = 0$. ■

Lemma 3.2.3. *Let $L \subsetneq H$ be a proper Hopf subalgebra. Then there is a finite set $\{u_i\} \subseteq L \otimes L$, whose image is a basis in $\mathrm{H}^2(k, L)$. Moreover if $K \subseteq L$, then there exists an element $z \in H \setminus L$ such that $\Delta(z) = z \otimes 1 + 1 \otimes z + \sum \alpha_i u_i$, where the $\alpha_i \in k$ are not all zero.*

Proof. By the definition of the complex $(L^{\otimes \bullet}, d^\bullet)$, $\mathrm{H}^2(k, L) = \ker d^2/\mathrm{Im}d^1$. Hence there exists a set $\{u_i\} \subseteq \mathrm{Ker}d^2 \subseteq L \otimes L$, whose image is a basis in $\mathrm{H}^2(k, L)$. It is finite since L is finite-dimensional. Furthermore we assume that $K \subseteq L$. As a result of [35, Theorem 5.2.2(1)], there is a minimal number d (≥ 2) such that $L_d \neq H_d$, whence we choose some $z \in H_d \setminus L_d \subseteq H \setminus L$. By [35, Lemma 5.3.2(2)], $\Delta(z) = z \otimes 1 + 1 \otimes z + u$, where $u \in H_{d-1} \otimes H_{d-1} = L_{d-1} \otimes L_{d-1} \subseteq L \otimes L$. Consider $(L^{\otimes \bullet}, d^\bullet)$ as a subcomplex of $(H^{\otimes \bullet}, d^\bullet)$. Hence $d^2(u) = d^2 d^1(-z) = 0$ and u is a 2-cocycle in the subcomplex. In regard to the chosen basis $\{u_i\}$ in $\mathrm{H}^2(k, L)$, there are coefficients $\alpha_i \in k$ and an element $y \in L$ such that

$$\begin{aligned} u - \sum \alpha_i u_i &= d^1(y) = 1 \otimes y - \Delta(y) + y \otimes 1; \\ \Delta(z + y) &= (z + y) \otimes 1 + 1 \otimes (z + y) + \sum \alpha_i u_i. \end{aligned}$$

Finally, $z + y \notin L$ because of $z \notin L$ and $y \in L$. The α_i are not all zero, otherwise $z + y \in H_1 = K_1 \subseteq L$. ■

Lemma 3.2.4. *Let $H = (kG)^*$, where G is a p-group. Then H is connected and there exists a set $\{u_i | 1 \leq i \leq n\} \subseteq H \otimes H$ satisfying*

(1) The image of $\{u_i\}$ is a basis in $\mathrm{H}^2(k, H)$;

(2) $u_i^p = u_i$ *in* $H \otimes H$ *for all* $1 \leq i \leq n$.

Proof. Consider $k \supset \mathbb{F}_p$ as a field extension. It is well known that $\mathbb{F}_pG$ and kG are scalar local because G is a p-group. Therefore by [35, Proposition 5.2.9(2)], their duals are connected. As shown in [35, Example 1.3.6], $L := (\mathbb{F}_pG)^*$ has a basis $\{f_x | x \in G\}$, where f_x is the characteristic function on the element $x \in G$ and its multiplication and comultiplication structures are described as follows:

$$\begin{aligned} f_x f_y &= \delta_{x,y} f_x, \\ \Delta(f_x) &= \sum_{uv=x} f_u \otimes f_v. \end{aligned}$$

Obviously, there exists a set $\{u_i | 1 \leq i \leq n\} \subseteq L \otimes L$, whose image becomes a basis in $\mathrm{H}^2(\mathbb{F}_p, L)$. Moreover each $u_i = \sum \alpha_i f_{x_i} \otimes f_{y_i}$ for some $\alpha_i \in \mathbb{F}_p$. Hence

$$\begin{aligned} u_i^p &= \left(\sum \alpha_i f_{x_i} \otimes f_{y_i}\right)^p \\ &= \sum \alpha_i^p f_{x_i}^p \otimes f_{y_i}^p \\ &= \sum \alpha_i f_{x_i} \otimes f_{y_i} \\ &= u_i \end{aligned}$$

for all i. Furthermore, $\mathrm{H}^2(\mathbb{F}_p, L) \otimes k$ is naturally isomorphic to $\mathrm{H}^2(k, H)$ as k-vector spaces because the base change functor $\otimes_{\mathbb{F}_p} k$ is exact. Then $\{u_i\}$ becomes a basis for the latter through the natural isomorphism. ■

Lemma 3.2.5. *Let* H *be commutative, and* $L \subsetneq H$ *be an essential extension. Furthermore assume that* $L = (kG)^*$ *for some* p*-group* G*. Then there exists some element* $z \in H$ *satisfying the following conditions:*

(1) L *and* z *generate* H *as an algebra.*

(2) $\Delta(z) = z \otimes 1 + 1 \otimes z + u$*, where* u *is a 2-cocycle in the complex* $(L^{\otimes \bullet}, d^{\bullet})$.

(3) $z^{p^n} \notin L$ *for all* $n \geq 0$.

(4) z satisfies some relation: $z^{p^l} + \lambda_{l-1} z^{p^{l-1}} + \cdots + \lambda_1 z + a = 0$ in H, where $\lambda_i \in k$ for all $1 \leq i \leq l-1$ with $\lambda_1 \neq 0$ and $a \in L$.

Moreover H is semisimple.

Proof. Choose a finite set $\{u_i\} \subseteq L \otimes L$, which represents a basis in $\mathrm{H}^2(k, L)$. By Lemma 3.2.4, we can assume that $u_i^p = u_i$ for all i. Moreover apply Lemma 3.2.3 to $L \subsetneq H$, there exists an element $z \in H \setminus L$ such that

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \sum \alpha_i u_i,$$

where the $\alpha_i \in k$ are not all zero. Because of Lemma 3.2.1, H is generated by L and z as an algebra. A simple calculation shows that:

$$\begin{aligned} \Delta\left(z^{p^n}\right) &= z^{p^n} \otimes 1 + 1 \otimes z^{p^n} + \left(\sum \alpha_i u_i\right)^{p^n} \\ &= z^{p^n} \otimes 1 + 1 \otimes z^{p^n} + \sum \alpha_i^{p^n} u_i \end{aligned}$$

for all $n \geq 0$. By definition $d^1\left(z^{p^n}\right) = -\sum \alpha_i^{p^n} u_i$, which is never a 2-coboundary in the complex $(L^{\otimes \bullet}, d^\bullet)$. Therefore $z^{p^n} \notin L$ for all $n \geq 0$. Furthermore by Theorem 2.2.5, we see z satisfies some relation

$$z^{p^l} + \lambda_{l-1} z^{p^{l-1}} + \cdots + \lambda_1 z + a = 0,$$

in H, where all $\lambda_i \in k$ with $a \in L$. The condition (3) ensures that there exists a smallest index m such that $\lambda_m \neq 0$. Replace z with z^{p^m}, which still satisfies all the conditions (1) to (4) in the assertion.

Finally, H is isomorphic as an algebra to a certain crossed product $L\#_\sigma(H/L^+H)$ by [17, Theorem 7.2.11]. The quotient Hopf algebra H/L^+H is generated by the image $\bar{z}$ chosen above satisfying

$$\bar{z}^{p^l} + \lambda_{l-1} \bar{z}^{p^{l-1}} + \cdots + \lambda_1 \bar{z} + \epsilon(a) = 0,$$

where all $\lambda_i \in k$ with $\lambda_1 \neq 0$. Hence it is a polynomial with distinctive roots in $\bar{k}$. Then the quotient Hopf algebra is semisimple and so is H by [11, Theorem 2.6]. ∎

Recall that char$k = p$, and H is a finite-dimensional connected Hopf algebra. We use K to denote the Hopf subalgebra generated by the primitive space $\mathfrak{g}$ of H.

Theorem 3.2.6. *Suppose k is algebraically closed. The following are equivalent:*

(1) H is semisimple.

(2) K is semisimple.

(3) $K \cong (kN)^*$, for $N \cong (C_p)^n$.

(4) $H \cong (kG)^*$, for G a p-group.

Proof. Condition (1) implies (2) because of [35, Corollary 2.2.2(2)] and Nichols-Zoeller Theorem [37]. By [35, Corollary 2.3.5], (2) implies (3). Since group algebras are cosemisimple, their duals are semisimple. Hence (3) implies (2) and (4) imply (1). Because H is finite-dimensional, there exists a finite chain of Hopf subalgebras

$$K = F_0 H \subsetneq F_1 H \subsetneq \cdots \subsetneq F_n H = H,$$

where each step is an essential extension. We prove (3) implies (4) by induction on the length n. When $K = H$, there is nothing to prove. We assume the statement is true for $n \leq d$ and suppose that $n = d+1$. By induction when $1 \leq i \leq d$,

$$F_i H \cong (kG_i)^*,$$

for G_i a p-group. Furthermore if H is commutative, by Lemma 3.2.5, H is semisimple. Hence it is the dual of a group algebra by [35, Theorem 2.3.1]. Remark **??** gives the order of the group. Thus the inductive step is complete.

It remains to show that H is commutative. We complete it by proving $F_j H \subseteq Z(H)$ inductively again for all j. When $j = 0$, we have $F_0 H = K \subseteq Z(H)$ by Lemma 3.2.2. Now assume it is true for $j = m$ and let $j = m+1$. In the essential extension $F_d H \subsetneq H$, by Lemma 3.2.1, there exists some $z \in H \setminus F_d H$ satisfying: (1) z and $F_d H$ generate H; (2) $\Delta(z) = z \otimes 1 + 1 \otimes z + u$, where $u \in F_d H \otimes F_d H$. Similarly by Lemma 3.2.5, $F_{m+1} H$ is generated by F_mH and some $y \in F_{m+1}H \setminus F_mH$ such that: (1) $\Delta(y) = y \otimes 1 + 1 \otimes y + v$, where $v \in F_mH \otimes F_mH$; (2) y satisfies some relation

$$y^{p^l} + \lambda_{l-1} y^{p^{l-1}} + \cdots + \lambda_1 y + a = 0,$$

where $\lambda_i \in k$ with $\lambda_1 \neq 0$ and $a \in F_mH$. By induction, $F_{m+1}H \subseteq Z(H)$ if and only if $[F_{m+1}, z] = 0$ if and only if $[y, z] = 0$. Moreover since $F_m \subseteq Z(H)$ and F_dH is commutative, then

$$\begin{aligned} \Delta([y,z]) &= [\Delta(y), \Delta(z)] \\ &= [y \otimes 1 + 1 \otimes y + v, z \otimes 1 + 1 \otimes z + u] \\ &= [y,z] \otimes 1 + 1 \otimes [y,z]. \end{aligned}$$

Hence we can write $[y, z] = x$ for some primitive element $x \in K$ and

$$\begin{aligned} 0 &= \left[y^{p^l} + \lambda_{l-1} y^{p^{l-1}} + \cdots + \lambda_1 y + a, z \right] \\ &= (\mathrm{ad} y)^{p^l}(z) + \lambda_{l-1} (\mathrm{ad} y)^{p^{l-1}}(z) + \cdots + \lambda_1 [y,z] + [a,z] \\ &= \lambda_1 x. \end{aligned}$$

Therefore $[y, z] = 0$ for $\lambda_1 \neq 0$. ■

Corollary 3.2.7. *If H is semisimple, then H is commutative.*

Proof. By [35, Corollary 2.2.2], H is a separable k-algebra. Without loss of generality, by we can assume k to algebraically closed of characteristic $p \neq 0$ by a base field extension. Then the result follows from Theorem 3.2.6. ■

Corollary 3.2.8. *The following are equivalent:*

(1) H is semismple.

(2) $\epsilon(\int_H^r) \neq 0$.

(3) $\epsilon(\int_H^l) \neq 0$.

(4) K is semisimple.

(5) $\mathfrak{g}$ *is abelian and* $\mathfrak{g} = k\mathfrak{g}^p$.

(6) $\epsilon(\int_K^r) \neq 0$.

(7) $\epsilon(\int_K^l) \neq 0$.

Proof. The equivalence of conditions (1), (2) and (3) is Maschke's Theorem [31]. That (4) is equivalent to (5) is Hochschild's result. Let $E \supset k$ be a field extension, and J be the Jacobson radical of H^*. We see $J \otimes E$ is the Jacobson radical of $(H \otimes E)^*$ because it is nilpotent and has codimension one. Therefore by [35, Proposition 5.2.9(2)], $(H \otimes E)_n = H_n \otimes E$ for any $n \geq 0$. By Maschke's theorem [31] again, the semisimplicity of Hopf algebras is preserved by base change [35, Corollary 2.2.2]. Therefore we can extend the base filed k to its algebraically closure and apply Theorem 3.2.6. ■

Chapter 4

CONNECTED HOPF ALGEBRAS OF DIMENSION P AND P^2

The starting point for classifying finite-dimensional connected Hopf algebras turns out to be when the dimension of the Hopf algebras is just p. It is obvious that such Hopf algebras are primitively generated, i.e., by some primitive element x. As a consequence of the characteristic of the base field, x^p is still primitive. This implies that $x^p = \lambda x$ for some $\lambda \in \mathbf{k}$, since the dimension of the primitive space is one. By rescaling of the variable, we can always assume the coefficient λ to be zero or one. Thus we have the result of Theorem 1.0.1

Corollary 4.0.9. *All local Hopf algebras of dimension p are isomorphic to $\mathbf{k}[x]/(x^p)$ with comultiplication either $\Delta(x) = x \otimes 1 + 1 \otimes x$ or $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x$.*

Proof. By Proposition 2.1.4(1), p-dimensional local Hopf algebras are in one-to-one correspondence with p-dimensional connected Hopf algebras by vector space dual. Therefore by Theorem 1.0.1, there are two non-isomorphic classes of local Hopf algebras of dimension p. It is clear that $\mathbf{k}[x]/(x^p)$ is a local algebra of dimension p. Regarding the coalgebra structure, when $\Delta(x) = x \otimes 1 + 1 \otimes x$, it is connected. When $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x$, $\Delta(x + 1) = (x + 1) \otimes (x + 1)$, which is a group-like element. Therefore it is cosemisimple. They are certainly non-isomorphic as coalgebras. ■

In the rest of the section, we concentrate on the classification of connected Hopf algebras of dimension p^2. We first consider the case when $\dim \mathrm{P}(H) = 1$. By Corollary 3.1.3, we have $\mathbf{k} \subset K \subset H$, where K is generated by some $x \in \mathrm{P}(H)$. By Proposition 2.1.4(5), we know K is isomorphic to the restricted universal enveloping algebra of the one-dimensional restricted Lie algebra spanned by x. Therefore by Proposition 2.4.2, $\mathrm{H}^2(\mathbf{k}, K)$ is one-dimensional with the basis representing by the element

$$\boldsymbol{\omega}(x) = \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\, x^i \otimes x^{p-i}.$$

Furthermore, by Theorem 2.4.6, there exists some $y \in H \setminus K$ such that $\Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)$.

Lemma 4.0.10. *Let H be a connected Hopf algebra of dimension p^2 with $\dim \mathrm{P}(H) = 1$. Then H is isomorphic to one of the following*

(1) $\mathbf{k}[x,y]/(x^p, y^p)$,

(2) $\mathbf{k}[x,y]/(x^p, y^p - x)$,

(3) $\mathbf{k}[x,y]/(x^p - x, y^p - y)$,

where the coalgebra structure is given by

$$\begin{aligned} \Delta(x) &= x \otimes 1 + 1 \otimes x, \\ \Delta(y) &= y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x). \end{aligned} \tag{4.0.1}$$

Proof. By the previous argument, we can find elements $x, y \in H$ with the comultiplications given in (4.0.1). They generate a Hopf subalgebra of H by Remark 5. Since H has dimension p^2, H is generated by x, y. It is clear that $[x,y]$ is primitive since

$$\begin{aligned} \Delta([x,y]) &= [\Delta(x), \Delta(y)] \\ &= [x \otimes 1 + 1 \otimes x, y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)] \\ &= [x,y] \otimes 1 + 1 \otimes [x,y]. \end{aligned}$$

In other words, we can write $[x,y] = \lambda x$ for some $\lambda \in \mathbf{k}$, which implies that $[x^n, y] = n\lambda\, x^n$

for any $n \geq 1$. Therefore we can show that

$$\begin{aligned}
[\boldsymbol{\omega}(x), y \otimes 1 + 1 \otimes y] &= \left[\sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\ x^i \otimes x^{p-i}\ ,\ y \otimes 1 + 1 \otimes y\right] \qquad (4.0.2)\\
&= \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\ \left([x^i, y] \otimes x^{p-i} + x^i \otimes [x^{p-i}, y]\right)\\
&= \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\ \left(i\lambda\ x^i \otimes x^{p-i} + x^i \otimes (p-i)\lambda\ x^{p-i}\right)\\
&= \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!}\lambda\ x^i \otimes x^{p-i}\\
&= 0.
\end{aligned}$$

Since $\boldsymbol{\omega}(x)^p = \boldsymbol{\omega}(x^p)$, we have

$$\Delta\left(y^p\right) = (y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x))^p = y^p \otimes 1 + 1 \otimes y^p + \boldsymbol{\omega}(x^p). \qquad (4.0.3)$$

By Theorem 1.0.1, we can assume that $x^p = 0$ or $x^p = x$. When $x^p = 0$, according to the above equation (4.0.3), y^p is primitive. Then we can write $y^p = \mu x$ for some $\mu \in \mathbf{k}$. Thus $\lambda^p x = x\ \mathrm{ad}(y)^p = [x, y^p] = [x, \mu x] = 0$, which implies that $\lambda = 0$. By further rescaling of the variables, we can assume μ to be either one or zero, which yields the first two classes. On the other hand, when $x^p = x$, by (4.0.3) again, $y^p - y$ is primitive. Then we can write $y^p = y + \mu x$ for some $\mu \in \mathbf{k}$. Moreover, $[x, y] = [x^p, y] = \mathrm{ad}(x)^p y = 0$. After the linear translation $y = y' + \sigma x$ satisfying $\sigma^p = \sigma + \mu$, we have $y'^p = y'$ while $\Delta(y') = y' \otimes 1 + 1 \otimes y' + \boldsymbol{\omega}(x)$. This gives the third class. It remains to show those three Hopf algebras are non-isomorphic. The first two are local with different number of minimal generators and the third one is semisimple. Hence they are non-isomorphic as algebras. This completes the classification. ■

Finally, the classification for connected Hopf algebras of dimension p^2 follows.

Proof of Theorem 1.0.2. By Proposition 2.1.4(6), we know $\dim \mathrm{P}(H) \leq 2$. If $\dim \mathrm{P}(H) = 2$, then H is primitively generated and $H \cong u(\mathfrak{g})$ for some two-dimensional restricted Lie algebra $\mathfrak{g}$ by Proposition 2.1.4(5). Therefore Proposition 2.3.2 provides the classification. When $\dim \mathrm{P}(H) = 1$, it is directly from Lemma 4.0.10. Finally, it is clear that the Hopf algebras given in (1)-(5) are non-isomorphic to the ones given in (6)-(8), since their primitive spaces have different dimension. The Hopf algebras in (1)-(5) are obviously non-isomorphic as algebras. Neither are the ones in (6)-(8). This completes the proof. ∎

Corollary 4.0.11. *Let H be a local Hopf algebra of dimension p^2. Then H is isomorphic to either $k[x,y]/(x^p,y^p)$ or $k[x]/(x^{p^2})$ as algebras. When $H \cong k[x,y]/(x^p,y^p)$, the coalgebra structure is given by one of the following:*

(1) $\Delta(x) = x \otimes 1 + 1 \otimes x,$
$\Delta(y) = y \otimes 1 + 1 \otimes y,$

(2) $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x,$
$\Delta(y) = y \otimes 1 + 1 \otimes y,$

(3) $\Delta(x) = x \otimes 1 + 1 \otimes x,$
$\Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x),$

(4) $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x,$
$\Delta(y) = y \otimes 1 + 1 \otimes y + y \otimes y,$

(5) $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x,$
$\Delta(y) = y \otimes 1 + 1 \otimes y + x \otimes y.$

When $H \cong k[x]/(x^{p^2})$, the coalgebra structure is given by

(6) $\Delta(x) = x \otimes 1 + 1 \otimes x,$

(7) $\Delta(x) = x \otimes 1 + 1 \otimes x + \boldsymbol{\omega}(x^p),$

(8) $\Delta(x) = x \otimes 1 + 1 \otimes x + x \otimes x.$

Proof. Denote the dual Hopf algebra of H by H^*. By Proposition 2.1.4(1), H^* is a connected Hopf algebra of dimension p^2. When $\dim \mathrm{P}(H^*) = 2$, as shown in Theorem 1.0.2, there are five non-isomorphic classes for H^*. By duality, there are also five non-isomorphic classes for H. Furthermore, from Proposition 2.1.4(4), $\dim J/J^2 = \dim \mathrm{P}(H^*) = 2$, where J is the Jacobson radical of H. Notice that H^* is cocommutative. Then H is commutative and we have $H \cong \mathbf{k}[x,y]/(x^p, y^p)$ by [59, Thm. 14.4]. It is easy to check that the coalgebra structures given in (1)-(5) are non-isomorphic. The same argument applies to the other case. Theorem 1.0.2 shows that when $\dim \mathrm{P}(H^*) = 1$, there are three non-isomorphic classes. Since $\dim J/J^2 = \dim \mathrm{P}(H^*) = 1$, H is isomorphic to $\mathbf{k}[x]/(x^{p^2})$ as algebras. Because those given in (6)-(8) are non-isomorphic as coalgebras. They complete the list. ■

Remark 11. In fact, the Hopf algebras in Corollary 4.0.11 (1)-(8) are in one-to-one correspondence with those in Theorem 1.0.2 (1)-(8) via duality. Below, we describe explicitly the realization of the generator(s) of each Hopf algebra as linear functional(s) on the corresponding one in Theorem 1.0.2. For the Hopf algebras in Corollary 4.0.11 (1)-(5), there are two generators x and y. The resulting linear functionals are denoted by ξ_x and ξ_y. For those in Corollary 4.0.11 (6)-(8), x is the only generator. The resulting linear functional is denoted by ξ_x, respectively. It is sufficient to give the values of ξ_x and ξ_y on the basis

$\{x^iy^j|0 \le i,j \le p-1\}$ of each Hopf algebra in Theorem 1.0.2.

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i=1,\ j=0 \\ 0 & \text{otherwise} \end{cases}, \quad \xi_y\left(x^iy^j\right) = \begin{cases} 1 & i=0,\ j=1 \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i\neq 0,\ j=0 \\ 0 & \text{otherwise} \end{cases}, \quad \xi_y\left(x^iy^j\right) = \begin{cases} 1 & i=0,\ j=1 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i=1,\ j=0 \\ 0 & \text{otherwise} \end{cases}, \quad \xi_y\left(x^iy^j\right) = \begin{cases} -1 & i=0,\ j=1 \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i\neq 0,\ j=0 \\ 0 & \text{otherwise} \end{cases}, \quad \xi_y\left(x^iy^j\right) = \begin{cases} 1 & i=0,\ j\neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i\neq 0,\ j=0 \\ 0 & \text{otherwise} \end{cases}, \quad \xi_y\left(x^iy^j\right) = \begin{cases} 1 & j=1 \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

$$\xi_x\left(x^iy^j\right) = \begin{cases} 1 & i=1,\ j=0 \\ 0 & \text{otherwise} \end{cases}. \tag{6-8}$$

Theorem 4.0.12. *Let H be a finite-dimensional connected Hopf algebra with* $\dim \mathrm{P}(H) = 1$. *Then the center of H contains* $\mathrm{P}(H)$.

Proof. Suppose $\mathrm{P}(H)$ is spanned by x. By Corollary 3.1.3, H has an increasing sequence of normal Hopf subalgebras:

$$\mathbf{k} = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = H$$

satisfying N_1 is generated by x and $N_{n-1} \subset H$ is normal with p-index one. We show by induction on n such that the center of H contains x. It is trivial when $n = 1$. Assume that $n \ge 2$. Then by Theorem 2.4.5, we can find some $y \in H \setminus N_{n-1}$ such that $\Delta(y) = y \otimes 1 + 1 \otimes y + u$, where $u \in N_{n-1} \otimes N_{n-1}$, which together with N_{n-1} generate H. Apply Theorem 2.2.5 to $N_{n-1} \subset H$, we have $y^p + \lambda\, y + a = 0$ for some $\lambda \in \mathbf{k}$ and $a \in N_{n-1}$.

By induction, $x \in Z(N_{n-1})$. Then it suffices to show $[x, y] = 0$. It is easy to check that $[x, y]$ is primitive. Therefore we can write $[x, y] = \mu x$ for some $\mu \in \mathbf{k}$. By rescaling, we can further assume either $x^p = 0$ or $x^p = x$. When $x^p = 0$, by Theorem 3.1.4, H is local. Then its quotient H/N_{n-1}^+H, which is generated by the image of y, is local too. Hence the image of y in H/N_{n-1}^+H is nilpotent since it is primitive. Thus in the relation $y^p + \lambda\ y + a = 0$, we must have $\lambda = 0$ and $y^p + a = 0$. A calculation therefore shows that $\mu^p x = x(\mathrm{ad} y)^p = [x, y^p] = [x, -a] = 0$ which implies that $[x, y] = \mu x = 0$. When $x^p = x$, we have $[x, y] = [x^p, y] = (\mathrm{ad} x)^p y = 0$. This completes the proof. ■

Chapter 5

CONNECTED HOPF ALGEBRAS OF DIMENSION P^3 I

5.1 *When* $\mathbf{P}(H)$ *is one-dimensional*

Let H be a connected Hopf algebra of dimension p^3, and K be the Hopf subalgebra of H generated by its primitive space. By Remark 6, $K \cong u(P(H))$, the restricted universal enveloping algebra of $P(H)$. Hence, $\dim K = p,\, p^2,\, p^3$. In this chapter, our main results are divided into three cases: $\dim K = p$ (Theorem 1.0.3), $\dim K = p^2$ and K is noncommutative (Theorem 1.0.4), and $\dim K = p^3$ (Theorem 1.0.5). Hopf algebras in isomorphism classes of H are always presented in the form of

$$\mathbf{k}\langle x,\, y,\, z\rangle / I,$$

where I is an ideal generated by relations. And the comultiplication is given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x,$$
$$\Delta(y) = y \otimes 1 + 1 \otimes y + Y,$$
$$\Delta(z) = z \otimes 1 + 1 \otimes z + Z,$$

for some elements Y and Z in $(\mathbf{k}\langle x,\, y,\, z\rangle/I) \otimes (\mathbf{k}\langle x,\, y,\, z\rangle/I)$.

Recall from Definition 9 that the *first order* of the inclusion $K \subset H$ is the minimal integer i such that $K_i \subsetneq H_i$, and that the *p-index* of K in H is $n - m$. We will also use *the second term of the Hochschild cohomology* $\mathrm{H}^2(\mathbf{k}, H)$ of H with coefficients in the trivial H-bicomodule $\mathbf{k}$. It can be computed as the homology of the following complex [44, Lemma 1.1]:

$$\mathbf{k} \xrightarrow{0} H \xrightarrow{d^1} H \otimes H \xrightarrow{d^2} H \otimes H \otimes H \longrightarrow \cdots,$$

where the differentials d^1 and d^2 are defined as, for any $h,\, g \in H$,

$$d^1(h) = 1 \otimes h - \Delta(h) + h \otimes 1,$$
$$d^2(h \otimes g) = 1 \otimes h \otimes g - \Delta(h) \otimes g + h \otimes \Delta(g) - h \otimes g \otimes 1.$$

Then

$$\mathrm{H}^2(\mathbf{k}, H) := \operatorname{Ker} d^2 / \operatorname{Im} d^1.$$

In this section, we suppose that $\dim K = p$, or equivalently $\dim P(H) = 1$. It is clear that K is generated by a primitive element, which will be denoted by x. Since $\dim P(H) = 1$, it follows from Theorem 4.0.12 that x is in the center of H. By Corollary 3.1.3, H is always cocommutative and contains a chain of normal Hopf subalgebras $K \subset F \subset H$, where $\dim F = p^2$. In particular, $\dim P(F) = 1$. Following the classification of connected Hopf algebras of dimension p^2 with one-dimensional primitive space provided in Lemma 4.0.10, we can write F as one of the following:

$$\begin{aligned} &\mathbf{k}[x, y]/(x^p - x, y^p - y), \\ &\mathbf{k}[x, y]/(x^p, y^p - x), \\ &\mathbf{k}[x, y]/(x^p, y^p), \end{aligned} \tag{5.1.1}$$

with

$$\begin{gathered} \Delta(x) = x \otimes 1 + 1 \otimes x, \quad \Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x), \\ \epsilon(x) = \epsilon(y) = 0, \quad S(x) = -x, \quad S(y) = -y. \end{gathered}$$

Next, we will obtain the comultiplication of the third generator of H. By Lemma 2.4.1, $\dim \mathrm{H}^2(\mathbf{k}, F) = \dim \mathrm{H}^2(F^*, \mathbf{k})$. Direct computation shows that $F^* \cong \mathbf{k}[x]/(x^{p^2})$ as algebras. Then $\dim \mathrm{H}^2(\mathbf{k}, F) = \dim \mathrm{H}^2(F^*, \mathbf{k}) = 1$. Suppose $\mathrm{H}^2(\mathbf{k}, F)$ is spanned by the image of a cocycle $u \in F \otimes F$. Let m be the first order of the inclusion $F \subset H$. Note that the p-index of F in H is one. Then $\dim H_m/F_m = 1$ by Lemma 2.2.1. Furthermore, by Theorem 2.4.5, d^1 induces a $\mathbf{k}$-vector space isomorphism from H_m/F_m to $\mathrm{H}^2(\mathbf{k}, F)$. Therefore, there is some $z \in H \setminus F$ such that $d^1(z) = 1 \otimes z - \Delta(z) + z \otimes 1 = -u$. That is, $\Delta(z) = z \otimes 1 + 1 \otimes z + u$. Note that the comultiplication for F in the three cases of (5.1.1) are the same. One can compute u directly by using the Hopf algebra structures of F in (5.1.1).

In fact, a similar computation has been done by Henderson in [26] to classify low-dimensional connected graded Hopf algebras over fields of characteristic p. In [26, Theorem 3.3, type h-3], the connected graded Hopf algebra of dimension p^3 is generated by x_1, y_1, z_1

with

$$\bar{\psi}(y_1) = \sum_{r,s>0,\ r+s=p} \frac{1}{r!s!} x_1^r \otimes x_1^s$$

and

$$\bar{\psi}(z_1) = \sum_{r,s>0,\ r+s=p} \frac{1}{r!s!} y_1^r \otimes y_1^s - \bar{\psi}(y_1)(\Delta(y_1))^{p-1},$$

where $\bar{\psi}$ is the same as $-d^1$ in our notation (i.e., $\bar{\psi}(y_1) = \Delta(y_1) - y_1 \otimes 1 - 1 \otimes y_1$). Note that the expression

$$\sum_{r,s>0,\ r+s=p} \frac{1}{r!s!} x_1^r \otimes x_1^s$$

is the same as $-\boldsymbol{\omega}(x_1)$, since $(p-1)! \equiv -1(\text{mod } p)$. Thus,

$$-d^1(z_1) = \bar{\psi}(z_1) = -\boldsymbol{\omega}(y_1) + \boldsymbol{\omega}(x_1)[\Delta(y_1)]^{p-1}.$$

The Hopf subalgebra F_1 generated by x_1, y_1 in [26, Theorem 3.3 type h-3] is isomorphic to F as coalgebras via $\phi : x_1 \to x,\ y_1 \to -y$. Moreover, $[x_1,\ y_1] = [x,\ y] = 0$. Then, $\bar{\psi}(z_1)$, associated with the coalgebra structure, represents a basis in $\mathrm{H}^2(\mathbf{k}, F_1)$. Hence, back to our setting F and $z \in H \setminus F$, we can choose u as

$$\begin{aligned}(\phi \otimes \phi)(-d^1(z_1)) =& (\phi \otimes \phi)(-\boldsymbol{\omega}(y_1) + \boldsymbol{\omega}(x_1)[\Delta(y_1)]^{p-1}) \\ =& -\boldsymbol{\omega}(\phi(y_1)) + \boldsymbol{\omega}(\phi(x_1))[\Delta(\phi(y_1))]^{p-1} \\ =& \boldsymbol{\omega}(y) + \boldsymbol{\omega}(x)[\Delta(y)]^{p-1}.\end{aligned}$$

Note that F and z generate a Hopf subalgebra of H. Since $z \in H \setminus F$ and F has p-index one in H, then H is generated by x, y, z. Moreover, we can assume

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)[y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)]^{p-1} + \boldsymbol{\omega}(y)$$

for all the three cases in (5.1.1).

Lemma 5.1.1. *Let x, y, F and z be as above and further assume that $x^p = 0$. Then*

(i) $u = \boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \boldsymbol{\omega}(y)$,

(ii) $[y, z] = \gamma x$ *for some* $\gamma \in \mathbf{k}$, *and*

$$\Delta(z^p + \gamma^{p-1}x^{p-1}y) = (z^p + \gamma^{p-1}x^{p-1}y) \otimes 1 + 1 \otimes (z^p + \gamma^{p-1}x^{p-1}y) + \boldsymbol{\omega}(y^p).$$

Proof. i) First, we rewrite $u = \boldsymbol{\omega}(x)[y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)]^{p-1} + \boldsymbol{\omega}(y)$ as

$$\boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \sum_{i=1}^{p-1} \binom{p-1}{i} \boldsymbol{\omega}(x)^{i+1}(y \otimes 1 + 1 \otimes y)^{p-1-i} + \boldsymbol{\omega}(y).$$

Since $x^p = 0$, it is easy to see that $\boldsymbol{\omega}(x)^n = 0$ for $n \geq 2$, and so

$$u = \boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \boldsymbol{\omega}(y).$$

ii) Note that x is in the center of H. Then, we have

$$\Delta([y,\ z]) = [\Delta(y), \Delta(z)] = [y, z] \otimes 1 + 1 \otimes [y, z].$$

Hence, $[y, z]$ is primitive in H. So we can write $[y, z] = \gamma x$ for some $\gamma \in \mathbf{k}$. For positive integers m and n, it follows by direct computation that

$$(y^m)(\mathrm{ad} z)^n = \begin{cases} \frac{m!}{(m-n)!}\gamma^n x^n y^{m-n} & m \geq n, \\ 0 & m < n. \end{cases} \tag{5.1.2}$$

By Lemma 2.3.1,

$$\begin{aligned} \Delta(z^p) &= \Delta(z)^p = (u + z \otimes 1 + 1 \otimes z)^p \\ &= u^p + (z \otimes 1 + 1 \otimes z)^p + \sum_{i=1}^{p-1} s_i, \end{aligned}$$

where is_i is the coefficient of λ^{i-1} in $u[\mathrm{ad}(\lambda u + z \otimes 1 + 1 \otimes z)]^{p-1}$. Since $[x, z] = 0$ and $[y,\ z] = \gamma x$, we have $u[\mathrm{ad}(\lambda u + z \otimes 1 + 1 \otimes z)]^i \in (F \otimes F)[\lambda]$ for any integer $i \geq 0$. Moreover, F is commutative. Hence, for any $f \in F \otimes F$, we have

$$f\,[\mathrm{ad}(\lambda u + z \otimes 1 + 1 \otimes z)] = f(\mathrm{ad} z \otimes 1 + 1 \otimes \mathrm{ad} z).$$

Thus,

$$u[\mathrm{ad}(\lambda u + z \otimes 1 + 1 \otimes z)]^{p-1} = u(\mathrm{ad} z \otimes 1 + 1 \otimes \mathrm{ad} z)^{p-1}.$$

By i), $u^p = [\boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \boldsymbol{\omega}(y)]^p = \boldsymbol{\omega}(y)^p = \boldsymbol{\omega}(y^p)$. Therefore,

$$\Delta(z^p) = z^p \otimes 1 + 1 \otimes z^p + \boldsymbol{\omega}(y^p) + u(\mathrm{ad} z \otimes 1 + 1 \otimes \mathrm{ad} z)^{p-1}.$$

The last term of $\Delta(z^p)$ is the sum of $[\boldsymbol{\omega}(x)(y\otimes 1+1\otimes y)^{p-1}](\mathrm{ad}z\otimes 1+1\otimes \mathrm{ad}z)^{p-1}$ and $\boldsymbol{\omega}(y)(\mathrm{ad}z\otimes 1+1\otimes \mathrm{ad}z)^{p-1}$, which we will refer to as I_1 and I_2, respectively.

First of all, $I_1=\boldsymbol{\omega}(x)[(y\otimes 1+1\otimes y)^{p-1}(\mathrm{ad}z\otimes 1+1\otimes \mathrm{ad}z)^{p-1}]$, since x is in the center of H. After binomial expansion,

$$I_1=\boldsymbol{\omega}(x)\sum_{i,j=0}^{p-1}\binom{p-1}{i}\binom{p-1}{j}y^i(\mathrm{ad}z)^j\otimes y^{p-1-i}(\mathrm{ad}z)^{p-1-j}.$$

By (5.1.2), the terms for $i\neq j$ in the above summation all vanish. Hence,

$$\begin{aligned}I_1&=\boldsymbol{\omega}(x)\sum_{i=0}^{p-1}\binom{p-1}{i}\binom{p-1}{i}y^i(\mathrm{ad}z)^i\otimes y^{p-1-i}(\mathrm{ad}z)^{p-1-i}\\&=\boldsymbol{\omega}(x)\sum_{i=0}^{p-1}\frac{(p-1)!^2}{i!(p-1-i)!}\gamma^{p-1}x^i\otimes x^{p-1-i}.\end{aligned}$$

Note that $(p-1)!=-1 \pmod p$. Then

$$I_1=-\gamma^{p-1}\boldsymbol{\omega}(x)\,(x\otimes 1+1\otimes x)^{p-1}=-\gamma^{p-1}\boldsymbol{\omega}(x)\,\Delta(x)^{p-1}.$$

For I_2, we follow a similar argument. By direct expansion,

$$I_2=\sum_{i=1}^{p-1}\sum_{j=0}^{p-1}t(i,j),$$

where

$$t(i,j)=\frac{(p-1)!}{i!(p-i)!}\binom{p-1}{j}y^i(\mathrm{ad}z)^j\otimes y^{p-i}(\mathrm{ad}z)^{p-1-j}.$$

Again by (5.1.2), the terms for $i\neq j$ or $i\neq j+1$ all vanish. Then, we have

$$\begin{aligned}I_2=&t(1,0)+t(p-1,p-1)+\sum_{j=1}^{p-2}[t(j,j)+t(j+1,j)]\\=&-\gamma^{p-1}y\otimes x^{p-1}-\gamma^{p-1}x^{p-1}\otimes y-\gamma^{p-1}\sum_{j=1}^{p-2}\left[\binom{p-1}{j}x^j\otimes x^{p-1-j}y+\binom{p-1}{j}x^jy\otimes x^{p-1-j}\right]\\=&-\gamma^{p-1}\left[(x\otimes 1+1\otimes x)^{p-1}(y\otimes 1+1\otimes y)-x^{p-1}y\otimes 1-1\otimes x^{p-1}y\right].\end{aligned}$$

Thus,

$$\begin{aligned}\Delta(z^p)&=z^p\otimes 1+1\otimes z^p+\boldsymbol{\omega}(y^p)+I_1+I_2\\&=z^p\otimes 1+1\otimes z^p+\boldsymbol{\omega}(y^p)-\Delta(\gamma^{p-1}x^{p-1}y)+(\gamma^{p-1}x^{p-1}y\otimes 1+1\otimes\gamma^{p-1}x^{p-1}y).\end{aligned}$$

The second assertion of ii) follows immediately. ■

Theorem 5.1.2. *Suppose that x and y are described in* (5.1.1)*, that is,*

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \quad \Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x),$$
$$\epsilon(x) = \epsilon(y) = 0, \ S(x) = -x, \ S(y) = -y.$$

Then H is isomorphic to

(A1) $\mathbf{k}[x, y, z]/(x^p - x, y^p - y, z^p - z)$ *with*

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)\,[y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)]^{p-1} + \boldsymbol{\omega}(y),$$
$$\epsilon(z) = 0, \ S(z) = -z,$$

or one of the following

(A2) $H(\alpha) := \mathbf{k}[x, y, z]/(x^p, y^p - x, z^p - y - \alpha x)$,

(A3) $\mathbf{k}[x, y, z]/(x^p, y^p, z^p)$,

(A4) $\mathbf{k}[x, y, z]/(x^p, y^p, z^p - x)$,

(A5) $A(\beta) := \mathbf{k}\langle x, y, z\rangle/(x^p, y^p, \ [x, y], [x, z], [y, z] - x, z^p + x^{p-1}y - \beta x)$,

where $\alpha, \beta \in \mathbf{k}$ and

$$\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} + \boldsymbol{\omega}(y),$$
$$\epsilon(z) = 0, \ S(z) = -z.$$

Proof. Retain the information on x, y, F, and z obtained prior to Lemma 5.1.1. Then H is generated by F and z. There are three cases according to (5.1.1).

Case 1. Suppose that $F = \mathbf{k}[x, y]/(x^p - x, y^p - y)$. Note that $P(H)$ is a *torus* in the sense of [34]. Then by [34, Theorem 0.1], H is commutative and semisimple. In particular, $[y, \ z] = 0$. Consider $u^p = \{\boldsymbol{\omega}(x)[y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)]^{p-1} + \boldsymbol{\omega}(y)\}^p$. It follows from $[x, y] = 0$, $x^p = x$, $y^p = y$, and char$\mathbf{k} = p$ that $u^p = u$. Hence

$$\Delta(z^p - z) = \Delta(z)^p - \Delta(z) = (z^p - z) \otimes 1 + 1 \otimes (z^p - z).$$

That is, $z^p - z$ is primitive. There is some $\lambda \in \mathbf{k}$ such that $z^p - z = \lambda x$. Now consider the shifting $z' = z + \alpha x$ for some $\alpha \in \mathbf{k}$. It is clear that $\Delta(z') = z' \otimes 1 + 1 \otimes z' + u$. If the scalar α satisfies $\lambda + \alpha^p - \alpha = 0$, then we have $z'^p - z' = z^p - z + (\alpha^p - \alpha)x = 0$. In other words, we can assume, up to isomorphism, that $z^p = z$. This gives (A1).

Case 2. Suppose $F = \mathbf{k}[x,\ y]/(x^p,\ y^p - x)$. Note that $x^p = y^p - x = 0$. By Lemma 5.1.1 (ii), we can write $[y,\ z] = \gamma x$ for some $\gamma \in \mathbf{k}$ and

$$\Delta(z^p + \gamma^{p-1}x^{p-1}y) = (z^p + \gamma^{p-1}x^{p-1}y) \otimes 1 + 1 \otimes (z^p + \gamma^{p-1}x^{p-1}y) + \boldsymbol{\omega}(x).$$

Moreover, $\Delta(y) = y \otimes 1 + 1 \otimes y + \boldsymbol{\omega}(x)$. Hence $z^p + \gamma^{p-1}x^{p-1}y - y$ is primitive. Thus, $z^p + \gamma^{p-1}x^{p-1}y = y + \alpha x$ for some $\alpha \in \mathbf{k}$. Note that $[z^p + \gamma^{p-1}x^{p-1}y,\ z] = \gamma^{p-1}x^{p-1}[y,\ z] = \gamma^p x^p = 0$ and that $[y + \alpha x,\ z] = [y,\ z] = \gamma x$. Thus, $\gamma = 0$, $[y,\ z] = 0$, and so $z^p = y + \alpha x$. This gives (A2).

Case 3. Suppose $F = \mathbf{k}[x,\ y]/(x^p,\ y^p)$. By Lemma 5.1.1 ii), we can write $[y,\ z] = \gamma x$ for some $\gamma \in \mathbf{k}$ and $z^p + \gamma^{p-1}x^{p-1}y$ is primitive, since $\boldsymbol{\omega}(y^p) = 0$. So we can write $z^p + \gamma^{p-1}x^{p-1}y = \alpha x$ for some $\alpha \in \mathbf{k}$.

When $\gamma = 0$ and $\alpha = 0$, it follows that $[y,\ z] = 0$ and $z^p = 0$. This gives (A3).

When $\gamma = 0$ and $\alpha \neq 0$, consider the rescaling $x' = ax,\ y' = a^p y,\ z' = a^{p^2} z$ of the variables $x,\ y,\ z$, where $a \in \mathbf{k}^\times$. One can check that the rescaling preserves the comultiplication on the generators, that is, $\Delta(x') = x' \otimes 1 + 1 \otimes x'$, $\Delta(y') = y' \otimes 1 + 1 \otimes y' + \boldsymbol{\omega}(x')$, and $\Delta(z') = z' \otimes 1 + 1 \otimes z' + \boldsymbol{\omega}(x')[y' \otimes 1 + 1 \otimes y']^{p-1} + \boldsymbol{\omega}(y')$. It is clear that $x'^p = 0$, $y'^p = 0$, and $[y',\ z'] = 0$. Let $a = \alpha^{-p^3+1}$. Then $z'^p = a^{p^3} z^p = a^{p^3}\alpha x = a^{p^3-1}\alpha x' = x'$. Therefore, we can assume, up to isomorphism, that $z^p = x$. This gives (A4).

When $\gamma \neq 0$, consider again the rescaling $x' = ax,\ y' = a^p y,\ z' = a^{p^2} z$ of the variables $x,\ y,\ z$, for some $a \in \mathbf{k}^\times$. It is clear that $x'^p = 0$, $y'^p = 0$. Let $a = \gamma^{-1/(p^2+p-1)}$. Then $[y',\ z'] = a^{p^2+p}[y,\ z] = a^{p+p^2}\gamma x = a^{p^2+p-1}\gamma x' = x'$. Hence, up to isomorphism, we can assume that $\gamma = 1$. This gives (A5). ■

Remark 12. The Hopf algebra in Theorem 5.1.2 (A1), namely, $H = \mathbf{k}[x,\ y,\ z]/(x^p - x,\ y^p - y,\ z^p - z)$, is semisimple and isomorphic to $(\mathbf{k}C_{p^3})^*$, where C_{p^3} is the cyclic group of order p^3.

Notice that the Hopf algebras in Theorem 5.1.2 (A2) and (A5) are subject to parameters α and β, respectively. Next, we discuss the isomorphism classes with respect to the choices of the parameters.

Proposition 5.1.3. *Let $A(\beta)$ be any Hopf algebra described in Theorem 5.1.2* (A5) *and $H(\alpha)$ be any Hopf algebra described in Theorem 5.1.2* (A2)*. Then*

(i) When $p = 2$, $A(\beta)$ are all isomorphic. When $p > 2$, $A(\beta)$ is parametrized by $\mathbf{k}/\sqrt[p^2+p-1]{1}$.

(ii) $H(\alpha)$ are all isomorphic.

Proof. (i) Denote the generators of $A(\beta')$ and $A(\beta)$ by x', y', z' and x, y, z, respectively. Suppose $A(\beta')$ and $A(\beta)$ are isomorphic as Hopf algebras via $\phi: A(\beta') \to A(\beta)$. Then ϕ induces an isomorphism $\phi_{\mathrm{gr}}: \mathrm{gr}A(\beta') \to \mathrm{gr}A(\beta)$ for their associated graded Hopf algebras with respect to their coradical filtrations (see Definition 7). It is clear that

$$\mathrm{gr}A(\beta) = \mathbf{k}\langle \bar{x}, \bar{y}, \bar{z}\rangle / (\bar{x}^p, \bar{y}^p, \bar{z}^p)$$

with comultiplication given by

$$\begin{aligned}
\Delta(\bar{x}) &= \bar{x} \otimes 1 + 1 \otimes \bar{x}, \\
\Delta(\bar{y}) &= \bar{y} \otimes 1 + 1 \otimes \bar{y} + \boldsymbol{\omega}(\bar{x}), \\
\Delta(\bar{z}) &= \bar{z} \otimes 1 + 1 \otimes \bar{z} + \boldsymbol{\omega}(\bar{x})(\bar{y} \otimes 1 + 1 \otimes \bar{y})^{p-1} + \boldsymbol{\omega}(\bar{y}).
\end{aligned}$$

Hence, there exists some scalar $\gamma \in \mathbf{k}^\times$ such that

$$\phi_{\mathrm{gr}}(\bar{x'}) = \gamma \bar{x},\ \phi_{\mathrm{gr}}(\bar{y'}) = \gamma^p \bar{y},\ \phi_{\mathrm{gr}}(\bar{z'}) = \gamma^{p^2} \bar{z}.$$

Now, back to the map $\phi: A(\beta') \to A(\beta)$. Since the first order of the inclusion $K \subset F$ is p, we have $\phi(y') = \gamma^p y + A$ for some $A \in F_{p-1} = K_{p-1} \subset K$. Similarly, we have $\phi(z') = \gamma^{p^2} z + B$ for some $B \in F$. That is,

$$\phi(x') = \gamma x,\ \phi(y') = \gamma^p y + A,\ \phi(z') = \gamma^{p^2} z + B,$$

where $A \in K$ and $B \in F$.

Since ϕ is a coalgebra map, $(\phi \otimes \phi)\Delta(y') = \Delta[\phi(y')]$. Then, it can be shown that $\Delta(A) = A \otimes 1 + 1 \otimes A$. Hence, we can write $A = ax$ for some $a \in \mathbf{k}$. Similarly, it follows from $(\phi \otimes \phi)\Delta(z') = \Delta[\phi(z')]$ that

$$\begin{aligned} &\Delta(B) - B \otimes 1 - 1 \otimes B \\ =&\gamma^p \boldsymbol{\omega}(x)\left[\gamma^p(y \otimes 1 + 1 \otimes y) + a(x \otimes 1 + 1 \otimes x)\right]^{p-1} + \boldsymbol{\omega}(\gamma^p y + ax) \\ &- \gamma^{p^2}\boldsymbol{\omega}(x)(y \otimes 1 + 1 \otimes y)^{p-1} - \gamma^{p^2}\boldsymbol{\omega}(y). \end{aligned} \tag{5.1.3}$$

Direct computation shows that the element

$$\sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} (\gamma^p y)^i (ax)^{p-i} + a^p y$$

satisfies the above equation (5.1.3) in B. (The computation is tedious and omitted here.) If B_1 and B_2 are both solutions to the equation (5.1.3), then $d^1(B_1 - B_2) = 0$, and so B_1 and B_2 differ by a primitive element. Thus, we can write

$$B = M + a^p y + bx, \text{ where } b \in \mathbf{k} \text{ and } M := \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}(\gamma^p y)^i (ax)^{p-i}.$$

It follows immediately that $M \in F$ and $M^p = 0$. In summary, the isomorphism ϕ can be written as:

$$\begin{cases} \phi(x') = \gamma x, \\ \phi(y') = \gamma^p y + ax, \\ \phi(z') = \gamma^{p^2} z + M + a^p y + bx, \end{cases} \tag{5.1.4}$$

for some $a, b \in \mathbf{k}$ and $\gamma \in \mathbf{k}^\times$.

On the other hand, we claim that ϕ is an algebra map. Indeed,

$$\begin{aligned} \phi([y', z'] - x') &= 0, \\ \phi\Big((z')^p + (x')^{p-1}y' - \beta' x'\Big) &= 0. \end{aligned}$$

First, we claim that

$$\phi(z')^p = \begin{cases} \gamma^{p^3} z^p & \text{for } p > 2, \\ \gamma^8 z^2 + \gamma^4 a^2 x & \text{for} p = 2. \end{cases}$$

Since $[x,y]=[x,z]=x^p=y^p=0$, we have

$$\begin{aligned}\phi(z')^p &= (\gamma^{p^2}z+M+a^py+bx)^p\\ &= (\gamma^{p^2}z+M+a^py)^p\\ &= (\gamma^{p^2}z+M)^p+S,\end{aligned}$$

where $S=\sum_{i=1}^{p-1}s_i$ with is_i being the coefficient of λ^{i-1} in

$$(a^py)\Big[\mathrm{ad}(\lambda a^py+\gamma^{p^2}z+M)\Big]^{p-1}.$$

Note that

$$[a^py,\lambda a^py+\gamma^{p^2}z+M]=\gamma^{p^2}a^px.$$

Then, since x is in the center of $A(\beta)$, we have $S=0$ for $p>2$. When $p=2$, we have $S=\gamma^4a^2x$. By (5.1.2) and the fact that $x^p=0$, one can check that

$$(y^ix^{p-i})(\mathrm{ad}z)^{p-1}=x^{p-i}[y^i(\mathrm{ad}z)^{p-1}]=0.$$

Hence $M[\mathrm{ad}(\gamma^{p^2}z)]^{p-1}=0$, and so

$$(\gamma^{p^2}z+M)^p=\gamma^{p^3}z^p.$$

This proves the claim.

Next, the condition $\phi([y',z']-x')=0$ implies that

$$\Big[\gamma^py+ax,\quad \gamma^{p^2}z+M+a^py+bx\Big]=\gamma x.$$

In view of the algebraic relations in $A(\beta)$, this yields

$$\gamma^{p^2+p-1}=1.$$

Moreover, $\phi\Big((z')^p+(x')^{p-1}y'-\beta'x'\Big)=0$ implies that $\phi(z')^p+\gamma^{2p-1}x^{p-1}y-\beta'\gamma x=0$. Combining with the relation $z^p+x^{p-1}y-\beta x=0$, we have

$$\phi(z')^p-\gamma^{2p-1}z^p+(\beta\gamma^{2p-1}-\beta'\gamma)x=0 \tag{5.1.5}$$

In summary, we see that any isomorphism from $A(\beta') \to A(\beta)$ must be in the form of (5.1.3) for some $a, b \in \mathbf{k}$, $\gamma \in \mathbf{k}^{\times}$,

$$M = \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}(\gamma^p y)^i (ax)^{p-i},$$

and satisfy the following condition:

$$\begin{cases} \gamma^{p^2+p-1} = 1, \\ \phi(z')^p - \gamma^{2p-1}z^p + (\beta\gamma^{2p-1} - \beta'\gamma)x = 0, \end{cases} \tag{5.1.6}$$

where

$$\phi(z')^p = \begin{cases} \gamma^{p^3} z^p & \text{for } p > 2, \\ \gamma^8 z^2 + \gamma^4 a^2 x & \text{for } p = 2. \end{cases}$$

We can check that any $\mathbf{k}$-linear map from $A(\beta') \to A(\beta)$ as described above for some $a, b \in \mathbf{k}$, $\gamma \in \mathbf{k}^{\times}$ preserves the algebra and coalgebra structure and so is a bialgebra map. By [17, Proposition 4.2.5], any bialgebra map is always a Hopf algebra map. Moreover, any such a map induces an isomorphism between the associated graded algebra of $A(\beta')$ and $A(\beta)$ with respect to the coradical filtration, and then becomes a Hopf algebra isomorphism. Therefore, any map given in (5.1.4) is an isomorphism from $A(\beta')$ to $A(\beta)$ if and only if (5.1.6) also holds.

When $p > 2$, it follows from (5.1.6) that

$$\gamma^{p^3-2p+1} = 1 \quad \text{and} \quad \beta' = \beta\gamma^{2p-2}.$$

Note that p^2+p-1 divides p^3-2p+1 and that $(p^2+p-1,\, 2p-2) = 1$ for $p > 2$. Therefore, $A(\beta') \cong A(\beta)$ if and only if there is a map $\phi :\, A(\beta') \to A(\beta)$ in the form of (5.1.4) for some $a, b \in \mathbf{k}$ and a (p^2+p-1)-th root of unity γ such that $\beta' = \gamma\beta$.

When $p = 2$, it follows from (5.1.6) that

$$\gamma^8 z^2 + \gamma^4 a^2 x - \gamma^3 z^2 + \beta\gamma^3 - \beta'\gamma = 0.$$

Hence, $A(\beta') \cong A(\beta)$ if and only if there is a map $\phi :\, A(\beta') \to A(\beta)$ in the form of (**??**) with $\gamma^5 = 1$ and $a^2 = \beta'\gamma^{-3} - \beta\gamma^{-1}$. In other words, when $p = 2$, $A(\beta') \cong A(\beta)$ for any $\beta, \beta' \in \mathbf{k}$.

(ii) Denote the generators of $H(\alpha')$ and $H(\alpha)$ by x', y', z' and x, y, z, respectively. Similar computation used in (i) shows that the following map ψ is an isomorphism from $H(\alpha')$ to $H(\alpha)$

$$\begin{cases} \psi(x') = x, \\ \psi(y') = y + ax, \\ \psi(z') = z + \displaystyle\sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} y^i (ax)^{p-i} + a^p y, \end{cases}$$

where $a \in \mathbf{k}$ such that $a^2 - a = \alpha' - \alpha$. Therefore, $H(\alpha') \cong H(\alpha)$ for any $\alpha, \alpha' \in \mathbf{k}$. ■

Proof of Theorem 1.0.3. In Theorem 5.1.2, the type (A5) is the only one with noncommutative algebra structure. It is clear that (A1) to (A4) are not isomorphic to each other as commutative algebras. Moreover, in Proposition 5.1.3, let $\beta = 0$ when $p = 2$ in (A5) and $\alpha = 0$ in (A2). Then the theorem follows by combining Theorem 5.1.2 and Proposition 5.1.3. ■

5.2 *When* $\mathbf{P}(H)$ *is two-dimensional and nonabelian*

In this section, suppose $\dim K = p^2$ and K is noncommutative. By Theorem 1.0.2(5), we can write

$$K = \mathbf{k}\langle x, y\rangle / ([x, y] - y, x^p - x, y^p),$$

where x and y are primitive elements with $\epsilon(x) = \epsilon(y) = 0$, $S(x) = -x$, and $S(y) = -y$. The following lemma contains some computational results needed later. Throughout, the following expression is used:

$$f(x) = \sum_{i=1}^{p-1} \frac{(-1)^{i-1}}{(p-i)} x^i.$$

Lemma 5.2.1. *Let x, y and K as above. Then we have*

(i) $[x \otimes 1 + 1 \otimes x, \boldsymbol{\omega}(y)] = 0,$

(ii) $[y \otimes 1 + 1 \otimes y, \boldsymbol{\omega}(x)] = \Delta[yf(x)] - yf(x) \otimes 1 - 1 \otimes yf(x).$

(iii) If $e \in H$ is primitive such that $[x, e] = [y, e] = 0$, then $e = 0$.

Proof. i) Note that $xy = yx + y$. Then, by induction, $[x, y^i] = iy^i$ for any positive integer i. Hence

$$[x \otimes 1 + 1 \otimes x, y^i \otimes y^{p-i}] = [x, y^i] \otimes y^{p-i} + y^i \otimes [x, y^{p-i}] = iy^i \otimes y^{p-i} + y^i \otimes (p-i)y^{p-i} = 0.$$

Therefore,

$$[x \otimes 1 + 1 \otimes x, \boldsymbol{\omega}(y)] = \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}[x \otimes 1 + 1 \otimes x, y^i \otimes y^{p-i}] = 0.$$

ii) Again by $xy = yx + y$, one can show inductively that

$$[y, x^i] = -[x^i, y] = -\sum_{j=0}^{i-1} \binom{i}{j} yx^j$$

for all $i \geq 1$. Note that the index i and $p - i$ are symmetric in $\boldsymbol{\omega}(x)$. Hence,

$$\begin{aligned}[y \otimes 1 + 1 \otimes y, \boldsymbol{\omega}(x)] &= \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} \left([y, x^{p-i}] \otimes x^i + x^i \otimes [y, x^{p-i}]\right) \\ &= -\sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} \sum_{j=0}^{p-i-1} \binom{p-i}{j} \left(yx^j \otimes x^i + x^i \otimes yx^j\right).\end{aligned}$$

Moreover, since $\mathrm{char}\mathbf{k} = p$, we have

$$\frac{(p-1)!}{(p-1-i-j)!} = (-1)^{i+j}(i+j)!.$$

It follows by direct computation that for any indices i, j the coefficient $\frac{(p-1)!}{i!(p-i)!}\binom{p-i}{j}$ can be rewritten as $\frac{(-1)^{i+j}}{p-i-j}\binom{i+j}{i}$. Hence

$$[y \otimes 1 + 1 \otimes y, \boldsymbol{\omega}(x)] = \sum_{i=1}^{p-1} \sum_{j=0}^{p-i-1} \frac{(-1)^{i+j+1}}{p-i-j} \binom{i+j}{i} \left(yx^j \otimes x^i + x^i \otimes yx^j\right).$$

To find $\Delta[yf(x)]$, we first define

$$A_l = (y \otimes 1 + 1 \otimes y)\Big[(x \otimes 1 + 1 \otimes x)^l - x^l \otimes 1 - 1 \otimes x^l\Big],$$

for positive integer l, which can be rewritten as

$$\begin{aligned}(y \otimes 1 + 1 \otimes y) \sum_{m=1}^{l-1} \binom{l}{m} x^{l-m} \otimes x^m &= \sum_{m=1}^{l-1} \binom{l}{m} \left(yx^{l-m} \otimes x^m + x^{l-m} \otimes yx^m\right) \\ &= \sum_{m=1}^{l-1} \binom{l}{m} \left(yx^{l-m} \otimes x^m + x^m \otimes yx^{l-m}\right).\end{aligned}$$

Then we obtain

$$\begin{aligned}
\Delta[yf(x)] &= \Delta(y)f(\Delta(x)) = (y\otimes 1+1\otimes y)\left[\sum_{l=1}^{p-1}\frac{(-1)^{l-1}}{p-l}(x\otimes 1+1\otimes x)^l\right]\\
&= \sum_{l=1}^{p-1}\frac{(-1)^{l-1}}{p-l}\left[(y\otimes 1+1\otimes y)\left(x^l\otimes 1+1\otimes x^l\right)+A_l\right]\\
&= \sum_{l=1}^{p-1}\frac{(-1)^{l-1}}{p-l}\left[yx^l\otimes 1+1\otimes yx^l+\sum_{m=1}^{l}\binom{l}{m}\left(yx^{l-m}\otimes x^m+x^m\otimes yx^{l-m}\right)\right]\\
&= yf(x)\otimes 1+1\otimes yf(x)+\sum_{l=1}^{p-1}\sum_{m=1}^{l}\frac{(-1)^{l-1}}{p-l}\binom{l}{m}\left[yx^{l-m}\otimes x^m+x^m\otimes yx^{l-m}\right].
\end{aligned}$$

Changing the order of the double summation $\sum_{l=1}^{p-1}\sum_{m=1}^{l}$ and replacing $l-m$ by j and m by i, we have

$$\Delta(yf(x))-yf(x)\otimes 1-1\otimes yf(x)=\sum_{i=1}^{p-1}\sum_{j=0}^{p-1-i}\frac{(-1)^{i+j-1}}{p-i-j}\binom{i+j}{i}\left[yx^j\otimes x^i+x^i\otimes yx^j\right],$$

which is the same as $[y\otimes 1+1\otimes y,\boldsymbol{\omega}(x)]$.

iii) Let $e\in H$ be a primitive element. Since $K=u(P(H))$, we can write $e=ux+vy$ for some $u,v\in\mathbf{k}$. Thus $[x,e]=vy$ and $[y,e]=-uy$. Hence $e=0$ if $[x,e]=[y,e]=0$. ■

Lemma 5.2.2. *There exists some $z\in H\setminus K$ such that H is generated by K and z, and the comultipilication of z, up to isomorphism, is one of the following*

(1) $\Delta(z)=z\otimes 1+1\otimes z+\boldsymbol{\omega}(y)$,

(2) $\Delta(z)=z\otimes 1+1\otimes z+\boldsymbol{\omega}(x)$,

(3) $\Delta(z)=z\otimes 1+1\otimes z-2x\otimes y$ *for* $p>2$.

Moreover, the comultiplication of z remains the same if it is shifted by any primitive element.

Proof. Suppose that H is cocommutative. By Theorem 2.4.6, there exists some $u\in H\setminus K$ such that

$$\Delta(u)=u\otimes 1+1\otimes u+\boldsymbol{\omega}(\alpha x+\beta y),$$

where $\alpha, \beta \in \mathbf{k}$, not all zero. If $\alpha = 0$, then $\beta \neq 0$. Letting $z = \beta^{-p}u$, we have $\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(y)$. This gives (1). If $\alpha \neq 0$, let $z = \alpha^{-p}u$. Then $\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x + my)$ with $m = \beta\alpha^{-1}$. Note that $(\mathrm{ad}(\lambda my + x))^{p-1}(my) = my$ for any $\lambda \in \mathbf{k}$. Then, we have $(x + my)^p = x^p + (my)^p + my = x + my$. It is clear that $[x + my, y] = y$. Thus, we can assume that $\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)$ by a shifting $x - my$ of x. This gives (2).

Now suppose that H is noncocommutative. By Proposition 2.4.2, $\{\boldsymbol{\omega}(x),\ \boldsymbol{\omega}(y),\ x \otimes y\}$ is a basis of $\mathrm{H}^2(\mathbf{k}, K)$. Then by Theorem 2.4.5, there exists some $u \in H \setminus K$ such that

$$\Delta(u) = u \otimes 1 + 1 \otimes u + \alpha\boldsymbol{\omega}(x) + \beta\boldsymbol{\omega}(y) + \gamma x \otimes y,$$

where $\alpha, \beta, \gamma \in \mathbf{k}$ and $\gamma \neq 0$. It is clear that $[\Delta(x), \alpha\boldsymbol{\omega}(x)] = 0$. By Lemma 5.2.1 i), $[\Delta(x), \beta\boldsymbol{\omega}(y)] = 0$. Thus,

$$\begin{aligned}\Delta([x, u]) &= [\Delta(x), \Delta(u)] \\ &= [x, u] \otimes 1 + 1 \otimes [x, u] + [\Delta(x),\ \gamma\, x \otimes y] \\ &= [x, u] \otimes 1 + 1 \otimes [x, u] + \gamma x \otimes y.\end{aligned}$$

We will show that $p \neq 2$ by contradiction. Suppose $p = 2$ and consider $\dim(H_2/K_2)$. First, we have $\dim\big(H_2/K_2\big) \leq 1$ by Lemma 2.2.1 and the fact that K has p-index one in H. Direct computation shows that

$$\Delta([y, u]) = [y, u] \otimes 1 + 1 \otimes [y, u] + \alpha(x \otimes y + y \otimes x) + \gamma y \otimes y.$$

Apply d^1 to the elements $[x, u]$ and $[y, u] + \alpha xy$ of H_2, that is,

$$d^1([x, u]) = \gamma x \otimes y \quad \text{and} \quad d^1([y, u] + \alpha xy) = \gamma y \otimes y.$$

By Proposition 2.4.2, $x \otimes y$ and $y \otimes y$ are linearly independent in $\mathrm{H}^2(\mathbf{k}, K)$. Moreover, by Theorem 2.4.5, d^1 induces an injection from H_2/K_2 to $\mathrm{H}^2(\mathbf{k}, K)$. Hence, $\dim\big(H_2/K_2\big) \geq 2$, a contradiction. Therefore, $p > 2$. Let $z = -2[x, u]/\gamma$. Then $\Delta(z) = z \otimes 1 + 1 \otimes z - 2x \otimes y$, which gives (3).

In all the cases, $z \notin K$ by direct computation using PBW Theorem. Note that the p-index of K in H is one. Hence H is generated by K and z. The last statement of the lemma is obvious. ■

Proof of Theorem 1.0.4. Now we assume that H is generated by K and some $z \in H \setminus K$ with the three types of comultiplication of z described in the preceding lemma.

Case 1. Suppose $\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(y)$. It is clear that $[\Delta(y), \boldsymbol{\omega}(y)] = 0$. By Lemma 5.2.1 i), $[\Delta(x), \boldsymbol{\omega}(y)] = 0$. Hence both $[x, z]$ and $[y, z]$ are primitive and we can assume that

$$[x, z] = ax + by,\ \ [y, z] = cx + dy \text{ for some } \ a, b, c, d \in \mathbf{k}.$$

Since $\mathrm{char}\mathbf{k} = p$ and $[x, y] = y$, we have $[x^p, z] = \mathrm{ad}(x)^p(z) = by$. Then $[x, z] = [x^p, z]$ implies that $a = 0$. Replacing z with $z + dx - by$, the commutator relations can be reduced to

$$[x, y] = y,\ \ [x, z] = 0,\ \ [y, z] = cx \text{ for some } \ c \in \mathbf{k}.$$

Applying these relations, it follows that

$$(xy)z = zyx + zy + cx^2 + cx \text{ and } x(yz) = zyx + zy + cx^2.$$

Then, by associativity, we have $c = 0$ or $[y, z] = 0$. Moreover, since $\mathrm{char}\mathbf{k} = p$ and $[y, z] = 0$, we have

$$\Delta(z^p) = \Delta(z)^p = z^p \otimes 1 + 1 \otimes z^p + \boldsymbol{\omega}(y^p) = z^p \otimes 1 + 1 \otimes z^p.$$

Hence z^p is primitive. But $[x, z] = [y, z] = 0$ implies $[x, z^p] = [y, z^p] = 0$, and so $z^p = 0$ by Lemma 5.2.1 iii). This gives (1).

Case 2. Suppose $\Delta(z) = z \otimes 1 + 1 \otimes z + \boldsymbol{\omega}(x)$. It is easy to see that $[x, z]$ is primitive. By Lemma 5.2.1 ii), we have

$$\begin{aligned}
\Delta\Big([y, z] - yf(x)\Big) &= [\Delta(y), \Delta(z)] - \Delta(yf(x)) \\
&= [y, z] \otimes 1 + 1 \otimes [y, z] + [y \otimes 1 + 1 \otimes y, \boldsymbol{\omega}(x)] - \Delta[yf(x)] \\
&= ([y, z] - yf(x)) \otimes 1 + 1 \otimes ([y, z] - yf(x)).
\end{aligned}$$

Hence $[y, z] - yf(x)$ is also primitive. Then we can assume that

$$[x, z] = ax + by,\ \ [y, z] = yf(x) + cx + dy \text{ for some } a, b, c, d \in \mathbf{k}.$$

Similar arguments involving $[x, z] = [x^p, z]$ and the replacement of z with $z + dx - by$ show that the above commutator relations can be reduced to

$$[x, y] = y,\ \ [x, z] = 0,\ \ [y, z] = yf(x) + cx \text{ for some } c \in \mathbf{k}.$$

Applying these relations, we have

$$(xy)z = zyx + zy + yf(x)(x+1) + cx^2 + cx,$$
$$x(yz) = zyx + zy + yf(x)(x+1) + cx.$$

Hence by associativity, $c = 0$ and $[y, z] = yf(x)$. It remains to determine z^p. Again since $\mathrm{char}\mathbf{k} = p$, we have

$$\Delta(z^p) = \Delta(z)^p = z^p \otimes 1 + 1 \otimes z^p + \boldsymbol{\omega}(x^p) = z^p \otimes 1 + 1 \otimes z^p + \boldsymbol{\omega}(x).$$

Thus $z^p - z$ is primitive. Note that

$$[x, z^p - z] = (x)\mathrm{ad}(z)^p - [x, z] = 0,$$
$$[y, z^p - z] = (y)\mathrm{ad}(z)^p - yf(x) = yf(x)^p - yf(x) = 0.$$

Hence $z^p = z$ by Lemma 5.2.1 iii). This gives (2).

Case 3. Suppose $p > 2$ and $\Delta(z) = z \otimes 1 + 1 \otimes z - 2x \otimes y$. Then we have

$$\Delta([x, z]) = [x, z] \otimes 1 + 1 \otimes [x, z] - 2x \otimes y.$$

Hence $[x, z] - z$ can be written as $ax + by$ for some $a, b \in \mathbf{k}$. That is, $[x, z] = z + ax + by$. It follows that $[x^p, z] = \mathrm{ad}(x)^p(z) = z + ax + pby = z + ax$. On the other hand, $[x^p, z] = [x, z] = z + ax + by$. Thus, $b = 0$ and $[x, z] = z + ax$. By a shifting $z + ax$ of z, we can assume that $[x, z] = z$. To determine $[y,\ z]$, we consider $[y, z] - y^2$. It follows from $[x,\ y] = y$ and $\Delta(z) = z \otimes 1 + 1 \otimes z - 2x \otimes y$ that

$$\Delta([y, z] - y^2) = \left([y, z] - y^2\right) \otimes 1 + 1 \otimes \left([y, z] - y^2\right).$$

Then we can write $[y, z] = y^2 + cx + dy$ for some $c, d \in \mathbf{k}$. Applying the three commutators $[x, y] = y$, $[x, z] = z$ and $[y, z] = y^2 + cx + dy$, we have

$$x(yz) = zyx + zy + y^2x + 2y^2 + cx^2 + dyx + dy,$$
$$(xy)z = zyx + zy + y^2x + 2y^2 + cx^2 + dyx + 2cx + 2dy.$$

By associativity, $c = d = 0$, that is, $[y, z] = y^2$.

Next, we determine z^p. Note that $y^p = 0$. By Lemma 2.3.1, we have

$$\Delta(z^p) = (z \otimes 1 + 1 \otimes z - 2x \otimes y)^p = z^p \otimes 1 + 1 \otimes z^p + \sum_{i=1}^{p-1} s_i,$$

where is_i is the coefficient of λ^{i-1} in $(-2x \otimes y)\mathrm{ad}(-2\lambda x \otimes y + z \otimes 1 + 1 \otimes z)^{p-1}$. Set $A_0 = -2x \otimes y$. For $n = 1, 2, \ldots$, denote

$$A_n = [A_{n-1},\ -2\lambda x \otimes y + z \otimes 1 + 1 \otimes z].$$

Then is_i is the coefficient of λ^{i-1} in A_{p-1}. Note that

$$A_1 = [-2x \otimes y,\ -2\lambda x \otimes y + z \otimes 1 + 1 \otimes z] = -2z \otimes y - 2x \otimes y^2.$$

We make the inductive assumption $A_n = a_n z \otimes y^n + b_n x \otimes y^{n+1}$ where $a_n, b_n \in \mathbf{k}[\lambda]$, the polynomial ring in λ over $\mathbf{k}$. Then

$$\begin{aligned} A_{n+1} &= \big[a_n z \otimes y^n + b_n x \otimes y^{n+1},\ -2\lambda x \otimes y + z \otimes 1 + 1 \otimes z\big] \\ &= -2\lambda a_n [z, x] \otimes y^{n+1} + a_n z \otimes [y^n, z] + b_n [x, z] \otimes y^{n+1} + b_n x \otimes [y^{n+1}, z]. \end{aligned}$$

Note that $[y^n, z] = ny^{n+1}$ by $[y, z] = y^2$. Hence

$$A_{n+1} = (2\lambda + na_n + b_n) z \otimes y^{n+1} + (n+1) b_n x \otimes y^{n+2}.$$

That is, $a_{n+1} = 2\lambda + na_n + b_n$ and $b_{n+1} = (n+1)b_n$. Then, combining with the initial condition $a_1 = b_1 = -2$, we have

$$a_{p-1} = \sum_{i=1}^{p-1} c_{i-1} \lambda^{i-1} \text{ for some } c_{i-1} \in \mathbf{k},$$

and

$$A_{p-1} = a_{p-1} z \otimes y^{p-1} = \sum_{i=1}^{p-1} c_{i-1}\, z \otimes y^{p-1} \lambda^{i-1}.$$

Therefore,

$$\Delta(z^p) = z^p \otimes 1 + 1 \otimes z^p + \sum_{i=1}^{p-1} s_i = z^p \otimes 1 + 1 \otimes z^p + \sum_{i=1}^{p-1} \frac{c_{i-1}}{i}\, z \otimes y^{p-1}.$$

Next, we denote $a = \sum_{i=1}^{p-1} c_{i-1}/i$ and show $a = 0$ by coassociativity. Consider

$$\begin{aligned}(\Delta \otimes \mathrm{Id})\,\Delta\,(z^p) =& (\Delta \otimes \mathrm{Id})\,(z^p \otimes 1 + 1 \otimes z^p + az \otimes y^{p-1}) \\ =& \Delta(z^p) \otimes 1 + 1 \otimes 1 \otimes z^p + a\Delta(z) \otimes y^{p-1} \\ =& \Delta(z^p) \otimes 1 + 1 \otimes 1 \otimes z^p + a(z \otimes 1 \otimes y^{p-1} + 1 \otimes z \otimes y^{p-1} - 2x \otimes y \otimes y^{p-1}), \\ (\mathrm{Id} \otimes \Delta)\,\Delta\,(z^p) =& (\mathrm{Id} \otimes \Delta)\,(z^p \otimes 1 + 1 \otimes z^p + az \otimes y^{p-1}) \\ =& z^p \otimes 1 \otimes 1 + 1 \otimes \Delta(z^p) + az \otimes \Delta(y^{p-1}).\end{aligned}$$

Note that neither $1 \otimes \Delta(z^p)$ nor $z \otimes \Delta(y^{p-1})$ contains a term in $x \otimes y \otimes y^{p-1}$. Then $a = 0$ by coassociativity. Hence $\Delta(z^p) = z^p \otimes 1 + 1 \otimes z^p$ and z^p is primitive. Moreover, $[x, z^p] = x(\mathrm{ad}z)^p = 0$ and $[y, z^p] = y(\mathrm{ad}z)^p = p!y^{p+1} = 0$. Thus $z^p = 0$ by Lemma 5.2.1 iii). This gives (3).

■

5.3 When $\mathbf{P}(H)$ is three-dimensional

In this section, assume $\dim K = p^3$, that is, H is primitively generated. It is sufficient to classify all restricted Lie algebras of dimension three. Let $\mathfrak{g}$ be a Lie algebra of dimension three (not necessarily restricted), spanned by x, y, z. The classification of such $\mathfrak{g}$ is well known (see, for example, [45, §3]):

Lemma 5.3.1. *The Lie structure of a three-dimensional Lie algebra over* $\mathbf{k}$*, spanned by* x, y, z*, is one of the following, up to isomorphism.*

1) $[x, y] = [x, z] = [y, z] = 0,$

2) $[x, y] = z, [x, z] = [y, z] = 0,$

3) $[x, y] = z, [x, z] = x, [y, z] = -y,$

4) $[x, y] = y, [x, z] = [y, z] = 0,$

5) $[x, y] = 0, [x, z] = \lambda x, [y, z] = \lambda^{-1} y,$ *for some* $\lambda \in \mathbf{k}^\times$.

Moreover, type 1) is abelian, type 2) is Heisenberg, type 4) and type 5) are both non-semisimple and non-nilpotent, and type 3) is the only simple one.

For the purpose of this section, we are only interested in the restricted Lie algebras of such types. It then remains to determine the p-map structure of $\mathfrak{g}$ (if it exists). The next lemma follows directly from Corollary 2.3.4.

Lemma 5.3.2. *When $\mathfrak{g}$ is abelian, the p-map structure of $\mathfrak{g}$ is one of the following, up to isomorphism.*

(1) $x^p = y, y^p = z, z^p = 0,$

(2) $x^p = 0, y^p = z, z^p = 0,$

(3) $x^p = 0, y^p = 0, z^p = 0,$

(4) $x^p = 0, y^p = 0, z^p = z,$

(5) $x^p = y, y^p = 0, z^p = z,$

(6) $x^p = 0, y^p = y, z^p = z,$

(7) $x^p = x, y^p = y, z^p = z.$

Next, we classify nonabelian restricted Lie algebras of dimension three. In Lemma 5.3.3 and Lemma 5.3.5, to obtain the most simplified p-map structure of $\mathfrak{g}$, we will rescale the generators x, y, z when it is necessary. That is, we will take $x = a\tilde{x}$, $y = b\tilde{y}$, and $z = c\tilde{z}$ for some $a, b, c \in \mathbf{k}^{\times}$ so that $\tilde{x}$, $\tilde{y}$ and $\tilde{z}$ are satisfying the same Lie bracket defining relations of x, y, z. Moreover, some shifting (e.g., $x' = x + uy$, $x' = x + vz$ for some $u, v \in k$) might be necessary too. Once the p-map of $\mathfrak{g}$ is simplified, the restricted Lie algebra $\mathfrak{g}$ will still be represented using x, y, and z, after rescaling or shifting.

Lemma 5.3.3. *If $\mathfrak{g}$ is Heisenberg, then the p-map of $\mathfrak{g}$ is one of the following*

(1) $x^p = 0, y^p = 0, z^p = 0,$

(2) $x^p = 0, y^p = 0, z^p = z$,

(3) $x^p = z, y^p = 0, z^p = 0$.

If $p = 2$, then the p-maps in (1) *and* (3) *are isomorphic. If $p \neq 2$, then there are three different isomorphism classes.*

Proof. As in Lemma 5.3.1 2), the Lie stricture of $\mathfrak{g}$ is given by $[x, y] = z, [x, z] = [y, z] = 0$. It is straight forward to verify that $(\mathrm{ad}x)^p$, $(\mathrm{ad}y)^p$, $(\mathrm{ad}z)^p$ vanish on $\mathfrak{g}$. Then $x^p,\ y^p,\ z^p$ are all in the center of $\mathfrak{g}$. Hence, $x^p = \alpha z$, $y^p = \beta z$ and $z^p = \gamma z$ for some $\alpha, \beta, \gamma \in \mathbf{k}$. The case (1) is obvious if $\alpha = \beta = \gamma = 0$.

When $\alpha = \beta = 0$ and $\gamma \neq 0$, we can assume $\gamma = 1$ by rescaling with the scalars $ab = c$ and $c^{p-1} = \gamma$. This gives (2).

When $\alpha \neq 0$ and $\beta = \gamma = 0$, we can assume that $\alpha = 1$ by rescaling with $ab = c$ and $a^p = \alpha c$. This leads to (3). Due to the symmetry of x and y, the case when $\beta \neq 0$ and $\alpha = \gamma = 0$ gives a restricted Lie algebra isomorphic to the one with the p-map in (3).

When $\alpha \neq 0$, $\beta = 0$ and $\gamma \neq 0$ (or symmetrically $\alpha = 0$, $\beta \neq 0$ and $\gamma \neq 0$), we can assume that $\alpha = 1$, $\beta = 0$ and $\gamma = 1$ by rescaling with $c^{p-1} = \gamma$, $a^p = \alpha c$, and $ab = c$. That is, $x^p = z,\ y^p = 0,\ z^p = z$. Now set $x' = x - z$. Then $(x')^p = (x - z)^p = 0$, $[x', y] = z$, and $[x', z] = 0$. Therefore, these cases also give (2).

The remaining case is when both α and β are nonzero. Set $x' = x + uy$ for some $u \in \mathbf{k}$. Then

$$(x')^p = (x + uy)^p = x^p + u^p y^p + \sum_{i=1}^{p-1} s_i,$$

where is_i is the coefficient of λ^{i-1} in $x[\mathrm{ad}(\lambda x + uy)^{p-1}]$. If $p > 2$, then $(x')^p = x^p + (uy)^p = (\alpha + u^p\beta)z$, since $[x, z] = [y, z] = 0$. We can choose u such that $(x')^p = 0$. If $p = 2$, then $(x')^2 = x^2 + u^2y^2 + [x, x + uy] = (\alpha + u + u^2\beta)z$. Again, we can choose u properly such that $(x')^p = 0$. Note that $[x', y] = z$ and $[x', z] = 0$. This case reduces to one of the previous two cases and does not give any new isomorphism classes with different p-maps.

Lastly, it is clear that the p-map in (2) produces a non-p-nilpotent restricted Lie algebra and so gives a distinct isomorphism class. When $p > 2$, the p-map in (1) is trivial, i.e., any linear combination of x, y, z maps to zero under the p-map. Hence the p-maps in (1) and

(3) give distinct isomorphism classes of $\mathfrak{g}$ for $p > 2$. When $p = 2$, the p-map in (1) is not trivial, since $(x + y)^2 = z$. Then in this case the p-maps in (1) and (3) are isomorphic via the mapping $x \mapsto x + y$, $y \mapsto y$, $z \mapsto z$. This completes the proof. ■

Lemma 5.3.4. *Assume $\mathfrak{g}$ is simple. If $p = 2$, then the p-map does not exist. If $p > 2$, then the p-map is given by $x^p = y^p = 0$, $z^p = z$, up to isomorphism.*

Proof. By Lemma 5.3.1 3), $[x, y] = z, [x, z] = x, [y, z] = -y$. For any $\alpha, \beta, \gamma \in \mathbf{k}$, it holds that $[\alpha x + \beta y + \gamma z, y] = \alpha z + \gamma y$. But $[x^2, y] = (\mathrm{ad}x)^2(y) = [x, [x, y]] = [x, z] = x$. Hence there is no restricted map when $p = 2$. Now assume that $p > 2$. Since $(\mathrm{ad}x)^p$ and $(\mathrm{ad}y)^p$ vanish on $\mathfrak{g}$, we have $x^p = y^p = 0$. Moreover, it follows from $[x, z^p] = x$ and $[y, z^p] = -y$ that $z^p = z$. This completes the proof. ■

Lemma 5.3.5. *If $\mathfrak{g}$ has the Lie structure $[x, y] = y, [x, z] = [y, z] = 0$ in Lemma 5.3.1, 4), then the p-map of $\mathfrak{g}$ is one of the following, up to isomorphism.*

(1) $x^p = x, y^p = 0, z^p = 0,$

(2) $x^p = x, y^p = z, z^p = z,$

(3) $x^p = x, y^p = z, z^p = 0,$

(4) $x^p = x, y^p = 0, z^p = z.$

Proof. Let $w = k_1x + k_2y + k_3z$ be an element of $\mathfrak{g}$ for $k_1, k_2, k_3 \in \mathbf{k}$. Then $[w, x] = -k_2y$, $[w, y] = k_1y$, and $[w, z] = 0$. In particular, the center of $\mathfrak{g}$ is $\mathbf{k}z$. Note that $[x^p, x] = [x^p, z] = 0$, $[x^p, y] = y$, and y^p, z^p are in the center of $\mathfrak{g}$. Then, $x^p = x + \alpha z$, $y^p = \beta z$, and $z^p = \gamma z$ for some $\alpha, \beta, \gamma \in \mathbf{k}$. Consider the shifting $x + vz$, where v is a scalar such that $\alpha + v^p\gamma = v$. Then, $(x + vz)^p = x + vz$, $[x + vz, y] = y$, and $[x + vz, z] = 0$. Thus we can assume that $\alpha =$, i.e., $x^p = x$.

Obviously, $\beta = \gamma = 0$ gives 1). If both β and γ are nonzero, we can assume $\beta = \gamma = 1$ by rescaling with $c^p = \gamma c$ and $b^p = \beta c$. This gives 2). For the remaining two cases, we can assume $\beta = 1$, $\gamma = 0$ or $\beta = 0$, $\gamma = 1$ by rescaling with $b^p = \beta c$ or $c^p = \gamma c$, and so obtain 3) and 4), respectively.

It can be shown as follows that the four p-maps give four distinct isomorphism classes of $\mathfrak{g}$. Note that $[\mathfrak{g},\mathfrak{g}] = \mathbf{k}y$. Then $[\mathfrak{g},\mathfrak{g}]^p = 0$ for (1) and (4) while $[\mathfrak{g},\mathfrak{g}]^p = \mathbf{k}z$ for (2) and (3). Next, $\dim \mathfrak{g}^p = 1$ for (1) but $\dim \mathfrak{g}^p = 2$ for (4). Lastly, (2) produces a restricted Lie algebra with p-nilpotent center but (3) does not. ■

Lemma 5.3.6. *Suppose $\mathfrak{g}$ has the Lie structure $[x,y] = 0, [x,z] = \lambda x, [y,z] = \lambda^{-1}y$, for some $\lambda \in \mathbf{k}^\times$ as in Lemma 5.3.1, 5). If $\mathfrak{g}$ is a restricted Lie algebra, then $\lambda^{p-1} = \pm 1$, and the p-map of $\mathfrak{g}$ is, up to isomorphism,*

$$x^p = 0, y^p = 0, z^p = \lambda^{p-1}z.$$

When $p > 2$, there are $p+1$ isomorphism classes of such restricted Lie algebras. When $p = 2$, there is only one such restricted Lie algebra.

Proof. One can check that the center of $\mathfrak{g}$ is trivial. It is also clear that x^p and y^p are both in the center of $\mathfrak{g}$. Hence, $x^p = y^p = 0$. It follows from the given Lie bracket relation that $[x,\, z^p] = \lambda^p x$, $[y,\, z^p] = \lambda^{-p}y$, $[z^p,\, z] = 0$. Suppose that $z^p = \alpha x + \beta y + \gamma z$ for some $\alpha, \beta, \gamma \in \mathbf{k}$. Then $[x,\, z^p] = \lambda\gamma x$, $[y,\, z^p] = \lambda^{-1}\gamma y$, and $[z, z^p] = -\lambda\alpha x - \lambda^{-1}\beta y$. Hence, $\alpha = \beta = 0$, $\lambda^{p-1} = \gamma = \lambda^{-(p-1)}$, which further implies that $\gamma = \pm 1$.

When $p > 2$, distinguished by the roots of 1 or the roots of -1, there are two types of p-maps producing two classes of restricted Lie algebras. Denote them by $\mathfrak{g}_1(\lambda)$ and $\mathfrak{g}_{-1}(\mu)$, respectively, where $\lambda^{p-1} = 1$ and $\mu^{p-1} = -1$. It is clear that $\mathfrak{g}_1(\lambda) \not\cong \mathfrak{g}_{-1}(\mu)$ for any λ and μ. Due to the symmetry of x and y, we have $\mathfrak{g}_1(\lambda) \cong \mathfrak{g}_1(\lambda')$ if and only if $\lambda' = \lambda^{-1}$ or $\lambda' = \lambda$. The same holds for $\mathfrak{g}_{-1}(\mu)$. Then, for any fixed $p > 2$, there are $p+1$ isomorphism classes for restricted Lie algebras with the given Lie structure. The result for $p = 2$ is clear. ■

Proof of Theorem 1.0.5. The theorem follows from Lemmas 5.3.2-5.3.6. ■

Remark 13. The isomorphism classes in Theorem 1.0.5 are grouped by semisimple, local, and neither. By [35, Theorem 2.3.3] and Corollary 2.3.4, type (1) is the only semisimple one. By Theorem 3.1.4, finite-dimensional primitively generated connected Hopf algebras are local if and only if all primitives are nilpotent. It is clear that types (2)-(6) are the only ones with x, y, z all nilpotent. The remaining types (7)-(16) are neither semisimple nor local.

5.4 Algebra structures of connected Hopf algebra of dimension p^3

According to [13, 24, 51, 63] with respect to algebra structures, up to GK-dimension 4, affine connected Hopf algebras are all isomorphic to universal enveloping algebras. Moreover, D.-G. Wang, J.J. Zhang, and G. Zhuang in [51] studied the algebra structures of connected Hopf algebras over an algebraically closed field of characteristic 0. Under the assumption that when the GK-dimension equals the dimension of the primitive space plus one, it is proved that the algebra structure of Hopf algebra is always isomorphic to some universal enveloping algebra; see [51, Theorem 0.5 or Theorem 2.7].

For finite-dimensional connected Hopf algebras in positive characteristic, we do not expect the similar algebraic property when we replace the universal enveloping algebra by its restricted version. According to Theorem 1.0.1 and Theorem 1.0.2, any connected Hopf algebra of dimension less than p^3 is isomorphic to some restricted enveloping algebra with respect to algebra structures. But when we move to dimension p^3, the isomorphism class (2) in Theorem 1.0.4 gives us a counterexample. For convenience, we denote by A the correpsonding algebra, namely A is the quotient algebra of the $\mathbf{k}$-algebra generated by three variables x, y, z subject to the following relations:

$$[x, y] - y, [x, z], [y, z] - yf(x), x^p - x, y^p, \text{ and } z^p - z, \tag{5.4.1}$$

where $f(x) := \sum_{i=1}^{p-1}(-1)^{i-1}(p-i)^{-1}x^i$. For the sake of the notation, we will sometimes simply write f for the element $f(x)$.

Lemma 5.4.1. *The center of the algebra A is trivial.*

Proof. As stated before, A is the quotient algebra of the free algebra generated by three variables x, y, z subject to the relations (5.4.1). Therefore, by Diamond Lemma [10], A has a basis $\{z^i y^j x^k | 0 \le i, j, k \le p-1\}$. Moreover, we use the lexicographical order on the index set $I = \{(i, j, k) | 0 \le i, j, k \le p-1\}$ defined as $(\alpha_1, \alpha_2, \alpha_3) <_{\text{lex}} (\beta_1, \beta_2, \beta_3)$ if and only if

$$\alpha_1 < \beta_1 \text{ or } (\alpha_1 = \beta_1, \alpha_2 < \beta_2), \text{ or } (\alpha_1 = \beta_1, \alpha_2 = \beta_2, \alpha_3 < \beta_3).$$

Suppose, the element $C = \sum_{\alpha \in I} a_\alpha z^{\alpha_1} y^{\alpha_2} x^{\alpha_3}$ belongs to the center of A. We can check directly the following identities in A inductively:

$$[x, y^n] = ny^n, \tag{5.4.2}$$

$$[y, x^n] = -y\left((x+1)^n - x^n\right), \tag{5.4.3}$$

$$[y, z^n] = \binom{n}{1} z^{n-1} yf + \binom{n}{2} z^{n-2} yf^2 + \cdots + \binom{n}{0} yf^n, \tag{5.4.4}$$

for any integer $n \geq 1$. By using the condition $[x, C] = 0$ and (5.4.2), we have

$$\sum_{\alpha \in I} \alpha_2 a_\alpha z^{\alpha_1} y^{\alpha_2} x^{\alpha_3} = 0.$$

Then $\alpha_2 = 0$ whenever $a_\alpha \neq 0$. So we can assume that $C = \sum_{\alpha \in J} a_\alpha z^{\alpha_1} x^{\alpha_3}$ where J is the index subset of I with the zero middle index. Furthermore the condition $[y, C] = 0$ combining (5.4.3) and (5.4.4) implies that

$$\begin{aligned}
[y, C] =& \sum_{\alpha \in J} a_\alpha [y, z^{\alpha_1}] x^{\alpha_3} + \sum_{\alpha \in J} a_\alpha z^{\alpha_1} [y, x^{\alpha_3}] \\
=& \sum_{\alpha \in J} a_\alpha \left[\binom{\alpha_1}{1} z^{\alpha_1 - 1} yf + \binom{\alpha_1}{2} z^{\alpha_1 - 2} yf^2 + \cdots + \binom{\alpha_1}{0} yf^{\alpha_1} \right] x^{\alpha_3} \\
& - \sum_{\alpha \in J} a_\alpha z^{\alpha_1} \left[\binom{\alpha_3}{1} x^{\alpha_3 - 1} + \binom{\alpha_3}{2} x^{\alpha_3 - 2} + \cdots + \binom{\alpha_3}{0} \right] \\
=& 0.
\end{aligned} \tag{5.4.5}$$

Choose the leading term of C under the lexicographical order and denote it by $az^m x^n$ where $a \neq 0$. From (5.4.5), it is clear that the leading term of $[y, C]$ is $-naz^m x^{n-1}$. Hence we have $n = 0$. Suppose $m \geq 1$. Then we can rewrite C as

$$az^m + bz^{m-1} g(x) + \delta,$$

where $b \in \mathbf{k}$, $g(x)$ is an element of A only in terms of x and δ is the tail term satisfying $\delta <_{\text{lex}} z^{m-1}$. By using (5.4.5) again, we see the leading term of $[y, C]$ now becomes

$$amz^{m-1} yf + bz^{m-1} [y, g(x)] = amz^{m-1} yf - bz^{m-1} y [g(x+1) - g(x)].$$

Since $am \neq 0$, we have

$$f(x) = (b/am)[g(x+1) - g(x)] \tag{5.4.6}$$

in the subalgebra S of A generated by x. It is easy to see that $S = k[x]/(x^p - x)$. We fix a basis $\{1, x, x^2, \cdots, x^{p-1}\}$ for S and write

$$g(x) = a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

for some coefficients $a_i \in \mathbf{k}$. Then by the definition of $f(x)$ in relations (5.4.1), we see that (5.4.6) is impossible since $g(x+1) - g(x)$ does not have the leading term x^{p-1}. We have a contradiction. Then m must be zero and we can further assume that $C = g(x)$. Suppose $g(x)$ is not a constant. Since $\mathbf{k}$ is algebraically closed, $g(x)$ has at least one root $\alpha \in \mathbf{k}$. By (5.4.3) again, we know $[y, g(x)] = -y[g(x+1) - g(x)]$. So $g(x+1) = g(x)$ and $g(x)$ has p-distinct roots $\alpha, \alpha+1, \cdots, \alpha+p-1$. It is a contradiction since $g(x)$ has degree less than p. So $C \in \mathbf{k}$ and the center of A is trivial. ∎

In the following, we point out the Jacobson radical of A and the corresponding associated graded ring, which are easy to check.

Proposition 5.4.2. *The Jacobson radical J_A of A is generated by y and*

$$A/J_A \cong \underbrace{\mathbf{k} \times \mathbf{k} \times \cdots \times \mathbf{k}}_{2p}.$$

Moreover for the associated graded ring of A with respect to J_A-adic filtration, we have

$$\mathrm{gr}_{J_A} A \cong A, \ \textit{for} \ \deg x = \deg z = 0, \deg y = 1.$$

Lemma 5.4.3. *Let $\mathfrak{g}$ be a finite-dimensional restricted Lie algebra over $\mathbf{k}$. If every irreducible restricted representation of $\mathfrak{g}$ is one-dimensional, then $[\mathfrak{g}, \mathfrak{g}]$ is p-nilpotent in $\mathfrak{g}$.*

Proof. Denote by $u(\mathfrak{g})$ the restricted universal enveloping algebra of $\mathfrak{g}$. By its construction, irreducible restricted representations of $\mathfrak{g}$ are in one-to-one correspondence with simple modules over $u(\mathfrak{g})$. Let M be any simple module over $u(\mathfrak{g})$, which is one-dimensional by assumption. Then every element of $\mathfrak{g}$ acts on M by a scalar. Hence $[\mathfrak{g}, \mathfrak{g}]M = 0$, which implies that the commutator $[\mathfrak{g}, \mathfrak{g}]$ annihilates all the simple modules over $u(\mathfrak{g})$. So $[\mathfrak{g}, \mathfrak{g}]$ lies inside the Jacobson radical of $u(\mathfrak{g})$ by definition. Since $u(\mathfrak{g})$ is finite-dimensional, the

Jacobson radical of $u(\mathfrak{g})$ is nilpotent. Thus we have $[\mathfrak{g}, \mathfrak{g}]$ is p-nilpotent after we translate everything back into $\mathfrak{g}$. ■

We are now ready to show that there exists a finite-dimensional connected Hopf algebra in positive characteristic, which as an algebra is not isomorphic to any restricted universal enveloping algebras.

Proposition 5.4.4. *Let* $\mathbf{k}$ *be an algebraically closed field of characteristic* $p > 0$*. As an algebra over* $\mathbf{k}$*,* A *is not isomorphic to any restricted universal enveloping algebras.*

Proof. From the classification of restricted universal enveloping algebras in Theorem 1.0.5, it is clear to see that (1)-(14) all have non-trivial center. Then by Lemma 5.4.1, it suffices to compare A with (15) and (16). Every irreducible representation of A is one-dimensional by Lemma 5.4.2. But in (15), we see that $z \in [\mathfrak{g}, \mathfrak{g}]$, which is not p-nilpotent. Hence A and (15) cannot be isomorphic as algebras by Lemma 5.4.3. For (16), its Jacobson radical is generated by x, y, whose quotient algebra is isomorphic to $\underbrace{\mathbf{k} \times \mathbf{k} \times \cdots \times \mathbf{k}}_{p}$. Again by Lemma 5.4.2, we know A and (16) cannot be isomorphic. This completes the proof. ■

Chapter 6

CONNECTED HOPF ALGEBRAS WITH LARGE ABELIAN PRIMITIVE SPACE

6.1 Main results

The motivation of this chapter is to classify the remaining case in Chapter 5, i.e., p^3-dimensional connected Hopf algebras with abelian primitive space of dimension 2. We will generalize the original problem by studying a larger family of connected Hopf algebras with similar properties. We first give the description of the family as below. Let $\mathscr{H}$ be the set of all finite-dimensional connected Hopf algebras H satisfying

(1) $\dim H = p^{d+1}$ for some $d \geq 1$;

(2) primitive space $\mathrm{P}(H)$ is an abelian restricted Lie algebra of dimension d.

In this chapter, we classify all such Hopf algebras in $\mathscr{H}$. Note that in the above description if we let $d = 2$, it becomes the classification of the remaining case in dimension p^3. We will follow the terminologies discussed in Section 2.5. Our first main result establishes the bijections between some cohomological groups and the extensions of connected Hopf algebras up to equivalence. In particular, part (iii) implies that there exists a natural bijection between the isomorphism classes of Hopf algebras, in which we are interested, and the group orbits in $\mathcal{H}^2(B, A)$ deleting the subgroup $\mathcal{H}^2(\mathfrak{g}, \mathfrak{h})$ regarding restricted Lie algebra extensions.

Theorem 6.1.1. *Let $\mathfrak{h}$ be a finite-dimensional abelian restricted Lie algebra, and $\mathfrak{g}$ be a one-dimensional restricted Lie algebra. Denote by A and B the restricted enveloping algebra of $\mathfrak{h}$ and $\mathfrak{g}$, respectively. Suppose ρ is an algebraic representation of $\mathfrak{g}$ on $\mathfrak{h}$. We have the following* 1-1 *correspondences:*

(i) *View* $\mathfrak{h}$ *as a (left) restricted* $\mathfrak{g}$*-module via* ρ*. Thus,*

$$\{\textit{equivalence classes of restricted Lie algebra extensions of } \mathfrak{h} \textit{ by } \mathfrak{g}\} \longleftrightarrow \left\{\textit{elements of } \mathcal{H}^2(\mathfrak{g},\mathfrak{h})\right\}.$$

(ii) *Fix the type* $T = (\mathfrak{h}, \mathfrak{g}, \rho)$*. Thus,*

$$\{\textit{equivalence classes of Hopf algebra extensions of type } T\} \longleftrightarrow \left\{\textit{elements of } \mathcal{H}^2(B,A)\right\}.$$

(iii) *In* $\mathscr{H}$*,*

$$\{\textit{isomorphism classes of Hopf algebras of type } T\} \longleftrightarrow \left\{\mathrm{Aut}(T)\textit{-orbits in } \mathcal{H}^2(T)\right\}.$$

Next, we try to find all the isomorphism classes in $\mathscr{H}$. We will let the type T vary through all possible types. The best way to think about the scenario, is to construct a functor $\mathrm{p}_{\mathscr{H}}$ from the category of $\mathscr{H}$ to the category $\mathscr{T}$ of all triples $T = (\mathfrak{h}, \mathfrak{g}, \rho)$. For the second category, we do not require $\dim \mathfrak{g} = 1$ in an arbitrary object T. The morphisms between two objects are pairs of restricted Lie algebra maps, which are compatible with the algebraic representations. Therefore, we can have automorphism groups and isomorphism classes in the category $\mathscr{T}$. In particular, all types are considered to be special objects of $\mathscr{T}$ where $\dim \mathfrak{g} = 1$.

Theorem 6.1.2. *Isomorphism classes in* $\mathscr{H}$ *are in* 1-1 *correspondence with elements of the disjoint union*

$$\coprod_T \mathcal{H}^2(T)/\mathrm{Aut}(T),$$

where T *runs through isomorphism classes of all types in* $\mathscr{T}$*.*

In order to prove the main results, we use the following techniques. They will give us the Hopf algebra structures of the extensions in precious theorem. We consider a general construction of finite-dimensional connected Hopf algebras from the data

$$\mathscr{D} = \big(T, z, \chi, \Theta\big),$$

where we choose a triple $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ in $\mathscr{T}$, and let z be a nonzero element of $\mathfrak{g}$. The other ingredients χ and Θ are related to the coalgebra and algebra structures in the construction.

Theorem 6.1.3. *For the constructed $u(\mathscr{D})$, we have*

(i) *$u(\mathscr{D})$ is a connected Hopf algebra of dimension p^{d+n}, where $d = \dim \mathfrak{h}$ and p^n is the dimension of the subalgebra generated by z in $u(\mathfrak{g})$;*

(ii) *the primitive space of $u(\mathscr{D})$ is isomorphic to $\mathfrak{h}$ if and only if $\{[\mathcal{D}_z^i(\chi)]|0 \leq i \leq n-1\}$ are linearly independent in $\mathrm{H}^2(\Omega A)$.*

The next result builds a bridge between the general construction we have and the extensions we try to classify.

Theorem 6.1.4. *Any extension of type T is isomorphic to $u(\mathscr{D})$, for some $\mathscr{D} = (T, z, \chi, \Theta)$.*

Convention 2. Throughout this chapter, let $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ be an object in $\mathscr{T}$. We choose a basis for $\mathfrak{h}$, denoted by $x_1, x_2, \cdots, x_d$, and keep the notations A, B for the restricted enveloping algebras of $\mathfrak{h}$, $\mathfrak{g}$ respectively. Let z be a nonzero element of $\mathfrak{g}$, where the minimal relation among $z, z^p, z^{p^2} \cdots$ is denoted by

$$z^{p^n} + \lambda_{n-1} z^{p^{n-1}} + \cdots \lambda_1 z^p + \lambda_0 z = 0.$$

Except in the next section, we always assume that $\dim \mathfrak{g} = 1$. Therefore, the element z is fixed as a basis for $\mathfrak{g}$. The minimal relation is written as $z^p + \lambda z = 0$ for some $\lambda \in \mathbf{k}$. Note that it also gives the restricted map in $\mathfrak{g}$.

6.2 A general construction

In this section, our aim is to construct a connected Hopf algebra $u(\mathscr{D})$ from the following data

$$\mathscr{D} = \big(T,\ z,\ \chi,\ \Theta\big). \tag{6.2.1}$$

We will first explain all the elements in $\mathscr{D}$. Let $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ and z be described in Convention 2. For the general construction, we do not require that $\dim \mathfrak{g} = 1$.

In order to explain all the other elements χ and Θ in (6.2.1), we need to introduce some new concepts. We use $\mathrm{Hom}_{\mathrm{gr}\mathbb{K}}(\Omega A, \Omega A)$ to denote all the $\mathbb{K}$-linear graded maps from ΩA

to itself. Note that by Proposition 2.5.3, ΩA is a B-module algebra via ρ, where the action commutes with the differentials. Therefore, we can consider ρ_z as a degree zero cochain map from ΩA to itself.

Definition 17. We define three degree zero cochain maps in $\mathrm{Hom}_{\mathrm{gr}\mathbb{K}}(\Omega A, \Omega A)$.

(i) For any element $a = \sum_{(a)} a_1 \otimes a_2 \otimes \cdots \otimes a_n$ in $(A^+)^n$, the *p-th map* $\mathcal{P}$ is given by $\mathcal{P}(a) = \sum_{(a)} a_1^p \otimes a_2^p \otimes \cdots \otimes a_n^p$.

(ii) Inductively, we define $\mathcal{D}_z^0 = \mathrm{Id}$ and $\mathcal{D}_z^m = \mathcal{P} \circ \mathcal{D}_z^{m-1} + \rho_z^{p^m - p^{m-1}} \circ \mathcal{D}_z^{m-1}$ for any $m \geq 1$.

(iii) The *z-operator* on ΩA is given by $\mathbf{\Phi}_z := \mathcal{D}_z^n + \lambda_{n-1}\mathcal{D}_z^{n-1} + \cdots + \lambda_1 \mathcal{D}_z^1 + \lambda_0 \mathcal{D}_z^0$.

The reason why we give the definitions above is from the next lemma, which is important for later use (by abuse of notations, we will also consider $\mathcal{P}, \mathcal{D}_z^m, \mathbf{\Phi}_z$ as maps from $(A^+)^m$ to itself for any integer $m \geq 0$). Let F be the algebra generated by A and an indeterminate x, subject to the relations $[x, x_i] = \rho_z(x_i)$ for all $1 \leq i \leq d$.

Lemma 6.2.1. *Let $f \in A^+ \otimes A^+$. In the tensor algebra $F \otimes F$, we have*

$$(x \otimes 1 + 1 \otimes x + f)^{p^m} = x^{p^m} \otimes 1 + 1 \otimes x^{p^m} + \mathcal{D}_z^m(f),$$

for all $m \geq 0$.

Proof. We will prove the statement by induction on $m \geq 0$. The statement is trivial for $m = 0$. Suppose it is true for $m = n$. Write $X = x \otimes 1 + 1 \otimes x$ and observe that

$$(\mathrm{ad}X^{p^n})^{p-1} = (\mathrm{ad}X)^{p^{n+1}-p^n} = (\mathrm{ad}x \otimes 1 + 1 \otimes \mathrm{ad}x)^{p^{n+1}-p^n} = \rho_z^{p^{n+1}-p^n}.$$

Hence by Lemma 2.3.1 (A is commutative), we have

$$\begin{aligned}
(X+f)^{p^{n+1}} &= [X^{p^n} + \mathcal{D}_z^n(f)]^p \\
&= X^{p^{n+1}} + (\mathcal{D}_z^n(f))^p + (\mathrm{ad}X^{p^n})^{p-1}\mathcal{D}_z^n(f) \\
&= X^{p^{n+1}} + (\mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-p^n} \circ \mathcal{D}_z^n)(f) \\
&= x^{p^{n+1}} \otimes 1 + 1 \otimes x^{p^{n+1}} + \mathcal{D}_z^{n+1}(f).
\end{aligned}$$

Thus, the statement is true for $m = n+1$, and the proof of the induction step is complete. ■

Before we move on to define χ, we list some basic facts regarding those maps we just defined.

Proposition 6.2.2. *The following are true:*

(i) All maps $\mathcal{P}, \mathcal{D}_z^m$ *and* $\mathbf{\Phi}_z$ *commute with the differentials of* ΩA*.*

(ii) $\mathcal{D}_z^m = \mathcal{P} \circ \mathcal{D}_z^{m-1} + \rho_z^{p^m-1}$ *for all* $m \geq 1$*.*

(iii) $\rho_z \circ \mathbf{\Phi}_z = 0$*.*

Proof. (i) We first show that $\mathcal{P}$ commutes with the differential d. Because A is commutative and the comultiplication Δ in A is an algebra map, it follows that $\mathcal{P} \circ \overline{\Delta} = \overline{\Delta} \circ \mathcal{P}$. By the definition of d (see Equation (2.4.1)), we have

$$\begin{aligned}
\mathcal{P} \circ [\sum_{i=0}^{n-1} (-1)^{i+1}\ 1^i \otimes \overline{\Delta} \otimes 1^{n-i-1}] &= \sum_{i=0}^{n-1} (-1)^{i+1}\ 1^i \otimes \mathcal{P} \circ \overline{\Delta} \otimes 1^{n-i-1} \\
&= \sum_{i=0}^{n-1} (-1)^{i+1}\ 1^i \otimes \overline{\Delta} \circ \mathcal{P} \otimes 1^{n-i-1} \\
&= [\sum_{i=0}^{n-1} (-1)^{i+1}\ 1^i \otimes \overline{\Delta} \otimes 1^{n-i-1}] \circ \mathcal{P}.
\end{aligned}$$

This shows that $\mathcal{P} \circ d = d \circ \mathcal{P}$. Next, we prove inductively that $\mathcal{D}_z^m \circ d = d \circ \mathcal{D}_z^m$ for $m \geq 0$. It is true for $m = 0$ by definition. Suppose it holds for $m = n$. By Proposition 2.5.2, we know $\rho_z d = d \rho_z$. Then

$$\begin{aligned}
d \circ \mathcal{D}_z^{n+1} &= d \circ (\mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-p^n} \circ \mathcal{D}_z^n) \\
&= (\mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-p^n} \circ \mathcal{D}_z^n) \circ d \\
&= \mathcal{D}_z^{n+1} \circ d.
\end{aligned}$$

Thus, the induction step is complete. Finally, $\mathbf{\Phi}_z \circ d = d \circ \mathbf{\Phi}_z$ since the z-operator $\mathbf{\Phi}_z$ is a linear combination of $\mathcal{D}_z^m$'s.

(ii) We prove the statement by induction on $m \geq 1$. When $m = 1$, the statement is just the definition. Suppose it is true for $m = n$. In characteristic p, it is clear that any derivation vanishes on A^p, which implies that $\rho_z \circ \mathcal{P} = 0$. Thus

$$\begin{aligned}\mathcal{D}_z^{n+1} &= \mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-p^n} \circ \mathcal{D}_z^n \\ &= \mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-p^n} \circ (\mathcal{P} \circ \mathcal{D}_z^{n-1} + \rho_z^{p^n-1}) \\ &= \mathcal{P} \circ \mathcal{D}_z^n + \rho_z^{p^{n+1}-1}.\end{aligned}$$

Then, the statement is true for $m = n+1$, and it completes the induction step.

(iii) By definition and (ii), we have

$$\begin{aligned}\rho_z \circ \mathbf{\Phi}_z &= \rho_z \circ (\mathcal{D}_z^n + \cdots + \lambda_1 \mathcal{D}_z^1 + \lambda_0 \mathcal{D}_z^0) \\ &= \rho_z \circ \left(\mathcal{P} \circ \mathcal{D}_z^{n-1} + \cdots + \lambda_1 \mathcal{P} \circ \mathcal{D}_z^0\right) + \rho_z(\rho_z^{p^n-1} + \cdots + \lambda_1\ \rho_z^{p-1} + \lambda_0) \\ &= \ (\rho_z)^{p^n} + \lambda_{n-1} \, (\rho_z)^{p^{n-1}} + \cdots + \lambda_1 \, (\rho_z)^p + \lambda_0 \rho_z \\ &= \rho_{\left(z^{p^n} + \lambda_{n-1} z^{p^{n-1}} + \cdots + \lambda_1 z^p + \lambda_0 z\right)} \\ &= 0.\end{aligned}$$

This concludes the proof. ■

By Proposition 6.2.2(i), we can view $\mathbf{\Phi}_z$ as a map from $\mathrm{H}^\bullet(\Omega A)$ to itself preserving the degree. Now, we are able to give the description of χ in (6.2.1).

Definition 18. Let $\chi \in A^+ \otimes A^+$. We say that χ is a *z-cocycle* if

(i) $\chi \in \mathrm{Z}^2(\Omega A)$,

(ii) $\mathbf{\Phi}_z(\chi) \in \mathrm{B}^2(\Omega A)$.

We say any cohomology class $\xi \in \mathrm{H}^2(\Omega A)$ is *z-characteristic* if $\mathbf{\Phi}_z(\xi) = 0$. It is clear that χ is a z-cocycle if and only if $[\chi]$ is z-characteristic in $\mathrm{H}^2(\Omega A)$.

In the data $\mathscr{D}$ of (6.2.1), we let $\chi \in (A^+)^2$ be a z-cocycle, and $\Theta \in A^+$ satisfying

$$\mathbf{\Phi}_z(\chi) = d^1(\Theta), \quad \rho_z(\Theta) = 0. \tag{6.2.2}$$

We construct the connected Hopf algebra $u(\mathscr{D})$ explicitly. As an algebra, it is generated by A, that is, by x_i's satisfying the relations in the restricted enveloping algebra, and an indeterminate x, subject to the relations

$$\begin{aligned} [x, x_i] &= \rho_z(x_i), \text{ for all } 1 \leq i \leq d, \\ x^{p^n} + \lambda_{n-1} x^{p^{n-1}} &+ \cdots + \lambda_1 x^p + \lambda_0 x + \Theta = 0. \end{aligned} \tag{6.2.3}$$

The coalgebra structure is given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \chi, \quad \Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i, \tag{6.2.4}$$

for all $1 \leq i \leq d$.

In order to prove Theorem 6.1.3, we first show a PBW Theorem for $u(\mathscr{D})$. This will also cover the dimensionality in statement (i).

Lemma 6.2.3. *The following set is a basis for* $u(\mathscr{D})$*:*

$$\left\{ x_1^{\sigma_1} \; x_2^{\sigma_2} \; \cdots \; x_d^{\sigma_d} \; x^{\sigma_{d+1}} \;\middle|\; 0 \leq \sigma_1, \cdots, \sigma_d \leq p-1, \; 0 \leq \sigma_{d+1} \leq p^n - 1 \right\}.$$

Proof. By the construction above, it is clear that, as an algebra, $u(\mathscr{D})$ is isomorphic to the quotient algebra $\mathbf{k}\langle x_1, x_2, \cdots, x_d, x\rangle / I$, where the relation I is generated by

$$\begin{aligned} x_j x_i &= x_i x_j, \text{ for } 1 \leq i < j \leq d, \\ x_i^p &= \sum_{j=1}^{d} a_{ij} x_j, \text{ for } 1 \leq i \leq d, \\ x x_i &= x_i x + \rho_z(x_i), \text{ for } 1 \leq i \leq d, \\ x^{p^n} &= -\sum_{i=0}^{n-1} \lambda_i x^{p^i} - \Theta. \end{aligned}$$

The coefficients a_{ij} above are determined by the restricted map on $\mathfrak{h}$. Therefore, we can find all the possible ambiguities as below.

$$(x_k x_j)\, x_i = x_k\, (x_j x_i)\,,\ \text{for } 1 \le i < j < \mathbf{k} \le d, \tag{a}$$

$$x_j(x_i^p) = (x_j x_i)\, x_i^{p-1},\ \text{for } 1 \le i \le j \le d, \tag{b}$$

$$x(x_j x_i) = (x x_j)\, x_i,\ \text{for } 1 \le i < j \le d, \tag{c}$$

$$x(x_i^p) = (x x_i)\, x_i^{p-1}, \tag{d}$$

$$x(x^{p^n}) = \left(x^2\right) x^{p^n-1}, \tag{e}$$

$$(x^{p^n})x_i = x^{p^n-1}(x x_i). \tag{f}$$

It is easy to check that ambiguities $(a), (b)$ and (c) are resolvable. For (d), by Definition 14, we have

$$x\,(x_i^p) = x(\sum_{j=1}^{d} a_{ij}x_j) = (\sum_{j=1}^{d} a_{ij}x_j)x + \rho_z(\sum_{j=1}^{d} a_{ij}x_j) = (\sum_{j=1}^{d} a_{ij}x_j)x + \rho_z\,(a_i^p) = (\sum_{j=1}^{d} a_{ij}x_j)x.$$

On the other hand,

$$(x x_i)x_i^{p-1} = x_i(x x_i^{p-1}) + \rho_z(x_i)x_i^{p-1} = \cdots = (x_i^p)x + p[\rho_z(x_i)x_i^{p-1}] = (\sum_{j=1}^{d} a_{ij}x_j)x.$$

Hence, it is resolvable. For ambiguity (e), by the condition (6.2.2), we have

$$\begin{aligned} x(x^{p^n}) &= x(-\sum_{i=0}^{n-1} \lambda_i\ x^{p^i} - \Theta) = (-\sum_{i=0}^{n-1} \lambda_i\ x^{p^i} - \Theta)x - \rho_z(\Theta) \\ &= (-\sum_{i=0}^{n-1} \lambda_i\ x^{p^i} - \Theta)x. \end{aligned}$$

On the other hand,

$$(x^2)x^{p^n-1} = (x^{p^n})x = (-\sum_{i=0}^{n-1} \lambda_i\ x^{p^i} - \Theta)x.$$

Thus, it is resolvable. Finally, we turn to the last ambiguity (f). By induction, it is easy to show that $x^{s-1}\,(x x_i) = \sum_{j=0}^{s} \binom{s}{j}\ \rho_z^j(x_i)\ x^{s-j}$, for all $s \ge 1$. Hence,

$$x^{p^n-1}(x x_i) = x_i(x^{p^n}) + \rho_z^{p^n}(x_i) = x_i(-\sum_{i=0}^{n-1} \lambda_i\ x^{p^i} - \Theta) + \rho_z^{p^n}(x_i).$$

On the other hand,

$$(x^{p^n})x_i = (-\sum_{i=0}^{n-1}\lambda_i\ x^{p^i} - \Theta)x_i = x_i(-\sum_{i=0}^{n-1}\lambda_i\ x^{p^i} - \Theta) - \sum_{i=0}^{n-1}\lambda_i\ \rho_z^{p^i}(x_i)$$
$$= x_i(-\sum_{i=0}^{n-1}\lambda_i\ x^{p^i} - \Theta) + \rho_{(-\sum_{i=0}^{n-1}\lambda_i z^{p^i})}(x_i) = x_i(-\sum_{i=0}^{n-1}\lambda_i\ x^{p^i} - \Theta) + \rho_z^{p^n}(x_i)\,.$$

Therefore, it is resolvable, and the result follows from the Diamond Lemma [10]. ■

Proof of Theorem 6.1.3. (i) It remains to show that $u(\mathscr{D})$ is a connected Hopf algebra. Firstly, we prove that it is a bialgebra. Denote by F the algebra generated by A and x, subject to the relations $[x, x_i] = \rho_z(x_i)$, for all $1 \le i \le d$. Suppose the comultiplication is defined on the generators of F by Equation (6.2.4). Since

$$\begin{aligned}\Delta([x, x_i] - \rho_z(x_i)) &= [\Delta(x), \Delta(x_i)] - \Delta(\rho_z(x_i)) \\ &= [x\otimes 1 + 1\otimes x + \chi,\ x_i\otimes 1 + 1\otimes x_i] - \rho_z(x_i)\otimes 1 - 1\otimes \rho_z(x_i) \\ &= \{[x, x_i] - \rho_z(x_i)\}\otimes 1 + 1\otimes\{[x, x_i] - \rho_z(x_i)\},\end{aligned}$$

it follows that Δ extends to an algebra map from F to $F\otimes F$. Regarding the coassociativity, since all x_i's are primitive, and

$$(1\otimes\Delta)\Delta(x) - (\Delta\otimes 1)\Delta(x) = 1\otimes\chi - (\Delta\otimes 1)(\chi) + (1\otimes\Delta)(\chi) - \chi\otimes 1 = d^2(\chi) = 0,$$

we know it holds for the generators, hence it is true for all F. Moreover, we define $\epsilon(x) = \epsilon(x_i) = 0$, for all $1 \le i \le d$. Then, it is direct to check that ϵ is the counit, and $(F, m, u, \Delta, \epsilon)$ becomes a bialgebra.

Next, we denote $X = x^{p^n} + \lambda_{n-1}x^{p^{n-1}} + \cdots + \lambda_0 x + \Theta$ as an element in F. Because $u(\mathscr{D}) \simeq F/(X)$, in order to show that $u(\mathscr{D})$ is a bialgebra, it suffices to show that (X) is a bi-ideal in F. According to Lemma 6.2.1, we have

$$\Delta(x^{p^s}) = (x\otimes 1 + 1\otimes x + \chi)^{p^s} = x^{p^s}\otimes 1 + 1\otimes x^{p^s} + \mathcal{D}_z^s(\chi),$$

for all $s \ge 0$. Thus

$$\begin{aligned}\Delta(X) &= X\otimes 1 + 1\otimes X + [\mathcal{D}_z^n(\chi) + \lambda_{n-1}\mathcal{D}_z^{n-1}(\chi) + \cdots + \lambda_0\chi] + [\Delta(\Theta) - \Theta\otimes 1 - 1\otimes\Theta] \\ &= X\otimes 1 + 1\otimes X + \mathbf{\Phi}_z(\chi) - d^1(\Theta) \\ &= X\otimes 1 + 1\otimes X.\end{aligned}$$

The last equality comes from (6.2.2). Also, it is easy to see that $\epsilon(X) = 0$ since $\Theta \in A^+$, which gives the conclusion.

Secondly, we prove that $u(\mathscr{D})$, as a coalgebra, is connected , thus the antipode exists automatically [47, Lemma 14]. Choose an integer $s \geq 1$ such that $\chi \in \sum_{0\leq i\leq s} A_i \otimes A_{s-i}$, where $\{A_i\}$ denotes the coradical filtration of A. By Lemma 6.2.3, we can define an exhausted filtration of $u(\mathscr{D})$, whose m-th term $u(\mathscr{D})_m$ is spanned by

$$\{x_1^{\sigma_1}\ x_2^{\sigma_2}\ \cdots\ x_d^{\sigma_d}\ x^{\sigma_{d+1}}\ \big|\ \sigma_1 + \cdots + \sigma_d + s\sigma_{d+1} \leq m\}.$$

By the relations (6.2.3), it is definitely an algebra filtration. Furthermore, by [35, Proposition 5.5.3], it is clear that $A_m \subseteq u(\mathscr{D})_m$ for all $m \geq 0$. Hence

$$\Delta(x) \in \sum_{i=0}^{s} u(\mathscr{D})_i \otimes u(\mathscr{D})_{s-i}.$$

Then, direct computation shows that it is also a coalgebra filtration. Note that $u(\mathscr{D})_0 = \mathbf{k}$, and the result follows from [35, Lemma 5.3.4].

(ii) In order to find all the primitives in $u(\mathscr{D})$, we need the following lemma.

Lemma 6.2.4. *Let $a \in u(\mathscr{D})$. Thus, $\Delta(a) - a \otimes 1 - 1 \otimes a \in A \otimes A$ if and only if $a \in A + \sum_{i=0}^{n-1} \mathbf{k}x^{p^i}$.*

Proof. By Lemma 6.2.3, we can view $u(\mathscr{D})$ as a free left A-module equipped with the basis $\{x^i | 0 \leq i \leq p^n - 1\}$. Hence, we can write every element $a \in u(\mathscr{D})$ as

$$a = \sum_{i=0}^{p^n-1} a_i x^i, \tag{6.2.5}$$

for some $a_i \in A$ in a unique way. Moreover, the tensor algebra $u(\mathscr{D}) \otimes u(\mathscr{D})$ becomes a free left $A \otimes A$-module with the basis $\{x^i \otimes x^j | 0 \leq i, j \leq p^n - 1\}$. According to Lemma 6.2.1, we know

$$\Delta(a_i x^{p^i}) = \Delta(a_i)(x^{p^i} \otimes 1 + 1 \otimes x^{p^i} + b_i),$$

for some $b_i \in A \otimes A$ when $0 \leq i \leq n-1$. Now, one direction of the proof is clear, and we will prove the other direction.

Define the index set $S = \{1, 2, \cdots, p^n - 1\} \setminus \{1, p, \cdots, p^{n-1}\}$. Firstly, we show that $a_i = 0$, whenever $i \in S$, by contradiction. The contradiction is obtained by looking at the coefficient of the possible highest term in $\Delta(a) - a \otimes 1 - 1 \otimes a$. Suppose it is not true. Then, we can find the maximal index $m \in S$ such that $a_m \neq 0$. By definition, we can write $m = p^t l$, where $l > 1$ and $l \not\equiv 0 \pmod{p}$. Hence, by [29, Lemma 5.1], $\binom{m}{p^t} \equiv l \pmod{p}$. Note that in $\Delta(a) - a \otimes 1 - 1 \otimes a$, the coefficient for $\boldsymbol{\omega}^{p^t} \otimes \boldsymbol{\omega}^{m-p^t}$ is $l\Delta(a_m) = 0$. Since A is counital, we have $a_m = 0$. This implies a contradiction.

Secondly, since $a_s = 0$ for all $s \in S$, Equation (6.2.5) can be simplified as

$$a = a_0 + \sum_{i=0}^{n-1} a_{p^i} x^{p^i}.$$

It remains to show that all $a_{p^i} \in \mathbf{k}$. By Lemma 6.2.1, it is easy to see that the term $x^{p^i} \otimes 1$ in $\Delta(a) - a \otimes 1 - 1 \otimes a$ has coefficient $\Delta(a_{p^i}) - a_{p^i} \otimes 1$. Again, since A is counital, we have $a_{p^i} \in \mathbf{k}$. This completes the proof. ■

We continue our proof for (ii). Let a be a primitive element in $u(\mathscr{D})$. By Lemma 6.2.4, we can write

$$a = \sum_{(\sigma)} \mu_\sigma x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_d^{\sigma_d} + \sum_{i=0}^{n-1} \mu_i x^{p^i},$$

for some coefficients in $\mathbf{k}$. Note that

$$d^1(x^{p^i}) = x^{p^i} \otimes 1 + 1 \otimes x^{p^i} - \Delta(x^{p^i}) = x^{p^i} \otimes 1 + 1 \otimes x^{p^i} - (x \otimes 1 + 1 \otimes x + \chi)^{p^i} = -\mathcal{D}_z^i(\chi)$$

by Lemma 6.2.1. Since $d^1(a) = 0$, we have

$$d^1(\sum_{(\sigma)} \mu_\sigma x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_d^{\sigma_d}) = -\sum_{i=0}^{n-1} \mu_i d^1(x^{p^i}) = \sum_{i=0}^{n-1} \mu_i \mathcal{D}_z^i(\chi).$$

Hence, if we pass to the homology $\mathrm{H}^2(\Omega A)$, we have

$$\sum_{i=0}^{n-1} \mu_i [\mathcal{D}_z^i(\chi)] = 0. \tag{6.2.6}$$

For one direction, suppose $\{[\mathcal{D}_z^i(\chi)] | 0 \leq i \leq n-1\}$ are linearly independent in $\mathrm{H}^2(\Omega A)$. By Equation (6.2.6), we have all $\mu_i = 0$. Hence, $a \in A$, which yields that the primitive space of $u(\mathscr{D})$ is equal to $\mathrm{P}(A) \simeq \mathfrak{h}$. On the other hand, suppose they are linearly dependent in $\mathrm{H}^2(\Omega A)$. Thus, there are coefficients $\mu_i \in \mathbf{k}$, not all zero, such that $\sum_{i=0}^{n-1} \mu_i \mathcal{D}_z^i(\chi) = d^1(b)$ for some element $b \in A^+$. Direct computation shows that $\sum_{i=0}^{n-1} \mu_i x^{p^i} + b$ is primitive, which is certainly not in A. This shows the other direction, and completes the proof.

■

6.3 Extensions of connected Hopf algebras

In this section, we classify up to equivalence the following short exact sequence of finite-dimensional connected Hopf algebras

$$1 \longrightarrow u(\mathfrak{h}) \xrightarrow{\iota} H \xrightarrow{\pi} u(\mathfrak{g}) \longrightarrow 1, \tag{6.3.1}$$

by an abelian group. We keep the notations in Convention 2, where $\mathfrak{h}$ is finite abelian and $\dim \mathfrak{g} = 1$ with basis z satisfying $z^p + \lambda z = 0$. We recall some basic facts regarding extensions.

Definition 19. A sequence of Hopf algebras

$$1 \longrightarrow A \xrightarrow{\iota} C \xrightarrow{\pi} B \longrightarrow 1,$$

where 1 denotes the Hopf algebra $\mathbf{k}$, is *exact* if [2, Proposition 1.2.3]

(i) ι is injective. Identify then A with its image,

(ii) π is surjective,

(iii) $\pi\iota = \epsilon$,

(iv) $\ker \pi = CA^+$,

(v) $A = \{x \in C : (\pi \otimes \mathrm{Id})\Delta(x) = 1 \otimes x\}$.

We also say that C is an *extension* of A by B, and two extensions C, C' are *equivalent* if we have an isomorphism $\vartheta : C \to C'$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & C & \xrightarrow{\pi} & B & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle\vartheta} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota'} & C' & \xrightarrow{\pi'} & B & \longrightarrow & 1. \end{array} \tag{6.3.2}$$

By [32, Lemma-Definition 1.1], in finite-dimensional case, sequence (6.3.1) is exact if and only if

(i) $u(\mathfrak{h})$ is a normal Hopf subalgebra of H via the injection ι (in finite-dimensional case, A is a normal Hopf subalgebra of H if $A^+H = HA^+$),

(ii) $H/u(\mathfrak{h})^+H \simeq u(\mathfrak{g})$ via the projection π.

Moreover, we have $\dim H = \dim u(\mathfrak{h}) \dim u(\mathfrak{g}) = p^{\dim \mathfrak{h} + \dim \mathfrak{g}}$ by [41, p. 290].

If H is primitively generated in sequence (6.3.1), we have a short exact sequence of restricted Lie algebras.

$$1 \longrightarrow \mathfrak{h} \xrightarrow{\iota} \mathrm{P}(H) \xrightarrow{\pi} \mathfrak{g} \longrightarrow 1.$$

Choose some element x in $\mathrm{P}(H)$ satisfying $\pi(x) = z$. Since $\dim \mathfrak{g} = 1$, it suffices to define the representation ρ of $\mathfrak{g}$ on $\mathfrak{h}$ by giving its value on z. Let $\rho_z(h) = [x, h]$ for any $h \in \mathfrak{h}$. Since $\mathfrak{h}$ is abelian, the value $\rho_z(h)$ is independent of the choice of x. Moreover, it is easy to see that ρ is indeed an algebraic representation of $\mathfrak{g}$ on $\mathfrak{h}$.

Remark 14. In particular, when $\mathfrak{h}$ is p-nilpotent, we know $\mathfrak{h}$ is a restricted $\mathfrak{g}$-module via ρ in the sense of [60, Exercise 7.6.4]. Hence, equivalence classes of extensions of $\mathfrak{h}$ by $\mathfrak{g}$ are in 1-1 correspondence with elements in the second Hochschild cohomology of $\mathfrak{g}$ with coefficients in $\mathfrak{h}$ [60, Definition 7.2.2].

More generally, for any extension H described in sequence (6.3.1), we can define a type $T = (\mathfrak{h}, \mathfrak{g}, \rho) \in \mathscr{T}$, which is invariant under the equivalence of extensions. Identify $A = u(\mathfrak{h})$ with its image in H via ι. Let $n \geq 1$ be the minimal integer such that $A_n \subsetneq H_n$

(see Definition 9(2)). Note that H induces an extension for their associated graded Hopf algebras Definition 7:

$$1 \longrightarrow \mathrm{gr}A \longrightarrow \mathrm{gr}H \longrightarrow \mathrm{gr}B \longrightarrow 1.$$

By Theorem **??**, we know gr$A$ is isomorphic to

$$\mathbf{k}[\overline{x_1}, \overline{x_2}, \cdots, \overline{x_d}]/[\overline{x_1}^p, \overline{x_2}^p, \cdots, \overline{x_d}^p),$$

as algebras, and gr$H \simeq$ gr$A[\overline{x}]/(\overline{x}^p)$, where $x \in H_n \setminus A_n$. Moreover, through the projection π, we have natural isomorphisms

$$H_n/A_n \simeq \mathfrak{g} \simeq \mathrm{P}(H/A^+H)$$

as one-dimensional vector spaces (see Lemma 2.2.1). As a consequence, we can choose $x \in H_n \setminus A_n$ satisfying $x \in H^+$ and $\pi(x) = z$. We define the representation ρ associated to the extension H by $\rho_z(h) = [x, h]$ for all $h \in \mathfrak{h}$. It is clear that the definition is independent of the choice of x since $\mathfrak{h}$ is abelian.

Proposition 6.3.1. *The representation ρ is an algebraic representation of $\mathfrak{g}$ on $\mathfrak{h}$.*

Proof. Firstly, we show that ρ is well-defined. We know $H_{n-1} = A_{n-1}$ by the choice of n. Then by [35, Lemma 5.3.2], we have

$$\Delta(x) - x \otimes 1 - 1 \otimes x \in H_{n-1} \otimes H_{n-1} = A_{n-1} \otimes A_{n-1} \subseteq A \otimes A.$$

So we can write $\Delta(x) = x \otimes 1 + 1 \otimes x + \chi$ for some $\chi \in A^+ \otimes A^+$. For any $h \in \mathfrak{h}$, direct computation shows that $[x, h]$ is primitive. Thus, by Lemma 2.2.2, we have $[x, h] \in \mathrm{P}(H) \cap A = \mathfrak{h}$ since A is normal. It proves that $\rho_z \in \mathrm{End}_k(\mathfrak{h})$.

Secondly, by Theorem 2.2.5, we have relation $x^p + \sigma x + \Theta = 0$ for some $\sigma \in \mathbf{k}$ and $\Theta \in A^+$. Thus, $\pi(x^p + \sigma x + \Theta) = z^p + \sigma z = 0$, which yields that $\sigma = \lambda$. In Definition 14, (i) is trivial and (iii), (iv) come from the fact that $\rho_z = \mathrm{ad}x \in \mathrm{Der}(A)$. For (ii), we have

$$(\rho_z)^p(h) = (\mathrm{ad}x)^p(h) = [x^p, h] = [-\lambda x - \Theta, h] = [-\lambda x, h] = \rho_{(-\lambda z)}(x) = \rho_{(z^p)}(h).$$

This proves that ρ is an algebraic representation of $\mathfrak{g}$ on $\mathfrak{h}$, which completes the proof. ∎

The fact that ρ is invariant under the equivalence of extensions is implied by the following lemma, which is also used in the next section.

Lemma 6.3.2. *In the commutative diagram below*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & u(\mathfrak{h}) & \xrightarrow{\iota} & H & \xrightarrow{\pi} & u(\mathfrak{g}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\vartheta} & & \downarrow{\scriptstyle\psi} & & \\ 1 & \longrightarrow & u(\mathfrak{h}') & \xrightarrow{\iota'} & H' & \xrightarrow{\pi'} & u(\mathfrak{g}') & \longrightarrow & 1, \end{array}$$

suppose both rows are exact satisfying $\dim \mathfrak{g} = \dim \mathfrak{g}' = 1$. *Moreover, let ρ and ρ' be the corresponding algebraic representations. Thus, (ϕ, ψ), when restricted to their primitive spaces, is a morphism from $(\mathfrak{h}, \mathfrak{g}, \rho)$ to $(\mathfrak{h}', \mathfrak{g}', \rho')$ in $\mathscr{T}$.*

Proof. If ψ is zero, then there is nothing to prove. In the remaining, suppose $\psi \neq 0$. Let n be the minimal integer such that $A_n \subsetneq H_n$. Following the definition of the algebraic representation ρ in the top row, we choose some $x \in H_n \setminus A_n$ such that $x \in H^+$ and $\pi(x) = z$. Thus, $\rho_z(h) = [x, h]$ for any $h \in \mathfrak{g}$.

Now, we turn to the second row. Denote $z' = \psi(z)$, which is nonzero since $\dim \mathfrak{g} = 1$ and $\psi \neq 0$. Similarly, we define A' and the integer n' regarding $A' \subseteq H'$. Note that the commutative diagram in the statement yields another commutative diagram with respect to their associated graded Hopf algebras. Hence, we have, by abuse of the notations for π, ϑ, etc., the following commutative square

$$\begin{array}{ccc} H_n/A_n & \xrightarrow{\pi} & \mathfrak{g} \\ \downarrow{\scriptstyle\vartheta} & & \downarrow{\scriptstyle\psi} \\ H'_{n'}/A'_{n'} & \xrightarrow{\pi'} & \mathfrak{g}'. \end{array}$$

If we denote $x' = \vartheta(x)$, then we know $x' \in H'_{n'} \setminus A'_{n'}$ and $\pi'(x') = z'$. Still by definition, we have $\rho_{z'}(h') = [x', h']$ for any $h' \in \mathfrak{h}$. Since $\dim \mathfrak{g} = 1$, it suffices to check the Diagram (2.5.1) commutes for $z \in \mathfrak{g}$ and any $h \in \mathfrak{h}$, which is clear from the above setup. This completes the proof. ■

Given any short exact sequence in (6.3.1), then we have a type T in $\mathscr{T}$, which is called the type of the extension H. Now, we fix the type $T = (\mathfrak{g}, \mathfrak{h}, \rho)$. We want to classify all extensions of type T. Recall that the z-operator is given by

$$\mathbf{\Phi}_z = \mathcal{D}_z^1 + \lambda\mathcal{D}_z^0 = \mathcal{P} + \lambda \circ \mathrm{Id} + \rho_z^{p-1}.$$

Let H be any extension of type T. Summarize the results we have known so far. There exists some $x \in H^+ \setminus A$ satisfying that

(i) $\Delta(x) = 1 \otimes x + 1 \otimes x + \chi$, for some $\chi \in A^+ \otimes A^+$.

(ii) $\pi(x) = z$ and $x^p + \lambda x + \Theta = 0$, for some $\Theta \in A^+$.

(iii) $[x, x_i] = \rho_z(x_i)$, for all $1 \leq i \leq d$.

Moreover,

Lemma 6.3.3. *We know χ is a z-cocycle satisfying $\mathbf{\Phi}_z(\chi) = d^1(\Theta)$ and $\rho_z(\Theta) = 0$.*

Proof. We first show that χ is a cocycle. By the coassociativity of Δ, we have $(1\otimes\Delta)\Delta(z) = (\Delta \otimes 1)\Delta(z)$. Direct computation yields that $1 \otimes \chi + (1 \otimes \Delta)(\chi) = (\Delta \otimes 1)(\chi) + \chi \otimes 1$. By writing $\chi = \sum_{(\chi)} \chi_1 \otimes \chi_2 \in A^+ \otimes A^+$, we have

$$\begin{aligned} d^2(\chi) = & -(\overline{\Delta} \otimes 1)(\chi) + (1 \otimes \overline{\Delta})(\chi) \\ = & -(\Delta \otimes 1)(\chi) + \sum(1 \otimes \chi_1 + \chi_1 \otimes 1) \otimes \chi_2 + (1 \otimes \Delta)(\chi) - \sum \chi_1 \otimes (\chi_2 \otimes 1 + 1 \otimes \chi_2) \\ = & -(\Delta \otimes 1)(\chi) + 1 \otimes \chi + (1 \otimes \Delta)(\chi) - \chi \otimes 1 \\ = & \, 0. \end{aligned}$$

Hence, $\chi \in \mathrm{Z}^2(\Omega A)$. Moreover, by Lemma 6.2.1, we have

$$\begin{aligned} \Delta(x^p + \lambda x + \Theta) &= (x \otimes 1 + x \otimes 1 + \chi)^p + \lambda(x \otimes 1 + 1 \otimes x + \chi) + \Delta(\Theta) \\ &= (x^p + \lambda x) \otimes 1 + 1 \otimes (x^p + \lambda x) + [\mathcal{D}_z^1(\chi) + \lambda\chi] + \Delta(\Theta) \\ &= -\Theta \otimes 1 - 1 \otimes \Theta + \mathbf{\Phi}_z(\chi) + \Delta(\Theta) \\ &= \mathbf{\Phi}_z(\chi) - d^1(\Theta). \end{aligned}$$

The last equality comes from the definition $d^1(\Theta) = -\overline{\Delta}(\Theta)$. So we have $\mathbf{\Phi}_z(\chi) = d^1(\Theta)$. Moreover, by Summary (ii) and (iii), we have

$$\rho_z(\Theta) = [x, \Theta] = [x, -x^p - \lambda x] = 0.$$

This completes the proof. ■

Proof of Theorem 6.1.4. In the data $\mathscr{D}$, let χ and Θ be as in the summary (i) and (ii). Note that the data $\mathscr{D}$ is well-defined by previous lemma. Moreover, in sequence (6.3.1), we have $\dim H = p^{\dim \mathfrak{h} + \dim \mathfrak{g}} = p^{d+1}$. Hence, the isomorphism comes from the construction of $u(\mathscr{D})$ and the degree argument (see Lemma 6.2.3). This completes the proof. ■

We will define a cohomological type group $\mathcal{H}^2(B, A)$, which classifies all the extensions of type T up to equivalence.

Definition 20. In the set $Z^2(\Omega A) \times A^+$, we define

(i) a subset $\mathcal{E}^2(B, A)$, where (χ, Θ) belongs to $\mathcal{E}^2(B, A)$ if

$$\mathbf{\Phi}_z(\chi) = d^1(\Theta), \quad \rho_z(\Theta) = 0;$$

(ii) an equivalence relation $\sim$, where $(\chi, \Theta) \sim (\chi', \Theta')$ if there exists some $a \in A^+$ such that

$$d^1(a) = \chi - \chi', \quad \mathbf{\Phi}_z(a) = \Theta - \Theta'.$$

Since the differential d^1 and the z-operator $\mathbf{\Phi}_z$ are $\mathbb{K}$-linear, and vanishing on zero, it follows that the equivalence relation is well-defined in the set $Z^2(\Omega A) \times A^+$. Moreover, $Z^2(\Omega A) \times A^+$ becomes an abelian group via $(\chi, \Theta) + (\chi', \Theta') = (\chi + \chi', \Theta + \Theta')$.

Lemma 6.3.4. *The subset $\mathcal{E}^2(B, A)$ is a subgroup of $Z^2(\Omega A) \times A^+$ and it is invariant under the equivalence relation.*

Proof. It is easy to see that $\mathcal{E}^2(B, A)$ is a subgroup of $Z^2(\Omega A) \times A^+$. Here, we only check that it is invariant under the equivalence relation. Let (χ, Θ) be any element of $\mathcal{E}^2(B, A)$. Suppose it is equivalent to some element (χ', Θ') of $Z^2(\Omega A) \times A^+$. We need to show that (χ', Θ') is also in $\mathcal{E}^2(B, A)$. By definition, there is some $a \in A^+$ such that

$$\chi' = \chi - d^1(a), \quad \Theta' = \Theta - \mathbf{\Phi}_z(a).$$

Thus,

$$\mathbf{\Phi}_z(\chi') = \mathbf{\Phi}_z(\chi) - \mathbf{\Phi}_z[d^1(a)] = d^1[\Theta - \mathbf{\Phi}_z(a)] = d^1(\Theta'),$$

and, by Proposition 6.2.2,

$$\rho_z(\Theta') = \rho_z[\Theta - \mathbf{\Phi}_z(a)] = \rho_z(\Theta) - \rho_z \circ \mathbf{\Phi}_z(a) = 0.$$

So, (χ', Θ') belongs to $\mathcal{E}^2(B, A)$, which completes the proof. ■

Therefore, we can define

$$\mathcal{H}^2(B, A) := \mathcal{E}^2(B, A)/\sim .$$

In particular, when the extension H is primitively generated, it includes all the restricted Lie algebra extensions of $\mathfrak{h}$ by $\mathfrak{g}$.

Definition 21. In the set $\mathrm{B}^2(\Omega A) \times A^+$, we define a subset $\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$, where (χ, Θ) belongs to $\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$ if

$$\mathbf{\Phi}_z(\chi) = d^1(\Theta), \quad \rho_z(\Theta) = 0.$$

We can view $\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$ as a subset of $\mathcal{E}^2(B, A)$ by considering $\mathrm{B}^2(\Omega A) \times A^+$ as a subset of $\mathrm{Z}^2(\Omega A) \times A^+$. Moreover, it is invariant under the equivalence relation $\sim$ in $\mathrm{Z}^2(\Omega A) \times A^+$. Thus, we can define

$$\mathcal{H}^2(\mathfrak{g}, \mathfrak{h}) := \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})/\sim .$$

By definition, it is a subgroup of $\mathcal{H}^2(B, A)$.

Proof of Theorem 6.1.1(ii). Firstly, we define a map from $\mathcal{E}^2(B, A)$ to all the extensions of A by B of type T. For any point $(\chi, \Theta) \in \mathcal{E}^2(B, A)$, take the data $\mathscr{D} = (T, z, \chi, \Theta)$. We show that $u(\mathscr{D})$ is an extension of A by B, which is of type T. Let us recall the construction of $u(\mathscr{D})$. As an algebra, it is generated by $x_1, x_2, \cdots, x_d$ and x, subject to the relations in A and

$$[x, x_i] = \rho_z(x_i), \text{ for all } 1 \le i \le d, \tag{6.3.3}$$

$$x^p + \lambda x + \Theta = 0. \tag{6.3.4}$$

The coalgebra structure is given by

$$\Delta(x) = x \otimes 1 + 1 \otimes x + \chi, \ \Delta(x_i) = 1 \otimes x_i + 1 \otimes x_i, \text{ for all } 1 \le i \le d. \tag{6.3.5}$$

It directly follows from the construction (6.3.3) that $A^+u(\mathscr{D}) = u(\mathscr{D})A^+$. Hence A is normal in $u(\mathscr{D})$. Now, consider the following sequence:

$$1 \longrightarrow A \xrightarrow{\iota} u(\mathscr{D}) \xrightarrow{\pi} B \longrightarrow 1,$$

where ι is the natural injection, and $\pi(x_i) = 0$ for all $1 \le i \le d$ and $\pi(x) = z$. Because of Relation (6.3.4), we have $\pi(x^p + \lambda x + \Theta) = z^p + \lambda z = 0$. And $(\pi \otimes \pi)\Delta(x) = \Delta(z) = \Delta[\pi(x)]$ by the comultiplications given in (6.3.5). Hence, π is a well-defined Hopf algebra projection. It is clear that $u(\mathscr{D})/u(\mathscr{D})^+A \simeq B$ via π. Hence $u(\mathscr{D})$ is an extension of A by B. Moreover, the extension is of type T by Relation (6.3.3). Therefore, we have a map from $\mathcal{E}^2(B, A)$ to all the extensions of A by B of type T.

Secondly, by Theorem 6.1.4, we know the map above is surjective. It remains to show that the equivalence relation defined in $\mathcal{E}^2(B, A)$ respects the equivalence of extensions. It is implied by the following lemma, which completes the proof.

■

Lemma 6.3.5. *Let (χ, Θ) and (χ', Θ') be two points in $\mathcal{E}^2(B, A)$. Any equivalence ϑ : $u(\mathscr{D}) \mapsto u(\mathscr{D}')$ can be written as*

$$\vartheta(x_i) = x_i, \quad \vartheta(x) = x' - a, \tag{6.3.6}$$

for all $1 \le i \le d$ and some $a \in A^+$. Moreover, ϑ is an equivalence if and only if

$$d^1(a) = \chi - \chi', \quad \mathbf{\Phi}_z(a) = \Theta - \Theta'. \tag{6.3.7}$$

Proof. Firstly, we prove one direction. Let $\vartheta : u(\mathscr{D}) \mapsto u(\mathscr{D}')$ be an equivalence. Hence, it is an isomorphism of Hopf algebras, which yields the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & u(\mathscr{D}) & \xrightarrow{\pi} & B & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle\vartheta} & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & u(\mathscr{D}') & \xrightarrow{\pi'} & B & \longrightarrow & 1. \end{array} \tag{6.3.8}$$

Suppose $u(\mathscr{D}')$ is generated by $x_1, x_2, \cdots, x_d$ and x' satisfying $\pi'(x') = z$ as we did for $u(\mathscr{D})$. Note that $\vartheta = \text{Id}$ on A. Since ϑ is a coalgebra map, we have

$$\Delta[\vartheta(x)] = (\vartheta \otimes \vartheta)\Delta(x). \tag{6.3.9}$$

This implies that $\Delta[\vartheta(x)] - \vartheta(x) \otimes 1 - 1 \otimes \vartheta(x) \in A \otimes A$. Thus, we can write $\vartheta(x) = \gamma x' - a$ for some $\gamma \in \mathbf{k}^\times$ and $a \in A^+$ by Lemma 6.2.4. Because of the commutativity of the Diagram (6.3.8), $\pi(x) = \pi'\vartheta(x) = z$, which yields that $\gamma = 1$. Hence, ϑ must be in the form of (6.3.6).

Moreover, direct computation in Equation (6.3.9) shows that $d^1(a) = a\otimes 1 + 1\otimes a - \Delta(a) = \chi - \chi'$. Also since ϑ is an algebra map, we have

$$\vartheta(x^p + \lambda x + \Theta) = x'^p + \lambda x' + \Theta - (\mathcal{D}_z^1 + \lambda \circ \mathrm{Id})(a) = \Theta - \Theta' - \Phi_z(a) = 0.$$

Here, we use the fact that $(x'-a)^p = x'^p - a^p - (\mathrm{ad}x')^{p-1}(a) = x'^p - a^p - \rho_z^{p-1}(a) = x'^p - \mathcal{D}_z^1(a)$. Therefore, we have the conditions in (6.3.7).

Secondly, for the other direction, let ϑ be in the from of (6.3.6) satisfying (6.3.7). By the same calculation, it is easy to see that ϑ is a well-defined bialgebra map from $u(\mathscr{D})$ to $u(\mathscr{D}')$. Then, it is a Hopf algebra map by [17, Proposition 4.2.5]. Finally, according to the form of ϑ, it is certainly a bijection, which makes the Diagram (6.3.8) commutative. This completes the proof. ■

Proof of Theorem 6.1.1(i). We can view $\mathfrak{h}$ as a restricted $\mathfrak{g}$-module via ρ. Then, any restricted Lie algebra extension $\mathfrak{l}$ of $\mathfrak{h}$ by $\mathfrak{g}$ yields a primitively generated extension of A by B given by $u(\mathfrak{l})$. It is clear that it is of type T and vice visa. Hence, equivalence classes of such extensions correspond to a subgroup of $\mathcal{H}^2(B, A)$, which describes all primitively generated extensions. By Theorem 6.1.3(ii), the subgroup is represented by points (χ, Θ) in $\mathcal{E}^2(B, A)$, where $[\chi] = 0$ in $\mathrm{H}^2(\Omega A)$ or $\chi \in \mathrm{B}^2(\Omega A)$. Then, the result follows from the definition of $\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$. ■

6.4 Group quotient of the cohomological type group

In this section, we classify all finite-dimensional connected Hopf algebras with large abelian primitive space according to their types. We will first describe the type for each object in $\mathscr{H}$.

We construct a functor from $\mathscr{H}$ to $\mathscr{T}$, i.e., $\mathrm{p}_{\mathscr{H}} : \mathscr{H} \longrightarrow \mathscr{T}$, and we say that an object $H \in \mathscr{H}$ has type T if $\mathrm{p}_{\mathscr{H}}(H) = T$. As a consequence, isomorphic objects in $\mathscr{H}$ must have isomorphic images in $\mathscr{T}$ via the functor $\mathrm{p}_{\mathscr{H}}$. In other words, objects in $\mathscr{H}$ are classified, at first step, by their types in $\mathscr{T}$. We start by showing that H is always an extension in the sense of (6.3.1).

Lemma 6.4.1. *Let H be a Hopf algebra in $\mathscr{H}$, and A be the Hopf subalgebra of H generated by $\mathrm{P}(H)$. Then, A is normal in H. Moreover, we have the following short exact sequence:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & H & \longrightarrow & H/A^{+}H & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & u(\mathfrak{h}) & \longrightarrow & H & \longrightarrow & u(\mathfrak{g}) & \longrightarrow & 1, \end{array} \tag{6.4.1}$$

where $\mathfrak{h} = \mathrm{P}(H)$, and $\mathfrak{g} = \mathrm{P}(H/A^{+}H)$ which is one-dimensional.

Proof. Firstly, we show that A is a normal Hopf subalgebra of H. Let n be the minimal integer such that $A_n \subsetneq H_n$. Choose any $x \in H_n \backslash A_n$. Following the argument in Proposition 6.3.1, we know $\Delta(x) - x \otimes 1 - 1 \otimes x \in A \otimes A$. Since A is commutative, it is easy to check that $[x, \mathrm{P}(H)] \subseteq \mathrm{P}(H) \subset A$. Thus, $[x, A] \subseteq A$ for A is generated by $\mathrm{P}(H)$. It follows from $\dim H / \dim A = p$ that $\dim(H_n/K_n) = 1$ by Lemma 2.2.1. This implies that H_n is spanned by A_n and x. Hence, $[H_n, A] \subseteq A$, and A is normal in H by Lemma 2.2.2.

Secondly, we can make a natural identification $A = u(\mathrm{P}(H))$ since A is primitively generated by $\mathrm{P}(H)$ according to Proposition 2.1.4(5). Regrading the dimension of the quotient Hopf algebra, we have $\dim(H/A^{+}H) = p$. Then by Theorem 1.0.1, we know $H/A^{+}H$ must be primitively generated by $\mathrm{P}(H/A^{+}H)$, which is one-dimensional. This completes the proof. ■

For any object $H \in \mathscr{H}$, its *type* is defined to be the type of the extension as in Diagram (6.4.1), i.e.,

$$\mathrm{p}_{\mathscr{H}}(H) := \left(\mathrm{P}(H),\ \mathrm{P}(H/A^{+}H),\ \rho\right).$$

It remains to show that $\mathrm{p}_{\mathscr{H}}$ respects the identify map and composition of maps in $\mathscr{H}$. Suppose $\phi : H \to H'$ is a Hopf algebra map between two objects $H, H' \in \mathscr{H}$. We denote restricted Lie algebras $\mathfrak{h}$ (resp. $\mathfrak{h}'$) and $\mathfrak{g}$ (resp. $\mathfrak{g}'$) regarding H (resp. H') as in Lemma 6.4.1. Since every Hopf algebra map sends primitive elements to primitive elements, it follows that there is a restriction $\phi| : u(\mathfrak{h}) \to u(\mathfrak{h}')$. Moreover, by passing to the quotient, the following diagram commutes:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & u(\mathfrak{h}) & \longrightarrow & H & \longrightarrow & u(\mathfrak{g}) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi|} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \overline{\phi}} & & \\ 1 & \longrightarrow & u(\mathfrak{h}') & \longrightarrow & H' & \longrightarrow & u(\mathfrak{g}') & \longrightarrow & 1. \end{array}$$

Therefore, by Lemma 6.3.2, we conclude that $\mathrm{p}_{\mathscr{H}}$ is a well-defined functor.

Let $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ be as in Convention 2. We are interested in constructing a set, whose points naturally are in 1-1 correspondence with all the isomorphism classes in $\mathscr{H}$ of type T. We define

$$\mathcal{H}^2(T) = \mathcal{H}^2(B, A) \setminus \mathcal{H}^2(\mathfrak{g}, \mathfrak{h}).$$

Next, we define a group action of $\mathrm{Aut}(T)$ on $\mathcal{H}^2(T)$. Recall that any automorphism $\phi \in \mathrm{Aut}(T)$ consists of two automorphisms of $\mathfrak{h}$ and $\mathfrak{g}$, which extend to automorphisms of A and B respectively. For simplicity, we will keep the same notation ϕ for any of these automorphisms. It is easy to see that there exists a group character $\gamma : \mathrm{Aut}(T) \to \mathbf{k}^\times$ such that γ_ϕ is given by

$$\phi(z) = \gamma_\phi z,$$

for any $\phi \in \mathrm{Aut}(T)$. We first define the group action on the set $\mathrm{Z}^2(\Omega A) \times A^+$ as

$$\phi.(\chi, \Theta) = (\phi.\chi, \phi.\Theta) := (\gamma_\phi^{-1}(\phi \otimes \phi)(\chi), \gamma_\phi^{-p}\phi(\Theta)), \tag{6.4.2}$$

for any $\phi \in \mathrm{Aut}(T)$. We claim that it is well-defined. Choose any point $(\chi, \Theta) \in \mathrm{Z}^2(\Omega A) \times A^+$. We need to show that $\phi.\chi \in \mathrm{Z}^2(\Omega A)$ and $\phi.\Theta \in A^+$. For the first part, since Δ is an algebra map, we have $\overline{\Delta}\phi = (\phi \otimes \phi)\overline{\Delta}$ on A^+. Hence,

$$d^2(\phi.\chi) = (-\overline{\Delta} \otimes 1 + 1 \otimes \overline{\Delta})[\gamma_\phi^{-1}(\phi \otimes \phi)(\chi)] = \gamma_\phi^{-1}(\phi \otimes \phi \otimes \phi)[d^2(\chi)] = 0.$$

This shows that $\phi.\chi \in \mathrm{Z}^2(\boldsymbol{\omega} A)$, and certainly $\phi.\Theta \in A^+$. Then, it is direct to check that the above definition gives a group action, which proves the claim. Moreover,

Lemma 6.4.2. *The subsets $\mathcal{E}^2(B, A)$, $\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$ are* $\mathrm{Aut}(T)$*-invariant. Furthermore, the equivalence relation is preserved by the* $\mathrm{Aut}(T)$*-action.*

Proof. Firstly, we show that $\mathcal{E}^2(B,A)$ is Aut(T)-invariant. Let $\phi \in \mathrm{Aut}(T)$. Since $z^p+\lambda z = 0$, it follows that $\phi(z^p)=\phi(z)^p=\phi(-\lambda z)$. Thus, $\lambda\gamma_\phi^p = \lambda\gamma_\phi$ by the definition of the group character γ. By the commutative diagram (2.5.1), it is easy to see that $\rho_{\phi(z)}[(\phi\otimes\phi)(\chi)] = (\phi\otimes\phi)[\rho_z(\chi)]$. Then for any $(\chi,\Theta)\in\mathcal{E}^2(B,A)$, we have

$$\begin{aligned}
\mathbf{\Phi}_z(\phi.\chi) &= (\phi.\chi)^p + \lambda(\phi.\chi) + \rho_z^{p-1}(\phi.\chi) \\
&= [\gamma_\phi^{-1}(\phi\otimes\phi)(\chi)]^p + \lambda\gamma_\phi^{-1}(\phi\otimes\phi)(\chi) + \rho_z^{p-1}[\gamma_\phi^{-1}(\phi\otimes\phi)(\chi)] \\
&= \gamma_\phi^{-p}(\phi\otimes\phi)(\chi^p) + \gamma_\phi^{-p}(\phi\otimes\phi)(\lambda\chi) + \gamma_\phi^{-p}\rho_{\phi(z)}^{p-1}[(\phi\otimes\phi)(\chi)] \\
&= \gamma_\phi^{-p}(\phi\otimes\phi)[\chi^p + \lambda\chi + \rho_z^{p-1}(\chi)] \\
&= \gamma_\phi^{-p}(\phi\otimes\phi)[\mathbf{\Phi}_z(\chi)] \\
&= \gamma_\phi^{-p}(\phi\otimes\phi)[d^1(\Theta)] \\
&= d^1[\gamma_\phi^{-p}\phi(\Theta)] \\
&= d^1(\phi.\Theta).
\end{aligned}$$

Moreover, $\rho_z(\phi.\Theta) = \gamma_\phi^{-p-1}\rho_{\phi(z)}[\phi(\Theta)] = \gamma_\phi^{-p-1}\phi[\rho_z(\Theta)] = 0$. Therefore, $\phi.(\Theta,\chi)\in\mathcal{E}^2(B,A)$ by definition, which proves that $\mathcal{E}^2(B,A)$ is Aut(T)-invariant. It is similar to check that $\mathcal{L}^2(\mathfrak{g},\mathfrak{h})$ is Aut(T)-invariant. Let $(\chi,\Theta)\in\mathcal{L}^2(\mathfrak{g},\mathfrak{h})$ such that $\chi\in\mathrm{B}^2(\Omega A)$. Thus, we can write $\chi = d^1(a)$ for some $a\in A^+$. Since ϕ is an automorphism of A as Hopf algebras, following the definition of d^1, we have

$$\begin{aligned}
d^1(\gamma_\phi^{-1}\phi(a)) &= \gamma_\phi^{-1}\phi(a)\otimes 1 + 1\otimes\gamma_\phi^{-1}\phi(a) - \Delta[\gamma_\phi^{-1}\phi(a)] \\
&= \gamma_\phi^{-1}(\phi\otimes\phi)[a\otimes 1 + 1\otimes a - \Delta(a)] \\
&= \gamma_\phi^{-1}(\phi\otimes\phi)[d^1(a)] \\
&= \gamma_\phi^{-1}(\phi\otimes\phi)(\chi)
\end{aligned}$$

So we have $\phi.\chi\in\mathrm{B}^2(\Omega A)$, which proves that $\mathcal{L}^2(\mathfrak{g},\mathfrak{h})$ is also Aut(T)-invariant.

Secondly, we need to show that the equivalence relation defined on $\mathrm{Z}^2(\Omega A)\times A^+$ respects the Aut(T)-action. Suppose we have $(\chi,\Theta)\sim(\chi',\Theta')$. Thus, there exists some $a\in A^+$ such that

$$d^1(a) = \chi - \chi', \quad \mathbf{\Phi}_z(a) = \Theta - \Theta'.$$

Let $b = \gamma_\phi^{-1}\phi(a) \in A^+$. Direct computation shows that $d^1(b) = \phi.\chi - \phi.\chi'$ and

$$\begin{aligned}\mathbf{\Phi}_z(b) &= b^p + \lambda b + \rho_z^{p-1}(b)\\ &= \gamma_\phi^{-p}\phi(a)^p + \lambda\gamma_\phi^{-1}\phi(a) + \gamma_\phi^{-p}\rho_{\phi(z)}^{p-1}[\phi(a)]\\ &= \gamma_\phi^{-p}\phi[a^p + \lambda a + \rho_z^{p-1}(a)]\\ &= \gamma_\phi^{-p}\phi[\mathbf{\Phi}_z(a)]\\ &= \gamma_\phi^{-p}\phi(\Theta - \Theta')\\ &= \phi.\Theta - \phi.\Theta'.\end{aligned}$$

Hence $\phi.(\chi, \Theta) \sim \phi.(\chi', \Theta')$, which completes the proof. ∎

As a consequence of the previous lemma, we have an induced $\mathrm{Aut}(T)$-action on $\mathcal{H}^2(T) = \mathcal{H}^2(B, A) \setminus \mathcal{H}^2(\mathfrak{g}, \mathfrak{h})$.

Proof of Theorem 6.1.1(iii). We first show that the Hopf algebras of type T in $\mathscr{H}$ are naturally in 1-1 correspondence with the points in $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$. Let H be any Hopf algebra in $\mathscr{H}$ of type T. By Lemma 6.4.1, we know it is an extension of A by B. According to Theorem 6.1.4, we can assume that H is generated, as an algebra, by all x_i's and x, subject to the relations in A and

$$[x, x_i] = \rho_z(x_i), \quad x^p + \lambda x + \Theta = 0.$$

The coalgebra structure is given by

$$\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i, \quad \Delta(x) = x \otimes 1 + 1 \otimes x + \chi,$$

where (χ, Θ) lies in $\mathcal{E}^2(B, A)$. Moreover, by Theorem 6.1.3(ii), $H \in \mathscr{H}$ if and only if $\chi \notin \mathrm{B}^2(\Omega A)$. This shows the 1-1 correspondence.

Secondly, in order to find isomorphism classes in $\mathscr{H}$ of type T, we need to further consider the $\mathrm{Aut}(T)$-action on $\mathcal{H}^2(T)$. Therefore, the result comes from the following lemma.

∎

Lemma 6.4.3. *Let (χ, θ) and (χ', Θ') be two points in $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$, and H and H' be the corresponding objects in $\mathscr{H}$. Then, for any map $f : H \to H'$, we have $\phi \in \mathrm{Mor}(T, T)$*

with $\phi(z) = \gamma z$ for some $\gamma \in \mathbf{k}$, and f can be written as

$$f(x_i) = \phi(x_i), \quad f(x) = \gamma x' - a,$$

for some $a \in A^+$. Moreover, f is an isomorphism if and only if $\phi \in \mathrm{Aut}(T)$ and

$$d^1(\gamma^{-1}a) = \phi.\chi - \chi', \quad \mathbf{\Phi}_z(\gamma^{-1}a) = \phi.\Theta - \Theta'.$$

Proof. By the functor $\mathrm{p}_{\mathscr{H}} : \mathscr{H} \to \mathscr{T}$, any map $f : H \to H'$ induces a morphism $\mathrm{p}_{\mathscr{H}}(f) =: \phi \in \mathrm{Mor}(T, T)$. Then, we can mimic the proof of Lemma 6.3.5 with appropriate adjustment in ϕ, which is not in general the identity map. Since the calculation is straightforward and similar, we omit the details here. ∎

Remark 15. Apparently, the construction of the $\mathrm{Aut}(T)$-orbits in $\mathcal{H}^2(T)$ depends on the choice of the basis of $\mathfrak{g}$. But, if we multiple the basis z by some nonzero scalar γ, the resulting subset $\mathcal{E}^2(B, A)$ is isomorphic to the previous one via $(\chi, \Theta) \to (\gamma^{-1}\chi, \gamma^{-p}\Theta)$, and so is $\mathcal{L}^2(B, A)$. Moreover, the isomorphism is compatible with the equivalence relation and the $\mathrm{Aut}(T)$-action. Since $\mathfrak{g}$ is one-dimensional, it ensures that our definition is unique up to isomorphisms.

Proof of Theorem 6.1.2. Because the type of any object in $\mathscr{H}$ is defined by the functor $\mathrm{p}_{\mathscr{H}} : \mathscr{H} \to \mathscr{T}$, two Hopf algebras in $\mathscr{H}$ cannot be isomorphic if their types are not isomorphic in $\mathscr{T}$. Thus, it suffices to show that for any two isomorphic types $T, T' \in \mathscr{T}$, there is a bijection between their fibers in $\mathscr{H}$ via Hopf algebra isomorphisms, i.e., there is a bijection $\Psi : \mathrm{p}_{\mathscr{H}}^{-1}(T) \to \mathrm{p}_{\mathscr{H}}^{-1}(T')$ where $\Psi(H) \simeq H$ for all $H \in \mathrm{p}_{\mathscr{H}}^{-1}(T)$.

Suppose T is isomorphic to $T' = (\mathfrak{h}', \mathfrak{g}', \rho')$ via ϕ. We let $\phi(z)$ be the basis for $\mathfrak{g}'$. From Section 6.4, we know that elements of $\mathrm{p}_{\mathscr{H}}^{-1}(T)$ are in 1-1 correspondence with elements of $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$. Also, it is true for $\mathrm{p}_{\mathscr{H}}^{-1}(T')$. Thus, we can define the bijection

$$\Psi(\chi, \Theta) := ((\phi \otimes \phi)(\chi), \phi(\Theta)),$$

for any point $(\chi, \Theta) \in \mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$. Direct computation shows that Ψ can be extended to isomorphisms of their corresponding Hopf algebras in $\mathscr{T}$ and $\mathscr{T}'$. This completes the proof. ∎

6.5 A realization of the group quotient

We like to realize the isomorphism classes in $\mathscr{H}$ of a given type as group quotient of some geometric space. Throughout this section, let $T = (\mathfrak{h}, \mathfrak{g}, \rho)$ be some type in $\mathscr{T}$ as in Convention 2. For simplicity, suppose the base field $\mathbf{k}$ is perfect.

Recall that the cobar construction on A is the following differential graded algebra

$$\mathbf{k} \xrightarrow{0} A^+ \xrightarrow{d^1} (A^+)^2 \xrightarrow{d^2} (A^+)^3 \longrightarrow \cdots,$$

where the differentials d^1 and d^2 are given by

$$d^1(a) = a \otimes 1 + 1 \otimes a - \Delta(a), \quad d^2(a \otimes b) = 1 \otimes a \otimes b - \Delta(a) \otimes b + a \otimes \Delta(b) - a \otimes b \otimes 1.$$

for any $a, b \in A^+$. It is clear that $\mathrm{H}^1(\Omega A) = \mathrm{P}(A) = \mathfrak{h}$. We define a map $\boldsymbol{\omega} : \mathrm{H}^1(\Omega A) \mapsto \mathrm{H}^2(\Omega A)$ as

$$\boldsymbol{\omega}(x) = [\sum_{1 \le i \le p-1} \binom{p}{i} / p \; x^i \otimes x^{p-i}],$$

for any $x \in \mathfrak{h}$. When A is commutative, it is easy to check that $\boldsymbol{\omega}$ is semi-linear with respect to the Frobenius map of $\mathbf{k}$ (see Lemma 2.4.3). By abuse of language, we also consider $\boldsymbol{\omega}(x) = \sum_{i=1}^{p-1} \binom{p}{i}/p \; x^i \otimes x^{p-i}$ as an element in $(A^+)^2$. Moreover, by Proposition 2.4.2, we have the vector space isomorphism

$$\mathrm{H}^2(\Omega A) = \begin{cases} S^2(\mathfrak{h}) & p = 2, \\ \Lambda^2(\mathfrak{h}) \oplus \boldsymbol{\omega}(\mathfrak{h}) & p > 2, \end{cases} \tag{6.5.1}$$

where $S^2(\mathfrak{h})$ and $\Lambda^2(\mathfrak{h})$ are the degree two part of the polynomial and exterior algebra respectively. In general, we claim that, as cohomology ring,

$$\mathrm{H}^\bullet(\Omega A) \simeq \begin{cases} S(\mathfrak{h}) & p = 2, \\ \Lambda(\mathfrak{h}) \otimes S(\boldsymbol{\omega}(\mathfrak{h})) & p > 2. \end{cases}$$

Let C_p^d be the elementary abelian p-group of rank d. Note that A^* is isomorphic, as an algebra, to the group algebra $\mathbf{k}[C_p^d]$. It is a well-known fact that (e.g., see [44, Proposition 1.4]):

$$\mathrm{H}^\bullet(\Omega A) \simeq \mathrm{HH}^\bullet(A^*, \mathbf{k}) \simeq \mathrm{H}^\bullet(C_p^d, \mathbf{k}),$$

where the right side is the group cohomology of C_p^d with coefficients in $\mathbf{k}$. Moreover, the isomorphism is on the complex level, and it is compatible with the cup product in the group cohomology and the tensor product in the cobar construction. Finally, by using the well-known group cohomology ring $\mathrm{H}^\bullet(C_p^d, \mathbf{k})$ (e.g. see [39, Section 4]) and Equation (6.5.1), we get our result.

In this section, we assume the characteristic $p > 2$. We can do the similar embedding for $p = 2$ by changing the formula of $\mathrm{H}^2(\Omega A)$ according to Equation (6.5.1). Firstly, we embed the affine space $\mathbb{A}_k^{d(d+1)/2} \times \mathbb{A}_k^d$ into $\mathrm{Z}^2(\Omega A) \times \mathfrak{h}$ by sending any point

$$P = (a_{ij}, b_k, c_l)_{1 \le i < j \le d, 1 \le \mathbf{k}, l \le d}$$

to some element (χ_P, Θ_P) such that

$$\chi_P = \sum_{1 \le i < j \le d} a_{ij} x_i \otimes x_j + \boldsymbol{\omega}\left(\sum_{1 \le i \le d} b_i x_i\right), \quad \Theta_P = \sum_{1 \le i \le d} c_i x_i.$$

Secondly, we know A, which is the restricted enveloping algebra of $\mathfrak{h}$, has the following basis

$$\{x_1^{\sigma_1} x_2^{\sigma_2} \cdots x_d^{\sigma_d} | 0 \le \sigma_1, \sigma_2, \cdots, \sigma_d \le p - 1\}$$

by the PBW Theorem. We denote by $A_{\ge 2}$ the subspace of A spanned by all these bases satisfying $\sigma_1 + \sigma_2 + \cdots + \sigma_d \ge 2$. Thus, we have a vector space decomposition $A^+ = A_{\ge 2} \oplus \mathfrak{h}$ (this decomposition depends on the choice of the basis of $\mathfrak{h}$).

Thirdly, we define the subset S_T of $\mathbb{A}_k^{d(d+1)/2} \times \mathbb{A}_k^d$, where $P \in S_T$ if

(i) $\chi_P \notin \mathrm{B}^2(\Omega A)$;

(ii) $\boldsymbol{\Phi}_z(\chi_P) = d^1(a)$;

(iii) $\rho_z(a + \Theta_P) = 0$,

for some $a \in A_{\ge 2}$. Note that the element $a \in A_{\ge 2}$ in the definition above is uniquely determined by χ_P. It is easy to see the uniqueness by taking the difference of two possible solutions. Hence, we will denote a by Ψ_P for any $P \in S_T$.

Next, we identify $\mathbb{A}_k^d = \mathfrak{h}$. Thus, the z-operator $\mathbf{\Phi}_z$, when restricted to $\mathfrak{h}$, becomes a regular map from A_k^d to itself. Moreover, we view $\mathfrak{h}$ as an abelian group via the vector space addition. Let $\mathfrak{h}$ act on A_k^d by subtraction, i.e., $\Theta.x := x - \mathbf{\Phi}_z(\Theta)$ for all $x \in \mathbb{A}_k^d$ and $\Theta \in \mathfrak{h}$.

Finally, we denote the quotient space by $\mathbb{A}_k^d/\mathfrak{h}$, and there is a quotient map

$$\mathbb{A}_k^{d(d+1)/2} \times \mathbb{A}_k^d \xrightarrow{\pi} \mathbb{A}^{d(d+1)/2} \times (\mathbb{A}_k^d/\mathfrak{h}).$$

Proposition 6.5.1. *Every equivalence class in $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$ can be represented by $(\chi_P, \Psi_P + \Theta_P)$ for some $P \in S_T$. Moreover, elements of $\mathcal{H}^2(T)$ are in* 1-1 *correspondence with points in the image of S_T via the quotient map π.*

Proof. Let (χ, Θ) be any point in $\mathcal{E}^2(B, A)\setminus\mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$. By definition, we know χ is a z-cocycle. Thus, we can write $\chi = \chi' + d^1(a)$ for some $a \in A^+$, where

$$\chi' = \sum_{1\le i<j\le d} a_{ij} x_i \otimes x_j + \boldsymbol{\omega}\left(\sum_{1\le i\le d} b_i x_i\right)$$

according to Equation (6.5.1). We denote $\Theta' = \Theta - \mathbf{\Phi}_z(a)$. It is direct to check that $(\chi', \Theta') \sim (\chi, \Theta)$, which is in $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$.

Now, we will show that (χ', Θ') corresponds to some point in S_T. By the vector space decomposition $A^+ = A_{\ge 2} \oplus \mathfrak{h}$, we can write $\Theta' = \Theta_2' + \Theta_1'$, where $\Theta_2' \in A_{\ge 2}$ and $\Theta_1' = \sum_{1\le i\le d} c_i x_i$. Let $P = (a_{ij}, b_i, c_i)$ be the point. By definition, it is clear that

$$(\chi_P, \Theta_P) = (\chi', \Theta_1').$$

Thus, direct computation shows that, in the definition of S_T, (ii) and (iii) are satisfied with $a = \Theta_2'$. Since (i) is obvious, it follows that $P \in S_T$. This proves the first half of the statement.

Next, we define a map $f : S_T \to \mathcal{H}^2(T)$ by

$$f(P) = [(\chi_P, \Psi_P + \Theta_P)].$$

That is, it sends any point P of S_T to the equivalence class of $(\chi_P, \Psi_P + \Theta_P)$ in $Z^2(\Omega A) \times A^+$. Moreover, the image of S_T is contained in $\mathcal{E}^2(B, A) \setminus \mathcal{L}^2(\mathfrak{g}, \mathfrak{h})$ by the definition of S_T. By the previous discussion, f is surjective. Hence, it remains to show that f factors through the quotient map π and the factorization is injective. Let P, Q be two points in S_T. We will prove that $f(P) = f(Q)$ if and only if $\pi(P) = \pi(Q)$, which will complete the proof. By Definition 20(ii), $f(P) = f(Q)$ if and only if there exists some $a \in A^+$ such that

$$d^1(a) = \chi_P - \chi_Q, \quad \mathbf{\Phi}_z(a) = (\Psi_P + \Theta_P) - (\Psi_Q + \Theta_Q).$$

Note that $d^1(a) = \chi_P - \chi_Q$ implies that the two cohomology classes represented by them are the same in $\mathrm{H}^2(\Omega A)$. Thus, it follows that $\chi_P = \chi_Q$ by the explicit expressions of χ_P and χ_Q according to Equation (6.5.1). Therefore, we have $f(P) = f(Q)$ if and only if $\chi_P = \chi_Q$ and there exists some $a \in \mathfrak{h}$ ($d^1(a) = 0$) such that $\mathbf{\Phi}_z(a) = \Theta_P - \Theta_Q$. In other words, the second condition means that Θ_P and Θ_Q are in the same orbit of the $\mathfrak{h}$-action on $\mathbb{A}_k^d$ via $\mathbf{\Phi}_z$. This proves the statement. ■

We still assume the basis field has characteristic $p > 2$. Recall that any $\xi \in \mathrm{H}^2(\Omega A)$ is z-characteristic if

$$\mathbf{\Phi}_z(\xi) = \xi^p + \lambda\xi + \rho_z^{p-1}(\xi) = 0.$$

Firstly, by Equation (6.5.1), we can write every element in $\mathrm{H}^2(\Omega A)$ as

$$\xi = \Lambda + \boldsymbol{\omega}(x),$$

where $\Lambda = \sum_{1\leq i<j\leq d} \mu_{ij} x_i \wedge x_j$ and $x = \sum_{1\leq i\leq d} \mu_i x_i$ for some coefficients in $\mathbf{k}$. Note that the two subspaces $\Lambda^2(\mathfrak{h})$ and $\boldsymbol{\omega}(\mathfrak{h})$ are all $\mathbf{\Phi}_z$-invariant. Hence, ξ is z-characteristic if and only if

$$\mathbf{\Phi}_z(\Lambda) = 0, \quad \mathbf{\Phi}_z[\boldsymbol{\omega}(x)] = 0.$$

Secondly, we show that the ρ-action is trivial on $\boldsymbol{\omega}(\mathfrak{h})$.

Lemma 6.5.2. *For any $x \in \mathfrak{h}$, we have $\rho_z[\boldsymbol{\omega}(x)] = d^1[-x^{p-1}\rho_z(x)]$. In particular, the ρ-action is trivial on $\boldsymbol{\omega}(\mathfrak{h})$.*

Proof. Since $\mathfrak{h}$ is abelian, we have $\rho_z(x^i) = ix^{i-1}\rho_z(x)$ for any $x \in \mathfrak{h}$. Thus,

$$\begin{aligned}\rho_z[\boldsymbol{\omega}(x)] &= \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\ \rho_z(x^i) \otimes x^{p-i} + \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!}\ x^i \otimes \rho_z(x^{p-i}) \\ &= \sum_{i=1}^{p-1} \frac{(p-1)!}{(i-1)!(p-i)!}\ x^{i-1}\rho_z(x) \otimes x^{p-i} + \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-1-i)!}\ x^i \otimes x^{p-1-i}\rho_z(x) \\ &= \sum_{i=0}^{p-2} \binom{p-1}{i}\ x^i\rho_z(x) \otimes x^{p-1-i} + \sum_{i=1}^{p-1} \binom{p-1}{i}\ x^i \otimes x^{p-1-i}\rho_z(x) \\ &= (x \otimes 1 + 1 \otimes x)^{p-1}[\rho_z(x) \otimes 1 + 1 \otimes \rho_z(x)] - [x^{p-1}\rho_z(x)] \otimes 1 - 1 \otimes [x^{p-1}\rho_z(x)] \\ &= d^1[-x^{p-1}\rho_z(x)].\end{aligned}$$

It implies that $\rho_z[\boldsymbol{\omega}(x)] = \epsilon(z)\boldsymbol{\omega}(x) = 0$ in $\mathrm{H}^2(\Omega A)$. This completes the proof. ∎

Next, applying previous results, we have

$$\boldsymbol{\Phi}_z(\Lambda) = \sum_{1 \le i < j \le d} \mu_{ij}^p x_i^p \wedge x_j^p + \sum_{1 \le i < j \le d} \lambda\mu_{ij} x_i \wedge x_j + \sum_{\substack{k+l=p-1 \\ 1 \le i < j \le d}} \binom{p-1}{k} \mu_{ij}\rho_z^k(x_i) \wedge \rho_z^l(x_j).$$

Moreover, we know $\boldsymbol{\omega}$ is semi-linear with respect to the Frobenius map of $\mathbf{k}$. Thus, by previous lemma,

$$\begin{aligned}\boldsymbol{\Phi}_z[\boldsymbol{\omega}(x)] &= \boldsymbol{\omega}(x)^p + \lambda\boldsymbol{\omega}(x) + \rho_z^{p-1}[\boldsymbol{\omega}(x)] \\ &= \boldsymbol{\omega}(x^p) + \boldsymbol{\omega}(\lambda^{1/p}x) \\ &= \boldsymbol{\omega}(x^p + \lambda^{1/p}x).\end{aligned}$$

Proposition 6.5.3. *By above notations, ξ is z-characteristic if and only if $x^p + \lambda^{1/p}x = 0$, and the following equality holds in $\Lambda^2(\mathfrak{h})$.*

$$\sum_{1 \le i < j \le d} \mu_{ij}^p x_i^p \wedge x_j^p + \sum_{1 \le i < j \le d} \lambda\mu_{ij} x_i \wedge x_j + \sum_{\substack{k+l=p-1 \\ 1 \le i < j \le d}} \binom{p-1}{k} \mu_{ij}\rho_z^k(x_i) \wedge \rho_z^l(x_j) = 0.$$

Another way to understand $\mathcal{H}^2(T)$ is to consider the following commutative diagram

$$\begin{array}{ccc} \mathcal{H}^2(T) & \hookrightarrow & \mathbb{A}^{d(d+1)/2} \times (\mathbb{A}_k^d/\mathfrak{h}) \\ \downarrow q & & \downarrow p_1 \\ \mathrm{H}^2(\Omega A) & = & \mathbb{A}_k^{d(d+1)/2}, \end{array}$$

where p_1 is the projection of the first component. Moreover, q sends every equivalence class $[(\chi, \Theta)]$ to the cohomology class in $\mathrm{H}^2(\Omega A)$ represented by χ. It is clear that q maps every equivalence class into a nonzero z-characteristic element in $\mathrm{H}^2(\Omega A)$. We are interested in the inverse problem: when does a z-characteristic element have preimage in $\mathcal{H}^2(T)$. In order to answer this question, we give the following definition.

Definition 22. Let ξ be z-characteristic in $\mathrm{H}^2(\Omega A)$, which is represented by some cocycle χ. We say ξ is *admissible* if there exists some $a \in A^+$ such that $\mathbf{\Phi}_z(\chi) = d^1(a)$ and $\rho_z(a) = 0$.

We need to show that the definition does not depend on the choice of the representative cocycle χ. Suppose χ' is another cocycle representing ξ. Then, there is some $X \in A^+$ satisfying $\chi' = \chi + d^1(X)$. If we have found some $a \in A^+$ satisfying $\mathbf{\Phi}_z(\chi) = d^1(a)$ and $\rho_z(a) = 0$. Let $b = a + \mathbf{\Phi}_z(X)$. It is easy to see that $\mathbf{\Phi}_z(\chi') = d^1(b)$ and $\rho_z(b) = \rho_z(a) + \rho_z \circ \mathbf{\Phi}_z(X) = 0$ by Proposition 6.2.2(iii). So, the property of admissibility is well-defined for any z-characteristic element in $\mathrm{H}^2(\Omega A)$.

Remark 16. We make some observations concerning the above definition.

(i) A z-characteristic element has preimage in $\mathcal{H}^2(T)$ if and only if it is nonzero admissible.

(ii) Let χ be a z-cocycle, and $a \in A_{\geq 2}$ be the unique element determined by $\mathbf{\Phi}_a(\chi) = d^1(a)$. Thus, $[\chi]$ is admissible if and only if $\rho_z(a) \in \mathrm{Im}\rho_z$.

(iii) The admissibility is preserved by base field extension.

In [45], a finite-dimensional restricted Lie algebra L is called a *torus* if it is abelian and every element of L is semisimple in $u(L)$, i.e., generates a semisimple subalgebra.

Proposition 6.5.4. *If either $\mathfrak{h}$ or $\mathfrak{g}$ is a torus, (either A or B is semisimple), thus, every z-characteristic element is admissible.*

Proof. Without loss of generality, we can assume the base field is algebraically closed. Here, we only treat the case when $p = 2$. For the other case $p > 2$, the argument is similar. In the following, let ξ be a z-characteristic element in $\mathrm{H}^2(\Omega A)$. Since the admissibility does not depend on the choice of the representing cocycle, we can write the cocycle as

$$\chi = \sum_{1\le i\le j\le d} \mu_{ij} x_i \otimes x_j$$

for some coefficients $\mu_{ij} \in \mathbf{k}$ according to Equation (6.5.1).

(i) $\mathfrak{h}$ is a torus. By [27], we can further assume that $x_i^p = x_i$ for $1 \le i \le d$. Hence, by Definition 14(iv), we know $\rho_z = 0$. Therefore,

$$\mathbf{\Phi}_z(\chi) = \chi^p + \lambda\chi + \rho_z^{p-1}(\chi) = \sum_{1\le i\le j\le d} (\mu_{ij}^p + \lambda\mu_{ij}) x_i \otimes x_j.$$

So χ is a z-cocycle if and only if all the coefficients $\mu_{ij}^p + \lambda\mu_{ij} = 0$ since $[x_i \otimes x_j]$ where $1 \le i \le j \le d$ is a basis for $\mathrm{H}^2(\Omega A)$. Then, we can take $a = 0$ in the above definition, which implies that ξ is admissible.

(ii) $\mathfrak{g}$ is a torus. Then, in the relation $z^p + \lambda z = 0$, we have $\lambda \ne 0$. By Definition 14(iv), we know $\rho_z(\mathfrak{h}^p) = 0$. Since the base field is algebraically closed, it follows that $\mathfrak{h}^p$ is a subspace, and hence ρ_z is diagonalizable on $\mathfrak{h}/\mathfrak{h}^p$. Without loss of generality, we can assume that in the basis $x_1, x_2, \cdots, x_d$ of $\mathfrak{h}$, the first s elements form a basis for the subspace $\mathfrak{h}^p$, and the images of the remaining $d-s$ elements are eigenvectors in the quotient space $\mathfrak{h}/\mathfrak{h}^p$. In other words, we can set up $\rho_z(x_i) = 0$ for all $1 \le i \le s$, and $\rho_z(x_j) = \sigma_i x_j + y_j$ for some $y_j \in \mathfrak{h}^p$, when $s+1 \le j \le d$. It is easy to see that, if the eigenvalue $\sigma_j = 0$, we have y_j=0. Therefore, by replacing x_j by $x_j + y_j/\sigma_j$ when $\sigma_j \ne 0$, we can always assume in the above setup $y_j = 0$ for all $s+1 \le j \le d$. Moreover, if we write $\sigma_i = 0$ for all $1 \le i \le s$, thus $\rho_z(x_i) = \sigma_i x_i$ for all $1 \le i \le d$.

Now, we consider the Hopf subalgebra of A, which is generated by the restricted Lie subalgebra $\mathfrak{h}^p$. We denote it by $C = u(\mathfrak{h}^p)$. Thus,

$$\begin{aligned} \mathbf{\Phi}_z(\chi) &= \chi^p + \sum_{1\le i\le j\le d} \lambda\mu_{ij} x_i \otimes x_j + \sum_{\substack{k+l=p-1\\ 1\le i\le j\le d}} \binom{p-1}{k} \mu_{ij} \rho_z^k(x_i) \wedge \rho_z^l(x_j) \qquad (6.5.2) \\ &= \chi^p + \sum_{1\le i\le j\le d} \mu_{ij}[\lambda + (\sigma_i + \sigma_j)^{p-1}] x_i \otimes x_j. \end{aligned}$$

Since the p-th map in ΩA commutes with the differential by Proposition 6.2.2(i), we can view χ^p as a cocycle in the subcomplex ΩC. Therefore, there exists some $X \in C^+$, where we can write

$$\chi^p = d^1(X) + \sum_{1\le i\le j\le s} \tau_{ij} x_i \otimes x_j.$$

Combine it with the above Equation (6.5.2), we get

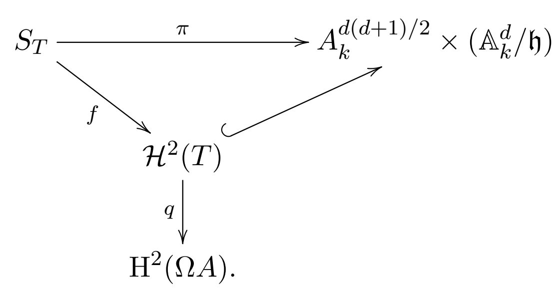
$$\mathbf{\Phi}_z(\chi) = d^1(X) + \sum_{1\le i\le j\le d} \phi_{ij} x_i \otimes x_j,$$

for some new coefficients $\phi_{ij} \in \mathbf{k}$. Hence, we have χ is a z-cocycle if and only if all the coefficients $\phi_{ij} = 0$ since $[x_i \otimes x_j]$ where $1 \le i \le j \le d$ is a basis for $\mathrm{H}^2(\Omega A)$. Then, we can take $a = X$ in the above definition. It is clear that $\rho_z(X) = 0$ for $X \in A^p$, which completes the proof. ■

Let ξ be a nonzero admissible z-cocycle in $\mathrm{H}^2(\Omega A)$. We like to know what does its fiber $q^{-1}(\xi)$ look like in $\mathcal{H}^2(T)$. As discussed before, the additive group $\mathfrak{h}$ acts on the affine space $\mathbb{A}_k^d = \mathfrak{h}$ by $\Theta.x = x - \mathbf{\Phi}_z(\Theta)$. Also, we can think ρ_z as a map from $\mathbb{A}_k^d$ to itself, whose kernel is a subspace. We denote it by $\mathrm{Ker}\rho_z$. Because of Proposition 6.2.2(iii), the $\mathfrak{h}$-action can be restricted to the subspace $\mathrm{Ker}\rho_z$.

Lemma 6.5.5. *Points in the fiber $q^{-1}(\xi)$ are in* 1-1 *correspondence with $\mathfrak{h}$-orbits in* $\mathrm{Ker}\rho_z$. *Moreover, the map q is injective if and only if* $\mathrm{Ker}\rho_z = \mathrm{Im}\mathbf{\Phi}_z$.

Proof. Consider the following commutative diagram:



As a consequence of Proposition 6.5.1, points in $q^{-1}(\xi)$ are in 1-1 correspondence with points in $\pi(fq)^{-1}(\xi)$. Following the notations used before, we have an embedding from S_T to $\mathrm{Z}^2(\Omega A) \times \mathfrak{h}$, where the image of any point P is written by (χ_P, Θ_P). Recall that Ψ_P denotes the unique element in $A_{\ge 2}$ such that

$$\mathbf{\Phi}_z(\chi_P) = d^1(\Psi_P), \quad \rho_z(\Psi_P + \Theta_P) = 0.$$

Since the nonzero z-characteristic element ξ is admissible, by Remark 16(i), there exists some point P in the fiber $(fg)^{-1}(\xi)$. It is clear, by definition, any other point Q belongs to $(fq)^{-1}(\chi)$ if and only if

$$\chi_Q = \chi_P =: \chi, \quad \rho_z(\Psi_Q + \Theta_Q) = 0.$$

Since $\Psi_P = \Psi_Q$, it follows that $\rho_z(\Theta_P - \Theta_Q) = 0$. Thus,

$$(fq)^{-1}(\xi) = \{Q \in S_T | (\chi_Q, \Theta_Q) \in (\chi, Q_P + \mathrm{Ker}\rho_z)\}.$$

Therefore, by definition, $\pi(fq)^{-1}(\xi) = \pi(\chi) \times (Q_P + \mathrm{Ker}\rho_z/\mathfrak{h}) \simeq \pi(\chi) \times (\mathrm{Ker}\rho_z/\mathfrak{h})$. This proves the first statement. The second statement is a direct application of the first one, since q is injective if and only if $\mathfrak{h}$-orbit in $\mathrm{Ker}\rho_z$ is single if and only if $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$. ■

We combine the results we have obtained so far in this section and the previous one.

Proposition 6.5.6. *Let either* $\mathfrak{h}$ *or* $\mathfrak{g}$ *be a torus, and assume that* $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$. *Then, elements in* $\mathcal{H}^2(T)$ *are in* 1-1 *correspondence with nonzero* z*-characteristic elements in* $\mathrm{H}^2(\Omega A)$.

Proof. Firstly, since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$, by previous lemma, we know $\mathcal{H}^2(T)$ can be embedded in $\mathrm{H}^2(\Omega A)$ via q. Secondly, by Remark 16(i), $q(\mathcal{H}^2(T))$ contains exactly those nonzero admissible z-characteristic elements. Finally, the result follows from Proposition 6.5.4. ■

Now, we will consider the $\mathrm{Aut}(T)$-action on $\mathcal{H}^2(T)$. Firstly, we assume that the base $p > 2$. Let $\phi \in \mathrm{Aut}(T)$. Recall that the group character $\gamma : \mathrm{Aut}(T) \to \mathbf{k}^\times$ is defined by $\phi(z) = \gamma_\phi z$. According to Equation (6.5.1), we can write any cohomology class $\xi \in \mathrm{H}^2(\Omega A)$ as

$$\xi = \sum_{1 \le i < j \le d} \mu_{ij} x_i \wedge x_j + \boldsymbol{\omega}\left(\sum_{1 \le i \le d} \mu_i x_i\right).$$

Regarding Equation (6.4.2), the action of $\phi \in \mathrm{Aut}(T)$ on $\mathrm{H}^2(\Omega A)$ is given by

$$\phi(\xi) = \sum_{1 \le i < j \le d} \gamma_\phi^{-1} \mu_{ij} \phi(x_i) \wedge \phi(x_j) + \boldsymbol{\omega}\left(\sum_{1 \le i \le d} {\gamma_\phi}^{-1/p} \mu_i \phi(x_i)\right).$$

The group action can be restricted to those nonzero admissible z-characteristic elements. And it is compatible with the G-action on $\mathcal{H}^2(T)$ via q.

Furthermore, if the base field is $\mathbb{K}$, then we can identify $\mathrm{H}^2(\Omega A) = \Lambda^1(\mathfrak{h}) \oplus \Lambda^2(\mathfrak{h})$, i.e., the degree one and two part of the exterior algebra $\Lambda(\mathfrak{h})$. Thus, we can rewrite

$$\xi = \sum_{1 \le i \le d} \mu_i x_i + \sum_{1 \le i < j \le d} \mu_{ij} x_i \wedge x_j.$$

Then, we have a group homomorphism from $\mathrm{Aut}(T)$ to the automorphism group of $\Lambda(\mathfrak{h})$, which is given by

$$\phi(\xi) = \sum_{1 \le i \le d} {\gamma_\phi}^{-1} \mu_i \phi(x_i) + \sum_{1 \le i < j \le d} \gamma_\phi^{-1} \mu_{ij} \phi(x_i) \wedge \phi(x_j).$$

The discussion for $p > 2$ is similar, so we omit it here.

Chapter 7

CONNECTED HOPF ALGEBRAS OF DIMENSION P^3 II

7.1 Preliminary results

In this chapter, we complete the classification of connected Hopf algebras of dimension p^3 whose primitive space is a two-dimensional abelian restricted Lie algebra. We assume that the base field $\mathbf{k}$ is algebraically closed of characteristic $p > 2$. We can do the similar things for $p = 2$. We use $\mathscr{H}$ to denote the collection of all such Hopf algebras. Let $\mathfrak{g}$ be a two-dimensional restricted Lie algebra with fixed basis x, y, and $\mathfrak{h}$ be a one-dimensional restricted Lie algebra with fixed basis z. Apply the results in previous chapter. We can view any Hopf algebra H in $\mathscr{H}$ as certain deformation of the restricted universal enveloping algebra of the semi-product $\mathfrak{g} \rtimes \mathfrak{h}$. Indeed, H is the quotient algebra of the free algebra generated by three variables x, y, z, where the algebra structure is given by the type $T = (\mathfrak{g}, \mathfrak{h}, \rho)$ with an element $\Theta \in u(\mathfrak{g})^+$ and the coalgebra structure is determined by some cocycle $\chi \in u(\mathfrak{g})^+ \otimes u(\mathfrak{g})^+$. To be more precise, H can be presented as $\mathbf{k}\langle x, y, z\rangle/\mathcal{I}$. The relation $\mathcal{I}$ is generated by

$$x^p - x^{[p]},\ y - y^{[p]},\ z^p - z^{[p]} + \Theta,\ [z, x] - \rho_z(x),\ [z, y] - \rho_z(y),$$

where $x^{[p]}, y^{[p]}, z^{[p]}$ denote the restricted maps in $\mathfrak{g}, \mathfrak{h}$. Regarding coalgebra structures, we have

$$\Delta(x) = x \otimes 1 + 1 \otimes x,\ \Delta(y) = y \otimes 1 + 1 \otimes y,\ \Delta(z) = z \otimes 1 + 1 \otimes z + \chi.$$

The data (T, z, χ, Θ) satisfy the following compatible conditions:

$$\mathbf{\Phi}_z(\chi) = \Theta \otimes 1 + 1 \otimes \Theta - \Delta(\Theta),\ \rho_z(\Theta) = 0,$$

where $\mathbf{\Phi}_z(\chi) = \chi^p - \lambda\chi + \rho_z^{p-1}(\chi)$. Note that the scalar λ is given by the restricted map on $\mathfrak{h}$: $z^{[p]} = \lambda z$.

In the following, we fix a type $T = (\mathfrak{g}, \mathfrak{h}, \rho)$ and associate it with a set $\mathcal{H}^2(T)$ and an automorphism group $\mathrm{Aut}(T)$. Then we have a quotient set $\mathcal{H}^2(T)/\mathrm{Aut}(T)$ with respect to some group action of $\mathrm{Aut}(T)$ on $\mathcal{H}^2(T)$. By Theorem 6.1.2, the isomorphism classes of $\mathscr{H}$ are in one-to-one correspondence with

$$\coprod_{T} \mathcal{H}^2(T)/\mathrm{Aut}(T),$$

where T goes through all isomorphism classes of possible types. A direct way to compute $\mathcal{H}^2(T)$ is to first compute the subset S_T in $\mathbb{A}^5$. Let $P = (a, b, c, d, e) \in \mathbb{A}^5$ be any point. Define an element (χ_P, Θ_P) in $Z^2(\Omega u(\mathfrak{g})) \times \mathfrak{g}$ such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(bx + cy),\ \Theta_P = dx + ey. \tag{7.1.1}$$

Note that there is a natural decomposition $u(\mathfrak{g}) = u(\mathfrak{g})_{\geq 2} \oplus \mathfrak{g} \oplus \mathbf{k}$. We say P belongs to S_T if and only if

(i) a, b, c are not all zero,

(ii) $\boldsymbol{\Phi}_z(\chi_p) = \Psi_P \times 1 + 1 \otimes \Psi_P - \Delta(\Psi_P)$,

(iii) $\rho_z(\Psi_P + \Theta_P) = 0$,

for some $\Psi_P \in u(\mathfrak{g})_{\geq 2}$. Note that Ψ_P is uniquely determined by χ_P. Next we identify $\mathfrak{g}$ with $\mathbb{A}^2$ and define an equivalence relation $\sim$ in $\mathbb{A}^2$ such that $\alpha \sim \beta$ if and only if $\alpha - \beta = \boldsymbol{\Phi}_z(\Theta)$ for some $\Theta \in \mathbb{A}^2$. By Proposition 6.5.1, $\mathcal{H}^2(T)$ can be naturally realized as the image of S_T under the quotient map

$$\mathbb{A}^3 \times \mathbb{A}^2 \overset{\pi}{\twoheadrightarrow} \mathbb{A}^3 \times (\mathbb{A}^2/\sim).$$

Finally, we will explain the group action. Let ϕ be any element in the automorphism group $\mathrm{Aut}(T)$. By definition, ϕ consists of two automorphisms of restricted Lie algebras for $\mathfrak{g}$ and $\mathfrak{h}$, which we still denote by ϕ. And the following compatible conditions hold:

$$\rho_{\phi(z)}\left[\phi(x)\right] = \phi\left[\rho_z(x)\right],\ \rho_{\phi(z)}\left[\phi(y)\right] = \phi\left[\rho_z(y)\right].$$

Suppose $\phi(z) = \gamma z$ for some $\gamma \in \mathbf{k}^{\times}$. We can realize the Aut$(T)$-action via S_T and the quotient map π. Consider ϕ acts on the point $P \in S_T$ as in (7.1.1). Set up

$$\chi = \gamma^{-1} a\phi(x) \otimes \phi(y) + \boldsymbol{\omega}\left[\gamma^{-\frac{1}{p}}\phi(bx+cy)\right],\ \Theta = \gamma^{-p}\phi\left(\Psi_P + \Theta_P\right).$$

Then we can rewrite $(\chi, \Theta) = (\chi_Q, \Theta_Q + \Psi_Q) + (d^1(\sigma), \boldsymbol{\Phi}_z(\sigma))$ for some $Q \in S_T$ and $\sigma \in u(\mathfrak{g})^+$. Therefore, the group element ϕ maps P to Q in S_T via ϕ, which factors through the quotient map π. We summarize some facts regrading the calculation of S_T:

- Suppose Im$\boldsymbol{\Phi}_z$ on $\mathfrak{g}$ is a subspace spanned by x or y, then we can consider $\mathcal{H}^2(T)$ as a subset of $\mathbb{A}^5$ by taking the corresponding coefficient in Θ_P to be zero via the quotient map.

- To find the z-characteristic element χ_P, we use its definition such that $\boldsymbol{\Phi}_z(\chi_P) = \chi^P - \lambda\chi_P + \rho_z^{p-1}(\chi_P) = 0$. By Lemma 6.5.2, ρ_z acts on $\boldsymbol{\omega}(bx+cy)$ trivially.

- By Lemma 6.5.5, when Im$\boldsymbol{\Phi}_z$ = Kerρ_z in $\mathfrak{g}$, we can take Θ_P to be a fixed element of $\mathfrak{g}$ and consider S_T as a subset of $\mathbb{A}^3$.

7.2 Classification of all types

In this section, we classify all possible types $T = (\mathfrak{g}, \mathfrak{h}, \rho)$. For two-dimensional restricted Lie algebra $\mathfrak{g}$, there are 4 isomorphism classes:

(A) $x^p = 0, y^p = 0,$

(B) $x^p = 0, y^p = 0,$

(C) $x^p = y, y^p = 0,$

(D) $x^p = x, y^p = x.$

For one-dimensional restricted Lie algebra $\mathfrak{h}$, there are two isomorphism classes:

(N) $z^p = 0,$

(S) $z^p = z$.

Then for each combination, we need to figure out the algebraic representation ρ accordingly. Because $\mathfrak{h}$ is one-dimensional, the representation ρ is uniquely determined by ρ_z, which can be denoted by a 2×2-matrix M such that

$$\rho_z \begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}.$$

Let $\mathfrak{g} = A$ and $\mathfrak{h} = N$. We know $(\rho_z)^p = \rho_{z^p} = 0$, so $M^p = 0$. After a linear transformation of the basis x, y, we can assume that $M = 0$ or $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. By the similar arguments, we get the following classification of all the possible types:

(T1) $\mathfrak{g} = A, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T2) $\mathfrak{g} = A, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$,

(T3) $\mathfrak{g} = A, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T4) $\mathfrak{g} = A, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ for $\lambda \in \mathbb{F}_p$. Two λ, λ' give isomorphic ones if and only if $\lambda = \lambda'$ or $\lambda = 1/\lambda'$ provided $\lambda' \neq 0$,

(T5) $\mathfrak{g} = B, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T6) $\mathfrak{g} = B, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$,

(T7) $\mathfrak{g} = B, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, (T8) $\mathfrak{g} = B, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$,

(T9) $\mathfrak{g} = B, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$,

(T10) $\mathfrak{g} = C, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T11) $\mathfrak{g} = C, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$,

(T12) $\mathfrak{g} = C, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T13) $\mathfrak{g} = C, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$,

(T14) $\mathfrak{g} = C, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$,

(T15) $\mathfrak{g} = D, \mathfrak{h} = N, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

(T16) $\mathfrak{g} = D, \mathfrak{h} = S, \rho_z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Proposition 7.2.1. *For types (T3), (T12), (T15) and the special case $\lambda = -1$ in (T4), we have the set $\mathcal{H}^2(T)$ is empty.*

Proof. According to Proposition 6.5.1, it suffices to show that the only z-characteristic element in $\mathrm{H}^2(\Omega u(\mathfrak{g}))$ is zero for all the types in the statement. In the following, let $\chi = ax \otimes y + \boldsymbol{\omega}(bx + cy)$ for some coefficients $a, b, c \in \mathbf{k}$.

For (T3), $\mathbf{\Phi}_z(\chi) = \chi^p - \chi + \rho_z^{p-1}(\chi) = -\chi = 0$. Then $a = b = c = 0$.

For (T4) when $\lambda = -1$, $\mathbf{\Phi}_z(\chi) = \chi^p - \chi + \rho_z^{p-1}(\chi) = -\chi + \rho_z^{p-1}(ax \otimes y) = -\chi = 0$. Hence $a = b = c = 0$.

For (T12), $\mathbf{\Phi}_z(\chi) = \chi^p - \chi + \rho_z^{p-1}(\chi) = \boldsymbol{\omega}(b^p y) - ax \otimes y - \boldsymbol{\omega}(bx + cy) = 0$. Hence $a = b = c = 0$.

For (T15), $\mathbf{\Phi}_z(\chi) = \chi^p - \chi + \rho_z^{p-1}(\chi) = a^p x \otimes y + \boldsymbol{\omega}(b^p x + c^p y) = 0$. Hence $a = b = c = 0$. ■

7.3 Classification according to different types

For each type T in the classification above, we identify the set $\mathcal{H}^2(T)$ with the subset S_T in $\mathbb{A}^5$ via the quotient map. Moreover, direct computation shows that $\mathrm{Im}\mathbf{\Phi}_z$ on $\mathfrak{g}$ can only be 0, the entire space, or the subspace spanned by x or y. Hence in the equivalence classes of $\mathbb{A}^2$ by $\sim$, we can represent any point (d, e) of $\mathbb{A}^2$ by $(d, e), (0, 0), (0, e), (d, 0)$ accordingly. So we can consider $\mathcal{H}^2(T)$ as a subset of $\mathbb{A}^n$ with $n \leq 5$.

For the automorphism group, we know $\mathrm{Aut}(T)$ is a subgroup of $\mathrm{GL}(\mathbf{k}) \times \mathbf{k}^\times$. Any element ϕ of $\mathrm{Aut}(T)$ can be written as

$$\begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} \times \gamma.$$

Let P be a point of $\mathcal{H}^2(T)$ represented by $(a, b, c, d, e) \in \mathbb{A}^5$. The group action of ϕ is given by

$$\begin{aligned}
&\phi\left(\chi_P\right) \\
&= \gamma^{-1}(\phi \otimes \phi)\left[ax \otimes y + \boldsymbol{\omega}(bx + cy)\right] \\
&= \gamma^{-1} a \det \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} x \otimes y + \boldsymbol{\omega}\left[\gamma^{-\frac{1}{p}}(bx, cy) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix}\right] - d^1\left[\gamma^{-1} a (\frac{1}{2}\alpha\sigma x^2 + \beta\sigma xy + \frac{1}{2}\beta\tau y^2)\right],
\end{aligned}$$

and

$$\phi\left(\Psi_P + \Theta_P\right) = \gamma^{-p}\phi(\Psi_P) + \gamma^{-p}(dx, ey) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix}.$$

In the set $\mathcal{H}^2(T)$, the image of P under ϕ is equivalence to the point Q such that

$$\chi_Q = \gamma^{-1} a \det \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} x \otimes y + \boldsymbol{\omega} \left[\gamma^{-\frac{1}{p}} (bx, cy) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} \right],$$

and

$$\Psi_Q + \Theta_Q = \gamma^{-p} \phi(\Psi_P) + \gamma^{-p}(dx, ey) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} + \boldsymbol{\Phi}_z \left[\gamma^{-1} a (\frac{1}{2} \alpha\sigma x^2 + \beta\sigma xy + \frac{1}{2} \beta\tau y^2) \right].$$

Hence

$$\phi(a) = \gamma^{-1} \det \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} a, \ \phi(b,c) = \gamma^{-\frac{1}{p}} (b,c) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix},$$

and $\phi(d,e)$ are the corresponding coefficients of x, y in the linear part of

$$\gamma^{-p} \phi(\Psi_P) + \gamma^{-p}(dx, ey) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} + \boldsymbol{\Phi}_z \left[\gamma^{-1} a (\frac{1}{2} \alpha\sigma x^2 + \beta\sigma xy + \frac{1}{2} \beta\tau y^2) \right].$$

In particular if the following condition holds:

$$\gamma^{-p} \phi(\Psi_P) + \Phi_z \left[\gamma^{-1} a (\frac{1}{2} \alpha\sigma x^2 + \beta\sigma xy + \frac{1}{2} \beta\tau y^2) \right] \text{has zero linear part.} \tag{7.3.1}$$

Then we have the group action given by:

$$\phi[a,(b,c),(d,e)] = \left[\gamma^{-1} \det \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} a, \gamma^{-\frac{1}{p}} (b,c) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix}, \gamma^{-p}(d,e) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} \right].$$

In the following, we will compute the set $\mathcal{H}^2(T)$ and the group action of $\mathrm{Aut}(T)$ according to each type T in the classification.

Case (T1). We can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^5 \setminus \{(0,0,0,d,e) | d, e \in \mathbf{k}\}$. Any element of the automorphism group $\mathrm{Aut}(T)$ is denoted as

$$\phi = \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} \times \gamma \in \mathrm{GL}(2) \times \mathbf{k}^{\times}.$$

Let $[a,(b,c),(d,e)] \in \mathcal{H}^2(T)$. It is easy to check the Condition (7.3.1) holds. Then the group action is given by

$$\phi[a,(b,c),(d,e)] = \left[\gamma^{-1} \det \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} a, \gamma^{-\frac{1}{p}} (b,c) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix}, \gamma^{-p}(d,e) \begin{pmatrix} \alpha & \beta \\ \sigma & \tau \end{pmatrix} \right].$$

Therefore the orbits of $\mathcal{H}^2(T)/\mathrm{Aut}(T)$ contain 8 discrete points, which are represented by

$$P_1=(1,0,0,0,0),P_2=(1,0,0,1,0),P_3=(0,1,0,0,0),P_4=(0,1,0,1,0),$$
$$P_5=(0,1,0,0,1),P_6=(1,1,0,0,0),P_7=(1,1,0,1,0),P_8=(1,1,0,0,1).$$

The corresponding isomorphism classes are:

(i) $\chi = x\otimes y, \Theta=0$,

(ii) $\chi = x\otimes y, \Theta=x$,

(iii) $\chi = \boldsymbol{\omega}(x), \Theta=0$,

(iv) $\chi = \boldsymbol{\omega}(x), \Theta=x$,

(v) $\chi = \boldsymbol{\omega}(x), \Theta=y$,

(vi) $\chi = x\otimes y+\boldsymbol{\omega}(x), \Theta=0$,

(vii) $\chi = x\otimes y+\boldsymbol{\omega}(x), \Theta=x$,

(viii) $\chi = x\otimes y+\boldsymbol{\omega}(x), \Theta=y$.

Case (T2). We can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^4\setminus\{(0,0,0,d)|d\in\mathbf{k}\}$. Any point P in $\mathcal{H}^2(T)$ can be represented by (a,b,c,d) such that

$$\chi_P = ax\otimes y+\boldsymbol{\omega}(bx+cy)$$

and $\Psi_P=b^p xy^{p-1}, \Theta_P=dy$. The automorphism group is

$$\mathrm{Aut}(T)=\left\{\begin{pmatrix}\alpha & \beta\\ 0 & \alpha\gamma\end{pmatrix}\times\gamma\in \mathrm{GL}(2)\times\mathbf{k}^\times\right\}.$$

It is easy to check the Condition (7.3.1) holds. Then the group action is given by

$$\phi[a,(b,c),d]=\left[\alpha^2 a,\gamma^{-\frac{1}{p}}(b,c)\begin{pmatrix}\alpha & \beta\\ 0 & \alpha\gamma\end{pmatrix},\gamma^{-p+1}\alpha d\right].$$

As a consequence, the orbits of $\mathcal{H}^2(T)/\mathrm{Aut}(T)$ contain 6 discrete points and 2 lines represented by:

$$P_1 = (1,0,0,0), P_2 = (1,0,0,1), P_3 = (0,1,0,0), P_4 = (0,1,0,1),$$
$$P_5 = (0,0,1,0), P_6 = (0,0,1,1),$$

and

$$L_1 = (1,1,0,\lambda), L_2 = (1,0,1,\lambda).$$

The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0,$

(ii) $\chi = x \otimes y, \Theta = y,$

(iii) $\chi = \boldsymbol{\omega}(x), \Theta = xy^{p-1},$

(iv) $\chi = \boldsymbol{\omega}(x), \Theta = xy^{p-1} + y,$

(v) $\chi = \boldsymbol{\omega}(y), \Theta = 0,$

(vi) $\chi = \boldsymbol{\omega}(y), \Theta = y,$

(vii) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = xy^{p-1} + \lambda y$, parametrized by $\mathbf{k}/\{\pm 1\}$,

(viii) $\chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda y$, parametrized by $\mathbf{k}$.

Case (T4). Suppose $\lambda \neq -1$. We can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^1 \setminus \{0\}$. Any point P in $\mathcal{H}^2(T)$ is represented by some nonzero scalar $a \in \mathbf{k}$ such that

$$\chi_P = ax \otimes y,$$

and $\Psi_P = \Theta_P = 0$. Any element ϕ of the automorphism group $\mathrm{Aut}(T)$ is denoted as $(M, \gamma) \in \mathrm{GL}(2) \times \mathbf{k}^\times$. When $\lambda = 1$, then $\gamma = 1$; if $\lambda \neq 1$, then $\gamma = 1$ and M is diagonal. The group action is given by

$$\phi(a) = (\det M)a.$$

The orbits only has 1 point represented by: $a = 1$. The corresponding isomorphism class is:

(i) $\chi = x \otimes y, \Theta = 0$.

Case (T5). We can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^3 \setminus \{(0,0,c) | c \in \mathbf{k}\}$. Any point P in $\mathcal{H}^2(T)$ is represented by (a,b,c) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_p = 0, \Theta_p = cy$. Also we have $\mathrm{Aut}(T) = \mathbb{F}_p^\times \times \mathbf{k}^\times \times \mathbf{k}^\times$ and we can write any element ϕ of $\mathrm{Aut}(T)$ as $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \times \gamma$ where $\alpha \in \mathbb{F}_p^\times$ and $\beta, \gamma \in \mathbf{k}^\times$. Then the orbits consist of 4 points and 1 line represented by:

$$P_1 = (1,0,0), P_2 = (1,0,1), P_3 = (0,1,0), P_4 = (0,1,1),$$

and $L_1 = (1,1,\lambda)$. The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0$,

(ii) $\chi = x \otimes y, \Theta = y$,

(iii) $\chi = \boldsymbol{\omega}(y), \Theta = 0$,

(iv) $\chi = \boldsymbol{\omega}(y), \Theta = y$,

(v) $\chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda y$, parametrized by $\mathbf{k} / \sqrt[\frac{p-1}{2}]{1}$.

Case (T6). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$ on $\mathfrak{g}$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^2 \setminus \{(0,0)\}$. Any point P of $\mathcal{H}^2(T)$ can be represented by (a,b) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_P = b^p x^{p-1} y, \Theta_P = -b^p y$. We have the automorphism group

$$\mathrm{Aut}(T) = \left\{ \begin{pmatrix} \beta\gamma & 0 \\ 0 & \beta \end{pmatrix} \times \gamma \middle| \beta, \gamma \in \mathbf{k}^\times, \beta\gamma \in \mathbb{F}_p^\times \right\}.$$

Choose any $\phi \in \mathrm{Aut}(T)$. The group action is given by

$$\phi(a,b) = (\beta^2 a, \gamma^{-\frac{1}{p}}\beta b y).$$

The orbits consist of 1 point and 1 line represented by: $P_1 = (1,0)$ and $L_1 = (\lambda, 1)$. The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0$,

(ii) $\chi = \lambda x \otimes y + \boldsymbol{\omega}(y), \Theta = (x^{p-1} - 1)y$, parametrized by $\mathbf{k}/\sqrt[\frac{p^2-1}{2}]{1}$.

Case (T7). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$ on $\mathfrak{g}$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{F}_p^\times$. Any point P in $\mathcal{H}^2(T)$ is represented by some nonzero scalar $a \in \mathbb{F}_p$ such that

$$\chi_P = \boldsymbol{\omega}(ax),$$

and $\Psi_P = \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathbb{F}_p^\times \times \mathbf{k}^\times \times \mathbb{F}_p^\times$ and we can write any element of $\mathrm{Aut}(T)$ as

$$\phi = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \times \gamma,$$

where $\alpha, \gamma \in \mathbb{F}_p^\times, \beta \in \mathbf{k}^\times$. The group action is given by

$$\phi(a) = \gamma^{-\frac{1}{p}}\alpha a.$$

The orbits only has 1 point represented by: $a = 1$. The corresponding isomorphism class is:

(i) $\chi = \boldsymbol{\omega}(x), \Theta = 0$.

Case (T8). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$ on $\mathfrak{g}$, we can identify $\mathcal{H}^2(T)$ with $\mathbf{k} \times \mathbb{F}_p \setminus \{(0,0)\}$. Any point P in $\mathcal{H}^2(T)$ is represented by (a,b) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_P = \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathbb{F}_p^\times \times \mathbf{k}^\times$ and we can write any element of $\mathrm{Aut}(T)$ as

$$\phi = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \times 1,$$

where $\alpha \in \mathbb{F}_p^\times, \beta \in \mathbf{k}^\times$. The group action is given by:

$$\phi(a, b) = (\alpha\beta a, \alpha b).$$

The orbits consist of three points represented by:

$$P_1 = (1, 0), P_2 = (0, 1), P_3 = (1, 1).$$

The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0,$

(ii) $\chi = \boldsymbol{\omega}(x), \Theta = 0,$

(iii) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = 0.$

Case (T9). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$ on $\mathfrak{g}$, we can identify $\mathcal{H}^2(T)$ with $\mathbf{k} \times \mathbb{F}_p \setminus \{(0, 0)\}$. Any point P in $\mathcal{H}^2(T)$ is represented by (a, b) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_P = -\frac{a}{2}x^2, \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathbb{F}_p^\times$ and we can write any element of $\mathrm{Aut}(T)$ as

$$\phi = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \times 1,$$

where $\alpha \in \mathbb{F}_p^\times$. The group action is given by:

$$\phi(a, b) = (\alpha^2 a, \alpha b).$$

The orbits consist of two lines represented by:

$$L_1 = (\lambda, 0), L_2 = (\lambda, 1).$$

The corresponding isomorphism classes are:

(i) $\chi = \lambda x \otimes y, \Theta = -\frac{\lambda}{2}x^2$, parametrized by $\mathbf{k}/(\mathbb{F}_p^\times)^2$,

(ii) $\chi = \lambda x \otimes y + \boldsymbol{\omega}(x), \Theta = -\frac{\lambda}{2}x^2$, parametrized by $\mathbf{k}$.

Case (T10). We can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^3 \setminus \{(0,0,c)|c \in \mathbf{k}\}$. Any point P in $\mathcal{H}^2(T)$ is represented by (a,b,c) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_P = 0, \Theta_P = cx$. We have the automorphism group

$$\mathrm{Aut}(T) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} \times \gamma \in \mathrm{GL}(2) \times \mathbf{k}^\times \right\}.$$

It is easy to check the Condition (7.3.1) holds. Then the group action for any $\phi \in \mathrm{Aut}(T)$ is given by:

$$\phi(a,b,c) = (\gamma^{-1}\alpha^{p+1}a, \gamma^{-\frac{1}{p}}\alpha^p b, \gamma^{-p}\alpha^p c).$$

The orbits consist of 4 points and 1 line represented by:

$$P_1 = (1,0,0), P_2 = (1,0,1), P_3 = (0,1,0), P_4 = (0,1,1),$$

and $L_1 = (1,1,\lambda)$. The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0$,

(ii) $\chi = x \otimes y, \Theta = x$,

(iii) $\chi = \boldsymbol{\omega}(y), \Theta = 0$,

(iv) $\chi = \boldsymbol{\omega}(y), \Theta = x$,

(v) $\chi = x \otimes y + \boldsymbol{\omega}(y), \Theta = \lambda x$, parametrized by $\mathbf{k}/\sqrt[p^2-p-1]{1}$.

Case (T11). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\boldsymbol{\Phi}_z$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^2 \setminus \{(0,0)\}$. Any point P in $\mathcal{H}^2(T)$ is represented by (a,b) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(by),$$

and $\Psi_P = \Theta_P = 0$. We have the automorphism group

$$\mathrm{Aut}(T) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^p \end{pmatrix} \times \alpha^{p-1} \in \mathrm{GL}(2) \times \mathbf{k}^\times \right\}.$$

Then the group action for any $\phi \in \mathrm{Aut}(T)$ is given by:

$$\phi(a, b, c) = (\alpha^2 a, \alpha^{\frac{p^2-p+1}{p}} b).$$

The orbits consist of 1 point and 1 line represented by

$$P_1 = (1, 0), L_1 = (\lambda, 1).$$

The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0$,

(ii) $\chi = \lambda x \otimes y + \boldsymbol{\omega}(y), \Theta = 0$, parametrized by $\mathbf{k}/\sqrt[p^2-p+1]{1}$.

Case (T13). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\Phi_z$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^1 \setminus \{0\}$. Any point P in $\mathcal{H}^2(T)$ is represented by some nonzero scalar a such that

$$\chi_P = a x \otimes y,$$

and $\Psi_P = \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathbf{k}^\times$ and we can write any element $\phi \in \mathrm{Aut}(T)$ as

$$\phi = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix} \times 1 \in \mathrm{GL}(2) \times \mathbf{k}^\times.$$

Then the group action is given by:

$$\phi(a) = \alpha^{p+1} a.$$

The orbits consist of 1 point represented by: $a = 1$. The corresponding isomorphism class is:

(i) $\chi = x \otimes y, \Theta = 0$.

Case (T14). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\mathbf{\Phi}_z$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{A}^1 \setminus \{0\}$. Any point P in $\mathcal{H}^2(T)$ is represented by some nonzero scalar a such that

$$\chi_P = ax \otimes y,$$

and $\Psi_P = -\frac{1}{2}y^2, \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathbf{k}^\times$ and we can write any element $\phi \in \mathrm{Aut}(T)$ as

$$\phi = \begin{pmatrix} \alpha & \alpha - \alpha^p \\ 0 & \alpha^p \end{pmatrix} \times 1 \in \mathrm{GL}(2) \times \mathbf{k}^\times.$$

Then the group action is given by:

$$\phi(a) = \alpha^{p+1}a.$$

The orbits consist of 1 point represented by: $a = 1$. The corresponding isomorphism class is:

(i) $\chi = x \otimes y, \Theta = -\frac{1}{2}y^2$.

Case (T16). Since $\mathrm{Ker}\rho_z = \mathrm{Im}\mathbf{\Phi}_z$, we can identify $\mathcal{H}^2(T)$ with $\mathbb{F}_p^3 \setminus \{(0,0,0)\}$. Any point P of $\mathcal{H}^(T)$ is represented by (a, b, c) such that

$$\chi_P = ax \otimes y + \boldsymbol{\omega}(bx + cy)$$

and $\Psi_P = \Theta_P = 0$. The automorphism group is $\mathrm{Aut}(T) = \mathrm{GL}(2, \mathbb{F}_p) \times \mathbb{F}_p^\times$. And we can write any element $\phi \in \mathrm{Aut}(T)$ as $(M, \gamma) \in \mathrm{GL}(2, \mathbb{F}_p) \times \mathbb{F}_p^\times$. Then the group action is given by

$$\phi[a, (b, c)] = \left[\gamma^{-1}(\det M)a, \gamma^{-1}(b, c)M\right].$$

The orbits consist of 3 points represented by

$$P_1 = (1, 0, 0), P_2 = (0, 1, 0), P_3 = (1, 1, 0).$$

The corresponding isomorphism classes are:

(i) $\chi = x \otimes y, \Theta = 0$,

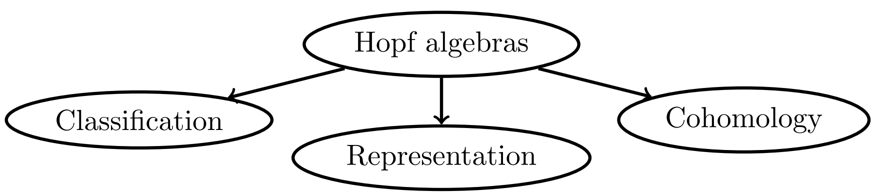
(ii) $\chi = \boldsymbol{\omega}(x), \Theta = 0$,

(iii) $\chi = x \otimes y + \boldsymbol{\omega}(x), \Theta = 0$.

Chapter 8

OPEN QUESTIONS AND FUTURE PROJECTS

In the last chapter, we are going to ask several questions concerning our classification and propose some related future projects. First of all, we like to classify the remaining case when $p = 2$ for p^3-dimensional connected Hopf algebras whose primitive space is a two-dimensional abelian restricted Lie algebra. Regarding classification of higher dimensional connected Hopf algebras, I want to pay special attention to those connected ones that are almost primitively generated and understand their algebra structures. Then, I like to study the irreducible representations of Hopf algebras of dimension p^n for small n. Finally, I want to compute the cohomology ring of non-commutative and non-cocommutative Hopf algebras in positive characteristic. The future projects can be summarized in the following three directions.



8.1 Classification

The classification of finite-dimensional connected Hopf algebras contains the classification of the following objects as special cases:

(1) p-groups in group theory,

(2) finite unipotent group schemes in algebraic geometry,

(3) finite-dimensional restricted Lie algebras in Lie theory.

Since none of the three above cases' classification are well known, there is little hope to completely classify all finite-dimensional connected Hopf algebras. However, I propose three sub-projects which are more practical and all of them have connections with other people's research. Let H be any finite-dimensional connected Hopf algebra over $\mathbf{k} = \overline{\mathbf{k}}$ and char$\mathbf{k} = p > 0$.

Definition 23. Suppose $\dim H = p^n$ for some integer $n \geq 1$. We say that H is **almost primitively generated** if $\dim \mathrm{P}(H) = n - 1$.

Recall that in Chapter 6, all H that are almost primitively generated are classified provided $\mathrm{P}(H)$ is an abelian restricted Lie algebra. Hence, I want to complete the classification in this case as continuous work.

Project A: Classify all H that are almost primitively generated and $\mathrm{P}(H)$ is not abelian.

The results are known for dimension $\leq p^3$ by Theorem 1.0.4, and it is open for dim $\geq p^4$. Through this sub-project, I believe that we can discover many interesting algebras. The second sub-project is related to the classification in characteristic zero. By [51, Corollary 4.25], any connected Hopf algebra of GK-dimension at most four is isomorphic, as an algebra, to some universal enveloping algebra. Moreover, the statement is confirmed [51, Theorem 0.5] for connected Hopf algebra A satisfying $\dim \mathrm{P}(A) = \text{GK-dim}A - 1 < \infty$. But we have the following fact in positive characteristic:

Fact: As an algebra, type (2) in Theorem 1.0.4 is not isomorphic to any restricted universal enveloping algebra.

Since the representation and cohomology ring of any Hopf algebra only depend on its algebra structure, it is natural to compare these Hopf algebras with restricted universal enveloping algebras.

Project B: Determine the condition when H is isomorphic, as an algebra, to some restricted universal enveloping algebra.

Another interesting direction is to study the structure of isomorphism classes. In Chapter 6, a one-to-one correspondence is constructed between isomorphism classes of connected Hopf algebras with large abelian primitive space and orbits of certain group actions on some geometric objects. Moreover, all infinite families of isomorphism classes for connected Hopf algebras of dimension at most p^3 are parametrized by finite group quotients of the affine line.

Project C: Classify parametric families in larger dimension and discover natural ways to describe them.

8.2 Representation

I am interested in the irreducible representations of Hopf algebras of dimension p^n in positive characteristic. In the following, we work over a base field $\mathbf{k} = \overline{\mathbf{k}}$.

Definition 24. A finite-dimensional algebra A is said to be of **Frobenius type** if every irreducible representation V satisfies $\dim V \,|\, \dim A$.

In characteristic zero, this Frobenius property is well known for Hopf algebras of dimension p and p^2 provided by their complete classification.

(1) In dimension p, it is equivalent to Kaplansky's eighth conjecture, which is proved by Zhu [61].

(2) In dimension p^2, it is proved by Masuoka (semisimple) [34] and Ng (non-semisimple) [38].

Moreover, it is confirmed for any Hopf algebra of dimension p^n in characteristic zero by Montgomery and Witherspoon [36].

In positive characteristic, we could ask the same question for p^n-dimensional Hopf algebras. For example, assume that the Hopf algebra H has dimension p. Etingof and Gelaki give a positive answer [20] when $\mathrm{char}\mathbf{k} > p$. And the question remains open in dimension p for $\mathrm{char}\mathbf{k} \leq p$. Furthermore, the property of being Frobenius type is closely related to the classification problem in low dimensions. It is easy to show that if the answer were affirmative, then every Hopf algebra of dimension p or p^2 would be pointed. Therefore, the classification of Hopf algebras in dimension p and p^2 will be complete [52] in positive characteristic.

Project D: Prove (or disprove) that any Hopf algebra of dimension p and p^2 in positive characteristic is of Frobenius type.

We can view Project D as a generalization of Kaplansky's eighth conjecture.

8.3 Cohomology

For a finite-dimensional Hopf algebra A, we can compute its cohomology ring $\mathrm{H}^\bullet(A, \mathbf{k}) := \mathrm{Ext}^\bullet_A(\mathbf{k}, \mathbf{k})$, which is conjectured to be always finitely generated. This conjecture has a long history and it has been verified in various special cases by many people.

(1) (Golod '59, Venkov '59, Evens '61): For finite groups over a field of positive characteristic.

(2) (Friedlander-Suslin '97): For finite group schemes over a field of positive characteristic. Equivalently, this holds for finite dimensional co-commutative Hopf algebras.

(3) (Ginzburg-Kumar '93, Bendel-Nakano-Parshall-Pillen '07): For finite dimensional (Lusztig's) small quantum groups $u_q(\mathfrak{g})$ over $\mathbb{C}$.

(4) (Mastnak-Pevtsova-Schauenburg-Witherspoon '10): More generally, for finite-dimensional pointed Hopf algebras (under some assumptions) over $\mathbb{C}$ classified by Andruskiewitsch and Schneider.

Recently, Etingof and Ostrik have generalized it to a conjecture about finite tensor categories [21]. For this finite generation conjecture, little has been done for non-commutative and non-cocommutative Hopf algebras in positive characteristic. However, in the thesis we find a lot of new examples belonging to this set. They are

(1) type (B4) Radford algebra in [52],

(2) type (3) Hopf algebra in Theorem 1.0.4,

(3) many p^3-dimensional connected Hopf algebras with two-dimensional abelian primitive space classified in Theorem 1.0.6,

(4) pointed rank one Hopf algebras in positive characteristic classified by Scherotzke [40].

Project E: Compute the cohomology rings of such non-commutative and non-cocommutative Hopf algebras.

In the following, assume that $\mathbf{k} = \overline{\mathbf{k}}$ and $\mathrm{char}\mathbf{k} = p > 2$. Recall the Nichols algebra A from [15, Corollary 3.14]:

$$A = \mathbf{k}\langle a, b\rangle/(a^p, b^p, ba - ab - \frac{1}{2}a^2).$$

The augmentation of A is given by $\epsilon(a) = \epsilon(b) = 0$. We denote the semisimple Hopf algebra $K = \mathbf{k}[x]/(x^p - x)$, where x is primitive. Now A becomes a K-Hopf module algebra via

$$\delta_x(a) = a,\ \delta_x(b) = 0.$$

Then, it is clear to see that as an algebra, type (3) in Theorem 1.0.4 is isomorphic to the smash product $A\#K$. Since K is semisimple, we have $\mathrm{H}^\bullet(A\#K, \mathbf{k}) \cong \mathrm{H}^\bullet(A, \mathbf{k})^K$. We know that $\mathrm{H}^\bullet(A, \mathbf{k})$ is finitely generated; see for example [48]. Therefore, we only need to investigate the invariant ring of $\mathrm{H}^\bullet(A, \mathbf{k})$ under the semisimple K-action.

The idea of semisimple Hopf actions plays an important role in the computation of cohomology rings. A recent result of Etingof and Walton [22] says that over an algebraically closed field of characteristic zero if a commutative domain arises as a semsimple H-Hopf module algebra via an inner faithful H-action, then H must be a group algebra. They also conjecture in [22, Conjecture 5.3] that:

Conjecture: Suppose the base field $\mathbf{k}$ is algebraically closed of characteristic $p > 0$. If a semisimple Hopf algebra K coacts inner faithfully on a commutative domain A, then K is itself commutative.

If we consider the dual version of the above conjecture for the Hopf actions, it is equivalent to the statement that any finite-dimensional cosemisimple Hopf algebra inner faithfully acting on a commutative domain must be a group algebra. Note that in positive characteristic, cosemisimplicity and semisimplicity are generally not equivalent. Since we are concerned about semisimple Hopf actions, we state the similar conjecture for semisimple Hopf actions over a base field $\mathbf{k}$ algebraically closed of characteristic $p > 0$.

Conjecture F: If a semisimple Hopf algebra H inner faithfully acts on a commutative domain A, then H must be cocommutative.

By Masuoka's result of semisimple connected Hopf algebras in positive characteristic [34], it is easy to prove the above conjecture for the special case when H is semisimple connected in characteristic $p > 0$. Because $H \cong (\mathbf{k}G)^*$ for some p-group G, then $\mathbf{k}G$ coacts on A by duality. Then it is easy to show that the commutative domain A must be graded by an abelian group if the coaction is inner faithful.

BIBLIOGRAPHY

[1] N. Andruskiewitsch, On finite-dimensional Hopf algebras, preprint, arXiv:1403.7838.

[2] N. Andruskiewitsch and J. Devoto, Extensions of Hopf algebras, Algebra i Analiz 7 (1995), 17-52.

[3] N. Andruskiewitsch and H.-J. Schneider, Hopf algebras of order p^2 and braided Hopf algebras of order p, J. Algebra, 199 (1998), 430-454.

[4] N. Andruskiewitsch and H.-J. Schneider, Lifting of quantum linear spaces and pointed Hopf algebras of order p^3, J. Algebra, 209 (1998), 658-691.

[5] N. Andruskiewitsch and H.-J. Schneider, Finite quantum groups and Cartan matrices, Adv. Math. 154 (2000) 1-45.

[6] N. Andruskiewitsch and H.-J. Schneider, Pointed Hopf algebras, in: S. Montgomery, H.J. Schneider (Eds.), New Directions in Hopf Algebras, Cambridge University Press, Cambridge pp. 1-68.

[7] M. Beattie, A survey of Hopf algebras of low dimension, Acta Appl. Math. 108 (2009), 19-31.

[8] M. Beattie and G. Garcia, Techniques for classifying Hopf algebras and applications to dimension p^3, Comm. Algebra 41 (2013), 3108-3129.

[9] M. Beattie and G. Garcia, Classifying Hopf algebras of a given dimension, Contemp. Math. 585 (2013), 125-152.

[10] G. Bergman, The diamond lemma for ring theory, Adv. Math. 29 (1978), 178-218.

[11] R.J. Blattner and S. Montgomery, Crossed products and Galois extensions of Hopf algebras, Pacific J. Math. 137 (1989), 37-54.

[12] K. A. Brown, S. O'Hagan, J.J. Zhang and G. Zhuang, Connected Hopf algebras and iterated Ore extensions, preprint, arXiv:1308.1998.

[13] K.A. Brown and J.J. Zhang, Prime regular Hopf algebras of GK-dimension one, Proc. London Math. Soc. (3) 101 (2010), 260-302.

[14] S. Caenepeel and S. Dascalescu, Pointed Hopf algebras of dimension p^3, J. Algebra 209 (1998), 622-634.

[15] C. Cibils, A. Lauve and S. Witherspoon, Hopf quivers and Nichols algebras in positive characteristic, Proc. Amer. Math. Soc. 137 (2009), 4029-4041.

[16] Y.-L. Cheng and S.-H. Ng, On Hopf algebras of dimension $4p$, J. Algebra, 328 (2011), 399-419.

[17] S. Dăscălescu, C. Năstăsescu and Ş. Raianu, Hopf algebra: An introduction, vol. 235, Marcel Dekker, New York (2001).

[18] M. Demazure and A. Grothendieck et coll. Schémas en groupes I-III (SGA3) Lecture Notes in Math. vol. 151-153 Springer-Verlag, 1970.

[19] M. Demazure and P. Gabriel, Groupes algébriques I, North Hollad, Amsterdam, 1970.

[20] P. Etingof and S. Gelaki, On finite-dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, Internat. Math. Res. Notices, 16 (1998), 851-864.

[21] P. Etingof and V. Ostrik, Finite tensor categories, Mosc. Math. J, 4 (2004), 627-654.

[22] P. Etingof and C. Walton, Semisimple Hopf actions on commutative domains, (to appear) Adv. Math. 2014, arXiv:1301.4161.

[23] Y. Félix, S. Halperin and J.C. Thomas, Rational Homotopy Theory, Springer-Verlag GTM 205, 2001.

[24] K.R. Goodearl and J.J. Zhang, Noetherian Hopf algebra domains of Gelfand-Kirillov dimension two, J. Algebra 324 (2010), Special Issue in Honor of Susan Montgomery, 3131-3168.

[25] M. Hazewinkel, Witt Vectors. I. Handbook of algebra. vol. 6, Amsterdam: Elsevier/North-Holland, 319-472 (2009).

[26] G.D. Henderson, Low-dimensional cocommutative connected Hopf algebras, J. Pure Appl. Algebra 102 (1995), 173-193.

[27] G. Hochschild, Representations of restricted Lie algebras of characteristic p, Proc. AMS 5 (1954), 603-605.

[28] J.E. Humphreys, Introduction to Lie algebras and representation theory, vol. 9, Springer,1980.

[29] I.M. Isaacs, Algebra: a graduate course, Brooks/Cole Publishing, Pacific Grove, 1994.

[30] N. Jacobson, Lie Algebras, Dover Publications Inc., New York, 1979.

[31] R.G. Larson and D.E. Radford, An associative orthogonal bilinear form for Hopf algebras, J. Algebra 91 (1969), 75-93.

[32] A. Masuoka, Coideal subalgebras in finite Hopf algebras, J. Algebra 163 (1994), 819-831.

[33] A. Masuoka, The p^n theorem for semisimple Hopf algebras, Proc. Amer. Math. Soc. 124 (1996), 735-738.

[34] A. Masuoka, Semisimplicity criteria for irreducible Hopf algebras in positive characteristic, Proc. AMS 137 (2009), 1925-1932.

[35] S. Montgomery, Hopf Algebras and Their Actions on Rings, Amer. Math. Soc. 82 (1993).

[36] S. Montgomery and S. Witherspoon, Irreducible representations of crossed products, J. Pure. Appl. Alg. 129 (1998), 315-326.

[37] W.D. Nichols and M.B. Zoeller, A Hopf algebra freeness theorem, Amer. J. Math. 111 (1989), 381-385.

[38] S.-H. Ng, Non-semisimple Hopf algebras of dimension p^2, J. Algebra, 255 (2002), 182-197.

[39] D. Quillen, The spectrum of an equivalent cohomology ring: I, Ann. Math. 94 (1971), 549-572.

[40] S. Scherotzke, Classification of pointed rank one Hopf algebras, J. Alg. 319 (2008), 2889-2912.

[41] H.J. Schneider, Normal basis and transitivity of crossed products for Hopf algebras, J. Algebra 152 (1992), 289-312.

[42] W.M. Singer, Extension theory for connected Hopf algebras, J. Algebra 21 (1972), 1-16.

[43] D. Ştefan, Hopf subalgebras of pointed Hopf algebras and applications, Proc. Amer. Math. Soc. 125 (1997), 3191-3194.

[44] D. Ştefan and F.V. Oystaeyen, Hochschild cohomology and the coradical filtration of pointed coalgebras: applications. J. Algebra 210 (1998), 535-556.

[45] H. Strade and R. Farnsteiner, Modular Lie algebras and their representations, Monogr. Textbook Pure Appl. Math. 116 (1988) Marcel Dekker, New York and Basel.

[46] M.E. Sweedler, Hopf algebras, Benjamin, New York, 1969.

[47] M. Takeuchi, Free Hopf algebras generated by coalgebras, J. Math. Soc. Jan. 23 (1971), 561-582.

[48] V. Nguyen and S. Witherspoon, Finite generation of the cohomology of some skew group algebras, preprint, arXiv:1310.0724.

[49] D.-G. Wang, J.J. Zhang and G. Zhuang, Coassociative Lie algebras, Glasg. Math. J. 55A (2013), 195-215.

[50] D.-G. Wang, J.J. Zhang and G.-B. Zhuang, Lower bounds of Growth of Hopf algebras, Trans. Amer. Math. Soc. 365 (2013), 4963-4986.

[51] D.-G. Wang, J.J. Zhang and G. Zhuang, Connected Hopf algebras of Gelfand-Kirillov dimension four, to appear Trans. Amer. Math. Soc. preprint arXiv1302.2270.

[52] L. Wang and X. Wang, Classification of pointed Hopf algebras of dimension p^2 over any algebraically closed field, Algebr. Represent. Theory, 17 (2014), no.4, 1267-1276.

[53] L. Wang and X. Wang, Classification of connected Hopf algebras of dimension p^3 I, preprint arXiv:1212.5626.

[54] X. Wang, Isomorphism classes of finite dimensional connected Hopf algebras in positive characteristic, preprint arXiv:1310.7073.

[55] X. Wang, Another proof of Masuoka's Theorem for semisimple irreducible Hopf algebras, arXiv:1212.0622.

[56] X. Wang, Connected Hopf algebras of dimension p^2, J. Algebra 391 (2013), 93-113.

[57] X. Wang, Local criteria for cocommutative Hopf algebras, Comm. Algebra, 42 (2014), no. 12, 5180-5191.

[58] X. Wang,Isomorphism classes of finite dimensional connected Hopf algebras in positive characteristic, preprint arXiv:1310.7073.

[59] W.C. Waterhouse, Introduction to affine group schemes, vol. 66, Springer, 1979.

[60] C. Weibel, An introduction to homological algebra, Cambridge University Press, Cambridge (1994).

[61] Y. Zhu, Hopf algebras of prime dimension, Internat. Math. Res. Notices, 1 (1994), 53-59.

[62] G. Zhuang, Existence of Hopf subalgebras of GK-dimension two, J. Pure Appl. Algebra 215 (2011), 2912-2922.

[63] G. Zhuang, Properties of connected Hopf algebras of finite Gelfand-Kirillov dimension, J. London Math. Soc. 87 (2013), 877-898.