Pointed and ambiskew Hopf algebras

by

Monica Macauley

A thesis submitted to the
Faculty of Information and Mathematical Sciences
at the University of Glasgow
for the degree of
Doctor of Philosophy

May 2010

Abstract

This thesis is concerned with properties of pointed Hopf algebras: that is, Hopf algebras whose coradicals are the group algebras of their grouplike elements. These have been fruitfully studied via their associated graded Hopf algebras with respect to the coradical filtration. In fact, the associated graded Hopf algebra $\operatorname{gr} H$ of a pointed Hopf algebra H can be decomposed into a braided graded Hopf algebra of coinvariants adjoined to a group algebra by a process called bosonisation.

Chapter 1 consists of background material, which fully explains the process outlined above.

In Chapter 2, we outline and discuss the main results of Kharchenko in [32], which gives a PBW-basis for a certain class of associated graded Hopf algebras $\operatorname{gr} H$ of pointed Hopf algebras H. The hypotheses on $\operatorname{gr} H$ are that its grouplikes form an abelian group that acts on the braided Hopf algebra of coinvariants diagonalisably - that is, by multiplication by scalars, which are called the braiding coefficients. In Theorem 2.4.1, we give an expanded proof of [32, Corollary 5].

This provides a tool which we use in Chapter 3 to show that the ordering of the PBW-generators in Kharchenko's PBW-basis for $\operatorname{gr} H$ may be permuted in the case where there are only a finite number of generators. We then use this in order to prove that $\operatorname{gr} H$, and hence H, satisfy certain homological properties.

In Chapter 4, we prove a result giving sufficient conditions on the braiding coefficients for the braided Hopf algebra of coinvariants to be a free algebra, thus answering a question of Andruskiewitsch and Schneider in [2].

Chapter 5 switches the focus to a type of skew-polynomial algebras called ambiskew polynomial algebras, defined over a base algebra R. We drop the hypothesis that R is commutative, which was generally assumed in previous work on these algebras. We then give necessary and sufficient conditions for a Hopf algebra structure on R to be extended to a Hopf algebra structure on the ambiskew polynomial algebra, generalising work of Hartwig in [22]. We also calculate explicitly their coradical filtration, which gives as a corollary some theorems of Montgomery [43] and Boca [11] on the coradical filtration of $U_q(\mathfrak{sl}_2)$. Finally, we consider some homological and ring-theoretic properties of ambiskew polynomial algebras.

Acknowledgements

I would like to thank my supervisor, Ken Brown, for his invaluable advice and encouragement throughout my studies. This thesis would not have been possible without his help and patience. I am also grateful to the EPSRC for providing financial support and to the University of Glasgow Mathematics department for funding my attendance at several conferences.

There are many people who have made my time at the Mathematics department such a pleasure. They include Uli Krähmer, for his helpful comments on my work, and Marjory Macleod, for her assistance on numerous occasions. Thanks are also due to my fellow postgraduates, especially my office-mates: Susan, Robert, Ehsan, Yunfei and Stephen, for providing welcome distractions.

My special thanks go to my family - Mum, Dad and Gavin - and to Craig, for their constant love and support.

Statement

This thesis is submitted in accordance with the regulations for the degree of Doctor of Philosophy at the University of Glasgow.

Chapters 1 and 2 cover background material and known results. The results in later chapters are the author's own work, with the exception of results which are explicitly referenced.

Contents

1 Introduction **1**

1.1 Preliminaries . . . 1

1.1.1 Notation and conventions . . . 1

1.1.2 Filtrations and gradings of Hopf algebras . . . 2

1.1.3 Skew (Laurent) polynomial rings . . . 5

1.1.4 Skew group rings . . . 6

1.2 Quantised enveloping algebras . . . 6

1.2.1 Gaussian binomial coefficients . . . 6

1.2.2 The definition . . . 7

1.3 Pointed Hopf algebras . . . 8

1.3.1 Definition and examples . . . 8

1.3.2 Braided vector spaces and Yetter-Drinfeld modules . . . 9

1.3.3 Braided Hopf algebras . . . 11

1.3.4 Bosonisation . . . 12

1.3.5 Decomposition of pointed Hopf algebras . . . 13

2 A PBW-basis for diagonal Nichols algebras **16**

2.1 Lyndon words . . . 16

2.2 Brackets in the free algebra . . . 19

2.2.1 General definition . . . 19

2.2.2 Skew-commutators . . . 21

2.3 Constructing the PBW-basis . . . 25

2.4 A condition ensuring that H is noetherian . . . 29

3 Homological properties of pointed Hopf algebras **38**

3.1 Re-ordering the PBW-basis . . . 38

3.1.1 Some technical lemmas about hard super-letters . . . 39
3.1.2 Proof of the theorem: transposition case . . . 41
3.1.3 Proof of the theorem: general case . . . 42
3.2 Homological and other properties . . . 45
3.2.1 Global dimension . . . 46
3.2.2 GK dimension . . . 49
3.2.3 The Auslander-Gorenstein property . . . 51
3.2.4 The Cohen-Macaulay property . . . 53
3.2.5 AS-Gorenstein . . . 56
3.2.6 Values for global and injective dimensions . . . 56
3.2.7 Application to pointed Hopf algebras . . . 57

4 Diagonal Nichols algebras **59**
4.1 Nichols algebras . . . 60
4.2 Skew-derivations of graded coalgebras . . . 61
4.3 Skew-derivations in the diagonal braiding case . . . 65
4.4 Conditions implying $B(V) \cong T(V)$ . . . 70
4.4.1 Notation . . . 70
4.4.2 Main theorem . . . 71

5 Ambiskew Hopf algebras **79**
5.1 Definition . . . 79
5.2 Hopf algebra structure . . . 80
5.2.1 The main theorem . . . 80
5.2.2 Examples . . . 90
5.3 Coradical filtration . . . 94
5.3.1 Comultiplication formulas . . . 95
5.3.2 The filtration . . . 98
5.4 Properties of ambiskew polynomial algebras . . . 103
5.4.1 Homological properties . . . 103
5.4.2 Polynomial identity . . . 107

References **115**

Chapter 1

Introduction

We start by introducing some background material which will feature prominently throughout this thesis. In particular, we focus on pointed Hopf algebras, which are studied using filtered and graded techniques. The coradical filtration of a pointed Hopf algebra H is a Hopf algebra filtration, and the associated graded Hopf algebra $\operatorname{gr} H$ can be described as a bosonisation between a subalgebra of coinvariants and a group algebra. This technique greatly simplifies the problem of classifying pointed Hopf algebras.

1.1 Preliminaries

1.1.1 Notation and conventions

Throughout, k will denote a field and k^* will denote $k \setminus \{0\}$. All algebras, coalgebras and Hopf algebras are k-vector spaces, and the unadorned tensor product $\otimes$ denotes the tensor product over k.

If A is an algebra, we sometimes write $A = (A, m, u)$, where $m\colon A \otimes A \to A$ is the multiplication map and $u\colon k \to A$ is the unit map. We usually omit explicit labels for these maps, instead denoting $m(a \otimes b)$ by ab for all $a, b \in A$. For any coalgebra $C = (C, \Delta, \varepsilon)$, $\Delta\colon C \to C \otimes C$ and $\varepsilon\colon C \to k$ denote the comultiplication (or coproduct) and counit maps for C, respectively. We denote the grouplike elements of C by $G(C)$ and the primitive elements of C by $P(C)$. Similarly, if $H = (H, m, u, \Delta, \varepsilon, S)$ is a Hopf algebra, then m, u, Δ and ε retain their meanings above and $S\colon H \to H$ denotes the antipode of H. Again, we usually do not give a label to the multiplication or unit maps of H. We write $G(H)$, $P(H)$ for the grouplikes and primitives of H, respectively.

Sweedler notation is used for elements in the image of Δ as follows: for $h \in H$, we write

$$\Delta(h) = \sum h_1 \otimes h_2 \in H \otimes H.$$

If V is a left H-comodule, with coaction $\delta\colon V \to H \otimes V$, we write

$$\delta(v) := \sum v_{-1} \otimes v_0 \in H \otimes V.$$

The *left adjoint action* of H on itself is given by

$$\mathrm{ad}_l(h)(a) := \sum h_1 a S(h_2),$$

and the *right adjoint action* is given by

$$\mathrm{ad}_r(h)(a) := \sum S(h_1) a h_2,$$

for all $a, h \in H$.

1.1.2 Filtrations and gradings of Hopf algebras

When studying an algebraic structure, a common technique is to filter it and then consider the associated graded structure. The advantage of this approach is that the resulting object is often more straightforward to understand, but nevertheless retains many of the algebraic properties of the original structure without losing the key information. Here, we develop this technique for algebras, coalgebras and Hopf algebras.

Algebra filtrations and gradings

Definition 1.1.1. (i) Let A be an algebra. An *algebra filtration* of A is a family $\{A_n : n \geq 0\}$ of subspaces of A such that

(a) $A_n \subseteq A_{n+1}$ for all $n \geq 0$,

(b) $A_m A_n \subseteq A_{m+n}$ for all $m, n \geq 0$,

(c) $\bigcup_{n\geq 0} A_n = A$.

Due to (c), this is sometimes known as an *exhaustive* algebra filtation.

(ii) A *graded algebra* is an algebra $\overline{A}$ together with a family $\{\overline{A}_n\colon n \geq 0\}$ of subspaces of $\overline{A}$ such that

(a) $\overline{A}_m \overline{A}_n \subseteq \overline{A}_{m+n}$ for all $m, n \geq 0$,

(b) $\overline{A} = \bigoplus_{n\geq 0} \overline{A}_n$ as a vector space.

If A is an algebra with filtration $\{A_n\}$, we can construct a graded algebra from A in a natural way. Define a family of vector spaces $\{\overline{A}_n\}$ by

$$\overline{A}_n := \begin{cases} A_0 & n = 0 \\ A_n/A_{n-1} & n > 0. \end{cases}$$

The *associated graded algebra* of A is defined to be

$$\operatorname{gr} A := \bigoplus_{n \geq 0} \overline{A}_n.$$

The multiplication in $\operatorname{gr} A$ works as follows. For $a \in A_n \setminus A_{n-1}$, the *degree* of a is said to be n, and we write $\bar{a} := a + A_{n-1} \in \overline{A}_n$. If $c \in A$ has degree m, then $\bar{c} := c + A_{m-1} \in \overline{A}_m$ and we define $\bar{a}\bar{c} := ac + A_{m+n-1} \in \overline{A}_{m+n}$. Note that if $\bar{a}\bar{c} \in A_{m+n-1}$ then $\bar{a}\bar{c} = 0$; otherwise $\bar{a}\bar{c} = \overline{ac}$.

Definition 1.1.2. A graded algebra $\overline{A} = \bigoplus_{n \geq 0} \overline{A}_n$ is *connected* if $\overline{A}_0 = k$.

Coalgebra filtrations and gradings

Definition 1.1.3. (i) Let $C = (C, \Delta, \varepsilon)$ be a coalgebra. A *coalgebra filtration* of C is a family $\{C_n : n \geq 0\}$ of subspaces of C such that

(a) $C_n \subseteq C_{n+1}$ for all $n \geq 0$,

(b) $\Delta(C_n) \subseteq \sum_{i=0}^{n} C_i \otimes C_{n-i}$ for all $n \geq 0$,

(c) $\bigcup_{n \geq 0} C_n = C$.

(ii) A *graded coalgebra* is a coalgebra $\overline{C} = (\overline{C}, \overline{\Delta}, \bar{\varepsilon})$ together with a family $\{\overline{C}_n \colon n \geq 0\}$ of subspaces of $\overline{C}$ such that

(a) $\overline{\Delta}(\overline{C}_n) \subseteq \sum_{i=0}^{n} \overline{C}_i \otimes \overline{C}_{n-i}$,

(b) $\overline{C} = \bigoplus_{n \geq 0} \overline{C}_n$ as a vector space.

If C is a coalgebra with filtration $\{C_n\}$, we can construct a graded coalgebra from C. Analogously to the process for algebras, we define a family $\{\overline{C}_n\}$ of vector spaces by setting

$$\overline{C}_n := \begin{cases} C_0 & n = 0 \\ C_n/C_{n-1} & n > 0. \end{cases}$$

The *associated graded coalgebra* of C is

$$\operatorname{gr} C := \bigoplus_{n \geq 0} \overline{C}_n,$$

which, by [49, Exercise 11.1(1)], is a graded coalgebra with the following definitions for the coproduct $\overline{\Delta}\colon \operatorname{gr} C \to \operatorname{gr} C \otimes \operatorname{gr} C$ and counit $\overline{\varepsilon}\colon \operatorname{gr} C \to k$. The restriction of the coproduct

$$\overline{\Delta}|_{\overline{C}_n} : \overline{C}_n \to \sum_{i=0}^{n} \overline{C}_i \otimes \overline{C}_{n-i}$$

is the unique map that makes the following diagram, from [49, §11.1], commute:

$$\begin{tikzcd}
C_n \arrow[r, "\Delta|_{C_n}"] \arrow[d, "f"'] & \sum_{i=0}^{n} C_i \otimes C_{n-i} \arrow[d, "g"] \\
\overline{C}_n \arrow[r, "h"] \arrow[dr, "\overline{\Delta}|_{\overline{C}_n}"'] & \sum_{i=0}^{n}(C_i \otimes C_{n-i})/\sum_{j=0}^{n-1}(C_j \otimes C_{n-1-j}) \arrow[d, "i"] \\
& \sum_{i=0}^{n} \overline{C}_i \otimes \overline{C}_{n-i}
\end{tikzcd}$$

In the diagram, f and g are the canonical quotient maps, while h is induced by $\Delta|_{C_n}$ and is well-defined by Definition 1.1.3 (i)(b). The map i writes $^{-}$ over each tensorand of a coset representative in its domain; it is well-defined by the definition of this operation.

The restriction of the counit $\overline{\varepsilon}|_{\overline{C}_n} : \overline{C}_n \to k$ is defined by

$$\overline{\varepsilon}|_{\overline{C}_n} = \begin{cases} \varepsilon|_{C_0} & n = 0 \\ 0 & n > 0. \end{cases}$$

Recall that a *simple coalgebra* is a coalgebra with no proper subcoalgebras, and that the *coradical* of a coalgebra is the sum of all its simple subcoalgebras. An important example of a coalgebra filtration of a coalgebra C is the *coradical filtration* . This is defined by taking C_0 to be the coradical of C, and, for all $n \geq 0$,

$$C_{n+1} := \{c \in C \colon \Delta(c) \in C_n \otimes C + C \otimes C_0\}.$$

It is a coalgebra filtration by [42, Theorem 5.2.2].

Hopf algebra filtrations and gradings

Definition 1.1.4. (i) Let H be a Hopf algebra. A *Hopf algebra filtration* of H is a family $\{H_n \colon n \geq 0\}$ of subspaces of H such that

(a) $\{H_n\}$ is an algebra filtration of H,

(b) $\{H_n\}$ is a coalgebra filtration of H,

(c) $S(H_n) \subseteq H_n$ for all $n \geq 0$.

(ii) A *graded Hopf algebra* is a Hopf algebra $\overline{H} := (\overline{H}, \overline{\Delta}, \overline{\varepsilon}, \overline{S})$ together with a family $\{\overline{H}_n : n \geq 0\}$ of subspaces of $\overline{H}$ such that

(a) $\{\overline{H}_n\}$ is an algebra grading for H,

(b) $\{\overline{H}_n\}$ is a coalgebra grading for H,

(c) $\overline{S}(\overline{H}_n) \subseteq \overline{H}_n$ for all $n \geq 0$.

Let H be a Hopf algebra with Hopf algebra filtration $\{H_n\}$. Obviously, the associated graded algebra and coalgebra of H coincide; in fact,

$$\operatorname{gr} H = \bigoplus_{n \geq 0} \overline{H}_n$$

is the *associated graded Hopf algebra* of H. The antipode $\overline{S}\colon \operatorname{gr} H \to \operatorname{gr} H$ is defined by

$$\overline{S}(\bar{h}) := S(h) + H_{n-1},$$

for $\bar{h} = h + H_{n-1}$. It is well-defined by Definition 1.1.4 (i)(c).

For any Hopf algebra H, we can consider the coradical filtration of H, which in general is only a coalgebra filtration. We are able to state exactly when this filtration is, in fact, a Hopf algebra filtration:

Lemma 1.1.5. *[42, Lemma 5.2.8] Let $\{H_n\}$ be the coradical filtration of H. Then $\{H_n\}$ is a Hopf algebra filtration if and only if H_0 is a Hopf subalgebra of H.*

1.1.3 Skew (Laurent) polynomial rings

Roughly speaking, a skew polynomial ring consists of polynomials in a variable X, with coefficients in a ring R, where multiplication of X with the elements of R is not necessarily commutative.

Definition 1.1.6. Let R be a ring, let σ be a ring automorphism of R and let $\delta\colon R \to R$ be a (σ, id)-derivation of R: that is, δ satisfies

$$\delta(rs) = \sigma(r)\delta(s) + \delta(r)s,$$

for all $r, s \in R$. The *skew polynomial ring* $R[X; \sigma, \delta]$ is the ring generated by R and the indeterminate X that satisfies the following properties:

(i) $R[X; \sigma, \delta]$ is a free left R-module, with basis $\{1, X, X^2, \ldots\}$,

(ii) $Xr = \sigma(r)X + \delta(r)$, for all $r \in R$.

If $\sigma = \mathrm{id}$, we write $R[X;\delta]$ and if $\delta = 0$, we write $R[X;\sigma]$.

We also have the notion of a skew Laurent polynomial ring:

Definition 1.1.7. Let R be a ring and let σ be a ring automorphism of R. The *skew Laurent polynomial ring* $R[X^{\pm 1};\sigma]$ is the ring generated by R and $X^{\pm 1}$, where $X^{-1}X = XX^{-1} = 1$, that satisfies the following properties:

(i) $R[X^{\pm 1};\sigma]$ is a free left R-module, with basis $\{\ldots, X^{-2}, X^{-1}, 1, X, X^2, \ldots\}$,

(ii) $Xr = \sigma(r)X$, for all $r \in R$.

An alternative way to think about a skew Laurent polynomial ring is as a localisation of a skew-polynomial ring: $R[X^{\pm 1};\sigma] \cong R[X;\sigma][X]^{-1}$.

1.1.4 Skew group rings

Let R be a ring and let G be a group. The group ring RG is the free left R-module with the elements of G as its basis and multiplication arising from the multiplication in R and G: $(rg)(sh) = (rs)(gh)$, for all $r, s \in R$, $g, h \in G$, extended linearly to all of RG. In particular, this means that $gr = (1_R g)(r 1_G) = rg$, for all $r \in R$, $g \in G$. There is a more general notion of a group ring that allows for noncommutativity between elements of G and R:

Definition 1.1.8. Let R be a ring and let G be a group acting on R via ring automorphisms, which we write as $g \cdot r := g(r)$ for all $r \in R$ and $g \in G$. The *skew group ring* $R * G$ is the free left R-module with the elements of G as its basis and multiplication defined by $(rg)(sh) = (rg(s))(gh)$. In particular, we have $gr = (1_R g)(r 1_G) = g(r)g$.

1.2 Quantised enveloping algebras

Quantised enveloping algebras were discovered in the 1980s by Drinfel'd [17] and Jimbo [24], and have their origins in mathematical physics, with applications to many other areas of mathematics. They will appear as examples throughout this thesis.

1.2.1 Gaussian binomial coefficients

Let $0 \neq q \in k$. For any integer $n > 0$, let

$$(n)_q := 1 + \ldots + q^{n-1} = \frac{q^n - 1}{q - 1}.$$

The *q-factorial* is defined by setting $(0)!_q := 1$ and

$$(n)!_q := (1)_q(2)_q \cdots (n)_q = \frac{(q-1)(q^2-1)\cdots(q^n-1)}{(q-1)^n}.$$

In fact, $(n)!_q$ is a polynomial in q with integer coefficients; when $q = 1$, it is equal to the ordinary factorial $n!$. For $0 \leq i \leq n$, we define the *Gaussian binomial coefficient* or *q-binomial coefficient* by

$$\binom{n}{i}_q = \frac{(n)!_q}{(i)!_q(n-i)!_q}.$$

This is also a polynomial in q with integer coefficients whose evaluation at $q = 1$ is equal to the usual binomial coefficient $\binom{n}{i}$ [31, Proposition IV.2.1(a)]. There are analogues of the identities for binomial coefficients [31, Proposition IV.2.1(c)]:

$$\binom{n}{i}_q = \binom{n-i}{i}_q + q^{n-i}\binom{n-1}{i-1}_q = \binom{n-1}{q-1}_q + q^i\binom{n-1}{i}_q. \tag{1.1}$$

If q is a primitive nth root of unity, then

$$\binom{n}{i}_q = 0, \quad \text{for all } 1 \leq i \leq n-1. \tag{1.2}$$

There is an alternative type of q-binomial coefficient that is more convenient when studying quantised enveloping algebras. For integers $0 \leq i \leq n$, define

$$\begin{aligned}
[n]_q &:= \frac{q^n - q^{-n}}{q - q^{-1}}, \\
[n]!_q &:= [1]_q[2]_q \cdots [n]_q, \\
\begin{bmatrix} n \\ i \end{bmatrix}_q &:= \frac{[n]!_q}{[i]!_q[n-i]!_q}.
\end{aligned}$$

The following equation shows the relationship between the two types of q-binomial coefficients [13, I.6.1(1)]:

$$\begin{bmatrix} n \\ i \end{bmatrix}_q = q^{i(i-n)}\binom{n}{i}_{q^2}.$$

1.2.2 The definition

Let $\mathfrak{g}$ be a simple Lie algebra over $\mathbb{C}$ of rank n and let $C := (a_{ij})$ be its Cartan matrix. There are integers $d_1, \ldots, d_n \in \{1, 2, 3\}$ such that $d_i a_{ij} = d_j a_{ji}$; that is $(d_i a_{ij})$ is a symmetric matrix. Let $q \in k^*$, set $q_i := q^{d_i}$ for all $1 \leq i \leq n$ and suppose that ${q_i}^2 \neq 1$.

The *quantised enveloping algebra of* $\mathfrak{g}$, denoted $U_q(\mathfrak{g})$, is a k-algebra whose construction depends on the above choices of C and q. It is the k-algebra with generators $E_1, \ldots, E_n$,

$F_1, \ldots, F_n$ and ${K_1}^{\pm 1}, \ldots, {K_n}^{\pm 1}$, and relations

$$K_i E_j {K_i}^{-1} = {q_i}^{a_{ij}} E_j, \qquad K_i F_j {K_i}^{-1} = {q_i}^{-a_{ij}} F_j,$$
$$K_i K_j = K_j K_i, \qquad E_i F_j - F_j E_i = \delta_{ij} \frac{K_i - {K_i}^{-1}}{q_i - {q_i}^{-1}},$$

$$\sum_{l=0}^{1-a_{ij}} (-1)^l \begin{bmatrix} 1-a_{ij} \\ l \end{bmatrix}_{q_i} {E_i}^{1-a_{ij}-l} E_j {E_i}^l = 0 \ \ (i \neq j),$$
$$\sum_{l=0}^{1-a_{ij}} (-1)^l \begin{bmatrix} 1-a_{ij} \\ l \end{bmatrix}_{q_i} {F_i}^{1-a_{ij}-l} F_j {F_i}^l = 0 \ \ (i \neq j).$$

There is a free abelian group G of rank n contained in $U_q(\mathfrak{g})$:

$$G = \langle {K_i}^{\pm 1} \colon 1 \leq i \leq n \rangle. \tag{1.3}$$

The following definitions make $U_q(\mathfrak{g})$ into a Hopf algebra: for all $1 \leq i \leq n$,

$$\Delta(K_i) = K_i \otimes K_i, \qquad \varepsilon(K_i) = 0, \qquad S(K_i) = {K_i}^{-1},$$
$$\Delta(E_i) = E_i \otimes 1 + K_i \otimes E_i, \qquad \varepsilon(E_i) = 0, \qquad S(E_i) = -{K_i}^{-1} E_i,$$
$$\Delta(F_i) = F_i \otimes {K_i}^{-1} + 1 \otimes F_i, \qquad \varepsilon(F_i) = 0, \qquad S(F_i) = -F_i K_i.$$

There are Hopf subalgebras of $U_q(\mathfrak{g})$ which can be viewed as quantisations of the positive and negative Borel Lie subalgebras of $\mathfrak{g}$. These are $U_q^{\geq 0}(\mathfrak{g})$, which is the Hopf subalgebra generated by the ${K_i}^{\pm 1}$ and the E_i, $1 \leq i \leq n$, and $U_q^{\leq 0}(\mathfrak{g})$, which is generated by the ${K_i}^{\pm 1}$ and the F_i, $1 \leq i \leq n$.

1.3 Pointed Hopf algebras

1.3.1 Definition and examples

Definition 1.3.1. A *pointed coalgebra* is a coalgebra C with the property that every simple subcoalgebra of C is one-dimensional.

Since a subcoalgebra is closed under comultiplication, a one-dimensional subcoalgebra must be of the form kg, for some $g \in G(C)$. Therefore, C is pointed if and only if $C_0 = kG(C)$, where C_0 is the coradical of C.

Some examples of pointed coalgebras are as follows. Note that, in each case, the coalgebra involved is, in fact, a Hopf algebra. Hopf algebras generated by grouplikes and skew-primitives are pointed, and the following examples are of this type.

Examples 1.3.2. (i) Let G be a group. The coradical of the group algebra kG is kG itself, so kG is pointed.

(ii) Let $\mathfrak{g}$ be a Lie algebra. The coradical of the universal enveloping algebra $U(\mathfrak{g})$ is k [42, Example 5.1.6], so $U(\mathfrak{g})$ is pointed.

(iii) Let $\mathfrak{g}$ be a semisimple Lie algebra and let $0 \neq q \in k$. By [43, Theorem 2.2], the coradical of $U_q(\mathfrak{g})$ is kG, where G is as in (1.3). Hence, $U_q(\mathfrak{g})$ is pointed.

1.3.2 Braided vector spaces and Yetter-Drinfeld modules

We leave aside pointed Hopf algebras in this section and the next, in order to introduce some concepts involving braidings.

Definition 1.3.3. A *braided vector space* is a vector space V with an automorphism c of $V \otimes V$ that satisfies the braid equation, that is,

$$(c \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes c)(c \otimes \mathrm{id}_V) = (\mathrm{id}_V \otimes c)(c \otimes \mathrm{id}_V)(\mathrm{id}_V \otimes c).$$

Some important examples of braided vector spaces come from the category ${}^H_H\mathcal{YD}$ of Yetter-Drinfeld modules over a Hopf algebra H.

Definition 1.3.4. Let H be a Hopf algebra. A *left Yetter-Drinfeld module* V over H is a k-vector space which is both a left H-module and a left H-comodule and satisfies the compatibility condition

$$\delta(h \cdot v) = \sum h_1 v_{-1} S(h_3) \otimes h_2 \cdot v_0,$$

for all $h \in H$ and $v \in V$.

The tensor product of two Yetter-Drinfeld modules over H is also a Yetter-Drinfeld module, with the standard action as in [42, Definition 1.8.1] and coaction as in [42, Definition 1.8.2]. Morphisms in ${}^H_H\mathcal{YD}$ are k-linear maps that preserve the action and coaction by H.

If $V, W \in {}^H_H\mathcal{YD}$, then we can define a linear map $c_{V,W} \colon V \otimes W \to W \otimes V$ by

$$c_{V,W}(v \otimes w) = \sum (v_{-1} \cdot w) \otimes v_0.$$

The map $c_{V,V}$ makes V into a braided vector space.

We will mainly be concerned with the case when $H = kG$, where G is a group. In this situation, a vector space V is an H-comodule if and only if it is a G-graded vector space [42, Example 1.6.7]. That is,

$$V = \bigoplus_{g \in G} V_g, \tag{1.4}$$

where $V_g = \{v \in V : \delta(v) = g \otimes v\}$. We will denote ${}^{kG}_{kG}\mathcal{YD}$ by ${}^{G}_{G}\mathcal{YD}$.

Remarks 1.3.5. [2, Remark 1.4] Let G be a group and V a G-graded vector space that is a left kG-module. Define a linear automorphism $c \colon V \otimes V \to V \otimes V$ by

$$c(x \otimes y) = (g \cdot y) \otimes x,$$

for all $x \in V_g$, $y \in V$. Then

(i) It follows immediately from the compatibility condition for Yetter-Drinfeld modules that $V \in {}^{G}_{G}\mathcal{YD}$ if and only if $gV_h \subseteq V_{ghg^{-1}}$ for all $g, h \in G$.

(ii) If $V \in {}^{G}_{G}\mathcal{YD}$, then (V, c) is a braided vector space.

Now, let G be abelian with $\hat{G} = \mathrm{Hom}(G, k)$. The Yetter-Drinfeld condition simplifies, so that $V \in {}^{G}_{G}\mathcal{YD}$ if and only if V is a G-graded G-module, whose homogeneous components are G-submodules. We call the action of G on V *diagonalisable* if

$$V = \bigoplus_{g \in G, \chi \in \hat{G}} V_g^{\chi},$$

where

$$V_g^{\chi} = \{v \in V : \delta(v) = g \otimes v, h \cdot v = \chi(h)v \text{ for all } h \in G\}.$$

In particular, if G is finite with $|G|^{-1} \in k$ and such that k contains a primitive $|G|$th root of unity, then every V in ${}^{G}_{G}\mathcal{YD}$ is diagonalisable.

Suppose that V is a finite-dimensional vector space of dimension θ and that V is a diagonalisable member of ${}^{G}_{G}\mathcal{YD}$. Pick a basis $x_1, \ldots, x_\theta$ of V, where $x_i \in V_{g_i}^{\chi_i}$ for not necessarily distinct members $\chi_1, \ldots, \chi_\theta$ of $\hat{G}$ and $g_1, \ldots, g_\theta$ of G, so that

$$c(x_i \otimes x_j) = \chi_j(g_i) x_j \otimes x_i, \tag{1.5}$$

for all $1 \leq i, j \leq \theta$. Denote $\chi_j(g_i)$ by r_{ij}, for convenience.

Definition 1.3.6. A finite-dimensional braided vector space (V, c) is of *diagonal type* if V has a basis $x_1, \ldots, x_\theta$ such that

$$c(x_i \otimes x_j) = r_{ij} x_j \otimes x_i,$$

for some $r_{ij} \in k^*$, $1 \leq i, j \leq \theta$.

Clearly, when G is an abelian group acting diagonalisably on V, (V, c) is of diagonal type. Conversely, any finite-dimensional braided vector V space of diagonal type can be realised as a Yetter-Drinfeld module over an abelian group G acting diagonalisably on V: with V as in the definition above, let $g_1, \ldots, g_\theta \in \mathrm{GL}(V)$ be defined by $g_i(x_j) = r_{ij} x_j$ and take G to be the group generated by $g_1, \ldots g_\theta$.

1.3.3 Braided Hopf algebras

The majority of the material in this section is taken from [2, §1.3]. Let H be a Hopf algebra. We can define algebras in ${}^H_H\mathcal{YD}$ in the usual way. That is, $R \in {}^H_H\mathcal{YD}$ is an algebra in ${}^H_H\mathcal{YD}$ if there are maps $m_R \colon R \otimes R \to R$ and $u_R \colon k \to R$, which are morphisms in ${}^H_H\mathcal{YD}$ and make R into an associative algebra. Similarly, $R \in {}^H_H\mathcal{YD}$ is a coalgebra if there are maps $\Delta_R \colon R \to R \otimes R$ and $\varepsilon_R \colon R \otimes k$, which are morphisms in ${}^H_H\mathcal{YD}$ and make R into a coassociative coalgebra.

If R, T are algebras in ${}^H_H\mathcal{YD}$, then we can define a "twisted" version of the usual algebra $R \otimes T$, which we denote $R \underline{\otimes} T$. Let $c := c_{R,T}$ and define the product in $R \underline{\otimes} T$ by

$$m_{R \underline{\otimes} T} = (m_R \otimes m_T)(\mathrm{id} \otimes c \otimes \mathrm{id}).$$

Definition 1.3.7. [2, Definition 1.7]

(i) $R = (R, m_R, u_R, \Delta_R, \varepsilon_R)$ is a *braided bialgebra* in ${}^H_H\mathcal{YD}$ if the following hold:

  (a) (R, m_R, u_R) is an algebra in ${}^H_H\mathcal{YD}$,

  (b) $(R, \Delta_R, \varepsilon_R)$ is a coalgebra in ${}^H_H\mathcal{YD}$,

  (c) $\Delta_R \colon R \to R \underline{\otimes} R$ and $\varepsilon_R \colon R \to k$ are morphisms of algebras.

(ii) $R = (R, m_R, u_R, \Delta_R, \varepsilon_R, S_R)$ is a *braided Hopf algebra* in ${}^H_H\mathcal{YD}$ if $(R, m_R, u_R, \Delta_R, \varepsilon_R)$ is a braided bialgebra and $\mathrm{id} \in \mathrm{End}(R)$ is convolution invertible with inverse S_R.

(iii) A *graded braided Hopf algebra* is a braided Hopf algebra $R = (R, m_R, u_R, \Delta_R, \varepsilon_R, S_R) \in {}^H_H\mathcal{YD}$ together with a family $\{R_n \colon n \geq 0\}$ of subspaces of R, such that

(a) $R = \bigoplus_{n\geq 0} R_n$ as a vector space;

(b) $R_m R_n \subseteq R_{m+n}$ for all $m, n \geq 0$,

(c) $\Delta_R(R_n) \subseteq \sum_{i=0}^{n} R_i \otimes R_{n-i}$ for all $n \geq 0$,

(d) $S_R(R_n) \subseteq R_n$ for all $n \geq 0$.

The following map is used extensively in Chapter 4. When c is the "flip" map, this gives the left adjoint action.

Definition 1.3.8. Let R be a braided Hopf algebra in ${}^H_H\mathcal{YD}$ and let $c := c_{R,R} \colon R \otimes R \to R \otimes R$, with $c(r \otimes t) := \sum (r_{-1} \cdot t) \otimes r_0$ for all $r, t \in R$. The *braided adjoint representation of* R is the map $\mathrm{ad}_c \colon R \to \mathrm{End}(R)$ defined by

$$\mathrm{ad}_c(x)(y) = m(m \otimes S)(\mathrm{id} \otimes c)(\Delta \otimes \mathrm{id})(x \otimes y),$$

for all $x, y \in R$.

Note that if x is primitive, then, for all $y \in R$,

$$\mathrm{ad}_c(x)(y) = m(\mathrm{id} - c)(x \otimes y).$$

1.3.4 Bosonisation

Let $H = (H, \Delta_H, \varepsilon_H, S_H)$ be a Hopf algebra, and let $R = (R, \Delta_R, \varepsilon_R, S_R)$ be a braided Hopf algebra in ${}^H_H\mathcal{YD}$. We change the usual Sweedler notation for Δ_R slightly by writing

$$\Delta_R(r) = \sum r^1 \otimes r^2,$$

in order to emphasise that R is a *braided* Hopf algebra.

We now consider a new Hopf algebra formed from R and H by a process called bosonisation, which was first studied by Radford in [46] and then rediscovered by Majid in [39].

Definition 1.3.9. The *bosonisation* of R by H is a (non-braided) Hopf algebra, denoted $R\#H$, with underlying vector space $R \otimes H$. We write $r\#h$ for the element $r \otimes h$, where $r \in R$, $h \in H$. The multiplication, comultiplication, counit and antipode in $R\#H$ are defined as follows:

$$\begin{aligned}
(r\#h)(s\#l) &:= \sum r(h_1 \cdot s)\#h_2 l, \\
\Delta(r\#h) &:= \sum r^1\#(r^2)_{-1}h_1 \otimes (r^2)_0\#h_2, \\
\varepsilon(r\#h) &:= \varepsilon_R(r)\varepsilon_H(h), \\
S(r\#h) &:= \sum (1\#S_H(r_{-1}h))(S_R(r_0)\#1).
\end{aligned}$$

Proofs that these definitions satisfy the necessary axioms for $R\#H$ to be a Hopf algebra can be found in [46].

Suppose that $H = kG$, where G is a group, and that G acts on R via automorphisms. Then the rule for multiplication in $R\#kG$ reduces to the multiplication in the skew group ring $R * G$. Hence, as algebras, $R\#kG \cong R * G$ via $r\#g \mapsto rg$.

1.3.5 Decomposition of pointed Hopf algebras

We now return to pointed Hopf algebras, and use the tools developed in the previous sections to obtain a description of the associated graded Hopf algebra of a pointed Hopf algebra as a bosonisation.

Let H be a pointed Hopf algebra, with coradical filtration $\{H_n \colon n \geq 0\}$. Then $H_0 = kG$, where $G := G(H)$. By Lemma 1.1.5, this means that $\{H_n\}$ is a Hopf algebra filtration of H. We can therefore form the associated graded Hopf algebra of H with respect to this filtration. We write $\operatorname{gr} H = (\operatorname{gr} H, \overline{m}, \overline{u}, \overline{\Delta}, \overline{\varepsilon}, \overline{S})$, with $\operatorname{gr} H = \bigoplus_{n \geq 0} \overline{H}_n$.

Define the Hopf algebra projection $\pi \colon \operatorname{gr} H \to \overline{H}_0$ in the obvious way. The algebra of coinvariants with respect to π is

$$B := (\operatorname{gr} H)^{\operatorname{co}\pi} = \{h \in \operatorname{gr} H \colon (\operatorname{id} \otimes \pi)\overline{\Delta}(h) = h \otimes 1\}.$$

Then, by [46, Theorem 3], B is a braided Hopf algebra in ${}^G_G\mathcal{YD}$ in the following way:

- The action of kG on B is the restriction of the left adjoint action of $\operatorname{gr} H$ on B,
- The coaction is $(\pi \otimes \operatorname{id})\overline{\Delta}|_B \colon B \to kG \otimes B$,
- B is a subalgebra of $\operatorname{gr} H$,
- The comultiplication Δ_B, counit ε_B and antipode S_B in B are given by

$$\begin{aligned}
\Delta_B &:= (\overline{m} \otimes \operatorname{id})(\operatorname{id} \otimes \pi \circ \overline{S} \otimes \operatorname{id})(\operatorname{id} \otimes \overline{\Delta})\overline{\Delta}|_B \colon B \to B \otimes B \\
\varepsilon_B &:= \overline{\varepsilon}|_B \colon B \to k, \\
S_B &:= \overline{m}(\pi \otimes \overline{S})\overline{\Delta}|_B \colon B \to B.
\end{aligned}$$

Furthermore, B has a Hopf algebra grading with the simplest possible structure for the degree 0 and 1 components.

Corollary 1.3.10. *(i) B has a Hopf algebra grading $\{\overline{B}_n\}$ inherited from $\operatorname{gr} H$ in a natural way: $\overline{B}_n := B \cap \overline{H}_n$,* *(ii)* $\overline{B}_0 = k$,

(iii) $\overline{B}_1 = P(B)$.

Proof. (i) The coradical filtration of $\operatorname{gr} H$ coincides with the standard ascending filtration $\{(\operatorname{gr} H)_n : n \geq 0\}$ of $\operatorname{gr} H$, where $(\operatorname{gr} H)_n := \bigoplus_{0 \leq m \leq n} \overline{H}_m$. By [42, Lemma 5.2.12], the coradical filtration of B is therefore given by $\{B \cap (\operatorname{gr} H)_n : n \geq 0\}$. Filtering B in this way and taking the associated graded Hopf algebra results in a graded Hopf algebra with grading $\{B \cap \overline{H}_n : n \geq 0\}$. This graded Hopf algebra is isomorphic to B, by [40, 1.6.4] and [49, §11.1].

(ii) Let $b = \sum_{i=1}^{t} \alpha_i g_i \in \overline{B}_0$, where $\alpha_i \in k$ and $g_i \in G$ are distinct, $1 \leq i \leq t$. Then $(\mathrm{id} \otimes \pi)\overline{\Delta}(b) = \sum_{i=1}^{t} \alpha_i g_i \otimes g_i = \sum_{i=1}^{t} \alpha_i g_i \otimes 1$. Since $G \otimes G$ is a k-basis for $kG \otimes kG$, this can happen if and only if $t = 1$ and $g_1 = 1$, which means $b \in k$.

(iii) This is clear by (ii). $\square$

Let $V := \overline{B}_1$; the subalgebra of B generated by $\overline{B}_1$ is a *Nichols algebra* , which we denote by $B(V)$. Therefore, B is a Nichols algebra if and only if $B = k\langle \overline{B}_1 \rangle$. We will provide a formal definition of Nichols algebras in Chapter 4.

Recall from Definition 1.3.9 that the bosonisation $B\#kG$ is a Hopf algebra. By [46, Theorem 3], there is a Hopf algebra isomorphism $B\#kG \cong \operatorname{gr} H$ with $b\#g \mapsto bg$. The inverse Hopf algebra isomorphism $\operatorname{gr} H \cong B\#kG$ is given by

$$h \mapsto \sum h_1(\pi \circ \overline{S})(h_2)\#\pi(h_3),$$

for $h \in \operatorname{gr} H$ [21, Theorem 3.3].

Therefore, studying the structure and properties of $B\#kG$ can provide us with information about the pointed Hopf algebra H, through lifting properties from $\operatorname{gr} H$ to H. The survey article [2] divides the classification problem of pointed Hopf algebras into three steps:

(i) Determining the structure of the Nichols algebras $B(V)$,

(ii) Investigating the properties of the pointed Hopf algebras H, with $G := G(H)$, such that $\operatorname{gr} H \cong B(V)\#kG$,

(iii) Determining which pointed Hopf algebras H satisfy $\operatorname{gr} H \cong B(V)\#kG$. This is equivalent to determining which pointed Hopf algebras are generated by grouplike and skew-primitive elements. [2, Conjecture 5.7] suggests that finite-dimensional pointed Hopf algebras over algebraically closed fields of characteristic zero satisfy this condition. However, this is known to be false for infinite-dimensional pointed Hopf algebras and for finite-dimensional pointed Hopf algebras over a field of positive characteristic.

Chapter 2

A PBW-basis for diagonal Nichols algebras

This chapter is mainly drawn from [32], which employs some unusual terminology. We provide more explanation where needed and simplify some of the definitions and their consequences. This enables us to state the main results, Theorems 2.2.11 and 2.3.7, and goes a little way towards their outline proofs, which gives context for later results in Chapters 3 and 4. However, we expand the proof of Theorem 2.4.1 from that in [32], since the technique from it is used in Chapter 3.

We start with an alphabet of n letters and introduce some combinatorial definitions on words in these letters. We then show a way of constructing certain polynomials from words in non-commuting variables, which can be multiplied together in a particular order to give a PBW-basis for a free algebra in n variables. From this basis, we obtain a PBW-basis for the Hopf algebra bosonisation of a Hopf algebra generated by skew-primitive elements and a group algebra, when the skew-primitives commute with the group elements up to multiplication by scalars. Finally, as an application of the basis, we show that the bosonisation Hopf algebra is noetherian if there is only a finite number of PBW-generators.

2.1 Lyndon words

Let $X = \{x_1, \ldots, x_n\}$ be a finite, totally ordered set with ordering

$$x_1 < x_2 < \cdots < x_n,$$

and let $\mathbb{X}$ be the set of words in the elements of X. The *empty word* is denoted 1, and the *length* $l(u)$ of a word $u \in \mathbb{X}$ is the number of letters in u. The *structure* of u is $(m_1, \ldots, m_n) \in \mathbb{Z}_{\geq 0}{}^n$, where u contains m_i occurrences of x_i, for $1 \leq i \leq n$. To each x_i, associate a positive integer d_i; define the *degree* of u by $\deg(u) := m_1 d_1 + \ldots + m_n d_n$.

The *lexicographic order* on $\mathbb{X}$ is the total order defined by $u < v$ if and only if either

- $v = uu'$ for some $u' \in \mathbb{X}$, that is, u is the beginning of v, or
- $u = wx_iu',\ v = wx_jv'$ for some $w, u', v' \in \mathbb{X}$ and $i < j$. That is, by moving from left to right in u and v until the occurrence of the first distinct letters, x_i and x_j respectively, we have $i < j$.

This is the ordering that is found in dictionaries. For example, the set of words of length two or less in two letters is ordered as follows:

$$x_1 < x_1{}^2 < x_1x_2 < x_2 < x_2x_1 < x_2{}^2.$$

The ordering is preserved by left multiplication, but not always by right multiplication. For example, $x_1 < x_1{}^2$, but $x_1{}^2x_2 < x_1x_2$. However, if $u < v$ and u is not the beginning of v, then the ordering is preserved by right multiplication, even right multiplication by different words. In particular, this holds when $l(u) = l(v)$.

Consequently, we can always "cancel" words from orderings on the left: $wu < wv$ implies $u < v$. However, if $uw < vw$, we can only cancel on the right when u is not the beginning of v. Again, this holds when $l(u) = l(v)$.

Definition 2.1.1. A non-empty word $u \in \mathbb{X}$ is called a *Lyndon word* (*standard word* in [32]) if u is less than any of its proper endings. That is, $u \neq 1$ and for every possible decomposition $u = vw$, with $v, w \in \mathbb{X}$ non-empty, then $u < w$.

There is an alternative condition for checking whether a word is Lyndon:

Lemma 2.1.2. *[32, Lemma 2] A non-empty word u is Lyndon if and only if, for every decomposition $u = vw$ where $v, w \in \mathbb{X}$ are non-empty, then $u < wv$.*

Proof. If $u = vw$ is Lyndon, with $v, w \in \mathbb{X}$ non-empty, then $u < w$ by definition. Clearly, u is not the beginning of w and so the ordering $u < w$ is preserved under right multiplication of either side by any word. Right-multiplying by v on the right hand side gives $u < wv$, as required.

For the converse, suppose u is such that for every decomposition $u = vw$, where $v, w \in \mathbb{X}$ are non-empty, we have $u < wv$. For any such decomposition $u = vw$, it is clear that $u \neq w$, since $l(u) > l(v)$, so either $u < w$ or $u > w$. Suppose $u > w$; we show that this leads to a contradiction and the lemma follows. Since $u < wv$, we must have that w is the beginning of u and so $u = ww'$ for some non-empty $w' \in \mathbb{X}$. By hypothesis,

$$u = ww' < wv \text{ and } u = vw < w'w.$$

Since $l(v) = l(w')$, we can cancel the w's, which gives both $w' < v$ and $v < w'$, a contradiction. $\square$

The simplest non-trivial examples of Lyndon words are those defined on an alphabet of two letters.

Example 2.1.3. The Lyndon words of length five or less in two letters are as follows:

$$x_1,\ x_2,\ x_1x_2,\ {x_1}^2x_2,\ x_1{x_2}^2,\ {x_1}^3x_2,\ {x_1}^2{x_2}^2,\ x_1{x_2}^3,$$
$${x_1}^4x_2,\ {x_1}^3{x_2}^2,\ {x_1}^2x_2x_1x_2,\ {x_1}^2{x_2}^3,\ x_1x_2x_1{x_2}^2,\ x_1{x_2}^4.$$

We note in passing, since it is not required later, that the Lyndon words in two letters are x_2 and

$$ {x_1}^{m_1}{x_2}^{n_1}\cdots{x_1}^{m_t}{x_2}^{n_t}, \qquad m_i > 0\ \forall\ i,\ n_j > 0\ \forall\ j < t,\ n_t \geq 0, \tag{2.1}$$

such that for all $0 \leq i \leq t$, $\exists\, k \geq 0$ such that $\forall\, 0 \leq j < k$,

$$m_{1+j} = m_{i+j},\ n_{1+j} = n_{i+j}$$

and either

$$m_{1+k} > m_{i+k}$$

or

$$m_{1+k} = m_{i+k} \text{ and } n_{1+k} < n_{i+k}.$$

Evidently, for any X, there is an infinite number of Lyndon words, and it is difficult, even for $|X| = 2$, to write down an explicit description of them. However, there is an algorithm that gives a unique way of decomposing a Lyndon word into Lyndon words of smaller length:

Theorem 2.1.4. *[51, Theorem 13] Every non-empty Lyndon word $u \in \mathbb{X} \setminus X$ has a fixed decomposition $u = u'u''$, with u' and u'' non-empty Lyndon words such that either $u' \in X$ or the decomposition of u' is $u' = vw$ with $w \geq u''$.*

This decomposition is called the *Shirshov decomposition* of u and is obtained inductively by choosing u'' to be the longest proper ending of u that is a Lyndon word.

2.2 Brackets in the free algebra

2.2.1 General definition

Let $k\langle X\rangle$ denote the free k-algebra generated by X. Any element of $k\langle X\rangle$ is a linear combination of words in $\mathbb{X}$, so we will sometimes refer to it as a polynomial, even though the letters do not commute and so, for example, $x_1x_2x_1$ is not equal to ${x_1}^2x_2$. We can equally well think of $k\langle X\rangle$ as the monoid algebra $k\mathbb{X}$, or as the tensor algebra $T(V)$, where V is the vector space with basis X.

For $f \in k\langle X\rangle$, the *leading word* $\overline{f}$ of f is the lexicographically smallest word occurring with nonzero coefficient in f. For example, if $f = 2x_1 + x_1x_2 + 5x_2 + 2x_2x_1$, then $\overline{f} = x_1$.

In general, $\overline{fg} \neq \overline{f}\,\overline{g}$. For example, if $f = x_1 + x_1x_2$ and $g = x_3$ then

$$\overline{fg} = x_1x_2x_3 \neq x_1x_3 = \overline{f}\,\overline{g}.$$

However, if $\overline{f}$ is not the beginning of any other word in f then

$$\overline{fg} = \overline{f}\,\overline{g}. \tag{2.2}$$

In particular, if f and g are homogeneous polynomials, the above equation holds.

Definition 2.2.1. Let $[\ ,\ ]\colon k\langle X\rangle \times k\langle X\rangle \to k\langle X\rangle$ be a bilinear operation. The set of *nonassociative words* is defined inductively as follows:

(i) the empty word 1 and all letters $x \in X$ are nonassociative words;

(ii) $a \in k\langle X\rangle \setminus X$ is a nonassociative word if and only if $a = [b, c]$ for some nonassociative words $b, c \in k\langle X\rangle$.

Note that, despite the name, in general a nonassociative word is not a member of $\mathbb{X}$ but rather a linear combination of words in $\mathbb{X}$.

Let $a = [b, c] \in k\langle X\rangle$ be a nonassociative word and suppose $b \notin X$. Then $b = [d, e]$ for some $d, e \in k\langle X\rangle$. Likewise, we can replace c with $[f, g]$ if $c \notin X$. We can then repeat the process with d, e, f, g, etc., until the only subwords that appear are letters. For example, $[[x_1, x_2], x_1]$ and $[x_1, [x_2, x_1]]$ are nonassociative words written in this form. Both polynomials arise by inserting brackets into the word $x_1x_2x_1$ in a particular way. Clearly, there is more than one possible outcome. However, if u is a Lyndon word, we can define a unique method for inserting brackets into the word u. We will denote the resulting nonassociative word by $[u]$ and define it inductively as follows:

Definition 2.2.2. The set

$$\{[u] \in k\langle X\rangle : u \text{ a Lyndon word}\}$$

is called the set of *nonassociative Lyndon words*, where

(i) for $u \in X$, $[u] = u$;

(ii) for $l(u) > 1$, let $u = u'u''$ be the Shirshov decomposition of u. Then

$$[u] = [[u'], [u'']].$$

The uniqueness of the definition of $[u]$ follows by the uniqueness of the Shirshov decomposition in Theorem 2.1.4. Therefore, there is a bijective correspondence between Lyndon words and nonassociative Lyndon words, given by $u \mapsto [u]$.

Examples 2.2.3. (i) Let $u = x_1{x_2}^n$, where $n \geq 1$. Then

$$\begin{aligned}[u] &= [[x_1{x_2}^{n-1}], x_2]\\ &= [[[x_1{x_2}^{n-2}], x_2], x_2]\\ &\vdots\\ &= [\cdots[[x_1, x_2], x_2], \cdots, x_2].\end{aligned}$$

(ii) Let $u = {x_1}^2 x_2 x_1 {x_2}^2$. Then

$$\begin{aligned}[u] &= [x_1, [x_1 x_2 x_1 {x_2}^2]]\\ &= [x_1, [[x_1 x_2], [x_1 {x_2}^2]]]\\ &= [x_1, [[x_1, x_2], [[x_1 x_2], x_2]]]\\ &= [x_1, [[x_1, x_2], [[x_1, x_2], x_2]]].\end{aligned}$$

(iii) Let $u = x_1 {x_2}^2 x_3 x_2 {x_3}^2$. Then

$$\begin{aligned}[u] &= [x_1, [{x_2}^2 x_3 x_2 {x_3}^2]]\\ &= [x_1, [x_2, [x_2 x_3 x_2 {x_3}^2]]]\\ &= [x_1, [x_2, [[x_2 x_3], [x_2 {x_3}^2]]]]\\ &= [x_1, [x_2, [[x_2, x_3], [x_2, [{x_3}^2]]]]]\\ &= [x_1, [x_2, [[x_2, x_3], [x_2, [x_3, x_3]]]]].\end{aligned}$$

2.2.2 Skew-commutators

We will now define a particular type of bilinear map $[\ ,\ ]\colon k\langle X\rangle \otimes k\langle X\rangle \to k\langle X\rangle$, which we will adopt for the rest of this chapter.

Let G be an abelian group and associate every $x_i \in X$ with $g_i \in G$ and a character $\chi^i\colon G \to k \setminus \{0\}$. For a word $u = x_{i_1} \cdots x_{i_t}$, let $g_u := g_{i_1} \cdots g_{i_t}$. Similarly, we define the character $\chi^u := \chi^{i_1} \cdots \chi^{i_t}$. For $u, v \in \mathbb{X}$, let $p_{u,v} = \chi^u(g_v)$. It is easy to check the following equalities:

$$p_{uu_1,v} = p_{u,v}p_{u_1,v}, \;\; p_{u,vv_1} = p_{u,v}p_{u,v_1}. \tag{2.3}$$

We now define

$$[\ ,\ ]\colon \mathbb{X} \otimes \mathbb{X} \to k\langle X\rangle, \qquad [u,v] = uv - p_{u,v}vu, \tag{2.4}$$

for $u, v \in \mathbb{X}$. When either term is a product of words, we have the following formulas:

$$[u, vw] = [u, v]w + p_{u,v}v[u, w] \tag{2.5}$$

$$[uv, w] = p_{v,w}[u, w]v + u[v, w]. \tag{2.6}$$

By specifying that $[\ ,\ ]$ should be bilinear, we can extend it uniquely to produce a map, which we also denote by $[\ ,\ ]$:

$$[\ ,\ ]\colon k\langle X\rangle \otimes k\langle X\rangle \to k\langle X\rangle.$$

Example 2.2.4. (i) The "trivial" example. Let $X = \{x_1, \ldots, x_n\}$ and let $G = \{1\}$. Consequently, χ is the trivial character, and $[x_i, x_j] = x_ix_j - x_jx_i$ for all $1 \le i, j \le n$. Even this case is, in fact, highly non-trivial. It yields, as a special case of Theorem 2.2.11, the famous theorem of Jacobson on the enveloping algebra of free Lie algebras [23, Theorem V.7], as will be explained at the end of §2.2.2.

(ii) This will be a recurring example, which we revisit in Examples 2.3.1, 2.3.4 and 2.3.8. It leads to a PBW-basis for $U_q^{\ge 0}(\mathfrak{sl}_3)$, the quantised enveloping algebra of the positive Borel Lie subalgebra of $\mathfrak{sl}_3$, introduced in §1.2.2. Let $X = \{x_1, x_2\}$ with $x_1 < x_2$. Let G be the group $\mathbb{Z} \times \mathbb{Z}$ and let g_1, g_2 together generate G. Fix $q \in k \setminus \{0\}$ and define characters $\chi^1, \chi^2\colon G \to k \setminus \{0\}$ by

$$\chi^1(g_1) = q^{-2}, \;\; \chi^1(g_2) = q,$$
$$\chi^2(g_1) = q, \;\; \chi^2(g_2) = q^{-2}.$$

We associate x_1 with g_1 and x_2 with g_2. Following the procedure above, we have a bilinear operation $[\ ,\ ]\colon k\langle X\rangle \times k\langle X\rangle \to k\langle X\rangle$, where, for example,

$$\begin{aligned}
[x_1, x_2] &= x_1x_2 - \chi^1(g_2)x_2x_1 = x_1x_2 - qx_2x_1, \\
[x_1, [x_1, x_2]] &= [x_1, x_1x_2 - qx_2x_1] \\
&= {x_1}^2x_2 - (\chi^1(g_1)\chi^1(g_2) + q)x_1x_2x_1 + q\chi^1(g_2)\chi^1(g_1)x_2{x_1}^2 \\
&= {x_1}^2x_2 - (q^{-1} + q)x_1x_2x_1 + x_2{x_1}^2. \qquad (2.7)
\end{aligned}$$

This definition behaves nicely with respect to the Lyndon nonassociative words.

Lemma 2.2.5. *Let $u \in \mathbb{X}$ be a Lyndon word, with corresponding nonassociative Lyndon word $[u]$.*

(i) If $[u] = [[v], [w]]$ then $[u] = [v][w] - p_{v,w}[w][v]$.

(ii) The polynomial $[u]$ has degree $l(u)$, is homogeneous in the letters of u (with the same multiplicities) and has leading word u with coefficient 1.

Proof. First, note that if $l(u) = 1$, then $[u] = u$ is a polynomial of degree $l(u)$ which is homogeneous in u. We now prove by induction on $l(u) > 1$ that if $[u] = [[v], [w]]$ then $[u] = [v][w] - p_{v,w}[w][v]$, and that the first two claims in (ii) are true.

We have $l(v) < l(u)$, $l(w) < l(u)$ and we can write $[v]$ and $[w]$ as sums of words with coefficients from k:

$$[v] = \sum_i \alpha_i v_i, \qquad [w] = \sum_j \beta_j w_j$$

for some $\alpha_i, \beta_j \in k$ and $v_i, w_j \in \mathbb{X}$. By induction, $[v]$ is a polynomial of degree $l(v)$ which is homogeneous in the letters of v. Hence, for all i, v_i is a monomial of degree $l(v)$ which is equal to a permutation of the letters of v. The obvious analogous conditions hold for $[w]$, and for w_j for all j. By (2.3), $p_{v_i,w_j} = p_{v,w}$ for all i, j. Therefore, using the bilinearity of $[\ ,\ ]$,

$$\begin{aligned}
[u] = [[v], [w]] &= \sum_{i,j} \alpha_i\beta_j[v_i, w_j] \\
&= \sum_{i,j} \alpha_i\beta_j(v_iw_j - p_{v_i,w_j}w_jv_i) \\
&= \sum_{i,j} \alpha_i\beta_j(v_iw_j - p_{v,w}w_jv_i) \\
&= [v][w] - p_{v,w}[w][v].
\end{aligned}$$

This proves (i) for u. Moreover, since $u = vw$, it is clear that $[u]$ is a polynomial of degree $l(u)$ which is homogeneous in the letters of u.

It only remains to prove that the leading word of $[u]$ is u with coefficient 1. Again, we induct on $l(u)$. If $l(u) = 1$, the statement is trivial. If $l(u) > 1$,

$$[u] = [[v], [w]] = [v][w] - p_{v,w}[w][v]$$

for some nonassociative Lyndon words $[v]$ and $[w]$. By (2.2) and induction, the leading word of $[v][w]$ is vw with coefficient 1; the leading word of $[w][v]$ is wv and $u = vw < wv$, by Lemma 2.1.2. □

Definition 2.2.6. Let $u \in \mathbb{X}$ be a Lyndon word. Then $[u]$, the corresponding nonassociative Lyndon word, is called a *super-letter*.

As for the general definition of $[\ ,\ ]$, there is a bijective correspondence between Lyndon words and super-letters, defined by $u \mapsto [u]$. Therefore, we can define an order on the set of super-letters by

$$[u] < [v] \Leftrightarrow u < v. \tag{2.8}$$

Using this total ordering, we can consider the set of super-letters as an alphabet and make the obvious definition of a "super-word".

Definition 2.2.7. (i) A word $[u]$ in super-letters is called a *super-word*.

(ii) Let $[u] := [u_1] \cdots [u_t]$, where $[u_1], \dots, [u_t]$ are super-letters. The super-word $[u]$ is *monotonic* if, in the ordering (2.8), $[u_1] \geq \cdots \geq [u_t]$.

Recall from the start of §2.1 the definitions of the structure and degree of a word $u \in \mathbb{X}$. By Lemma 2.2.5, super-letters, and hence super-words, are homogeneous in each x_i, so their structures and degrees can be defined in the obvious way. This notion of the degree of a super-letter or super-word should not be confused with the polynomial degree of the polynomial in x_i it defines. Since G is commutative, g_u and χ^u are the same for words of the same structure and hence for super-letters and super-words of the same structure.

It turns out that the ordering on monotonic super-words works in exactly the way we would expect:

Lemma 2.2.8. *[32, Lemma 5] Let*

$$V = [v_1][v_2] \cdots [v_m], \qquad W = [w_1][w_2] \cdots [w_n]$$

be monotonic super-words, so $[v_1], \ldots, [v_m]$ *and* $[w_1], \ldots, [w_n]$ *are super-letters, with* $v_1 \geq v_2 \geq \ldots \geq v_m$ *and* $w_1 \geq w_2 \geq \ldots \geq w_n$*. Let*

$$v := v_1 v_2 \cdots v_m, \qquad w := w_1 w_2 \cdots w_n.$$

Then, with the lexicographic ordering on super-words, defined using the ordering on super-letters defined in (2.8)*,* $V < W$ *if and only if* $v < w$*. Moreover, the leading word of* V *is* v *with coefficient 1.*

We also have the following lemma about the representation of non-Lyndon nonassociative words as a linear combination of super-words:

Lemma 2.2.9. *[32, Lemma 6] Let* u *and* u_1 *be Lyndon words with* $u < u_1$*. Then* $[[u], [u_1]]$ *is a linear combination of super-words* W*, where*

$$W = [w_1] \cdots [w_t], \ \ [w_i] \ \text{ super-letters}$$

such that $[u] < [w_i] < [u_1]$ *for all* i*, and such that* $uu_1 \leq w_i$ *for all* i*. The degree of every super-word* W *in the variables* $x_1, \ldots, x_n$ *is equal to that of* uu_1*.*

We provide a full proof of the following lemma, since a similar technique will be used later in the chapter and in Chapter 3.

Lemma 2.2.10. *[32, Lemma 7] Let* W *be a non-monotonic super-word. Then* W *is a linear combination of lexicographically greater monotonic super-words of the same structure, whose super-letters lie between (not strictly) the greatest and least super-letters of* W*.*

Proof. We induct on the polynomial degree of the polynomial defined by W, which is the same as the length of the underlying word of W. When W is of degree 1, W must be a letter, which is monotonic, so there is nothing to prove. Now assume that the lemma holds for super-words of polynomial degree less than m and let m be the degree of the polynomial defined by W.

Let the structure of W be $(m_1, \ldots, m_n)$, where $m_1 + \cdots + m_n = m$. Consider the finite set $\mathcal{S}$ of super-words with the same structure as W. The lexicographically greatest such super-word is

$$[x_n]^{m_n}[x_{n-1}]^{m_{n-1}} \cdots [x_1]^{m_1},$$

which is monotonic. We suppose that

$$W \text{ is the lexicographically greatest super-word in } \mathcal{S} \text{ such that the lemma fails} \tag{2.9}$$

and aim for a contradiction.

If W is a super-letter, then it is monotonic and there is nothing to prove. Therefore, let $W = UU_1U_2 \cdots U_t$, where $t \geq 1$, $U, U_1, U_2, \ldots, U_t$ are super-letters and $\deg(U_1 \cdots U_t) < m$. If $U_1 \cdots U_t$ is non-monotonic, by the induction hypothesis it is a linear combination of lexicographically greater monotonic super-words of the same structure. Therefore, without loss of generality, we can assume that $U_1 \cdots U_t$ is monotonic: that is,

$$U_1 \geq U_2 \geq \cdots \geq U_t.$$

If $U \geq U_1$, then W is monotonic and there is nothing to prove, so suppose $U < U_1$. Then by Lemma 2.2.5,

$$W = [U, U_1]U_2 \cdots U_t + p_{u,u_1} U_1 U U_2 \cdots U_t, \tag{2.10}$$

where $U = [u]$ and $U_1 = [u_1]$. Consider the second summand in the above equation: $U_1UU_2 \cdots U_t$ is a member of $\mathcal{S}$ and is lexicographically greater than W, since $U_1 > U$. Therefore, by our assumption (2.9), the second summand satisfies the lemma. Now consider the first summand in (2.10). By Lemma 2.2.9,

$$[U, U_1] = \sum_i \alpha_i \prod_j [w_{ij}],$$

where for all i, j, $\alpha_i \in k$ and $[w_{ij}]$ is a super-letter with $[w_{ij}] > U$. Consequently, $\prod_j [w_{ij}]U_2 \cdots U_s > W$. Using assumption (2.9), the first summand of (2.10), and hence W, can be written in the required form. □

The importance of the monotonic super-words can be seen in the following theorem:

Theorem 2.2.11. *[32, Theorem 1] The set of all monotonic super-words is a basis for* $k\langle X \rangle$.

Consider the special case where G is the trivial group, so $\chi = 1$. Let $\mathfrak{g}$ be the free Lie algebra on $\{x_1, \ldots, x_n\}$. The theorem reduces to [23, Theorem V.7], which states that $U(\mathfrak{g}) \cong k\langle X \rangle$.

2.3 Constructing the PBW-basis

Let H be a Hopf algebra generated by an abelian group $G = G(H)$ of grouplike elements and by skew-primitive elements $a_1, \ldots a_n$, where each a_i is associated with an element

$g_i \in G$, such that

$$\Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i,$$

and a character $\chi^i \colon G \to k \setminus \{0\}$. In addition, we assume the following commutation rule holds:

$$a_i g = \chi^i(g) \cdot g a_i, \tag{2.11}$$

for all $g \in G$. In other words, G acts diagonalisably on the vector space spanned by the a_i, $1 \leq i \leq n$. There could, of course, be relations among the a_i, $1 \leq i \leq n$, and the $g \in G$. However, we will construct H as a quotient of a free algebra acted on by a group algebra, which provides a way to apply the theory from the previous section to H.

Let $x_1, \ldots, x_n$ be indeterminates, and let $k\langle x_1, \ldots, x_n \rangle$ denote the free algebra on $\{x_1, \ldots, x_n\}$. Let G act as k-algebra automorphisms of $k\langle x_1, \ldots, x_n \rangle$ by setting

$$g(x_i) := \chi^i(g) x_i, \tag{2.12}$$

for $g \in G$ and $1 \leq i \leq n$, and form the skew group algebra

$$T := k\langle x_1, \ldots, x_n \rangle * G.$$

Define $\Delta \colon T \to T \otimes T$ by

$$\Delta(g) = g \otimes g, \qquad \Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i,$$

for $g \in G$ and $1 \leq i \leq n$. If T is to be a Hopf algebra with comultiplication Δ, this uniquely determines the counit $\varepsilon \colon T \to k$ and antipode $S \colon T \to T$ by

$$\varepsilon(g) = 1, \qquad \varepsilon(x_i) = 0$$
$$S(g) = g^{-1}, \qquad S(x_i) = -{g_{x_i}}^{-1} x_i,$$

for $g \in G$ and $1 \leq i \leq n$. In fact, it can be easily checked that these maps make T into a Hopf algebra, with $G = G(T)$. Then, clearly, there is an epimorphism of Hopf algebras $T \to H$, defined by $\pi(x_i) = a_i$, $1 \leq i \leq n$, and $\pi(g) = g$ for all $g \in G$. It restricts to a Hopf algebra epimorphism

$$\pi \colon k\langle x_1, \ldots, x_n \rangle \twoheadrightarrow k\langle a_1, \ldots, a_n \rangle \subset H.$$

Using G and χ, T can be endowed with a skew-commutator, as in (2.4).

Example 2.3.1. Suppose X, G, χ^1 and χ^2 are as in Examples 2.2.4 (ii). We construct the Hopf algebras T as above. We have $T = k\langle X\rangle * G$, where the relations are

$$g_1x_1 = q^{-2}x_1g_1,\;\; g_2x_1 = qx_1g_2,\;\; g_1x_2 = qx_2g_1,\;\; g_2x_2 = q^{-2}x_2g_2.$$

The Hopf algebra structure on T is obtained by making all $g \in G$ grouplike, and setting

$$\Delta(x_1) = x_1 \otimes 1 + g_1 \otimes x_1,\;\; \varepsilon(x_1) = 0,\;\; S(x_1) = -{g_1}^{-1}x_1,$$
$$\Delta(x_2) = x_2 \otimes 1 + g_2 \otimes x_2,\;\; \varepsilon(x_1) = 0,\;\; S(x_1) = -{g_1}^{-1}x_1.$$

Keeping the same G, χ^1 and χ^2, let H be a Hopf algebra generated by $G = G(H)$ together with skew-primitive elements a_1, a_2, associated to g_1, χ^1 and g_2, χ^2, respectively, such that (2.12) holds, with the additional relations

$${a_i}^2a_j - (q + q^{-1})a_ia_ja_i + a_j{a_i}^2 = 0,$$

for $i, j \in \{1, 2\}$ with $i \neq j$. Then there is an obvious Hopf algebra epimorphism $T \to H$, which restricts to a Hopf algebra epimorphism

$$k\langle x_1, x_2\rangle \twoheadrightarrow \frac{k\langle a_1, a_2\rangle}{\langle {a_i}^2a_j - (q + q^{-1})a_ia_ja_i + a_j{a_i}^2 \colon i \neq j\rangle}.$$

The map π enables us to translate the definitions and results from the previous section and those above to H. When we speak of, for example, a super-letter in H, this means an element of H that is equal to $\pi([u])$ for some super-letter $[u] \in T$. Similarly, we can define super-words and monotonic super-words in H.

Definition 2.3.2. (i) A *G-super-word* is a product in T of the form gW, where $g \in G$ and $W \in T$ is a super-word.

(ii) A *monotonic* G-super-word is a G-super-word gW such that W is a monotonic superword.

By (2.12) every product of a super-word and a grouplike is a G-super-word of the same structure. It is a consequence of Theorem 2.2.11 and the construction of T that T is spanned by the monotonic G-superwords.

Recall the definition of structure and degree of super-words and super-letters in T. Since the relations in H may not respect the degree in T, the deg function is not well-defined on H. This forms the basis for the following definition.

Definition 2.3.3. A super-letter $\pi([u]) \in H$ is *hard* if it is not a linear combination of the following elements of H:

- super-words $\pi(W)$ with $\deg(W) = \deg([u])$ such that if

$$W = [u_1] \cdots [u_n], \qquad [u_1], \ldots, [u_n] \text{ super-letters,}$$

  then $[u_i] > [u]$ for $1 \leq i \leq n$;

- G-super-words $g\pi(V)$ such that $\deg(V) < \deg([u])$.

Example 2.3.4. Let H and T be as in Example 2.3.1. Then $[{x_1}^2 x_2]$ is a super-letter in T, but $\pi([{x_1}^2 x_2])$ is not a hard super-letter in H, since, using (2.7),

$$\begin{aligned}
\pi([{x_1}^2 x_2]) &= \pi({x_1}^2 x_2 - (q + q^{-1}) x_1 x_2 x_1 + x_2 {x_1}^2) \\
&= {a_1}^2 a_2 - (q + q^{-1}) a_1 a_2 a_1 + a_2 {a_1}^2 \\
&= 0.
\end{aligned}$$

In fact, it can be shown that the only hard super-letters in H are $\pi(x_1) = a_1$, $\pi(x_2) = a_2$ and $\pi([x_1 x_2]) = a_1 a_2 - q a_2 a_1$.

Definition 2.3.5. The *height* $h(\pi([u]))$ of a super-letter $\pi([u]) \in H$ of degree d is the least natural number with the following properties:

(i) $p_{u,u}$ is a primitive t^{th} root of unity for some $t \geq 1$ and either $h = t$ or $h = tl^m$, where $l = \operatorname{char} k > 0$ and m is a non-negative integer.

(ii) the super-word $\pi([u]^h)$ is a linear combination of the following elements of H:

   - super-words of degree hd in lexicographically greater super-letters than $[u]$;
   - G-super-words of a lesser degree than $[u]$.

If no such natural number $h(\pi([u]))$ exists, we say $h = \infty$.

Definition 2.3.6. A monotonic G-super-word in H,

$$g\pi(W) = g\pi([u_1]^{k_1} \cdots [u_n]^{k_n}), \qquad [u_1] > [u_2] > \cdots > [u_n]$$

is *restricted* if $k_i < h(\pi([u_i]))$ for all $1 \leq i \leq n$.

We are now able to state the theorem giving a PBW-basis for H.

Theorem 2.3.7. *[32, Theorem 2] The set of monotonic restricted G-super-words in hard super-letters forms a basis for H.*

A motivating example to illustrate the application of this theorem is the Borel Hopf subalgebra ${U_q}^{\geq 0}(\mathfrak{g})$ of $U_q(\mathfrak{g})$, for a semisimple Lie algebra $\mathfrak{g}$. A PBW-basis for ${U_q}^{\geq 0}(\mathfrak{g})$ can be found in [16, Theorem 9.3(i)]. We consider the simplest non-trivial case: $\mathfrak{g} = \mathfrak{sl}_3$ and show that it is a Hopf algebra of the form of H:

Example 2.3.8. ${U_q}^{\geq 0}(\mathfrak{sl}_3(k))$ is the k-algebra with generators $E_1, E_2, K_1^{\pm 1}, K_2^{\pm 1}$, and relations, for $i, j \in \{1, 2\}$:

$$K_i K_j = K_j K_i$$
$$K_i E_j {K_i}^{-1} = q^2 E_j \ \ (i = j), \ \ K_i E_j {K_i}^{-1} = q^{-1} E_j \ \ (i \neq j),$$
$$ {E_i}^2 E_j - (q + q^{-1}) E_i E_j E_i + E_j {E_i}^2 = 0 \ \ (i \neq j).$$

There is a Hopf algebra structure on ${U_q}^{\geq 0}(\mathfrak{sl}_3(k))$ determined by the following:

$$\begin{aligned} \Delta(K_i) &= K_i \otimes K_i, & \varepsilon(K_i) &= 1, & S(K_i) &= {K_i}^{-1}, \\ \Delta(E_i) &= E_i \otimes 1 + K_i \otimes E_i, & \varepsilon(E_i) &= 0, & S(E_i) &= -{K_i}^{-1} E_i. \end{aligned}$$

Let H be as in Example 2.3.1. Then, as Hopf algebras, $H \cong {U_q}^{\geq 0}(\mathfrak{sl}_3)$ via

$$a_1 \mapsto E_1, \ \ a_2 \mapsto E_2, \ \ g_1 \mapsto K_1, \ \ g_2 \mapsto K_2.$$

Therefore, the above theorem gives a PBW basis for ${U_q}^{\geq 0}(\mathfrak{sl}_3)$:

$$\{ {K_1}^p {K_2}^q {E_2}^i (E_1 E_2 - q E_2 E_1)^j {E_1}^l \colon i, j, l \in \mathbb{Z}^{\geq 0}, p, q \in \mathbb{Z} \}.$$

2.4 A condition ensuring that H is noetherian

Throughout §2.4, we keep the assumptions on H from §2.3, including (2.11) and (2.12). In addition, we assume that

$$H \text{ has only finitely many hard super-letters.} \tag{2.13}$$

Theorem 2.4.1. *[32, Corollary 5] If* (2.13) *holds and G is finitely generated, then H is left and right noetherian.*

In order to prove Theorem 2.4.1, we construct a filtration on H such that the associated graded algebra $\operatorname{gr} H$ is noetherian.

The filtration

Let R be the set of all words in $k\langle a_1, \dots a_n\rangle$ whose degree is at most $D\hat{h}$, where

$$D = \max\{\text{degree of a hard super-letter in } H\}$$

and

$$\hat{h} = \max\{2, \max\{h\colon h \text{ is height of a hard super-letter in } H \text{ of finite height}\}\}.$$

For a word $u \in R$, let

$$\mathcal{L}(u) = \{u' \in R\colon u' \geq u\}$$

and define

$$n(u) = |\mathcal{L}(u)|.$$

Since a_1 is the lexicographically smallest word in R, we have $L := n(a_1) = |R|$. We choose $M \in \mathbb{N}$ such that M is greater than the maximum length of any word in R.

Definition 2.4.2. (i) The filtration degree on hard super-letters $\pi([u]) \in H$ is defined by

$$\operatorname{Deg}(\pi([u])) = M^{L+1}\deg(u) + M^{n(u)}. \tag{2.14}$$

(ii) The filtration degree of a PBW-basis element $g\pi(W) \in H$ is the sum of the filtration degrees of the super-letters of $\pi(W)$. That is, if

$$W = [w_1][w_2]\cdots[w_t], \qquad [w_1] \geq [w_2] \geq \ldots \geq [w_t]$$

where $\pi([w_i])$ is a hard super-letter for all i, and $\pi(W)$ is restricted, then

$$\operatorname{Deg}(g\pi(W)) = \operatorname{Deg}(\pi([w_1])) + \operatorname{Deg}(\pi([w_2])) + \cdots + \operatorname{Deg}(\pi([w_t])).$$

(iii) The filtration degree of any element $h \in H$ is the maximal filtration degree of the basis elements occurring in its PBW-basis decomposition. That is, if h has PBW-basis decomposition

$$h = \sum_i \alpha_i \pi(g_i W_i),$$

where $\alpha_i \in k$ and $g_i W_i$ are PBW-basis elements for all i, then

$$\operatorname{Deg}(h) = \max\{\operatorname{Deg}(\pi(g_i W_i)\}.$$

Lemma 2.4.3. *[32, Lemma 14] If* (2.13) *holds , then the function* Deg *defines a filtration on H, with*

$$H_0 = kG, \qquad H_k = \{T \in H\colon \operatorname{Deg}(T) \leq k\}. \tag{2.15}$$

Proof. All that needs to be shown is that $H_k H_s \subset H_{k+s}$. That is, we must show that, for elements T_1 and T_2 of H, that

$$\operatorname{Deg}(T_1 T_2) \leq \operatorname{Deg} T_1 + \operatorname{Deg} T_2. \tag{2.16}$$

To do this, we construct another degree D' associated to linear combinations of G-superwords - in other words, elements of H that are not necessarily written in the form of their PBW-basis decomposition. For $h \in H$, $D'(h)$ will depend not only on h, but on the particular way in which h is expressed as a linear combination of G-super-words, so D' is not a well-defined function. To avoid cumbersome notation, we will suppress the particular expression of h when we write $D'(h)$, if the expression is clear from the context.

Definition 2.4.4. (i) The D' degree of any super-letter $\pi([u]) \in H$, which we do not assume to be necessarily hard, is given by formula (2.14).

(ii) The D'-degree of a product of super-letters is the sum of D'-degrees of its factors. That is, if $U \in R$ with

$$U = g\pi([u_1][u_2]\cdots[u_t]),$$

where $g \in G$, and, for all i, $\pi[u_i]$ is a super-letter, which we do not assume to be necessarily hard, then

$$D'(U) = D'(\pi([u_1])) + D'(\pi([u_2])) + \cdots + D'(\pi([u_t])).$$

(iii) The D'-degree of an element $h \in H$ is the maximum D'-degree of its summands. That is, if

$$h = \sum_i \alpha_i \pi(g_i U_i),$$

where $\alpha_i \in k$ and $g_i U_i$ is a G-super-word, which we do not assume to be necessarily monotonic, restricted, or a word in hard super-letters, then

$$D'(h) = \max\{D'(\pi(g_i U_i)\}.$$

We shall prove below that,

$$\begin{array}{l}\textit{if } h \in H \textit{ is written as any possible linear combination of the image of} \\ G\textit{-super-words under } \pi, \textit{then } D'(h) \textit{ does not increase when } h \textit{ is expressed} \\ \textit{as a linear combination of PBW-basis elements.}\end{array} \tag{2.17}$$

Before doing this, we note that (2.16) would then follow. For, when $h \in H$ is written in its PBW-basis decomposition form, we have, by the definition of D',

$$D'(h) = \mathrm{Deg}(h). \tag{2.18}$$

Let T_1 and T_2 be given in their PBW-basis form and consider the form of T_1T_2 given by simply juxtaposing the linear combinations of PBW-basis elements defining T_1 and T_2. Then

$$\mathrm{Deg}(T_1T_2) \leq D'(T_1T_2) = \mathrm{Deg}\, T_1 + \mathrm{Deg}\, T_2,$$

where the inequality follows from (2.18) and (2.17), and the equality from (ii) of Definition 2.4.4 and (2.18).

We now prove (2.17). Note that expressing any element of H as a linear combination of PBW-basis elements requires the following operations:

(i) Replacing any non-hard super-letter by a linear combination of super-words of the same degree in lexicographically greater super-letters plus a linear combination of G-super-words of lesser degree. We can do this by Definition 2.3.3, the definition of "hard".

(ii) Replacing instances of $\pi([u]^h)$, where $\pi([u])$ is a hard super-letter and $h = h(\pi([u]))$, by a linear combination of super-words of the same degree in lexicographically greater super-letters plus a linear combination of the image of G-super-words under π of lesser degree. We can do this by Definition 2.3.5, the definition of "height".

(iii) Replacing any non-monotonic super-word with a linear combination of monotonic super-words of the same degree in lexicographically greater super-letters. We can do this by Lemma 2.2.10.

These three operations are then repeated, if necessary. This process must lead to the PBW-basis decomposition, since it can only be carried out a finite number of times. This is because each step replaces a super-letter or super-word with a linear combination of super-words, each super-word either having strictly smaller degree, or having the same degree but being lexicographically bigger, and there are only finitely many super-words satisfying these conditions. We consider each of these operations separately and show that carrying out each of them does not increase D'.

(i) Let $\pi([u]) \in R$ be a non-hard super-letter. Then we can write $\pi([u])$ as follows:

$$\pi([u]) = \sum_i \alpha_i \prod_{j=1}^{m(i)} \pi([w_{ij}]) + \sum_s \beta_s g_s \prod_{t=1}^{m'(s)} \pi([v_{st}]). \tag{2.19}$$

In (2.19), $\alpha_i, \beta_j \in k$ for all i, j; $g_s \in G$ for all s; and $\pi([w_{ij}])$ and $\pi([v_{st}])$ are super-letters for all i, j, s, t; such that

- $[w_{ij}] > [u]$ for all i, j,
- $\sum_j \deg w_{ij} = \deg u$ for all i, j,
- $\sum_t \deg v_{st} \leq \deg u - 1$.

By definition of R, all w_{ij}, all products $\prod_j^{m(i)} w_{ij}$, all v_{st} and all products $\prod_t^{m'(s)} v_{st}$ belong to R. Therefore, their lengths are less than M and so the number of factors $m(i), m'(s)$ in every summand is less than M. Hence

$$\begin{aligned} D'\Big(\prod_j^{m(i)} \pi([w_{ij}])\Big) &= \sum_j M^{L+1} \deg w_{ij} + \sum_j M^{n(w_{ij})} \\ &= M^{L+1} \deg u + \sum_j M^{n(w_{ij})} \\ &< M^{L+1} \deg u + M \cdot M^{n(u)-1} \\ &= M^{L+1} \deg u + M^{n(u)} = D'(\pi([u])). \end{aligned}$$

Similarly,

$$\begin{aligned} D'\Big(\prod_t^{m'(s)} \pi([v_{st}])\Big) &= \sum_s M^{L+1} \deg v_{st} + \sum_s M^{n(v_{st})} \\ &< M^{L+1}(\deg u - 1) + M \cdot M^{L} \\ &= M^{L+1} \deg u \\ &= D'(\pi([u])) - M^{n(u)} < D'(\pi([u])). \end{aligned}$$

Therefore,

$$D'(\sum_i \alpha_i \prod_{j=1}^{m(i)} \pi([w_{ij}]) + \sum_s \beta_s g_s \prod_{t=1}^{m'(s)} \pi([v_{st}])) < D'(\pi([u])).$$

(ii) The argument is exactly the same when $\pi([u]^h)$ is replaced with

$$\sum_i \alpha_i \prod_{j=1}^{m(i)} \pi([w_{ij}]) + \sum_s \beta_s g_s \prod_{t=1}^{m'(s)} \pi([v_{st}]).$$

(iii) We now use the process of Lemma 2.2.10 to replace non-monotonic super-words.

Let W be a non-monotonic super-word. By Lemma 2.2.10, W can be written as a linear combination of monotonic super-words of the same degree. We induct on the degree of the polynomial defined by W to prove that $D'(\pi(W))$ is unincreased.

If the degree of the polynomial defined by W is 1, W is trivially always monotonic. If the polynomial degree is 2, since W is non-monotonic, we have

$$W = [u][u_1], \qquad u < u_1,$$

where $u, u_1 \in X$. By Lemma 2.2.5,

$$W = [u, u_1] + p_{u,u_1}[u_1][u].$$

For the second summand,

$$D'(\pi(p_{u,u_1}[u_1][u])) = D'(\pi(W)),$$

since it is just a scalar multiple of a rearrangement of the super-letters of W. We now calculate a bound for the first summand. By Lemma 2.2.9,

$$[u, u_1] = \sum_i \prod_j [w_{ij}],$$

where $[w_{ij}] > [u]$ and $\prod_j [w_{ij}]$ has the same degree as W, for all i, j. Hence, $w_{ij} \in R$, so $n(w_{ij}) \leq n(w) - 1$. Also, the number of factors in $\prod_j [w_{ij}]$ is less than M. Therefore,

$$\begin{aligned} D'(\prod_j \pi([w_{ij}])) &= \sum_j M^{L+1} \deg(w_{ij}) + \sum_j M^{n(w_{ij})} \\ &= M^{L+1} \deg w + \sum_j M^{n(w_{ij})} \\ &< M^{L+1} \deg w + M \cdot M^{n(w)-1} \\ &= M^{L+1} \deg w + M^{n(w)} = D'(\pi(W)). \end{aligned}$$

So we have

$$\pi(W) = \sum_i \prod_j \pi([w_{ij}]) + \pi(p_{u,u_1}[u_1][u]),$$

where the RHS is a linear combination of monotonic super-words, as required. We have just shown that both summands have D'-degree less than or equal to $D'(\pi(W))$, so the polynomial degree 2 case is proved.

Now for the induction step. Suppose the polynomial degree is $n \geq 2$ and let $W = UU_1 \cdots U_t$ be non-monotonic. Then from (2.10) in the proof of Lemma 2.2.10, $W = \sum_k UW_i$, such that

$$UW_k = [U, V_1]V_2 \cdots V_s + p_{u,v_1} V_1 U V_2 \cdots V_s, \qquad V_1 \geq V_2 \geq \cdots \geq V_s.$$

The second summand has D'-degree equal to that of W, since it is just a scalar multiple of a rearrangement of the super-letters of W. By Lemma 2.2.9, we can write the first summand as

$$[U, V_1]V_2 \cdots V_s = \sum_i \prod_j [w_{ij}]V_2 \cdots V_s,$$

where $[w_{ij}] > U$ and $\prod_j [w_{ij}]$ has the same structure as UV_1, for all i, j. The exact same calculation as for the polynomial degree 2 case shows that

$$D'(\sum_i \prod_j \pi([w_{ij}])) < D'(\pi(UV_1)). \tag{2.20}$$

Hence, we have

$$D'(\sum_i \prod_j \pi([w_{ij}]V_2 \cdots V_s)) < D'(\pi(UV_1V_2 \cdots V_s)) = D'(\pi(W)).$$

So we can write $\pi(W)$ as a linear combination of monotonic super-words such that the D'-degree of every summand is less than or equal to $D'(\pi(W))$. Thus, the lemma is proved. □

Note that for hard super-letters $\pi([u]), \pi([v])$ with $[u] < [v]$ and $h = h(\pi[u])$, we have the following inequalities:

$$\mathrm{Deg}(\pi([u][v] - p_{u,v}[v][u])) < \mathrm{Deg}(\pi([u])) + \mathrm{Deg}(\pi([v])) \tag{2.21}$$

and similarly

$$\mathrm{Deg}(\pi([u]^h)) < h\,\mathrm{Deg}(\pi([u])). \tag{2.22}$$

Proof. For (2.21), since $\pi([u]), \pi([v])$ are hard, we have

$$D'(\pi([u][v])) = \mathrm{Deg}(\pi([u][v])) = \mathrm{Deg}(\pi([u])) + \mathrm{Deg}(\pi([v])).$$

Therefore, (2.21) follows from (2.20) in part (iii) of the process described in the above proof, when we take $[u] = U$ and $[v] = V_1$.

For (2.22), note that $D'(\pi([u]^h)) = h\,\mathrm{Deg}(\pi([u]))$, since $\pi([u])$ is hard. Therefore, (2.22) follows from part (ii) of the above process. □

Associated graded algebra

Let the finitely many hard super-letters of H be denoted

$$[u_1] < [u_2] < \ldots < [u_s].$$

To each hard super-letter $[u_i]$, we associate a new variable x_{u_i}. For $1 \leq m \leq s$, let

$${H_m}^* = k\langle x_{u_1}, \ldots, x_{u_m}\rangle / J_m,$$

where J_m is the ideal of ${H_m}^*$ generated by all elements of the form

$$x_{u_i} x_{u_j} - p_{u_i,u_j} x_{u_j} x_{u_i}, \tag{2.23}$$

for all $1 \leq i < j \leq m$. Let the action of G on ${H_i}^*$ be given by $g \cdot x_{u_i} = \chi^{u_i}(g) \cdot x_{u_i}$, for all $1 \leq i \leq s$. We may thus form the skew group algebra ${H_m}^* * G$. Let $H^* := {H_s}^*$ and let

$$S = (H^* * G)/\langle {x_u}^h \colon [u] \text{ of finite height } h\rangle.$$

Theorem 2.4.5. *[32, Theorem 3] If* (2.13) *holds, then* $\mathrm{gr}\, H$*, the associated graded algebra of* H *with respect to the* Deg*-filtration, is isomorphic to* S*.*

Proof. The algebra on the right hand side of the isomorphism can be expressed as the quotient of the free algebra on the set

$$\{x_u \colon [u] \text{ a hard super-letter}\} \cup \{g_i \colon 1 \leq i \leq t\},$$

where t is the number of generators of G, subject to the relations

- the defining relations for G;
- $g \cdot x_{u_i} = \chi^{u_i}(g) \cdot x_{u_i}$, for all $1 \leq i \leq s$;
- the relations (2.23).

Since $\mathrm{gr}\, H$ has a generating set of the same cardinality (say labelled by ${x_u}'$ and ${g_u}'$), for which all of the above relations hold, thanks to (2.21) and (2.22), there is an algebra epimorphism from S to $\mathrm{gr}\, H$, sending x_u to ${x_u}'$. That this is injective follows from the facts that

(i) S has a PBW-basis,

(ii) $\operatorname{gr} H$ has a PBW-basis,

both exactly the same. $\square$

We can now finish the proof of Theorem 2.4.1. Clearly, ${H_1}^* = k[x_{u_1}]$, which is noetherian by [20, Theorem 1.9]. For all $1 \leq m \leq s$, ${H_{m+1}}^*$ is a factor of a skew polynomial ring over ${H_m}^*$:

$${H_{m+1}}^* = {H_m}^*[x_{u_{m+1}}; \sigma_m],$$

where σ_m is the automorphism of ${H_m}^*$ defined by $\sigma_m(x_{u_i}) := p_{u_i,u_{m+1}} x_{u_i}$. Therefore, $H^* = {H_s}^*$ is noetherian by inductive application of [40, Theorem 1.2.9]. Furthermore, $H^* * G$ is noetherian by [40, Theorem 1.5.2]. By Theorem 2.4.5,

$$\operatorname{gr} H \cong (H^* * G)/\langle {x_u}^h \colon [u] \text{ of finite height } h\rangle,$$

and so $\operatorname{gr} H$ is also noetherian. Finally, H is noetherian by [40, Theorem 1.6.9].

Chapter 3

Homological properties of pointed Hopf algebras

This chapter involves the application of the tools developed in the previous chapter, namely the PBW-basis for a Nichols algebra of a diagonally braided vector space, and its Deg filtration when there are only a finite number of PBW-generators. Throughout this chapter, let H be a Hopf algebra as in §2.3; that is, H is generated by an abelian group $G = G(H)$ of group-like elements and by skew-primitive semi-invariant elements $a_1, \ldots a_n$, such that (2.11) holds. Suppose that H has a finite number of hard super-letters, denoted

$$U_1 < U_2 < \ldots < U_m.$$

Firstly, we prove that the order of the PBW-generators in the basis may be permuted, with the resulting set of ordered monomials remaining a basis. Next, we use this to determine various homological properties satisfied by the Nichols algebra of a diagonally braided vector space, under certain conditions.

3.1 Re-ordering the PBW-basis

Theorem 2.3.7 gives the PBW-basis of H as

$$\{{U_1}^{k_1}{U_2}^{k_2}\cdots{U_m}^{k_m}: \ \ 0 \leq k_i < h(U_i) \ \forall \ i\}. \tag{3.1}$$

The ordering of the PBW-generators in the super-words constituting the basis elements is determined by the lexicographic ordering of $U_1, \ldots, U_m$. However, we could impose a different ordering on $U_1, \ldots, U_m$ and consider super-words of the same form as the PBW-basis with respect to this new ordering. That is, there is an action of the symmetric group

S_m on the set (3.1) which permutes the ordering of the hard super-letters in the following way. For all $W := {U_1}^{k_1}{U_2}^{k_2}\cdots{U_m}^{k_m}$, with $0 \le k_i < h(U_i)$ for all $1 \le i \le m$, and for all $\sigma \in S_m$, define

$$\sigma^{-1} \cdot W := {U_{\sigma(1)}}^{k_{\sigma(1)}}{U_{\sigma(2)}}^{k_{\sigma(2)}}\cdots{U_{\sigma(m)}}^{k_{\sigma(m)}}.$$

The section is concerned with the proof of the following theorem.

Theorem 3.1.1. *Let $\sigma \in S_m$, the symmetric group on m letters. Then*

$$S := \{{U_{\sigma(1)}}^{k_{\sigma(1)}}{U_{\sigma(2)}}^{k_{\sigma(2)}}\cdots{U_{\sigma(m)}}^{k_{\sigma(m)}} : \ \ 0 \le k_i < h(U_i)\ \ \forall\ \ i\}$$

is a PBW-basis for H.

Remark. On first glance, it might be thought that the ability to permute the hard super-letters, or PBW-basis generators, is a straightforward consequence of reordering the alphabet $\{x_1, \dots, x_n\}$ with which we started Chapter 2. However, doing so gives a new set of Lyndon words and so a different set of hard super-letters, rather than a rearrangement of the original set. For example, swapping the ordering of x_1 and x_2 in Example 2.2.4 leads to a PBW-basis for $U_q(\mathfrak{sl}_3)$ of the form

$$\{{K_1}^p{K_2}^q{E_1}^i(E_2E_1 - qE_1E_2)^j{E_2}^l : i,j,l \in \mathbb{Z}^{\ge 0}, p,q \in \mathbb{Z}\}.$$

Here, we obtain a new hard super-letter $E_2E_1 - qE_1E_2$, rather than $E_1E_2 - qE_2E_1$, as previously. In this case, there is only a small difference between "new" and "old" hard super-letters, but in a more complex example with a greater number of hard super-letters, it may be more pronounced.

3.1.1 Some technical lemmas about hard super-letters

First, we need the following lemma, which extends Lemma 2.2.5.

Lemma 3.1.2. *Let $V = [v], W = [w]$ be super-letters. Then, for $k, l \ge 1$,*

$$[V^k, W^l] = V^kW^l - p_{v^k,w^l}W^lV^k.$$

Proof. We do a double induction on k, l. If $k = l = 1$, this is just Lemma 2.2.5. Now suppose $k > 1$, and $l = 1$. Then

$$\begin{aligned}
[V^k, W] &= [V^{k-1}V, W] = p_{v,w}[V^{k-1}, W]V + V^{k-1}[V, W] \\
&= p_{v,w}(V^{k-1}WV - p_{v^{k-1},w}WV^k) + V^{k-1}(VW - p_{v,w}WV) \\
&= V^kW - p_{v^k,w}WV^k,
\end{aligned}$$

where the first line follows by (2.6), the second by induction and Lemma 2.2.5, and the third by (2.3).

Now suppose $k > 1$ and $l > 1$. Then

$$\begin{aligned}[V^k, W^l] &= [V^k, WW^{l-1}] = [V^k, W]W^{l-1} + p_{v^k,w}W[V^k, W^{l-1}] \\ &= (V^kW - p_{v^k,w}WV^k)W^{l-1} + p_{v^k,w}W(V^kW^{l-1} - p_{v^k,w^{l-1}}W^{l-1}V^k) \\ &= V^kW^l - p_{v^k,w^l}W^lV^k,\end{aligned}$$

where the first line follows by (2.5), the second by the previous paragraph and by induction, and the third by (2.3). □

The following lemma extends (2.21).

Lemma 3.1.3. *Let $V > W$ be hard super-letters. Then, for $k, l \geq 1$,*

$$\mathrm{Deg}([W^l, V^k]) < k \,\mathrm{Deg}\, V + l \,\mathrm{Deg}\, W.$$

Proof. With an obvious abuse of notation, in $\mathrm{gr}\, H$, $WV = p_{w,v}VW$. Hence, still in $\mathrm{gr}\, H$,

$$W^lV^k = (p_{w,v})^{k+l}V^kW^l = p_{w^l,v^k}V^kW^l,$$

by (2.3). Therefore, by Lemma 3.1.2,

$$\begin{aligned}\mathrm{Deg}([W^l, V^k]) &= \mathrm{Deg}(W^lV^k - p_{w^l,v^k}V^kW^l) \\ &< \mathrm{Deg}\, V^k + \mathrm{Deg}\, W^l \\ &= k\,\mathrm{Deg}\, V + l\,\mathrm{Deg}\, W. \quad \square \end{aligned} \tag{3.2}$$

Lemma 3.1.4. *Let $\sigma \in S_m$ and let*

$$W := {U_{\sigma(1)}}^{k_{\sigma(1)}}{U_{\sigma(2)}}^{k_{\sigma(2)}} \cdots {U_{\sigma(m)}}^{k_{\sigma(m)}}, \qquad 0 \leq k_i < h(U_i) \;\; \forall \;\; i.$$

Then

$$\mathrm{Deg}(W) = k_1 \,\mathrm{Deg}(U_1) + \cdots + k_m \,\mathrm{Deg}(U_m).$$

Proof. Let $\widehat{W}$ be a super-word in the hard super-letters $U_1, \ldots, U_m$, with exactly k_i occurrences of U_i, where $0 \leq k_i < h(U_i)$ for $1 \leq i \leq m$. We prove a slightly stronger result than in the statement of the lemma: namely, that

$$\mathrm{Deg}(\widehat{W}) = k_1 \,\mathrm{Deg}(U_1) + \cdots + k_m \,\mathrm{Deg}(U_m). \tag{3.3}$$

Let $\mathcal{S}$ be the set of super-words in $U_1, \ldots, U_m$ with the same structure as $\widehat{W}$. If $\widehat{W}$ is the lexicographically biggest super-word in this set, then

$$\widehat{W} = {U_m}^{k_m} \cdots {U_1}^{k_1}.$$

Therefore, $\widehat{W}$ is a PBW-basis element, and (3.3) certainly holds, by Definition 2.4.2 (ii).

We now induct on the lexicographic ordering of the elements of $\mathcal{S}$. Suppose $\widehat{W}$ is not the lexicographically biggest super-word in $\mathcal{S}$. Then $\widehat{W} = W' U_p U_{p+q} W''$ for some words W', W'' in $U_1, \ldots, U_m$, some $1 \leq p \leq m$ and some $0 < q \leq m - p$. Therefore,

$$\widehat{W} = W'[U_p, U_{p+q}]W'' + p_{u_p, u_{p+q}} W' U_{p+q} U_p W'' \tag{3.4}$$

It can be seen from (2.21) that

$$D'([U_p, U_{p+q}]) < D'(U_p U_{p+q}). \tag{3.5}$$

Therefore,

$$\mathrm{Deg}(W'[U_p, U_{p+q}]W'') \leq D'(W'[U_p, U_{p+q}]W'') < D'(\widehat{W}),$$

where the first inequality arises from (2.17) and the second from (3.5). By induction,

$$\mathrm{Deg}(p_{u_p, u_{p+q}} W' U_{p+q} U_p W'') = k_1 \,\mathrm{Deg}(U_1) + \cdots + k_m \,\mathrm{Deg}(U_m) = D'(\widehat{W}),$$

and so

$$\mathrm{Deg}(W'[U_p, U_{p+q}]W'') < \mathrm{Deg}(p_{u_p, u_{p+q}} W' U_{p+q} U_p W'').$$

Applying this fact, together with Definition 2.4.2 (iii), to (3.4), completes the proof. □

3.1.2 Proof of the theorem: transposition case

We can now take a step towards proving Theorem 3.1.1 in the easiest case: when σ is a simple transposition.

Lemma 3.1.5. *Let $\sigma \in S_m$ be a simple transposition, so $\sigma = (i, i+1)$ for some $1 \leq i \leq m - 1$. Then the monomials of the form*

$${U_1}^{k_1} \cdots {U_{i-1}}^{k_{i-1}} {U_{i+1}}^{k_{i+1}} {U_i}^{k_i} {U_{i+2}}^{k_{i+2}} \cdots {U_m}^{k_m}, \qquad 0 \leq k_i < h(U_i) \ \forall \ i, \tag{3.6}$$

span H.

Proof. We need to show that any element

$$B := {U_1}^{l_1}{U_2}^{l_2}\cdots {U_m}^{l_m}, \qquad 0 \le l_i < h(U_i)\ \forall\ i,$$

of the usual PBW-basis of H is a linear combination of elements of the form of (3.6). We induct on $\operatorname{Deg}(B)$. Suppose $\operatorname{Deg}(B) = c$, where

$$c := \min\{\operatorname{Deg}(U_j)\colon 1 \le j \le m\}.$$

Then $B = U_j$ for some $1 \le j \le m$, which is of the same form as (3.6). Now suppose $\operatorname{Deg}(B) = d$ and that any PBW-basis element with Deg-value less than d is a linear combination of elements of the form of (3.6). We have, by Lemma 3.1.2,

$$\begin{aligned} B = {} & (p_{{u_{i+1}}^{l_{i+1}},{u_i}^{l_i}})^{-1}{U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}[{U_{i+1}}^{l_{i+1}},{U_i}^{l_i}]{U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m} \\ & + (p_{{u_{i+1}}^{l_{i+1}},{u_i}^{l_i}})^{-1}{U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}{U_{i+1}}^{l_{i+1}}{U_i}^{l_i}{U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m}. \end{aligned}$$

The second summand is of the same form as (3.6). Consider the first summand. We have

$$\begin{aligned} & \operatorname{Deg}({U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}[{U_{i+1}}^{l_{i+1}},{U_i}^{l_i}]{U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m}) \\ & \quad \le \operatorname{Deg}({U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}) + \operatorname{Deg}([{U_{i+1}}^{l_{i+1}},{U_i}^{l_i}]) + \operatorname{Deg}({U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m}) \text{ by (2.16)} \\ & \quad < \operatorname{Deg}({U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}) + l_i \operatorname{Deg}(U_i) + l_{i+1}\operatorname{Deg}(U_{i+1}) \\ & \qquad\qquad + \operatorname{Deg}({U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m}) \text{ by Lemma 3.1.3} \\ & \quad = \operatorname{Deg}(B) = d \text{ by Definition 2.4.2 (ii).} \end{aligned}$$

Hence, by induction, ${U_1}^{l_1}\cdots {U_{i-1}}^{l_{i-1}}[{U_{i+1}}^{l_{i+1}},{U_i}^{l_i}]{U_{i+2}}^{l_{i+2}}\cdots {U_m}^{l_m}$ is a linear combination of elements of the form of (3.6), as required. Therefore, so is B. □

3.1.3 Proof of the theorem: general case

The previous lemma enables us to prove the spanning part of Theorem 3.1.1.

Lemma 3.1.6. *Let $\sigma \in S_m$. Then the monomials of the form*

$${U_{\sigma(1)}}^{k_{\sigma(1)}}{U_{\sigma(2)}}^{k_{\sigma(2)}}\cdots {U_{\sigma(m)}}^{k_{\sigma(m)}}, \qquad 0 \le k_i < h(U_i)\ \forall\ i,$$

span H.

Proof. σ^{-1} can be expressed as a product of simple transpositions:

$$\sigma^{-1} = (i_t, i_t + 1)(i_{t-1}, i_{t-1} + 1)\cdots(i_1, i_1 + 1).$$

We will induct on t. If $t = 1$, this is just Lemma 3.1.5. Now suppose $t > 1$ and let

$$\sigma'^{-1} = (i_{t-1}, i_{t-1}+1) \cdots (i_1, i_1+1).$$

By induction, if B is one of the usual PBW-basis elements of H, then B is a linear combination of elements of the form

$$U_{\sigma'(1)}{}^{l_{\sigma'(1)}} U_{\sigma'(2)}{}^{l_{\sigma'(2)}} \cdots U_{\sigma'(m)}{}^{l_{\sigma'(m)}}, \qquad 0 \le l_i < h(U_i) \ \forall \ i. \tag{3.7}$$

Let $j := i_t$. Since $\sigma^{-1} = (j, j+1)\sigma'^{-1}$, we also have $\sigma'(j, j+1) = \sigma$ and it is enough to show that an element C of the form of (3.7) can be expressed as a linear combination of elements of the form

$$U_{\sigma'(1)}{}^{k_{\sigma'(1)}} U_{\sigma'(2)}{}^{k_{\sigma'(2)}} \cdots U_{\sigma'(j+1)}{}^{k_{\sigma'(j+1)}} U_{\sigma'(j)}{}^{k_{\sigma'(j)}} U_{\sigma'(j+2)}{}^{k_{\sigma'(j+2)}} \cdots U_{\sigma'(m)}{}^{k_{\sigma'(m)}}, \tag{3.8}$$

where $0 \le k_i < h(U_i)$ for all $1 \le i \le m$. We induct on $\mathrm{Deg}(C)$. Let $\mathrm{Deg}(C) = c$, where

$$c := \min\{\mathrm{Deg}(U_j) \colon 1 \le j \le m\}.$$

Then $C = U_j$ for some $1 \le j \le m$, which is of the form of (3.8).

Now let $\mathrm{Deg}(C) = d$ and suppose the lemma holds for elements of the form of (3.7) with Deg-value less than d. First, suppose $U_{\sigma'(j)} < U_{\sigma'(j+1)}$. We have

$$\begin{aligned} C = U_{\sigma'(1)}{}^{l_{\sigma'(1)}} \cdots U_{\sigma'(j-1)}{}^{l_{\sigma'(j-1)}} [U_{\sigma'(j)}{}^{l_{\sigma'(j)}}, U_{\sigma'(j+1)}{}^{l_{\sigma'(j+1)}}] \\ \cdot U_{\sigma'(j+2)}{}^{l_{\sigma'(j+2)}} \cdots U_{\sigma'(m)}{}^{l_{\sigma'(m)}} \\ + p\, U_{\sigma'(1)}{}^{l_{\sigma'(1)}} \cdots U_{\sigma'(j-1)}{}^{l_{\sigma'(j-1)}} U_{\sigma'(j+1)}{}^{l_{\sigma'(j+1)}} U_{\sigma'(j)}{}^{l_{\sigma'(j)}} \\ \cdot U_{\sigma'(j+2)}{}^{l_{\sigma'(j+2)}} \cdots U_{\sigma'(m)}{}^{l_{\sigma'(m)}}, \end{aligned} \tag{3.9}$$

where

$$p = p_{u_{\sigma'(j)}{}^{l_{\sigma'(j)}}, u_{\sigma'(j+1)}{}^{l_{\sigma'(j+1)}}}.$$

The second summand of (3.9) is of the form of (3.8). Consider the first summand. By Lemma 3.1.3,

$$\mathrm{Deg}([U_{\sigma'(j)}{}^{l_{\sigma'(j)}}, U_{\sigma'(j+1)}{}^{l_{\sigma'(j+1)}}]) < l_{\sigma'(j)} \,\mathrm{Deg}(U_{\sigma'(j)}) + l_{\sigma'(j+1)} \,\mathrm{Deg}(U_{\sigma'(j+1)}).$$

Hence,

$$\begin{aligned}
&\operatorname{Deg}({U_{\sigma'(1)}}^{l_{\sigma'(1)}} \cdots {U_{\sigma'(j-1)}}^{l_{\sigma'(j-1)}}[{U_{\sigma'(j)}}^{l_{\sigma'(j)}}, {U_{\sigma'(j+1)}}^{l_{\sigma'(j+1)}}]{U_{\sigma'(j+2)}}^{l_{\sigma'(j+2)}} \cdots {U_{\sigma'(m)}}^{l_{\sigma'(m)}}) \\
&\quad \leq \operatorname{Deg}({U_{\sigma'(1)}}^{l_{\sigma'(1)}} \cdots {U_{\sigma'(j-1)}}^{l_{\sigma'(j-1)}}) + \operatorname{Deg}([{U_{\sigma'(j)}}^{l_{\sigma'(j)}}, {U_{\sigma'(j+1)}}^{l_{\sigma'(j+1)}}]) \\
&\qquad\qquad + \operatorname{Deg}({U_{\sigma'(j+2)}}^{l_{\sigma'(j+2)}} \cdots {U_{\sigma'(m)}}^{l_{\sigma'(m)}}) \text{ by (2.16)} \\
&\quad < \operatorname{Deg}({U_{\sigma'(1)}}^{l_{\sigma'(1)}} \cdots {U_{\sigma'(j-1)}}^{l_{\sigma'(j-1)}}) + l_{\sigma'(j)} \operatorname{Deg}(U_{\sigma'(j)}) + l_{\sigma'(j+1)} \operatorname{Deg}(U_{\sigma'(j+1)}) \\
&\qquad\qquad + \operatorname{Deg}({U_{\sigma'(j+2)}}^{l_{\sigma'(j+2)}} \cdots {U_{\sigma'(m)}}^{l_{\sigma'(m)}}) \text{ by Lemma 3.1.3} \\
&\quad = \operatorname{Deg}(C) = d \text{ by Lemma 3.1.4.}
\end{aligned}$$

So, by induction, the first summand of (3.9) is a linear combination of elements of the form of (3.8), and hence so is C.

Now suppose $U_{\sigma'(j+1)} < U_{\sigma'(j)}$. Then

$$\begin{aligned}
C = p^{-1} &{U_{\sigma'(1)}}^{l_{\sigma'(1)}} {U_{\sigma'(2)}}^{l_{\sigma'(2)}} \cdots [{U_{\sigma'(j+1)}}^{l_{\sigma'(j+1)}}, {U_{\sigma'(j)}}^{l_{\sigma'(j)}}] \\
&+ p^{-1} {U_{\sigma'(1)}}^{l_{\sigma'(1)}} {U_{\sigma'(2)}}^{l_{\sigma'(2)}} \cdots {U_{\sigma'(j+1)}}^{l_{\sigma'(j+1)}} {U_{\sigma'(j)}}^{l_{\sigma'(j)}},
\end{aligned}$$

where

$$p = p_{{u_{\sigma'(j+1)}}^{l_{\sigma'(j+1)}}, {u_{\sigma'(j)}}^{l_{\sigma'(j)}}}.$$

The second summand is of the form of (3.8). The calculation to show that the first summand has Deg-value less than $\operatorname{Deg}(C)$ is almost identical to that of the previous case. Thus, the lemma is proved. □

We are now in a position to prove Theorem 3.1.1.

Proof. Lemma 3.1.6 proves that S spans H, and so it only remains to prove that S is linearly independent over k. It can be seen in the proof of Lemma 3.1.6 that

$$S_q := \{s \in S\colon \operatorname{Deg}(s) \leq q\}$$

spans

$$H_q := \{h \in H\colon \operatorname{Deg}(h) \leq q\}.$$

By Lemma 3.1.4, H_q is also spanned by the usual PBW-basis elements with Deg-value less than or equal to m, which are obviously linearly independent. Since $|S_q| = \dim_k H_q$, S_q is linearly independent for all q, and hence so is S. □

3.2 Homological and other properties

We continue to assume that H is a Hopf algebra as in §2.3; that is, H is generated by an abelian group $G = G(H)$ of group-like elements and by skew-primitive semi-invariant elements $a_1, \ldots a_n$, such that (2.11) holds, and that H has a finite number of hard super-letters, denoted

$$U_1 < U_2 < \ldots < U_m.$$

By Theorem 2.4.5,

$$\operatorname{gr} H \cong (H^* * G)/J,$$

where

$$H^* = k[x_1;\sigma_1]\ldots[x_m;\sigma_m], \qquad J := \langle {x_i}^{h_i} : U_i \text{ of finite height } h_i \rangle,$$

where σ_i is the automorphism of $k[x_1;\sigma_1]\cdots[x_{i-1};\sigma_{i-1}]$ defined by $\sigma_i(x_j) := p_{u_i,u_j}x_j$ for all $1 \leq j < i$. This enables us to determine certain properties of $\operatorname{gr} H$, a more straightforward ring than H, and then lift these properties back to H.

It is sometimes helpful to work with different formulations of $\operatorname{gr} H$. Using [45, Lemma 1.4], we also have

$$\operatorname{gr} H \cong (H^*/I) * G, \tag{3.10}$$

where $I := J \cap H^* \lhd H^*$.

In addition, by the fundamental theorem of finitely generated abelian groups, we can write $G := \mathbb{Z}^t \oplus F$, where F is a finite group and $t \geq 0$. By [40, Lemma 1.5.9],

$$\operatorname{gr} H \cong (H^*/I) * G \cong (\cdots((H^*/I * F) * \mathbb{Z}) * \cdots) * \mathbb{Z}, \tag{3.11}$$

where t copies of $\mathbb{Z}$ appear. Therefore, we can apply [40, Proposition 1.5.11], which shows that

$$\operatorname{gr} H \cong (H^*/I) * G \cong ((H^*/I) * F)[y_1, y_1^{-1};\tau_1]\cdots[y_t, {y_t}^{-1};\tau_t]. \tag{3.12}$$

For all $1 \leq i \leq t$, the automorphism sends a generator of the ith copy of $\mathbb{Z}$ in (3.11) to y_i, and τ_i is the automorphism of $((H^*/I) * F)[y_1, y_1^{-1};\tau_1]\cdots[y_{i-1}, {y_{i-1}}^{-1};\tau_{i-1}]$ which conjugates by y_i.

Alternatively, we can replace the skew-Laurent polynomial rings above with localisations of skew-polynomial rings:

$$\operatorname{gr} H \cong (H^*/I) * G \cong ((H^*/I) * F)[y_1;\tau_1][y_1]^{-1}\cdots[y_t;\tau_t][y_t]^{-1}. \tag{3.13}$$

3.2.1 Global dimension

Definition 3.2.1. Let R be a ring. The *right global dimension* of R, $\mathrm{r\,gld}\,R$, is defined by

$$\begin{aligned}\mathrm{r\,gld}\,R &= \sup\{\mathrm{pd}\,M\colon M \text{ a right } R\text{-module}\}\\ &= \sup\{\mathrm{id}\,M\colon M \text{ a right } R\text{-module}\},\end{aligned}$$

where pd and id denote, respectively, projective dimension and injective dimension. The second equality follows from [47, Theorem 9.10]. The *left global dimension* of R, $\mathrm{l\,gld}\,R$, is defined in the obvious way. By [47, Corollary 9.23], $\mathrm{l\,gld}\,R = \mathrm{r\,gld}\,R$ when R is noetherian, and we denote the common value by $\mathrm{gld}\,R$.

We will prove the following proposition:

Proposition 3.2.2. *H has finite global dimension if and only if both of the following conditions hold:*

(i) no hard super-letter has finite height

(ii) either $\mathrm{char}\,k = 0$ or $\mathrm{char}\,k = p > 0$ and G has no elements of order p.

Backwards direction

Global dimension behaves nicely over certain types of ring extensions. Let R be a ring with finite global dimension d. The global dimension of a skew-polynomial ring $R[x;\sigma]$ is $d+1$ [40, Theorem 7.5.3] and the global dimension of $R * F$ is d, where F is a finite group acting on R via automorphisms and $|F|^{-1} \in R$ [40, Theorem 7.5.6]. In addition, global dimension does not increase when passing from an associated graded ring back to the original filtered ring [40, Corollary 7.6.18(i)].

The following lemma is a slight generalisation of [40, Corollary 7.5.6(ii)]:

Lemma 3.2.3. *Let R be a noetherian k-algebra with $\mathrm{gld}\,R < \infty$ and G a finitely generated abelian group with torsion-free rank t, which acts on R via automorphisms. Then if $\mathrm{char}\,k = 0$ or if G contains no elements of order p when $\mathrm{char}\,k = p > 0$, then*

$$\mathrm{r\,gld}(R * G) \leq \mathrm{r\,gld}\,R + t.$$

Proof. Let $G = F \oplus N$, where $N \cong \mathbb{Z}^t$ and $F = \oplus_{i=1}^{q} \mathbb{Z}/{p_i}^{t_i}\mathbb{Z}$, for non-negative integers t and q, distinct primes p_i and positive integers t_i, $1 \leq i \leq q$. By [40, Lemma 1.5.9],

$$R * G \cong (R * N) * F.$$

[40, Corollary 7.5.6(i)] shows that $\operatorname{r\,gld} R * N \leq \operatorname{r\,gld} R + h$. When $\operatorname{char} k = 0$, $|F|$ is obviously a unit in $R * N$. Now suppose $\operatorname{char} k = p > 0$. Then G contains no elements of order p, so $p_i \neq p$, $1 \leq i \leq q$. Hence, $|F| = \prod_{i=1}^{q} {p_i}^{t_i}$ is a unit in $R * N$. This means we can apply [40, Theorem 7.5.6], so

$$\operatorname{r\,gld}(R * G) = \operatorname{r\,gld}((R * N) * F) = \operatorname{r\,gld}(R * N) \leq \operatorname{r\,gld} R + t. \qquad \square$$

So we can now prove the backwards direction of Proposition 3.2.2.

Proposition 3.2.4. *Suppose no hard super-letter of H has finite height, and either $\operatorname{char} k = 0$ or G contains no elements of order p when $\operatorname{char} k = p > 0$. Then H has finite global dimension.*

Proof. Since no hard super-letter has finite height, $\operatorname{gr} H = H^* * G$, where H^* is an iterated skew polynomial ring in m indeterminates over k. By [40, Theorem 7.5.3], $\operatorname{gld} H^* = m$ and then by Lemma 3.2.3,

$$\operatorname{gld}(\operatorname{gr} H) \leq \operatorname{gld} H^* + t = m + t,$$

where t is the torsion-free rank of G. Then, by [40, Corollary 7.6.18],

$$\operatorname{gld} H \leq \operatorname{gld}(\operatorname{gr} H) \leq m + t. \qquad \square$$

Forwards direction

First, we prove a couple of lemmas concerning modules with infinite global dimension.

Lemma 3.2.5. *Let $S \subset R$ be rings such that R is a projective left S-module and, for some left R-module M, $\operatorname{pd}_S(M) = \infty$. Then $\operatorname{l\,gld}(R) = \infty$.*

Proof. We will show that $\operatorname{pd}_R(M) = \infty$; the lemma follows.

Suppose there is a finite projective resolution

$$0 \to P_n \to \cdots \to P_0 \to M \to 0$$

of M as a left R-module. Then for $0 \leq i \leq n$, P_i is a direct summand of a free left R-module. Since R is a projective left S-module, we have R is a direct summand of a free left S-module, and this implies that P_i is a direct summand of a free left S-module. Hence, P_i is a projective left S-module. Thus, we have constructed a finite projective resolution of M as a left S-module, contradicting our hypothesis. Therefore, $\operatorname{pd}_R(M) = \infty$. $\square$

Lemma 3.2.6. *Let k be a field and let $h > 1$. Then $k[x]/\langle x^h \rangle$ has infinite global dimension.*

Proof. Write R for $k[x]/\langle x^h \rangle$. The trivial R-module k has an infinite projective resolution:

$$\begin{tikzcd}
 & & 0 \arrow[dr] & & 0 & & & & \\
 & & & x^{h-1}R \arrow[ur] \arrow[dr] & & & & & \\
\cdots \arrow[rr] \arrow[dr] & & R \arrow[ur, "\psi"] \arrow[rr] & & R \arrow[rr] \arrow[dr, "\phi"] & & R \arrow[r, "\theta"] & k \arrow[r] & 0 \\
 & xR \arrow[ur] \arrow[dr] & & & & xR \arrow[ur] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

which repeats itself. The maps labelled above are defined by $\theta\colon 1+\langle x^h \rangle \mapsto 1$, $\phi\colon 1+\langle x^h \rangle \mapsto x + \langle x^h \rangle$ and $\psi\colon 1 + \langle x^h \rangle \mapsto x^{h-1} + \langle x^h \rangle$. Furthermore, the resolution cannot terminate. For, suppose first that xR is projective. Then the short exact sequence

$$0 \longrightarrow x^{h-1}R \longrightarrow R \xrightarrow{\phi} xR \longrightarrow 0$$

splits, so

$$R = x^{h-1}R \oplus A,$$

for some ideal A of R isomorphic to xR. But then $x^{h-1}R$ is both idempotently generated and nilpotent, which is impossible. If $x^{h-1}R$ is projective, the proof is similar. This proves that there is no finite length projective resolution of k by the generalised version of Schanuel's lemma [47, Exercise 3.37]. □

We can now prove the forwards direction of Proposition 3.2.2.

Proposition 3.2.7. *H has infinite global dimension if either of the following hold:*

(i) H has a hard super-letter with finite height;

(ii) $\operatorname{char} k = p > 0$ *and G has an element of order p.*

Proof. (i) Suppose H has a hard super-letter U_i of finite height h. Then by Theorem 3.1.1, H is a free left and right $k[U_i]$ module that is annihilated by ${U_i}^h$, so H is a free left and right $k[U_i]/{U_i}^h$-module. However, by Lemma 3.2.6, the trivial $k[U_i]/{U_i}^h$-module k has infinite projective dimension. Since H is free over $k[U_i]/{U_i}^h$, and k is also an H-module, Lemma 3.2.5 tells us that $\operatorname{gld}(H) = \infty$.

(ii) H is free over kC_p, where C_p is the cyclic group of order p. We have

$$kC_p \cong k[x]/\langle x^p \rangle,$$

where the isomorphism is defined by sending a generator of C_p to $x+1$. By Lemma 3.2.6, the trivial $k[x]/\langle x^p\rangle$-module k has infinite global dimension. Therefore, so does the kC_p-module k. Since k is also an H-module, it follows from Lemma 3.2.5 that $\mathrm{gld}(H) = \infty$. □

3.2.2 GK dimension

Gelfand-Kirillov dimension, or GK dimension for short, is a measure of the rate of growth of an affine algebra with respect to a generating subspace.

Definition 3.2.8. (i) Let $f\colon \mathbb{N} \to \mathbb{R}_{\geq 1}$. Then f has *polynomially bounded growth* if, for some $t \in \mathbb{R}$, $f(a) \leq a^t$ for $a \gg 0$, and then we define

$$\gamma(f) := \inf\{t\colon f(a) \leq a^t \text{ for } a \gg 0\}.$$

Otherwise, $\gamma(f) = \infty$.

(ii) Let R be an affine k-algebra with finite-dimensional generating subspace V and suppose that $1 \in V$. Then R has filtration $\{R_n\colon n \geq 0\}$ with $R_0 = k$ and $R_n = V^n$. The *GK dimension* of R, denoted by $\mathrm{GKdim}(R)$, is $\gamma(a \mapsto \dim_k R_a)$.

(iii) If S is a (not necessarily affine) k-algebra, then

$$\mathrm{GKdim}(S) := \sup\{\mathrm{GKdim}(R)\colon R \text{ an affine subalgebra of } S\}.$$

(iv) Let M be a finitely generated R-module and let M_0 be a finite-dimensional subspace of M such that $RM_0 = M$. For $n \geq 0$, define $M_n := R_n M_0$. The *GK dimension* of ${}_RM$ is $\gamma(a \mapsto \dim_k M_a)$.

For further details, see for example [40, Chapter 8]. Note that $\mathrm{GKdim}(R)$ is independent of the choice of generating subspace V by [40, Lemma 8.1.10]. In addition, $\mathrm{GKdim}(R) = \mathrm{GKdim}(R{*}F)$, where F is a finite group acting on R via automorphisms [40, Proposition 8.2.9], and GK dimension remains constant when passing from an associated graded ring to the original filtered ring [40, Lemma 8.6.5].

The following lemma will be needed later.

Lemma 3.2.9. *Let R be a k-algebra and let σ be an automorphism of R. Then, for all $t \geq 1$,*

$$\mathrm{GKdim}(R[x;\sigma]/\langle x^t\rangle) = \mathrm{GKdim}(R).$$

Proof. Let $T := R[x;\sigma]/\langle x^t\rangle$ and let $R' := \{r + \langle x^t\rangle\}$, a subalgebra of T that is isomorphic to R. Then T is a finitely generated left R'-module, generated by

$$1 + \langle x^t\rangle,\ \ x + \langle x^t\rangle,\ \ \ldots,\ \ x^{t-1} + \langle x^t\rangle.$$

Hence, $\mathrm{GKdim}(R) = \mathrm{GKdim}(R') = \mathrm{GKdim}(T)$, where the second equality follows from [40, Proposition 8.2.9(ii)]. □

A key step in determining the GK dimension of H involves locally algebraic maps. An endomorphism σ of an algebra R is *locally algebraic* if, for every finite-dimensional k-subspace $V \subset R$, then $V \subset W$, where W is a σ-stable finite-dimensional k-subspace. Clearly, σ is locally algebraic if R is spanned by elements $\{r \colon r \in \mathcal{R}\}$ such that $\sigma(r) = \alpha_r r$ for all $r \in \mathcal{R}$, where $\alpha_r \in k$.

Proposition 3.2.10. *[34, Proposition 1] Let R be an algebra and let σ be a locally algebraic automorphism of R. Then*

$$\mathrm{GKdim}(R[x,x^{-1};\sigma]) = \mathrm{GKdim}(R[x;\sigma]) = \mathrm{GKdim}(R) + 1.$$

We now calculate the GK dimension of H^*/I, where H^*/I is as in (3.10).

Lemma 3.2.11. *Let the number of hard super-letters of finite height be denoted by f. Then*

$$\mathrm{GKdim}(H^*/I) = m - f.$$

Proof. For $1 \leq t \leq m$, let A_t be the subalgebra of H^* generated by $x_1, \ldots, x_t$ and let I_t be the ideal of A_t generated by ${x_i}^{h_i}$, where $1 \leq i \leq t$ and U_i has finite height h_i. We prove by induction on t that $\mathrm{GKdim}(A_t/I_t) = t - f_t$, where f_t is the number of hard super-letters U_i, $1 \leq i \leq t$, with finite height. Since $A_m = H^*$ and $I_m = I$, the lemma follows.

For $t = 1$, $A_1 = k[x_1]$ and $\mathrm{GKdim}(A_1) = 1$ by [40, Proposition 8.1.15(i)]. If U_1 has infinite height, then $I_1 = \{0\}$ and $\mathrm{GKdim}(A_1/I_1) = \mathrm{GKdim}(A_1) = 1$. If U_1 has finite height h_1, then by Lemma 3.2.9, $\mathrm{GKdim}(A_1/I_1) = \mathrm{GKdim}(k) = 0$. Therefore, the claim holds for $t = 1$.

Now suppose $\mathrm{GKdim}(A_{t-1}/I_{t-1}) = t - 1 - f_{t-1}$. We have $A_t = A_{t-1}[x_t; \sigma_t]$, and so

$$A_t/I_t \cong \frac{(A_{t-1}/I_{t-1})[x_t; \overline{\sigma}_t]}{K},$$

where $\overline{\sigma}_t$ is the automorphism of A_{t-1}/I_{t-1} with $\overline{\sigma}_t(a + I_{t-1}) := \sigma_t(a) + I_{t-1}$, and K is the ideal of $(A_{t-1}/I_{t-1})[x_t; \overline{\sigma}_t]$ defined by

$$K := \begin{cases} \{0\} & \text{if } U_t \text{ has infinite height,} \\ \langle {x_t}^{h_t} \rangle & \text{if } U_t \text{ has finite height } h_t. \end{cases}$$

To see this, note that every element of A_t/I_t is expressible as $\sum_{i=0}^{q} a_i {x_t}^i + I_t$, for some $0 \leq q \leq t-1$ and some $a_i \in A_{t-1}$, $0 \leq a_i \leq m$. Define the isomorphism

$$\theta \colon A_t/I_t \to \frac{A_{t-1}/I_{t-1}[x_t; \sigma_t]}{K}, \qquad \theta(\sum_{i=0}^{q} a_i {x_t}^i + I_t) := \sum_{i=0}^{q} (a_i + I_{t-1}) {X_t}^i + K.$$

Suppose $K = 0$. Then, since σ_t is locally algebraic, we may apply Proposition 3.2.10, which shows that

$$\mathrm{GKdim}(A_t/I_t) = \mathrm{GKdim}(A_{t-1}/I_{t-1}) + 1 = t - 1 - f_{t-1} + 1 = t - f_t.$$

If $K = \langle {x_t}^{h_t} \rangle$, then applying Lemma 3.2.9 gives

$$\mathrm{GKdim}(A_t/I_t) = \mathrm{GKdim}(A_{t-1}/I_{t-1}) = t - 1 - f_{t-1} = t - (f_{t-1} + 1) = t - f_t,$$

as required. □

It is now straightforward to calculate the GK dimension of H.

Proposition 3.2.12. $\mathrm{GKdim}\, H = m - f + t$*, where* f *is the number of hard super-letters of finite height and* t *is the torsion-free rank of* G*.*

Proof. By Lemma 3.2.11, $\mathrm{GKdim}(H^*/I) = m - f$, and by [40, Proposition 8.2.9], $\mathrm{GKdim}((H^*/I) * F) = m - f$. (3.12) shows that $\mathrm{gr}\, H$ is an iterated skew Laurent polynomial ring over $(H^*/I) * F$. Since G is abelian and acts on H^*/I by multiplication by a scalar, all the maps τ_i are locally algebraic. We may therefore apply [34, Proposition 1], which gives $\mathrm{GKdim}(\mathrm{gr}\, H) = m - f + t$. Finally, by [40, Lemma 8.6.5], $\mathrm{GKdim}(H) = m - f + t$. □

3.2.3 The Auslander-Gorenstein property

We now study a class of noetherian rings whose modules satisfy a homological condition introduced by Auslander, involving the vanishing of certain Ext groups.

Definition 3.2.13. Let R be a noetherian ring. A finitely generated left or right R-module M satisfies the *Auslander condition* if, for all $j \geq 0$ and for all submodules N of $\operatorname{Ext}_R^j(M, R)$, we have $\operatorname{Ext}_R^i(N, R) = 0$ for all $i < j$. If $\operatorname{id}(R_R) < \infty$ and every such M satisfies the Auslander condition, we say that R is *Auslander-Gorenstein*. If, in addition, $\operatorname{gld}(R) < \infty$, R is said to be *Auslander-regular*.

Note that [54, Lemma A] shows that $\operatorname{id}(R_R) = \operatorname{id}({}_R R)$ when R is noetherian.

Examples of Auslander-Gorenstein rings include quasi-Frobenius rings [15] and the Weyl algebras over a field of characteristic 0 [9, §2.7]. A commutative noetherian ring is Auslander-Gorenstein if and only if it has finite injective dimension [5]; such rings are called *Gorenstein.* If R is an Auslander-Gorenstein ring, then the Auslander-Gorenstein property is retained by skew-polynomial rings $R[x; \sigma]$ [18, Theorem 4.2], by $R * F$, where F is a finite group acting by automorphisms on R [53, Proposition 3.9], by a localisation of R at a multiplicatively closed set of regular elements [1, Proposition 2.1], and, in the case where $R := \bigoplus_{n \geq 0} R_n$ is a graded ring, by factoring out by a normal regular element in R_n [37, Theorem 3.6].

We now consider a special type of filtration. Extend the notion of filtrations indexed by $\mathbb{N}$ in Definition 1.1.1 (i) to filtrations indexed by $\mathbb{Z}$ in the obvious way. That is, a ring R has a $\mathbb{Z}$-*filtration* if there is a family of additive subgroups $\{R_n : n \in \mathbb{Z}\}$ of R such that, for all $m, n \geq 0$, $R_n \subseteq R_{n+1}$, $R_m R_n \subseteq R_{m+n}$, and $R = \bigcup_{n \in \mathbb{Z}} R_n$.

Let R be a $\mathbb{Z}$-filtered ring with $\bigcap_{n \in \mathbb{Z}} R_n = 0$ and $1 \in R_0$. We take the following definitions from [10, §2]. The *filtered topology* on R is constructed using the distance function, which for $r, s \in R$ is defined by

$$d(r, s) = 2^n, \text{ where } r - s \in R_n \setminus R_{n-1}.$$

The filtration satisfies the *strong closure* condition if, for every $r_1, \ldots, r_t \in R$ and $n_1, \ldots, n_t \in \mathbb{Z}$, it follows that

$$R_{n_1} r_1 + \ldots + R_{n_t} r_t, \;\; r_1 R_{n_1} + \ldots + r_t R_{n_t}$$

are closed subsets of R in the filtered topology. If $\operatorname{gr} R$ is noetherian and the strong closure condition holds, we say that the filtration on R is *Zariskian*.

If A is a filtered algebra in the sense of Definition 1.1.1 (i), then A has a $\mathbb{Z}$-filtration $\{A_n : n \in \mathbb{Z}\}$ by setting $A_n := 0$ for $n < 0$. Suppose $1 \in A_0$. Then the filtered topology on A is discrete and so every subset of A is closed. In particular, the strong closure condition holds. Hence, if $\operatorname{gr} A$ is noetherian, then the filtration is Zariskian.

This type of filtration appears in the following theorem from [10]. Its statement here includes the remark immediately after the theorem.

Theorem 3.2.14. *[10, Theorem 3.9] Let R be a noetherian ring with a Zariskian filtration and suppose* $\operatorname{gr} R$ *is Auslander-Gorenstein (respectively, Auslander-regular). Then R is Auslander-Gorenstein (respectively, Auslander-regular).*

We apply this theorem in the following proposition.

Proposition 3.2.15. *H is Auslander-Gorenstein. Furthermore, H is Auslander-regular if and only if no hard super-letter has finite height and G has no elements of order p if $char k = p > 0$.*

Proof. We have $\operatorname{gr} H \cong (H^*/I) * G$. It is easy to see that k is Auslander-Gorenstein; since H^* is an iterated skew polynomial ring over k, we can apply [18, Theorem 4.2] to show that H^* is Auslander-Gorenstein. For $1 \leq i \leq n$ such that U_i has finite height h_i, ${x_i}^{h_i}$ is a normal regular homogeneous element of the graded ring H^*. Therefore, we can apply [37, Theorem 3.6], which shows that H^*/I is Auslander-Gorenstein.

As previously, let $G = \mathbb{Z}^t \oplus F$, where F is a finite group and $t \geq 1$. Then $(H^*/I) * F$ is Auslander-Gorenstein by [53, Proposition 3.9]. Consider the description of $\operatorname{gr} H$ in (3.13). By [18, Theorem 4.2], $((H^*/I) * F)[y_1; \sigma_1]$ is Auslander-Gorenstein, and by [1, Proposition 2.1] so is $((H^*/I) * F)[y_1, {y_1}^{-1}; \sigma_1] \cong ((H^*/I) * F)[y_1; \sigma_1][y_1]^{-1}$. Iterated application of these theorems shows that $(H^*/I) * G$ is Auslander-Gorenstein.

Clearly, $\operatorname{gr} H$ is a noetherian ring and arises from an $\mathbb{N}$-filtration on H. Therefore, the filtration on H is Zariskian and so H is Auslander-Gorenstein by Theorem 3.2.14.

Finally, H is Auslander-regular if and only if no hard super-letter has finite height and G has no elements of order p when $\operatorname{char} k = p > 0$ by Theorem 3.2.2. □

3.2.4 The Cohen-Macaulay property

The Cohen-Macaulay property comes from algebraic geometry and was originally defined only for commutative rings, where it involves Krull dimension. There have been various attempts to generalise this property to noncommutative rings using other dimension functions; we will use the following definition, which applies to noncommutative noetherian algebras and involves GK dimension:

Definition 3.2.16. Let R be a noetherian ring and M a finitely generated R-module. Then the *grade* of M is defined by

$$j(M) = \inf\{i \geq 0 \colon \operatorname{Ext}^i_R(M, R) \neq 0\},$$

or $j(M) = \infty$ if no i exists with $\operatorname{Ext}^i_R(M, R) \neq 0$. A noetherian algebra R is *Cohen-Macaulay* if

$$j(M) + \operatorname{GKdim}(M) = \operatorname{GKdim}(R) < \infty$$

for every nonzero finitely generated left or right R-module M.

Every commutative affine algebra of finite injective dimension is Auslander-Gorenstein and Cohen-Macaulay. This is also true of connected graded noetherian polynomial identity algebras of finite injective dimension [48, Theorem 1.1]. However, in general the Cohen-Macaulay condition is stricter for noncommutative rings: there are noncommutative Auslander-regular rings that are not Cohen-Macaulay, an example being the ring of 2×2 upper triangular matrices over k [15, §3].

The Cohen-Macaulay property is preserved when passing from an associated graded ring back to the original filtered ring, in the case where the original ring is noetherian [25, Theorem 1.2] (an amalgamation of results from [18] and [37]). In addition, every localisation of an Auslander-Gorenstein, Cohen-Macaulay ring at a multiplicatively closed set of normal elements is Cohen-Macaulay [1, Theorem 2.4]. The following lemmas give conditions under which the Cohen-Macaulay property, together with the Auslander-Gorenstein property, is preserved:

Lemma 3.2.17. *[36, Lemma, p.184] Let $S = R[x; \sigma, \delta]$ be a skew polynomial ring over an Auslander-regular, Cohen-Macaulay noetherian ring R. If R is a connected, graded algebra, and $\sigma(R_i) = R_i$ for all graded components R_i, then S is Cohen-Macaulay.*

Theorem 3.2.18. *[37, Theorem 5.10] Let $R = \oplus_{n \geq 0} R_n$ be a finitely generated graded k-algebra with $\dim_k R_0 < \infty$. Suppose $x \in R_d$ is a normal non-zero-divisor in R. Then $S = R/xR$ is Auslander-Gorenstein, Cohen-Macaulay and every finitely generated graded S-module has finite GK dimension if and only if the same is true for R.*

We need the following lemma, which must be well-known, but for which we could not find a suitable reference.

Lemma 3.2.19. *Let R be a ring, let F be a finite group acting on R by automorphisms and let $T := R * F$. Let M be a finitely generated T-module. Then*

$$\mathrm{GKdim}({}_RM) = \mathrm{GKdim}({}_TM).$$

Proof. Let V be a finite dimensional generating subspace of R. Since F acts on R via finite order automorphisms, without loss of generality we may assume that V is F-invariant, since we can enlarge V if necessary. We may also assume that $1 \in V$, so that setting $R_n := kV^n$ gives a filtration $\{R_n\}$ of R. Let $W = VG$ be the vector subspace of T with basis $\{vf : v \in V, f \in F\}$. Then setting $T_n := kW^n$ gives a filtration $\{T_n\}$ of T and in fact T_n has basis $\{rf : r \in R_n, f \in F\}$.

Let M have finite dimensional generating subspace M_0 as a T-module. Then, again by enlarging M_0 if necessary, we may assume that M_0 is F-invariant. Clearly, M_0 is also a generating space for M as an R-module. Let $M_n := T_nM_0$. Then, since M_0 is F-invariant, we also have $M_n = R_nM_0$. Therefore, $\mathrm{GKdim}({}_RM) = \gamma(a \mapsto \dim_k M_a) = \mathrm{GKdim}({}_TM)$, as required. □

We apply these in proving the following proposition:

Proposition 3.2.20. *H is Cohen-Macaulay.*

Proof. It is easy to see that the field k is Cohen-Macaulay. Furthermore, H^* satisfies the conditions needed for a repeated application of Lemma 3.2.17 and so is Cohen-Macaulay. By Theorem 3.2.18, H^*/I is Cohen-Macaulay, since H^* is Auslander-regular and has finite GK dimension.

We now show that $\mathrm{gr}\, H$ is Cohen-Macaulay. As before, let $G = F \oplus \mathbb{Z}^t$ for a finite group F and some $t \geq 1$. First, we show directly that $R := (H^*/I) * F$ is Cohen-Macaulay. Let M be a finitely generated R-module. Then M is also a finitely generated H^*/I-module, and

$$j({}_{H^*/I}M) + \mathrm{GKdim}({}_{H^*/I}M) = \mathrm{GKdim}(H^*/I),$$

since H^*/I is Cohen-Macaulay. By [4, Lemma 5.4], $j({}_{H^*/I}M) = j({}_RM)$, by [40, Proposition 8.2.9], $\mathrm{GKdim}(R) = \mathrm{GKdim}(H^*/I)$, and by Lemma 3.2.19, $\mathrm{GKdim}({}_RM) = \mathrm{GKdim}({}_{A/I}M)$. Hence, R is Cohen-Macaulay. Consider the formulation of $\mathrm{gr}\, H$ in (3.13) as an iterated series of localisations of skew-polynomial rings over R. Lemma 3.2.17 takes care of the skew-polynomial ring part, while [1, Proposition 2.4] deals with the localisations. Therefore, iterated application of both results shows that $\mathrm{gr}\, H$ is Cohen-Macaulay.

Finally, since $\operatorname{gr} H$ is Cohen-Macaulay, so is H by [25, Theorem 1.2] $\square$

3.2.5 AS-Gorenstein

We take our definition of AS-Gorenstein from [12, Definition 1.2]. Recall that an *augmented algebra* R is an algebra equipped with an algebra map $R \to k$ called an *augmentation.* Since $A/\ker \varepsilon \cong k$, this makes k into a right and left R-module. One obvious example of an augmented algebra is a Hopf algebra with its counit map. Another example is a connected graded algebra $R = \bigoplus_{n \geq 0} \overline{R}_n$; here $\overline{R}_0 = k$ and the augmentation is the canonical surjection $R \to \overline{R}_0$.

Definition 3.2.21. Let R be an augmented algebra with augmentation $\varepsilon \colon R \to k$. Then R is *Artin-Schelter-Gorenstein*, or *AS-Gorenstein* if the following conditions hold:

(i) $\operatorname{id}({}_R R) = d < \infty$,

(ii) $\dim_k \operatorname{Ext}^d_A({}_A k, {}_A A) = 1$ and $\operatorname{Ext}^i_A({}_A k, {}_A A) = 0$ for $i \neq d$,

(iii) The corresponding right module versions of (i) and (ii) also hold.

If, in addition, $\operatorname{gld} A = d$, we say that A is *Artin-Schelter-regular* or *AS-regular*.

Lemma 3.2.22. *[12, Lemma 6.1] Let R be a noetherian Hopf algebra with finite GK-dimension. If R is Auslander-Gorenstein (respectively, Auslander-regular) and Cohen-Macaulay, then R is AS-Gorenstein (respectively, AS-regular).*

The above lemma, together with Propositions 3.2.2, 3.2.15 and 3.2.20, prove:

Proposition 3.2.23. *H is AS-Gorenstein. Furthermore, H is AS-regular if and only if no hard super-letter has finite height and G contains no elements of order p when $\operatorname{char} k = p > 0$.*

3.2.6 Values for global and injective dimensions

We can use the Cohen-Macaulay property together with Proposition 3.2.12 to calculate values for the global and injective dimensions of H. This relies on the fact that if R is a ring and M is a non-zero finitely generated R-module, then $j(M) \leq \operatorname{pd}(M) \leq \operatorname{gld}(R)$ [47, Exercise 9.6] and if R is noetherian then $j(M) \leq \operatorname{id}(R)$ [37, Remark 2.2(1)].

Theorem 3.2.24. *Let f be the number of hard super-letters of finite height and let t be the torsion-free rank of G. Then* *(i) H has finite global dimension equal to $m+t$ if and only if both of the following conditions hold:*

(a) no hard super-letter has finite height

(b) either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and G has no elements of order p.

(ii) H has finite injective dimension equal to $m - f + t$.

Proof. Consider the trivial H-module k. Clearly, $\operatorname{GKdim}({}_Hk) = 0$, so by the Cohen-Macaulay property and Proposition 3.2.12,

$$j({}_Hk) = \operatorname{GKdim}(H) = m - f + t,$$

where f is the number of hard super-letters of finite height and t is the torsion-free rank of G.

(i) By Proposition 3.2.2, H has finite global dimension if and only if the conditions in the statement of this theorem hold, and its proof shows that in this case $\operatorname{gld}(H) \leq m+t$. When H has finite global dimension, $f = 0$ and so $j({}_Hk) = m + t \leq \operatorname{pd}({}_Hk)$. Thus $\operatorname{pd}({}_Hk) = \operatorname{gld}({}_Hk) = m + t$.

(ii) The previous part shows that $\operatorname{id}(H^* * G) \leq m + t$. Since $H^* * G$ is Auslander-Gorenstein, [37, Theorem 3.6] shows that $\operatorname{id}(\operatorname{gr} H) \leq m - f + t$. By [10, Theorem 3.9], $\operatorname{id}(H) \leq m - f + t$. As in the previous part, $j({}_Hk) = m - f + t \leq \operatorname{id}(H)$, and so $\operatorname{id}({}_Hk) = \operatorname{id}(H) = m - f + t$. □

3.2.7 Application to pointed Hopf algebras

Let P be a pointed Hopf algebra and let $\operatorname{gr} P$ be the associated graded Hopf algebra of P with respect to the coradical filtration. As in §1.3.5, we have $\operatorname{gr} P \cong B\#kG$, where $G := G(P)$ is a group and $B \in {}^G_G\mathcal{YD}$ is a braided Hopf algebra. Therefore, when G is finitely generated, abelian and acts diagonalisably on B, $\operatorname{gr} P$ is of the form of the Hopf algebra H, which we studied in Chapter 2. However, our work in Chapter 3 has depended upon H having a finite number of hard super-letters, in order to be able to define the Deg-filtration on H from §2.4. If we knew that $\operatorname{gr} P$ had a finite number of hard super-letters, we would be able to lift back to P the properties we have considered in this chapter. As it stands, we can only be certain that these properties hold for a class $\mathcal{P}$ of Hopf algebras defined by $P \in \mathcal{P}$ if and only if P is a pointed Hopf algebra with $G := G(P)$ finitely generated, abelian and acting diagonalisably on B, and $\operatorname{gr} P$ has a finite number of hard super-letters. This last condition makes it an unwieldy class to work with, but $\mathcal{P}$ does provide further evidence for the conjecture of Brown [14, Question E] that all noetherian Hopf algebras are AS-Gorenstein.

It is not clear if there are conditions on P that would enable us to determine if $\operatorname{gr} P$ has only a finite number of hard super-letters. A first guess would be the following.

Conjecture 3.2.25. *Let P be a pointed Hopf algebra, where $G := G(P)$ is finitely generated, abelian and acts diagonalisably on B, the subalgebra of coinvariants. Then the following conditions are equivalent:*

(i) P has a finite number of hard super-letters,

(ii) P is noetherian,

(iii) P has finite GK-dimension.

Clearly, (i) $\Rightarrow$ (ii) is Theorem 2.4.1, and (i) $\Rightarrow$ (iii) is Proposition 3.2.12. We have been unable to prove the backwards directions of these implications. For example, if we assume that P has an infinite number of hard super-letters and try to construct a strictly ascending infinite chain of right or left ideals, we run into difficulties associated with manipulating an infinite set of hard super-letters. The root of the problem is that any finite subset of the hard super-letters is not necessarily closed under multiplication.

Chapter 4

Diagonal Nichols algebras

A Nichols algebra, denoted $B(V)$, is a certain braided graded Hopf algebra in ${}^H_H\mathcal{YD}$, the category of Yetter-Drinfeld modules over a Hopf algebra H, characterised up to isomorphism by its degree 1 graded component V, which is also the k-vector space spanned by its primitive elements and generates $B(V)$ as a k-algebra. For any braided vector space V, $B(V)$ is the quotient of the tensor algebra $T(V)$ by its largest biideal generated by homogeneous primitive elements of degree 2 or more. As we saw in §1.3.4, the bosonisation $B(V)\#H$ is a (non-braided) Hopf algebra, and it was in this context that Nichols algebras first arose under the name "bialgebras of type 1", in the thesis [44] of Nichols, who considered the case where $H = k\Gamma$ for a group Γ.

The vector space V is a Yetter-Drinfeld submodule of $B(V)$ endowed with a braiding $c\colon V \otimes V \to V \otimes V$. This braiding is the key to determining the structure of $B(V)$. For a given pair (V, c), it can be complicated to calculate the homogeneous primitives of degree 2 or more in order to write down $B(V)$ explicitly as a quotient of $T(V)$. Furthermore, it is usually difficult to verify whether such primitive elements actually exist; if there are none, then clearly $B(V) \cong T(V)$.

In this chapter, we consider the case where $H = k\Gamma$, for an abelian group Γ acting diagonalisably on V. That is, there exists a basis of V such that, for all x_i and x_j in the basis, we have

$$c(x_i \otimes x_j) = r_{ij} x_j \otimes x_i,$$

for some $r_{ij} \in k^*$. The main theorem establishes conditions on the scalars r_{ij} that are sufficient to give $B(V) \cong T(V)$.

4.1 Nichols algebras

Definition 4.1.1. Let $V \in {}^H_H\mathcal{YD}$, with associated braiding c. The *Nichols algebra* of (V, c) is a braided graded Hopf algebra $B(V) = \bigoplus_{n\geq 0} B_n \in {}^H_H\mathcal{YD}$ with

(i) $B_0 \cong k$ and $B_1 \cong V$ in ${}^H_H\mathcal{YD}$,

(ii) $B_1 = P(B(V))$, the primitive elements of $B(V)$,

(iii) $B(V) = k\langle B_1\rangle$, i.e. $B(V)$ is generated as an algebra by the elements of B_1.

We can show the existence of $B(V)$ and obtain a more concrete description of it, as follows. The tensor algebra $T(V) = \bigoplus_{n\geq 0} T^n(V)$ is a graded Hopf algebra in ${}^H_H\mathcal{YD}$, where $\Delta\colon T(V) \to T(V)\underline{\otimes}T(V)$ is defined by

$$\Delta(v) = v \otimes 1 + 1 \otimes v$$

for all $v \in V$; see [3, §2.1]. The existence of an antipode follows from [42, Lemma 5.2.10], which also shows that all braided bialgebra quotients of $T(V)$ are braided Hopf algebras in ${}^H_H\mathcal{YD}$.

Recall that a biideal of a bialgebra is a subset that is both an ideal and a coideal. Let $\mathcal{S}$ be the set of all biideals of $T(V)$ that are generated by homogeneous elements of degree greater than or equal to 2. Let

$$I(V) = \sum_{I\in\mathcal{S}} I,$$

so $I(V)$ is the largest element of $\mathcal{S}$. Then we have the following proposition proving the existence and uniqueness of $B(V)$, up to isomorphism:

Proposition 4.1.2. *[2, Proposition 2.2], [41, Lemma 2.1] Let V be a braided vector space, let $\mathcal{S}$ be as above and let $I \in \mathcal{S}$. Then the following are equivalent:*

(i) $I = I(V)$,

(ii) $V = P(T(V)/I)$,

(iii) $B(V) = T(V)/I(V)$.

Proof. (i) $\Rightarrow$ (ii): Let $n \geq 2$ and consider the inverse image $X \subseteq T^n(V)$ of the primitive elements of degree n in $T(V)/I(V)$. Then X is a coideal of $T(V)$ and $\langle X, I(V)\rangle \in \mathcal{S}$, so $\langle X, I(V)\rangle \subseteq I(V)$ since $I(V)$ is maximal in $\mathcal{S}$. Hence $X \mapsto 0$ and the claim is proven since the primitive elements of $T(V)/I(V)$ form a graded submodule.

(ii) $\Rightarrow$ (i): We can apply [42, Lemma 5.3.3] to the surjective map $f\colon T(V)/I \to T(V)/I(V)$, since the coradical of $T(V)/I$ is k and f is injective on $P(T(V)/I)$. Hence, f is injective and so $I = I(V)$.

(ii) $\Rightarrow$ (iii): Follows by definition of $B(V)$. □

Define $I^n(V) := I(V) \cap T^n(V)$. Then, it is clear that

$$B(V) = \bigoplus_{n\geq 0} T^n(V)/I^n(V). \tag{4.1}$$

4.2 Skew-derivations of graded coalgebras

Let $R = \bigoplus_{n\geq 0} R_n$ be a connected, graded coalgebra and let $\pi_n\colon R \to R_n$ be the canonical projection map, for all $n \geq 0$. Define, for all $i, j \geq 0$,

$$\Delta_{i,j}\colon R_{i+j} \xrightarrow{\Delta} R \otimes R \xrightarrow{\pi_i\otimes\pi_j} R_i \otimes R_j.$$

By Definition 1.1.3 (ii)(a),

$$\Delta|_{R_n} = \sum_{i=0}^{n} \Delta_{i,n-i}.$$

Since R is connected, if $n \geq 0$ and $x \in R_n$, then it is easy to see that

$$\Delta_{0,n}(x) = 1 \otimes x, \qquad \Delta_{n,0}(x) = x \otimes 1. \tag{4.2}$$

More generally, we can define a map $\Delta^k\colon R \to R^{\otimes k+1}$, where $k \geq 1$, by $\Delta^0 = \mathrm{id}_R$, $\Delta^1 = \Delta$ and

$$\Delta^k = (\mathrm{id}_{R^{\otimes k-1}} \otimes \Delta)\Delta^{k-1}. \tag{4.3}$$

Now, for all $k \geq 1$ and for all non-negative integers $i_1, \ldots, i_k$, let

$$\Delta_{i_1,\ldots,i_k}\colon R_{i_1+\cdots i_k} \to R_{i_1} \otimes \cdots \otimes R_{i_k},$$

be the composition

$$(\pi_{i_1} \otimes \cdots \otimes \pi_{i_k}) \circ \Delta^{k-1}.$$

Using (4.3) and the definition of a graded coalgebra, it's easy to see by induction on k that

$$\Delta^{k-1}(R_n) \subseteq \sum_{i_1=0}^{n} \sum_{i_2=0}^{n-i_1} \cdots \sum_{i_{k-1}=0}^{n-(i_1+\cdots+i_{k-2})} R_{i_1} \otimes R_{i_2} \cdots \otimes R_{i_{k-1}} \otimes R_{n-(i_1+\cdots+i_{k-1})}. \tag{4.4}$$

By (4.4), if $x \in R_n$, then $\Delta^{k-1}(x)$ can have a nonzero summand in $R_1{}^{\otimes k}$ only when

$$i_1 = i_2 = \cdots = i_{k-1} = 1, \;\; n = i_1 + \cdots i_{k-1} + 1 = k.$$

Therefore,

$$\Delta^{k-1}(x) \text{ has no nonzero summand in } {R_1}^{\otimes k} \text{ when } n \neq k. \tag{4.5}$$

Lemma 4.2.1. *[41, Lemma 2.3] The following are equivalent:*

(i) $P(R) = R_1$.

(ii) For all $n \geq 2$, $\Delta_{1,\ldots,1} \colon R_n \to {R_1}^{\otimes n}$ *is injective.*

(iii) For all $n \geq 2$ *and for all* $1 \leq i \leq n-1$, $\Delta_{i,n-i} \colon R_n \to R_i \otimes R_{n-i}$ *is injective.*

(iv) For all $n \geq 2$, $\Delta_{n-1,1}$ *is injective.*

Proof. For all $n \geq 1$, define $\Phi_n \colon R \to {R_1}^{\otimes n}$ to be the composition

$$\Phi_n \colon R \xrightarrow{\Delta^{n-1}} R^{\otimes n} \xrightarrow{{\pi_1}^{\otimes n}} {R_1}^{\otimes n}.$$

Clearly, $\Delta_{1,\ldots 1} \colon R_n \to {R_1}^{\otimes n}$ is the restriction of Φ_n to R_n. Note that for all $i \geq 0$, $j \geq 0$,

$$(\Delta^i \otimes \Delta^j)\Delta = \Delta^{i+j+1}, \tag{4.6}$$

(this is just an easy double induction on i and j using the coassociativity property). Therefore, we see that, for $1 \leq i \leq n-1$,

$$\begin{aligned}(\Phi_i \otimes \Phi_{n-i})\Delta &= (({\pi_1}^{\otimes i} \circ \Delta^{i-1}) \otimes ({\pi_1}^{\otimes n-i} \circ \Delta^{n-i-1}))\Delta \\ &= {\pi_1}^{\otimes n}(\Delta^{i-1} \otimes \Delta^{n-i-1})\Delta \\ &= {\pi_1}^{\otimes n} \circ \Delta^{n-1} \text{ by (4.6)} \\ &= \Phi_n. \end{aligned} \tag{4.7}$$

Now, let $x \in R_n$ and write $\Delta(x) = \sum_{j=0}^{n} y_j$, where

$$y_j = \Delta_{j,n-j}(x) = z_j \otimes {z_j}' \in R_j \otimes R_{n-j} \tag{4.8}$$

for all $0 \leq j \leq n$. Strictly speaking, we should write $y_j = \sum z_j \otimes {z_j}'$, but we suppress the summation sign, as in some variants of Sweedler notation.

Therefore, for all $1 \leq i \leq n-1$,

$$\begin{aligned}\Phi_n(x) &= (\Phi_i \otimes \Phi_{n-i})\Delta(x) \text{ by (4.7)} \\ &= \sum_{j=0}^{n} {\pi_1}^{\otimes i}\Delta^{i-1}(z_j) \otimes {\pi_1}^{\otimes n-i}\Delta^{n-i-1}({z_j}') \text{ using (4.8)} \\ &= {\pi_1}^{\otimes i}\Delta^{i-1}(z_i) \otimes {\pi_1}^{\otimes n-i}\Delta^{n-i-1}({z_i}') \text{ by applying (4.5) to } z_j, z_j' \\ &= \Phi_i(z_i) \otimes \Phi_{n-i}({z_i}') \qquad (4.9) \\ &= (\Phi_i \otimes \Phi_{n-i})(y_i). \qquad (4.10)\end{aligned}$$

To prove (i) $\Rightarrow$ (ii), we induct on $n \geq 2$. Suppose (i), and let $x \in R_n$ as above. For $n = 2$, by (4.2),

$$\begin{aligned}\Delta(x) &= \Delta_{0,2}(x) + \Delta_{1,1}(x) + \Delta_{2,0}(x)\\ &= 1 \otimes x + \Delta_{1,1}(x) + x \otimes 1,\end{aligned}$$

and since $x \notin P(R)$, $\Delta_{1,1}(x) \neq 0$. Now, let $n > 2$ and suppose that (ii) has been proved for the domain R_i, for $2 \leq i < n$. (4.10) shows that

$$\Delta_{\underbrace{1,\ldots,1}_{n}}(x) = (\Delta_{\underbrace{1,\ldots,1}_{i}} \otimes \Delta_{\underbrace{1,\ldots,1}_{n-i}})(y_i).$$

By induction, both the maps $\Delta_{\underbrace{1,\ldots,1}_{i}}$ and $\Delta_{\underbrace{1,\ldots,1}_{n-i}}$ are injective and so it is easy to see that $\Delta_{\underbrace{1,\ldots,1}_{i}} \otimes \Delta_{\underbrace{1,\ldots,1}_{n-i}}$ is injective. Thus, if $\Delta_{\underbrace{1,\ldots,1}_{n}}(x) = 0$, then $y_i = 0$ for all $1 \leq i \leq n-1$, so that $x \in P(R)$ by (4.2). By (i), we must have $x = 0$.

(ii) $\Rightarrow$ (iii): Assume (ii), fix $n \geq 2$ and i, where $1 \leq i \leq n-1$. Let $x \in R_n$. Then by (4.10),

$$\Delta_{1,\ldots,1}(x) = \Phi_n(x) = (\Phi_i \otimes \Phi_{n-i})\Delta_{i,n-i}(x).$$

Since $\Delta_{1,\ldots,1}$ is injective, so is $\Delta_{i,n-i}$.

(iii) $\Rightarrow$ (iv) is trivial. For (iv) $\Rightarrow$ (i), note that (iv) implies $P(R) \cap R_n = 0$. Since every primitive element of a graded coalgebra is a sum of homogeneous primitive elements, (i) follows. $\square$

We have the following corollary to Lemma 4.2.1:

Corollary 4.2.2. *Let $n \geq 2$ and suppose that $P(R_m) = 0$ for $1 < m < n$. Then, for all $1 \leq i \leq n-1$,*

$$\ker \Delta_{i,n-i} = \sum_{j=1}^{n-1} \ker \Delta_{j,n-j} = \bigcap_{j=1}^{n-1} \ker \Delta_{j,n-j} = P(R_n).$$

Proof. Fix i, with $1 \leq i \leq n-1$. We prove that $\ker \Delta_{i,n-i}$ is equal to each of the other subspaces above. Let $x \in \ker \Delta_{i,n-i}$ and write $\Delta(x) = \sum_{j=0}^{n} y_j$, where $y_j \in R_j \otimes R_{n-j}$. Clearly, $y_i = 0$. By (4.10),

$$0 = (\Phi_i \otimes \Phi_{n-i})(y_i) = \Phi_n(x) = (\Phi_j \otimes \Phi_{n-j})(y_j),$$

for all $1 \leq j \leq n-1$. The proof of Lemma 4.2.1 shows that for $2 \leq m < n$, the maps Φ_j and Φ_{n-j} are injective, for all $1 \leq j \leq n-1$. Hence, we must have $y_j = 0$ for all $1 \leq i \leq n-1$. The first two equalities follow immediately; the third follows from (4.2). $\square$

Now, let H be a Hopf algebra, let $V \in^H_H \mathcal{YD}$ be finite dimensional as a vector space and let $R = T(V)/I$ for some $I \in \mathcal{S}$. In order to determine whether $R = B(V)$, we must determine whether there are any primitive elements in R_n for $n \geq 2$. If we know that there are no primitives in the graded components of degree less than n, the above corollary reduces the problem to determining $\ker \Delta_{i,n-i}$ for any $1 \leq i \leq n-1$. In the case where $H = k\Gamma$ for a group Γ, there is a convenient tool for calculating primitives in R, which exploits this fact for $i = n-1$. It was originally introduced by Nichols in [44, 3.3]; see also [41].

Since V is a Γ-graded Γ-module by the Yetter-Drinfeld condition, we may pick a basis $x_1, \dots, x_\theta$ of V, where $x_i \in V_{g_i}$ as defined in (1.4), for not necessarily distinct members $g_1, \dots, g_\theta$ of Γ. Define algebra automorphisms $\sigma_i \colon R \to R$ by $x \mapsto g_i \cdot x$ for all $x \in R$. For $1 \leq i \leq \theta$, let $D_i \colon R \to R$ be a k-linear map with $D_i(1) := 0$; for $a \in R_n$, define $D_i(a) \in R_{n-1}$ by

$$\Delta_{n-1,1}(a) := \sum_{i=1}^{\theta} D_i(a) \otimes x_i.$$

We have the following proposition:

Proposition 4.2.3. *Let Γ be a group, let $V \in^\Gamma_\Gamma \mathcal{YD}$ and let $R = T(V)/I$ for some $I \in \mathcal{S}$. Then*

(i) [41, Proposition 2.4(i)] For all $1 \leq i \leq \theta$, $D_i \colon R \to R$ is the unique (id, σ_i)-derivation of R such that $D_i(x_j) = \delta_{i,j}$, where $\delta_{i,j}$ denotes the Kronecker delta.

(ii) [41, Proposition 2.4(ii)] $R = B(V)$ if and only if $K := \bigcap_{i=1}^{\theta} \ker D_i = k$.

(iii) Fix $n \geq 1$, and suppose $B_m = R_m$ for all $0 \leq m < n$. Then, as a vector space,

$$B_n \cong R_n/(K \cap R_n).$$

Proof. (i) Let $a \in R_n$, $b \in R_m$ for some $m, n \geq 1$. Then, for a suitable choice of element

$z \in \sum_{h=0}^{m+n-2} R_h \otimes R_{m+n-h}$,

$$\begin{aligned}\Delta(ab) = \Delta(a)\Delta(b) &= \left(\sum_{j=0}^{n} \Delta_{j,n-j}(a)\right)\left(\sum_{k=0}^{m} \Delta_{k,m-k}(b)\right) \\ &= \left(a \otimes 1 + \sum_{i=1}^{\theta} D_i(a) \otimes x_i + \sum_{j=0}^{n-2} \Delta_{j,n-j}(a)\right) \\ &\qquad \cdot \left(b \otimes 1 + \sum_{l=1}^{\theta} D_l(b) \otimes x_l + \sum_{k=0}^{n-2} \Delta_{k,n-k}(b)\right) \\ &= ab \otimes 1 + \sum_{l=1}^{\theta} aD_l(b) \otimes x_l + \sum_{i=1}^{\theta} D_i(a)(g_i \cdot b) \otimes x_i + z \\ &= ab \otimes 1 + \sum_{i=1}^{\theta} (D_i(a)\sigma_i(b) + aD_i(b)) \otimes x_i + z.\end{aligned}$$

Therefore,

$$D_i(ab) = D_i(a)\sigma_i(b) + aD_i(b),$$

so D_i is an (id, σ_i)-derivation. Furthermore, since x_j is primitive for all $1 \leq j \leq \theta$, we have $D_i(x_j) = \delta_{i,j}$. Since R is generated by $x_1, \ldots, x_\theta$, D_i is uniquely determined.

(ii) By Proposition 4.1.2, $R = B(V)$ if and only if $I = I(V)$ if and only if $P(R) = R_1$. Since $K \cap R_n = \ker \Delta_{n-1,1}$, the claim follows from the equivalence of (i) and (iv) in Lemma 4.2.1.

(iii) By Corollary 4.2.2, $K \cap R_n = I_n(V)$. □

4.3 Skew-derivations in the diagonal braiding case

For the rest of this chapter, let Γ be a group and set $H = k\Gamma$. Let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable. It follows that, when describing the braiding induced by the action of Γ on V as in (1.5), we can, without loss of generality, assume that Γ is finitely generated torsion-free abelian of rank at most θ. As in (1.5), we may choose a basis $x_1, \ldots, x_\theta$ of V with $x_i \in V_{g_i}^{\chi_i}$, so $c\colon V \otimes V \to V \otimes V$ is defined by

$$c(x_i \otimes x_j) = \chi_j(g_i)x_j \otimes x_i := r_{ij}x_j \otimes x_i, \tag{4.11}$$

for $1 \leq i, j \leq \theta$.

Setting $R = T(V)$ in Proposition 4.2.3 gives maps $D_i\colon T(V) \to T(V)$, which restrict to linear maps $D_{i,n}\colon T^n(V) \to T^{n-1}(V)$. This section establishes some lemmas concerning the kernels of these maps. First, we make a definition.

Definition 4.3.1. (i) (a) Let ${\mathbb{Z}_{\geq 0}}^\theta$ denote the θ-fold direct product of the non-negative integers. For any positive integer i, we will define

$$\mathbf{i} := (0, \ldots, 1, \ldots, 0) \in {\mathbb{Z}_{\geq 0}}^\theta,$$

with 1 in the ith component and all other entries 0.

(b) Given $\mathbf{t} = (t_1, \ldots, t_\theta) \in {\mathbb{Z}_{\geq 0}}^\theta$, let $L(\mathbf{t}) := \sum_{j=1}^\theta t_j$.

(c) For any $\mathbf{t} \in {\mathbb{Z}_{\geq 0}}^\theta$ write $n := L(\mathbf{t})$ and let $\omega_{\mathbf{t}}^n(V)$ be the subspace of $T^n(V)$ spanned by all the monomials with exactly t_j x_j's for all j. For convenience, we define ${\omega_{\mathbf{0}}}^0(V) := k$, and we extend the definition to $\mathbf{t} \in \mathbb{Z}^\theta$ as follows: if $\mathbf{t} \in \mathbb{Z}^\theta \setminus {\mathbb{Z}_{\geq 0}}^\theta$, define

$$\omega_{\mathbf{t}}^n(V) := 0.$$

(ii) Let $m \in T^n(V)$ be a monomial. The *left x_j-index* of m is the integer $p \geq 0$, which equals n if $m = {x_j}^n$; otherwise it is defined by

$$m = {x_j}^p x_l m', \tag{4.12}$$

where $p < n$, $l \neq j$, and m' is a monomial in $T^{n-p-1}(V)$. There is the obvious corresponding definition of *right x_j-index.*

(iii) Let $a = \sum_{i=1}^m \lambda_i a_i \in T^n(V)$, where $\lambda_i \in k^*$ and the a_i are distinct monomials. The *left x_j-index* of a is

$$p := \min\{p_i := \text{left}\, x_j\text{-index of } \; a_i \colon 1 \leq i \leq m\}.$$

There is the obvious corresponding definition of *right x_j-index.*

Recall Definition 1.3.8, which gives a map $\mathrm{ad}_c \colon T(V) \to \mathrm{End}(T(V))$.

Lemma 4.3.2. *Let n be a positive integer and let i be an integer, $1 \leq i \leq \theta$. Then*

(i) For all $\mathbf{t}$ with $L(\mathbf{t}) = n$,

$$D_{i,n}(\omega_{\mathbf{t}}^n(V)) \subseteq \omega_{\mathbf{t}-\mathbf{i}}^{n-1}(V).$$

(ii) $\ker D_{i,n}$ is an H-submodule of $T^n(V)$.

(iii) $\mathrm{ad}_c(x_l)(\ker D_{i,n-1}) \subseteq \ker D_{i,n}$, for all l, $1 \leq l \leq \theta$.

(iv) $\mathrm{ad}_c(x_l)(\ker D_{i,n-1})$ is an H-submodule of $T^n(V)$, for all l, $1 \leq l \leq \theta$.

Proof. (i) The proof is by induction on n. When $n = 1$, $t_l = 1$ for some l and $t_i = 0$ for all $i \neq l$, meaning that

$$\omega^1_{\mathbf{t}}(V) = kx_l.$$

Since

$$D_{i,1}(kx_l) = \begin{cases} k = \omega^0_{\mathbf{0}}(V) & i = l, \\ 0 & i \neq l, \end{cases}$$

the claim holds for $n = 1$. Now, consider $n > 1$ and let m be a monomial in $\omega^n_{\mathbf{t}}(V)$. It's enough to prove that

$$D_{i,n}(m) \in \omega^{n-1}_{\mathbf{t}-\mathbf{i}}(V).$$

First, suppose that $m = x_i m'$ for some $m' \in \omega^{n-1}_{\mathbf{t}-\mathbf{i}}(V)$. By induction $D_{i,n-1}(m') \in \omega^{n-2}_{\mathbf{t}-2\mathbf{i}}(V)$. Thus, since Γ acts diagonalisably on V, and therefore m' is an eigenvector for g_i,

$$\begin{aligned} D_{i,n}(m) &= D_{i,1}(x_i)(g_i \cdot m') + x_i D_{i,n-1}(m') \\ &\in \omega^{n-1}_{\mathbf{t}-\mathbf{i}}(V) + x_i \omega^{n-2}_{\mathbf{t}-2\mathbf{i}}(V) \\ &\subseteq \omega^{n-1}_{\mathbf{t}-\mathbf{i}}(V)). \end{aligned}$$

Next, suppose that $m = x_l m''$, for some $m'' \in \omega^{n-1}_{\mathbf{t}-\mathbf{l}}(V))$ with $i \neq l$. Then, by induction $D_{i,n-1}(m'') \in \omega^{n-2}_{\mathbf{t}-\mathbf{l}-\mathbf{i}}(V))$, and so

$$\begin{aligned} D_{i,n}(m) = D_{i,1}(x_l)(g_i \cdot m'') + x_l D_{i,n-1}(m'') &= x_l D_{i,n-1}(m'') \\ \in x_l \omega^{n-2}_{\mathbf{t}-\mathbf{l}-\mathbf{i}}(V)) \subseteq \omega^{n-1}_{\mathbf{t}-\mathbf{i}}(V)). \end{aligned}$$

(ii) It is enough to show that $\ker D_{i,n}$ is g_j-invariant, for all $1 \leq j \leq \theta$. Let $t_n := \{\mathbf{t} \in {\mathbb{Z}_{\geq 0}}^{\theta} \colon L(\mathbf{t}) = n\}$. Note that $T^n(V) = \bigoplus_{\mathbf{t} \in t_n} \omega^n_{\mathbf{t}}(V)$, and $T^{n-1}(V) = \bigoplus_{\mathbf{t} \in t_{n-1}} \omega^{n-1}_{\mathbf{t}}(V)$. Thus, in view of (i),

$$\ker D_{i,n} = \bigoplus_{\mathbf{t} \in t_n} (\omega^n_{\mathbf{t}}(V) \cap \ker D_{i,n}). \tag{4.13}$$

But, for a fixed $\mathbf{t} \in t_n$, $\omega^n_{\mathbf{t}}(V)$ is contained in the g_j-eigenspace of $T^n(V)$ with eigenvalue ${r_{j1}}^{t_1} \cdots {r_{j\theta}}^{t_\theta}$. So, clearly, $\omega^n_{\mathbf{t}}(V) \cap \ker D_{i,n}$ is g_j-invariant, and the result follows from (4.13).

(iii) If $l \neq i$, this is obvious, so suppose $l = i$. By (4.13), and since $\mathrm{ad}_c(x_i)(\omega^{n-1}_{\mathbf{t}}(V)) \subseteq \omega^n_{\mathbf{t}+\mathbf{i}}(V)$, it is enough to prove that, for every $\mathbf{t} \in t_{n-1}$, $\mathrm{ad}_c(x_i)(\beta) \in \ker D_{i,n}$ when $\beta \in \omega^{n-1}_{\mathbf{t}}(V) \cap \ker D_{i,n-1}$. Then, for such a β,

$$g_i \cdot \beta = {r_{i1}}^{t_1} \cdots {r_{i\theta}}^{t_\theta} \beta := \lambda_\beta \beta,$$

for some $\lambda_\beta \in k^*$, and

$$\begin{aligned} D_{i,n}(\mathrm{ad}_c(x_i)(\beta)) &= D_{i,n}(x_i\beta - \lambda_\beta \beta x_i) \\ &= D_{i,1}(x_i)(g_i \cdot \beta) + x_i D_{i,n-1}(\beta) \\ &\qquad - \lambda_\beta D_{i,n-1}(\beta)(g_i \cdot x_i) - \lambda_\beta \beta D_{i,1}(x_i) \\ &= \lambda_\beta \beta + 0 - 0 - \lambda_\beta \beta \\ &= 0, \end{aligned}$$

as required.

(iv) It is enough to show that $\mathrm{ad}_c(x_l)(\ker D_{i,n-1})$ is g_j-invariant for all $1 \le j \le \theta$. By (iii),

$$\mathrm{ad}_c(x_l)(\omega_{\mathbf{t}}^{n-1}(V) \cap \ker D_{i,n-1}) \subseteq \omega_{\mathbf{t+1}}^{n}(V) \cap \ker D_{i,n}.$$

Therefore, as in (ii),

$$\mathrm{ad}_c(x_l)(\ker D_{i,n-1}) = \bigoplus_{\mathbf{t} \in t_n} \omega_{\mathbf{t}}^n(V) \cap (\mathrm{ad}_c(x_l)(\ker D_{i,n-1}), \tag{4.14}$$

and, since $\omega_{\mathbf{t}}^n(V)$ is contained in the g_j-eigenspace of $T^n(V)$ with eigenvalue ${r_{j1}}^{t_1} \cdots {r_{j\theta}}^{t_\theta}$, the summands on the right hand side of (4.14) are g_j-invariant for $1 \le j \le \theta$ and the result follows. □

Lemma 4.3.3. *Let n be a positive integer, let $1 \le i \le \theta$ and suppose that ${r_{ii}}^k \neq 1$ for any k, $1 < k \le n$. Then*

(i) $D_{i,n}$ has image $T^{n-1}(V)$.

(ii) $\dim_k(\ker(D_{i,n})) = \theta^{n-1}(\theta - 1)$.

Proof. (i) It is enough to show that each monomial $m \in T^{n-1}(V)$ is in $\mathrm{im}\, D_{i,n}$, and this follows by induction on n. When $n = 1$, $m \in k$ and so $D_{i,1}(mx_i) = m$. Now, for a given $n > 1$, we argue by a sub-induction on the left x_i-index of m.

Suppose first that the left x_i-index of m is 0, so

$$m = x_l m',$$

where $l \neq i$ and $m' \in T^{n-2}(V)$. Then $m' = D_{i,n-1}(\beta)$ for some $\beta \in T^{n-1}(V)$, by induction on n. Therefore,

$$D_{i,n}(x_l\beta) = D_{i,1}(x_l)(g_i \cdot \beta) + x_l D_{i,n-1}(\beta) = x_l m' = m,$$

and so $m \in \operatorname{im} D_{i,n}$.

Now suppose that the left x_i-index of m is $p > 0$, and that monomials in $T^{n-1}(V)$ with left x_i-index less than p are in $\operatorname{im} D_{i,n}$. If $m = {x_i}^{n-1}$, then

$$\begin{aligned} D_{i,n}({x_i}^n) &= (1 + r_{ii} + \cdots + {r_{ii}}^{n-1}){x_i}^{n-1} \\ &= (1 + r_{ii} + \cdots + {r_{ii}}^{n-1})m, \end{aligned}$$

and we get $m \in \operatorname{im} D_{i,n}$, since r_{ii} is not a non-identity nth root of unity. Otherwise, $m \in \omega^{n-1}_{\mathbf{t}}(V)$ for some $\mathbf{t} \in t_{n-1}$, with $\mathbf{t} \neq (n-1)\mathbf{i}$, and

$$m = {x_i}^p x_l m',$$

for some l with $1 \leq l \leq \theta$, $l \neq i$ and $m' \in T^{n-p-2}(V)$. By our induction on the degree of the graded components of $T(V)$, $m' = D_{i,n-p-1}(\beta)$ for some $\beta \in T^{n-p-1}(V)$. Therefore,

$$x_l m' = x_l D_{i,n-p-1}(\beta) = D_{i,n-p}(x_l\beta).$$

We have $x_l m' \in \omega^{n-p-1}_{\mathbf{t}-p\mathbf{i}}(V)$, and by Lemma 4.3.2 (i), $\beta \in \omega^{n-p-1}_{\mathbf{t}-(p-1)\mathbf{i}-\mathbf{l}}(V)$. Thus $g_i\beta = \lambda_\beta\beta$ for some $\lambda_\beta \in k^*$. Then

$$\begin{aligned} D_{i,n}({x_i}^p x_l\beta) &= (1 + r_{ii} + \cdots + {r_{ii}}^{p-1})r_{il}\lambda_\beta {x_i}^{p-1}x_l\beta + {x_i}^p D_{i,n-p}(x_l\beta) \\ &= (1 + r_{ii} + \cdots + {r_{ii}}^{p-1})r_{il}\lambda_\beta {x_i}^{p-1}x_l\beta + {x_i}^p x_l m'. \end{aligned}$$

Now ${x_i}^{p-1}x_l\beta \in T^{n-1}(V)$, with left x_i-index $p-1$. Hence, by induction on p, there exists $\alpha \in T^n(V)$ with

$$D_n(\alpha) = {x_i}^{p-1}x_l\beta.$$

Thus,

$$D_{i,n}({x_i}^p x_l\beta - (1 + r_{ii} + \cdots + {r_{ii}}^{p-1})r_{il}\lambda_\beta\alpha) = {x_i}^p x_l m' = m,$$

and the induction step is proved.

(ii) This follows from (i), since $\dim_k T^n(V) = \theta^n$ for all n. □

We also need the following lemma.

Lemma 4.3.4. *The linear map* $\operatorname{ad}_c(x_j)\colon T^n(V) \to T^{n+1}(V)$ *has*

- *kernel* 0 *if* ${r_{jj}}^n \neq 1$*;*
- *kernel* $k{x_j}^n$ *if* ${r_{jj}}^n = 1$.

Proof. Since $\mathrm{ad}_c(x_j)(x_j{}^n) = (1 - r_{jj}{}^n)x_j{}^{n+1}$, it is clear that

$$\ker \mathrm{ad}_c(x_j)|_{kx_j{}^n} = \begin{cases} \{0\} & \text{if } r_{jj}{}^n \neq 1 \\ kx_j{}^n & \text{if } r_{jj}{}^n = 1. \end{cases}$$

Observe also that, for all $\mathbf{t} \in t_n$, $\mathrm{ad}_c(x_j)(\omega^n_{\mathbf{t}}(V)) \subseteq \omega^{n+1}_{\mathbf{t}+\mathbf{j}}(V)$. So the lemma follows if we show that, for all $\mathbf{t} \neq n\mathbf{j}$,

$$\mathrm{ad}_c(x_j)|_{\omega^n_{\mathbf{t}}(V)} \text{ is a monomorphism.}$$

So suppose $\mathbf{t} \neq n\mathbf{j}$ and let $0 \neq \beta \in \omega^n_{\mathbf{t}}(V)$, so β is a g_j-eigenvector with eigenvalue $\lambda_\beta \in k^*$. Let p be the left x_j-index of β, and notice that, since $\mathbf{t} \neq n\mathbf{j}$ and $\beta \in \omega^n_{\mathbf{t}}(V)$, $p < n$. Then, suppose

$$0 = \mathrm{ad}_c(x_j)(\beta) = x_j\beta - \lambda_\beta \beta x_j.$$

That is,

$$x_j\beta = \lambda_\beta \beta x_j. \tag{4.15}$$

But the left x_j-index of $x_j\beta$ is $p+1$, whereas the left x_j-index of $\lambda_\beta\beta x_j$ is p. (For the second part of the last sentence, it is crucial that $p < n$, so that some x_l with $l \neq j$ does appear at the left hand end of m in at least one monomial $x_j{}^p m$ in the support of β.) Therefore, (4.15) is impossible, and we have a contradiction. □

4.4 Conditions implying $B(V) \cong T(V)$

4.4.1 Notation

For $n \geq 2$, let $\mathcal{B}_n$ denote the usual monomial basis of $T^n(V)$. For $\mathbf{t} = (t_1, \ldots, t_\theta) \in \mathbb{Z}_{\geq 0}{}^\theta$ with $L(\mathbf{t}) = n$, let $\mathcal{B}_{n,\mathbf{t}} \subseteq \mathcal{B}_n$ denote the monomial basis of $\omega^n_{\mathbf{t}}(V)$ and let $b_{\mathbf{t}} := x_1{}^{t_1} \cdots x_\theta{}^{t_\theta} \in B_{n,\mathbf{t}}$. For all $1 \leq j \leq n$, we define functions $\beta_j, \epsilon_j \colon \mathcal{B}_n \to \mathcal{B}_j$ by

$$\beta_j(m) = m_b, \qquad m = m_b m', \ m_b \in \mathcal{B}_j, \ m' \in \mathcal{B}_{n-j},$$
$$\epsilon_j(m) = m_e, \qquad m = m'' m_e, \ m_e \in \mathcal{B}_j, \ m'' \in \mathcal{B}_{n-j}.$$

That is, β_j returns the j letters at the *beginning*, while ϵ_j returns the j letters at the *end*. Clearly,

$$m = \beta_1(m)\epsilon_{n-1}(m) = \beta_{n-1}(m)\epsilon_1(m). \tag{4.16}$$

Let S_n denote the symmetric group on n letters and let $C_n := \langle \tau \rangle$ be the cyclic subgroup of S_n generated by the permutation

$$\tau := (1 \ 2 \ \cdots \ n).$$

S_n acts on the elements of $\mathcal{B}_{n,\mathbf{t}}$ by permuting indices. That is, if $\sigma \in S_n$ and $b = x_{i_1}x_{i_2}\cdots x_{i_n} \in \mathcal{B}_{n,\mathbf{t}}$, then $\sigma \cdot b$ is the monomial with x_{i_j} in the $\sigma(j)$ position. Clearly, this action is transitive; indeed every member of $\mathcal{B}_{n,\mathbf{t}}$ equals $\sigma \cdot b_{\mathbf{t}}$, for some $\sigma \in S_n$. For example, when $\theta = 2$, $n = 3$ and $\mathbf{t} = (2,1)$, we have $b_{\mathbf{t}} = {x_1}^2 x_2$ and

$$x_1x_2x_1 = (2\ \ 3) \cdot b_{\mathbf{t}}.$$

As a vector space, $\mathcal{B}_{n,\mathbf{t}}$ then splits as a direct sum of orbits under the action of C_n. For example, when $\theta = 2$, $n = 4$ and $\mathbf{t} = (2,2)$, the orbits are

$$\{b_{\mathbf{t}} = {x_1}^2{x_2}^2, \quad \tau \cdot b_{\mathbf{t}} = x_2{x_1}^2x_2, \quad \tau^2 \cdot b_{\mathbf{t}} = {x_2}^2{x_1}^2, \quad \tau^3 \cdot b_{\mathbf{t}} = x_1{x_2}^2x_1\},$$

and

$$\{(2\ \ 3) \cdot b_{\mathbf{t}} = x_1x_2x_1x_2, \quad \tau \cdot (2\ \ 3) \cdot b_{\mathbf{t}} = x_2x_1x_2x_1\},$$

An orbit of size n, like the first orbit above, is said to be a *long* orbit, while an orbit of size less than n, like the second orbit above, is called a *short* orbit.

For all $b \in \mathcal{B}_n$, clearly we have $\beta_{n-1}(b) = \epsilon_{n-1}(\tau \cdot b)$, which gives

$$\beta_{n-1}(\tau^{k-1} \cdot b) = \epsilon_{n-1}(\tau^k \cdot b), \tag{4.17}$$

for all $k \geq 1$.

For $b = x_{i_1}\cdots x_{i_n} \in \mathcal{B}_n$, define $\gamma(b) := \prod_{j=2}^{n} r_{i_1 i_j}$. Let $\mathcal{O}_b$ denote the orbit of C_n applied to b and let

$$\gamma(\mathcal{O}_b) := \prod_{a \in \mathcal{O}_b} \gamma(a).$$

4.4.2 Main theorem

This section is devoted to proving the following theorem:

Theorem 4.4.1. *Let Γ be a group and let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable, with basis $x_1, \ldots, x_\theta$ and braiding map $c\colon V \otimes V \to V \otimes V$ as in (4.11). Suppose that for all $n \geq 2$ and for all $b \in \mathcal{B}_n$, we have $\gamma(\mathcal{O}_b) \neq 1$. Then $B(V) \cong T(V)$.*

In fact, the theorem follows easily from the following proposition, using Proposition 4.2.3 (ii).

Proposition 4.4.2. *Let Γ be a group and let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable, with basis $x_1, \ldots, x_\theta$ and braiding map $c\colon V \otimes V \to V \otimes V$ as in (4.11). Let $m \geq 2$ and suppose that*

$$\gamma(\mathcal{O}_b) \neq 1 \ \textit{ for any } \ b \in \mathcal{B}_i \ \textit{ with } \ 2 \leq i \leq m. \tag{4.18}$$

Then

(i) for $1 \leq j \leq \theta$,

$$\ker D_{j,m} = \sum_{l=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,m-1}). \tag{4.19}$$

(ii)

$$\bigcap_{j=1}^{\theta} \ker D_{j,m} = 0. \tag{4.20}$$

The proof is by induction on $m \geq 2$. We first prove that (4.19) and (4.20) hold for $m = 2$. In this case, (4.18) becomes $r_{ii} \neq 1$ and $r_{ij}r_{ji} \neq 1$ for any $1 \leq i \neq j \leq \theta$. Fix j, $1 \leq j \leq \theta$. In this case, (4.19) becomes

$$\ker D_{j,2} = \sum_{l=1}^{\theta} \mathrm{ad}_c(x_l)(kx_1 \oplus \cdots \oplus kx_{j-1} \oplus kx_{j+1} \oplus \cdots \oplus kx_\theta). \tag{4.21}$$

By Lemma 4.3.2 (iii), the right hand side of (4.21) is contained in the left. For the reverse containment, suppose $\alpha_{ab} \in k$ are such that

$$u = \sum_{a=1}^{\theta} \sum_{b=1}^{\theta} \alpha_{ab} x_a x_b \in \ker D_{j,2},$$

where $\alpha_{ab} \in k$, $1 \leq a, b \leq \theta$. Then

$$\begin{aligned}
D_{j,2}(u) &= \alpha_{jj}(1 - r_{jj})x_j \\
&\qquad + \alpha_{1j}x_1 + \cdots + \alpha_{(j-1)j}x_{j-1} + \alpha_{(j+1)j}x_{j+1} + \cdots + \alpha_{\theta j}x_\theta \\
&\qquad\quad + \alpha_{j1}r_{j1}x_1 + \cdots + \alpha_{j(j-1)}r_{j(j-1)}x_{j-1} \\
&\qquad\qquad + \alpha_{j(j+1)}r_{j(j+1)}x_{j+1} + \cdots + \alpha_{j\theta}r_{j\theta}x_\theta \\
&= (\alpha_{1j} + r_{j1}\alpha_{j1})x_1 + \cdots + \alpha_{jj}(1 - r_{jj})x_{jj} + \cdots + (\alpha_{\theta j} + r_{j\theta}\alpha_{j\theta})x_\theta \\
&= 0.
\end{aligned}$$

Therefore,

$$\alpha_{1j} = -r_{j1}\alpha_{j1}, \ldots, \alpha_{jj} = 0, \ldots, \alpha_{\theta j} = -r_{j\theta}\alpha_{j\theta}.$$

Hence,

$$\begin{aligned}
u = {} & \mathrm{ad}_c(x_j)(\alpha_{j1}x_1) + \cdots + \mathrm{ad}_c(x_j)(0x_j) + \cdots + \mathrm{ad}_c(x_j)(\alpha_{j\theta}x_\theta) \\
& + \sum_{a \neq j} \sum_{b \neq j} \alpha_{ab} x_a x_b.
\end{aligned}$$

Let $1 \leq a, b \leq \theta$ with $a \neq j$, $b \neq j$. Then, since (4.18) holds,

$$x_a x_b = \mathrm{ad}_c(x_a)((1 - r_{ab}r_{ba})^{-1}x_b) + \mathrm{ad}_c(x_b)((1 - r_{ab}r_{ba})^{-1}r_{ab}x_a).$$

This proves that u is a linear combination of the required form, and so (4.19) holds when $m = 2$. By Lemma 4.3.3 (ii), $\dim_k \ker D_{j,2} = \theta(\theta - 1)$, which is therefore equal to the dimension of the space on the right hand side of (4.21). Therefore, the sum on the right hand side of (4.21) is a direct sum. Using the fact that $\mathrm{ad}_c(x_l)$ is a monomorphism,

$$\begin{aligned} \bigcap_{j=1}^{\theta} \ker D_{j,2} &= \bigcap_{j=1}^{\theta} \bigoplus_{l=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,1}) \\ &= \bigoplus_{l=1}^{\theta} \left(\bigcap_{j=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,1}) \right) \\ &= \bigoplus_{l=1}^{\theta} \mathrm{ad}_c(x_l) \left(\bigcap_{j=1}^{\theta} \ker D_{j,1} \right) \\ &= 0, \end{aligned}$$

so (4.20) holds when $m = 2$.

The following lemma is the instrumental step in the proof by induction of Proposition 4.4.2.

Lemma 4.4.3. *Let Γ be a group and let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable, with basis $x_1, \ldots, x_\theta$ and braiding map $c\colon V \otimes V \to V \otimes V$ as in* (4.11)*. Let $n \geq 2$ and suppose that* (4.18) *holds for $m = n$ and that* (4.19) *and* (4.20) *hold for $2 \leq m \leq n - 1$. Then*

$$T^n(V) = \bigoplus_{j=1}^{\theta} \mathrm{ad}_c(x_j)(T^{n-1}(V)).$$

Proof. Since (4.18) holds for $m = n$, taking $b = {x_j}^n$ shows that $\gamma(b) = {r_{jj}}^{n-1} \neq 1$, for all $1 \leq j \leq \theta$. Therefore, by Lemma 4.3.4, it is enough to prove that the sum

$$\sum_{j=1}^{\theta} \mathrm{ad}_c(x_j)(T^{n-1}(V)) \tag{4.22}$$

is a direct sum, since it would then have the same dimension as $T^n(V)$. Note that $T^n(V) = \bigoplus_{\mathbf{t} \in t_n}^{n} \omega^n_{\mathbf{t}}(V)$, that $\omega^n_{\mathbf{t}}(V)$ is a $k\Gamma$-submodule of $T^n(V)$ contained in a single Γ-eigenspace and that for fixed j with $1 \leq j \leq \theta$, $\mathrm{ad}_c(x_j)(\omega^{n-1}_{\hat{\mathbf{t}}}(V)) \subseteq \omega^n_{\hat{\mathbf{t}}+\mathbf{j}}(V)$ for all $\hat{\mathbf{t}} \in t_{n-1}$.

Therefore,

$$\begin{aligned}
\sum_{j=1}^{\theta} \mathrm{ad}_c(x_j)(T^{n-1}(V)) &= \sum_{j=1}^{\theta} \bigoplus_{\mathbf{t}\in t_{n-1}} \mathrm{ad}_c(x_j)(\omega_{\mathbf{t}}^{n-1}(V)) \\
&= \sum_{j=1}^{\theta} \bigoplus_{\mathbf{t}\in t_n} \big(\mathrm{ad}_c(x_j)(T^{n-1}(V)) \cap \omega_{\mathbf{t}}^{n}(V)\big) \\
&= \bigoplus_{\mathbf{t}\in t_n} \sum_{j=1}^{\theta} \big(\mathrm{ad}_c(x_j)(T^{n-1}(V)) \cap \omega_{\mathbf{t}}^{n}(V)\big) \\
&= \bigoplus_{\mathbf{t}\in t_n} \sum_{j=1}^{\theta} \mathrm{ad}_c(x_j)(\omega_{\mathbf{t}-\mathbf{j}}^{n-1}(V)),
\end{aligned}$$

where we set $\omega_{\mathbf{t}}^{m}(V) = 0$ if $\mathbf{t} \in \mathbb{Z}^\theta \setminus {\mathbb{Z}_{\geq 0}}^\theta$. Let $d_{n,\mathbf{t}} := \dim_k \omega_{\mathbf{t}}^{n}(V)$. Then, if

$$a \in \sum_{j=1}^{\theta} \mathrm{ad}_c(x_j)(\omega_{\mathbf{t}-\mathbf{j}}^{n}(V)),$$

we can write a as a linear combination in two ways: firstly, in terms of the bases $\mathcal{B}_{n-1,\mathbf{t}-\mathbf{j}}$ for $1 \leq j \leq \theta$; secondly, since $a \in \omega_{\mathbf{t}}^{n}(V)$, in terms of the basis $\mathcal{B}_{n,\mathbf{t}}$. That is,

$$\begin{aligned}
a &= \sum_{j=1}^{\theta} \sum_{k=1}^{d_{n-1,\mathbf{t}-\mathbf{j}}} \alpha_{jk}\, \mathrm{ad}_c(x_j)(b_{jk}) && (4.23)\\
&= \sum_{l=1}^{d_{n,\mathbf{t}}} \mu_l m_l && (4.24)
\end{aligned}$$

where $\alpha_{jk}, \mu_l \in k$, $b_{jk} \in \mathcal{B}_{n-1,\mathbf{t}-\mathbf{j}}$ and $m_l \in \mathcal{B}_{n,\mathbf{t}}$, for $1 \leq j \leq \theta$, $1 \leq k \leq d_{n-1,\mathbf{t}-\mathbf{j}}$, $1 \leq l \leq d_{n,\mathbf{t}}$. The idea is to compare the coefficients of the monomials in (4.24) with those in (4.23), and so write the μ_l in terms of the α_{jk}. We then show that if $a = 0$, then $\alpha_{jk} = 0$ for all $1 \leq j \leq \theta$ and $1 \leq k \leq d_{n-1,\mathbf{t}-\mathbf{j}}$, which is enough to prove that (4.22) is a direct sum.

For convenience later on, if $b = b_{jk} \in \mathcal{B}_{n-1,\mathbf{t}-\mathbf{j}}$ for some $1 \leq j \leq \theta$ and $1 \leq k \leq d_{n-1,\mathbf{t}-\mathbf{j}}$, we will write $\alpha_b := \alpha_{jk}$. Similarly, if $m = m_l \in \mathcal{B}_{n,\mathbf{t}}$ for some $1 \leq l \leq d_{n,\mathbf{t}}$, we will write $\mu_m := \mu_l$.

Let $m := m_l \in \mathcal{B}_{n,\mathbf{t}}$ for some l, $1 \leq l \leq d_{n,\mathbf{t}}$ and let q denote the size of the orbit of m under C_n. Then, by (4.16), m is in the support of exactly two terms of (4.23), namely

$$\mathrm{ad}_c(\beta_1(m))(\epsilon_{n-1}(m)) = m - \gamma(m)(\tau^{q-1} \cdot m),$$

and

$$\mathrm{ad}_c(\epsilon_1(m))(\beta_{n-1}(m)) = \tau \cdot m - \gamma(\tau \cdot m)m.$$

Hence,

$$\mu_m = \alpha_{\epsilon_{n-1}(m)} - \gamma(\tau \cdot m)\alpha_{\beta_{n-1}(m)}.$$

Therefore, for any $k \geq 1$, the coefficient of $\tau^k \cdot m$ is

$$\begin{aligned}\mu_{\tau^k \cdot m} &= \alpha_{\epsilon_{n-1}(\tau^k \cdot m)} - \gamma(\tau^{k+1} \cdot m)\alpha_{\beta_{n-1}(\tau^k \cdot m)} \\ &= \alpha_{\beta_{n-1}(\tau^{k-1} \cdot m)} - \gamma(\tau^{k+1} \cdot m)\alpha_{\beta_{n-1}(\tau^k \cdot m)},\end{aligned}$$

where the second equality follows from (4.17).

Now, suppose $a = 0$, so $\mu_m = 0$. Then

$$\alpha_{\epsilon_{n-1}(m)} = \gamma(\tau \cdot m)\alpha_{\beta_{n-1}(m)}, \tag{4.25}$$

and, since $\mu_{\tau^k \cdot m} = 0$ for all $k \geq 1$,

$$\alpha_{\beta_{n-1}(\tau^{k-1} \cdot m)} = \gamma(\tau^{k+1} \cdot m)\alpha_{\beta_{n-1}(\tau^k \cdot m)}. \tag{4.26}$$

Hence, we have

$$\begin{aligned}\alpha_{\epsilon_{n-1}(m)} &= \gamma(\tau \cdot m)\alpha_{\beta_{n-1}(\tau^0 \cdot m)} \text{ by (4.25)} \\ &= \gamma(\tau \cdot m)\gamma(\tau^2 \cdot m)\alpha_{\beta_{n-1}(\tau^1 \cdot m)} && (4.27) \\ &\qquad \text{by applying (4.26) with } k = 1 \\ &= \gamma(\tau \cdot m)\gamma(\tau^2 \cdot m)\gamma(\tau^3 \cdot m)\alpha_{\beta_{n-1}(\tau^2 \cdot m)} && (4.28) \\ &\qquad \text{by applying (4.26) with } k = 2 \\ &\vdots \\ &= \prod_{k=1}^{q} \gamma(\tau^k \cdot m)\alpha_{\beta_{n-1}(\tau^{q-1} \cdot m)} && (4.29) \\ &\qquad \text{by applying (4.26) with } k = q-1.\end{aligned}$$

However, since $\tau^q \cdot m = m$, we have

$$\prod_{k=1}^{q} \gamma(\tau^k \cdot m) = \prod_{k=0}^{q-1} \gamma(\tau^k \cdot m) = \gamma(\mathcal{O}_m). \tag{4.30}$$

Using (4.17) and the fact that $\tau^q \cdot m = m$, we see that

$$\begin{aligned}\alpha_{\beta_{n-1}(\tau^{q-1} \cdot m)} &= \alpha_{\epsilon_{n-1}(\tau^q \cdot m)} \\ &= \alpha_{\epsilon_{n-1}(m)}. && (4.31)\end{aligned}$$

Substituting (4.30) and (4.31) into (4.29) gives

$$\alpha_{\epsilon_{n-1}(m)} = \gamma(\mathcal{O}_m)\alpha_{\epsilon_{n-1}(m)}.$$

Since $\gamma(\mathcal{O}_m) \neq 1$ by hypothesis, $\alpha_{\epsilon_{n-1}(m)} = 0$.

It is easy to see that, for all $1 \leq j \leq \theta$ and $1 \leq k \leq d_{n-1,\mathbf{t}-\mathbf{j}}$, $\alpha_{jk} = \alpha_{\epsilon_{n-1}(m)}$ for some $m \in \omega^{n-1}_{\mathbf{t}-\mathbf{j}}(V)$ (just take m to be $x_l b_{jk}$ for any $1 \leq l \leq \theta$). Therefore, $\alpha_{jk} = 0$, and the lemma follows. □

We can now finish the inductive proof of Proposition 4.4.2. We assume that (4.18) holds for $m = n$ and that (4.19) and (4.20) hold for $2 \leq m \leq n-1$.

Proof. (i) By Lemma 4.3.2 (iii), for all $1 \leq j \leq \theta$,

$$\sum_{l=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,n-1}) \subseteq \ker D_{j,n}.$$

By Lemma 4.4.3, the above sum is direct. The hypothesis (4.18) implies that ${r_{ii}}^k \neq 1$ for any $1 \leq k \leq n-1$. Therefore, by Lemma 4.3.3 (ii), $\dim_k(\ker D_{j,n-1}) = \theta^{n-2}(\theta-1)$ for $1 \leq j \leq \theta$. Hence, the dimension of the above sum is $\theta^{n-1}(\theta-1)$, which is equal to the dimension of $\ker D_{j,n}$, meaning that the inclusion is an equality, as required for (4.19).

(ii) By part (i), using the fact that the sum $\sum_{l=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,n-1})$ is direct, and that, by Lemma 4.3.4, for $1 \leq l \leq \theta$, $\mathrm{ad}_c(x_l)$ is a monomorphism,

$$\begin{aligned}
\bigcap_{j=1}^{\theta} \ker D_{j,n} &= \bigcap_{j=1}^{\theta}\left(\bigoplus_{l=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,n-1})\right) \\
&= \bigoplus_{l=1}^{\theta}\left(\bigcap_{j=1}^{\theta} \mathrm{ad}_c(x_l)(\ker D_{j,n-1})\right) \\
&= \bigoplus_{l=1}^{\theta} \mathrm{ad}_c(x_l)\left(\bigcap_{j=1}^{\theta} \ker D_{j,n-1}\right) \\
&= 0, \ \text{ by(4.20) with } m = n-1.
\end{aligned}$$

□

Theorem 4.4.1 gives sufficient conditions for $B(V) \cong T(V)$ in terms of the action of the symmetric group. This condition is difficult to describe purely in terms of restrictions on the scalars r_{ij}. However, the following corollary gives stronger conditions that are easier to describe explicitly.

Corollary 4.4.4. *Let Γ be a group and let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable, with basis $x_1, \ldots, x_\theta$ and braiding map $c\colon V \otimes V \to V \otimes V$ as in* (4.11)*. Suppose that there do not exist non-negative integers $t_1, \ldots, t_\theta$ such that*

- $2 \le \sum_{i=1}^{\theta} t_i$,
- $\prod_{i,j=1}^{\theta} r_{ij}^{k_{ij}} = 1$, *where* $k_{ij} = t_i t_j - \delta_{ij} t_i$.

Then $B(V) \cong T(V)$.

Proof. Let $\gamma = \prod_{i,j=1}^{\theta} {r_{ij}}^{k_{ij}}$. Let $\mathbf{t} := (t_1, \ldots, t_\theta) \in \mathbb{Z}_{\ge 0}$ and let $n := \sum_{i=1}^{\theta} t_i$. Then for all $m \in B_{n,\mathbf{t}}$ with $|\mathcal{O}_m| = q$, we have $(\gamma(\mathcal{O}_m))^{n/q} = \gamma$. To see this, first suppose that $q = n$; that is, that $\mathcal{O}_m$ is a long orbit. Then for all $1 \le i \le \theta$, x_i occurs t_i times at the start of a monomial in $\mathcal{O}_m$. Each time this happens, there are $t_i - 1$ instances of x_i in last $n-1$ letters of the monomial and t_j instances of x_j in the last $n-1$ letters for all $1 \le j \ne i \le \theta$. This means that r_{ii} occurs $t_i(t_i - 1)$ times and r_{ij} occurs $t_i t_j$ times in $\gamma(\mathcal{O}_m)$, as required. Now suppose that $\mathcal{O}_m$ is a short orbit. If we treated it as a long orbit, listing each member with n/q repetitions, then the scalar associated with this orbit would be $\gamma(\mathcal{O}_m)^{n/q}$. By the same argument as for the long orbit case, this is equal to γ.

If $\gamma \ne 1$, then $\gamma(\mathcal{O}_m) \ne 1$. Therefore, we may apply Theorem 4.4.1, which shows that $B(V) \cong T(V)$. □

A corollary of Theorem 4.4.1 answers a question of Andruskiewitsch and Schneider [2, Example 3.5]:

Corollary 4.4.5. *Let Γ be a group and let $V \in {}^{\Gamma}_{\Gamma}\mathcal{YD}$ be finite dimensional and diagonalisable, with a basis such that the braiding map $c := r\tau\colon V \otimes V \to V \otimes V$, where $\tau\colon V \otimes V \to V \otimes V$ is the "flip" map. Then $B(V) \cong T(V)$ if and only if either $r = 1$ or r is not a root of unity.*

Proof. Let $x_1, \ldots, x_\theta$ be a basis of V. Suppose $r \ne 1$ and r is a primitive nth root of unity. Then, for all $1 \le i \le \theta$, and for all $1 \le j \le \theta$ with $j \ne i$, $D_{j,n}({x_i}^n) = 0$ and

$$D_{i,n}({x_i}^n) = (1 + r + \ldots + r^{n-1}){x_i}^{n-1} = 0,$$

so ${x_i}^n \in I(V)$ and hence $B(V) \ncong T(V)$. If $r = 1$, then the braiding of V is trivial and clearly $B(V) \cong T(V)$. Conversely, if $r \ne 1$ and r is not a root of unity, then the conditions of Theorem 4.4.1 are satisfied and hence $B(V) \cong T(V)$. □

Remark. An equivalent problem was previously studied by Frønsdal in [19], although he does not express it in the language of Nichols algebras. He obtains a result that is equivalent to Lemma 4.4.3, although his methods and presentation are different to the above. It seems that Andruskiewitsch and Schneider were not aware of this when compiling the survey article [2], since they do not reference [19] and consider [2, Example 3.5] to be an open question.

The results here were originally obtained independently of [19], although in the form of Corollary 4.4.4 rather than in the form of Theorem 4.4.1. After completing this work, we adapted the technique of [19] involving the action of the symmetric group on the monomials in order to sharpen our result.

Chapter 5

Ambiskew Hopf algebras

In this chapter, we consider a type of iterated skew polynomial ring called an ambiskew polynomial algebra, which we denote by A. These algebras were first given this name in [28], although they had appeared previously in the literature - for example, in [29]. They are closely related to down-up algebras [8] and to generalised Weyl algebras [6].

In previous work on these algebras, the base ring R has been a commutative affine algebra. Here, we remove the commutativity assumption on R. In the case where R is a Hopf algebra, we examine the conditions under which its Hopf structure extends to a Hopf structure on A, with a certain assumption about the coproduct on the skew-polynomial variables. We also calculate the coradical filtration of A when the coradical of R is a Hopf algebra. Lastly, we consider some properties of A, including the conditions under which A satisfies a polynomial identity.

5.1 Definition

Let k be an algebraically closed field of characteristic zero and let R be an affine k-algebra. Let σ be an automorphism of R, let $h \in Z(R)$ and let $0 \neq \xi \in k$. We define $A = A(R, X_+, X_-, \sigma, h, \xi)$ to be the k-algebra generated by R and two indeterminates, X_+ and X_-, subject to the relations

$$X_\pm a = \sigma^{\pm 1}(a) X_\pm, \tag{5.1}$$

$$X_+ X_- = h + \xi X_- X_+, \tag{5.2}$$

for all $a \in R$. The algebra A is called an *ambiskew polynomial algebra*.

A has the structure of an iterated skew polynomial ring over R, as follows. The subring of A generated by R and X_+ is just the skew polynomial ring $R[X_+,\sigma]$. We can extend $\sigma^{-1}\colon R \to R$ to a map which we continue to denote by $\sigma^{-1}\colon R[X_+,\sigma] \to R[X_+,\sigma]$ by defining $\sigma^{-1}(X_+) = \xi^{-1}X_+$. Define the $(\sigma^{-1}, \mathrm{id})$-derivation $\delta\colon R[X_+,\sigma] \to R[X_+,\sigma]$ by $\delta(R) = 0$, $\delta(X_+) = -\xi^{-1}h$. This is well-defined since h is central in R. Then

$$A = R[X_+,\sigma][X_-,\sigma^{-1},\delta].$$

Consequently, A is a free left and right R-module, with basis

$$\{X_+{}^m X_-{}^n \colon m, n \geq 0\}. \tag{5.3}$$

In addition, $A \otimes A$ is a free left and right $R \otimes R$-module, with basis

$$\{X_-{}^m X_+{}^n \otimes X_-{}^p X_+{}^q \colon m, n, p, q \geq 0\}. \tag{5.4}$$

5.2 Hopf algebra structure

5.2.1 The main theorem

Let R be an affine k-algebra equipped with a Hopf structure. We will state and prove a theorem giving conditions which are necessary and sufficient to ensure an extension of this Hopf structure to A, with the proviso that

$$\Delta(X_\pm) = X_\pm \otimes r_\pm + l_\pm \otimes X_\pm, \tag{5.5}$$

for some $l_\pm, r_\pm \in R$. This question was previously considered in [22, Theorem 3.1], where R is assumed to be commutative. We obtain a generalisation of this theorem for not necessarily commutative R.

Lemma 5.2.1. *(i) Suppose R is equipped with a bialgebra structure, which extends to a bialgebra structure on $A := (A, m, u, \Delta, \varepsilon)$ such that* (5.5) *holds. Then*

(a) $r_\pm$ and $l_\pm$ are grouplike,

(b) $[r_+, r_-] = [l_+, l_-] = 0$.

(ii) Suppose R is equipped with a Hopf algebra structure, which extends to a Hopf algebra structure on $A := (A, m, u, \Delta, \varepsilon, S)$ such that (5.5) *holds. Let $\chi := \varepsilon \circ \sigma \colon R \to k$. Then*

(a) $\sigma(r_\pm) = \chi(r_\pm)r_\pm$ and $\sigma(l_\pm) = \chi(l_\pm)l_\pm$,

(b) r_+r_- and l_+l_- are central in R.

Proof. In this proof, we suppose that $\Delta\colon A \to A \otimes A$ and $\varepsilon\colon A \to k$ are algebra homomorphisms extending, respectively, the coproduct and counit on R. We show that Δ preserves (5.1) and (5.2), and Δ and ε satisfy, respectively, the coassociativity and counit axioms if and only if certain conditions hold. This means that we prove slightly more than is required, but for convenience later we will refer back to some of these calculations.

(i) (a) If $\varepsilon\colon A \to k$ is any algebra homomorphism extending the counit on R, then ε satisfies the counit condition for A if and only if

$$m(\mathrm{id} \otimes \varepsilon)\Delta(X_\pm) = X_\pm \varepsilon(r_\pm) + l_\pm \varepsilon(X_\pm) = X_\pm,$$
$$m(\varepsilon \otimes \mathrm{id})\Delta(X_\pm) = \varepsilon(X_\pm) r_\pm + \varepsilon(l_\pm) X_\pm = X_\pm.$$

Rearranging gives

$$(1 - \varepsilon(r_\pm))X_\pm = l_\pm \varepsilon(X_\pm)$$
$$(1 - \varepsilon(l_\pm))X_\pm = \varepsilon(X_\pm) r_\pm.$$

By the fact that A is a free R-module with basis (5.3), both sides must be zero, so ε satisfies the counit condition if and only if

$$\varepsilon(X_\pm) = 0 \text{ and } \varepsilon(l_\pm) = \varepsilon(r_\pm) = 1. \tag{5.6}$$

Furthermore, if $\Delta\colon A \to A \otimes A$ is an algebra homomorphism extending the coproduct on R, then the coassociativity condition for Δ is equivalent to

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

and this holds if and only if

$$X_\pm \otimes (\Delta(r_\pm) - r_\pm \otimes r_\pm) = (\Delta(l_\pm) - l_\pm \otimes l_\pm) \otimes X_\pm.$$

By the facts that $A \otimes A$ is a free $R \otimes R$-module on basis (5.4) and that $\Delta(R) \subseteq R \otimes R$, both sides must be zero. Therefore, Δ is coassociative if and only if

$$\Delta(l_\pm) = l_\pm \otimes l_\pm \text{ and } \Delta(r_\pm) = r_\pm \otimes r_\pm. \tag{5.7}$$

(b) Δ preserves (5.2) if and only if

$$\begin{aligned}
&\Delta(X_+)\Delta(X_-) = \Delta(h) + \xi\Delta(X_-)\Delta(X_+)\\
&\Leftrightarrow (h + \xi X_-X_+) \otimes r_+r_- + l_+l_- \otimes (h + \xi X_-X_+)\\
&\quad - \Delta(h) - \xi X_-X_+ \otimes r_-r_+ - \xi l_-l_+ \otimes X_-X_+\\
&\qquad + (\sigma(l_-) \otimes r_+ - \xi l_- \otimes \sigma^{-1}(r_+))X_+ \otimes X_-\\
&\qquad\quad + (l_+ \otimes \sigma(r_-) - \xi\sigma^{-1}(l_+) \otimes r_-)X_- \otimes X_+ = 0\\
&\Leftrightarrow h \otimes r_+r_- + l_+l_- \otimes h - \Delta(h)\\
&\quad + (\xi \otimes (r_+r_- - r_-r_+))X_-X_+ \otimes 1\\
&\qquad ((l_+l_- - l_-l_+) \otimes \xi)1 \otimes X_-X_+\\
&\qquad\quad + (\sigma(l_-) \otimes r_+ - \xi l_- \otimes \sigma^{-1}(r_+))X_+ \otimes X_-\\
&\qquad\qquad + (l_+ \otimes \sigma(r_-) - \xi\sigma^{-1}(l_+) \otimes r_-)X_- \otimes X_+ = 0
\end{aligned}$$

Using the linear independence of the $R \otimes R$-basis (5.4) of $A \otimes A$ and the fact that $\xi \neq 0$, this shows that Δ preserves (5.2) if and only if

$$\Delta(h) = h \otimes r_+r_- + l_+l_- \otimes h, \tag{5.8}$$

$$[r_+, r_-] = [l_+, l_-] = 0, \tag{5.9}$$

$$\sigma(l_-) \otimes r_+ = \xi l_- \otimes \sigma^{-1}(r_+), \tag{5.10}$$

$$l_+ \otimes \sigma(r_-) = \xi\sigma^{-1}(l_+) \otimes r_-. \tag{5.11}$$

(ii) (a) Note that if R is a Hopf algebra, the antipode condition implies that the group-like elements $r_\pm$ and $l_\pm$ are invertible [42, Example 1.5.3].

For all $a \in R$, using (5.5) and (5.1),

$$\begin{aligned}
\Delta(X_\pm)\Delta(a) &= (l_\pm \otimes X_\pm + X_\pm \otimes r_\pm)\left(\sum a_1 \otimes a_2\right)\\
&= \sum l_\pm a_1 \otimes X_\pm a_2 + X_\pm a_1 \otimes r_\pm a_2\\
&= \sum l_\pm a_1 \otimes \sigma^{\pm1}(a_2)X_\pm + \sigma^{\pm1}(a_1)X_\pm \otimes r_\pm a_2.
\end{aligned} \tag{5.12}$$

Δ preserves (5.1) if and only if, for all $a \in R$,

$$\Delta(X_\pm)\Delta(a) = \Delta(\sigma^{\pm1}(a))\Delta(X_\pm).$$

By (5.5) and (5.12), this is equivalent to

$$\sum l_\pm a_1 \otimes \sigma^{\pm1}(a_2)X_\pm + \sigma^{\pm1}(a_1)X_\pm \otimes r_\pm a_2 = \Delta(\sigma^{\pm1}(a))(X_\pm \otimes r_\pm + l_\pm \otimes X_\pm);$$

that is,

$$\left(\sum l_\pm a_1 \otimes \sigma^{\pm 1}(a_2) - \Delta(\sigma^{\pm 1}(a))(l_\pm \otimes 1)\right)(1 \otimes X_\pm)$$
$$= \left(\sum \Delta(\sigma^{\pm 1}(a))(1 \otimes r_\pm) - \sigma^{\pm 1}(a_1) \otimes r_\pm a_2\right)(X_\pm \otimes 1).$$

Therefore, Δ preserves (5.1) if and only if, for all $a \in R$,

$$(\Delta(\sigma^{\pm 1}(a))(l_\pm \otimes 1) - (l_\pm \otimes 1)(\mathrm{id} \otimes \sigma^{\pm 1})\Delta(a))(1 \otimes X_\pm)$$
$$+ (\Delta(\sigma^{\pm 1}(a))(1 \otimes r_\pm) - (1 \otimes r_\pm)(\sigma^{\pm 1} \otimes \mathrm{id})\Delta(a))(X_\pm \otimes 1) = 0.$$

Using the linear independence of the $R \otimes R$-basis (5.4) of $A \otimes A$, this is equivalent to

$$\Delta(\sigma^{\pm 1}(a))(l_\pm \otimes 1) = (l_\pm \otimes 1)(\mathrm{id} \otimes \sigma^{\pm 1})\Delta(a),$$

and

$$\Delta(\sigma^{\pm 1}(a))(1 \otimes r_\pm) = (1 \otimes r_\pm)(\sigma^{\pm 1} \otimes \mathrm{id})\Delta(a).$$

Since $r_\pm$ and $l_\pm$ are invertible, Δ preserves (5.1) if and only if

$$\Delta(\sigma^{\pm 1}(a)) = (\mathrm{ad}_l(l_\pm) \otimes \mathrm{id})(\mathrm{id} \otimes \sigma^{\pm 1})\Delta(a), \tag{5.13}$$

and

$$\Delta(\sigma^{\pm 1}(a)) = (\mathrm{id} \otimes \mathrm{ad}_l(r_\pm))(\sigma^{\pm 1} \otimes \mathrm{id})\Delta(a). \tag{5.14}$$

Putting $a = r_\pm$ in (5.14) shows that

$$\Delta(\sigma^{\pm 1}(r_\pm)) = \sigma^{\pm 1}(r_\pm) \otimes r_\pm.$$

Applying $m(\varepsilon \otimes \mathrm{id})$ to both sides gives

$$\sigma^{\pm 1}(r_\pm) = (\varepsilon \circ \sigma^{\pm 1})(r_\pm) r_\pm.$$

This gives the result as stated in (ii)(a) for $\sigma(r_+)$, and shows that

$$\sigma^{-1}(r_-) = (\varepsilon \circ \sigma^{-1})(r_-) r_-.$$

Applying σ to both sides and rearranging gives

$$\sigma(r_-) = ((\varepsilon \circ \sigma^{-1})(r_-))^{-1} r_-. \tag{5.15}$$

Applying ε to both sides shows that

$$(\varepsilon \circ \sigma)(r_-) = ((\varepsilon \circ \sigma^{-1})(r_-))^{-1}.$$

Substituting this into (5.15) gives the stated value in (ii)(a) for $\sigma(r_-)$. A similar calculation leads to the corresponding result for $\sigma(l_\pm)$.

(b) By (5.14), for all $a, b \in R$,

$$\Delta(\sigma(a)) = \sum \sigma(a_1) \otimes r_+ a_2 {r_+}^{-1}$$
$$\Delta(\sigma^{-1}(b)) = \sum \sigma^{-1}(b_1) \otimes r_- b_2 {r_-}^{-1}.$$

Taking $b = \sigma(a)$ in the last equation shows that

$$\Delta(a) = \sum a_1 \otimes r_- r_+ a_2 {r_+}^{-1} {r_-}^{-1}.$$

Applying $m(\varepsilon \otimes \mathrm{id})$ gives $a = r_- r_+ a (r_- r_+)^{-1}$ for all $a \in R$, so $r_- r_+$ is central in R. By (5.9), $r_+ r_-$ is central in R. A similar argument using (5.13) shows that $l_+ l_-$ is central in R. □

Let R be a Hopf algebra, so that $r_\pm$ is invertible, by Lemma 5.2.1 (i)(a) and [42, Example 1.5.3]. We can equally well think of A as the ambiskew polynomial algebra with the variables $X_\pm$ replaced by $X_\pm {r_\pm}^{-1}$, with slight adjustments to σ, ξ and h, as follows:

Lemma 5.2.2. *Let R be an affine Hopf algebra and let $A = A(R, X_+, X_-, \sigma, \xi, h)$ be an ambiskew algebra. Suppose $r_\pm \in R$ is invertible and set $\chi := \varepsilon \circ \sigma \colon R \to k$. Then we also have*

$$A = A(R, X_+ {r_+}^{-1}, X_- {r_-}^{-1}, \hat{\sigma}, \hat{\xi}, \hat{h}),$$

where $\hat{\sigma} = \mathrm{ad}_l(r_+) \circ \sigma$, $\hat{\xi} = \xi \chi(r_+ r_-)^{-1}$ and $\hat{h} = \chi(r_+)^{-1} h (r_+ r_-)^{-1}$.

Proof. Since $r_\pm$ is invertible, both sets are the same. We only have to check the equivalence of relations (5.1) and (5.2) with the ambiskew relations for our new ambiskew data: that is, for all $a \in R$, we should have

$$(X_\pm {r_\pm}^{-1}) a = \hat{\sigma}^{\pm 1}(a)(X_\pm {r_\pm}^{-1}), \tag{5.16}$$
$$(X_+ {r_+}^{-1})(X_- {r_-}^{-1}) = \hat{\xi}(X_- {r_-}^{-1})(X_+ {r_+}^{-1}) + \hat{h}. \tag{5.17}$$

Since $r_\pm$ is a grouplike element in a Hopf algebra, $\mathrm{ad}_l(r_\pm)(a) = r_\pm a {r_\pm}^{-1}$ for all $a \in R$. It is easy to check, using Lemma 5.2.1 (i)(b) and (ii)(a),(b), that $\hat{\sigma}^{-1} = \mathrm{ad}_l(r_-) \circ \sigma^{-1}$. Firstly, we show that (5.16) holds: for all $a \in R$,

$$\begin{aligned}
(X_\pm {r_\pm}^{-1}) a &= \sigma^{\pm 1}({r_\pm}^{-1} a) X_\pm (r_\pm {r_\pm}^{-1}) \\
&= \chi(r_\pm)^{\mp 1} {r_\pm}^{-1} \sigma^{\pm 1}(a) X_\pm (r_\pm {r_\pm}^{-1}) \text{ by Lemma 5.2.1 (ii)(a)} \\
&= \chi(r_\pm)^{\mp 1} {r_\pm}^{-1} \sigma^{\pm 1}(a) \sigma^{\pm 1}(r_\pm)(X_\pm {r_\pm}^{-1}) \text{ by (5.1)} \\
&= \chi(r_\pm)^{\mp 1} \chi(r_\pm)^{\pm 1} {r_\pm}^{-1} \sigma^{\pm 1}(a) r_\pm (X_\pm {r_\pm}^{-1}) \text{ by Lemma 5.2.1 (ii)(a)} \\
&= \hat{\sigma}^{\pm 1}(a)(X_\pm {r_\pm}^{-1}),
\end{aligned}$$

as required. Secondly, we show (5.17) holds:

$$\begin{aligned}(X_+{r_+}^{-1})(X_-{r_-}^{-1}) &= X_+X_-\sigma({r_+}^{-1}){r_-}^{-1} \\ &= \chi(r_+)^{-1}X_+X_-{r_+}^{-1}{r_-}^{-1} \text{ by Lemma 5.2.1 (ii)(a)} \\ &= \chi(r_+)^{-1}(\xi X_-X_+ + h){r_+}^{-1}{r_-}^{-1} \text{ by (5.2)} \\ &= \chi(r_+)^{-1}\xi X_-\sigma({r_-}^{-1})X_+{r_+}^{-1} + \hat{h} \text{ by Lemma 5.2.1 (i)(b) and (5.1)} \\ &= \chi(r_+)^{-1}\chi(r_-)^{-1}\xi(X_-{r_-}^{-1})(X_+{r_+}^{-1}) + \hat{h} \text{ by Lemma 5.2.1 (ii)(a)} \\ &= \hat{\xi}(X_-{r_-}^{-1})(X_+{r_+}^{-1}) + \hat{h},\end{aligned}$$

as required. □

The previous lemma shows that we may adjust the ambiskew data and relabel our variables if necessary to make $X_\pm$ skew-primitive. So, without loss of generality, we can assume that

$$\Delta(X_\pm) = X_\pm \otimes 1 + y_\pm \otimes X_\pm, \tag{5.18}$$

for some $y_\pm \in R$, which significantly simplifies our later calculations. Here our approach differs from [22], which omits this step.

Let H be a Hopf algebra. Recall that $\mathrm{Alg}_k(H,k)$, the set of algebra homomorphisms $H \to k$, is a group under the convolution product [49, Theorem 4.0.5]. If $\phi \in \mathrm{Alg}_k(H,k)$ let $\phi^{-1} \in \mathrm{Alg}_k(H,k)$ denote its convolution inverse. In fact, $\phi^{-1} = \phi \circ S$. Recall also that the *left winding automorphism* $\tau^l_\phi \colon H \to H$ is defined by

$$\tau^l_\phi(h) = m(\phi \otimes \mathrm{id})\Delta(h) = \sum \phi(h_1)h_2,$$

and the *right winding automorphism* $\tau^r_\phi \colon H \to H$ is defined by

$$\tau^r_\phi(h) = m(\mathrm{id} \otimes \phi)\Delta(h) = \sum h_1\phi(h_2).$$

It is easy to check that $(\tau^l_\phi)^{-1} = \tau^l_{\phi^{-1}}$ and $(\tau^r_\phi)^{-1} = \tau^r_{\phi^{-1}}$.

Theorem 5.2.3. *Suppose R is equipped with a Hopf algebra structure. Let $\chi := \varepsilon \circ \sigma \colon R \to k$. Then the Hopf algebra structure on R extends to a Hopf algebra structure on A, where the coproduct Δ satisfies* (5.18), *if and only if*

- *$y_\pm$ is grouplike. That is,*

$$\Delta(y_\pm) = y_\pm \otimes y_\pm, \tag{A}$$

$$\varepsilon(y_\pm) = 1. \tag{B}$$

- *$y_\pm$ satisfies*

$$y_+y_- = y_-y_+ \in Z(R). \tag{C}$$

- *$X_\pm$ satisfies*

$$\varepsilon(X_\pm) = 0, \tag{D}$$
$$S(X_\pm) = -{y_\pm}^{-1}X_\pm. \tag{E}$$

- *h satisfies*

$$\Delta(h) = h \otimes 1 + y_-y_+ \otimes h, \tag{F}$$
$$\varepsilon(h) = 0, \tag{G}$$
$$S(h) = -(y_-y_+)^{-1}h. \tag{H}$$

- *σ satisfies the compatibility conditions*

$$\sigma^{\pm1}|_R = \tau^l_{\chi^{\pm1}}, \tag{I}$$
$$\sigma^{\pm1}|_R = \mathrm{ad}_l(y_\pm) \circ \tau^r_{\chi^{\pm1}}, \tag{J}$$
$$\sigma^{\mp1} \circ S|_R = \mathrm{ad}_r(y_\pm) \circ S \circ \sigma^{\pm1}|_R, \tag{K}$$
$$\sigma(y_\pm) = \xi y_\pm. \tag{L}$$

Proof. Under our assumption (5.18), A is a Hopf algebra if and only if the definitions of Δ, ε and S on $X_\pm$ satisfy, respectively, the coassociativity, counit and antipode conditions, and are well-defined on relations (5.1) and (5.2).

Firstly, we consider ε. Assume for the moment that Δ as defined is a k-algebra homomorphism from A to $A \otimes A$. Then ε is a counit if and only if (5.6) holds with $l_\pm = y_\pm$ and $r_\pm = 1$, which is equivalent to (B) and (D). Consequently, ε automatically preserves (5.1). Using (D), we see that ε preserves (5.2) if and only if (G) holds.

Secondly, we consider Δ. Δ is coassociative if and only if (5.7) holds, with $l_\pm = y_\pm$ and $r_\pm = 1$, which is equivalent to (A). Furthermore, Δ preserves (5.1) if and only if (5.13) and (5.14) hold, with $l_\pm = y_\pm$ and $r_\pm = 1$, which are equivalent to

$$\Delta \circ \sigma|_R{}^{\pm1} = (\sigma^{\pm1} \otimes \mathrm{id}) \circ \Delta|_R, \tag{5.19}$$
$$\Delta \circ \sigma|_R{}^{\pm1} = (\mathrm{ad}_l(y_\pm) \otimes \mathrm{id})(\mathrm{id} \otimes \sigma^{\pm1}) \circ \Delta|_R. \tag{5.20}$$

Applying $m(\varepsilon \otimes \mathrm{id})$ to the first equation and $m(\mathrm{id} \otimes \varepsilon)$ to the second gives

$$\sigma^{\pm 1}|_R = \tau^l_{\chi_\pm}, \tag{5.21}$$

$$\sigma^{\pm 1}|_R = \mathrm{ad}_l(y_\pm) \circ \tau^r_{\chi_\pm}, \tag{5.22}$$

where we set $\chi_+ := \chi$ and $\chi_- := \varepsilon \circ \sigma^{-1}$. Conversely, if (5.21) and (5.22) hold, it is easy to check that (5.19) and (5.20) hold. We leave aside (5.21) and (5.22) momentarily, but will presently show that they are equivalent to (I) and (J). Δ preserves (5.2) if and only if (5.8) to (5.11) hold, with $l_\pm = y_\pm$ and $r_\pm = 1$. (5.8) is equivalent to (F), (5.9) is equivalent to (C) by Lemma 5.2.1 (ii)(b), and (5.10) and (5.11) are both equivalent to (L).

Lastly, we consider S. Assume first that $S\colon A \to A$ is an antihomomorphism. S has the antipode property if and only if

$$0 = \varepsilon(X_\pm) = X_\pm + y_\pm S(X_\pm) = S(X_\pm) + {y_\pm}^{-1} X_\pm,$$

which is equivalent to (E).

Now we examine the antihomomorphism property of S. S preserves (5.1) if and only if, for all $a \in R$,

$$\begin{aligned}
S(X_\pm a) &= S(\sigma^{\pm 1}(a) X_\pm) \\
\Leftrightarrow S(a) S(X_\pm) &= S(X_\pm) S(\sigma^{\pm 1}(a)) \\
\Leftrightarrow S(a) {y_\pm}^{-1} X_\pm &= {y_\pm}^{-1} X_\pm S(\sigma^{\pm 1}(a)) \\
\Leftrightarrow S(a) {y_\pm}^{-1} X_\pm &= {y_\pm}^{-1} \sigma^{\pm 1}(S(\sigma^{\pm 1}(a))) X_\pm \\
\Leftrightarrow S(a) {y_\pm}^{-1} &= {y_\pm}^{-1} \sigma^{\pm 1}(S(\sigma^{\pm 1}(a))) \\
S(a) &= {y_\pm}^{-1} \sigma^{\pm 1}(S(\sigma^{\pm 1}(a))) y_\pm \\
\Leftrightarrow \sigma^{\mp 1}(S(a)) &= \sigma^{\mp}({y_\pm}^{-1}) S(\sigma^{\pm 1}(a)) \sigma^{\mp}(y_\pm).
\end{aligned}$$

By (L), this is equivalent to (K). Consequently, it is easy to check that $\varepsilon \circ \sigma \circ S = \varepsilon \circ \sigma^{-1}$ - in other words, that $\varepsilon \circ \sigma^{-1} = \chi^{-1}$, the convolution inverse of χ in $\mathrm{Alg}_k(R, k)$. This shows that (5.21) and (5.22) are equivalent to (I) and (J).

S preserves (5.2) if and only if

$$\begin{aligned}
S(X_+X_-) &= S(h) + \xi S(X_-X_+) \\
\Leftrightarrow S(X_-)S(X_+) &= S(h) + \xi S(X_+)S(X_-) \\
\Leftrightarrow {y_-}^{-1}X_-{y_+}^{-1}X_+ &= S(h) + \xi {y_+}^{-1}X_+{y_-}^{-1}X_- \\
\Leftrightarrow {y_-}^{-1}\sigma^{-1}({y_+}^{-1})X_-X_+ &= S(h) + \xi {y_+}^{-1}\sigma({y_-}^{-1})X_+X_- \\
\Leftrightarrow \xi {y_-}^{-1}{y_+}^{-1}X_-X_+ &= S(h) + {y_+}^{-1}{y_-}^{-1}(h + \xi X_-X_+) \text{ by (5.2) and (L)} \\
\Leftrightarrow S(h) + {y_+}^{-1}{y_-}^{-1}h + \xi({y_+}^{-1}&{y_-}^{-1} - {y_-}^{-1}{y_+}^{-1})X_-X_+ = 0.
\end{aligned}$$

Using the linear independence of the R-basis (5.3) of A, this is equivalent to (H) and (C). □

Given a fixed Hopf algebra R whose structure extends to a Hopf algebra structure on A with (5.18), we are interested in determining the interplay between the ambiskew data - σ, h and ξ - and the data resulting from the Hopf algebra structure - $y_\pm$ and χ. The following corollary clarifies this matter somewhat.

For $g, h \in G(R)$, let

$$P_{g,h}(R) := \{a \in R\colon \Delta(a) = a \otimes g + h \otimes a\}.$$

For all $g, h \in G(R)$, $P_{g,h}(R)$ is non-empty because it contains 0.

Corollary 5.2.4. *Let R be a Hopf algebra and let $y_\pm \in G(R)$. Let $\chi\colon R \to k$ be an algebra homomorphism such that the following hold:*

(i) $\chi(y_+) = \chi(y_-)$,

(ii) $\mathrm{ad}_l(y_\pm) = \tau^l_{\chi^{\pm 1}} \circ \tau^r_{\chi^{\mp 1}}$.

Then there is an ambiskew Hopf algebra $A = A(R, X_+, X_-, \sigma, \xi, h)$ extending the Hopf algebra structure of R with (5.18)*, where we set $\sigma := \tau^l_\chi$ and $\xi := \chi(y_+)$, and choose h to be any member of $P_{1,y_-y_+}(R)$ that is central in R. Furthermore, every ambiskew Hopf algebra extending the Hopf algebra structure of R arises in this way.*

Proof. Let $y_\pm \in G(R)$ and suppose that there exists an algebra homomorphism $\chi\colon R \to k$ such that (i) and (ii) hold. Make the definitions for σ, ξ and h above. We must show that A satisfies the conditions of Theorem 5.2.3. By hypothesis, (A) and (B) hold. Any left winding automorphism commutes with any right winding automorphism. Therefore, (ii) shows that $\mathrm{ad}_l(y_+) = \tau^r_{\chi^{-1}} \circ \tau^l_\chi$ and $\mathrm{ad}_l(y_-) = \tau^l_{\chi^{-1}} \circ \tau^r_\chi$. We also have $(\tau^l_\chi)^{-1} = \tau^l_{\chi^{-1}}$ and $(\tau^r_\chi)^{-1} = \tau^r_{\chi^{-1}}$, so considering the composition $\mathrm{ad}_l(y_+) \circ \mathrm{ad}_l(y_-) = \mathrm{ad}_l(y_+y_-)$ shows that $\mathrm{ad}_l(y_+y_-) = \mathrm{id}$, and hence y_+y_- is central in R. Consequently, $(y_+y_-)y_- = y_-(y_+y_-)$ and thus $y_-y_+ = y_+y_-$, so (C) holds. We can define $\varepsilon(X_\pm)$ and $S(X_\pm)$ as in (D) and (E). By our choice of h, (F) - (H) hold. Using (ii) together with the definition of σ gives (I) and (J). To check (K), note the following facts. Firstly, $\mathrm{ad}_l(y_\pm)$ commutes with S and $\mathrm{ad}_r(y_\pm) \circ \mathrm{ad}_l(y_\pm) = \mathrm{id}$. Secondly, since χ and χ^{-1} are convolution inverses, we have $\chi^{\pm 1} = \chi^{\mp} \circ S$. Thirdly, for all $a \in R$, the antihomomorphism property of S implies that $\Delta \circ S(a) = \sum S(a_2) \otimes S(a_1)$. Therefore, for all $a \in R$,

$$\begin{aligned}
\mathrm{ad}_r(y_\pm) \circ S \circ \sigma^{\pm 1}(a) &= \mathrm{ad}_r(y_\pm) \circ S \circ \mathrm{ad}_l(y_\pm) \circ \tau^r_{\chi^{\pm 1}}(a) \\
&= \mathrm{ad}_r(y_\pm) \circ \mathrm{ad}_l(y_\pm) \circ S \circ \tau^r_{\chi^{\pm 1}}(a) \\
&= S \circ \tau^r_{\chi^{\pm 1}}(a) = S\left(\sum a_1 \chi^{\pm 1}(a_2)\right) \\
&= \sum \chi^{\pm 1}(a_2) S(a_1) = \sum \chi^{\mp 1}(S(a_2)) S(a_1) \\
&= \tau^l_{\chi^{\mp 1}} \circ S(a) = \sigma^{\mp 1} \circ S(a),
\end{aligned}$$

and so (K) holds. This shows that A is a Hopf algebra.

Now suppose that $A = A(R, X_+, X_-, \sigma, \xi, h)$ is an ambiskew Hopf algebra such that (5.18) holds and let $\chi := \varepsilon \circ \sigma$. Then (i) holds by Theorem 5.2.3 (L). Equating the expressions for $\sigma^{\pm 1}$ in (I) and (J) gives (ii). $\square$

Therefore, the problem of studying ambiskew Hopf algebras with (5.18) reduces to studying the possible choices of $y_\pm \in G(R)$ and algebra homomorphisms $\chi\colon R \to k$ satisfying

$$\chi(y_+) = \chi(y_-) \text{ and } \mathrm{ad}_l(y_\pm) = \tau^l_{\chi^{\pm 1}} \circ \tau^r_{\chi^{\mp 1}}. \tag{5.23}$$

When A is a Hopf algebra, we can also describe in more detail the behaviour of certain subspaces of R with respect to $y_\pm$ and σ.

Corollary 5.2.5. *Suppose R is equipped with a Hopf algebra structure that extends to a Hopf algebra structure on A such that* (5.18) *holds. Let $\sigma := \tau^l_\chi$, where $\chi\colon R \to k$. Then the following conditions hold:*

(i) Let $\tau\colon R \otimes R \to R \otimes R$ denote the "flip" map. Then, for all $a \in R$ such that $\tau \circ \Delta(a) = \Delta(a)$, we have $y_\pm a = a y_\pm$.

(ii) Let $G := G(R)$. Then

(a) $\sigma|_G \colon G \to G$ *is defined by, for* $g \in G$*,*

$$\sigma|_G(g) = \chi(g)g,$$

where $\chi(y_\pm) = \xi$*,*

(b) $y_\pm$ *is central in* G*.*

(iii) Let $\mathfrak{g} := P(R)$*, the Lie algebra of primitive elements of* R*. Then*

(a) $\sigma|_{\mathfrak{g}} \colon \mathfrak{g} \to \mathfrak{g} + k$ *is defined by, for* $x \in \mathfrak{g}$*,*

$$\sigma|_{\mathfrak{g}}(x) = x + \chi(x),$$

(b) $y_\pm$ *commutes with all elements of* $\mathfrak{g}$*.*

Proof. (i) Let $a \in R$ satisfy $\tau \circ \Delta(a) = \Delta(a)$. This implies that $\tau^l_{\chi^{\pm 1}}(a) = \tau^r_{\chi^{\pm 1}}(a)$. Therefore, Corollary 5.2.4 (ii) shows that

$$\mathrm{ad}_l(y_\pm)(a) = \tau^l_{\chi^{\pm 1}} \circ \tau^l_{\chi^{\mp 1}}(a) = a,$$

and hence $y_\pm$ commutes with a.

(ii) (a) By Theorem 5.2.3 (I), for all $g \in G$, $\sigma(g) = \chi(g)g$. Theorem 5.2.3 (L) shows that $\chi(y_\pm) = \xi$.

(b) Theorem 5.2.3 (A) and (B) show that $y_\pm$ is grouplike, and (i) shows that $y_\pm \in Z(G)$.

(iii) (a) If $x \in \mathfrak{g}$, then x is primitive, so Theorem 5.2.3 (I) shows that $\sigma(x) = x + \chi(x)$.

(b) This follows from (i). □

5.2.2 Examples

The following list of examples can be found in [22, §4]. In each case, R is a commutative algebra.

Examples 5.2.6. (i) $U(\mathfrak{sl}_2)$. Let $R = k[H]$, with Hopf structure given by requiring that H is primitive. Let $\sigma \colon R \to R$ be defined by $\sigma(H) = H - 1$, $\xi = y_\pm = 1$ and $h = H$. Then $A \cong U(\mathfrak{sl}_2)$.

(ii) $U_q(\mathfrak{sl}_2)$, where $q^2 \in k \setminus \{0, \pm 1\}$. Let $R = k[K^{\pm 1}]$, which has a Hopf structure given by requiring $K^{\pm 1}$ to be grouplike. Let $\sigma\colon R \to R$ be defined by $\sigma(K) = q^{-2}K$, let $\xi = q^{-2}$, let $h = (K^2 - 1)/(q - q^{-1})$ and let $y_\pm = K$. Then $A \cong U_q(\mathfrak{sl}_2)$ as Hopf algebras via $X_+ \mapsto E$, $X_- \mapsto FK$.

(iii) $U(\mathfrak{h}_3)$. Let $R = k[c]$, with Hopf structure given by requiring that c is primitive. Let $\sigma = \mathrm{id}_R\colon R \to R$, let $\xi = y_\pm = 1$ and let $h = c$. Then $A \cong U(\mathfrak{h}_3)$, the universal enveloping algebra of the three dimensional Heisenberg Lie algebra.

We now consider special cases of Theorem 5.2.3 obtained by imposing further conditions on R. We first consider the case when R is commutative, but after this we see the advantage of dropping the commutativity assumption for R, because we can take R to be a group algebra of a nonabelian group or an enveloping algebra of a nonabelian Lie algebra, for example. By Corollary 5.2.4, we only have to consider any further conditions on $y_\pm$ imposed by the structure of R and the resulting effect on (5.23).

R commutative

In this case, our result is an alternative presentation of [22, Theorem 3.1].

Proposition 5.2.7. *Let R be a commutative Hopf algebra, let $y_\pm \in G(R)$ and let $\chi\colon R \to k$ be central in $\mathrm{Alg}_k(R,k)$ with $\chi(y_+) = \chi(y_-)$. Then there is an ambiskew Hopf algebra $A := A(R, X_+, X_-, \sigma, \xi, h)$ extending the Hopf algebra structure of R such that (5.18) holds, with $\sigma := \tau^l_\chi$, $\xi := \chi(y_+)$ and $h \in P_{1,y_+y_-}(R)$. Furthermore, every ambiskew Hopf algebra extending the Hopf algebra structure of R with (5.18) arises in this way.*

Proof. Since R is commutative, $\mathrm{ad}_l(y_\pm) = \mathrm{id}$. Consequently, (5.23) holds if and only if $\chi(y_+) = \chi(y_-)$ and $\chi \in Z(\mathrm{Alg}_k(R,k))$. The result follows by Corollary 5.2.4. □

R cocommutative

Proposition 5.2.8. *Let R be a cocommutative Hopf algebra, let $y_\pm \in G(R) \cap Z(R)$, let $\chi\colon R \to k$ be an algebra homomorphism with $\chi(y_+) = \chi(y_-)$ and let either of the following hold:*

(i) $h \in k(1 - y_-y_+)$,

(ii) h is central in R and primitive, $\chi(y_+) = \pm 1$ and $y_+ = {y_-}^{-1}$.

Then there is an ambiskew Hopf algebra $A := A(R, X_+, X_-, \sigma, \xi, h)$ *extending the Hopf algebra structure of* R *such that* (5.18) *holds, with* $\sigma := \tau^l_\chi$ *and* $\xi := \chi(y_+)$*. Furthermore, every ambiskew Hopf algebra extending the Hopf algebra structure of* R *with* (5.18) *arises in this way.*

Proof. By Corollary 5.2.5 (i), for A to be a Hopf algebra, we must have $y_\pm \in Z(R)$, and so $\mathrm{ad}_l(y_\pm) = \mathrm{id}$. Then (5.23) holds if and only if $\chi(y_+) = \chi(y_-)$ and $\chi \in Z(\mathrm{Alg}_k(R, k)) = \mathrm{Alg}_k(R, k)$ by the fact that R is cocommutative. Corollary 5.2.4 shows that this defines an ambiskew Hopf algebra and that every ambiskew Hopf algebra with (5.18) arises in this way, with an arbitrary choice of $h \in P_{1,y_-y_+}(R) \cap Z(R)$. We now consider the structure of $P_{1,y_-y_+}(R)$.

Since R is a cocommutative Hopf algebra over the algebraically closed field k, R is pointed. To see this, let C be a simple subcoalgebra of R. Then C is finite-dimensional by [42, Corollary 5.1.2(1)], and its dual space C^* is a finite dimensional commutative k-algebra by [42, Lemma 1.2.2]. In addition, by [42, Lemma 5.1.4], C is a simple coalgebra if and only if C^* is a finite-dimensional commutative simple algebra. By the Artin-Wedderburn theorem [7, Theorem 3.2.2], $C^* \cong k$. Therefore, we also have $C \cong k$ and so C is one-dimensional.

Let $G := G(R)$ and let $g, h \in G$. It is easy to check that $k(g - h)$ is a vector subspace of $P_{g,h}(R)$; let $P'_{g,h}(R)$ denote its vector space complement. That is, $P_{g,h}(R) = k(g-h) \oplus P'_{g,h}(R)$. Since R is cocommutative, we have $P_{g,h} = P_{h,g}$ and hence also

$$P'_{g,h}(R) = P'_{h,g}(R) \tag{5.24}$$

for all $g, h \in G$.

Let $\{R_n : n \geq 0\}$ denote the coradical filtration of R. Then, by [50, Proposition 2],

$$R_1 = kG \oplus \bigoplus_{g,h \in G} P'_{g,h}(R).$$

This implies that $P'_{g,h}(R) \cap P'_{e,f}(R) = \{0\}$ unless $g = e$ and $h = f$. Consequently, (5.24) forces $P'_{g,h}(R) = \{0\}$ unless $g = h$, and so

$$P_{g,h}(R) = \begin{cases} k(g-h) & g \neq h, \\ P'_{g,h}(R) & g = h. \end{cases}$$

The above shows that there are two possible scenarios for P_{1,y_-y_+}, and hence for h:

(i) $h \in k(1 - y_-y_+)$,

(ii) $y_-y_+ = 1$, so h is primitive. In this case, $\chi(y_+y_-) = \chi(y_+)^2 = 1$. □

Remark. Examples 5.2.6 covers both possibilities for the choice of h in the above proposition. Examples (i) and (iii) are of the second type, while example (ii) is of the first type.

R a group algebra

Proposition 5.2.9. *Let G be a group and let $R := kG$. Let $y_\pm \in Z(G)$, let $\chi\colon G \to k$ be a character of G with $\chi(y_+) = \chi(y_-)$ and let $h \in k(1 - y_-y_+)$. Then there is an ambiskew Hopf algebra $A := A(R, X_+, X_-, \sigma, \xi, h)$ extending the Hopf algebra structure of R such that* (5.18) *holds, with $\sigma(g) := \chi(g)g$ for all $g \in G$ and $\xi := \chi(y_+)$. Furthermore, every ambiskew Hopf algebra extending the Hopf algebra structure of R with* (5.18) *arises in this way.*

Proof. This follows by Corollary 5.2.8, noting that by Corollary 5.2.5 (ii) $\sigma(g) = \chi(g)g$ for all $g \in G$. Clearly, $P_{1,y_-y_+}(R) = k(1 - y_-y_+)$ and this is a central subalgebra of R. □

R an enveloping algebra of a Lie algebra

Proposition 5.2.10. *Let $R = U(\mathfrak{g})$, for some Lie algebra $\mathfrak{g}$.*

(i) Let $y_\pm = 1$, let $\chi\colon U(\mathfrak{g}) \to k$ be a character of $U(\mathfrak{g})$ and let $h \in Z(\mathfrak{g})$. Then there is an ambiskew Hopf algebra $A := A(R, X_+, X_-, \sigma, \xi, h)$ extending the Hopf algebra structure of R such that (5.18) *holds, with $\sigma(x) := x + \chi(x)$ for all $x \in \mathfrak{g}$ and $\xi := 1$. Furthermore, every ambiskew Hopf algebra extending the Hopf algebra structure of R with* (5.18) *arises in this way.*

(ii) Suppose R has a Hopf structure that extends to a Hopf structure on A with (5.18). *Then $A \cong U(\mathfrak{h}_\chi)$, where $h_\chi := \mathfrak{g} \oplus kX_+ \oplus kX_-$ is a Lie algebra. Its Lie bracket restricted to $\mathfrak{g}$ is the same as the Lie bracket on $\mathfrak{g}$; we define, for all $x \in \mathfrak{g}$,*

$$[x, X_+] := -\chi(x)X_+,$$
$$[x, X_-] := \chi(x)X_-,$$
$$[X_+, X_-] := h.$$

Proof. (i) By [42, Example 5.1.6], 1 is the only grouplike in $U(\mathfrak{g})$, so we must have $y_\pm = 1$ for A to be a Hopf algebra. Clearly the condition $\chi(y_+) = \chi(y_-)$ holds. If

$x \in \mathfrak{g}$, then x is primitive, so Corollary 5.2.5 (iii) shows that $\sigma(x) = x + \chi(x)$. In addition, h is central in R and primitive and by [42, Proposition 5.5.3], the set of primitive elements of $U(\mathfrak{g})$ is $\mathfrak{g}$. The result follows by Corollary 5.2.8.

(ii) To see that h_χ is a Lie algebra, we only need to check that its Lie bracket as defined satisfies the Jacobi identity. However, the commutator bracket on any associative algebra satisfies this [40, §1.7.1]. Since A satisfies the same relations as $U(\mathfrak{h}_\chi)$, there is clearly an algebra epimorphism $\theta\colon U(\mathfrak{h}_\chi) \twoheadrightarrow A$. Moreover, $U(\mathfrak{h}_\chi)$ and A have the same vector space basis, and θ is bijective on the monomials forming the basis of $U(\mathfrak{h}_\chi)$. Therefore, θ is an isomorphism. □

R the quantised enveloping algebra of $\mathfrak{sl}_2$

In the cases where R is a cocommutative Hopf algebra, Proposition 5.2.8 shows that $y_\pm$ has to be central. A natural question is whether this must always be the case for any Hopf algebra R. In fact, the answer is no, as the case $R = U_q(\mathfrak{sl}_2)$ shows:

Example 5.2.11. Let $R = U_q(\mathfrak{sl}_2)$, where $q \in k \setminus \{0, 1\}$ and q is a primitive $4n$th root of unity for some $n > 1$. Here we have

$$G(R) \cap Z(R) = \{K^{2mn} \colon m \in \mathbb{Z}\}.$$

Define $\chi\colon R \to k$ by $\chi(E) := -1$, $\chi(F) := 1$ and $\chi(K) := -1$, and let $\sigma := \tau^l_\chi$. Then the Hopf algebra structure of R extends to a Hopf algebra structure on A with (5.18) by making the following definitions, where $y_\pm$ are not central. Set

- $y_+ := K^{mn}, y_- := K^{tn}$ for some odd integers m and t,
- $\xi := (-1)^{mn}$,
- $h \in k(1 - K^{(m+t)n})$.

5.3 Coradical filtration

In this section, we continue to suppose that R is a Hopf algebra and that the Hopf structure on R extends to a Hopf structure on A such that (5.18) holds. In the case when the coradical of R is a Hopf algebra, we investigate the coradical filtration of A, which we show depends on whether or not ξ is a root of unity.

5.3.1 Comultiplication formulas

Recall the definition of Gaussian binomial coefficients from §1.2.1. These coefficients occur in the image of the comultiplication map applied to powers of $X_\pm$, with $q := \xi^{\pm 1}$:

Lemma 5.3.1. *Let R have a Hopf algebra structure that extends to a Hopf algebra structure on A such that* (5.18) *holds. Then*

(i) for all $m \geq 0$,

$$\Delta({X_\pm}^m) = \sum_{j=0}^{m} \binom{m}{j}_{\xi^{\pm 1}} {y_\pm}^{m-j} {X_\pm}^j \otimes {X_\pm}^{m-j},$$

(ii) for all $m, n \geq 0$,

$$\Delta({X_+}^n {X_-}^m) = \sum_{j=0}^{n} \sum_{k=0}^{m} \binom{n}{j}_{\xi} \binom{m}{k}_{\xi^{-1}} \xi^{j(m-k)} \\ {y_+}^{n-j} {y_-}^{m-k} {X_+}^j {X_-}^k \otimes {X_+}^{n-j} {X_-}^{m-k}.$$

Proof. (i) Induction on m. The $m = 0$ case is obvious. For the induction step, if the formula holds for m, then

$$\begin{aligned}
\Delta({X_\pm}^{m+1}) &= \left(\sum_{j=0}^{m} \binom{m}{j}_{\xi^{\pm 1}} {y_\pm}^{m-j} {X_\pm}^j \otimes {X_\pm}^{m-j} \right) (y_\pm \otimes X_\pm + X_\pm \otimes 1) \\
&= \sum_{j=0}^{m} \binom{m}{j}_{\xi^{\pm 1}} ({y_\pm}^{m-j} \sigma^{\pm j}(y_\pm) {X_\pm}^j \otimes {X_\pm}^{m+1-j} + {y_\pm}^{m-j} {X_\pm}^{j+1} \otimes {X_\pm}^{m-j}) \\
&= {y_\pm}^{m+1} (1 \otimes {X_\pm}^{m+1}) \\
&\qquad + \sum_{j=1}^{m} \left(\binom{m}{j}_{\xi^{\pm 1}} \xi^{\pm j} + \binom{m}{j-1}_{\xi^{\pm 1}} \right) {y_\pm}^{m+1-j} {X_\pm}^j \otimes {X_\pm}^{m+1-j} \\
&\qquad\qquad + {X_\pm}^{m+1} \otimes 1 \\
&= \sum_{j=0}^{m+1} \binom{m+1}{j}_{\xi^{\pm 1}} {y_\pm}^{m+1-j} {X_\pm}^j \otimes {X_\pm}^{m+1-j},
\end{aligned}$$

as required, where the last equality uses (1.1).

(ii) By the previous part,

$$\begin{aligned}\Delta({X_+}^n {X_-}^m) &= \left(\sum_{j=0}^{n} \binom{n}{j}_{\xi} {y_+}^{n-j}{X_+}^j \otimes {X_+}^{n-j}\right) \\ &\qquad \cdot \left(\sum_{k=0}^{m} \binom{m}{k}_{\xi^{-1}} {y_-}^{m-k}{X_-}^k \otimes {X_-}^{m-k}\right) \\ &= \sum_{j=0}^{n}\sum_{k=0}^{m} \binom{n}{j}_{\xi}\binom{m}{k}_{\xi^{-1}} {y_+}^{n-j}\sigma^j({y_-}^{m-k}) \\ &\qquad {X_+}^j{X_-}^k \otimes {X_+}^{n-j}{X_-}^{m-k} \\ &= \sum_{j=0}^{n}\sum_{k=0}^{m} \binom{n}{j}_{\xi}\binom{m}{k}_{\xi^{-1}} \xi^{j(m-k)}{y_+}^{n-j}{y_-}^{m-k} \\ &\qquad {X_+}^j{X_-}^k \otimes {X_+}^{n-j}{X_-}^{m-k},\end{aligned}$$

as required. □

Suppose ξ is a primitive dth root of unity for some $d > 1$. For all non-negative integers m, we define non-negative integers q_m and r_m, with $0 \leq r_m \leq d-1$, by setting

$$m := dq_m + r_m.$$

If $\xi = 1$ or ξ is not a root of unity, for all non-negative integers m, set $q_m := m$ and $r_m := 0$.

Define a partial order $\prec$ on $\mathbb{Z}_{\geq 0}$ by $p \prec m$ if $q_p \leq q_m$ and $r_p \leq r_m$, for any $p, m \in \mathbb{Z}_{\geq 0}$. If $\xi = 1$ or ξ is not a non-trivial root of unity, then $p \prec m$ if and only if $p \leq m$, for all non-negative integers m and p.

Lemma 5.3.2. *Let R have a Hopf algebra structure that extends to a Hopf algebra structure on A such that* (5.18) *holds. Then*

(i) for all $m \geq 0$,

$$\Delta({X_\pm}^m) = \sum_{0 \leq p \prec m} \alpha_p {y_\pm}^{m-p}{X_\pm}^p \otimes {X_\pm}^{m-p},$$

where $\alpha_p \in k^*$ for all $p \prec m$,

(ii) for all $m, n \geq 0$,

$$\Delta({X_+}^n {X_-}^m) = \sum_{v \prec n}\sum_{p \prec m} \beta_{v,p} {y_+}^{n-v}{y_-}^{m-p}{X_+}^v{X_-}^p \otimes {X_+}^{n-v}{X_-}^{m-p},$$

where $\beta_{v,p} \in k^*$ for all $v \prec n$ and $p \prec m$.

Proof. (i) If $\xi = 1$ or ξ is not a non-trivial root of unity, then $p \prec m$ if and only if $0 \leq p \leq m$. Therefore, this is just Lemma 5.3.1 (i), with $\alpha_p := \binom{m}{p}_{\xi^{\pm 1}}$ for all $0 \leq p \leq m$. By the definition of Gaussian binomial coefficient, and with our hypothesis on ξ, it is easy to see that $\alpha_p \neq 0$ for all $p \prec m$.

Suppose now that ξ is a primitive dth root of unity. Using (1.2) we see that

$$\binom{d}{j}_{\xi^{\pm 1}} = 0, \qquad 0 < j < d.$$

Hence, the formula for $\Delta({X_\pm}^d)$ in Lemma 5.3.1 (i) becomes

$$\Delta({X_\pm}^d) = {y_\pm}^d \otimes {X_\pm}^d + {X_\pm}^d \otimes 1.$$

Furthermore, by Theorem 5.2.3 (L), $\sigma^{\pm 1}({y_\pm}^d) = \xi^{\pm d} {y_\pm}^d = {y_\pm}^d$, and so ${y_\pm}^d$ commutes with $X_\pm$. Therefore, for all integers $q \geq 0$,

$$\Delta({X_\pm}^d)^q = \sum_{i=0}^{q} \binom{q}{i} {y_\pm}^{d(q-i)} {X_\pm}^{di} \otimes {X_\pm}^{d(q-i)},$$

where $\binom{q}{i}$ denotes the ordinary binomial coefficient. Setting $m := dq_m + r_m$ and using the above equation together with Lemma 5.3.1 (i) gives

$$\begin{aligned}
\Delta({X_\pm}^m) &= \Delta({X_\pm}^d)^{q_m} \Delta({X_\pm}^{r_m}) \\
&= \left(\sum_{i=0}^{q_m} \binom{q_m}{i} {y_\pm}^{d(q_m-i)} {X_\pm}^{di} \otimes {X_\pm}^{d(q_m-i)} \right) \\
&\qquad \cdot \left(\sum_{j=0}^{r_m} \binom{r_m}{j}_{\xi^{\pm 1}} {y_\pm}^{r_m-j} {X_\pm}^{j} \otimes {X_\pm}^{r_m-j} \right) \\
&= \sum_{i=0}^{q_m} \sum_{j=0}^{r_m} \binom{q_m}{i} \binom{r_m}{j}_{\xi^{\pm 1}} {y_\pm}^{d(q_m-i)+r_m-j} {X_\pm}^{di+j} \otimes {X_\pm}^{d(q_m-i)+r_m-j} \\
&= \sum_{i=0}^{q_m} \sum_{j=0}^{r_m} \binom{q_m}{i} \binom{r_m}{j}_{\xi^{\pm 1}} {y_\pm}^{m-(di+j)} {X_\pm}^{di+j} \otimes {X_\pm}^{m-(di+j)} \\
&= \sum_{0 \leq p \prec m} \alpha_p {y_\pm}^{m-p} {X_\pm}^{p} \otimes {X_\pm}^{m-p},
\end{aligned}$$

where $\alpha_p := \binom{q_m}{i}\binom{r_m}{j}_{\xi^{\pm 1}}$ for $p := di + j$, with $0 \leq i \leq q_m$ and $0 \leq j \leq r_m \leq d-1$. By the fact that ξ is not a root of unity of order less than d, and by definition of the Gausssian binomial coefficients, $\binom{r_m}{j}_{\xi^{\pm 1}} \neq 0$ for all $0 \leq j \leq r_m \leq d-1$. Therefore, $\alpha_p \neq 0$, for all $p \prec m$.

(ii) Using (i), we have

$$\Delta({X_+}^n {X_-}^m) = \left(\sum_{v \prec n} \alpha_v {y_+}^{n-v} {X_+}^v \otimes {X_+}^{n-v}\right) \cdot \left(\sum_{p \prec m} \gamma_p {y_-}^{m-p} {X_-}^p \otimes {X_-}^{m-p}\right)$$
$$= \sum_{v \prec n} \sum_{p \prec m} \alpha_v \gamma_p \xi^{v(m-p)} {y_+}^{n-v} {y_-}^{m-p} {X_+}^v {X_-}^p \otimes {X_+}^{n-v} {X_-}^{m-p}$$
$$= \sum_{v \prec n} \sum_{p \prec m} \beta_{v,p} {y_+}^{n-v} {y_-}^{m-p} {X_+}^v {X_-}^p \otimes {X_+}^{n-v} {X_-}^{m-p},$$

where $\beta_{v,p} := \alpha_v \gamma_p \xi^{v(m-p)} \in k^*$, as required. □

5.3.2 The filtration

Let $\{R_q \colon q \geq 0\}$ denote the coradical filtration of R and let $\{A_t \colon t \geq 0\}$ denote the coradical filtration of A. We will calculate the coradical filtration of A in terms of the coradical filtration of R.

For all non-negative integers m, we continue the notation q_m, r_m and $\prec$ from the previous section. Set $\widehat{m} := q_m + r_m$. We need the following elementary lemma:

Lemma 5.3.3. *With the above notation, for all non-negative integers m, p with $p \prec m$, we have $\widehat{m-p} = \widehat{m} - \widehat{p}$.*

Proof. If $\xi = 1$ or ξ is not a non-trivial root of unity, then this is immediate. Suppose that ξ is a primitive dth root of unity for some $d > 1$. Then $m = q_m d + r_m$ and $p = q_p d + r_p$, where $0 \leq q_p \leq q_m$ and $0 \leq r_p \leq r_m \leq d-1$. Therefore, $m - p = (q_m - q_p)d + (r_m - r_p)$ where $0 \leq r_m - r_p \leq d-1$. Then

$$\widehat{m-p} = (q_m - q_p) + (r_m - r_p) = (q_m + r_m) - (q_p + r_p) = \widehat{m} - \widehat{p},$$

as required. □

Define a family $\{F_t \colon t \geq 0\}$ of subspaces of A by

$$F_t := \sum_{q + \widehat{m} + \widehat{n} \leq t} R_q {X_+}^m {X_-}^n.$$

Lemma 5.3.4. *Suppose that R_0 is a Hopf subalgebra of R. Then $\{F_t\}$ as defined above is a coalgebra filtration.*

Proof. It is clear that $F_t \subseteq F_{t+1}$ for all $t \geq 0$ and that $A = \bigcup_{t\geq 0} F_t$, so all that remains to be proven is that $\Delta(F_t) \subseteq \sum_{i=0}^{t} F_i \otimes F_{t-i}$. Let $rX_+{}^nX_-{}^m \in F_t$, where $r \in R_q$ and $q + \widehat{m} + \widehat{n} \leq t$. Lemma 5.3.2 (ii) shows that $\Delta(rX_+{}^nX_-{}^m)$ is a sum of terms of the form

$$\beta_{v,p} r_1 y_+{}^{n-v} y_-{}^{m-p} X_+{}^v X_-{}^p \otimes r_2 X_+{}^{n-v} X_-{}^{m-p}, \tag{5.25}$$

where $v \prec n$, $p \prec m$, $\beta_{v,p} \in k^*$. By definition of the coradical filtration of R, we have $\Delta(r) \in \sum_{j=0}^{q} R_j \otimes R_{q-j}$, so without loss of generality we can suppose that $r_1 \in R_j$ and $r_2 \in R_{q-j}$ for some $0 \leq j \leq q$. Also, since the coradical filtration of R is a Hopf algebra filtration by Lemma 1.1.5 and $y_\pm \in R_0$, we have $r_1 y_+{}^{n-v} y_-{}^{m-p} \in R_j$. Therefore, (5.25) is contained in $F_u \otimes F_w$, where $u = j + \widehat{v} + \widehat{p}$ and $w = q - j + \widehat{n-v} + \widehat{m-p}$. It is enough to show that $u + w \leq t$. We have, using Lemma 5.3.3,

$$\begin{aligned} u + w &= q + \widehat{v} + \widehat{p} + \widehat{n-v} + \widehat{m-p} \\ &= q + \widehat{v} + \widehat{p} + \widehat{n} - \widehat{v} + \widehat{m} - \widehat{p} \\ &= q + \widehat{n} + \widehat{m} \leq t, \end{aligned}$$

as required. $\square$

Theorem 5.3.5. *Let R have a Hopf algebra structure that extends to a Hopf algebra structure on A such that* (5.18) *holds and suppose that R_0 is a Hopf subalgebra of R. Then the coradical filtration of A is given by*

$$A_t = \sum_{q+\widehat{m}+\widehat{n}\leq t} R_q X_+{}^m X_-{}^n.$$

Proof. Let $\{A_t \colon t \geq 0\}$ denote the coradical filtration of A. As previously, let $\{F_t \colon t \geq 0\}$ denote the subspaces of A defined by

$$F_t := \sum_{q+\widehat{m}+\widehat{n}\leq t} R_q X_+{}^m X_-{}^n.$$

We must show that $F_t = A_t$ for all $t \geq 0$.

Firstly, we prove that $F_t \subseteq A_t$ for all $t \geq 0$ by an easy induction on t. We have $R_0 = A_0 \cap R$ by [42, Lemma 5.2.12]. Therefore, $F_0 = R_0 \subseteq A_0$. Now suppose that $F_t \subseteq A_t$

for some $t \geq 0$. Then, by induction and Lemma 5.3.4,

$$\begin{aligned}\Delta(F_{t+1}) &\subseteq \sum_{i=0}^{t+1} F_i \otimes F_{t+1-i} \\ &= \sum_{i=0}^{t} F_i \otimes F_{t+1-i} + F_{t+1} \otimes F_0 \\ &\subseteq F_t \otimes A + A \otimes F_0 \\ &\subseteq A_t \otimes A + A \otimes A_0,\end{aligned}$$

as required.

Secondly, we show that $A_t \subseteq F_t$ for all $t \geq 0$, again by induction on t. Lemma 5.3.4 shows that $\{F_t\}$ is a coalgebra filtration of A, so we may apply [42, Lemma 5.3.4], which proves the $t = 0$ case. Now suppose that $A_t \subseteq F_t$ for some $t \geq 0$; we will prove that $A_{t+1} \subseteq F_{t+1}$.

The formula in Lemma 5.3.2 shows that when the coproduct is applied to a member of the R-basis (5.3) of A of the form ${X_+}^m {X_-}^n$, the powers of X_+ and X_- on either side of the tensor sign add, respectively, to m and n. The fact that there is an $R \otimes R$-basis (5.4) of $A \otimes A$ means there is no cancellation of summands when the coproduct is applied to an R-linear combination of the basis (5.3) of A. Therefore, when proving $A_{t+1} \subseteq F_{t+1}$, it is enough to consider an R-multiple of a member of the basis (5.3) in A_{t+1} and prove that it is contained in F_{t+1}.

Let $r{X_+}^n {X_-}^m \in A_{t+1}$; without loss of generality we can suppose that $r \in R_q \setminus R_{q-1}$ for some $q \geq 0$ since $R = \bigcup_{q \geq 0} R_q$. Lemma 5.3.2 (ii), together with the definition of the coradical filtration and induction, gives

$$\begin{aligned}\Delta(r{X_+}^m {X_-}^n) &= \Delta(r) \sum_{v \prec n} \sum_{p \prec m} \beta_{v,p} {y_+}^{n-v} {y_-}^{m-p} {X_+}^v {X_-}^p \otimes {X_+}^{n-v} {X_-}^{m-p} \qquad (5.26) \\ &\in A_t \otimes A + A \otimes A_0 \subseteq F_t \otimes A + A \otimes F_0,\end{aligned}$$

where $\beta_{v,p} \in k^*$ for all $v \prec n$ and $p \prec m$. By definition of the coradical filtration of R, there is a summand $x \otimes z \in (R_q \setminus R_{q-1}) \otimes R_0$ of $\Delta(r)$. By (5.26), $\Delta(r{X_+}^m {X_-}^n)$ has summands

$$\sum_{v \prec n} \sum_{p \prec m} \beta_{v,p} x {y_+}^{n-v} {y_-}^{m-p} {X_+}^v {X_-}^p \otimes z {X_+}^{n-v} {X_-}^{m-p} \in F_t \otimes A + A \otimes F_0. \qquad (5.27)$$

A summand of (5.27) is contained in $A \otimes F_0$ if and only if $v = n$ and $p = m$; all other summands are contained in $F_t \otimes A$. By definition of F_t, we have

$$q + \widehat{v} + \widehat{p} \leq t, \qquad (5.28)$$

for all $v \prec n$ and $p \prec m$.

We must prove that $q + \widehat{m} + \widehat{n} \leq t + 1$, which we do by considering five cases. As previously, in the cases where ξ is a primitive dth root of unity for some $d > 1$, write $m := q_m d + r_m$ and $n := q_n d + r_n$, where $q_m, q_n \geq 0$ and $0 \leq r_m, r_n \leq d - 1$. In addition, if $m = n = 0$ then it is easy to see that $q \leq t + 1$. Therefore, we can suppose that at least one of m, n is non-zero; without loss of generality suppose $n \geq 1$.

(i) $\xi = 1$ or ξ is not a non-trivial root of unity. In this case, $\prec$ is the same as $\leq$ and we may drop the $\widehat{\ }$ notation. Consider the summand of (5.27) given by taking $v := n-1$ and $p := m$, which is contained in $F_t \otimes A$. Then (5.28) implies that $q+n-1+m \leq t$ and so we have $q + n + m \leq t + 1$.

(ii) ξ is a primitive dth root of unity for some $d > 1$ and $r_m = r_n = 0$. Therefore, $n = q_n d$ and $m = q_m d$ for some $q_n \geq 1$ and some $q_m \geq 0$. Consider the summand of (5.27) given by taking $v := (q_n - 1)d$ and $p := m$, which is contained in $F_t \otimes A$. Then $\widehat{v} = \widehat{n} - 1$, and by (5.28), $q + \widehat{n} - 1 + \widehat{m} \leq t$, as required.

(iii) ξ is a primitive dth root of unity for some $d > 1$ and $r_m = 0$ and $r_n \geq 1$. Consider the summand of (5.27) given by taking $v := n - 1$ and $p := m$, which is contained in $F_t \otimes A$. Then $\widehat{v} = \widehat{n} - 1$ and (5.28) gives $q + \widehat{n} - 1 + \widehat{m} \leq t$, as required.

(iv) ξ is a primitive dth root of unity for some $d > 1$ and $r_m \geq 1$ and $r_n = 0$. This is very similar to the previous case: consider $p := m - 1$, $v := n$.

(v) ξ is a primitive dth root of unity for some $d > 1$ and $r_m, r_n \geq 1$. This is similar to the previous two cases: consider $v := n - 1$ and $p := m$.

All cases show that $q + \widehat{m} + \widehat{n} \leq t + 1$, which implies that $A_{t+1} \subseteq F_{t+1}$ and completes the proof. □

Corollary 5.3.6. *Let R have a Hopf algebra structure that extends to a Hopf algebra structure on A such that (5.18) holds and suppose that R_0 is a Hopf subalgebra of R. Then*

$$A_1 = \begin{cases} R_1 \oplus R_0 X_\pm & \xi = 1 \text{ or } \xi \text{ not a root of 1} \\ R_1 \oplus R_0 X_\pm \oplus R_0 {X_\pm}^d & \xi \text{ a primitive } d\text{th root of 1.} \end{cases}$$

Proof. The case $\xi = 1$ or ξ is not a root of unity is immediate. Suppose that ξ is a primitive dth root of unity for $d > 1$ and let m be a non-negative integer with $m := q_m d + r_m$. Then

$\widehat{m} = q_m + r_m = 1$ if and only if either $q_m = 1$ and $r_m = 0$, or $q_m = 0$ and $r_m = 1$. This proves the root of unity case. □

Example 5.3.7. By Examples 5.2.6 (ii), for $q \in k \setminus \{0, \pm 1\}$, $A := U_q(\mathfrak{sl}_2)$ is an ambiskew Hopf algebra with (5.18), where $R := k[K^{\pm 1}]$, $X_+ := E$, $X_- := FK$ and $\xi := q^{-2}$. Since R is a group algebra, its coradical filtration is given by $R_n = R$ for all $n \geq 0$.

When q is not a root of unity, Theorem 5.3.5 gives the coradical filtration $\{A_t\}$ of $U_q(\mathfrak{sl}_2)$ as

$$\begin{aligned} A_t &= \sum_{m+n \leq t} R{X_+}^n {X_-}^m \\ &= \sum_{m+n \leq t} k[K^{\pm 1}] E^n (FK)^m \\ &= \sum_{m+n \leq t} k[K^{\pm 1}] E^n F^m. \end{aligned}$$

In other words, the coradical filtration is the filtration by degree, where we set $\deg(K) = 0$ and $\deg(E) = \deg(F) = 1$. Montgomery calculated the coradical filtration of $U_q(\mathfrak{sl}_2)$, when q is not a root of unity, in [43, Theorem 2.7].

When q is a non-trivial root of unity, Theorem 5.3.5 shows that the coradical filtration of $U_q(\mathfrak{sl}_2)$ depends upon the order of q^2. Let d be the order of q^2. Retaining our previous notation, the coradical filtration $\{A_t\}$ of $U_q(\mathfrak{sl}_2)$ is

$$\begin{aligned} A_t &= \sum_{\widehat{m}+\widehat{n} \leq t} R{X_+}^n {X_-}^m \\ &= \sum_{\widehat{m}+\widehat{n} \leq t} k[K^{\pm 1}] E^n (FK)^m \\ &= \sum_{\widehat{m}+\widehat{n} \leq t} k[K^{\pm 1}] E^n F^m. \end{aligned}$$

Boca calculated the coradical filtration of $U_q(\mathfrak{sl}_2)$ in [11] when q is a root of unity.

Corollary 5.3.8. *Suppose R is a Hopf algebra and the Hopf structure on R extends to a Hopf structure on A such that* (5.18) *holds. Then R is pointed if and only if A is pointed.*

Proof. Suppose A is pointed. Any simple subcoalgebra of R is a simple subcoalgebra of A, and is therefore one-dimensional. Hence, R is pointed.

Conversely, suppose R is pointed. Then by Theorem 5.3.5, $A_0 = R_0 = kG(R)$, so A is pointed. □

5.4 Properties of ambiskew polynomial algebras

We now consider a range of properties and determine under which conditions they hold for A.

5.4.1 Homological properties

We revisit many of the properties that were studied in Chapter 3 and consider whether A satisfies them.

Proposition 5.4.1. *(i) Let R be an affine algebra and A an ambiskew polynomial algebra over R. Then*

(a) R is right (left) noetherian if and only if A is right (left) noetherian.

(b) R is a domain if and only if A is a domain.

(c) If R is Auslander-Gorenstein, then so is A.

(ii) Suppose R is semiprime, noetherian and has a Hopf algebra structure that extends to a Hopf algebra structure on A such that (5.18) *holds. Then R has finite global dimension if and only if A does, and in this case* $\operatorname{gld} A = \operatorname{gld} R + 2$.

Proof. (i) (a) We prove this for right noetherian; the proof for left noetherian is almost identical. Let R be right noetherian. Then A is right noetherian by the skew-polynomial ring structure of A over R and [40, Theorem 1.2.9 (iv)]. Conversely, suppose A is right noetherian and let

$$I_1 \subset I_2 \subset \cdots$$

be an ascending chain of right ideals of R. Then

$$I_1 A \subset I_2 A \subset \cdots$$

is an ascending chain of right ideals of A, and so there exists an integer n such that $I_j A = I_{j+1} A$ for all $j \geq n$. Since A is a free left R-module, $I_j = I_{j+1}$ for all $j \geq n$ and hence R is right noetherian.

(b) The backwards direction is trivial and the forwards direction follows from the skew-polynomial ring structure of A over R and [40, Theorem 1.2.9 (i)].

(c) This follows from the skew-polynomial ring structure of A over R and [18, Theorem 4.2].

(ii) Suppose $\operatorname{gld} R < \infty$. Then $S := R[X_+;\sigma]$ is a Hopf subalgebra of A, $\operatorname{gld} S = \operatorname{gld} R+1$, by [40, Theorem 7.5.3 (iii)], and S is semiprime by [40, Proposition 7.9.14]. Now the trivial A-module k is also an S-module and $\operatorname{pd}_S k = \operatorname{gld} S = \operatorname{gld} R+1$. This is because $\operatorname{gld} H = \operatorname{pd}_H k$ for any Hopf algebra H; a proof of this can be found in [38, §2.4]. Therefore, [40, Corollary 7.9.18] shows that $\operatorname{gld} A = \operatorname{gld} S + 1 = \operatorname{gld} R + 2$.

Now suppose $\operatorname{gld} A < \infty$. Since A has basis $\{{X_+}^i {X_-}^j : i, j \geq 0\}$ as a right and left R-module,

$$A \cong \bigoplus_{i,j\geq 0} R{X_+}^i{X_-}^j = R \oplus \bigoplus_{\substack{i\geq 0, j\geq 0\\ i>0 \text{ or } j>0}} R{X_+}^i{X_-}^j$$

as an R-bimodule. Therefore, we can apply [40, Theorem 7.2.8 (i)], which gives

$$\operatorname{gld} R \leq \operatorname{gld} A + \operatorname{pd} A_R = \operatorname{gld} A,$$

where the last equality follows from the fact that A is a free right R-module. □

No example seems to be known at present of a noetherian Hopf algebra of finite global dimension that is not semiprime. The most striking positive case is for rings satisfying a polynomial identity (a property that we consider later, in §5.4.2) and is due to Wu and Zhang [52], incorporating results of Stafford and Zhang [48]. This enables us to deduce the following corollary:

Corollary 5.4.2. *Suppose R is noetherian, satisfies a polynomial identity, and has a Hopf algebra structure that extends to a Hopf algebra structure on A such that* (5.18) *holds. Then R has finite global dimension if and only if A does, and in this case* $\operatorname{gld} A = \operatorname{gld} R + 2$.

We now consider the Cohen-Macaulay and AS-Gorenstein properties. In order to prove these, we assume that R is a pointed Hopf algebra and its Hopf algebra structure extends to a Hopf algebra structure on A such that (5.18) holds.

Lemma 5.4.3. *With the above hypotheses, let $\{R_n : n \geq 0\}$ denote the coradical filtration of R and let* $\operatorname{gr} R := \bigoplus_{n\geq 0} \overline{R}_n$ *denote the associated graded algebra of R with respect to this filtration. Then*

(i) (a) $\sigma(R_n) = R_n$ for all $n \geq 0$,

(b) σ induces an algebra automorphism $\overline{\sigma}$ of $\operatorname{gr} R$ *with $\overline{\sigma}(\overline{R}_n) = \overline{R}_n$ for all $n \geq 0$,*

(ii) (a) $R[X_+;\sigma]$ has a Hopf algebra filtration $\{E_n : n \geq 0\}$, defined by

$$E_n := \sum_{i+j\leq n} R_i {X_+}^j,$$

(b) *Let S denote the associated graded Hopf algebra of $R[X_+;\sigma]$ with respect to the above filtration. Then $S \cong (\mathrm{gr}\, R)[X_+;\overline{\sigma}]$,*

(iii) (a) *A has a Hopf algebra filtration $\{F_n : n \geq 0\}$ defined by*

$$F_n := \sum_{i+j\leq n} E_i X_-{}^j,$$

(b) *Let T denote the associated graded Hopf algebra of A with respect to the above filtration and extend $\overline{\sigma}$ to an automorphism of S by defining $\overline{\sigma}(X_+) := \xi X_+$. Then $T \cong S[X_-;\overline{\sigma}^{-1}]$.*

Proof. (i) (a) By the definition of the coradical filtration and Theorem 5.2.3 (I), $\sigma(R_n) \subseteq R_n$, and $\sigma^{-1}(R_n) \subseteq R_n$ for all $n \geq 0$. Applying σ to the second inclusion gives $R_n \subseteq \sigma(R_n)$, so $\sigma(R_n) = R_n$.

(b) Let $r \in R_n$ and define $\overline{\sigma}(r + R_{n-1}) := \sigma(r) + R_{n-1}$. By part (a), $\overline{\sigma}$ is well-defined and bijective. It is an algebra homomorphism because it is induced by the algebra homomorphism σ.

(ii) (a) Note that $\{R_n\}$ is a Hopf algebra filtration of R by Lemma 1.1.5. Together with (i)(a), this shows that $\{E_n\}$ is an algebra filtration of $R[X_+;\sigma]$. Furthermore, by (5.18), $\Delta(X_+) \in E_1 \otimes E_0 + E_0 \otimes E_1$. Since $\{E_n\}$ is an algebra filtration and $R[X_+;\sigma]$ is generated by R and X_+, this proves $\{E_n\}$ is a coalgebra filtration. Similarly, by Theorem 5.2.3 (E), $\{E_n\}$ is a Hopf algebra filtration.

(b) $\mathrm{gr}\, R$ is a Hopf algebra, and so is $(\mathrm{gr}\, R)[X_+;\sigma]$ when we set $\Delta(X_+) := X_+ \otimes 1 + y_+ \otimes X_+$, where $y_+ \in \overline{R}_0$ is grouplike. (This can be seen by replacing R and σ with $\mathrm{gr}\, R$ and $\overline{\sigma}$ in Theorem 5.2.3 and taking the Hopf subalgebra generated by $\mathrm{gr}\, R$ and X_+.) Furthermore, $(\mathrm{gr}\, R)[X_+;\sigma] := \bigoplus_{n\geq 0} \overline{V}_n$ is a graded Hopf algebra, where $\overline{V}_n := \sum_{i+j=n} \overline{R}_i X_+{}^j$ for $n \geq 0$. Let $S = \bigoplus_{n\geq 0} \overline{E}_n$, where $\overline{E}_0 = E_0$ and $\overline{E}_n := E_n/E_{n-1}$ for $n \geq 1$. The isomorphism follows by identifying $\overline{E}_n$ with $\overline{V}_n$.

(iii) (a) By (ii)(a), $\{E_n\}$ is a Hopf algebra filtration. Together with (i)(a) and the definition $\sigma^{-1}(X_+) := \xi^{-1} X_+$, which shows that $\sigma^{-1}(E_i X_-{}^j) = E_i X_-{}^j$ for all $i, j \geq 0$, we see that $\{F_n\}$ is an algebra filtration. It is easy to see it is a coalgebra filtration using (5.18) and a Hopf algebra filtration using Theorem 5.2.3 (E).

(b) Setting (5.18) makes $S[X_-;\overline{\sigma}^{-1}]$ into a Hopf algebra (use Theorem 5.2.3, replacing R, σ and h with $\operatorname{gr} R$, $\overline{\sigma}$ and 0). Similarly to (ii)(b), we can give $S[X_-;\overline{\sigma}^{-1}]$ the obvious Hopf algebra grading and identify it with T. Note that the relation (5.2) in A becomes $X_+X_- = \xi X_-X_+$ in T, because with respect to the filtration $\{F_n\}$, the degree of h is 0 or 1 whereas the degree of X_+X_- and ξX_-X_+ is 2. □

If R is Cohen-Macaulay, or is AS-Gorenstein, we would like to be able to establish whether or not A satisfies these properties. However, the Cohen-Macaulay property involves GK-dimension, which in general does not behave well with respect to general skew-polynomial algebras: note that Proposition 3.2.10 only applies to skew-polynomial algebras where the automorphism is locally algebraic and the derivation map is zero. [40, Example 8.2.6] shows that this fails when the locally algebraic hypothesis is removed; there are also examples of skew-polynomial algebras $S[X;\mathrm{id},\delta]$ where $\operatorname{GKdim}(S) = 0$ and $\operatorname{GKdim}(S[X;\mathrm{id},\delta]) = \infty$ [33, §3.9]. In addition, Lemma 3.2.17 only applies to skew-polynomial algebras over connected graded algebras.

Therefore, we need to impose further conditions on R. We now assume that $\operatorname{gr} R$ is of the type we encountered in Chapter 3 - that is, that $G := G(R)$ is a finitely generated abelian group acting diagonalisably on its subalgebra of coinvariants and that $\operatorname{gr} R$ has a finite number of hard superletters.

Proposition 5.4.4. *Let R be a pointed Hopf algebra with the above assumptions on* $\operatorname{gr} R$ *and suppose that the Hopf algebra structure on R extends to a Hopf algebra structure on A such that* (5.18) *holds. Then*

(i) A is Cohen-Macaulay.

(ii) A is AS-Gorenstein, and is AS-regular if and only if R has finite global dimension.

Proof. (i) By Lemma 5.4.3 (iii)(a) and (b), when A is given the filtration $\{F_n : n \geq 0\}$, its associated graded Hopf algebra algebra T is isomorphic to $(\operatorname{gr} R)[X_+;\overline{\sigma}][X_-;\overline{\sigma}^{-1}]$. By our assumptions, $\operatorname{gr} R$ is a Hopf algebra of the same form as H in §2.3. In fact, this means that so is $(\operatorname{gr} R)[X_+;\overline{\sigma}][X_-;\overline{\sigma}^{-1}]$: we associate $X_\pm$ to $y_\pm \in G$ and $\chi^{X_\pm} := \chi^{\pm 1}|_G : G \to k$, where $\sigma = \tau^l_\chi$. It is clear that (2.11) holds for $X_\pm$, since Corollary 5.2.5 (ii)(a) shows that $\overline{\sigma}^{\pm 1}(g) = \sigma^{\pm 1}(g) = \chi^{X_\pm}(g)g$ for all $g \in G$. Let $\mathcal{B}$ denote the PBW-basis of $\operatorname{gr} R$. Then a PBW-basis for $(\operatorname{gr} R)[X_+;\overline{\sigma}][X_-;\overline{\sigma}^{-1}]$ is given by the set $\{b{X_+}^i{X_-}^j : b \in \mathcal{B},\ i, j \geq 0\}$, since $X_\pm$ are clearly hard super-letters and there are no others. Hence, since $\operatorname{gr} R$ has a finite number of PBW-generators, then so does $(\operatorname{gr} R)[X_+; \overline{\sigma}][X_-; \overline{\sigma}^{-1}]$, which is isomorphic to T. Therefore, by Proposition 3.2.20, T is Cohen-Macaulay and [25, Theorem 1.2] shows that A is Cohen-Macaulay.

(ii) This follows by our assumptions, part (i), and Proposition 3.2.23. The AS-regularity part is clear from Proposition 5.4.1 (ii). □

5.4.2 Polynomial identity

We finish by looking at a ring-theoretic property: the question of when an ambiskew algebra A satisfies a polynomial identity. Surprisingly, this does not seem to have been considered in the literature. No Hopf algebra assumptions are used in this section.

Definition 5.4.5. Let S be a ring. Then S is a *polynomial identity ring* (*P.I. ring*) if there is a monic polynomial $f(X_1, \dots, X_n) \in \mathbb{Z} < X_1, \dots, X_n >$ such that $f(s_1, \dots, s_n) = 0$ for all $s_1, \dots, s_n \in R$. The *P.I. degree* of S is the least possible degree of any such polynomial f.

Suppose $\sigma\colon R \to R$ has finite order $n \geq 1$. Then it is diagonalisable and its eigenvalues are the nth roots of unity. Hence, as a vector space, R is a direct sum of its eigenspaces. That is, for η a primitive nth root of unity,

$$R = \bigoplus_{i=0}^{n-1} R_i,$$

where $R_i = \{r \in R\colon \sigma(r) = \eta^i r\}$. In fact, this decomposition is a $k\langle\sigma\rangle$-module decomposition. Since $h \in R$, we have

$$h = \sum_{k=0}^{n-1} h_k, \tag{5.29}$$

where $h_k \in R_k$ for all $0 \leq k \leq n-1$.

Suppose that ξ is a tth root of unity for some $t \geq 1$, where $t|n$. Since ξ is then an nth root of unity,

$$\xi = \eta^j \tag{5.30}$$

for some η a primitive nth root of unity and $0 \leq j \leq n-1$.

We have a basic lemma about the relations in A:

Lemma 5.4.6. *Let $A = A(R, X_+, X_-, \sigma, h, \xi)$ be an ambiskew algebra.*

(i) For $n \geq 1$,

$$X_+{}^n X_- = \xi^n X_- X_+{}^n + \left(\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) \right) X_+{}^{n-1}.$$

(ii) For $n \geq 1$,

$$X_-{}^n X_+ = \xi^{-n} X_+ X_-{}^n - \left(\sum_{i=1}^{n} \xi^{-i} \sigma^{-(n-i)}(h) \right) X_-{}^{n-1}.$$

(iii) $X_+{}^n$ *is central in* A *if and only if* $X_-{}^n$ *is central in* A.

(iv) Suppose σ *has order* $n \geq 1$ *and* ξ *is a root of unity in* k *with order* r *for some* $r > 1$, *where* r *does not divide* n. *Let* m *be the least common multiple of* n *and* r. *Then* $X_+{}^m$ *and* $X_-{}^m$ *are central in* A.

(v) Suppose σ *has order* $n \geq 1$ *and* ξ *is a root of unity in* k *that has order* r *for some* $r > 1$, *where* r *divides* n. *Then* $X_+{}^n$ *and* $X_-{}^n$ *are central in* A *if and only if* $h_j = 0$, *where* j *is as in* (5.30) *and* h_j *is as in* (5.29).

Proof. (i) The formula clearly holds for $n = 1$. Now, suppose it holds up to $n-1$. Then

$$\begin{aligned} X_+{}^n X_- &= X_+ \left(\xi^{n-1} X_- X_+{}^{n-1} + \left(\sum_{i=0}^{n-2} \xi^{n-i-2} \sigma^i(h) \right) X_+{}^{n-2} \right) \\ &= \xi^{n-1} X_+ X_- X_+{}^{n-1} + \left(\sum_{i=0}^{n-2} \xi^{n-i-2} \sigma^{i+1}(h) \right) X_+{}^{n-1} \\ &= \xi^{n-1} (\xi X_- X_+ + h) X_+{}^{n-1} + \left(\sum_{i=1}^{n-1} \xi^{n-i-1} \sigma^i(h) \right) X_+{}^{n-1} \\ &= \xi^n X_- X_+{}^n + \left(\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) X_+{}^{n-1} \right), \end{aligned}$$

as required.

(ii) Similar to (i).

(iii) This follows immediately from parts (i) and (ii) and the fact that

$$\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) = \xi^{n-1} \sigma^n \left(\sum_{i=1}^{n} \xi^{-i} \sigma^{-(n-i)}(h) \right).$$

(iv) Clearly, $X_+{}^m$ commutes with X_+ and with elements of R. Let $m = pn$ for some positive integer p. Using part (i), we see that

$$\begin{aligned}
{X_+}^m X_- &= \xi^m X_- {X_+}^m + \left(\sum_{i=0}^{m-1} \xi^{m-i-1} \sigma^i(h) \right) {X_+}^{m-1} \\
&= X_- {X_+}^m + \left(\sum_{i=0}^{n-1} \sum_{j=1}^{p} \xi^{nj-i-1} \sigma^i(h) \right) {X_+}^{m-1} \qquad (5.31) \\
&= X_- {X_+}^m + \left(\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) \sum_{j=1}^{p} \xi^{n(j-1)} \right) {X_+}^{m-1} \\
&= X_- {X_+}^m + \left(\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) \sum_{j=0}^{p-1} (\xi^n)^j \right) {X_+}^{m-1} \\
&= X_- {X_+}^m, \qquad (5.32)
\end{aligned}$$

where (5.31) follows from the fact that the order of σ is n, and (5.32) follows from the fact that

$$\sum_{j=0}^{p-1} (\xi^n)^j = 0,$$

since ξ^n is a primitive pth root of unity. Therefore, ${X_+}^m$ commutes with X_- and so is central in A. By part (iii), ${X_-}^m$ is also central in A.

(v) By part (i), since $\xi^n = 1$, we have

$${X_+}^n X_- = X_- {X_+}^n + \left(\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) \right) {X_+}^{n-1}.$$

Consider the coefficient of the ${X_+}^{n-1}$ in the above equation. We have

$$\begin{aligned}
\sum_{i=0}^{n-1} \xi^{n-i-1} \sigma^i(h) &= \xi^{n-1} \sum_{i=0}^{n-1} \xi^{-i} \sum_{k=0}^{n-1} \sigma^i(h_k) \\
&= \xi^{n-1} \sum_{i=0}^{n-1} \xi^{-i} \sum_{k=0}^{n-1} \eta^{ik} h_k \\
&= \xi^{n-1} \sum_{i=0}^{n-1} \eta^{-ij} \sum_{k=0}^{n-1} \eta^{ik} h_k \\
&= \xi^{n-1} \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} \left(\eta^{(k-j)}\right)^i h_k,
\end{aligned}$$

and ${X_+}^n$ is central if and only if this is zero. Equivalently, ${X_+}^n$ is central if and only if, for all $0 \le k \le n-1$, either $h_k = 0$ or

$$\sum_{i=0}^{n-1} \left(\eta^{(k-j)}\right)^i = 0. \qquad (5.33)$$

Since η is a primitive nth root of unity, so is η^{k-j} for all $k \neq j$. Therefore, (5.33) holds for all $k \neq j$; for $k = j$, the left hand side of (5.33) is $n \neq 0$. Therefore, ${X_+}^n$ is central if and only if $h_j = 0$. The same is true for ${X_-}^n$ because by part (iii) ${X_-}^n$ is central if and only if ${X_+}^n$ is central. $\square$

Remark. A simple example illustrating part (v) of the above lemma is as follows. Set $R := k[Y]$, $\sigma(Y) := -Y$ and $\xi := -1$. Then σ and ξ both have order 2, $\xi = \eta$ and the eigenspace decomposition of R in (5.30) is $R := R_0 \oplus R_1$, where $R_0 = k[Y^2]$ and R_1 has basis consisting of the monomials in Y of odd degree. Part (i) of the lemma shows that

$${X_+}^2 X_- = X_+ {X_-}^2 + (-h + \sigma(h))X_+.$$

It is easy to see that ${X_+}^2$ is central if and only if $h_1 = 0$; for example, setting $h := Y$ gives

$${X_+}^2 X_- = X_+ {X_-}^2 - 2YX_+.$$

We also have the following lemma:

Lemma 5.4.7. *Let R be commutative and suppose that σ has order $n \geq 1$. Then R is a finitely generated module over R^σ.*

Proof. We first show, by a well-known argument from invariant theory, that R is integral over R^σ. Let $x \in R$ and let

$$f(X) = \prod_{i=0}^{n-1} (X - \sigma^i(x)). \tag{5.34}$$

Then $f(x) = 0$, since (5.34) evaluated at x has a factor $x - \sigma^0(x) = 0$. Also, (5.34) is a polynomial of the form

$$f(X) = X^n + c_{n-1}X^{n-1} + \ldots + c_0,$$

where, for $0 \leq j \leq n-1$, the c_j are symmetric polynomials in the σ-invariant set $\{\sigma^i(x) \colon 0 \leq i \leq n-1\}$. Since c_j is symmetric, it is invariant under the action of σ, so $c_j \in R^\sigma$, as required.

We have that R is an affine k-algebra, so it is certainly an affine R^σ-algebra. We can therefore apply [30, Proposition 16.3 B], which proves that R is a finitely generated R^σ-module. $\square$

In order to determine when A satisfies a polynomial identity, we make use of the following theorem, which is originally due to Jøndrup [27]. Note that an *inner derivation* of a ring S is a derivation $\delta\colon S \to S$ such that there exists some $a \in S$ with $\delta(s) = sa - as$ for all $s \in S$. Recall that a prime P.I. ring S is (right and left) Goldie, by Posner's Theorem [40, Theorem 13.6.5], and so possesses a simple artinian classical ring of quotients, $\mathrm{Fract}(S)$, by [20, Theorem 6.18].

Theorem 5.4.8. *[13, Theorem I.4.1] Let S be a prime P.I. algebra over a field of characteristic 0 and let $T := S[X, \tau, \delta]$ be a skew-polynomial ring, with τ an automorphism of S. Then*

(i) If $\tau|_{Z(S)} = \mathrm{id}$, then there exists a unit $u \in$ Fract(S) such that τ is the map given by conjugation by u, and T is P.I. if and only if

$$u\delta \text{ is an inner derivation on Fract}(S). \tag{5.35}$$

(ii) If $\tau|_{Z(S)} \neq \mathrm{id}$, then T is P.I. if and only if

$$\tau^n|_{Z(S)} = \mathrm{id} \tag{5.36}$$

for some $n > 1$.

Another theorem of Jøndrup determines the P.I. degree of certain skew-polynomial rings over P.I. rings.

Theorem 5.4.9. *[26] Let k be an algebraically closed field of characteristic 0. Let R be a prime affine k-algebra of P.I. degree d, let σ be an automorphism of R of finite order and let δ be a σ-derivation. Then if the skew-polynomial ring $R[X, \sigma, \delta]$ is a P.I. ring, its P.I. degree is equal to dl, where l is the order of the restriction of σ to $Z(R)$.*

We can now consider the conditions under which A is a P.I. ring in the special case where R is a commutative domain. In the commutative setting, being prime is the same as being a domain.

Theorem 5.4.10. *Suppose R is a commutative domain. Then the following are equivalent:*

(i) A is P.I.

(ii) A is a finite module over its centre.

(iii) The following conditions hold:

(a) $\sigma|_R$ has finite order $n \geq 1$;

(b) ξ has finite order $t \geq 1$;

(c) if $t|n$, then $h_j = 0$, where j is as in (5.30) and h_j is as in (5.29).

Proof. (ii) $\Rightarrow$ (i): [40, Corollary 13.1.13(i)].

(i) $\Rightarrow$ (iii): Suppose (i) holds. Then $R[X_+, \sigma]$ is a P.I. skew polynomial ring over R, so Theorem 5.4.8 tells us that $\sigma\colon R \to R$ has finite order $n \geq 1$. We therefore have

$$R^\sigma[{X_+}^n] \subseteq Z(R[X_+, \sigma]),$$

and in fact this is an equality. For, suppose $f = \sum_{i=0}^m r_i {X_+}^i \in Z(R[X_+, \sigma])$. Then, for all $r \in R$,

$$\sum_{i=0}^m r r_i {X_+}^i = rf = fr = \sum_{i=0}^m r_i \sigma^i(r) {X_+}^i,$$

and, since R is a domain, we have either $r_i = 0$ or $\sigma^i = \mathrm{id}$. Therefore, $r_i \neq 0$ only if $i = np$ for some $p \geq 0$. Furthermore,

$$\sum_{i=0}^m \sigma(r_i) {X_+}^{i+1} = X_+ f = f X_+ = \sum_{i=0}^m r_i {X_+}^{i+1},$$

and so $r_i \in R^\sigma$, which gives $f \in R^\sigma[{X_+}^n]$. So we have

$$R^\sigma[{X_+}^n] = Z(R[X_+, \sigma]) \tag{5.37}$$

Since A is P.I., a second application of Theorem 5.4.8, this time taking $S = R[X_+, \sigma]$ and $\tau = \sigma^{-1}$, shows that one of the following conditions must hold: either

$$\sigma^{-1}|_{R^\sigma[{X_+}^n]} = \mathrm{id}, \text{ and } \delta \text{ satisfies (5.35)} \tag{5.38}$$

or

$$\sigma^{-1}|_{R^\sigma[{X_+}^n]} \text{ has finite order } p > 1. \tag{5.39}$$

If (5.38) holds, then

$$\sigma^{-1}({X_+}^n) = \xi^{-n} {X_+}^n = {X_+}^n,$$

so ξ has finite order t for some $t \geq 1$, where t divides n. Furthermore, there exists a unit $u \in \mathrm{Fract}R[X_+, \sigma]$ such that $u\delta$ is an inner derivation on $\mathrm{Fract}R[X_+, \sigma]$. We have

$$R^\sigma[{X_+}^n] \hookrightarrow \mathrm{Fract}R^\sigma[{X_+}^n] \hookrightarrow \mathrm{Fract}R[{X_+}^n].$$

Since $R^\sigma[{X_+}^n]$ is central in $\mathrm{Fract}R[{X_+}^n]$, its only inner derivation is the zero map. Hence $u\delta$ is zero on $R^\sigma[{X_+}^n]$, and in particular $u\delta({X_+}^n) = 0$. Therefore, $\delta({X_+}^n) = 0$. By Lemma 5.4.6 (v), we have $h_j = 0$.

If (5.39) holds, then

$$\sigma^{-p}({X_+}^n) = \xi^{-np}{X_+}^n = {X_+}^n,$$

and so ξ has finite order $t \geq 1$, where t divides np. However, the fact that $\sigma^{-1}|_{R^\sigma[X_+]} \neq \mathrm{id}$ means that $t \nmid n$.

(iii) $\Rightarrow$ (ii): Suppose (iii) holds. Then R^σ is central in A. Suppose $t \nmid n$, so by Lemma 5.4.6 (iv), ${X_+}^m$ is central in A, where $m = \text{g.c.d.}(n, t)$. Hence, by Lemma 5.4.6 (iii), so is ${X_-}^m$ and the centre of A is

$$Z(A) := R^\sigma[{X_+}^m, {X_-}^m].$$

Clearly, A is finitely generated over $R[{X_+}^m, {X_-}^m]$, with generators

$$\{{X_+}^i{X_-}^j : 0 \leq i, j \leq m\},$$

and by Lemma 5.4.7, $R[{X_+}^m, {X_-}^m]$ is finitely generated over $Z(A)$. Hence, (ii) holds in this case.

Now suppose $t|n$. By hypothesis, $h_j = 0$, so ${X_\pm}^n$ are central in A. Therefore, the centre of A is

$$Z(A) := R^\sigma[{X_+}^n, {X_-}^n],$$

and, as in the case where $t \nmid n$, A is a finitely generated module over $Z(A)$, so (ii) holds. □

Corollary 5.4.11. *Let R be a commutative domain and suppose A is P.I.. Then the P.I. degree of A is $2mn$, where σ has order $n \geq 1$, ξ has order $t \geq 1$, and $m = l.c.m.(n, t)$.*

Proof. We have, as can be seen in the proof of Theorem 5.4.10,

$$R^\sigma[X_+^n, \sigma] = Z(R[X_+, \sigma]).$$

R has P.I. degree 2, and $R[X_+; \sigma]$ has P.I. degree $2n$ by Corollary 5.4.9. A second application of Corollary 5.4.9 shows that the P.I. degree of A is $2mn$. □

Remarks. (i) (a) Let S be a left or right noetherian ring. Then $N(S)$, the prime radical of S, is a nilpotent ideal [20, Theorem 3.11], and S is a P.I. ring if and only if the factor ring $S/N(S)$ is a P.I. ring [40, Lemma 13.1.7].

(b) Let $A := A(R, X_+, X_-, \sigma, \xi, h)$ and suppose that R is left or right noetherian. Let $N := N(R)$. For all prime ideals P of R, $\sigma^{\pm 1}(P)$ is a prime ideal of R and so is contained in N. Therefore, $\sigma(N) = N$. Furthermore, NA is a left ideal of

A; by (5.1), it is a two-sided ideal of A. Let $\overline{A} := \overline{A}(\overline{R}, X_+, X_-, \overline{\sigma}, \xi, \overline{h})$ be the ambiskew polynomial algebra with ambiskew data as follows: $\overline{R} := R/N$, $\overline{\sigma}$ is the automorphism of R/N induced by σ and $\overline{h} := h + N$. Then $A/NA \cong \overline{A}$ and NA is nilpotent. In fact, since $\overline{A}$ is an iterated skew-polynomial ring over a semiprime right or left noetherian ring, it is semiprime [40, Proposition 7.9.14] and so $N(A) = NA$.

(ii) By (i)(a) and (i)(b), for an ambiskew algebra A over a left or right noetherian ring R, obtaining necessary and sufficient conditions for $\overline{A}$ to be P.I. also gives necessary and sufficient conditions for A to be P.I., so we may reduce to the case where R is semiprime. That is, if we could prove an analogue of Theorem 5.4.10 for left or right noetherian semiprime rings, we would have the complete picture in the case when R is left or right noetherian.

(iii) For a noetherian semiprime ring R, a partial answer to this question can be deduced from [35, Proposition 3.2, Theorem 3.7]. Let $S := R[X_+; \sigma]$. These results show that A is P.I. if and only if R is P.I., $\sigma|_{Z(R)}$ has finite order and the centre of A contains a non-constant polynomial in X_- with coefficients in S and with regular leading coefficient. However, this last condition is very abstract and it is not clear how to state it explicitly in terms of conditions upon σ, ξ and h. With further work, it may be possible to produce an analogue of Theorem 5.4.10 in this setting.

References

[1] K. Ajitabh, S. P. Smith, and J. J. Zhang. Injective resolutions of some regular rings. *J. Pure Appl. Algebra*, 140(1):1–21, 1999.

[2] N. Andruskiewitsch and H.-J. Schneider. Pointed Hopf algebras. *Mathematical Research Institute Publications*, 43:1–68, 2002.

[3] Nicolás Andruskiewitsch and Hans-Jürgen Schneider. Finite quantum groups and Cartan matrices. *Adv. Math.*, 154(1):1–45, 2000.

[4] Konstantin Ardakov and Kenneth A. Brown. Primeness, semiprimeness and localisation in Iwasawa algebras. *Trans. Amer. Math. Soc.*, 359(4):1499–1515 (electronic), 2007.

[5] Hyman Bass. On the ubiquity of Gorenstein rings. *Math. Z.*, 82:8–28, 1963.

[6] V. V. Bavula. Generalized Weyl algebras and their representations. *Algebra i Analiz*, 4(1):75–97, 1992.

[7] John A. Beachy. *Introductory lectures on rings and modules*, volume 47 of *London Mathematical Society student texts.* Cambridge University Press, Cambridge, 1999.

[8] Georgia Benkart and Tom Roby. Down-up algebras. *J. Algebra*, 209(1):305–344, 1998.

[9] J.-E. Björk. *Rings of differential operators*, volume 21 of *North-Holland Mathematical Library.* North-Holland Publishing Co., Amsterdam, 1979.

[10] Jan-Erik Björk. The Auslander condition on Noetherian rings. In *Séminaire d'Algèbre Paul Dubreil et Marie-Paul Malliavin, 39ème Année (Paris, 1987/1988)*, volume 1404 of *Lecture Notes in Math.*, pages 137–173. Springer, Berlin, 1989.

[11] Ioana Boca. The coradical filtration of $U_q(\mathfrak{sl}_2)$ at roots of unity. *Comm. Algebra*, 22(14):5769–5776, 1994.

[12] K. A. Brown and J. J. Zhang. Dualising complexes and twisted Hochschild (co)homology for Noetherian Hopf algebras. *J. Algebra*, 320(5):1814–1850, 2008.

[13] K.A. Brown and K.R. Goodearl. *Lectures on algebraic quantum groups.* Advanced courses in mathematics, CRM Barcelona. Birkhaüser, Basel; Boston, 2002.

[14] Kenneth A. Brown. Noetherian Hopf algebras. *Turkish J. Math.*, 31(suppl.):7–23, 2007.

[15] John Clark. Auslander-Gorenstein rings for beginners. In *International Symposium on Ring Theory (Kyongju, 1999)*, Trends Math., pages 95–115. Birkhäuser Boston, Boston, MA, 2001.

[16] C. De Concini and C. Procesi. Quantum groups. In *D-modules, representation theory, and quantum groups (Venice, 1992)*, volume 1565 of *Lecture Notes in Math.*, pages 31–140. Springer, Berlin, 1993.

[17] V. G. Drinfel′d. Hopf algebras and the quantum Yang-Baxter equation. *Dokl. Akad. Nauk SSSR*, 283(5):1060–1064, 1985.

[18] Eva Kristina Ekström. The Auslander condition on graded and filtered Noetherian rings. In *Séminaire d'Algèbre Paul Dubreil et Marie-Paul Malliavin, 39ème Année (Paris, 1987/1988)*, volume 1404 of *Lecture Notes in Math.*, pages 220–245. Springer, Berlin, 1989.

[19] Christian Frønsdal. On the classification of q-algebras. *Lett. Math. Phys.*, 53(2):105–120, 2000.

[20] K. R. Goodearl and R. B. Warfield, Jr. *An introduction to noncommutative Noetherian rings*, volume 61 of *London Mathematical Society Student Texts.* Cambridge University Press, Cambridge, second edition, 2004.

[21] Luzius Grunenfelder. About braided and ordinary Hopf algebras. *Milan J. Math.*, 71:121–140, 2003.

[22] Jonas T. Hartwig. Hopf structures on ambiskew polynomial rings. *J. Pure Appl. Algebra*, 212(4):863–883, 2008.

[23] Nathan Jacobson. *Lie algebras.* Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[24] Michio Jimbo. A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equation. *Lett. Math. Phys.*, 10(1):63–69, 1985.

[25] N. Jing and J. J. Zhang. Gorensteinness of invariant subrings of quantum algebras. *J. Algebra*, 221(2):669–691, 1999.

[26] S. Jøndrup. Representations of some PI algebras. *Comm. Algebra*, 31(6):2587–2602, 2003.

[27] Søren Jøndrup. Representations of skew polynomial algebras. *Proc. Amer. Math. Soc.*, 128(5):1301–1305, 2000.

[28] David A. Jordan. Down-up algebras and ambiskew polynomial rings. *J. Algebra*, 228(1):311–346, 2000.

[29] David A. Jordan and Imogen E. Wells. Invariants for automorphisms of certain iterated skew polynomial rings. *Proc. Edinburgh Math. Soc. (2)*, 39(3):461–472, 1996.

[30] Richard Kane. *Reflection groups and invariant theory.* CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 5. Springer-Verlag, New York, 2001.

[31] Christian Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1995.

[32] V. K. Kharchenko. A quantum analogue of the Poincaré-Birkhoff-Witt theorem. *Algebra Log.*, 38(4):476–507, 509, 1999.

[33] Günter R. Krause and Thomas H. Lenagan. *Growth of algebras and Gelfand-Kirillov dimension*, volume 22 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, revised edition, 2000.

[34] A. Leroy, J. Matczuk, and J. Okniński. On the Gel'fand-Kirillov dimension of normal localizations and twisted polynomial rings. In *Perspectives in ring theory (Antwerp, 1987)*, volume 233 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 205–214. Kluwer Acad. Publ., Dordrecht, 1988.

[35] André Leroy and Jerzy Matczuk. Goldie conditions for Ore extensions over semiprime rings. *Algebr. Represent. Theory*, 8(5):679–688, 2005.

[36] T. Levasseur and J. T. Stafford. The quantum coordinate ring of the special linear group. *J. Pure Appl. Algebra*, 86(2):181–186, 1993.

[37] Thierry Levasseur. Some properties of noncommutative regular graded rings. *Glasgow Math. J.*, 34(3):277–300, 1992.

[38] Maria E. Lorenz and Martin Lorenz. On crossed products of Hopf algebras. *Proc. Amer. Math. Soc.*, 123(1):33–38, 1995.

[39] Shahn Majid. Cross products by braided groups and bosonization. *J. Algebra*, 163(1):165–190, 1994.

[40] J. C. McConnell and J. C. Robson. *Noncommutative Noetherian rings*. Pure and Applied Mathematics (New York). John Wiley & Sons Ltd., Chichester, 1987. With the cooperation of L. W. Small, A Wiley-Interscience Publication.

[41] Alexander Milinski and Hans-Jürgen Schneider. Pointed indecomposable Hopf algebras over Coxeter groups. In *New trends in Hopf algebra theory (La Falda, 1999)*, volume 267 of *Contemp. Math.*, pages 215–236. Amer. Math. Soc., Providence, RI, 2000.

[42] S. Montgomery. *Hopf algebras and their actions on rings*, volume 82 of *CBMS Conf. Series*. Amer. Math. Soc., Providence, RI, 1993.

[43] S. Montgomery. Some remarks on filtrations of Hopf algebras. *Comm. Algebra*, 21(3):999–1007, 1993.

[44] Warren D. Nichols. Bialgebras of type one. *Comm. Algebra*, 6(15):1521–1552, 1978.

[45] Donald S. Passman. *Infinite crossed products*, volume 135 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1989.

[46] David E. Radford. The structure of Hopf algebras with a projection. *J. Algebra*, 92(2):322–347, 1985.

[47] Joseph J. Rotman. *An introduction to homological algebra*, volume 85 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1979.

[48] J. T. Stafford and J. J. Zhang. Homological properties of (graded) Noetherian PI rings. *J. Algebra*, 168(3):988–1026, 1994.

[49] Moss E. Sweedler. *Hopf algebras*. Mathematics Lecture Note Series. W. A. Benjamin, Inc., New York, 1969.

[50] Earl J. Taft and Robert Lee Wilson. On antipodes in pointed Hopf algebras. *J. Algebra*, 29:27–32, 1974.

[51] Stefan Ufer. PBW bases for a class of braided Hopf algebras. *J. Algebra*, 280(1):84–119, 2004.

[52] Q.-S. Wu and J. J. Zhang. Noetherian PI Hopf algebras are Gorenstein. *Trans. Amer. Math. Soc.*, 355(3):1043–1066 (electronic), 2003.

[53] Zhong Yi. Injective homogeneity and the Auslander-Gorenstein property. *Glasgow Math. J.*, 37(2):191–204, 1995.

[54] Abraham Zaks. Injective dimension of semi-primary rings. *J. Algebra*, 13:73–86, 1969.

Index

G-super-word, 27
  monotonic, 27

ambiskew polynomial algebra, 79
AS-Gorenstein, 56
AS-regular, 56
associated graded
  algebra, 3
  coalgebra, 3
  Hopf algebra, 5
Auslander-Gorenstein, 52
Auslander-regular, 52

bosonisation, 12
braided
  adjoint representation, 12
  bialgebra, 11
  Hopf algebra, 11
  vector space, 9

Cohen-Macaulay, 54
connected, 3
coradical, 4

diagonalisable action, 10

filtered topology, 52
filtration
  algebra, 2
  coalgebra, 3
  coradical, 4
  Deg, 30
  Hopf algebra, 4
  Zariskian, 52

Gaussian binomial coefficient, 7
GK dimension, 49
global dimension, 46
grade, 54
grading
  algebra, 2
  braided Hopf algebra, 11
  coalgebra, 3
  Hopf algebra, 5

inner derivation, 111

lexicographic order, 17
locally algebraic, 50

Nichols algebra, 14

P.I. degree, 107
P.I. ring, 107
pointed coalgebra, 8

Shirshov decomposition, 19
skew group ring, 6
skew Laurent polynomial ring, 6
skew polynomial ring, 5
strong closure condition, 52
super-letter, 23

hard, 27
height, 28
super-word, 23
monotonic, 23
restricted, 28

winding automorphism, 85
word
degree, 17
length, 17
Lyndon, 17
nonassociative, 19
nonassociative Lyndon, 20
structure, 17

Yetter-Drinfeld module, 9