Root multiplicities for Nichols algebras of diagonal type

Dissertation
zur Erlangung des Doktorgrades der Naturwissenschaften
dem Fachbereich Mathematik und Informatik
der Philips-Universität Marburg vorgelegt von

Ying Zheng Aus Anhui,China

Kandidatin:	Ying Zheng
Erstgutachter:	Prof. Dr. István Heckenberger
Zweitgutachter:	Prof. Dr. Ulrich Krähmer
Einreichungstermin:	06. Juli 2018
Prüfungstermin:	26. September 2018
Prüfungsort:	Marburg
Hochschulkennziffer:	1180

Abstract

In this thesis we chase the root multiplicities for Nichols algebras of diagonal type. Based on an inequality for the number of Lyndon words and an identity for the shuffle map, we illustrate when the multiplicity of a root is smaller than in the tensor algebra of a braided vector space of diagonal type, and determine the dimension of the kernel of the shuffle map considered as an operator acting on the free algebra. Moreover, we give an complete expression for the multiplicities of a class of roots for Nichols algebras of diagonal type of rank two.

The structure of Nichols algebras plays a crucial role in classification of Hopf algebras, see for example [5]. In particular, those of diagonal type rule a dominant position in a part of the theory, for example, the theory of pointed Hopf algebras see for example [3].

Based on Poincaré-Birkhoff-Witt basis given by V.Kharchenko, I. Heckenberger generalized the root system and Weyl group of Kac-Moody algebras [21] to the Nichols algebras of diagonal type [13], namely, root system and Weyl groupoid. By now, based on the notions of root system and Weyl groupoid there is a deep understanding of the structure of finite-dimensional Nichols algebras of diagonal type, specially for the structure of root system. It turned out that the roots are real roots with respect to the action of Weyl groupoid and their multiplicity is one[16, 10]. Whereas the knowledge about imaginary roots and their multiplicities is little for Nichols algebras of diagonal type. With our results we make a better understanding of the Nichols algebra theory in this respect.

The thesis contains three chapters. In the first chapter, we introduce some basic notions and notations, such as Nichols algebras, braided vector spaces, Yetter-Drinfel'd modules, Lyndon words and also some results about Nichols algebras, Lyndon words, etc. We also discuss the notions of root vector candidates, root vectors and root system of Nichols algebras of diagonal type.

In the second chapter, we provide a criterion to decide whether a given Nichols algebra of diagonal type is a free algebra. As an application we give a particular family of Nichols algebras of diagonal type. It turns out that the freeness of those Nichols algebras is characterized in terms of solutions of a quadratic diophantine equation. Further more we determine the dimension of the kernel of shuffle map (over field of characteristic zero).

In the last chapter, we explore the root multiplicities of Nichols algebras of diagonal type of rank two. We concentrate on the roots of the form $m\alpha_1 + 2\alpha_2$, $m \in \mathbb{N}_0$. We formulate and prove when a root vector candidate is a root vector(over field of characteristic zero). Moreover the multiplicity of a given root is formulated.

Keywords : Nichols algebra; multiplicity; root vector; free algebra; shuffle map; Lyndon word.

Acknowledgements

I would like to thanks all the people who have helped me during my Ph.D study.

First of all, I would like to give my appreciation to my supervisor, Prof. Dr. István Heckenberger for his endless help. I am deeply impressed by his patience for explaining all questions I had both in study and in life. I am grateful to his suggestion for the topic of root multiplicities for Nichols algebras of diagonal type and all the invaluable advices about research. His optimistic attitude to research gave me a lot courage to constantly explore in mathematics.

I would like to thank my another supervisor, Prof.Naihong Hu, who encouraged me to choose the way of Ph.D study. I am very grateful to him for all advices he gave in the very beginning for my Ph.D study, in particular, for suggesting me applying for the Ph.D joint-training program supported by China Scholarship Council and visiting Prof.Dr. István Heckenberger.

I would like to give my sincere thanks to Prof.Volkmar Welker and Prof. Sonia Natale for the wonderful courses they taught. I would like to thanks my colleague Eric Heymann-Heidelberger and my friend Zhiqiang yu, who helped me to correct mistakes in this thesis.

I would like to express my gratitude to the committee. Many thanks to Prof.Dr.Bernhard Mühlherr, Prof.Dr.Iika Agricola, Dr.Andreas Krug for the great suggestions they gave. I would like to thank Prof.Dr.Ulrich Krähmer as my second referee.

Finally, I wish to thank my colleagues in the department of Mathematics, Anh, Bastian, Janik, Abdalla for having a nice time with them. I would like to thank my parents, for the endless support and love. I give my gratitude to the financial support of China Scholarship Council (CSC).

Contents

Introduction

0.1 Background

Nichols algebras were motivated by Hopf algebra theory. The notion of Nichols algebra was originally introduced in the late 1970 by W.Nichols in the paper [26], where the Nichols algebra was called bialgebra of type one and the author attempted to classify certain finite-dimensional Hopf algebra. In several yeas later, Nichols algebras were rediscovered in several different languages which are all equivalent. For instance, they were used by S. L Woronwicz to explore covariant differential calculus [36, 35], and also were rediscovered by S. Majid [25]. P. Schauenburg rediscovered them to reformulate the construction of Lustig's algebra [31]. And later on M. Rosso used them to present the "upper triangular part" of quantum groups [29].

During recent twenty years, Nichols algebras received a big attention and the topic developed to an own-standing research field with many relationships to different fields (mainly algebraic or combinatorial) in mathematics. In particular, Nichols algebras are significant for the study of finite-dimensional Hopf algebras. In the theory of Hopf algebras, the classification of finite-dimensional Hopf algebras is a hard question. The lifting method raised by N. Andruskiewitsch and H.-J. Schneider [1] is a powerful method to study finite-dimensional Hopf algebras, specially for pointed Hopf algebras. Nichols algebras played as a fundamental object in the lifting method to classify finite dimensional pointed Hopf algebras [2, 4, 5].

Roughly speaking, let $\Bbbk$ be an algebraically closed field of characteristic zero and let H be a Hopf algebra over $\Bbbk$ whose coradical H_0 is a Hopf subalgebra. Let $H_0 \subseteq H_1 \subseteq \cdots \subseteq H$ be the coradical filtration of H and let gr$H$ denote the $\mathbb{N}_0$-graded Hopf algebra $\oplus_i H_i/H_{i-1}$. Let $R = (\mathrm{gr}H)^{coH_0} = \{a \in \mathrm{gr}H \mid (\mathrm{id} \otimes \pi)\Delta_{\mathrm{gr}H}(a) = a \otimes 1\}$, where $\pi : \mathrm{gr}H \to H_0$ is the canonical projection map. It turns out that R is a braided Hopf algebra in the braided category of Yetter-Drinfel'd modules over H_0 (see[27],[24]) and gr$H \cong R\#H_0$, where $\#$ is the biproduct [27] or called bosonization, in Majid's terminology [24]. H owns an invariant, which is the Nichols algebra $\mathcal{B}(V) \subset R$ generated by the vector space V of H_0-coinvariants of H_1/H_0. For the case of pointed Hopf algebras there is a conjecture [3] that over an algebraically closed field of characteristic zero any finite-dimensional pointed Hopf algebra is generated as algebra by group-like elements and skew primitive elements. Given a finite-dimensional pointed Hopf algebra H, we get that H_0 is a group algebra and gr$H \cong R\#H_0$. And the Conjecture is equivalent to $R = \mathcal{B}(V)$, that is the braided Hopf algebra R is a Nichols algebra.

Although Nichols algebras can be defined in any suitable braided monomial category, a big part of the theory is dominated by Nichols algebras of diagonal type. A Nichols algebra $\mathcal{B}(V)$ (or braided vector space (V, c)) is termed of diagonal type if there exist a basis $\{x_i | 1 \leq i \leq n\}$ of V and a braiding matrix $(q_{ij})_{1\leq i,j\leq n} \in (\Bbbk^\times)^{n\times n}$ such that $c(x_i \otimes x_j) = q_{ij}x_j \otimes x_i$, for any $1 \leq i, j \leq n$, where $\Bbbk$ is a field. V.K.Kharchenko [22] proved that a certain Hopf algebras which are generated by group-like and primitive elements have a (restricted) Poincaré-Birkhoff-Witt basis, which implies that Nichols algebras of diagonal type admit a Poincaré-Birkhoff-Witt basis. Further, Nichols algebra of diagonal type of rank n has a natural $\mathbb{N}_0^n$-grading. Bases on these the root system and Weyl groupoid of Nichols algebras of diagonal type were introduced in [13]. The positive root system of a Nichols algebra of diagonal type is defined to be the set of the of degrees of the Poincaré-Birkhoff-Witt generators of $\mathcal{B}(V)$ counted with multiplicities.

Root system and Weyl groupoid are basic invariants of Nichols algebras of diagonal type, and play a crucial role for the classification of finite-dimensional Nichols algebras of diagonal type. In [13, 3, 2, 29] the classification results both for infinite and for finite dimensional Nichols algebras of Cartan type are given. More explicitly, a braided vector space V of diagonal type with braiding matrix $(q_{ij})_{i,j\in I}$ is called Cartan type if there exists a generalized Cartan matrix $C = (c_{ij})_{i,j\in I}$ such that $q_{ij}q_{ji} = q_{ii}^{c_{ij}}$, for all $i, j \in I$. The Nichols algebra $\mathcal{B}(V)$ associated to V is finite-dimension if and only if C is of finite type and for any $i \in I$, q_{ii} is a root of unity. Further more, if it is in this case then the defining ideal is generated by quantum Serre relations.

In a series of papers [14, 16, 17], using the tools of root system and Weyl groupoid I.Heckenberger classified the finite-dimensional Nichols algebras of diagonal type over fields of characteristic zero. The explicit description of the defining ideal in generators and relations of finite-dimensional Nicohols algebras of diagonal type over field of characteristic zero were given in [6, 7]. The classifications of rank two and rank three Nichols algebras of diagonal type over fields of positive characteristic were solved in [33] and [34], respectively.

The root system and Weyl groupoid of Nichols algebras of diagonal type are known to be play a similar role as the root system and Weyl group of semi-simple Lie algebras (see for example [2]). In the general setting, one is constantly tempted to seek for relationships with Kac-Moody and Borcherds Lie (super) algebras. The latter seems to be very strong in the finite case because of the definitions of real roots in the two theories. However, the knowledge about imaginary roots and their multiplicities is little in the case of Kac-Moody algebras, and even poorer for Nichols algebras of diagonal type. For information on recent activities in the theory of Kac-Moody algebras we refer to [9].

A general, very difficult question is, what are the roots and their multiplicities of a given Nichols algebra of diagonal type. In the case of finite-dimensional Nichols algebras of diagonal type the answer is known: The roots are the real roots with respect to the action of the Weyl groupoid, and their multiplicity is one, see [16] [10]. The other extreme case is the one of free algebra, where the root vectors are parametrized by Lyndon words and appropriate powers of them. Roots of the form $m\alpha_1 + \alpha_2$ with $m \in \mathbb{N}_0$ are determined by using Rosso's lemma [29, Lemma 14]. In this thesis we devote to studying the roots multiplicities for Nichols algebras of diagonal type.

In this thesis we address two questions for Nichols algebras of diagonal type:

When the multiplicity of a root is smaller than in the tensor algebra, and what is the multiplicities of the roots which are of form $m\alpha_1 + 2\alpha_2$ with $m \in \mathbb{N}_0$. (The multiplicities of $m\alpha_1 + k\alpha_2$ with $k \in \{0, 1\}$ have been known before, see for example [31, 3].) The defining ideal of a Nichols algebra is spanned by the kernels of the braided symmetrizers [31], which decomposes into a product of shuffle maps. In [11], the authors studied identities involving shuffle maps. We use these identities to study the freeness of Nichols algebras of diagonal type and, over a field of characteristic zero we determine the dimension of the kernel of the shuffle map.

For the second question we focus on the Nichols algebras of diagonal type of rank 2. We define a family $(P_k)_{k\in\mathbb{N}_0}$ in the free algebra over a two-dimensional braided vector space of diagonal type, and relate the relations in the Nichols algebra of degree $m\alpha_1+2\alpha_2$ to this family. We find two of our results particularly interesting. First, we prove that if a root vector candidate is a root vector, then any lexicographically larger root vector candidate of the same degree is a root vector, too. Second, we describe precisely when a root vector candidate is a root vector. To do so, we define a subset $\mathbb{J}$ of $\mathbb{N}_0$ depending on the given braiding, which measures the multiplicities of all roots of the form $m\alpha_1 + 2\alpha_2$ in a simple way. For the calculation of $\mathbb{J}$ one needs only elementary (and simple) calculations with Laurent polynomials in three indeterminates. Unfortunately, the proof of this theorem requires that we work over a field of characteristic zero.

0.2 Structure of this thesis

The organization of this thesis is as follows. In Chapter 1, we present the basic notions and notations and some fundamental results. In Section 1.1 we recall the notions of Lyndon words and necklaces which are fundamental objects in this thesis. We also recall the results from [18], which give some inequalities about the number of Lyndon words (or about the number of Lyndon words and the number of necklace). In Section 1.2, some basic notions and general properties are recalled, such as the category of Yetter-Drinfel'd modules over a Hopf algebra, braided vector space and braided Hopf algebras, also the relations between Yetter-

Drinfel'd modules and braided vector spaces. Based on those notions we introduce the notion of Nichols algebra in this section. In Section 1.3, we recall the braided symmetrizer and recall some decompositions of braided symmetrizer in terms of shuffle maps. The identity which was study in [11] involving shuffle maps is also expressed in this section. In Section 1.4, we restate the Kharchenko's theorem [22, Theorem 2] and introduce the notions of root vector candidate, root vector and root system of a Nichols algebra of diagonal type. In Section 1.5, skew-derivations and reflections are introduced, which are fundamental tools in thesis to determine a root vector.

In Chapter 2, we concentrate on the question when the multiplicity of a root is smaller than in the tensor algebra. In particular, we provide a criterion to decide whether a given Nichols algebra of diagonal type is a free algebra in terms of polynomial equations for the entries of the braiding matrix. We define a family $(P_{\underline{m}})_{\underline{m}\in\mathbb{N}_0^n,|\underline{m}|\geq 2}$ of elements in the polynomial ring $\mathbb{Z}[p_{ij} \mid 1 \leq i,j \leq n]$, where $|(m_1, m_2, \ldots, m_n)| = \sum_{i=1}^n m_i$ in Section 2.1, which are related to the freeness of a Nichols algebra of diagonal type. Some basic properties and results are also proved section 2.1. In Section 2.2, we discuss the notion of a free prebraided module of diagonal type over a commutative ring and compute the determinant of shuffle map. The question when a given Nichols algebra of diagonal type is a free algebra is answered in Section 2.3. Let (V, c) be a n-dimensional braided vector space of diagonal type over $\Bbbk$ with braiding matrix $\boldsymbol{q} \in (\Bbbk^\times)^{n\times n}$, where $\Bbbk$ is a field. We obtain that $\mathcal{B}(V)$ is the free if and only if $P_{\underline{m}}(\boldsymbol{q}) \neq 0$ for all $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$. The proof is based on the inequalities described in Section 1.1 for detail see Theorem 2.3.3. As an application, we relate the freeness of Nichols algebras of diagonal type with braiding matrix $(q^{m_{ij}})_{1\leq i,j\leq n}$, $m_{ij} \in \mathbb{Z}$ for all i, j to solutions of a diophantine equation see Example 2.3.4. In Section 2.4 and Section 2.5, we determine the dimension of the kernel of shuffle map. Suppose that $\Bbbk$ is a field of characteristic zero. Assume $P_{\underline{m}}(\boldsymbol{q}) = 0$, then there is an upper bound on the dimension of the shuffle map which is given in Proposition 2.4.5. We prove that this upper bound is actually a lower bound in Section 2.5. We end this chapter by giving an example in which the defining relations of a Nichols algebra of diagonal type is two.

In Chapter 3, we focus on Nichols algebras of diagonal type of rank two. We devote to determining the multiplicities of the special roots $m\alpha_1 + 2\alpha_2$, where $m \in \mathbb{N}_0$ and α_1, α_2 is the standard basis of $\mathbb{Z}^2$. Some equations for Gaussian binomial coefficients are given in Section 3.1, which will be needed later. In Section 3.2 we describe some basic notations and fundamental results, which the results in this chapter are based on. In Section 3.3, we formulate and prove some interesting results. Proposition 3.3.3 illustrates that if a root vector candidate is a root vector, then any lexicographically larger root vector candidate of the same degree is a root vector, too. Theorem 3.3.16 and Corollary 3.3.17 describe precisely when a root vector candidate is a root vector. We give the multiplicity of root $m\alpha_1 + 2\alpha_2$, for any $m \in \mathbb{N}_0$ in Corollary 3.3.18. At the end of this section we illustrate these results on two examples, each of which is related to a quantized enveloping algebra of an affine Kac-Moody algebra of rank two see Examples 3.3.23 and 3.3.24.

The content of the thesis convers the results from [19] and [20]. All the results from Chapter 2 and Chapter 3 are joint with Prof. Dr. István Heckenberger.

Chapter 1

Basic Notations and Notions

In this chapter we recall some basic notions and notations which will be useful later.

1.1 Lyndon words

In this section we recall the notions of Lyndon words and necklaces and some relations about them. For an introduction see [23] also see [8].

As usual we write $\mathbb{N}$ and $\mathbb{Z}$ for the set of positive integers and the set of integers, respectively. Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Let $n \in \mathbb{N}$. For any $\underline{m} = (m_1, \ldots, m_n) \in \mathbb{N}_0^n$ we write $|\underline{m}| = \sum_{i=1}^n m_i$. For any $1 \leq i \leq n$ let $\underline{e}_i = (\delta_{ij})_{1 \leq j \leq n} \in \mathbb{N}_0^n$, and for any $k \in \mathbb{N}_0$ and any $\underline{m} = (m_1, \ldots, m_n) \in \mathbb{N}_0^n \setminus \{0\}$ let $\underline{m}/k = (m_1/k, m_2/k, \ldots, m_n/k)$. If additionally $\underline{m} \neq 0$, then let $\gcd(\underline{m})$ be the greatest common divisor of $m_1, \ldots, m_n$.

There is a partial ordering on $\mathbb{N}_0^n$ denoted by $\leq$: $\underline{m} \leq \underline{l}$ if and only if $m_i \leq l_i$ for all $1 \leq i \leq n$.

Let B be a set (called the alphabet) of n elements denoted by $b_1, b_2, \ldots, b_n$, and let $\mathbb{B}$ and $\mathbb{B}^\times$ be the set of words and non-empty words, respectively, with letters in B. For $w = b_{i_1} b_{i_2} \cdots b_{i_s} \in \mathbb{B}$, in which b_j occurs m_j times, $1 \leq j \leq n$, we write $\deg w = (m_1, m_2, \ldots, m_n)$ and call $\deg w$ the **degree** of w. We write $|w| = s$ and call s the length of w.

We fix a total order $\leq$ on B. There is a total order $\leq_{\text{lex}}$ on $\mathbb{B}$ induced by $\leq$, called the lexicographic order: For $u, v \in \mathbb{B}$, one lets $u \leq_{\text{lex}} v$ if and only if either $v = uw$ for some $w \in \mathbb{B}$, or there exist $w, u', v' \in \mathbb{B}$ and $x, y \in B$ such that $u = wxu'$, $v = wyv'$, $x \leq y$, and $x \neq y$.

A word $w \in \mathbb{B}^\times$ is called a **necklace** if for any decomposition $w = uv$ with $u, v \in \mathbb{B}^\times$, $w \leq_{\text{lex}} vu$. A word $w \in \mathbb{B}^\times$ is **Lyndon** if for any decomposition $w = uv$, $u, v \in \mathbb{B}^\times$, $w \leq_{\text{lex}} v$. For any $\underline{m} \in \mathbb{N}_0^n$ let $N_{\underline{m}}$ and $\ell_{\underline{m}}$ denote the number of necklaces and Lyndon words, respectively, of degree $\underline{m}$.

Remark 1.1.1. (1) Any Lyndon word is a necklace, and for any necklace w there is a unique pair $(v, k) \in \mathbb{B} \times \mathbb{N}$ such that v is Lyndon and $w = v^k$. Thus, for any $\underline{m} \in \mathbb{N}_0^n \setminus \{0\}$,

$$N_{\underline{m}} = \sum_{d | \gcd(\underline{m})} \ell_{\underline{m}/d}. \tag{1.1}$$

(2) A word $u \in \mathbb{B}^\times$ is a Lyndon word if and only if either $u \in B$, or there exist Lyndon words $w, v \in \mathbb{B}^\times$ such that $w <_{\text{lex}} v$ and $u = wv$.

Definition 1.1.2. Any Lyndon word u of length at least two has a unique decomposition into the product of two Lyndon words $u = wv$, where $|w|$ is minimal. It is called the **Shirshow decomposition** of u.

Example 1.1.3. Let $\mathbb{B} = \{b_1, b_2\}$ with $b_1 < b_2$, the Necklaces of Length at most three are

$$b_1,\ b_2,\ b_1b_2,\ b_1b_1b_2,\ b_1b_2b_2, b_1b_1, b_2b_2, b_1b_1b_1, b_2b_2b_2$$

The words $b_1, b_2, b_1b_2, b_1b_1b_2, b_1b_2b_2$ are Lyndon words, $b_1b_1, b_2b_2, b_1b_1b_1, b_2b_2b_2$ are not Lyndon words. The word $u = b_1b_1b_2b_1b_2b_2$ is a Lyndon word, let $w = b_1$ and $v = b_1b_2b_1b_2b_2$, then $u = wv$ is the Shirshow decomposition of u.

For the next part of this section, let us introduce some formulas and Inequalities about the number of Lyndon words for fixed degree.

Remark 1.1.4. There are explicit formulas in[18] and [30] for $N_{\underline{m}}$ and $\ell_{\underline{m}}$ for any $\underline{m} \in \mathbb{N}_0^n$.

$$N_{\underline{m}} = \frac{1}{|\underline{m}|} \sum_{k|\,\gcd(\underline{m})} \phi(k) \frac{(|\underline{m}|/k)!}{(m_1/k)! \cdots (m_n/k)!}$$
$$\ell_{\underline{m}} = \frac{1}{|\underline{m}|} \sum_{k|\,\gcd(\underline{m})} \mu(k) \frac{(|\underline{m}|/k)!}{(m_1/k)! \cdots (m_n/k)!},$$

where for any $k \in \mathbb{N}$, $\phi(k)$ denotes Euler's totient, that is, the number of positive integers in range $[1, k]$ that are relatively prime to k. And μ is the Möbius function, that is, for any $k \in \mathbb{N}$,

$$u(k) = \begin{cases} 1, k = 1 \\ (-1)^t, \ k = p_1 p_2 \dots p_t, \ for \ distinct \ primes \ p_i \\ 0, \ p^2 | k \ for \ some \ prime \ number \ p. \end{cases}$$

In particular,

$$\ell_{\underline{e}_i + k\underline{e}_j} = 1, \text{ for all } k \in \mathbb{N}_0; \tag{1.2}$$
$$\ell_{k\underline{e}_j} = \delta_{k,1}, \text{ for all } k \in \mathbb{N}_0. \tag{1.3}$$

Let us recall some results in [18] about the number of Lyndon words, which Chapter 2 is based on. Because of Equation (1.1), we restate the theorem as follows:

Theorem 1.1.5. ([18, Lemma 4.1, 4.2, Theorem 1.2]) Let $\underline{m} \in \mathbb{N}_0^n$. Assume that $m_t \neq 0$, $m_s \neq 0$, for some $t, s \in \{1, 2, \dots, n\}$ and $t \neq s$. Then,

(1).

$$\sum_{k|\gcd(\underline{m})} \ell_{\underline{m}/k} \leq \sum_{1 \leq i \leq n, m_i > 0} \ell_{\underline{m} - \underline{e}_i}.$$

(2).

$$\sum_{k|\gcd(\underline{m})} \ell_{\underline{m}/k} = \sum_{1 \leq i \leq n, m_i > 0} \ell_{\underline{m} - \underline{e}_i}, \tag{1.4}$$

if and only if $\underline{m}$ is one of the following cases

$$\underline{e}_i + m_i\underline{e}_j,\ 2\underline{e}_i + m_i\underline{e}_j,\ 3\underline{e}_i + 3\underline{e}_j,\ 3\underline{e}_i + 4\underline{e}_j,\ 3\underline{e}_i + 6\underline{e}_j,\ 4\underline{e}_i + 4\underline{e}_j,$$

except for $\underline{m} = \underline{e}_i + \underline{e}_j$, for $1 \leq i, j \leq n, i \neq j$ and $m_i \in \mathbb{N}$.

1.2 Braided vector space and Nichols algebras

In this section we recall the notions and notations about braided vector space, Yetter-Drinfel'd module and Nichols algebra, etc. For further details we refer to [3] ,[15].

Let $\Bbbk$ be a field and let $\Bbbk^\times = \Bbbk \backslash \{0\}$.

Definition 1.2.1. We call a pair (V, c) a braided vector space, if V is a vector space and $c : V \otimes V \to V \otimes V$ is an linear isomorphism of $V \otimes V$, and c satisfies the braid equation:

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

Definition 1.2.2. A braided vector space (V, c) is called diagonal type if V admits a basis $x_1,\ x_2,\ \ldots,\ x_\theta$ such that for all $1 \leq i, j \leq \theta$,

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

for some $q_{ij} \in \Bbbk^\times$. The matrix $(q_{ij})_{1 \leq i,j \leq \theta}$ is called the braiding matrix of (V, c).

In order to explain the notion of Nichols algebras, let us first collect some constructions about Hopf algebras.

Definition 1.2.3. Let H be a Hopf algebra. A vector space M is called a left Yetter-Drinfel'd over H, if M is a left comodule over H via $\delta : M \to H \otimes M$ which is also a left $H-$module with action denoted by $. : H \otimes M \to M$. And the coaction and action satisfy the compatibility condition, that is,

$$\delta(h.m) = h_{(1)} m_{(-1)} S(h_{(3)}) \otimes h_{(2)}.m_{(0)}, \tag{1.5}$$

where $\Delta(h) = h_{(1)} \otimes h_{(2)}$ and $\delta(m) = m_{(-1)} \otimes m_{(0)}$ are Sweedler notations, and S is the antipode of H. A Yetter-Drinfel'd module M is of diagonal type if $H = \Bbbk G$, where G is an abelian group, and M is a direct sum of one-dimensional Yetter-Drinfeld modules over the group algebra $\Bbbk G$.

We write ${}^H_H\mathcal{YD}$ for the category of Yetter-Drinfel'd modules over H. Morphisms in ${}^H_H\mathcal{YD}$ preserve both the action and coaction of H. Note that ${}^H_H\mathcal{YD}$ is a braided monomial category. In fact, the tensor product of two Yetter-Drinfel'd modules V, M is given by the tensor product over $\Bbbk$ and

$$\delta(x \otimes m) = x_{(-1)}m_{(-1)} \otimes x_{(0)}m_{(0)}, \quad h.(x \otimes m) = h_{(1)}.x \otimes h_{(2)}.m,$$

for all $x \in V$ and $m \in M$. The braiding $c_{\_,\_}$ is given by

$$c_{V,M}(x \otimes m) = x_{(-1)}.m \otimes x_{(0)},$$

$x \in V$ and $m \in M$. And any $V \in {}^H_H\mathcal{YD}$ has a braiding $c_{V,V}$ such that $(V, c_{V,V})$ is a braided vector space. Conversely, a braided vector space (V, c) can be realized as a Yetter-Drinfel'd module over some Hopf algebra if and only if the braiding c is rigid [32, section 2].

There are some relations between braided vector spaces and Yetter-Drinfel'd modules in ${}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$.

Remark 1.2.4. Let G be an abelian group. For any $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ of diagonal type, $(V, c_{V,V})$ is a braided vector space of diagonal type. In fact, let $V = \oplus_{i\in I}\Bbbk x_i$, where $\Bbbk x_i \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ for all $i \in I$, and $\{x_i \mid i \in I\}$ is a basis of V. Then there exist $g_i \in G$ and $q_{ij} \in \Bbbk^\times$ such that the coaction map $\delta(x_i) = g_i \otimes x_i$ and action map $g_i.x_j = q_{ij}x_j$, for all $i, j \in I$. Thus we get $c_{V,V}(x_i \otimes x_j) = q_{ij}x_j \otimes x_i$, for all $i, j \in I$. Hence $(V, c_{V,V})$ is a braided vector space of diagonal type.

For any braided vector space (V, c) of diagonal type, there exists an abelian group G such that V is a Yetter-Drinfeld module over $\Bbbk G$ of diagonal type. Indeed, suppose that $\{x_i \mid i \in I\}$ is a basis of V and $(q_{ij})_{i,j\in I} \in (\Bbbk^\times)^{|I|\times|I|}$ such that

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

for any $i, j \in I$. Let G be the abelian group generated by generators $\{g_i \mid i \in I\}$. The coaction and action of $\Bbbk G$ is given by

$$\delta(x_i) = g_i \otimes x_i$$

and

$$g_i.x_j = q_{ij}x_j,$$

for all $i, j \in I$. And it is easy to check that Equation 1.5 holds. Thus $\Bbbk x_i$ is Yetter-Drinfel'd module over $\Bbbk G$, for all $i \in I$, and $V = \oplus_{i \in I} \Bbbk x_i \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$. Therefore V is a Yetter-Drinfel'd module over $\Bbbk G$ of diagonal type.

Let H be a Hopf algebra and let $\mathcal{A}$ is an algebra in ${}^H_H\mathcal{YD}$, that is $\mathcal{A}$ is a Yetter-Drinfel'd module over H, and the multiplication map μ of $\mathcal{A}$ is a morphism of Yetter-Drinfel'd modules. Then $\mathcal{A} \otimes \mathcal{A}$ is an algebra in ${}^H_H\mathcal{YD}$ with the multiplication map $\mu_{\mathcal{A}\otimes\mathcal{A}}$ given by,

$$(a \otimes b)(c \otimes d) = a(b_{(-1)}.c) \otimes b_{(0)}d, \quad \text{for all } a, b, c, d \in \mathcal{A},$$

where . denotes the left action of H on $\mathcal{A}$.

Similarly, if $\mathcal{A}$ is a coalgebra in ${}^H_H\mathcal{YD}$, that is, $\mathcal{A}$ is a Yetter-Drinfel'd module over H and the comultiplication map Δ of $\mathcal{A}$ is a morphism in ${}^H_H\mathcal{YD}$, then $\mathcal{A} \otimes \mathcal{A}$ is a coalgebra in ${}^H_H\mathcal{YD}$ with the comultiplication $\Delta_{\mathcal{A}\otimes\mathcal{A}}$ given by

$$\begin{aligned} \Delta_{\mathcal{A}\otimes\mathcal{A}}(a \otimes b) &= (\mathrm{id} \otimes c \otimes \mathrm{id})(\Delta \otimes \Delta)(a \otimes b) \\ &= a_{(1)} \otimes a_{(2)(-1)}.b_{(1)} \otimes a_{(2)(0)} \otimes b_{(2)}. \end{aligned}$$

Definition 1.2.5. Let H be a Hopf algebra. A braided Hopf algebra in ${}^H_H\mathcal{YD}$ is a 6-tuble $(\mathcal{A}, \mu, 1, \Delta, \varepsilon, S_{\mathcal{A}})$, where

(1) $(\mathcal{A}, \mu, 1)$ is an algebra in ${}^H_H\mathcal{YD}$.

(2) $(\mathcal{A}, \Delta, \varepsilon)$ is a coalgebra in ${}^H_H\mathcal{YD}$. And Δ, ε are morphisms of algebras.

(3) $S_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ is a morphism in ${}^H_H\mathcal{YD}$, such that for all $a \in \mathcal{A}$

$$S_{\mathcal{A}}(a_{(1)})a_{(2)} = a_{(1)}S_{\mathcal{A}}(a_{(2)}) = \varepsilon(a)1,$$

where $\Delta(a) = a_{(1)} \otimes a_{(2)}$ is the coproduct of a.

Example 1.2.6. Let H be a Hopf algebra, and let V be a Yetter-Drinfel'd module in ${}_H^H\mathcal{YD}$. Let $T(V)$ be the tensor algebra over $\Bbbk$. Then $T(V)$ admits a Yetter-Drinfel'd module in ${}_H^H\mathcal{YD}$ and an algebra structure in ${}_H^H\mathcal{YD}$. Then $T(V)$ has a braided Hopf algebra structure in ${}_H^H\mathcal{YD}$ with coproduct and counit given by

$$\Delta(x) = 1 \otimes x + x \otimes 1, \ \varepsilon(x) = 0, \text{ for all } x \in V,$$

respectively. The existence of antipode of $T(V)$ see [3, Section 2.1]. Moreover, $T(V)$ is an $\mathbb{N}_0$-graded Hopf algebra in ${}_H^H\mathcal{YD}$, where $\deg v = n$, for all $v \in V^{\otimes n}$.

There is a unique maximal coideal denoted by $\mathcal{J}(V)$ among all the coideals of $T(V)$ which are contained in $\oplus_{k\geq 2} V^{\otimes k}$, and the coideal is $\mathbb{N}_0$-graded corresponding to the $\mathbb{N}_0$-grading of $T(V)$. In fact, let $\mathcal{D}$ be the set of all coideals of $T(V)$ contained in $\oplus_{k\geq 2} V^{\otimes k}$. Then $\sum_{\mathcal{I}\in\mathcal{D}} \mathcal{I}$ is the maximal coideal of $T(V)$ in $\mathcal{D}$. Hence $\mathcal{J}(V) = \sum_{\mathcal{I}\in\mathcal{D}} I$. For $\mathcal{J}(V)$ is homogeneous see the proof in [15, Lemma 2.1].

Definition 1.2.7. Let H be a Hopf algebra. Let V be a Yetter-Drinfel'd module over H. The Nichols algebra $\mathcal{B}(V)$ of V is defined as the quotient

$$\mathcal{B}(V) = T(V)/\mathcal{J}(V) = \Bbbk \oplus V \oplus (\oplus_{k\geq 2} V^{\otimes k}/\mathcal{J}(V))$$

A Nichols algebra $\mathcal{B}(V)$ is of diagonal type if V is a Yetter-Drinfel'd module of diagonal type. The dimension of V is called the rank of Nichols algebra $\mathcal{B}(V)$.

Remark 1.2.8. The coideal $\mathcal{J}(V)$ is actually also an ideal and a Yetter-Drinfel'd submodule in ${}_H^H\mathcal{YD}$. Indeed, one can prove this by analyzing that the ideal $\mathcal{I}$ of $T(V)$ generated by $\mathcal{J}(V)$ is also a coideal with $\mathcal{I} \cap V = \{0\}$ and the Yetter-Drinfel'd submodule $\mathcal{N}$ generated by $\mathcal{J}(V)$ is also a coideal with $\mathcal{N} \cap V = 0$. Then $\mathcal{B}(V)$ is a $\mathbb{N}_0$ -graded braided Hopf algebra in ${}_H^H\mathcal{YD}$.

Remark 1.2.9. Let V is an n-dimensional Yetter-Drinfel'd module of diagonal type, then by Remark 1.2.4 we get that there exist a basis $x_1, x_2, \ldots, x_n$ of V and $(q_{ij})_{1\leq i,j\leq n}$ such that

$$c_{V,V}(x_i \otimes x_j) = q_{ij} x_j \otimes x_i.$$

Assume that $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is the standard basis of $\mathbb{Z}^n$. Then both $T(V)$ and $\mathcal{B}(V)$ have a unique $\mathbb{Z}^n$-graded braided Hopf algebra structure such that $\deg(x_i) = \alpha_i$ for any $1 \leq i \leq n$. In particular, for $l \in \mathbb{N}_0$ the degree of $x_{i_1} x_{i_2} \cdots x_{i_l}$ is $\sum_{j=1}^{l} \alpha_{i_j}$.

There are many other characterizations of Nichols algebras. In the following we give one more.

For any braided Hopf algebra $\mathcal{A} \in {}^H_H\mathcal{YD}$, an element x in $\mathcal{A}$ is termed Primitive element if

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

Let $P(\mathcal{A})$ denote the set of primitive elements of $\mathcal{A}$. Note that $\varepsilon(x) = 0$ for all $x \in P(\mathcal{A})$.

Remark 1.2.10. First, it is clear that V generates $\mathcal{B}(V)$ as an algebra.

Second, $P(\mathcal{B}(V)) = V$. In factor all the components of a primitive element are primitive elements. One can prove this by using induction on the number of the components of $x \in P(\mathcal{B}(V))$. Let now $x \in \mathcal{B}(V)(n)$, $n \geq 2$ and let $\pi : T(V) \to \mathcal{B}(V)$ be the canonical map. As π is surjective coalgebra map then there is $y \in T(V)(n)$ such that $\pi(y) = x$. Then

$$(\pi \otimes \pi)(\Delta(y) - y \otimes 1 - 1 \otimes y) = 0,$$

thus

$$\Delta(y) - y \otimes 1 - 1 \otimes y \in \ker(\pi \otimes \pi) = \mathcal{J}(V) \otimes T(V) + T(V) \otimes \mathcal{J}(V).$$

Therefore $\mathcal{I}' = \Bbbk y + \mathcal{J}(V)$ is a graded coideal of $T(V)$ and $\mathcal{J}(V) \subset \mathcal{I}'$ thus $\mathcal{J} = \mathcal{I}'$, then $y \in \mathcal{J}$.

Theorem 1.2.11. Suppose that $\mathcal{I} \in {}^H_H\mathcal{YD}$ is a Yetter-Drinfel'd submodule of $T(V)$ with $\mathcal{I} \cap V = \{0\}$, then $T(V)/\mathcal{I} = \mathcal{B}(V)$ if and only if all primitive elements of $T(V)/\mathcal{I}$ are contained in V.

Proof. See [28, Corollary 15.5.8]. □

We end this section by giving two well known examples.

Example 1.2.12. Let (V, c) be one-dimensional braided vector space. Let $V = \Bbbk x$ and $q \in \Bbbk^{\times}$ such that $c(x \otimes x) = qx \otimes x$. Then from Remak 1.2.4, there is an abelian group G such that $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$.

(1) If q is a n-th root of unity then $\mathcal{B}(V) = T(V)/(x^n)$.

(2) If q is not a root of unity then $\mathcal{B}(V) = T(V)$.

In factor, it is will known that

$$\Delta(x^m) = \sum_{i=0}^{m} \binom{m}{i}_q (x^i \otimes x^{m-i}),$$

for all $m \in \mathbb{N}$. If q is a n-th root of unity then

$$\binom{n}{i}_q = 0$$

for any $1 \leq i \leq n-1$, hence

$$\Delta(x^n) = x^n \otimes 1 + 1 \otimes x^n,$$

thus $x^n \in \mathcal{J}(V)$. Therefore $\mathcal{B}(V) = T(V)/(x^n)$.

If q is not a root of unity, we know that $x^m \notin P(\mathcal{B}(V))$, for all $m \in \mathbb{N},\ m \geq 2$. Hence $\mathcal{B}(V) = T(V)$.

Example 1.2.13. In this example we discuss over the field $\mathbb{k} = \mathbb{Q}(q)$. Let $\theta \in \mathbb{N}$, and assume that $H = \mathbb{k}\mathbb{Z}^\theta$. Let $\{\alpha_1, \alpha_2, \dots, \alpha_\theta\}$ be the standard basis of $\mathbb{Z}^\theta$. we write the elements of $\mathbb{Z}^\theta$ exponentially: $e^{m_1\alpha_1+\cdots+m_2\alpha_2}$, where $m_i \in \mathbb{Z}$ for all $1 \leq i \leq \theta$. Let $A = (a_{ij})_{1\leq i,j\leq\theta} \in \mathbb{Z}^{\theta\times\theta}$ be a symmetrizable Cartan matrix, that is $a_{ii} = 2, a_{kj} \leq 0$ and $a_{kj} = 0$ if and only if $a_{jk} = 0$, for all $1 \leq i, j, k \leq \theta,\ j \neq k$. Let $d_1, d_2, \dots, d_\theta \in \mathbb{N}$, such that $d_i a_{ij} = d_j a_{ji}$. Suppose that $V \in {}^H_H\mathcal{YD}$ and $v = \mathrm{span}_{\mathbb{k}}\{x_i | 1 \leq i \leq \theta\}$, such that $\delta(x_i) = e^{\alpha_i} \otimes x_i$ and $e^{\alpha_i}.x_j = q^{d_i a_{ij}} x_j$, for all $1 \leq i, j \leq \theta$ then $\mathcal{B}(V) = U_q(\mathfrak{n}_+)$, where $U_q(\mathfrak{n}_+)$ is the quantized enveloping algebra of the positive part $\mathfrak{n}_+$ of the Kac-Moody Lie algebra $\mathfrak{g}(A)$. Let $\mathrm{ad}\, x_i(y) = x_i y - (e^{\alpha_i}.y)x$, for all $1 \leq i \leq \theta$ and $y \in T(V)$. One can prove that the ideal $\mathcal{J}(V)$ is generated by the quantum Serre relations

$$(\mathrm{ad}\, x_i)^{1-a_{ij}}(x_j), \text{ for all } 1 \leq i, j \leq \theta, \quad i \neq j.$$

1.3 The braided symmetrizer

In this section we recall the braided symmetrizer to give another expression for Nichols algebras.

In this section let (V, c) be a braided vector space over any $\Bbbk$.

For any $k \in \mathbb{N}$, $k \geq 2$, let $\mathbb{S}_k$ be the symmetric groups generated by $k-1$ generators $\tau_1, \tau_2, \ldots, \tau_{k-1}$ and relations:

$$\tau_i^2 = 1, \text{ for any } 1 \leq i \leq k-1,$$

$$\tau_i \tau_{i+1} \tau_i = \tau_{i+1} \tau_i \tau_{i+1}, \text{ for any } 1 \leq i \leq k-2,$$

$$\tau_i \tau_j = \tau_j \tau_i, \text{ for } 1 \leq i+1 < j \leq k-1.$$

We write $\mathbb{B}_k$ for the Artin braid group presented by $k-1$ strands $\sigma_1, \sigma_2, \ldots, \sigma_{k-1}$ and relations,

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \text{ for any } 1 \leq i \leq k-2,$$

$$\sigma_i \sigma_j = \sigma_j \sigma_i, \text{ for } 1 \leq i+1 < j \leq k-1.$$

Let $\Bbbk\mathbb{B}_n$ denote the group algebra of $\mathbb{B}_k$ over $\Bbbk$.

For any $k \geq 2$, let $\rho_k : \Bbbk\mathbb{B}_k \longrightarrow \mathrm{Aut}(V^{\otimes k})$ be the representation of $\Bbbk\mathbb{B}_k$ such that $\rho_k(\sigma_i)$ is the braiding c acting on the i-th and $i+1$-th factor of $V^{\otimes k}$, for any $1 \leq i \leq k-1$.

Let $\pi : \mathbb{B}_k \longrightarrow \mathbb{S}_k$ denote the natural projection with $\pi(\sigma_i) = \tau_i$, for all $1 \leq i \leq k-1$. Then there is a unique map section $s : \mathbb{S}_k \longrightarrow \mathbb{B}_k$ of π sending τ_i to σ_i, for all $1 \leq i \leq k-1$, such that $s(tw) = s(t)s(w)$ whenever $\ell(tw) = \ell(t) + \ell(w)$, where $\ell(w)$ denotes the minimal length of a representation of w as a product in the generators. In particular, if $w = \tau_{j_1}\tau_{j_2}\cdots\tau_{j_r}$ is the reduced expression of $w \in \mathbb{S}_k$, then $s(w) = \sigma_{j_1}\sigma_{j_2}\cdots\sigma_{j_r}$.

Let $S_k = \sum_{w \in \mathbb{S}_k} s(w) \in \Bbbk\mathbb{B}_k$. The map $\rho_k(S_k) \in \mathrm{Aut}(V^{\otimes k})$ is called the **braided symmetrizer**.

As an example here we computer S_k for $k = 2, 3$,

$$S_2 = 1 + \sigma_1;$$

$$S_3 = 1 + \sigma_1 + \sigma_2 + \sigma_1\sigma_2 + \sigma_2\sigma_1 + \sigma_1\sigma_2\sigma_1.$$

There is another characterization of Nichols algebras.

Proposition 1.3.1. [31, Theorem 2.9] Let $V \in {}^H_H\mathcal{YD}$, then

$$\mathcal{B}(V) = \Bbbk + V + \bigoplus_{k\geq 2} V^{\otimes k}/\ker(S_k).$$

This description of relation of $\mathcal{B}(V)$ does not mean that the relations are known. In general, it is very hard to calculate the kernels of the maps S_k.

Let us introduce some particular elements in $\mathbb{B}_m$, which can be used to express the braided symmetrizer.

For any $k \geq 2$ there is a unique group homomorphism $\tau : \mathbb{B}_k \longrightarrow \mathbb{B}_{k+1}$ with $\tau(\sigma_i) = \sigma_{i+1}$ for all $1 \leq i \leq k-1$. We also write τ for the algebra maps $\Bbbk\mathbb{B}_k \to \Bbbk\mathbb{B}_{k+1}$.

Let

$$\begin{aligned} T_k &= 1 + \sigma_k + \sigma_k\sigma_{k-1} + \cdots + \sigma_k\sigma_{k-1}\cdots\sigma_1; \\ U_k &= 1 + \sigma_1 + \sigma_1\sigma_2 + \cdots + \sigma_1\sigma_2\cdots\sigma_k; \\ S_{1,k} &= 1 + \sigma_1 + \sigma_2\sigma_1 + \cdots + \sigma_k\sigma_{k-1}\cdots\sigma_1. \end{aligned}$$

Lemma 1.3.2. For any $m \geq 2$,

$$\begin{aligned} S_m &= T_1T_2\cdots T_{m-1} \\ &= S_{1,m-1}\tau(S_{1,m-2})\tau^2(S_{1,m-3})\cdots\tau^{m-2}(S_{1,1}) \\ &= \tau^{m-2}(U_1)\tau^{m-3}(U_2)\cdots\tau(U_{m-2})U_{m-1}. \end{aligned}$$

Proof. For the proof of first identity and second identities see [11, Proposition 6.10] and for the third one see [12, Proposition 2]. □

A variant of the following equation appeared already in [11, Lemma 6.12].

Lemma 1.3.3. For any $k > m \geq 1$ the following equation holds in $\mathbb{B}_k$. In $\mathbb{B}_k$ with $k \geq 2$ the following equation

$$(1 - \sigma_m\cdots\sigma_2\sigma_1)S_{1,m} = S_{1,m-1}(1 - \sigma_m\cdots\sigma_2\sigma_1^2)$$

holds.

Proof. It is easy to check that

$$(\sigma_m\sigma_{m-1}\cdots\sigma_2\sigma_1)\sigma_i = \sigma_{i-1}(\sigma_m\sigma_{m-1}\cdots\sigma_2\sigma_1)$$

for all $2 \le i \le m < k$.

$$\begin{aligned}
&(\sigma_m\cdots\sigma_2\sigma_1)S_{1,m}\\
&= \sum_{t=1}^{m}(\sigma_m\cdots\sigma_2\sigma_1)\sigma_t\sigma_{t-1}\cdots\sigma_2\sigma_1 + \sigma_m\cdots\sigma_2\sigma_1\\
&= \sum_{t=1}^{m-1}\sigma_t\sigma_{t-1}\cdots\sigma_2\sigma_1(\sigma_m\cdots\sigma_2\sigma_1^2) + \sigma_m\cdots\sigma_2\sigma_1^2 + \sigma_m\cdots\sigma_2\sigma_1\\
&= S_{1,m-1}(\sigma_m\cdots\sigma_2\sigma_1^2) + \sigma_m\cdots\sigma_2\sigma_1
\end{aligned}$$

Hence,

$$\begin{aligned}
&(1-\sigma_m\cdots\sigma_2\sigma_1)S_{1,m}\\
&= S_{1,m} - S_{1,m-1}(\sigma_{m-1}\cdots\sigma_2\sigma_1^2) - \sigma_{m-1}\cdots\sigma_2\sigma_1\\
&= S_{1,m-1} - S_{1,m-1}(\sigma_m\cdots\sigma_2\sigma_1^2)\\
&= S_{1,m-1}(1-\sigma_m\cdots\sigma_2\sigma_1^2).
\end{aligned}$$

□

1.4 Poincaré-Birkhoff-Witt basis and root System for Nichols algebras of diagonal type

The main purpose of this section is to recall the Poincaré-Birkhoff-Witt basis and root System for Nichols algebras of diagonal type.

Let $\mathbb{k}$ ba a field and let $\mathbb{k}^\times = \mathbb{k}\backslash\{0\}$. Let G be an abelian group and let $V \in {}^{\mathbb{k}G}_{\mathbb{k}G}\mathcal{YD}$ be of diagonal type. Let $\{x_1, x_2, \ldots, x_n\}$ be a basis of V. Then there exists $(q_{ij})_{1\le i,j\le n} \in (\mathbb{k}^\times)^{n\times n}$ such that

$$c(x_i \otimes x_j) = q_{ij}x_j \otimes x_i.$$

Let $X = \{x_1, \dots, x_n\}$, and fix the total ordering on X such that $x_i < x_j$ whenever $1 \le i < j \le n$. Let $\mathbb{X}$ and $\mathbb{X}^\times$ denote the set of words and non-empty words over the alphabet X, respectively. The elements of $\mathbb{X}$ can naturally be viewed as elements of (any quotient of) $T(V)$, and as such they form a vector space basis of $T(V)$.

For a Lyndon word $u \in \mathbb{X}^\times$, following [22] we define the **super-letter** $[u] \in \mathcal{B}(V)$ inductively as follows:

(1) $[u] = u$, if $u \in X$, and

(2) $[u] = [v][w] - \chi(\deg(v), \deg(w))[w][v]$ if $u \in \mathbb{X}^\times$, $|u| \ge 2$, and $u = vw$ is the Shirshow decomposition of u.

Moreover, for any Lyndon word u and any integer $k \ge 2$ let $[u^k] = [u]^k$.

The total ordering on $\mathbb{X}$ induces a total ordering on the set of super-letters:

$$[u] < [v] \Leftrightarrow u <_{\mathrm{lex}} v.$$

For any $\alpha \in \mathbb{Z}^n$, let $o_\alpha \in \mathbb{N} \cup \{\infty\}$ be the multiplicative order of $\chi(\alpha, \alpha) \in \Bbbk^\times$. Moreover, let

$$O_\alpha = \begin{cases} \{1, o_\alpha, \infty\} & \text{if } o_\alpha = \infty \text{ or } \mathrm{char}(\Bbbk) = 0, \\ \{1, o_\alpha p^k, \infty \mid k \in \mathbb{N}_0\} & \text{if } o_\alpha < \infty,\ p = \mathrm{char}(\Bbbk) > 0. \end{cases}$$

Kharchenko proved the following fundamental result on Nichols algebras.

Theorem 1.4.1. [22] There exists a set L of Lyndon words and a function $h : L \to \mathbb{N} \cup \{\infty\}$, where $h(v) \in O_{\deg v} \setminus \{1\}$ for any $v \in L$, such that the elements

$$[v_k]^{m_k} \cdots [v_1]^{m_1}, \quad k \in \mathbb{N}_0,\ v_1, \dots, v_k \in L,\ v_1 <_{\mathrm{lex}} v_2 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} v_k,$$
$$0 < m_i < h(v_i) \text{ for any } i,$$

form a vector space basis of $\mathcal{B}(V)$.

In fact, the set L and the function h in the above theorem are uniquely determined.

In some situations it is more appropriate to work with a slightly different presentation of the above basis of $\mathcal{B}(V)$, in which the function h does not appear.

Definition 1.4.2. Let $w \in \mathbb{X}^\times$. We say that $[w]$ is a **root vector candidate** if $w = v^k$ for some Lyndon word v and $k \in O_{\deg v} \setminus \{\infty\}$.

Definition 1.4.3. A root vector candidate $[w]$, where $w \in \mathbb{X}^\times$, is called a **root vector (of $\mathcal{B}(V)$)** if $[w] \in \mathcal{B}(V)$ is not a linear combination of elements of the form $[v_k]^{m_k} \cdots [v_1]^{m_1}$, where $k \in \mathbb{N}_0$ and $[v_1], \dots, [v_k]$ are root vector candidates with $w <_{\mathrm{lex}} v_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} v_k$.

Remark 1.4.4. By [22, Corollary 2], for any Lyndon word $w \in \mathbb{X}^\times$ the root vector candidate $[w]$ is a root vector if and only if $w \in \mathcal{B}(V)$ is not a linear combination of elements of the form $[v_k]^{m_k} \cdots [v_1]^{m_1}$, where $k \in \mathbb{N}_0$ and $[v_1], \dots, [v_k]$ are root vector candidates with $w <_{\mathrm{lex}} v_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} v_k$.

Note that in Definition 1.4.3 it is not necessary to put assumptions on the degrees of the monomials, since $\mathcal{B}(V)$ is graded.

Example 1.4.5. Assume that $n \geq 2$. Let $k \in \mathbb{N}_0$. The only Lyndon word of degree $k\alpha_1 + \alpha_2$ in $\mathbb{X}$ is $x_1^k x_2$, and the only root vector candidate of degree $k\alpha_1 + \alpha_2$ is $[x_1^k x_2]$. Since $\mathcal{B}(V)$ is $\mathbb{N}_0^n$-graded, $[x_1^k x_2]$ is not a root vector if and only if $[x_1^k x_2] = 0$ in $\mathcal{B}(V)$. In our setting, the latter can be characterized in terms of the matrix $(q_{ij})_{1 \leq i,j \leq n}$ using Rossos Lemma [29, Lemma 14]: For any $k \geq 0$,

$$[x_1^{k+1} x_2] = 0 \quad \Leftrightarrow \quad (k+1)^!_{q_{11}} \prod_{i=0}^{k} (1 - q_{11}^i q_{12} q_{21}) = 0.$$

The Lyndon words of degree $k\alpha_1 + 2\alpha_2$ in $\mathbb{X}$ are the words $x_1^{k_1} x_2 x_1^{k_2} x_2$ with $k_1, k_2 \in \mathbb{N}_0$, $k_1 + k_2 = k$, $k_1 > k_2$. The elements $[x_1^{k_1} x_2 x_1^{k_2} x_2]$ are the only root vector candidates of degree $k\alpha_1 + 2\alpha_2$, except when k is even and $q_{11}^{k^2/4} (q_{12} q_{21})^{k/2} q_{22} = -1$. In the latter case, $[x_1^{k/2} x_2]^2$ is the only additional root vector candidate of degree $k\alpha_1 + 2\alpha_2$. The definition implies that the element $[x_1^{k_1} x_2 x_1^{k_2} x_2]$ with $k_1 + k_2 = k$, $k_1 \geq k_2$, is not a root vector if and only if there exists a relation in $\mathcal{B}(V)$ of the form

$$\sum_{i=k_2}^{k_1} \lambda_i [x_1^i x_2][x_1^{k-i} x_2] = 0$$

such that $\lambda_i \in \Bbbk$ for any $k_2 \leq i \leq k_1$ and

$$\lambda_{k_1} = 1, \quad \lambda_{k_2} = -\chi(k_1\alpha_1 + \alpha_2, k_2\alpha_1 + \alpha_2).$$

(This is also true if $k_1 = k_2$!)

Note that the definitions of a root vector candidate and a root vector depend on the bicharacter χ. Now Kharchenko's theorem can be restated as follows.

Theorem 1.4.6. Let $L \subseteq \mathbb{X}^\times$ such that $w \in L$ if and only if $[w]$ is a root vector. Then the elements

$$[v_k]^{m_k} \cdots [v_1]^{m_1}, \quad k \in \mathbb{N}_0,\ v_1, \ldots, v_k \in L,\ v_1 <_{\mathrm{lex}} v_2 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} v_k,$$
$$0 < m_i < \min(O_{\deg v_i} \setminus \{1\}) \text{ for any } i,$$

form a vector space basis of $\mathcal{B}(V)$.

(Note that $\min(O_\alpha \setminus \{1\})$ for $\alpha \in \mathbb{Z}^n$ equals o_α, except when $\alpha = 1$.) This reformulation of Kharchenko's theorem allows to define the set

$$\boldsymbol{\Delta}_+ = \{\deg(u) \mid u \in L\}$$

of **positive roots of** $\mathcal{B}(V)$ and the **root system** $\boldsymbol{\Delta} = \boldsymbol{\Delta}_+ \cup -\boldsymbol{\Delta}_+$ of $\mathcal{B}(V)$, see [13]. It turns out that this definition is independent of choices. For any $\alpha \in \boldsymbol{\Delta}_+$, the number of elements $u \in L$ with $\deg(u) = \alpha$ is called the **multiplicity of** α.

1.5 Skew-derivations and reflections

In this section we give some characterizations of Nichols algebras of diagonal type. Let G be an abelian group.

Let $V \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$ of diagonal type of finite dimension θ. Let $I = \{1, 2, \ldots, \theta\}$. We choose a basis $\{x_i | i \in I\}$ of V and elements $g_1, g_2, \ldots, g_\theta$ in G such that

$$\delta(x_i) = g_i \otimes x_i,\ g_i.x_j = q_{ij}x_i, \text{ for } i, j \in I,$$

where $q_{ij} \in \Bbbk^\times$, for $\leq i, j \leq \theta$.

Definition 1.5.1. A **bicharacter** on an abelian group G is a map $\chi : G \times G \to \Bbbk^\times$, such that

$$\chi(g_1 + g_2, g_3) = \chi(g_1, g_3)\chi(g_2, g_3),\ \ \chi(g_1, g_2 + g_3) = \chi(g_1, g_2)\chi(g_1, g_3).$$

for all $g_1, g_2, g_3 \in G$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_\theta$ be the standard basis of $\mathbb{Z}^\theta$ and $\chi : \mathbb{Z}^\theta \times \mathbb{Z}^\theta \to \Bbbk^\times$ be the bicharacter on $\mathbb{Z}^\theta$ such that $\chi(\alpha_i, \alpha_j) = q_{ij}$ for any $i, j \in I$.

From Remark 1.2.9 we conclude that both $T(V)$ and $\mathcal{B}(V)$ have a unique $\mathbb{Z}^\theta$-graded braided bialgebra structure such that $\deg(x_i) = \alpha_i$ for all $i \in I$. In particular, for any $\Bbbk \in \mathbb{N}_0$, and $l_1, l_2, \ldots, l_k \in I$ the degree of $x_{l_1}x_{l_2}\cdots x_{l_k}$ is $\sum_{i=1}^{k} \alpha_{l_i}$. We write $\deg(x)$ for the degree of any homogeneous element x of $T(V)$ or $\mathcal{B}(V)$.

For $i \in I$, there exist unique skew-derivations d_i and ∂_i of $T(V)$ such that

$$d_i(x_j) = \delta_{ij},\ \ d_i(xy) = d_i(x)y + \chi(\alpha, \alpha_i)xd_i(y), \tag{1.6}$$

$$\partial_i(x_j) = \delta_{ij},\ \ \partial_i(xy) = x\partial_i(y) + \chi(\alpha_i, \beta)\partial_i(x)y, \tag{1.7}$$

for any $j \in I$ and $x, y \in T(V)$ with $\deg(x) = \alpha$ and $\deg(y) = \beta$.

Theorem 1.5.2. [15, Theorem 2.11] The ideal $\mathcal{J}(V)$ is the largest ideal among all ideals $\mathcal{I}$ of $T(V)$ such that $\epsilon(\mathcal{I}) = 0$ and $d_i(\mathcal{I}) \subset \mathcal{I}$ for all $i \in I$.

The above Theorem 1.5.2 also holds for ∂_i.

One can use this Theorem to check whether a given ideal coincides with $\mathcal{J}(V)$.

Remark 1.5.3. Let V be as above.

(1) Theorem 1.5.2 guarantees that these skew-derivations of $T(V)$ induce skew-derivations of $\mathcal{B}(V)$ which will be denoted by the same symbols.

(2) An element $x \in \mathcal{B}(V)$ is constant if and only if $d_i(x) = 0$ in $\mathcal{B}(V)$ for any $i \in I$. In particular, a homogeneous element $x \in \mathcal{B}(V)$ of non-zero degree is zero if and only if $d_i(x) = 0$ in $\mathcal{B}(V)$ for any $i \in I$. Because of this, the

skew-derivations d_i, $i \in I$, and their relatives belong to the main tools in the study of Nichols algebras of diagonal type.

One can replace d_i by ∂_i.

Let us give one simple example to illustrate Remark 1.5.3.

Example 1.5.4. Let (V,c) be a braided vectoe space of diagonal type with basis $\{x_i \mid i \in I\}$ and $(q_{ij})_{i,j\in I}$ such that

$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i.$$

Then for all $m \in \mathbb{N}$, and $i \in I$,

(1) $d_i(x_i^m) = (m)_{q_{ii}} x_i^{m-1}$;

(2) $x_i^m = 0$ in $\mathcal{B}(V)$ if and only if $(m)^!_{q_{ii}} = 0$.

Proof. By induction on m and using Equation (1.6) one can prove (1).

(2) holds because of (1) and Remark 1.5.3(2). □

Since $\mathcal{B}(V)$ is an $\mathbb{N}_0^n$-graded coalgebra, let $\pi_\beta : \mathcal{B}(V) \to \mathcal{B}(V)(\beta)$ be the natural projection. We denote by

$$\Delta_{\beta,\gamma} : \mathcal{B}(V) \to \mathcal{B}(V)(\beta) \otimes \mathcal{B}(V)(\gamma), \quad x \mapsto x_{\beta,\gamma},$$

the (β,γ)-th component of the comulitiplication Δ, that is $\Delta_{\beta,\gamma} = (\pi_\beta \otimes \pi_\gamma)\Delta$.

For any $x \in \mathcal{B}(V)$ and any $\beta, \gamma \in \mathbb{N}_0^n$ there exist uniquely determined elements

$$x_{\beta,\gamma} \in \mathcal{B}(V)(\beta) \otimes \mathcal{B}(V)(\gamma),$$

such that $\Delta(x) = \sum_{\beta,\gamma\in\mathbb{N}_0^n} x_{\beta,\gamma}$.

Remark 1.5.5. The skew-derivations d_i, ∂_i with $i \in I$ are closely related to these maps:

$$\Delta_{\alpha_i,\alpha-\alpha_i}(x) = x_i \otimes d_i(x), \quad \Delta_{\alpha-\alpha_i,\alpha_i}(x) = \partial_i(x) \otimes x_i. \tag{1.8}$$

for any $i \in I$, $\alpha \in \mathbb{N}_0^n$, and any homogeneous element $x \in \mathcal{B}(V)$ of degree α.

At the end of this section we recall the reflections and some important results about the transformations of Nichols algebras, which will be useful latter.

Let $i \in I$. Assume that for any $j \in I\backslash\{i\}$ there exists $k \in \mathbb{N}_0$ such that $(k+1)_{q_{ii}}(1 - q_{ii}^k q_{ij} q_{ji}) = 0$. Following [13], we set $m_{ii} = 2$ and for any $j \in I\backslash\{i\}$ we define

$$m_{ij} = -min\{k \in \mathbb{N}_0 | (k+1)_{q_{ii}}(1 - q_{ii}^k q_{ij} q_{ji}) = 0\}.$$

Let $s_i \in \mathrm{GL}(\mathbb{Z}^\theta)$ defined by $s_i(\alpha_j) = \alpha_j - m_{ij}\alpha_i$, for all $j \in I$. The map s_i is a reflection. The reflection of V on the i-th vertex is the braided vector space $R_i(V)$ with basis $x'_1, \dots, x'_\theta$ such that for all $j, k \in I$

$$c(x'_j \otimes x'_k) = q'_{jk} x'_k \otimes x'_j,$$

where $q'_{jk} = \chi(s_i(\alpha_j), s_i(\alpha_k)) = q_{jk} q_{ik}^{-m_{ij}} q_{ji}^{-m_{ik}} q_{ii}^{m_{ij} m_{ik}}$.

Following [3] we define the adjoint representation ad of $T(V)$, for any $i \in I$ and $y \in T(V)$,

$$\operatorname{ad} x_i(y) = x_i y - \chi(\alpha_i, \deg(y)) y x_i,$$

Assume now $i \in I$ such that for any $j \in I\backslash\{i\}$ there exists $k \in \mathbb{N}_0$ such that $(k+1)_{q_{ii}}(1 - q_{ii}^k q_{ij} q_{ji}) = 0$. Let

$$m_{ij} = -min\{k \in \mathbb{N}_0 | (k+1)_{q_{ii}}(1 - q_{ii}^k q_{ij} q_{ji}) = 0\},$$

for any $j \neq i$.

Let $\mathcal{K}_i$ be the subalgebra of $\mathcal{B}(V)$ generated by $\{(\operatorname{ad} x_i)^m(x_j) \mid m \geq 0, j \neq i\}$. The subalgebra $\mathcal{K}_i$ is finitely generated. Indeed, using induction on m one can get the following equations, for any $j \neq i$, and $m \in \mathbb{N}_0$

$$d_i((\operatorname{ad} x_i)^m(x_j)) = (1 - q_{ii}^{m-1} q_{ij} q_{ji})(m)_{q_{ii}} (\operatorname{ad} x_i)^{m-1}(x_j),$$
$$d_j((\operatorname{ad} x_i)^m(x_j)) = 0, m \neq 0.$$

Clearly, $d_k((\operatorname{ad} x_i)^m(x_j)) = 0$, for any $k \neq i, j$. Thus $(\operatorname{ad} x_i)^m(x_j) = 0$ in $\mathcal{B}(V)$ for any $m > -m_{ij}$.

For $x \in \mathcal{K}_i$ let $L_x : \mathcal{B}(V) \to \mathcal{B}(V)$, given by

$$L_x(y) = xy, \text{ for all } y \in \mathcal{B}(V).$$

Let

$$V_i = \Bbbk d_i \oplus \oplus_{j \neq i} \Bbbk (\operatorname{ad} x_i)^{-m_{ij}}(x_j).$$

Note that $V_i \in {}^{\Bbbk G}_{\Bbbk G}\mathcal{YD}$.

Theorem 1.5.6. [13, Theorem 5.7, Theorem 5.9] Let $\mathcal{B}_i$ be the subalgebra of $\operatorname{End}(\mathcal{B}(V))$ generated by d_i and $L_x, x \in \mathcal{K}_i$. Then $\mathcal{B}_i$ is generated as an algebra by V_i. And furthermore, there is a coalgebra structure and an antipode on $\mathcal{B}_i$ such that $\mathcal{B}_i$ is isomorphic to the Nichols algebra $\mathcal{B}(V_i)$. And

$$\boldsymbol{\Delta}_+(\mathcal{B}_i) = (s_i(\boldsymbol{\Delta}_+(\mathcal{B}(V)))\backslash\{-\alpha_i\}) \cup \{\alpha_i\}.$$

Moreover $\operatorname{mult}(s_i(\alpha)) = \operatorname{mult}(\alpha)$, for all $\alpha \in \boldsymbol{\Delta}_+(\mathcal{B}(V))\backslash\{\alpha_i\}$.

Chapter 2

A characterization of Nichols algebras of diagonal type which are free algebras

In this Chapter we devote to exploring the freeness of Nichols algebras of diagonal type and to determine the dimension of the kernel of the shuffle map considered as an operator acting on the free algebra.

2.1 Some particular polynomials and some basic properties

In this section we will introduce and study some polynomials, which are crucial for present chapter.

For any ring R and any $q \in R$ let $(0)_q = 0$ and $(m)_q = 1 + q + \cdots + q^{m-1}$ for any $m \in \mathbb{N}$.

For any $\underline{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{N}_0^n \backslash \{0\}$, let

$$N(\underline{m}) = \gcd\{m_i(m_i - 1), m_j m_k \mid 1 \leq i, j, k \leq n, j < k\}.$$

Definition 2.1.1. For any $\underline{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$ let $P_{\underline{m}} \in \mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n]$ be as follows:

(1) If $\underline{m} = m_i \underline{e}_i$, where $1 \leq i \leq n$, and $m_i \in \mathbb{N}$, let

$$P_{\underline{m}} = (m_i)_{p_{ii}};$$

(2) If $\underline{m} = \underline{e}_i + m_j \underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, $m_j \in \mathbb{N}$, let

$$P_{\underline{m}} = 1 - p_{jj}^{m_j - 1} p_{ij} p_{ji};$$

(3) If $\underline{m} = 2\underline{e}_i + m_j \underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, $m_j \in \mathbb{N}$, let

$$P_{\underline{m}} = 1 + p_{jj}^{m_j(m_j-1)/2} (-p_{ij} p_{ji})^{m_j} p_{ii};$$

(4) If $\underline{m} = 3\underline{e}_i + 3\underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, let

$$P_{\underline{m}} = (3)_{p_{ii}^2 (p_{ij} p_{ji})^3 p_{jj}^2};$$

(5) If $\underline{m} = 3\underline{e}_i + 4\underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, let

$$P_{\underline{m}} = (1 - p_{ii}^2 (p_{ij} p_{ij})^4 p_{jj}^4)(3)_{p_{ii} (p_{ij} p_{ji})^2 p_{jj}^2};$$

(6) If $\underline{m} = 3\underline{e}_i + 6\underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, let

$$P_{\underline{m}} = (1 - p_{ii} (p_{ij} p_{ji})^3 p_{jj}^5)(3)_{p_{ii}^2 (p_{ij} p_{ji})^6 p_{jj}^{10}};$$

(7) If $\underline{m} = 4\underline{e}_i + 4\underline{e}_j$, where $1 \leq i, j \leq n$, $i \neq j$, let

$$P_{\underline{m}} = (1 + p_{ii}^3 (p_{ij} p_{ji})^4 p_{jj}^3)(1 + p_{ii}^6 (p_{ij} p_{ji})^8 p_{jj}^6);$$

(8) Otherwise, let

$$P_{\underline{m}} = 1 - \prod_{1 \leq i \leq n} p_{ii}^{m_i(m_i-1)} \prod_{1 \leq i < j \leq n} (p_{ij} p_{ji})^{m_i m_j}.$$

Moreover, let

$$Q_{\underline{m}} = \prod_{1 \leq i \leq n} p_{ii}^{m_i(m_i-1)/N(\underline{m})} \prod_{1 \leq i < j \leq n} (p_{ij} p_{ji})^{m_i m_j / N(\underline{m})}.$$

Remark 2.1.2. Let $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$. By definition of $N(\underline{m})$, $Q_{\underline{m}}$ is a well-defined non-constant monomial in $\mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n]$, and $Q_{\underline{m}}$ is not a non-trivial power of any other monomial. Moreover, $P_{\underline{m}}$ divides $1 - Q_{\underline{m}}^{N(\underline{m})}$. In particular, $P_{\underline{m}} = 1 - Q_{\underline{m}}^{N(\underline{m})}$ in the last case of Definition 2.1.1.

For any $i \in \mathbb{N}$ let $\Phi_i \in \mathbb{Z}[x]$ denote the i-th cyclotomic polynomial, that is, the minimal polynomial of any primitive i-th root of 1 in the complex numbers. Clearly, $x^k - 1 = \prod_{i|k} \Phi_i$ for any $k \in \mathbb{N}$.

Next we describe the irreducible factors of the polynomials $P_{\underline{m}}$.

Lemma 2.1.3. Let D be a Euclidean domain, let $\underline{m} = (m_1, \ldots, m_n)$ be a non-zero vector in D^n, and let $d = \gcd(m_1, \ldots, m_n)$. Then there is a matrix $M \in D^{n\times n}$ with $\underline{m}$ as its first row and determinant d.

Proof. View $\underline{m}$ as a $1 \times n$-matrix. Choose a composition f of elementary column transformations which maps $\underline{m}$ to the vector $(d, 0, \ldots, 0)$. Let M' be the diagonal matrix with diagonal entries $(d, 1, \ldots, 1)$. Then $M = f^{-1}(M')$ satisfies the desired properties. □

Remark 2.1.4. Lemma 2.1.3 also holds for principal ideal domains D. On the other hand, let $D = \Bbbk[x, y]$ for some field $\Bbbk$ and let $\underline{m} = (x, y)$. Then $\gcd(\underline{m}) = 1$, but there are no $a, b \in D$ with $xb - ya = 1$. Hence Lemma 2.1.3 does not hold for this D.

Lemma 2.1.5. Let $\underline{m} = (m_1, \ldots, m_n)$ be a non-zero vector in $\mathbb{Z}^n$ such that $\gcd(m_1, m_2, \ldots, m_n) = 1$. Then there is a ring automorphism φ of the Laurent polynomial ring $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ with $\varphi(x_1) = x_1^{m_1} \cdots x_n^{m_n}$.

Proof. By Lemma 2.1.3 there is a matrix $M \in \mathbb{Z}^{n\times n}$ with $\underline{m}$ as its first row and with determinant 1. Then $\varphi(x_i) = x_1^{m_{i1}} x_2^{m_{i2}} \cdots x_n^{m_{in}}$ for $1 \leq i \leq n$ defines a ring automorphism of $\mathbb{Z}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ as desired. □

Lemma 2.1.6. For any $k \in \mathbb{N}$ and any $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$, the polynomial $\Phi_k(Q_{\underline{m}}) \in \mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n]$ is irreducible. In particular, $Q_{\underline{m}}^k - 1 = \prod_{i|k} \Phi_i(Q_{\underline{m}})$ is the unique factorization of $Q_{\underline{m}}^k - 1$ into irreducibles, and each irreducible factor of $P_{\underline{m}}$ is of the form $\Phi_l(Q_{\underline{m}})$ for some $l \mid N(\underline{m})$.

Proof. Let $k \in \mathbb{N}$ and $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$. For any $1 \leq i, j, l \leq n$ let

$$m_{ii} = m_i(m_i - 1)/N(\underline{m}), \quad m_{jl} = m_j m_l/N(\underline{m}).$$

Then $\gcd(m_{ij} \mid 1 \leq i, j \leq n) = 1$ and $Q_{\underline{m}} = \prod_{1 \leq i,j \leq n} p_{ij}^{m_{ij}}$ by construction. By Lemma 2.1.5 there is a ring automorphism φ of the Laurent polynomial ring $\mathbb{Z}[p_{ij}^{\pm 1} \mid 1 \leq i, j \leq n]$ with $\varphi(p_{11}) = Q_{\underline{m}}$. Thus $\Phi_k(Q_{\underline{m}}) = \varphi(\Phi_k(p_{11}))$ is irreducible in $\mathbb{Z}[p_{ij}^{\pm 1} \mid 1 \leq i, j \leq n]$. Since $\Phi_k(Q_{\underline{m}})$ is not divisible in $\mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n]$ by any p_{ij} with $1 \leq i, j \leq n$, the polynomial $\Phi_k(Q_{\underline{m}})$ is irreducible. □

Lemma 2.1.7. Let $\underline{m}, \underline{l} \in \mathbb{N}_0^n$ with $|\underline{l}| \geq 2$. Suppose that there exist $1 \leq i < j \leq n$ such that $m_i, m_j \neq 0$. Then $P_{\underline{m}}$ and $P_{\underline{l}}$ are relatively prime if and only if $\underline{m} \neq \underline{l}$. In particular, $P_{\underline{m}}$ and $P_{\underline{l}}$ are relatively prime whenever $\underline{l} < \underline{m}$.

Proof. Recall that $P_{\underline{m}}$ is not constant. Thus, if $P_{\underline{m}}$ and $P_{\underline{l}}$ are relatively prime, then $\underline{m} \neq \underline{l}$.

Conversely, suppose that $P_{\underline{m}}$ and $P_{\underline{l}}$ are not relatively prime. Then, by Remark 2.1.2, $Q_{\underline{m}}^{N(\underline{m})} - 1$ and $Q_{\underline{l}}^{N(\underline{l})} - 1$ are not relatively prime. Let f be a non-constant common factor of $Q_{\underline{m}}^{N(\underline{m})} - 1$ and $Q_{\underline{l}}^{N(\underline{l})} - 2$. Lemma 2.1.6 implies that there exist non-constant monic polynomials $p_1, p_2 \in \mathbb{Z}[x]$ with $f = p_1(Q_{\underline{m}}) = p_2(Q_{\underline{l}})$. In particular, $Q_{\underline{m}} = Q_{\underline{l}}$. Let $1 \leq i < j \leq n$ with $m_i, m_j \neq 0$. Then $l_i, l_j \neq 0$, and the following equations hold:

$$\frac{m_i(m_i - 1)}{N(\underline{m})} = \frac{l_i(l_i - 1)}{N(\underline{l})}, \tag{2.1}$$

$$\frac{m_j(m_j - 1)}{N(\underline{m})} = \frac{l_j(l_j - 1)}{N(\underline{l})}, \tag{2.2}$$

$$\frac{m_i m_j}{N(\underline{m})} = \frac{l_i l_j}{N(\underline{l})}. \tag{2.3}$$

From Equation (2.1) and (2.3), one gets

$$l_j m_i - l_i m_j = l_j - m_j.$$

Similarly, using Equation (2.2) and (2.3), one gets

$$l_j m_i - l_i m_j = m_i - l_i. \tag{2.4}$$

Thus $m_i + m_j = l_i + l_j$. Let $t = m_i + m_j = l_i + l_j$. Replacing m_j with $t - m_i$ and l_j with $t - l_i$ in Equation (2.4), we get $t(m_i - l_i) = m_i - l_i$, and hence $m_i = l_i$ because of $t > 1$. Thus $m_j = l_j$. It follows that $\underline{m} = \underline{l}$. □

Now we pass to another family of polynomials, which are the main reason for our interest in the family $(P_{\underline{m}})_{\underline{m}\in\mathbb{N}_0^n, |\underline{m}|\geq 2}$.

Definition 2.1.8. For any $\underline{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{N}_0^n$, $|\underline{m}| \geq 2$, let

$$A_{\underline{m}} = \frac{\prod_{i:m_i>0}\prod_{k|\gcd(\underline{m}-\underline{e}_i)}(1 - Q_{\underline{m}}^{N(\underline{m})/k})^{\ell_{(\underline{m}-\underline{e}_i)/k}}}{\prod_{k|\gcd(\underline{m})}(1 - Q_{\underline{m}}^{N(\underline{m})/k})^{\ell_{\underline{m}/k}}}.$$

Note that any k with $k \mid \gcd(\underline{m} - \underline{e}_i)$ divides $m_i - 1$ and any m_j, $j \neq i$, and hence $k \mid N(\underline{m})$. Similarly, $k \mid \gcd(\underline{m})$ implies that $k \mid N(\underline{m})$. Therefore the numerator and the denominator of $A_{\underline{m}}$ are polynomials. If $\underline{m} = m_i\underline{e}_i$ for some $1 \leq i \leq n$ and $m_i \geq 2$, then $Q_{\underline{m}} = p_{ii}$ and

$$A_{m_i\underline{e}_i} = \frac{1 - Q_{\underline{m}}^{N(\underline{m})/(m_i-1)}}{1 - Q_{\underline{m}}^{N(\underline{m})/m_i}} = \frac{1 - Q_{\underline{m}}^{m_i}}{1 - Q_{\underline{m}}^{m_i-1}} = \frac{(m_i)_{p_{ii}}}{(m_i - 1)_{p_{ii}}}. \tag{2.5}$$

In order to show that every other $A_{\underline{m}}$ is a polynomial, we use some results in [18] about the number of Lyndon words, which was recalled in Theorem 1.1.5.

Lemma 2.1.9. Let $\underline{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{N}_0^n$. If there exist $i, j \in \{1, 2, \ldots, n\}$, $i \neq j$, such that $m_i \neq 0$, $m_j \neq 0$, then $A_{\underline{m}}$ is a polynomial in $\mathbb{Z}[p_{ij}, 1 \leq i, j \leq n]$.

Proof. The numerator of $A_{\underline{m}}$ is a multiple of $\prod_{i:m_i>0}(1 - Q_{\underline{m}}^{N(\underline{m})})^{\ell_{\underline{m}-\underline{e}_i}}$ and the denumerator of $A_{\underline{m}}$ is a divisor of $\prod_{k|\gcd(\underline{m})}(1 - Q_{\underline{m}}^{N(\underline{m})})^{\ell_{\underline{m}/k}}$. Thus the claim follows from Theorem 1.1.5(1). □

Proposition 2.1.10. Let $\underline{m} = (m_1, m_2, \ldots, m_n) \in \mathbb{N}_0^n$ with $m_s, m_t > 0$ for some $1 \leq s < t \leq n$. Then $P_{\underline{m}}$ is the product of the irreducible factors of $A_{\underline{m}}$.

Proof. We follow Definition 2.1.1 case by case to compare $A_{\underline{m}}$ and $P_{\underline{m}}$. Then the claim follows directly from Lemma 2.1.6.

(1) If $\underline{m} = m_i\underline{e}_i$ for some $1 \leq i \leq n$, $m_i \geq 2$, then the assumptions of the lemma are not fulfilled.

(2) Assume that $\underline{m} = \underline{e}_i + m_j\underline{e}_j$, $1 \le i,j \le n$, $i \ne j$, $m_j > 0$. Then $N(\underline{m}) = m_j$, $Q_{\underline{m}} = p_{ij}p_{ji}p_{jj}^{m_j-1}$, and

$$\begin{aligned} A_{\underline{m}} &= \frac{(1-Q_{\underline{m}}^{m_j})^{\ell_{\underline{e}_i+(m_j-1)\underline{e}_j}} \prod_{k|m_j}(1-Q_{\underline{m}}^{m_j/k})^{\ell_{m_j\underline{e}_j/k}}}{(1-Q_{\underline{m}}^{m_j})^{\ell_{\underline{m}}}} \\ &= \frac{(1-Q_{\underline{m}}^{m_j})(1-Q_{\underline{m}})}{1-Q_{\underline{m}}^{m_j}} = 1-Q_{\underline{m}} = 1-p_{ij}p_{ji}p_{jj}^{m_j-1} = P_{\underline{m}}, \end{aligned}$$

where we used Equations (1.2) and (1.3).

(3) Assume that $\underline{m} = 2\underline{e}_i + m_j\underline{e}_j$, $1 \le i,j \le n$, $i \ne j$, $m_j > 0$. Then $N(\underline{m}) = 2$ and $Q_{\underline{m}} = p_{ii}(p_{ij}p_{ji})^{m_j}p_{jj}^{m_j(m_j-1)/2}$. Moreover,

$$A_{\underline{m}} = \frac{(1-Q_{\underline{m}}^{N(\underline{m})})^{\ell_{\underline{m}-\underline{e}_i}} \prod_{k|\gcd(2,m_j-1)}(1-Q_{\underline{m}}^{N(\underline{m})/k})^{\ell_{(\underline{m}-\underline{e}_j)/k}}}{\prod_{k|\gcd(2,m_j)}(1-Q_{\underline{m}}^{N(\underline{m})/k})^{\ell_{\underline{m}/k}}}.$$

If m_j is even, then $\ell_{\underline{m}/2} + \ell_{\underline{m}} = \ell_{\underline{m}-\underline{e}_i} + \ell_{\underline{m}-\underline{e}_j}$ by Theorem 1.1.5(2). Thus

$$A_{\underline{m}} = \frac{(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}-\underline{e}_i}}(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}-\underline{e}_j}}}{(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}}}(1-Q_{\underline{m}})^{\ell_{\underline{m}/2}}} = 1+Q_{\underline{m}} = P_{\underline{m}}$$

by Equation (1.2).

If m_j is odd, then $\ell_{(\underline{m}-\underline{e}_i)} + \ell_{(\underline{m}-\underline{e}_j)} = \ell_{\underline{m}}$ by Theorem 1.1.5(2). Therefore

$$A_{\underline{m}} = \frac{(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}-\underline{e}_i}}(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}-\underline{e}_j}}(1-Q_{\underline{m}})^{\ell_{(\underline{m}-\underline{e}_j)/2}}}{(1-Q_{\underline{m}}^2)^{\ell_{\underline{m}}}} = 1-Q_{\underline{m}} = P_{\underline{m}}$$

by Equation (1.2).

(4) Assume that $\underline{m} = 3\underline{e}_i + 3\underline{e}_j$ with $1 \le i < j \le n$. Then $N(\underline{m}) = 3$, $Q_{\underline{m}} = p_{ii}^2(p_{ij}p_{ji})^3p_{jj}^2$, and $\ell_{(1,1)} + \ell_{(3,3)} = \ell_{(2,3)} + \ell_{(3,2)}$ by Theorem 1.1.5(2). Thus

$$\begin{aligned} A_{\underline{m}} &= \frac{\prod_{k|\gcd(2,3)}(1-Q_{\underline{m}}^{3/k})^{\ell_{(2,3)/k}} \prod_{k|\gcd(3,2)}(1-Q_{\underline{m}}^{3/k})^{\ell_{(3,2)/k}}}{\prod_{k|\gcd(3,3)}(1-Q_{\underline{m}}^{3/k})^{\ell_{(3,3)/k}}} \\ &= \frac{(1-Q_{\underline{m}}^3)^{\ell_{(2,3)}+\ell_{(3,2)}}}{(1-Q_{\underline{m}}^3)^{\ell_{(3,3)}}(1-Q_{\underline{m}})^{\ell_{(1,1)}}} = \frac{(1-Q_{\underline{m}}^3)^{\ell_{(1,1)}}}{(1-Q_{\underline{m}})^{\ell_{(1,1)}}} = (3)_{Q_{\underline{m}}} = P_{\underline{m}}. \end{aligned}$$

(5) If $\underline{m} = 3\underline{e}_i + 4\underline{e}_j$ with $1 \le i,j \le n$, $i \ne j$, then we get $N(\underline{m}) = 6$, $Q_{\underline{m}} = p_{ii}(p_{ij}p_{ji})^2 p_{jj}^2$, and $\ell_{(3,4)} = \ell_{(2,4)} + \ell_{(3,3)}$. Thus

$$\begin{aligned} A_{\underline{m}} &= \frac{\prod_{k|\gcd(2,4)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(2,4)/k}} \prod_{k|\gcd(3,3)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(3,3)/k}}}{\prod_{k|\gcd(3,4)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(3,4)/k}}} \\ &= \frac{(1-Q_{\underline{m}}^6)^{\ell_{(2,4)}}(1-Q_{\underline{m}}^3)^{\ell_{(1,2)}}(1-Q_{\underline{m}}^6)^{\ell_{(3,3)}}(1-Q_{\underline{m}}^2)^{\ell_{(1,1)}}}{(1-Q_{\underline{m}}^6)^{\ell_{(3,4)}}} \\ &= (1-Q_{\underline{m}}^2)(1-Q_{\underline{m}}^3) = (1-Q_{\underline{m}})^2(1+Q_{\underline{m}})(3)_{Q_{\underline{m}}} = (1-Q_{\underline{m}})P_{\underline{m}}. \end{aligned}$$

(6) If $\underline{m} = 3\underline{e}_i + 6\underline{e}_j$ with $1 \le i,j \le n$, $i \ne j$, then we get $N(\underline{m}) = 6$, $Q_{\underline{m}} = p_{ii}(p_{ij}p_{ji})^3 p_{jj}^5$, and $\ell_{(3,6)} + \ell_{(1,2)} = \ell_{(2,6)} + \ell_{(3,5)}$. Thus

$$\begin{aligned} A_{\underline{m}} &= \frac{\prod_{k|\gcd(2,6)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(2,6)/k}} \prod_{k|\gcd(3,5)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(3,5)/k}}}{\prod_{k|\gcd(3,6)}(1-Q_{\underline{m}}^{6/k})^{\ell_{(3,6)/k}}} \\ &= \frac{(1-Q_{\underline{m}}^6)^{\ell_{(2,6)}}(1-Q_{\underline{m}}^3)^{\ell_{(1,3)}}(1-Q_{\underline{m}}^6)^{\ell_{(3,5)}}}{(1-Q_{\underline{m}}^6)^{\ell_{(3,6)}}(1-Q_{\underline{m}}^2)^{\ell_{(1,2)}}} = \frac{(1-Q_{\underline{m}}^6)(1-Q_{\underline{m}}^3)}{1-Q_{\underline{m}}^2} \\ &= (1-Q_{\underline{m}})(3)_{Q_{\underline{m}}}^2(3)_{-Q_{\underline{m}}} = (3)_{Q_{\underline{m}}}P_{\underline{m}}. \end{aligned}$$

(7) If $\underline{m} = 4\underline{e}_i + 4\underline{e}_j$ with $1 \le i,j \le n$, $i \ne j$, then we get $N(\underline{m}) = 4$, $Q_{\underline{m}} = p_{ii}^3(p_{ij}p_{ji})^4 p_{jj}^3$, and $\ell_{(1,1)} + \ell_{(2,2)} + \ell_{(4,4)} = \ell_{(3,4)} + \ell_{(4,3)}$. Thus

$$\begin{aligned} A_{\underline{m}} &= \frac{\prod_{k|\gcd(3,4)}(1-Q_{\underline{m}}^{4/k})^{\ell_{(3,4)/k}} \prod_{k|\gcd(4,3)}(1-Q_{\underline{m}}^{4/k})^{\ell_{(4,3)/k}}}{\prod_{k|\gcd(4,4)}(1-Q_{\underline{m}}^{4/k})^{\ell_{(4,4)/k}}} \\ &= \frac{(1-Q_{\underline{m}}^4)^{\ell_{(3,4)}}(1-Q_{\underline{m}}^4)^{\ell_{(4,3)}}}{(1-Q_{\underline{m}}^4)^{\ell_{(4,4)}}(1-Q_{\underline{m}}^2)^{\ell_{(2,2)}}(1-Q_{\underline{m}})^{\ell_{(1,1)}}} = \frac{(1-Q_{\underline{m}}^4)^2}{(1-Q_{\underline{m}}^2)(1-Q_{\underline{m}})} \\ &= (1+Q_{\underline{m}}^2)^2(1+Q_{\underline{m}}) = (1+Q_{\underline{m}}^2)P_{\underline{m}} \end{aligned}$$

since $\ell_{(2,2)} = 1$.

(8) Now we suppose $\underline{m}$ is not equal to any of the above cases. By following the proof of Lemma 2.1.9 and using Theorem 1.1.5 we conclude that $Q_{\underline{m}}^{N(\underline{m})} - 1$ divides $A_{\underline{m}}$. Moreover, every irreducible factor of $A_{\underline{m}}$ is a factor of $P_{\underline{m}} = 1 - Q_{\underline{m}}^{N(\underline{m})}$. Since $P_{\underline{m}}$ is a product of pairwise non-associated irreducible factors, we conclude that $P_{\underline{m}}$ contains every irreducible factor of $A_{\underline{m}}$ precisely once.

Thus the proof is completed. □

Corollary 2.1.11. Let $\underline{m}, \underline{l} \in \mathbb{N}_0^n$ be different from $m\underline{e}_i$ for all $m \geq 0$ and $1 \leq i \leq n$. Then $A_{\underline{m}}$ and $A_{\underline{l}}$ are relatively prime if and only if $\underline{m} \neq \underline{l}$. In particular, $A_{\underline{m}}$ and $A_{\underline{l}}$ are relatively prime whenever $\underline{l} < \underline{m}$.

Proof. The claim follows from Lemma 2.1.7 and Proposition 2.1.10. □

2.2 The shuffle map over commutative rings

In this section let R be a unital commutative ring. We calculate the determinant of the shuffle map over R.

Definition 2.2.1. Let $\overline{V}$ be a finitely generated free module over R and let $\bar{c} : \overline{V} \otimes_R \overline{V} \to \overline{V} \otimes_R \overline{V}$ be an R-module endomorphism of $\overline{V} \otimes_R \overline{V}$. We say that $(\overline{V}, \bar{c})$ is a *free prebraided module of diagonal type over* R, if there exist a basis $x_1, x_2, \ldots, x_n$ of $\overline{V}$ and $(\overline{q}_{ij})_{1\leq i,j\leq n} \in R^{n\times n}$ with

$$\bar{c}(x_i \otimes x_j) = \overline{q}_{ij} x_j \otimes x_i \quad \text{for all } i, j.$$

Remark 2.2.2. If R is a field and $(\overline{V}, \bar{c})$ is a free braided free module of diagonal type over R such that $\overline{q}_{ij}$ is different from zero in R, for any $1 \leq i, j \leq n$, then $(\overline{V}, \bar{c})$ is a braided vector space of diagonal type.

Let $n \in \mathbb{N}$ and let $(\overline{V}, \bar{c})$ be a free prebraided module of diagonal type with basis $x_1, \ldots, x_n$. Let $I = \{1, 2, \ldots, n\}$ and $(\overline{q}_{ij})_{i,j\in I} \in R^{n\times n}$. Assume that

$$\bar{c}(x_i \otimes x_j) = \overline{q}_{ij} x_j \otimes x_i$$

for all $i, j \in I$. Let $\overline{V}^{\otimes k}$ denote the k-fold tensor product of $\overline{V}$ over R and let $T(\overline{V}) = \bigoplus_{k=0}^{\infty} \overline{V}^{\otimes k}$. Note that $\overline{V}^{\otimes k}$ is a free module over R for all $k \in \mathbb{N}$.

For any $\underline{m} \in \mathbb{N}^n$ let $\mathbb{X}_{\underline{m}}$ denote the set of words over I of degree $\underline{m}$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the standard basis of $\mathbb{Z}^n$. Then $T(\overline{V})$ admits a $\mathbb{Z}^n$-grading given by $\deg x_i = \alpha_i$, for all $i \in I$. Thus for any $i_1 i_2 \cdots i_l \in \mathbb{X}_{\underline{m}}$, the degree of $x_{i_1} x_{i_2} \cdots x_{i_l}$ is $\sum_{j=1}^{l} \alpha_{i_j}$, and we write $\deg x$ for the degree of any homogeneous element x of $T(\overline{V})$. For any $\underline{m} \in \mathbb{N}_0^n$ let $\overline{V}_{\underline{m}}$ denote the $\mathbb{Z}^n$-homogeneous component of $T(\overline{V})$ of degree $\underline{m}$.

For any $k \geq 2$, let $\mathbb{B}_k$ denote the monoid which is generated by generators $\sigma_1, \sigma_2, \dots \sigma_{k-1}$ and relations

(1) $\sigma_i \sigma_j = \sigma_j \sigma_i$ for $i, j \in \{1, 2, \dots, k-1\}$ with $|i - j| \geq 2$, and

(2) $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ for $1 \leq i \leq k-2$.

Let $S_{1,0} = 1 \in \mathbb{B}_k$, and for any $1 \leq m < k$ let

$$S_{1,m} = 1 + \sigma_1 + \sigma_2\sigma_1 + \cdots + \sigma_m \sigma_{m-1} \cdots \sigma_1.$$

Similarly to Lemma 2.6, we obtain the following Equation

$$(1 - \sigma_m \cdots \sigma_2 \sigma_1) S_{1,m} = S_{1,m-1}(1 - \sigma_m \cdots \sigma_2 \sigma_1^2). \tag{2.6}$$

For any $m \geq 2$ let $R\mathbb{B}_m$ denote the monoid ring of $\mathbb{B}_m$ over R and let $\overline{\rho}_m : R\mathbb{B}_m \to \mathrm{End}_R(\overline{V}^{\otimes m})$ be the ring homomorphism such that $\overline{\rho}_m(\sigma_i)$ is the prebraiding $\overline{c}$ applied to the i-th and $i+1$-th tensor factors of $\overline{V}^{\otimes m}$.

Let $f : \mathbb{Z}[p_{ij} \mid i, j \in I] \to R$ be the ring homomorphism such that

$$f(p_{ij}) = \overline{q}_{ij} \quad \text{for all } i, j \in I.$$

Lemma 2.2.3. For any $\underline{m} \in \mathbb{N}_0^n$ with $\underline{m} \neq 0$ and $m = |\underline{m}| \geq 2$ we have

$$\det(\overline{\rho}_m(1 - \sigma_{m-1} \cdots \sigma_2 \sigma_1)\big|\overline{V}_{\underline{m}}) = \prod_{k \mid \gcd(\underline{m})} (1 - f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{\underline{m}/k}}.$$

Moreover, if R is a field, $d = \mathrm{ord}(f(Q_{\underline{m}}))$, and $d \mid N(\underline{m})$, then

$$\dim(\ker(\overline{\rho}_m(1 - \sigma_{m-1} \cdots \sigma_2 \sigma_1)\big|\overline{V}_{\underline{m}})) = \sum_{k \mid \gcd(\underline{m}), k \mid N(\underline{m})/d} \ell_{\underline{m}/k}.$$

Proof. Consider the action of $\mathbb{Z}$ on $\mathbb{X}_{\underline{m}}$ given by

$$1 \cdot i_1 \cdots i_m = i_2 \cdots i_m i_1.$$

In any $\mathbb{Z}$-orbit of $\mathbb{X}_{\underline{m}}$ there is a unique element v^k, where v is a Lyndon word and $k \in \mathbb{N}$ with $k | m_i$ for each $1 \leq i \leq n$.

To any $\mathbb{Z}$-orbit $\mathcal{O}$ of $\mathbb{X}_{\underline{m}}$ we attach the submodule $\overline{V}_{\mathcal{O}}$ of $\overline{V}_{\underline{m}}$ generated by $x_{i_1}x_{i_2}\cdots x_{i_m}$ with $i_1i_2\cdots i_m\in\mathcal{O}$. Then

$$\overline{V}_{\underline{m}}=\bigoplus_{\mathcal{O}}\overline{V}_{\mathcal{O}}. \tag{2.7}$$

Let $\mathcal{O}$ be a $\mathbb{Z}$-orbit and let $k\geq 1$ and $v=i_1i_2\cdots i_l$ be the Lyndon word such that $v^k\in\mathcal{O}$. Then $l=m/k$. Let $\widetilde{v}=x_{i_1}x_{i_2}\cdots x_{i_l}\in T(\overline{V})$. Then

$$x_{i_t}x_{i_{t+1}}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}},\quad 1\leq t\leq l, \tag{2.8}$$

is a basis of $\overline{V}_{\mathcal{O}}$, where $x_{i_1}\cdots x_{i_0}=1$. Moreover, for all $1\leq t\leq l$,

$$\begin{aligned}&\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)(x_{i_t}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}})\\&=x_{i_t}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}}-\lambda_t x_{i_{t+1}}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_t},\end{aligned}$$

where $\lambda_t=\overline{q}^k_{i_ti_1}\overline{q}^k_{i_ti_2}\cdots\overline{q}^k_{i_ti_{t-1}}\overline{q}^{k-1}_{i_ti_t}\overline{q}^k_{i_ti_{t+1}}\cdots\overline{q}^k_{i_ti_l}$ and $x_{i_{t+1}}\cdots x_{i_t}=1$.

We obtain that the matrix of $\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)\big|\overline{V}_{\mathcal{O}}$ with respect to the basis (2.8) is $A=(a_{st})_{1\leq s,t\leq l}$, where

$$a_{st}=\begin{cases}1 & \text{if } s=t,\\ -\lambda_t & \text{if } s=t+1,\ 1\leq t\leq l-1,\\ -\lambda_l & \text{if } s=1,\ t=l,\\ 0 & \text{otherwise.}\end{cases}$$

Therefore,

$$\begin{aligned}&\det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)\big|\overline{V}_{\mathcal{O}})\\&=1+(-1)^{l+1}(-1)^l\lambda_1\lambda_2\cdots\lambda_l\\&=1-\prod_{1\leq t\leq l}\overline{q}^{k-1}_{i_ti_t}\prod_{1\leq t<s\leq l}(\overline{q}_{i_ti_s}\overline{q}_{i_si_t})^k\\&=1-\prod_{1\leq t\leq n}\overline{q}_{tt}^{m_t(m_t-1)/k}\prod_{1\leq t<s\leq n}(\overline{q}_{st}\overline{q}_{ts})^{m_tm_s/k}\\&=1-f(Q_{\underline{m}})^{N(\underline{m})/k}.\end{aligned}$$

Hence

$$\det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)\big|\overline{V}_{\underline{m}}) = \prod_{k|\gcd(\underline{m})}(1-f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{\underline{m}/k}}$$

because of the decomposition of $\overline{V}_{\underline{m}}$ in (2.7).

If R is a field, then the matrix A above has corank 0 or 1. Moreover, A has corank 1 if and only if $f(Q_{\underline{m}})^{N(\underline{m})/k}=1$, that is, if and only if $d \mid N(\underline{m})/k$, where $d=\mathrm{ord}(f(Q_{\underline{m}}))$. This implies the last claim. □

Lemma 2.2.4. For any $\underline{m}\in\mathbb{N}_0^n$ with $m=|\underline{m}|\geq 2$ we have

$$\det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)\big|\overline{V}_{\underline{m}}) = \prod_{i:m_i>0}\prod_{k|\gcd(\underline{m}-\underline{e}_i)}(1-f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{(\underline{m}-\underline{e}_i)/k}}.$$

Moreover, if R is a field, $d=\mathrm{ord}(f(Q_{\underline{m}}))$, and $d\mid N(\underline{m})$, then

$$\dim(\ker(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)\big|\overline{V}_{\underline{m}})) = \sum_{i:m_i>0}\sum_{k|\gcd(\underline{m}-\underline{e}_i),k|N(\underline{m})/d}\ell_{(\underline{m}-\underline{e}_i)/k}.$$

Proof. Let us consider the $\mathbb{Z}$-action on $\mathbb{X}_{\underline{m}}$ given by

$$1\cdot i_1i_2\cdots i_m = i_1i_3i_4\cdots i_mi_2.$$

Then $(m-1)\cdot i_1i_2\cdots i_m = i_1i_2\cdots i_m$. In any $\mathbb{Z}$-orbit of $\mathbb{X}_{\underline{m}}$ there is a unique element jv^k, where $j\in I$, v is a Lyndon word, and $k\geq 1$. Moreover, then $k\mid m_j-1$ and $k\mid m_t$ for each $1\leq t\leq n$ with $t\neq j$.

Again, to any $\mathbb{Z}$-orbit $\mathcal{O}$ we attach the submodule $\overline{V}_{\mathcal{O}}$ of $\overline{V}_{\underline{m}}$ generated by the monomials $x_{i_1}\cdots x_{i_m}$, where $i_1\cdots i_m\in\mathcal{O}$. Then

$$\overline{V}_{\underline{m}} = \bigoplus_{\mathcal{O}}\overline{V}_{\mathcal{O}}. \tag{2.9}$$

Let $v=i_1i_2\cdots i_l$ be a Lyndon word, $j\in\{1,\dots,n\}$, and $k\geq 1$. Assume that $\deg jv^k=\underline{m}$. Then $l=(m-1)/k$. Let $\widetilde{v}=x_{i_1}\cdots x_{i_l}\in T(\overline{V})$. Then the monomials

$$x_jx_{i_t}x_{i_{t+1}}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}},\quad 1\leq t\leq l, \tag{2.10}$$

form a basis of $\overline{V}_{\mathcal{O}}$ for the $\mathbb{Z}$-orbit $\mathcal{O}$ of jv^k, where $x_{i_1}\cdots x_{i_0}=1$.

For any $1\le t\le l$ one obtains that

$$\begin{aligned}&\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)(x_jx_{i_t}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}})\\&=x_jx_{i_t}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_{t-1}}-\overline{q}_{ji_t}\overline{q}_{i_tj}\lambda_tx_jx_{i_{t+1}}\cdots x_{i_l}\widetilde{v}^{k-1}x_{i_1}\cdots x_{i_t},\end{aligned}$$

where $x_{i_{l+1}}\cdots x_{i_l}=1$ and $\lambda_t=\overline{q}^k_{i_ti_1}\overline{q}^k_{i_ti_2}\cdots\overline{q}^k_{i_ti_{t-1}}\overline{q}^{k-1}_{i_ti_t}\overline{q}^k_{i_ti_{t+1}}\cdots\overline{q}^k_{i_ti_l}$ for all $1\le t\le l$. Thus the matrix of $\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)|\overline{V}_{\mathcal{O}}$ with respect to the basis (2.10) is $B=(b_{st})_{1\le s,t\le l}$, where

$$b_{st}=\begin{cases}1 & \text{if } s=t,\\ -\overline{q}_{ji_t}\overline{q}_{i_tj}\lambda_t & \text{if } s=t+1,\ 1\le t\le l-1,\\ -\overline{q}_{ji_l}\overline{q}_{i_lj}\lambda_l & \text{if } s=1,\ t=l,\\ 0 & \text{otherwise.}\end{cases}$$

Hence,

$$\begin{aligned}&\det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)\big|\overline{V}_{\mathcal{O}})\\&=1+(-1)^{l+1}(-1)^l\overline{q}_{ji_1}\overline{q}_{i_1j}\cdots\overline{q}_{ji_l}\overline{q}_{i_lj}\lambda_1\lambda_2\cdots\lambda_l\\&=1-\prod_{1\le t\le l}(\overline{q}_{ji_t}\overline{q}_{i_tj})\prod_{1\le t\le l}\overline{q}^{k-1}_{i_ti_t}\prod_{1\le t<s\le l}(\overline{q}_{i_ti_s}\overline{q}_{i_si_t})^k\\&=1-\prod_{1\le t\le n}\overline{q}_{tt}^{m_t(m_t-1)/k}\prod_{1\le t<s\le n}(\overline{q}_{st}\overline{q}_{ts})^{m_tm_s/k}\\&=1-f(Q_{\underline{m}})^{N(\underline{m})/k}.\end{aligned}$$

This implies the first claim.

If R is a field, then the matrix B above has corank 0 or 1. Moreover, B has corank 1 if and only if $f(Q_{\underline{m}})^{N(\underline{m})/k}=1$, that is, if and only if $d\mid N(\underline{m})/k$, where $d=\operatorname{ord}(f(Q_{\underline{m}}))$. This implies the last claim. □

Lemma 2.2.5. Let $\underline{m}\in\mathbb{N}_0^n$ with $m=|\underline{m}|\ge 2$. Then

$$\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})\prod_{k|\gcd(\underline{m})}(1-f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{\underline{m}/k}}$$

$$= \prod_{i:m_i>0} \Big(\det(\overline{\rho}_{m-1}(S_{1,m-2})|\overline{V}_{\underline{m}-\underline{e}_i}) \prod_{k|\gcd(\underline{m}-\underline{e}_i)} (1 - f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{(\underline{m}-\underline{e}_i)/k}} \Big).$$

Proof. From Equation (2.6) we conclude that

$$\begin{aligned} &\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}) \det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)|\overline{V}_{\underline{m}}) \\ &= \det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}) \det(\overline{\rho}_m(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)|\overline{V}_{\underline{m}}). \end{aligned}$$

Because of Lemma 2.2.3 and 2.2.4 the above equality is equivalent to

$$\begin{aligned} &\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}) \prod_{k|\gcd(\underline{m})} (1 - f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{\underline{m}/k}} \\ &= \det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}) \prod_{i:m_i>0} \prod_{k|\gcd(\underline{m}-\underline{e}_i)} (1 - f(Q_{\underline{m}})^{N(\underline{m})/k})^{\ell_{(\underline{m}-\underline{e}_i)/k}}. \end{aligned}$$

This implies the lemma. □

Proposition 2.2.6. Let $\underline{m} = (m_1, \dots, m_n) \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$.

(1) If $\underline{m} = m_i \underline{e}_i$ with $1 \leq i \leq n$ then $\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}} = (m_i)_{\overline{q}_{ii}}\mathrm{id}$.

(2) If there exist $1 \leq i < j \leq n$ with $m_i, m_j \neq 0$, then

$$\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}) = f(A_{\underline{m}}) \prod_{i:m_i>0} \det(\overline{\rho}_{m-1}(S_{1,m-2})|\overline{V}_{\underline{m}-\underline{e}_i}). \tag{2.11}$$

Proof. Claim (1) follows directly from the definition of $S_{1,m-1}$.

In order to prove part (2) of the Proposition it suffices to consider the polynomial ring $R = \mathbb{Z}[p_{ij} \mid 1 \leq i,j \leq n]$ and $f = \mathrm{id}$. In this case the claim follows from Lemma 2.2.5 and Lemma 2.1.9. □

2.3 Nichols algebras which are free algebras

In the remaining part of this chapter let $\Bbbk$ be a field, let $\Bbbk^\times = \Bbbk \setminus \{0\}$, and let (V, c) be an n-dimensional braided vector space of diagonal type with basis

$x_1, x_2, \ldots, x_n$ and braiding matrix $\boldsymbol{q} \in (\Bbbk^\times)^{n\times n}$. Let $T(V)$ and $\mathcal{B}(V)$ denote the tensor algebra and the Nichols algebra of V, respectively.

In this section we determine when $\mathcal{B}(V)$ is a free algebra, that is, $\mathcal{B}(V) = T(V)$.

Recall that for all $m \geq 2$ $\rho_m : \Bbbk\mathbb{B}_m \longrightarrow \mathrm{End}(V^{\otimes m})$ is the representation of $\Bbbk\mathbb{B}_m$ introduced in Section 1.3.

Lemma 2.3.1. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$.

(1) If $P_{\underline{m}}(\boldsymbol{q}) = 0$, then $\det(\rho_m(S_{1,m-1})|V_{\underline{m}}) = 0$.

(2) If $\det(\rho_m(S_{1,m-2})|V_{\underline{m}}) \neq 0$ and $\det(\rho_m(S_{1,m-1})|V_{\underline{m}}) = 0$ then $P_{\underline{m}}(\boldsymbol{q}) = 0$.

Proof. If $\underline{m} = m_i\underline{e}_i$ for some $1 \leq i \leq n$, $m_i \in \mathbb{N}$, then the claim holds because of Proposition 2.2.6(1).

Assume now that there exist $1 \leq i < j \leq n$ with $m_i, m_j \neq 0$. Then Proposition 2.1.10 implies that $A_m(\boldsymbol{q}) = 0$ if and only if $P_{\underline{m}}(\boldsymbol{q}) = 0$. Hence the lemma follows from Proposition 2.2.6(2). □

Proposition 2.3.2. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$.

(1) If $P_{\underline{m}}(\boldsymbol{q}) = 0$, then there is a non-trivial relation in $\mathcal{B}(V)$ of degree $\underline{m}$.

(2) If $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} \leq \underline{m}$ with $|\underline{l}| \geq 2$, then there is no non-trivial relation in $\mathcal{B}(V)$ of degree $\underline{m}$.

Proof. (1) Assume that $P_{\underline{m}}(\boldsymbol{q}) = 0$. Then $\det(\rho_m(S_{1,m-1})|V_{\underline{m}}) = 0$ by Lemma 2.3.1(1). Thus $\det(\rho_m(S_m)|V_{\underline{m}}) = 0$ by the definition of S_m, and the claim follows from Proposition 1.3.1.

(2) Assume that the Nichols algebra $\mathcal{B}(V)$ has a non-trivial relation in degree $\underline{m}$. Let $\underline{l} \leq \underline{m}$ be such that $\mathcal{B}(V)$ has a non-trivial relation in degree $\underline{l}$ and no non-trivial relation in any degree $< \underline{l}$. Let $l = |\underline{l}|$. Then $l \geq 2$, $\ker(\rho_l(S_{1,l-2})|V_{\underline{l}}) = 0$, and $\ker(\rho_l(S_{1,l-1})|V_{\underline{l}}) \neq 0$ by Proposition 1.3.1 and by the definition of S_l. Hence $P_{\underline{l}}(\boldsymbol{q}) = 0$ by Lemma 2.3.1(2). This proves (2). □

Based on the above proposition we obtain our first main Theorem as follows.

Theorem 2.3.3. We have $\mathcal{B}(V) = T(V)$ if and only if $P_{\underline{m}}(\boldsymbol{q}) \neq 0$ for all $\underline{m} \in \mathbb{N}^n$ with $|\underline{m}| \geq 2$.

Proof. The claim follows immediately from Proposition 2.3.2. □

Example 2.3.4. (Diophantine equation) Assume that the characteristic of $\Bbbk$ is neither 2 nor 3 and that $\boldsymbol{q} = (q^{a_{ij}})_{i,j\in I}$ with $q \in \Bbbk^\times$ not a root of 1 and $(a_{ij})_{i,j\in I} \in \mathbb{Z}^{n\times n}$. For any $\underline{m} = (m_1, \dots, m_n) \in \mathbb{N}_0^n$ let

$$K(\underline{m}) = \sum_{i,j=1}^{n} a_{ij} m_i m_j, \quad \lambda(\underline{m}) = \sum_{i=1}^{n} a_{ii} m_i.$$

Then $P_{\underline{m}}(\boldsymbol{q}) \neq 0$ in the following cases:

(1) $\underline{m} = m\underline{e}_i$, $m \geq 2$, $1 \leq i \leq n$,

(2) $\underline{m} = 2\underline{e}_i + 2m\underline{e}_j$, $m \geq 1$, $i, j \in I$, $i \neq j$,

(3) $\underline{m} = 3\underline{e}_i + 3\underline{e}_j$ or $\underline{m} = 4\underline{e}_i + 4\underline{e}_j$, $i, j \in I$, $i \neq j$.

Moreover, for any other $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$,

$$P_{\underline{m}}(\boldsymbol{q}) = 0 \text{ if and only if } K(\underline{m}) = \lambda(\underline{m}).$$

Hence, by Theorem 2.3.3, $\mathcal{B}(V) = T(V)$ if and only if there is no solution of the diophantine equation $K(\underline{m}) = \lambda(\underline{m})$ with $\underline{m} \in \mathbb{N}_0^n$, $|\underline{m}| \geq 2$, $\underline{m} \notin \{m\underline{e}_i \mid m \geq 2\} \cup \{2\underline{e}_i + 2m\underline{e}_j, 3\underline{e}_i + 3\underline{e}_j, 4\underline{e}_i + 4\underline{e}_j \mid m \geq 1, i, j \in I, i \neq j\}$.

We now provide concrete examples of Nichols algebras of diagonal type which are identified by this example as a free algebra. Let $n = 2$ and let a, b be positive integers with $a > b$. Let $q \in \Bbbk^\times$ be not a root of 1 and let $\boldsymbol{q} = (q_{ij})_{1\leq i,j\leq 2}$ with $q_{11} = q_{22} = q^a$ and $q_{12}, q_{21} \in q^{\mathbb{Z}}$ with $q_{12}q_{21} = q^{-b}$. For any $\underline{m} = (m_1, m_2) \in \mathbb{N}_0^2$ with $|\underline{m}| \geq 2$ we have

$$K(\underline{m}) = am_1^2 - bm_1m_2 + am_2^2, \quad \lambda(\underline{m}) = am_1 + am_2$$

and hence

$$K(\underline{m}) - \lambda(\underline{m}) = am_1^2 - bm_1m_2 + am_2^2 - (am_1 + am_2)$$

$$= a(m_1 - m_2)(m_1 - m_2 - 1) + (2a - b)m_2\Big(m_1 - 2 + \frac{2(a-b)}{2a-b}\Big).$$

Assume that $K(\underline{m}) = \lambda(\underline{m})$ and $m_1, m_2 > 0$. By symmetry of m_1, m_2, without loss of generality we may assume that $m_1 \geq m_2$. Then

$$2(m_1 - m_2)(m_1 - m_2 - 1) \geq 0, \quad m_2 > 0,$$

and $m_1 - 2 + \frac{2(a-b)}{2a-b} > m_1 - 2 \geq 0$ for $m_1 \geq 2$ since $a > b$. Hence $K(\underline{m}) = \lambda(\underline{m})$ implies that $m_1 = 1$ and hence $m_2 = 1$. However, $K(1,1) - \lambda(1,1) = -b \neq 0$. Therefore $K(\underline{m}) \neq \lambda(\underline{m})$ for all pairs $\underline{m} = (m_1, m_2)$ with $m_1, m_2 > 0$. Thus $\mathcal{B}(V) = T(V)$.

2.4 An upper bound on the dimension of the kernel of the shuffle map

Let $n \in \mathbb{N}$, $I = \{1, 2, \dots, n\}$, and let $R = \mathbb{Z}[\bar{q}_{ij}^{\pm 1} \mid i, j \in I]$. Let $(\overline{V}, \bar{c})$ be the free prebraided module of diagonal type over R with basis $\bar{x}_1, \bar{x}_2, \dots, \bar{x}_n$ and braiding matrix $\bar{\boldsymbol{q}} = (\bar{q}_{ij})_{i,j \in I}$ such that

$$\bar{c}(\bar{x}_i \otimes \bar{x}_j) = \bar{q}_{ij}\bar{x}_j \otimes \bar{x}_i.$$

Assume that $\mathrm{char}(\Bbbk) = 0$. Let (V, c) be an n-dimensional braided vector space over $\Bbbk$ with braiding matrix $\boldsymbol{q} = (q_{ij})_{i,j \in I}$ and with basis $x_1, x_2, \dots, x_n$ such that

$$c(x_i \otimes x_j) = q_{ij}x_j \otimes x_i \quad \text{for all } i, j \in I.$$

There are unique ring homomorphisms

$$\begin{aligned} \eta &: R \to \Bbbk, \\ \eta' &: \mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n] \to R, \\ \eta'' = \eta\eta' &: \mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n] \to \Bbbk \end{aligned}$$

with $\eta(\bar{q}_{ij}) = q_{ij}$, $\eta'(p_{ij}) = \bar{q}_{ij}$ for all $i, j \in I$. We view them as evaluation at $\boldsymbol{q}$, $\bar{\boldsymbol{q}}$, and $\boldsymbol{q}$, respectively. Correspondingly, we write

$$\eta(\bar{p}) = \bar{p}(\boldsymbol{q}), \quad \eta'(p) = p(\bar{\boldsymbol{q}}), \quad \eta''(p) = p(\boldsymbol{q})$$

for any $p \in \mathbb{Z}[p_{ij} \mid 1 \leq i, j \leq n]$ and any $\bar{p} \in R$.

Let $(\alpha_{ij})_{i,j \in I}$ be a basis of $\mathbb{Z}^{n \times n}$. For any $\alpha = \sum_{i,j \in I} a_{ij}\alpha_{ij}$ let

$$\bar{q}_\alpha = \prod_{i,j \in I} \bar{q}_{ij}^{a_{ij}} \in R, \quad q_\alpha = \bar{q}_\alpha(\boldsymbol{q}) = \prod_{i,j \in I} q_{ij}^{a_{ij}} \in \Bbbk^\times.$$

Lemma 2.4.1. Let $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$. Let $\eta_1 : \Bbbk[t, t^{-1}] \to \Bbbk$ be the ring homomorphism given by

$$\eta_1(t) = Q_{\underline{m}}(\boldsymbol{q}).$$

Then there exists a ring homomorphism $\eta_2 : R \to \Bbbk[t, t^{-1}]$ such that

$$\eta_2(Q_{\underline{m}}(\bar{\boldsymbol{q}})) = t, \quad \eta_1\eta_2 = \eta.$$

Proof. By Remark 2.1.2 and Lemma 2.1.5, there exists a ring automorphism φ of R with

$$\varphi(\bar{q}_{11}) = \prod_{i=1}^{n} \bar{q}_{ii}^{m_i(m_i-1)} \prod_{1 \leq i < j \leq n} (\bar{q}_{ij}\bar{q}_{ji})^{m_i m_j}.$$

Let $\eta_2' : R \to \Bbbk[t, t^{-1}]$ be the ring homomorphism with $\eta_2'(\bar{q}_{11}) = t$, $\eta_2'(\bar{q}_{ij}) = \varphi(\bar{q}_{ij})(\boldsymbol{q})$ for all $i, j \in I$ with $(i, j) \neq (1, 1)$. Then

$$\eta_2 = \eta_2'\varphi^{-1} : R \to \Bbbk[t, t^{-1}]$$

is a ring homomorphism and

$$\begin{aligned} \eta_2(Q_{\underline{m}}(\bar{\boldsymbol{q}})) &= \eta_2'\varphi^{-1}\varphi(\bar{q}_{11}) = t, \\ \eta_1\eta_2(\varphi(\bar{q}_{11})) &= \eta_1\eta_2(Q_{\underline{m}}(\bar{q})) = \eta_1(t) = Q_{\underline{m}}(\boldsymbol{q}), \\ \eta_1\eta_2(\varphi(\bar{q}_{ij})) &= \eta_1\eta_2'(\bar{q}_{ij}) = \eta_1(\varphi(\bar{q}_{ij})(\boldsymbol{q})) = \varphi(\bar{q}_{ij})(\boldsymbol{q}) \end{aligned}$$

for all $i, j \in I$ with $(i, j) \neq (1, 1)$. Thus $\eta_1\eta_2 = \eta$. □

Lemma 2.4.2. Let $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \geq 2$. Assume that $P_{\underline{m}}(\boldsymbol{q}) = 0$. Then $Q_{\underline{m}}(\boldsymbol{q})^{N(\underline{m})} = 1$. Let $d = \operatorname{ord}(Q_{\underline{m}}(\boldsymbol{q}))$. Then $\Phi_d(Q_{\underline{m}})$ is the unique irreducible factor f of $P_{\underline{m}} \in \mathbb{Z}[p_{ij} | i, j \in I]$ such that $f(\boldsymbol{q}) = 0$.

Proof. The claim follows directly from Remark 2.1.2 and Lemma 2.1.6. □

Lemma 2.4.3. *Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$. Assume that $P_{\underline{m}}(\boldsymbol{q}) = 0$. Let $d = \mathrm{ord}(Q_{\underline{m}}(\boldsymbol{q}))$ and $d' = N(\underline{m})/d$. Then*

(1) *$\Phi_d(Q_{\underline{m}}(\bar{\boldsymbol{q}}))$ does not appear in the prime decomposition of the polynomial $\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}) \in R$, and*

(2) *$\Phi_d(Q_{\underline{m}}(\bar{\boldsymbol{q}}))$ appears $n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$ times in the prime decomposition of $\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})$, where*

$$n_1(\boldsymbol{q}) = \sum_{i:m_i>0} \sum_{k|\gcd(\underline{m}-\underline{e}_i),k|d'} \ell_{(\underline{m}-\underline{e}_i)/k},$$

and

$$n_2(\boldsymbol{q}) = \sum_{k|\gcd(\underline{m}),k|d'} \ell_{\underline{m}/k}.$$

Proof. Assume first that $\underline{m} = m\underline{e}_i$ for some $i \in I$. Then $Q_{\underline{m}} = p_{ii}$, $P_{\underline{m}} = (m)_{p_{ii}}$, $N(\underline{m}) = m(m-1)$, $q_{ii} \neq 1$, and $d \mid m$, $d > 1$. Hence $\gcd(m-1, d') = m-1$, $\gcd(m, d') = m/d$, and therefore

$$\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}) = (m)_{\bar{q}_{ii}}, \quad n_1(\boldsymbol{q}) = 1, \quad n_2(\boldsymbol{q}) = 0$$

by Proposition 2.2.6(1) and Remark 1.1.4. Thus (2) holds in this case. Moreover, (1) is valid since $\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}) = (m-1)_{\bar{q}_{ii}}$ and d does not divide $m-1$.

Assume that there exists $1 \leq i < j \leq n$ with $m_i, m_j \neq 0$. Since $P_{k\underline{e}_i} = \det(\overline{\rho}_k(S_{1,k-1})|\overline{V}_{k\underline{e}_i})$ for all $k \geq 2$ and $i \in I$, Propositions 2.2.6(2) and 2.1.10 imply that any irreducible factor of $\det(\overline{\rho}_{m-1}(S_{1,m-2})|\overline{V}_{\underline{m}})$ is an irreducible factor of some $P_{\underline{l}}$ with $\underline{l} < \underline{m}$. Thus, by Proposition 2.1.10 and Lemma 2.1.7, $\Phi_d(Q_{\underline{m}}(\bar{\boldsymbol{q}}))$ and $\det(\overline{\rho}_{m-1}(S_{1,m-2})|\overline{V}_{\underline{m}})$ are relatively prime, which proves (1). By Proposition 2.2.6(2), for the proof of (2) it remains to determine the multiplicity of the irreducible factor $\Phi_d(Q_{\underline{m}})$ in $A_{\underline{m}}$. Let $k \in \mathbb{N}$ with $k|N(\underline{m})$. By Lemma 2.1.6, $\Phi_d(Q_{\underline{m}})$ has multiplicity 0 in $Q^{N(\underline{m})/k} - 1$, except when $k \mid d'$, in which case it has multiplicity 1. By Definition 2.1.8, there are

$$n_1(\boldsymbol{q}) = \sum_{i:m_i>0} \sum_{k|\gcd(\underline{m}-\underline{e}_i),k|d'} \ell_{(\underline{m}-\underline{e}_i)/k}$$

factors $\Phi_d(Q_{\underline{m}})$ in the numerator of $A_{\underline{m}}$ and

$$n_2(\boldsymbol{q}) = \sum_{k|\gcd(\underline{m}),k|d'} \ell_{\underline{m}/k}$$

factors $\Phi_d(Q_{\underline{m}})$ in the denominator of $A_{\underline{m}}$. This proves the lemma. $\square$

Note that under the hypothesis of Lemma 2.4.3, the two numbers $n_1(\boldsymbol{q})$ and $n_2(\boldsymbol{q})$ are the dimensions of kernels of $\rho(1-\sigma_{m-1}\cdots\sigma_2\sigma_1^2)$ and $\rho(1-\sigma_{m-1}\cdots\sigma_2\sigma_1)$, respectively.

Lemma 2.4.4. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$. Suppose that $P_{\underline{m}}(\boldsymbol{q}) = 0$ and $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} < \underline{m}$. Let $\eta_1 : \Bbbk[t, t^{-1}] \to \Bbbk$ and $\eta_2 : R \to \Bbbk[t, t^{-1}]$ be ring homomorphisms as in Lemma 2.4.1. Then the following hold,

(1) $\eta_1\eta_2(\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}})) \neq 0$ in $\Bbbk$,

(2) the polynomials $t - Q_{\underline{m}}(\boldsymbol{q})$ and $\eta_2(\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}))$ are relatively prime in $\Bbbk[t, t^{-1}]$, and

(3) the factor $t - Q_{\underline{m}}(\boldsymbol{q}) \in \Bbbk[t, t^{-1}]$ appears $n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$ times in the prime decomposition of $\eta_2(\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}))$.

Proof. (1) By Lemma 2.4.1, we have

$$\begin{aligned}\eta_1\eta_2(\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}})) =& \eta(\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}})) \\ =& \det(\rho_m(S_{1,m-2})|V_{\underline{m}}).\end{aligned}$$

As $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} < \underline{m}$, we get $\det(\rho_m(S_{1,m-2})|V_{\underline{m}}) \in \Bbbk^\times$ because of Proposition 2.3.2.

(2) By definition, $\eta_1(t - Q_{\underline{m}}(\boldsymbol{q})) = 0$. Thus (2) follows from (1).

(3) Assume first that $\underline{m} = m\underline{e}_i$ for some $i \in I$. Then

$$Q_{\underline{m}} = p_{ii},\ \overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}} = (m)_{\bar{q}_{ii}}\mathrm{id}$$

by Proposition 2.2.6(1), and hence

$$\eta_2(\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})) = (m)_t.$$

Since $(m)_{q_{ii}} = 0$ in $\Bbbk$ and $\mathrm{char}(\Bbbk) = 0$, the irreducible factor $t - q_{ii}$ appears once in $(m)_t$. Moreover, $n_1(\boldsymbol{q}) = 1$ and $n_2(\boldsymbol{q}) = 0$, see the first part of the proof of Lemma 2.4.3.

Assume now that there exist $1 \le i < j \le n$ with $m_i, m_j \ne 0$. By (1), $t - Q_{\underline{m}}(\boldsymbol{q})$ does not appear in the prime decomposition of $\eta_2(\det(\overline{\rho}_m(S_{1,m-2})|\overline{V}_{\underline{m}}))$. Hence, by Proposition 2.2.6(2), we have to determine the multiplicity M of $t - Q_{\underline{m}}(\boldsymbol{q})$ in the prime decomposition of $\eta_2(A_{\underline{m}}(\bar{\boldsymbol{q}}))$. By the definition of $A_{\underline{m}}$ and by Lemma 2.1.9, $\eta_2(A_{\underline{m}}(\bar{\boldsymbol{q}}))$ is a non-zero polynomial in $\Bbbk[t, t^{-1}]$. By Remark 2.1.2 and by Proposition 2.1.10, $A_{\underline{m}}$ is a product of polynomials of the form $\Phi_k(Q_{\underline{m}})$ with $k \mid N(\underline{m})$. Hence $\eta_2(A_{\underline{m}}(\bar{\boldsymbol{q}}))$ is a product of polynomials of the form $\Phi_k(t)$ with $k \mid N(\underline{m})$, and the multiplicity of $\Phi_k(t)$ with $k \mid N(\underline{m})$ in $\eta_2(A_{\underline{m}}(\bar{\boldsymbol{q}}))$ is the same as the multiplicity of $\Phi_k(Q_{\underline{m}})$ in $A_{\underline{m}}$. Let $d = \mathrm{ord}(Q_{\underline{m}}(\boldsymbol{q}))$. Then $t - Q_{\underline{m}}(\boldsymbol{q})$ divides $\Phi_k(t)$ if and only if $k = d$. Hence M is the multiplicity of $\Phi_d(Q_{\underline{m}})$ in $A_{\underline{m}}$. Therefore, by Proposition 2.2.6(2) and by Lemma 2.4.3, M is the multiplicity of $\Phi_d(Q_{\underline{m}}(\bar{\boldsymbol{q}}))$ in $\det(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})$, that is, $M = n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$. □

Proposition 2.4.5. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \ge 2$. Suppose that $P_{\underline{m}}(\boldsymbol{q}) = 0$ and that $P_{\underline{l}}(\boldsymbol{q}) \ne 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \ge 2$. Then

$$\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) \le n_1(\boldsymbol{q}) - n_2(\boldsymbol{q}).$$

Proof. Let $\eta_1 : \Bbbk[t, t^{-1}] \to \Bbbk$ and $\eta_2 : R \to \Bbbk[t, t^{-1}]$ be ring homomorphisms as in Lemma 2.4.1. Let M be the Smith normal form of $\eta_2(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})$, which is a diagonal matrix. Then $\det(M) = \det(\eta_2(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}})) \ne 0$ by Lemma 2.4.4(3), and hence there is no zero on the diagonal of M. Again by Lemma 2.4.4(3), $t - Q_{\underline{m}}(\boldsymbol{q})$ appears $n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$ times in the prime decomposition of $\det(M)$. Hence $t - Q_{\underline{m}}(\boldsymbol{q})$ appears in at most $n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$ diagonal entries of M as an irreducible factor. Then

$$\begin{aligned}\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) &= \dim(\ker(\eta_1\eta_2(\overline{\rho}_m(S_{1,m-1})|\overline{V}_{\underline{m}}))) \\ &= \dim(\ker(\eta_1(M)) \le n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})).\end{aligned}$$

Hence the proposition holds. □

2.5 The dimension of the kernel of shuffle map

We use some notation and conventions from the previous section. So let us assume that $\mathrm{char}(\Bbbk) = 0$. Let $n \in \mathbb{N}$, let $\boldsymbol{q} = (q_{ij})_{1\le i,j\le n} \in (\Bbbk^\times)^{n\times n}$, and let (V, c) be a braided vector space of diagonal type with basis $x_1, \dots, x_n$ such that $c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i$ for all $1 \le i, j \le n$. For each $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \ge 2$ let $n_1(\boldsymbol{q}), n_2(\boldsymbol{q}) \ge 0$ be the integers defined in Lemma 2.4.3(2).

In this section we determine the dimension of the kernel of the shuffle map $\rho_{|\underline{m}|}(S_{1,|\underline{m}|-1})|V_{\underline{m}}$ for those $\underline{m} \in \mathbb{N}_0^n$ with $|\underline{m}| \ge 2$, $P_{\underline{m}}(\boldsymbol{q}) = 0$, and $P_{\underline{l}}(\boldsymbol{q}) \ne 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \ge 2$.

Proposition 2.5.1. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \ge 2$. Suppose that $P_{\underline{m}}(\boldsymbol{q}) = 0$ and $P_{\underline{l}}(\boldsymbol{q}) \ne 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \ge 2$. Then

$$\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) \ge n_1(\boldsymbol{q}) - n_2(\boldsymbol{q}),$$

Proof. Since $P_{\underline{l}}(\boldsymbol{q}) \ne 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \ge 2$, it follows from Proposition 2.3.2 that $\rho_m(S_{1,m-2})|V_{\underline{m}}$ is injective. Hence

$$\begin{aligned}\ker(\rho_m(1 - \sigma_{m-1}\cdots\sigma_2\sigma_1)\rho_m(S_{1,m-1})|V_{\underline{m}})\\ = \ker(\rho_m(1 - \sigma_{m-1}\cdots\sigma_2\sigma_1^2)|V_{\underline{m}})\end{aligned}$$

because of Lemma 2.6. Therefore

$$\begin{aligned}\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) + \dim(\ker(\rho_m(1 - \sigma_{m-1}\cdots\sigma_2\sigma_1)|V_{\underline{m}}))\\ \ge \dim(\ker(\rho_m(1 - \sigma_{m-1}\cdots\sigma_2\sigma_1^2)|V_{\underline{m}})),\end{aligned}$$

that is,

$$\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) + n_2(\boldsymbol{q}) \ge n_1(\boldsymbol{q})$$

because of Lemmas 2.2.3 and 2.2.4. This proves the Proposition. □

Theorem 2.5.2. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \ge 2$. Assume that $P_{\underline{m}}(\boldsymbol{q}) = 0$ and $P_{\underline{l}}(\boldsymbol{q}) \ne 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \ge 2$. Then

$$\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) = n_1(\boldsymbol{q}) - n_2(\boldsymbol{q}).$$

Proof. The theorem follows immediately from Propositions 2.4.5 and Proposition 2.5.1. □

Remark 2.5.3. Let $\underline{m} \in \mathbb{N}_0^n$ with $m = |\underline{m}| \geq 2$. Assume $\ker(\rho_k(S_k)|V_{\underline{l}}) = 0$ for all $\underline{l} < \underline{m}$ with $k = |\underline{l}| \geq 2$. Then $\ker(\rho_k(S_{1,k-1})|V_{\underline{l}}) = 0$ for all $\underline{l} < \underline{m}$ with $k = |\underline{l}| \geq 2$ by the definition of S_k. Moreover, $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \geq 2$ by Proposition 2.3.2(1). Assume now that $\dim(\ker(\rho_m(S_m)|V_{\underline{m}})) > 0$. Then $P_{\underline{m}}(\boldsymbol{q}) = 0$ by Proposition 2.3.2(2). Thus

$$\dim(\ker(\rho_m(S_m)|V_{\underline{m}})) = n_1(\boldsymbol{q}) - n_2(\boldsymbol{q})$$

by Theorem 2.5.2 and by the bijectivity of the maps $\rho_k(S_{1,k-1})|V_{\underline{l}}$ for $\underline{l} < \underline{m}$ with $k = |\underline{l}| \geq 2$.

Example 2.5.4. Here we give an example of a Nichols algebra of diagonal type where in some degree one has two defining relations.

Let (V, c) be the two-dimensional braided vector space of diagonal type with basis x_1, x_2 and braiding matrix $\boldsymbol{q} = (q_{ij})_{1\leq i,j\leq 2} \in (\Bbbk^\times)^2$, such that

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

and $q_{11} = q_{22} = q_{12}q_{21} = q$, where $q \in \Bbbk^\times$ is a primitive fifth root of unity.

Let $\underline{m} = 3\underline{e}_1 + 4\underline{e}_2$. Then $N(\underline{m}) = \gcd(6, 12, 12) = 6$ and

$$Q_{\underline{m}} = p_{11}(p_{12}p_{21})^2 p_{22}^2, \qquad Q_{\underline{m}}(\boldsymbol{q}) = q^5 = 1.$$

Thus $d = \mathrm{ord}(Q_{\underline{m}}) = 1$ and $d' = N(\underline{m})/d = 6$.

Let us check that $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \geq 2$.

$$\begin{aligned}
&P_{(3,3)}(\boldsymbol{q}) = (3)_{q_{11}^2(q_{12}q_{21})^3 q_{22}^2} = (3)_{q^7} = (3)_q(3)_{-q};\\
&P_{(3,2)}(\boldsymbol{q}) = P_{(2,3)}(\boldsymbol{q}) = 1 - q_{11}(q_{12}q_{21})^3 q_{22}^3 = 1 - q^7 = 1 - q^2;\\
&P_{(3,1)}(\boldsymbol{q}) = P_{(1,3)}(\boldsymbol{q}) = 1 - q_{12}q_{21}q_{22}^2 = 1 - q^3;\\
&P_{(1,2)}(\boldsymbol{q}) = P_{(2,1)}(\boldsymbol{q}) = 1 - q_{11}q_{12}q_{21} = 1 - q^2;\\
&P_{(1,1)}(\boldsymbol{q}) = 1 - q_{11} = 1 - q;\\
&P_{(2,4)}(\boldsymbol{q}) = 1 + q_{22}^6(q_{12}q_{21})^4 q_{11} = 1 + q^{11} = 1 + q;
\end{aligned}$$

$$P_{(1,4)}(\boldsymbol{q}) = 1 - q_{22}^3 q_{12} q_{21} = 1 - q^4;$$
$$P_{(2,2)}(\boldsymbol{q}) = 1 + q_{22}(q_{12}q_{21})^2 q_{11} = 1 + q^4;$$

Moreover, $P_{(m,0)}(\boldsymbol{q}), P_{(0,m)}(\boldsymbol{q}) \neq 0$ for $m \in \{2,3,4\}$ since $(4)_q^! \neq 0$. Hence $P_{\underline{l}}(\boldsymbol{q}) \neq 0$ for all $\underline{l} < \underline{m}$ with $|\underline{l}| \geq 2$.

We now calculate $n_1(\boldsymbol{q})$ and $n_2(\boldsymbol{q})$. By definition,

$$\begin{aligned} n_1(\boldsymbol{q}) &= \sum_{k|\,\gcd(2,4),k|6} \ell_{(2,4)/k} + \sum_{k|\,\gcd(3,3),k|6} \ell_{(3,3)/k} \\ &= \ell_{(2,4)} + \ell_{(1,2)} + \ell_{(3,3)} + \ell_{(1,1)} = 7 \end{aligned}$$

since $\ell_{(2,4)} = 2$, $\ell_{(3,3)} = 3$, $\ell_{(1,2)} = \ell_{(1,1)} = 1$.

$$n_2(\boldsymbol{q}) = \sum_{k|\,\gcd(3,4),k|6} \ell_{(3,4)/k} = \ell_{(3,4)} = 5.$$

Hence $\dim(\ker(\rho_7(S_{1,6})|V_{(3,4)})) = n_1(\boldsymbol{q}) - n_2(\boldsymbol{q}) = 2$.

Chapter 3

Root multiplicities for Nichols algebras of diagonal type of rank two

One of the biggest open problems in the theory of Nichols algebras of diagonal type is to determine for any V (in a suitable class) the set L in Kharchenko's theorem. In this Chapter we focus on the Nichols algebras of diagonal type of rank two and we determine the subset of L of elements of degree $m\alpha_1 + 2\alpha_2$, where $m \in \mathbb{N}$.

We always write $\Bbbk$ as a field and $\Bbbk^\times = \Bbbk\backslash\{0\}$.

3.1 Quantum integers and Gaussian binomial coefficients

For our study of Nichols algebras we will need some non-standard formulas for quantum integers and Gaussian binomial coefficients.

In the ring $\mathbb{Z}[q]$, let $(0)_q = 0$ and for any $m \in \mathbb{N}$, let

$$(m)_q = 1 + q + q^2 + \cdots + q^{m-1}$$

and $(-m)_q = -(m)_q$. The polynomials $(m)_q$ with $m \in \mathbb{Z}$ are also known as quantum integers. Moreover, let $(0)_q^! = 1$, and for any $m \in \mathbb{N}$ let $(m)_q^! = \prod_{i=1}^m (i)_q$. For any $i, m \in \mathbb{Z}$ with $0 \le i \le m$, the rational function

$$\binom{m}{i}_q = \frac{(m)_q^!}{(i)_q^!(m-i)_q^!} \in \mathbb{Q}(q)$$

is in fact an element of $\mathbb{Z}[q]$ and is called a Gaussian binomial coefficient. For $m \in \mathbb{N}_0$, $i \in \mathbb{Z}$ with $i < 0$ or $i > m$ one defines $\binom{m}{i}_q = 0$. The Gaussian binomial coefficients satisfy the following formulas:

$$\binom{m}{i}_q = \binom{m}{m-i}_p, \tag{3.1}$$

$$\binom{m}{i}_q = q^i \binom{m-1}{i}_q + \binom{m-1}{i-1}_q, \tag{3.2}$$

$$\binom{m}{i}_q = \binom{m-1}{i}_q + q^{m-i}\binom{m-1}{i-1}_q \tag{3.3}$$

for any $m \in \mathbb{N}$, $i \in \mathbb{Z}$.

Lemma 3.1.1. Let $t \in \mathbb{N}_0$ and $k \in \mathbb{Z}$ with $k \ge -1$. Then

$$\sum_{j=t}^{k} q^{-j(j+1)/2} q^{(j-t)(j-t-1)/2} \binom{j}{t}_q = q^{-(t+1)(2k-t)/2} \binom{k+1}{t+1}_q.$$

Proof. We proceed by induction on k. For $k < t$ the claim is trivial. Assume now that $t, k \in \mathbb{N}_0$ and that the claim holds for t and $k-1$. The summand for $j = k$ on the left hand side is $q^{-(t+1)(2k-t)/2}\binom{k}{t}_q$. By subtracting this from both sides of the equation and using Equation (3.2), the claim follows from the induction hypothesis. □

Lemma 3.1.2. Let $m \in \mathbb{N}_0$ and $n \in \mathbb{Z}$. Then in $\mathbb{Z}[q, t]$ we have

$$\sum_{i=0}^{m} \binom{m}{i}_q q^{i(i-1)/2} \prod_{j=0}^{i-1}(q^{j+n}t^2 - t) \prod_{j=1}^{m-i}(1 - q^{m+n-j}t^2) = \prod_{j=0}^{m-1}(1 - q^j t).$$

Proof. We prove the claim by induction on m.

For $m = 0$ the claim is trivial. Now assume that the claim holds for some $m \in \mathbb{N}_0$. By applying Equation (3.3) we obtain that

$$\begin{aligned}
&\sum_{i=0}^{m+1} \binom{m+1}{i}_q q^{i(i-1)/2} \prod_{j=0}^{i-1}(q^{j+n}t^2 - t) \prod_{j=1}^{m+1-i} (1 - q^{m+n+1-j}t^2) \\
&= \sum_{i=0}^{m} \binom{m}{i}_q q^{i(i-1)/2} \prod_{j=0}^{i-1}(q^{j+n}t^2 - t) \prod_{j=1}^{m+1-i} (1 - q^{m+n+1-j}t^2) \\
&+ \sum_{i=1}^{m+1} \binom{m}{i-1}_q q^{m+1-i} q^{i(i-1)/2} \prod_{j=0}^{i-1}(q^{j+n}t^2 - t) \prod_{j=1}^{m+1-i} (1 - q^{m+n+1-j}t^2).
\end{aligned}$$

Regarding the first term, note that

$$\prod_{j=1}^{m+1-i} (1 - q^{m+n+1-j}t^2) = (1 - q^{m+n}t^2) \prod_{j=1}^{m-i}(1 - q^{m+n-j}t^2).$$

Hence, by induction hypothesis, the first term is equal to

$$(1 - q^{m+n}t^2) \prod_{j=0}^{m-1}(1 - q^j t).$$

Moreover, the second term is equal to

$$\sum_{i=0}^{m} \binom{m}{i}_q q^{m-i} q^{i(i+1)/2} \prod_{j=0}^{i}(q^{j+n}t^2 - t) \prod_{j=1}^{m-i}(1 - q^{m+n+1-j}t^2).$$

Now by using that

$$q^{m-i} q^{i(i+1)/2} \prod_{j=0}^{i}(q^{j+n}t^2 - t) = q^m q^{i(i-1)/2}(q^n t^2 - t) \prod_{j=0}^{i-1}(q^{j+n+1}t^2 - t),$$

induction hypothesis implies that the second term is equal to

$$q^m(q^n t^2 - t) \prod_{j=0}^{m-1}(1 - q^j t).$$

Since $1 - q^{m+n}t^2 + q^m(q^n t^2 - t) = 1 - q^m t$, the claim holds for $m + 1$. □

Lemma 3.1.3. Let $k, m \in \mathbb{N}_0$ and

$$Q_1^{k,m} = \sum_{i=0}^{m} \binom{m+1}{i}_q q^{i(2k+i-1)/2} \prod_{j=0}^{i-1} (q^{k+j}r^2 - r) \prod_{j=1}^{m-i} (1 - q^{2k+m-j}r^2)$$

$$Q_2^{k,m} = \frac{q^{(2k+m)(m+1)/2}(-r)^{m+1} - 1}{q^{2k+m}r^2 - 1} \prod_{i=0}^{m} (1 - q^{k+i}r)$$

in $\mathbb{Z}[q, r]$. Then $Q_1^{k,m} = Q_2^{k,m}$.

Proof. Clearly, $Q_1^{k,m} \in \mathbb{Z}[q, r]$. If m is odd then $q^{2k+m}r^2 - 1$ divides $(q^{2k+m}r^2)^{(m+1)/2} - 1$ in $\mathbb{Z}[q, r]$. If m is even, then

$$q^{2k+m}r^2 - 1 = (q^{k+m/2}r - 1)(q^{k+m/2}r + 1).$$

Since $q^{k+m/2}r - 1$ divides $\prod_{i=0}^{m}(1 - q^{k+i}r)$ and $q^{k+m/2}r + 1$ divides $-(q^{k+m/2}r)^{m+1} - 1$ in $\mathbb{Z}[q, r]$, we conclude that $Q_2^{k,m} \in \mathbb{Z}[q, r]$. Moreover,

$$\begin{aligned}
&Q_1^{k,m}(1 - q^{2k+m}r^2) \\
&= \sum_{i=0}^{m} \binom{m+1}{i}_q q^{i(2k+i-1)/2} \prod_{j=0}^{i-1} (q^{k+j}r^2 - r) \prod_{j=0}^{m-i} (1 - q^{2k+m-j}r^2) \\
&= \sum_{i=0}^{m+1} \binom{m+1}{i}_q q^{i(2k+i-1)/2} \prod_{j=0}^{i-1} (q^{k+j}r^2 - r) \prod_{j=1}^{m+1-i} (1 - q^{2k+m+1-j}r^2) \\
&\quad - q^{(m+1)(2k+m)/2} \prod_{j=0}^{m} (q^{k+j}r^2 - r).
\end{aligned}$$

By Lemma 3.1.2 for $m + 1$, $n = 0$ and $t = q^k r$, the first term is equal to $\prod_{j=0}^{m}(1 - q^{j+k}r)$. From this it follows that $Q_1^{k,m} = Q_2^{k,m}$. □

3.2 A family of some special elements of Nichols algebra

For the remaining part of this Chapter, let (V, c) be a two-dimensional braided vector of diagonal type. Let x_1, x_2 be a basis of V and $(q_{ij})_{1 \le i,j \le 2} \in (\mathbb{k}^\times)^{2\times 2}$

such that

$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i.$$

Let $q = q_{11}$, $r = q_{12}q_{21}$ and $s = q_{22}$. We write $\pi : T(V) \longrightarrow \mathcal{B}(V)$ for the canonical map.

In this section we introduce some special elements of $\mathcal{B}(V)$ and spell out some easy properties of them.

For all $k \in \mathbb{N}_0$ we define inductively $u_k \in T(V)$ by

$$u_0 = x_2, \quad u_k = x_1 u_{k-1} - q^{k-1} q_{12} u_{k-1} x_1 \tag{3.4}$$

for $k \geq 1$. Note that then $u_k = [x_1^k x_2]$ for any $k \in \mathbb{N}_0$. Recall that ad is the adjoint action of $T(V)$ on itself. Then

$$\operatorname{ad} x_1(y) = x_1 y - \chi(\alpha_1, \deg(y)) y x_1$$

for any homogeneous element $y \in T(V)$. In particular,

$$\operatorname{ad} x_1(u_k) = u_{k+1} \tag{3.5}$$

for any $k \in \mathbb{N}_0$.

Lemma 3.2.1. Let $m \in \mathbb{N}_0$. Then

$$\begin{aligned} d_1\big((\operatorname{ad} x_1)^m(y)\big) = {} & q^m (\operatorname{ad} x_1)^m (d_1(y)) \\ & + (m)_q (1 - q^{m-1} \chi(\alpha_1, \alpha)\chi(\alpha, \alpha_1))(\operatorname{ad} x_1)^{m-1}(y) \end{aligned}$$

for any homogeneous element $y \in T(V)$ of degree $\alpha \in \mathbb{N}_0^n$.

Proof. Let $y \in T(V)$ be a homogeneous element of degree $\alpha \in \mathbb{N}_0^n$. Then

$$\begin{aligned} d_1(\operatorname{ad} x_1(y)) &= d_1(x_1 y - \chi(\alpha_1, \alpha) y x_1) \\ &= y + q x_1 d_1(y) - \chi(\alpha_1, \alpha)(d_1(y) x_1 + \chi(\alpha, \alpha_1) y) \\ &= (1 - \chi(\alpha_1, \alpha)\chi(\alpha, \alpha_1)) y + q \operatorname{ad} x_1(d_1(y)). \end{aligned}$$

Now we prove the lemma by induction on m. For $m = 0$ the claim is trivial. Let now $m \in \mathbb{N}$ and assume that the claim holds for $m - 1$. Let $y \in T(V)$

be a homogeneous element of degree $\alpha \in \mathbb{N}_0$ and let $\beta = \alpha + (m-1)\alpha_1$, $q_\alpha = \chi(\alpha_1, \alpha)\chi(\alpha, \alpha_1)$. Then, by using the above formula, we conclude that

$$\begin{aligned} d_1\big((\operatorname{ad} x_1)^m(y)\big) =& q\operatorname{ad} x_1\big(d_1\big((\operatorname{ad} x_1)^{m-1}(y)\big)\big) \\ &+ (1 - \chi(\alpha_1, \beta)\chi(\beta, \alpha_1))(\operatorname{ad} x_1)^{m-1}(y) \\ =& q\operatorname{ad} x_1\big(q^{m-1}(\operatorname{ad} x_1)^{m-1}(d_1(y))\big) \\ &+ q\operatorname{ad} x_1\big((m-1)_q(1 - q^{m-2}q_\alpha)(\operatorname{ad} x_1)^{m-2}(y)\big) \\ &+ (1 - q^{2m-2}q_\alpha)(\operatorname{ad} x_1)^{m-1}(y) \end{aligned}$$

because of the induction hypothesis. From this one obtains the claim for m. $\square$

Remark 3.2.2. (1) It is well-known that

$$\Delta(u_k) = u_k \otimes 1 + \sum_{i=0}^{k} \binom{k}{i}_q \prod_{j=k-i}^{k-1} (1 - q^j r) x_1^i \otimes u_{k-i} \tag{3.6}$$

for any $k \in \mathbb{N}_0$. Hence from Equation (1.8) we conclude that

$$d_1(u_k) = (k)_q (1 - q^{k-1} r) u_{k-1}, \quad d_2(u_k) = \delta_{k0} 1 \tag{3.7}$$

for any $k \in \mathbb{N}_0$.

(2) For all $m \in \mathbb{N}_0$ let

$$b_m = \prod_{j=0}^{m-1} (1 - q^j r).$$

In particular, $b_0 = 1$. Then Remark 1.5.3(2) implies that $u_k = 0$ in $\mathcal{B}(V)$ if and only if $(k)_q^! b_k = 0$.

Later on, often a normalization of u_k, $k \in \mathbb{N}_0$, will be very useful. For all $k \in \mathbb{N}_0$ let

$$\hat{u}_k = \begin{cases} \frac{1}{(k)_q^! b_k} u_k & \text{if } (k)_q^! b_k \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The following equations for $k \in \mathbb{N}_0$ with $(k)^!_q b_k \neq 0$ follow directly from the analogous formulas for u_k.

$$\Delta(\hat{u}_k) = \hat{u}_k \otimes 1 + \sum_{i=0}^{k} \frac{x_1^i}{(i)^!_q} \otimes \hat{u}_{k-i}, \tag{3.8}$$

$$d_1(\hat{u}_k) = \hat{u}_{k-1}, \quad d_2(\hat{u}_k) = \delta_{k0}1, \tag{3.9}$$

$$\operatorname{ad} x_1(\hat{u}_k) = (k+1)_q(1-q^k r)\hat{u}_{k+1}, \tag{3.10}$$

where $\hat{u}_{-1} = 0$ in (3.9).

We end the section with a lemma.

Lemma 3.2.3. Let $k \in \mathbb{N}_0$ such that $(k)^!_q b_k \neq 0$ and let $\lambda_0, \dots, \lambda_k \in \Bbbk$. Let $Z = \sum_{i=0}^{k} \lambda_i (-q_{21})^i \hat{u}_i \hat{u}_{k-i}$ in $T(V)$. Then

$$d_1(Z) = -q_{21} \sum_{i=0}^{k-1} (\lambda_{i+1} - q^i \lambda_i)(-q_{21})^i \hat{u}_i \hat{u}_{k-1-i},$$
$$d_2(Z) = (\lambda_0 + (-r)^k s \lambda_k)\hat{u}_k.$$

Proof. This follows directly from Equations (1.6) and (3.9). □

3.3 Multiplicities

We use the notation from the previous section in this chapter. In this section we determine for all $m \in \mathbb{N}_0$ the set of root vectors of Nichols algebra $\mathcal{B}(V)$ of degree $m\alpha_1 + 2\alpha_2$.

Lemma 3.3.1. Let $m \in \mathbb{N}$ such that $u_m \neq 0$ in $\mathcal{B}(V)$. Then $u_m^2 = 0$ in $\mathcal{B}(V)$ if and only if $q^{m^2} r^m s = -1$ and $u_{m+1} = 0$ in $\mathcal{B}(V)$.

Proof. Assume first that $u_m^2 = 0$. For all $k \in \mathbb{N}_0$ let $\beta_k = k\alpha_1 + \alpha_2$. Using Equation 3.6 we obtain that

$$\Delta_{\beta_m,\beta_m}(u_m^2) = (1 + q^{m^2} r^m s) u_m \otimes u_m.$$

Since $u_m \neq 0$, we conclude that $q^{m^2} r^m s = -1$. Moreover,

$$\begin{aligned}\Delta_{\beta_{m+1},\beta_{m-1}}(u_m^2) & \\ &= (m)_q (1 - q^{m-1} r)(u_m x_1 + q^{m(m-1)} r^{m-1} s q_{21} x_1 u_m) \otimes u_{m-1} \\ &= (m)_q (1 - q^{m-1} r) q^{m(m-1)} r^{m-1} s q_{21} u_{m+1} \otimes u_{m-1}.\end{aligned}$$

Again, since $u_m \neq 0$, from Remark 3.2.2(2) it follows that $u_{m+1} = 0$.

Conversely, assume that $q^{m^2} r^m s = -1$ and that $u_{m+1} = 0$. Then we have $x_1 u_m = q^m q_{12} u_m x_1$, and hence

$$\begin{aligned}\Delta_{2\beta_m - \alpha_1, \alpha_1}(u_m^2) &= 0, \\ \Delta_{\beta_{2m}, \alpha_2}(u_m^2) &= b_m\big((x_1^m \otimes u_0)(u_m \otimes 1) + u_m x_1^m \otimes u_0\big) \\ &= b_m (q_{21}^m s q^{m^2} q_{12}^m + 1) u_m x_1^m \otimes u_0 \\ &= 0.\end{aligned}$$

Since $\mathcal{B}(V)$ is a strictly graded coalgebra, it follows that $u_m^2 = 0$. □

Lemma 3.3.2. Let $k, l \in \mathbb{N}_0$ with $k > l$. Assume that $(k)_q^! b_k \neq 0$ and that $[x_1^k x_2 x_1^{l+1} x_2]$ is not a root vector. Then $[x_1^k x_2 x_1^l x_2]$ is not a root vector.

Proof. Lyndon words of degree $(k+l+1)\alpha_1 + 2\alpha_2$, which are larger than $x_1^k x_2 x_1^{l+1} x_2$, are of the form $x_1^m x_2 x_1^{k+l+1-m} x_2$ with $(k+l+1)/2 < m < k$. Hence the assumption implies that there exists $(\lambda_i)_{l+1 \le i \le k} \in \Bbbk^{k-l}$ such that $\lambda_k = 1$ and $\sum_{i=l+1}^k \lambda_i \hat{u}_i \hat{u}_{k+l+1-i} = 0$ in $\mathcal{B}(V)$. Then

$$d_1\Big(\sum_{i=l+1}^{k} \lambda_i \hat{u}_i \hat{u}_{k+l+1-i}\Big) = \sum_{i=l+1}^{k} \lambda_i (\hat{u}_{i-1} \hat{u}_{k+l+1-i} + q^i q_{21} \hat{u}_i \hat{u}_{k+l-i}) = 0.$$

The coefficient of $\hat{u}_k \hat{u}_l$ in the last expression is $q^k q_{21}$ and hence the root vector candidate $[x_1^k x_2 x_1^l x_2]$ is not a root vector. □

Proposition 3.3.3. Let $k, l \in \mathbb{N}$ with $k \ge l$. Assume that $[x_1^k x_2 x_1^l x_2]$ is a root vector candidate but not a root vector. Then $[x_1^{k+1} x_2 x_1^{l-1} x_2]$ is not a root vector.

Proof. First assume that $k = l$. Then $[x_1^{k+1} x_2] = 0$ by Lemma 3.3.1. Therefore $[x_1^{k+1} x_2 x_1^{l-1} x_2]$ is not a root vector. Suppose now that $k > l$. Then $[x_1^k x_2 x_1^{l-1} x_2]$ is not a root vector by Lemma 3.3.2, and Remark 1.4.4 implies that $[x_1^{k+1} x_2 x_1^{l-1} x_2]$ is not a root vector. □

For any $n \in \mathbb{N}_0$ let

$$U_n = \bigoplus_{i=0}^{n} \Bbbk u_i u_{n-i} \subseteq T(V), \qquad U'_n = \bigoplus_{i=0}^{n-1} \Bbbk u_i u_{n-i} \subseteq T(V). \tag{3.11}$$

The subspaces U_n and U'_n will appear at several places as technical tools. Here we discuss some elementary results related to them.

Lemma 3.3.4. The map $\operatorname{ad} x_1 : U_m \to U_{m+1}$ is injective for any $m \in \mathbb{N}_0$.

Proof. Let $m \in \mathbb{N}_0$, $\lambda_0, \dots, \lambda_m \in \Bbbk$, and $v = \sum_{i=0}^{m} \lambda_i u_i u_{m-i}$. Then

$$\operatorname{ad} x_1(v) = \sum_{i=0}^{m} \lambda_i (u_{i+1} u_{m-i} + q^i q_{12} u_i u_{m+1-i})$$

by Equation (3.5). Assume that $v \neq 0$. Let $0 \leq j \leq m$ such that $\lambda_j \neq 0$ and either $j = m$ or $\lambda_{j+1} = 0$. Then the coefficient of $u_{j+1} u_{m-j}$ in the above expression is λ_j, and hence $\operatorname{ad} x_1(v) \neq 0$. □

Proposition 3.3.5. Let $k \in \mathbb{N}_0$ such that $(k)^!_q b_k \neq 0$. Let $v \in U'_k \cap \ker(\pi)$ and let $\mu_0, \dots, \mu_{k-1} \in \Bbbk$ such that

$$d_1(v) = \sum_{i=0}^{k-1} \mu_i (-q_{21})^i \hat{u}_i \hat{u}_{k-1-i}.$$

Then $\sum_{i=0}^{k-1} q^{-i(i+1)/2} \mu_i = 0$.

Proof. For any $\lambda = (\lambda_0, \dots, \lambda_k) \in \Bbbk^{k+1}$ let $\bar{\mu}(\lambda) = (\mu_i(\lambda))_{0 \leq i < k} \in \Bbbk^k$ such that

$$\mu_i(\lambda) = \lambda_{i+1} - \lambda_i q^i$$

whenever $0 \leq i < k$. Let $W = \{\lambda \in \Bbbk^{k+1} \mid \lambda_0 = 0\}$. Then the linear map $\bar{\mu} : W \to \Bbbk^k$, $\lambda \mapsto \bar{\mu}(\lambda)$, is bijective. The inverse map is given by

$$\bar{\mu}^{-1}(\mu_0, \dots, \mu_{k-1}) = (\lambda_i)_{0 \leq i \leq k}, \quad \lambda_i = \sum_{j=0}^{i-1} q^{(i+j)(i-j-1)/2} \mu_j. \tag{3.12}$$

Now let $\lambda = (\lambda_0, \lambda_1, \dots, \lambda_{k-1}, 0) \in \Bbbk^{k+1}$ such that

$$v = \sum_{i=0}^{k} \lambda_i (-q_{21})^i \hat{u}_i \hat{u}_{k-i}.$$

Since $v \in \ker(\pi)$, it follows from Remark 1.5.3(2) that $d_2(v) \in \ker(\pi)$. Since $v \in U'_k$ and $u_k \neq 0$ in $\mathcal{B}(V)$, Lemma 3.2.3 implies that $\lambda_0 = 0$, that is, $\lambda \in W$. Then we obtain from Equation (3.12) and from $\lambda_k = 0$ that $\sum_{j=0}^{k-1} q^{-j(j+1)/2} \mu_j(\lambda) = 0$. Moreover,

$$d_1(v) = -\, q_{21} \sum_{i=0}^{k-1} \mu_i(\lambda)(-q_{21})^i \hat{u}_i \hat{u}_{k-1-i}$$

by Lemma 3.2.3, and hence $\mu_j = -q_{21}\mu_j(\lambda)$ for any $0 \leq j < k$. This implies the claim. □

The following elements of $T(V)$ will play a fundamental role in Theorem 3.3.16.

Definition 3.3.6. For all $k \in \mathbb{N}_0$ with $(k)^!_q b_k \neq 0$, let

$$P_k = \sum_{i=0}^{k} (-q_{21})^i q^{i(i-1)/2} \hat{u}_i \hat{u}_{k-i} \in T(V). \tag{3.13}$$

Lemma 3.3.7. Let $k \in \mathbb{N}_0$ with $(k)^!_q b_k \neq 0$. Then $P_k = 0$ in $\mathcal{B}(V)$ if and only if $q^{k(k-1)/2}(-r)^k s = -1$.

Proof. By Lemma 3.2.3,

$$d_1(P_k) = 0, \quad d_2(P_k) = (1 + (-r)^k s q^{k(k-1)/2}) \hat{u}_k.$$

Since $(k)^!_q b_k \neq 0$, the claim follows from this and from Remark 1.5.3(2). □

We also introduce a family of elements $S(k,t)$ of $T(V)$, which are related to the elements P_k by Lemmas 3.3.9 and 3.3.10 below. Those lemmas themself are needed for Lemma 3.3.11, which is a crucial ingredient of the proof of Theorem 3.3.16.

Definition 3.3.8. For all $k, t \in \mathbb{N}_0$ with $0 \le t \le k$ and $(k)^!_q b_k \neq 0$ let

$$S(k,t) = \sum_{i=t}^{k} (-q_{21})^i q^{(i-t)(i-t-1)/2} \binom{i}{t}_q \hat{u}_i \hat{u}_{k-i} \in T(V).$$

In particular, $S(k,0) = P_k$.

Lemma 3.3.9. Let $k, t \in \mathbb{N}_0$ with $0 \le t \le k$ such that $(k+1)^!_q b_{k+1} \neq 0$. Then

$$\begin{aligned} q_{12}^{-1} \operatorname{ad} x_1(S(k,t)) = {} & q^t (1 - q^{k-t} r)(k+1-t)_q S(k+1,t) \\ & + r^{-1}(q^{2k-t} r^2 - 1)(t+1)_q S(k+1,t+1). \end{aligned}$$

Proof. First note that for $0 \le i \le k$ we get

$$\begin{aligned} \operatorname{ad} x_1(\hat{u}_i \hat{u}_{k-i}) = {} & (i+1)_q (1 - q^i r) \hat{u}_{i+1} \hat{u}_{k-i} \\ & + q^i q_{12} (k+1-i)_q (1 - q^{k-i} r) \hat{u}_i \hat{u}_{k+1-i} \end{aligned}$$

by Equation (3.10). Moreover, $(k+1)^!_q \neq 0$. Hence

$$\begin{aligned} & \operatorname{ad} x_1(S(k,t)) \\ & = \sum_{i=t}^{k} (-q_{21})^i q^{(i-t)(i-t-1)/2} (i+1)_q (1 - q^i r) \binom{i}{t}_q \hat{u}_{i+1} \hat{u}_{k-i} \\ & \quad + \sum_{i=t}^{k} (-q_{21})^i q^{(i-t)(i-t-1)/2} q^i q_{12} (k+1-i)_q (1 - q^{k-i} r) \binom{i}{t}_q \hat{u}_i \hat{u}_{k+1-i} \\ & = -q_{12} r^{-1} \sum_{i=t+1}^{k+1} (-q_{21})^i q^{(i-t-1)(i-t-2)/2} (i)_q (1 - q^{i-1} r) \binom{i-1}{t}_q \hat{u}_i \hat{u}_{k+1-i} \\ & \quad + q_{12} q^t \sum_{i=t}^{k+1} (-q_{21})^i q^{(i-t)(i-t+1)/2} (k+1-i)_q (1 - q^{k-i} r) \binom{i}{t}_q \hat{u}_i \hat{u}_{k+1-i}. \end{aligned}$$

Now in the first term we replace $(i)_q \binom{i-1}{t}_q$ by $(t+1)_q \binom{i}{t+1}_q$ and $(i-t)_q \binom{i}{t}_q$, respectively. We then rewrite this first term as

$$-q_{12} r^{-1} (t+1)_q \sum_{i=t+1}^{k+1} (-q_{21})^i q^{(i-t-1)(i-t-2)/2} \binom{i}{t+1}_q \hat{u}_i \hat{u}_{k+1-i} \tag{3.14}$$

$$+ q_{12}q^t \sum_{i=t+1}^{k+1} (-q_{21})^i q^{(i-t-1)(i-t)/2}(i-t)_q \binom{i}{t}_q \hat{u}_i\hat{u}_{k+1-i}. \tag{3.15}$$

The second term of $\operatorname{ad} x_1(S(k,t))$ can be written as

$$q_{12}q^t \sum_{i=t}^{k+1} (-q_{21})^i q^{(i-t)(i-t-1)/2} q^{i-t}(k+1-i)_q \binom{i}{t}_q \hat{u}_i\hat{u}_{k+1-i} \tag{3.16}$$

$$- q_{12}q^k r \sum_{i=t}^{k+1} (-q_{21})^i q^{(i-t)(i-t-1)/2}(k+1-i)_q \binom{i}{t}_q \hat{u}_i\hat{u}_{k+1-i}. \tag{3.17}$$

Now (3.14) is equal to $-q_{12}r^{-1}(t+1)_q S(k+1,t+1)$, and the sum of (3.15) and (3.16) is equal to $q_{12}q^t(k+1-t)_q S(k+1,t)$. Finally, in (3.17) we replace $(k+1-i)_q$ by $(k+1-t)_q - q^{k+1-i}(i-t)_q$ and $(i-t)_q\binom{i}{t}_q$ by $(t+1)_q\binom{i}{t+1}_q$. Thus (3.17) is equal to

$$-q_{12}q^k r(k+1-t)_q S(k+1,t) + q_{12}q^{2k-t} r(t+1)_q S(k+1,t+1).$$

This implies the lemma. □

Lemma 3.3.10. Let $m, k \in \mathbb{N}_0$ such that $(k+m)^!_q b_{k+m} \neq 0$. Then

$$q_{12}^{-m}(\operatorname{ad} x_1)^m(P_k) = \sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q} \lambda_{(m-i,k)}\beta_{(i,m,k)} S(k+m,i)$$

where for any $i, n, m' \in \mathbb{N}_0$,

$$\lambda_{(n,k)} = \prod_{j=1}^{n}(1-q^{k-1+j}r)(k+j)_q, \quad \beta_{(i,m',k)} = \prod_{j=1}^{i}(q^{m'+2k-j}r - r^{-1}).$$

Proof. Note first that for any $i, n \in \mathbb{N}_0$,

$$\lambda_{(n+1,k)} = (1-q^{k+n}r)(k+n+1)_q\lambda_{(n,k)}, \tag{3.18}$$

$$\beta_{(i,m,k)} = (q^{m+2k-i}r - r^{-1})\beta_{(i-1,m,k)}, \tag{3.19}$$

$$\beta_{(i,m+1,k)} = (q^{m+2k}r - r^{-1})\beta_{(i-1,m,k)}. \tag{3.20}$$

We prove the Lemma by induction on m.

For $m = 0$, both sides of the equation in the lemma are equal to P_k. Assume now that the formula in the Lemma holds for m and that $(k+m+1)^!_q b_{k+m+1} \neq 0$. Then

$$\begin{aligned}
&q_{12}^{-m-1}(\operatorname{ad} x_1)^{m+1}(P_k)\\
&= q_{12}^{-1}\operatorname{ad} x_1 \left(q_{12}^{-m}(\operatorname{ad} x_1)^m(P_k)\right)\\
&= q_{12}^{-1}\operatorname{ad} x_1 \left(\sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q}\lambda_{(m-i,k)}\beta_{(i,m,k)}S(k+m,i)\right)
\end{aligned}$$

by induction hypothesis. Now apply Lemma 3.3.9 to obtain that

$$\begin{aligned}
&q_{12}^{-m-1}(\operatorname{ad} x_1)^{m+1}(P_k)\\
&= \sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q}\lambda_{(m-i,k)}\beta_{(i,m,k)}\cdot\\
&\qquad q^i(1-q^{k+m-i}r)(k+m+1-i)_q S(k+m+1,i)\\
&\quad+\sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q}\lambda_{(m-i,k)}\beta_{(i,m,k)}\cdot\\
&\qquad (q^{2m+2k-i}r-r^{-1})(i+1)_q S(k+m+1,i+1).
\end{aligned}$$

In the first term we use (3.18), in the second we change the summation index. Then

$$\begin{aligned}
&q_{12}^{-m-1}(\operatorname{ad} x_1)^{m+1}(P_k)\\
&= \sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q}\lambda_{(m+1-i,k)}\beta_{(i,m,k)}q^i S(k+m+1,i)\\
&\quad+\sum_{i=1}^{m+1} \frac{(m)^!_q}{(m+1-i)^!_q}\lambda_{(m+1-i,k)}\beta_{(i-1,m,k)}\cdot\\
&\qquad (q^{2m+2k+1-i}r-r^{-1})(i)_q S(k+m+1,i).
\end{aligned}$$

Thus it remains to show that

$$(m+1-i)_q q^i\beta_{(i,m,k)} + (q^{2m+2k+1-i}r-r^{-1})(i)_q\beta_{(i-1,m,k)}$$

$$= (m+1)_q \beta_{(i,m+1,k)}$$

for any $0 \le i \le m+1$. The latter is easily done by expressing $\beta_{(i,m,k)}$ and $\beta_{(i,m+1,k)}$ via $\beta_{(i-1,m,k)}$ using Equations (3.19) and (3.20), respectively, and then comparing coefficients. This proves the claim for $m+1$. □

Recall the definitions of $Q_1^{k,m}, Q_2^{k,m} \in \mathbb{Z}[q,r]$ from Lemma 3.1.3. In this section we view $Q_1^{k,m}, Q_2^{k,m}$ as elements in $\Bbbk = \Bbbk \otimes_{\mathbb{Z}[q,r]} \mathbb{Z}[q,r]$ by identifying q and r in $\mathbb{Z}[q,r]$ with q and r in $\Bbbk$, respectively.

Lemma 3.3.11. Let $k,m \in \mathbb{N}_0$. Suppose that $(k+m+1)^!_q b_{k+m+1} \neq 0$ and that there exists $v \in U'_{k+m+1} \cap \ker(\pi)$ such that $d_1(v) = (\operatorname{ad} x_1)^m(P_k)$ in $T(V)$. Then $Q_2^{k,m} = 0$.

Proof. Let $v \in U'_{k+m+1} \cap \ker(\pi)$. Let $\mu_0, \dots, \mu_{k-1} \in \Bbbk$ such that

$$d_1(v) = \sum_{j=0}^{k+m} \mu_j (-q_{21})^j \hat{u}_j \hat{u}_{k+m-j}.$$

Then $\sum_{j=0}^{k+m} q^{-j(j+1)/2} \mu_j = 0$ by Proposition 3.3.5. Assume now also that $d_1(v) = (\operatorname{ad} x_1)^m(P_k)$. Then from Lemma 3.3.10 and Definition 3.3.8 we obtain that

$$q_{12}^m \sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q} \lambda_{(m-i,k)} \beta_{(i,m,k)} \sum_{j=i}^{k+m} q^{(j-i)(j-i-1)/2} q^{-j(j+1)/2} \binom{j}{i}_q = 0$$

in $\mathcal{B}(V)$. (We use the notation in Lemma 3.3.10.) Then by Lemma 3.1.1 it follows that

$$\sum_{i=0}^{m} \frac{(m)^!_q}{(m-i)^!_q} \lambda_{(m-i,k)} \beta_{(i,m,k)} q^{-(i+1)(2k+2m-i)/2} \binom{k+m+1}{i+1}_q = 0$$

Since

$$\lambda_{(m-i,k)} = \prod_{j=1}^{m-i} (1 - q^{k-1+j} r) \frac{(k+m-i)^!_q}{(k)^!_q},$$

$$\binom{k+m+1}{i+1}_q = \frac{(k+m+1)^!_q}{(i+1)^!_q (k+m-i)^!_q},$$

the latter implies that

$$\sum_{i=0}^{m} \binom{m+1}{i+1}_q \prod_{j=1}^{m-i} (1 - q^{k-1+j} r) \beta_{(i,m,k)} q^{-(i+1)(2k+2m-i)/2} = 0.$$

Now substitute $i = m - l$. It follows that

$$\sum_{l=0}^{m} \binom{m+1}{l}_q \prod_{j=0}^{l-1} (1 - q^{k+j} r) \prod_{j=1}^{m-l} (q^{2k+m-j} r - r^{-1}) q^{l(2k+l-1)/2} = 0.$$

The latter is equal to $(-r)^{-m} Q_1^{k,m}$. Thus $Q_2^{k,m} = 0$ by Lemma 3.1.3. □

Now we introduce the set $\mathbb{J}$ which is crucial for Theorem 3.3.16 below.

Definition 3.3.12. Let $\mathbb{J} = \mathbb{J}_{q,r,s} \subseteq \mathbb{N}_0$ be such that $j \in \mathbb{J}$ if and only if

$$q^{j(j-1)/2}(-r)^j s = -1 \text{ and } q^{j+n-1} r^2 \neq 1 \text{ for any } n \in \mathbb{J},\ n < j.$$

Lemma 3.3.13. For any $j \in \mathbb{J}$, the integers $j + 1$ and $j + 2$ are not in $\mathbb{J}$. In particular, for any $m \in \mathbb{N}_0$,

$$\left|\mathbb{J} \cap [0, m]\right| \leq \frac{m}{3} + 1.$$

Proof. Let $j \in \mathbb{N}_0$ and $t \in \mathbb{N}$. Assume that $j, j + t \in \mathbb{J}$. Then

$$q^{j(j-1)/2}(-r)^j s = -1, \quad q^{(j+t)(j+t-1)/2}(-r)^{j+t} s = -1,$$

and $q^{2j+t-1} r^2 \neq 1$. Hence $q^{t(2j+t-1)/2}(-r)^t = 1$. This gives a contradiction both for $t = 1$ and for $t = 2$. □

Example 3.3.14. By the definition of $\mathbb{J}$ and by Lemma 3.3.13 the following hold.

(1) $0 \in \mathbb{J}$ if and only if $s = -1$.

(2) $1 \in \mathbb{J}$ if and only if $rs = 1$ and $s \neq -1$.

(3) $2 \in \mathbb{J}$ if and only if $qr^2 s = -1$, $s \neq -1$, and $rs \neq 1$.

For the proof of the next theorem we will need a technicality.

Lemma 3.3.15. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $k, m \in \mathbb{N}_0$, and assume that $b_{k+m+1} \neq 0$ and $q^{2k+m}r^2 = 1$. Then $Q_2^{k,m} \neq 0$ in $\Bbbk$.

Proof. Assume first that m is odd and that $q^{2k+m}r^2 = 1$. Then

$$Q_2^{k,m} = \sum_{i=0}^{(m-1)/2} (q^{2k+m}r^2)^i \prod_{i=0}^{m}(1-q^{k+i}r) = \frac{m+1}{2}\prod_{i=0}^{m}(1-q^{k+i}r).$$

Since $b_{k+m+1} \neq 0$ and $\mathrm{char}(\Bbbk) = 0$, we conclude that $Q_2^{k,m} \neq 0$ in $\Bbbk$.

Assume now that $q^{2k+m}r^2 = 1$ and that m is even. Let $n = m/2$. Since $b_{k+m+1} \neq 0$, it follows that $q^{k+n}r = -1$. Hence

$$Q_2^{k,m} = \sum_{i=0}^{m}(-q^{k+n}r)^i \prod_{i=0}^{n-1}(1-q^{k+i}r) \prod_{i=n+1}^{m}(1-q^{k+i}r).$$

Thus we again obtain that $Q_2^{k,m} \neq 0$ in $\Bbbk$. □

Theorem 3.3.16. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $m \in \mathbb{N}_0$ such that $(m)_q^! b_m \neq 0$. Then the elements $(\mathrm{ad}\, x_1)^{m-j}(P_j)$ with $j \in \mathbb{J} \cap [0, m]$ form a basis of $\ker(\pi) \cap U_m$.

Proof. First note that $P_j \in \ker(\pi) \cap U_j$ for any $j \in \mathbb{J}$ because of Lemma 3.3.7. Hence $(\mathrm{ad}\, x_1)^{m-j}(P_j) \in \ker(\pi) \cap U_m$ for any $j \in \mathbb{J} \cap [0, m]$.

Now we prove by induction on m that the elements $(\mathrm{ad}\, x_1)^{m-j}(P_j)$ with $j \in \mathbb{J} \cap [0, m]$ are linearly independent. This is clear for $m = 0$. Assume now that $m > 0$, and for any $j \in \mathbb{J} \cap [0, m]$ let $\lambda_j \in \Bbbk$ such that

$$\sum_{j \in \mathbb{J} \cap [0,m]} \lambda_j (\mathrm{ad}\, x_1)^{m-j}(P_j) = 0.$$

If $m \notin \mathbb{J}$, then $\sum_{j \in \mathbb{J} \cap [0,m]} \lambda_j (\mathrm{ad}\, x_1)^{m-1-j}(P_j) = 0$ by Lemma 3.3.4. Hence $\lambda_j = 0$ for all $j \in \mathbb{J} \cap [0, m]$ by induction hypothesis.

Assume now that $m \in \mathbb{J}$. Lemma 3.2.3 implies that $d_1(P_n) = 0$ for any $n \in \mathbb{N}_0$, and hence

$$\sum_{j \in \mathbb{J} \cap [0,m-1]} \lambda_j d_1\big((\mathrm{ad}\, x_1)^{m-j}(P_j)\big) = 0.$$

From Lemma 3.2.1 then it follows that

$$\sum_{j\in\mathbb{J}\cap[0,m-1]} \lambda_j (m-j)_q (1-q^{m-j-1}q^{2j}r^2)(\operatorname{ad} x_1)^{m-1-j}(P_j) = 0.$$

Note that $q^{m+j-1}r^2 \neq 1$ for all $j \in \mathbb{J}\cap[0,m-1]$ because of $m \in \mathbb{J}$. Moreover, $(m)^!_q \neq 0$ by assumption. Therefore induction hypothesis implies that $\lambda_j = 0$ for all $j \in \mathbb{J}\cap[0,m-1]$. Then clearly $\lambda_m = 0$ holds, too.

It remains to show that

$$\dim\big(\ker(\pi)\cap U_m\big) = \big|\mathbb{J}\cap[0,m]\big|. \tag{3.21}$$

Again we proceed by induction on m. Note that $P_0 = u_0^2 \in \ker(\pi)$ if and only if $s = -1$, that is, $0 \in \mathbb{J}$, according to Lemma 3.3.7. Thus the claim holds for $m = 0$.

Let now $m \in \mathbb{N}$. Induction hypothesis and the first part of the proof of the Theorem imply that the elements $(\operatorname{ad} x_1)^{m-1-j}(P_j)$, where $j \in \mathbb{J}\cap[0,m-1]$, form a basis of $\ker(\pi)\cap U_{m-1}$. Since $\operatorname{ad} x_1$ is injective by Lemma 3.3.4 and since $\operatorname{ad} x_1(\ker(\pi)) \subseteq \ker(\pi)$, we further obtain that

$$\dim\big(\ker(\pi)\cap U_m\big) \geq \dim\big(\ker(\pi)\cap U_{m-1}\big).$$

Assume first that $\dim\big(\ker(\pi)\cap U_m\big) = \dim\big(\ker(\pi)\cap U_{m-1}\big)$. Then the elements $(\operatorname{ad} x_1)^{m-j}(P_j)$, where $j \in \mathbb{J}\cap[0,m-1]$, form a basis of $\ker(\pi)\cap U_m$. Moreover, the linear independence of the elements $(\operatorname{ad} x_1)^{m-j}(P_j)$, $j \in \mathbb{J}\cap[0,m]$, implies that $m \notin \mathbb{J}$. This proves (3.21).

Assume now that $\dim\big(\ker(\pi)\cap U_m\big) > \dim\big(\ker(\pi)\cap U_{m-1}\big)$. Since

$$d_1(\ker(\pi)\cap U_m) \subseteq \ker(\pi)\cap U_{m-1},$$

we conclude that $\ker(\pi)\cap U_m\cap\ker(d_1) \neq 0$. Since $(m)^!_q b_m \neq 0$, Lemma 3.2.3 implies that $\ker(d_1|U_m) = \Bbbk P_m$. Hence $P_m \in \ker(\pi)\cap U_m$,

$$\dim\big(\ker(\pi)\cap U_m\big) = 1 + \dim\big(\ker(\pi)\cap U_{m-1}\big), \tag{3.22}$$

and for any $j \in \mathbb{J}$ there exists $v_j \in \ker(\pi)\cap U_m$ such that

$$d_1(v_j) = (\operatorname{ad} x_1)^{m-1-j}(P_j).$$

Since $P_m \in \ker(\pi) \cap U_m$, we obtain from Lemma 3.3.7 that

$$q^{m(m-1)/2}(-r)^m s = -1.$$

Further, we may assume that $v_j \in \ker(\pi) \cap U'_m$ for any $j \in \mathbb{J} \cap [0, m-1]$. Hence $Q_2^{j,m-1-j} = 0$ for any $j \in \mathbb{J} \cap [0, m-1]$ by Lemma 3.3.11. Since $\mathrm{char}(\Bbbk) = 0$, from Lemma 3.3.15 we conclude that $q^{m+j-1}r^2 \neq 1$ for any $j \in \mathbb{J} \cap [0, m-1]$. Thus $m \in \mathbb{J}$. Then Equation (3.21) follows from (3.22) and from induction hypothesis. □

Corollary 3.3.17. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $k, l \in \mathbb{N}_0$ with $k \geq l$. Suppose that $(k+l)^!_q b_{k+l} \neq 0$, and that $q^{k^2} r^k s = -1$ if $k = l$. Then the following are equivalent.

(1) $[x_1^k x_2 x_1^l x_2]$ is a root vector,

(2) $\big|\mathbb{J} \cap [0, k+l]\big| \leq l$.

Proof. By assumption, $[x_1^k x_2 x_1^l x_2]$ is a root vector candidate. Proposition 3.3.3 and Example 1.4.5 imply that $[x_1^k x_2 x_1^l x_2]$ is a root vector if and only if any root vector candidate of degree $(k+l)\alpha_1 + 2\alpha_2$, which is not a root vector, is of the form $[x_1^{k_1} x_2 x_1^{k_2} x_2]$ with $k_1 + k_2 = k + l$, $0 \leq k_2 < l$. This just means that $\dim\big(\ker(\pi) \cap U_{k+l}\big) \leq l$. According to Theorem 3.3.16, the latter is equivalent to $\big|\mathbb{J} \cap [0, k+l]\big| \leq l$. □

Corollary 3.3.18. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $m \in \mathbb{N}_0$ such that $(m)^!_q b_m \neq 0$. Then the multiplicity of $m\alpha_1 + 2\alpha_2$ is

$$m' - \big|\mathbb{J} \cap [0, m]\big|,$$

where

$$m' = \begin{cases} (m+1)/2 & \text{if } m \text{ is odd,} \\ m/2 & \text{if } m \text{ is even and } q^{m^2/4} r^{m/2} s \neq -1, \\ m/2 + 1 & \text{if } m \text{ is even and } q^{m^2/4} r^{m/2} s = -1. \end{cases}$$

Proof. By Example 1.4.5, m' is just the number of root vector candidates of degree $m\alpha_1 + 2\alpha_2$. Corollary 3.3.17 implies that $|\mathbb{J} \cap [0, m]|$ is the number of root vector candidates of degree $m\alpha_1 + 2\alpha_2$ which are not root vectors. This implies the claim. $\square$

Remark 3.3.19. It is known that any real root has multiplicity one. The converse is generally not true: If $r \neq 1$, then $\alpha_1 + \alpha_2$ is a root with multiplicity one, but the condition, whether it is real or imaginary, is rather complicated. In particular, with our results we obtain a necessary condition for the reality of a root, but no sufficient condition.

The following proposition treats the question in Corollary 3.3.18 if the assumption on m is not satisfied. Recall that $R_1(V)$ is the reflection of V on the first vertex.

Proposition 3.3.20. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $k, m \in \mathbb{N}_0$ such that $(k)^!_q b_k \neq 0$, $(k+1)_q(1 - q^k r) = 0$, and $m \geq k$. Then the multiplicity of $m\alpha_1 + 2\alpha_2$ is the same as the multiplicity of $(2k - m)\alpha_1 + 2\alpha_2$ of $\mathcal{B}(R_1(V))$.

Proof. The claim is a very special case of the invariance of multiplicities under reflections, which was proved in [13]. $\square$

Remark 3.3.21. According to the explanations in Section 1.5, in Proposition 3.3.20 we have $c_{12} = -k$. Hence the braiding matrix $(q'_{ij})_{i,j \in \{1,2\}}$ of $R_1(V)$ satisfies

$$q'_{11} = q, \quad q'_{12}q'_{21} = r, \quad q'_{22} = s$$

whenever $q^k r = 1$, and

$$q'_{11} = q, \quad q'_{12}q'_{21} = q^2 r^{-1}, \quad q'_{22} = qr^k s$$

whenever $q^k r \neq 1$ (and then $(k+1)_q = 0$). Since $2k - m \leq k$, the multiplicity of $(2k - m)\alpha_1 + 2\alpha_2$ of $\mathcal{B}(R_1(V))$ can be obtained using Corollary 3.3.18 with the set $\mathbb{J}$ for $(q'_{ij})_{i,j \in \{1,2\}}$.

Finally, we discuss the multiplicity of roots in some special cases.

Corollary 3.3.22. Assume that $\mathrm{char}(\Bbbk) = 0$. Let $m \in \mathbb{N}_0$.

(1) Assume that $m \in \{1, 2, 3, 4, 6\}$ and that $(m)^!_q b_m \neq 0$. Then $m\alpha_1 + 2\alpha_2$ is not a root if and only if q, r, s satisfy the conditions given in Table 3.3.

(2) Assume that $m = 2k + 1 \geq 5$ is odd and that $(k + 3)^!_q b_{k+3} \neq 0$. Then $m\alpha_1 + 2\alpha_2$ is a root of $\mathcal{B}(V)$.

(3) Assume that $m = 2k \geq 8$ and that $(k + 4)^!_q b_{k+4} \neq 0$. Then $m\alpha_1 + 2\alpha_2$ is a root of $\mathcal{B}(V)$.

Proof. (1) We apply Corollary 3.3.18 case by case.

Assume that $m = 1$. Then $m' = 1$. Hence $\alpha_1 + 2\alpha_2$ is not a root if and only if $\big|\mathbb{J} \cap [0, 1]\big| = 1$. According to Example 3.3.14, this is equivalent to $(1+s)(1-rs) = 0$.

Assume that $m = 2$. Then $\big|\mathbb{J} \cap [0, 2]\big| \leq 1$ by Example 3.3.14, and equality holds if and only if $(1 + s)(1 - rs)(1 + qr^2 s) = 0$. Hence, if $qrs \neq -1$, then $m' = 1$ and the claim is proven. On the other hand, if $qrs = -1$, then $m' = 2$ and hence $2\alpha_1 + 2\alpha_2$ is a root. Note that in this case $(1 + s)(1 - rs)(1 + qr^2 s) \neq 0$ since

$$(m)^!_q b_m = (2)_q (1 - r)(1 - qr) \neq 0.$$

Thus the claim is valid also in this case.

Assume that $m = 3$. Then $m' = 2$. Hence $3\alpha_1 + 2\alpha_2$ is not a root if and only if $\big|\mathbb{J} \cap [0, 3]\big| = 2$. Due to Lemma 3.3.13, the latter is only possible if $\mathbb{J} \cap [0, 3] = \{0, 3\}$. This means that $s = -1$, $q^3 r^3 s = 1$, and $q^2 r^2 \neq 1$. Because of $(3)^!_q b_3 \neq 0$ we can rewrite this condition to $s = -1$, $(3)_{-qr} = 0$.

The conditions for $m = 4$ and $m = 6$ can be obtained similarly.

(2) Assume first that $(m)^!_q b_m \neq 0$. By Corollary 3.3.18, the multiplicity of $m\alpha_1 + 2\alpha_2$ is $k + 1 - \big|\mathbb{J} \cap [0, m]\big|$. By Lemma 3.3.13, $\big|\mathbb{J} \cap [0, m]\big| \leq m/3 + 1$. Since $3k - m = k - 1 > 0$, we conclude that $m\alpha_1 + 2\alpha_2$ is a root of $\mathcal{B}(V)$.

Assume now that $(m)^!_q b_m = 0$. Since $(k + 3)^!_q b_{k+3} \neq 0$ by assumption, for the Cartan matrix entry c_{12} we obtain that $k + 3 \leq -c_{12} < m$. Moreover,

$$s_1(m\alpha_1 + 2\alpha_2) = (-2c_{12} - m)\alpha_1 + 2\alpha_2$$

and $-2c_{12} - m$ is odd and lesser than $-c_{12}$. Moreover,

$$-2c_{12} - m - 5 = -2c_{12} - 2k - 6 \geq 0$$

and hence Proposition 3.3.20 and the previous paragraph for $R_1(V)$ imply that $m\alpha_1 + 2\alpha_2$ is a root of $\mathcal{B}(V)$.

(3) Similar to the proof of (2). Note that $2k\alpha_1 + 2\alpha_2$ is always a root if $q^{k^2} r^k s = -1$ and $(k+1)_q^! b_{k+1} \neq 0$ because of Lemma 3.3.1. Hence only the case where $q^{k^2} r^k s \neq -1$ has to be considered in detail. □

$m\alpha_1 + 2\alpha_2$	non-root conditions
$\alpha_1 + 2\alpha_2$	$(1+s)(1-rs) = 0$
$2\alpha_1 + 2\alpha_2$	$(1+s)(1-rs)(1+qr^2 s) = 0$
$3\alpha_1 + 2\alpha_2$	$s = -1, (3)_{-qr} = 0$
$4\alpha_1 + 2\alpha_2$	$s = -1$, $(3)_{-qr} = 0$ or $s = -1$, $q^3 r^2 = -1$ or $rs = 1$, $(3)_{-q^2 r} = 0$
$6\alpha_1 + 2\alpha_2$	$q = 1, s = -1$, $(3)_{-r} = 0$

Table 3.1: Table for Corollary 3.3.22

As an application we give two examples at the end of this chapter.

Example 3.3.23. Assume that $\mathrm{char}(\Bbbk) = 0$, $r = q^{-2}$, $s = q$, and that $q^2 \neq 1$. Then the braiding of V is of Cartan type with Cartan matrix $\begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$. The infinitesimal braiding of the positive part of the quantized enveloping algebra $U_v(\widehat{\mathfrak{sl}}_2)$ is of this form. In this case, $m\alpha_1 + \alpha_2$ is a root if and only if $0 \leq m \leq 2$. These roots always have multiplicity one. The root $\alpha_1 + \alpha_2$ is imaginary. By Definition 3.3.12 we obtain that

$$0, 1 \notin \mathbb{J}; \qquad 2 \in \mathbb{J} \text{ if and only if } q^2 = -1.$$

Corollary 3.3.18 allows us to determine the multiplicities of $m\alpha_1 + 2\alpha_2$ for $0 \leq m \leq 2$. We obtain that $2\alpha_2$ is not a root and that $\alpha_1 + 2\alpha_2$ is a root with multiplicity one. The multiplicity of $2\alpha_1 + 2\alpha_2$ is $1 - |\mathbb{J} \cap [0,2]|$, which is 1 if $q^2 \neq -1$ and 0 if $q^2 = -1$. The multiplicity of the root $2\alpha_1 + 2\alpha_2$ in the Kac-Moody algebra $\widehat{\mathfrak{sl}}_2$ is 1.

Note that $R_1(V)$ is of diagonal type with the same structure constants q, r, s as V, since V is of Cartan type, see [3] or [13]. Thus, according to Proposition 3.3.20, $3\alpha_1 + 2\alpha_2$ is a root of multiplicity 1 and $m\alpha_1 + 2\alpha_2$ with $m \geq 4$ is not a root.

Example 3.3.24. Assume that $\mathrm{char}(\Bbbk) = 0$, $r = q^{-4}$, $s = q^4$, and that $q^m \neq 1$ for any $1 \leq m \leq 4$. Then the braiding of V is of Cartan type with Cartan matrix $\begin{pmatrix} 2 & -4 \\ -1 & 2 \end{pmatrix}$. The infinitesimal braiding of the positive part of the quantized enveloping algebra $U_v(\mathfrak{g})$, where $\mathfrak{g}$ is of type $A_2^{(2)}$, is of this form. In this case, $m\alpha_1 + \alpha_2$ is a root if and only if $0 \leq m \leq 4$. These roots always have multiplicity one. By Definition 3.3.12 we obtain the following.

(1) $0 \in \mathbb{J}$ if and only if $q^4 = -1$.

(2) $1 \in \mathbb{J}$ if and only if $q^4 \neq -1$.

(3) $2, 3 \notin \mathbb{J}$.

(4) $4 \in \mathbb{J}$ if and only if $q^4 - q^2 + 1 = 0$.

Now we use Corollary 3.3.18 to determine the multiplicities of $m\alpha_1 + 2\alpha_2$ for $0 \leq m \leq 4$. We obtain that $|\mathbb{J} \cap [0,m]| = 1$ for $1 \leq m \leq 3$. Hence $2\alpha_2, \alpha_1 + 2\alpha_2$ and $2\alpha_1 + 2\alpha_2$ are not roots, $3\alpha_1 + 2\alpha_2$ is a (real) root of multiplicity 1, and the multiplicity of $4\alpha_1 + 2\alpha_2$ is $2 - |\mathbb{J} \cap [0,4]|$, which is 0 if $q^4 - q^2 + 1 = 0$ and 1 otherwise. The multiplicity of the root $4\alpha_1 + 2\alpha_2$ in the Kac-Moody algebra $\mathfrak{g}$ is 1.

Since V is of Cartan type, $R_1(V)$ is of diagonal type with the same structure constants q, r, s as V. Thus, according to Proposition 3.3.20, $5\alpha_1 + 2\alpha_2$ is a (real) root of multiplicity 1 and $m\alpha_1 + 2\alpha_2$ for $m > 5$ is not a root.

Deutsche Zusammenfassung

In dieser Arbeit betrachten wir die Multiplizitäten von Wurzel von Nichols-Algebren von diagonalem Typ. Basierend auf einer Ungleichung für die Anzahl der Lyndon-Wörter [18] und der Identität für die Shuffle-Map [11] werden wir darlegen, wann die Multiplizität einer Wurzel geringer ist als in der Tensoralgebra eines geflochtenen Vektorraumes von diagonalem Typ. Ferner werden wir die Dimension des Kerns der Shuffle-Map, welche wir als Operator betrachten, der auf der freien Algebra wirkt, bestimmen. Darüber hinaus geben wir einen expliziten Ausdruck für die Multiplizit ät einer Klasse von Wurzeln einer Nichols-Algebra von diagonalem Typ von Rang zwei an.

Mithilfe der Poincaré-Birkhoff-Witt Basis von V. Kharchenko [22] hat I. Heckenberger das Wurzelsystem und die Weyl-Gruppe von Kac-Moody-Algebren auf Nichols-Algebren von diagonalem Typ [13] verallgemeinert. Wir sagen eine Nichols-Algebra $\mathcal{B}(V)$ (oder ein geflochtener Vektorraum (V, c)) ist von diagonalem Typ, wenn es eine Basis $\{x_i | 1 \leq i \leq n\}$ von V und eine Matrix $(q_{ij})_{1\leq i,j\leq n} \in (\Bbbk^\times)^{n\times n}$ gibt, so dass $c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i$ für alle $1 \leq i, j \leq n$, wobei $\Bbbk$ ein Körper ist. Die Matrix $(q_{ij})_{1\leq i,j\leq n}$ wird als die *Verzopfungsmatrix* von $\mathcal{B}(V)$ (oder V) bezeichnet. Das Wurzelsystem und der Weyl-Gruppoid sind grundlegende Werkzeuge, um Nichols-Algebren von diagonalem Typ zu studieren. Diese Werkzeuge haben ein gutes Verständnis für die Struktur endlich dimensionaler Nichols-Algebren von diagonalem Typ ermöglicht. In einer Reihe von Arbeiten [14, 16, 17] hat I. Heckenberger die endlich dimensionalen Nichols-Algebren von diagonalem Typ über Körpern von Charakteristik Null klassifiziert. Es zeigte sich für endlich dimensionale Nichols-Algebren von diagonalem Typ, dass die Wurzeln bezüglich der Wirkung von Weyl-Gruppenoid reelle Wurzeln sind und ihre Multiplizität eins ist

[16, 10]. Jedoch ist das Wissen über imaginäre Wurzeln und ihre Multiplizitäten für Nichols-Algebren von diagonalem Typ gering. Unsere Ergebnisse verbessern das Verständnis der Nichols-Algebra-Theorie in dieser Hinsicht.

Die Arbeit enthält drei Kapitel. In Kapitel 1 werden die Begriffe der Nichols-Algebra $\mathcal{B}(V)$, des geflochtenen Vektorraums, des Lyndon-Worts und des Yetter-Drinfel'd-Moduls eingeführt. Außerdem diskutieren wir das Wurzelsystem sowie Wurzelvektorkandidaten und Wurzelvektoren einer Nichols-Algebra $\mathcal{B}(V)$ von diagonalem Typ.

In Kapitel 2 geben wir ein Kriterium an, um zu entscheiden, ob eine gegebene Nichols-Algebra von diagonalem Typ eine freie Algebra ist. Als eine Anwendung dieses Ergebnisses geben wir eine spezielle Familie von Nichols-Algebren von diagonalem Typ. Es stellt sich heraus, dass die Freiheit von diesen Nichols-Algebren mit den Lösungen einer bestimmten Sorte von quadratischen diophantischen Gleichungen verwandt ist. Es wird eine Familie von Elementen $(P_{\underline{m}})_{|\underline{m}|\geq 2, \underline{m}\in\mathbb{N}_0^n}$ im Polynomialring $\mathbb{Z}[q_{ij} \mid 1 \leq i,j \leq n]$ definiert, die in diesem Kapitel eine bedeutende Rolle spielen. Sei $\mathcal{B}(V)$ eine Nichols-Algebra von diagonalem Typ von Rang n mit Verzopfungsmatrix $\boldsymbol{q}$.

Satz 3.3.25. (siehe Satz 2.3.3) $\mathcal{B}(V)$ ist die freie Algebra genau dann, wenn $P_{\underline{m}}(\boldsymbol{q}) \neq 0$ für alle $\underline{m} \in \mathbb{N}_0^n$ mit $|\underline{m}| \geq 2$.

Angenommen, $\mathcal{B}(V)$ ist eine Nichols-Algebra von diagonalem Typ über einem Körper $\Bbbk$ von Charakteristik Null und $P_{\underline{m}}(\boldsymbol{q}) = 0$. Die zwei Zahlen $n_1(\boldsymbol{q}), n_2(\boldsymbol{q})$ werden in Lektion 2.4 definiert.

Satz 3.3.26. (siehe Satz 2.5.2) Angenommen, $\Bbbk$ ist ein Körper von Charakteristik Null. Sei $\underline{m} = (m_1, m_2, \dots, m_n) \in \mathbb{N}_0^n$ und $m = \sum_{i=1}^n m_i$ mit $m \geq 2$, so dass $P_{\underline{m}}(\boldsymbol{q}) = 0$, und $P_{\underline{l}} \neq 0$ für alle $\underline{l} < \underline{m}$. Dann gilt

$$\dim(\ker(\rho_m(S_{1,m-1})|V_{\underline{m}})) = n_1(\boldsymbol{q}) - n_2(\boldsymbol{q}).$$

In Kapitel 3 untersuchen wir die Multiplizitäten von Wurzel von Nichols-Algebren von diagonalem Typ von Rang zwei. Wir konzentrieren uns auf die Wurzeln der Form $m\alpha_1 + 2\alpha_2$, $m \in \mathbb{N}_0$, wobei $\{\alpha_1, \alpha_2\}$ die Standardbasis von

$\mathbb{Z}^2$ ist. Sei $q_{11} = q$, $q_{12}q_{21} = r$, $q_{22} = s$, wobei $(q_{ij})_{1\leq i,j\leq 2}$ die Verzopfungsmatrix von V ist. Wir beschäftigen uns mit der Frage, wann ein entsprechender Wurzelvektor-Kandidat ein Wurzelvektor ist (über Körpern von Charakteristik Null). Dazu definieren wir eine Menge $\mathbb{J}_{q,r,s} \in \mathbb{N}_0$, um das Ergebnis zu formulieren. Die Menge $\mathbb{J}_{q,r,s} \in \mathbb{N}_0$ misst auch die Multiplizitäten aller Wurzeln der Form $m\alpha_1 + 2\alpha_2$, $m \in \mathbb{N}_0$. Wir zeigen in Satz 3.3.3, wenn ein gegebener Wurzelvektor-Kandidat ein Wurzelvektor ist, dass jeder lexikografisch grössere Wurzelvektor-Kandidat desselben Grads ebenfalls ein Wurzelvektor ist. Korollar 3.3.17 gibt für diesen Fall eine vollständige Antwort auf die Frage, wann ein Wurzelvektor-Kandidat ein Wurzelvektor ist. Weiterhin geben wir für jedes $m \in \mathbb{N}_0$ die Multiplizität der Wurzel $m\alpha_1 + 2\alpha_2$ über einem Körper von Charakteristik Null in Korollar 3.3.18 an. Diese Ergebnisse basieren auf Satz 3.3.16.

Sei $b_k = \prod_{j=0}^{k-1}(1 - q^j r)$ mit $k \in \mathbb{N}_0$ und P_j das Element in (3.13). Für alle $n, k \in \mathbb{N}_0$ sei $U_n \subseteq \mathcal{B}(V)$ ein Unterraum in (3.11).

Satz 3.3.27. (siehe Satz 3.3.16) Angenommen, $\mathrm{char}(\Bbbk) = 0$. Sei $m \in \mathbb{N}_0$ so dass $(m)^!_q b_m \neq 0$. Dann bilden die Vektoren $(\mathrm{ad}\, x_1)^{m-j}(P_j)$ mit $j \in \mathbb{J} \cap [0, m]$ eine Basis von $\ker(\pi) \cap U_m$.

Bibliography

[1] N. Andruskiewitsch and H.-J. Schneider. Lifting of quantum linear Spaces and pointed Hopf algebras of order p^3. *Journal of Algebra*, 209.2 (1998): 658–691.

[2] N. Andruskiewitsch and H.-J. Schneider. Finite quantum groups and Cartan matrices. *Advances in Mathematics*, 154.1 (2000): 1–45.

[3] N. Andruskiewitsch and H.-J. Schneider. Pointed Hopf algebras. *In New Directions in Hopf Algebras volume* 43 *of MSRI Publications*. Cambridge University, Press, 2002.

[4] N. Andruskiewitsch and H.-J. Schneider. A characterization of quantum groups. *Journal für die reine und angewandte Mathematik* (*Crelles Journal*), 2004.577 (2004): 81-104.

[5] N. Andruskiewitsch and H.-J. Schneider. On the classification of finite-dimensional pointed Hopf algebras. *Annals of Mathematics*, (2010): 375-417.

[6] I. Angiono. On Nichols algebras of diagonal type. *Journal für die reine und angewandte Mathematik* (*Crelles Journal*), 2013.683 (2013): 189-251.

[7] I. Angiono. A presentation by generators and relations of Nichols algebras of diagonal type and convex orders on root systems. *Journal of European Mathematical Society*, 17 (2015): 2643-2671.

[8] J. Arndt. Matters Computational: ideas, algorithms, source code. *Springer Science* & *Business Media*, 2010.

[9] G. Arunkumar, D. Kus, and R. Venkatesh. Root multiplicities for Borcherds algebras and graph coloring. *Journal of Algebra*, 499 (2018): 538-569.

[10] M. Cuntz and I. Heckenberger. Weyl groupoids with at most three objects. *Journal of Pure and Applied Algebra*, 213.6 (2009): 1112-1128.

[11] G. Duchamp, A. Klyachko, D. Krob, and J-Y. Thibon. Noncommutative symmetric functions iii: Deformations of cauchy and convolution algebras. *Discrete Mathematics & Theoretical Computer Science*, 1.2 (1997): 159–216.

[12] X. Fang. Non-symmetrizable quantum groups: defining ideals and specialization. *arXiv:1303.5994*, (2013).

[13] I. Heckenberger. The Weyl groupoid of a Nichols algebra of diagonal type. *Inventiones Mathematicae*, 164.1 (2006):175–188.

[14] I. Heckenberger. Examples of finite-dimensional rank 2 Nichols algebras of diagonal type. *Compositio Mathematica*, 143.1 (2007): 165-190.

[15] I. Heckenberger. Nichols algebras. *Lectture at ECNU, Shanghai, July 2008.*

[16] I. Heckenberger. Rank 2 Nichols algebras with finite arithmetic root system. *Algebras and Representation Theory*, 11.2 (2008): 115-132.

[17] I. Heckenberger. Classification of arithmetic root systems. *Advances in Mathematics*, 220.1 (2009): 59–124.

[18] I. Heckenberger and J. Sawada. A pascal-like bound for the number of necklaces with fixed density. *arXiv:1801.09516*, 2018.

[19] I. Heckenberger and Y. Zheng. Root multiplicities for Nichols algebras of diagonal type of rank two. *Journal of Algebra*, 496 (2018): 91–115.

[20] I. Heckenberger and Y. Zheng. A characterization of Nichols algebras of diagonal type which are free algebras. *arXiv:1806.05903*, 2018

[21] V. G. Kac. Infinite-dimensional Lie algebras. *Cambridge university press*, volume 44. 1994.

[22] V. K. Kharchenko. A quantum analog of the Poincaré-Birkhoff-Witt theorem. *Algebra and Logic*, 38.4 (1999): 259–276.

[23] M. Lothaire. Combinatorics on words. *Cambridge university press, Volume* 17, 1997.

[24] S. Majid. Cross products by braided groups and bosonization. *Journal of Algebra*, 163.1 (1994): 165-190.

[25] S. Majid. Noncommutitive differentials and Yang-Mills on permutation groups S_n. *Hopf algebras in noncommutative geometry and physics, volume* 239 *of Lecture Notes in Pure and Applied Mathematics*, 189-213. Dekker, New York, 2005.

[26] W. Nichols. Bialgebras of type one. *Communications in Algebra*, 6.15 (1978): 1521-1552.

[27] D. E. Radford. The structure of Hopf algebras with a projection. *Journal of Algebra*, 92.2 (1985): 322-347.

[28] D. E. Radford. Hopf algebras. *Series on Knots and Everything,* 49. *World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ*, 2012.

[29] M. Rosso. Quantum groups and quantum shuffles. *Inventiones Mathematicae*, 133.2 (1998): 399–416.

[30] F. Ruskey and J. Sawada. An efficient algorithm for generating necklaces with fixed density. *SIAM Journal on Computing*, 29.2 (1999): 671–684.

[31] P. Schauenburg. A characterization of the Borel-like subalgebras of quantum enveloping algebras. *Communications in algebra*, 24.9 (1996): 2811–2823.

[32] M. Takeuchi. Survey of braided Hopf algebras. *Contemporary Mathematics*, 267 (2000): 301-324.

[33] J. Wang and I. Heckenberger. Rank 2 Nichols algebras of diagonal type over fields of positive characteristic. Symmetry, Integrability and Geometry. Methods and Applications, 11 (2015).

[34] J. Wang. Rank three Nichols algebras of diagonal type over arbitrary fields. *Israel Journal of Mathematics*, 218.1 (2017): 1-26.

[35] S. L. Woronowicz. Compact matrix pseudogroups. *Communications in Mathematical Physics*, 111.4 (1987): 613-665.

[36] S. L. Woronowicz. Differential calculus on compact matrix pseudogroups (quantum groups). *Communications in Mathematical Physics*, 122.1 (1989): 125-170.

Erklärung

Ich versichere, dass ich meine Dissertation

Root multiplicities for Nichols algebras of diagonal type

selbständig, ohne unerlaubte Hilfe angefertigt und mich dabei keiner anderen als der von mir ausdrüklich bezeichneten Quellen und Holfen bedient habe.

Die Dissertation wurde in der jetzigenoder einer ähnlichen Form noch bei keiner anderen Hochschule eingereicht und hat noch keinern sonstigen Prüfungszwecken gedient.

Marburg, den 02. July. 2018
Ying Zheng

CV of the author

Name:	Ying Zheng
	Philipps-Universität Marburg
Address:	Fachbereich Mathematik und Informatik
	Hans-Meerwein-Straße (Paketpost: 35043 Marburg)
Nationality:	Chinese
Email:	z12522y@163.com

Education:

2015.09-now Ph.D study at East China Normal University, Shanghai, China (Mast-Doctor combined program)
supervisor: Prof. Naihong Hu

2016.10-now as a visiting Ph.D student, Marburg University, Germany (Philipps-Universität Marburg)
supervisor: Prof. Dr. István Heckenberger

2013.09-2015.07 Master study at East China Normal University, Shanghai, China (Mast-Doctor combined program)
supervisor: Prof. Naihong Hu

Publications/Preprints:

(1). I. Heckenberger and Y. Zheng. A characterization of Nichols algebras of diagonal type which are free algebras. arXiv:1806.05903, 2018.

(2). I. Heckenberger and Y. Zheng. Root multiplicities for Nichols algebras of diagonal type of rank two. Journal of Algebra, 496:91–115, 2018.