Chapter 2
Poincaré-Birkhoff-Witt Basis

Abstract In this chapter, we demonstrate that every character Hopf algebra has a PBW basis. A Hopf algebra H is referred to as a character Hopf algebra if the group G of all group-like elements is commutative and H is generated over $\mathbf{k}[G]$ by skew-primitive semi-invariants, whereas a well-ordered subset $V \subseteq H$ is a set of PBW generators of H if there exists a function $h : V \to \mathbf{Z}^+ \cup \{\infty\}$, called the height function, such that the set of all products

$$gv_1^{n_1}v_2^{n_2} \cdots v_k^{n_k},$$

where $g \in G, \ \ v_1 < v_2 < \ldots < v_k \in V, \ \ n_i < h(v_i), 1 \leq i \leq k$ is a basis of H.

In this chapter, we demonstrate that every character Hopf algebra has a PBW basis. According to Definition 1.11, a Hopf algebra H is referred to as a character Hopf algebra if the group G of all group-like elements is commutative and H is generated over $\mathbf{k}[G]$ by skew-primitive semi-invariants.

Definition 2.1 A well-ordered subset V of a character Hopf algebra H is considered a set of *PBW generators* of H if there exists a function $h : V \to \mathbf{Z}^+ \cup \{\infty\}$, called the *height function*, such that the set of all products

$$gv_1^{n_1}v_2^{n_2} \cdots v_k^{n_k}, \tag{2.1}$$

where $g \in G, \ \ v_1 < v_2 < \ldots < v_k \in V, \ \ n_i < h(v_i), 1 \leq i \leq k$ is a basis of H. The value $h(v)$ is referred to as the *height* of v in V.

For example, the standard words, due to Theorem 1.1, form a set of PBW generators with infinite heights of the free character Hopf algebra $G\langle X\rangle$. This fact provides an idea concerning how to find the PBW basis of an arbitrary character Hopf algebra.

We establish a homomorphism $G\langle X\rangle \to H$ of the character Hopf algebras. The values of elements (2.1) in H span all of H but may be linearly dependent. If the value of a standard word v is a linear combination of the monomials (2.1) with $v_i < v$, then the values of elements (2.1), where $v_i \neq v$, continue to span H. Hence, the set of all standard words may be reduced to the set of "hard" standard words,

V. Kharchenko, *Quantum Lie Theory*, Lecture Notes in Mathematics 2150,
DOI 10.1007/978-3-319-22704-7_2

i.e., standard words v whose values in H are not linear combinations of (2.1) with $v_i < v$.

Then, one must demonstrate that the increasing products of "hard" standard words are linearly independent in H. For this task, we must use the coproduct. If U is such a linear combination, then we may (somehow) find its coproduct in the free character Hopf algebra

$$\Delta(U) = U \otimes 1 + \sum U_i' \otimes U_i'' + g \otimes U, \quad g \in G.$$

If $U = 0$ in H, then in $H \otimes H$ we have the equality

$$\sum U_i' \otimes U_i'' = 0. \tag{2.2}$$

This equality of tensors provides one equation corresponding to each basis element of the space spanned by all U_i''. Because the U_i'''s have degrees less than that of U, we may theoretically decompose them in linear combinations of increasing products of "hard" standard words that are already linearly independent in H (by induction). This amount of information is sufficient for obtaining the required contradiction.

Because of technical reasons, it was impossible to realize these considerations directly for "hard" standard words; Instead, developing the above logic for nonassociative standard words seemed possible, interpreting the bracket as the skew commutator of polynomials. Surprisingly, after this logic was developed, demonstrating that the "hard" standard words are indeed the PBW generators became straightforward.

The equality (2.2) is not equivalent to setting U to be zero but does indicate that U is skew-primitive. In other words, while solving the above system of equations, we will obtain information on the skew-primitive elements of character Hopf algebras. This information is given in Theorem 2.3.

2.1 PBW Bases of the Free Character Hopf Algebra

Let $G\langle Y\rangle = G\langle X\rangle$ be the free character Hopf algebra, see Sect. 1.5.3. Recall that $x_i,\ i \in I$ are free variables with the coproduct given by

$$\Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i, \quad \Delta(g_i) = g_i \otimes g_i, \tag{2.3}$$

whereas associated with each variable x_i is a character $\chi^i : G \to \mathbf{k}^*$ such that $g^{-1}x_i g = \chi_i(g) g x_i$, for all $g \in G$, see (1.66).

For every word u in X let g_u denotes a group-like element that appears from u by replacing each x_i with g_i. Similarly, χ^u is a character that appears from u by replacing each x_i with χ^i. Because both the group G and the group of characters are commutative, the values g_u, χ^u are defined on the set of all homogeneous elements in each $x_i \in X$. For a pair u, v of homogeneous polynomials in X put

$$p_{u,v} = \chi^u(g_v). \tag{2.4}$$

Obviously, the following equalities hold:

$$p_{uv,w} = p_{u,w}p_{v,w}, \quad p_{u,vw} = p_{u,v}p_{u,w}. \tag{2.5}$$

Sometimes it is more convenient to denote this bimultiplicative operator by $p(u, v)$. Of course, the operator $p(\text{-}, \text{-})$ is completely defined by the parameters $p_{ik} = \chi^i(g_k)$.

In terms of this operator, the brackets (1.67) take the form

$$[u, v] = uv - p_{u,v}vu, \quad [u, v]^* = uv - p^{-1}_{v,u}vu. \tag{2.6}$$

Lemma 2.1 *The brackets* $[,]$ *satisfy the following "Jacobi identity"*:

$$[[u, v], w] = [u, [v, w]] + p^{-1}_{w,v}[[u, w], v] + (p_{v,w} - p^{-1}_{w,v})[u, w] \cdot v, \tag{2.7}$$

where $\cdot$ *stands for usual multiplication in the free algebra.*

Proof We have

$$[[u, v], w] = [uv - p_{u,v}vu, w] = uvw - p_{uv,w}wuv - p_{u,v}vuw + p_{u,v}p_{vu,w}wvu.$$

Under the substitution $w \leftrightarrow v$, this equality becomes

$$[[u, w], v] = uwv - p_{uw,v}vuw - p_{u,w}wuv + p_{u,w}p_{wu,v}vwu.$$

Similarly,

$$[u, [v, w]] = [u, vw - p_{v,w}wv] = uvw - p_{u,wv}vwu - p_{v,w}uwv + p_{v,w}p_{u,wv}wvu,$$

and

$$[u, w] \cdot v = uwv - p_{u,w}wuv.$$

It remains to compare the coefficients at all six permutations of uvw in (2.7).

$$\begin{aligned}
uvw : &\quad 1 = 1;\\
wuv : &\quad -p_{uv,w} = -p^{-1}_{w,v}p_{u,w} + (p_{v,w} - p^{-1}_{w,v})p_{u,w};\\
vuw : &\quad -p_{u,v} = -p^{-1}_{w,v}p_{uw,v};\\
wvu : &\quad p_{u,v}p_{vu,w} = p_{v,w}p_{u,wv};
\end{aligned}$$

$$uwv: \quad 0 = p_{w,v}^{-1} - p_{v,w} + (p_{v,w} - p_{w,v}^{-1});$$

$$vwu: \quad 0 = p_{w,v}^{-1} p_{u,w} p_{wu,v} - p_{u,vw}.$$

□

Lemma 2.2 *The following formulas link the brackets to multiplication:*

$$[u, v \cdot w] = [u, v] \cdot w + p_{u,v} v \cdot [u, w], \tag{2.8}$$

$$[u \cdot v, w] = p_{v,w}[u, w] \cdot v + u \cdot [v, w]. \tag{2.9}$$

Proof We have, $[u, v \cdot w] = uvw - p_{u,vw} vwu = uvw - p_{u,v} vuw + p_{u,v} vuw - p_{u,v} p_{u,w} vwu = [u, v] \cdot w + p_{u,v} v \cdot [u, w]$. Similarly, $[u \cdot v, w] = uvw - p_{uv,w} wuv = uvw - p_{v,w} uwv + p_{v,w} uwv - p_{uv,w} wuv = u \cdot [v, w] + p_{v,w}[u, w] \cdot v$. □

Definition 2.2 A *super-letter* is a polynomial that equals a standard nonassociative word where the brackets $[,]$ are defined in (2.6).

Every noncommutative polynomial f in X is a linear combination of different words $f = \sum \alpha_i u_i$. Recall that a leading word of f is the maximal word u_i that occurs in this decomposition with nonzero coefficient.

Lemma 2.3 *A leading word of a super-letter* $[u]$ *with respect to the lexicographical order is the word* u, *and it occurs in the decomposition of* $[u]$ *with coefficient 1.*

Proof We use induction on length. If $[u] = [[v][w]]$ then the super-letter $[u]$ equals $[v][w] - p_{u,w}[w][v]$. By the inductive hypothesis, $[v]$ and $[w]$ are homogeneous polynomials with the leading words v and w, respectively. The leading word with respect to the lexicographical order of a product of two homogeneous polynomials equals the product of leading words of the factors. Therefore, the leading word of $[v][w]$ equals vw and has coefficient 1; the leading word of $[w][v]$ equals wv and is less than vw because $vw = u$ is a standard word. □

The proven Lemma demonstrates that different standard words u and v define distinct super-letters $[u]$ and $[v]$. We define the order on the set of all super-letters thus:

$$[u] > [v] \iff u > v. \tag{2.10}$$

Definition 2.3 A word in super-letters is called a *super-word*. A super-word is said to be *increasing* if it has the form

$$W = [u_1]^{k_1} [u_2]^{k_2} \cdots [u_m]^{k_m}, \tag{2.11}$$

where $u_1 < u_2 < \ldots < u_m$. On the set of all super-words, we fix the lexicographic order defined by the ordering of super-letters in (2.10).

Lemma 2.4 *An increasing super-word $W = [w_1]^{k_1}[w_2]^{k_2}\cdots[w_m]^{k_m}$ is greater than an increasing super-word $V = [v_1]^{m_1}[v_2]^{m_2}\cdots[v_k]^{m_k}$ if and only if the word $w = w_1^{k_1}w_2^{k_2}\cdots w_m^{k_m}$ is greater than the word $v = v_1^{m_1}v_2^{m_2}\cdots v_k^{m_k}$. Moreover, the leading word of the polynomial W, when decomposed into a linear combinations of words, equals w and has coefficient 1.*

Proof Let $W > V$. Then $w_1 \geq v_1$ in view of the ordering of super-letters. If $w_1 = v_1$, we can remove one factor from the left of both V and W, and then proceed by induction. Therefore, we will put $w_1 > v_1$. If w_1 is not the beginning of v_1, then the inequality $w_1 > v_1$ can be multiplied from the right by suitable distinct elements, which yields $w > v$, as required.

Let $v_1 = w_1T$, $T = (w_1^{k_1-1}w_2^{k_2}\cdots w_{s-1}^{k_{s-1}})w_s^l \cdot v_1'$, where $0 \leq l < k_s$. Here w_s is not a beginning of v_1', whereas the term between the parentheses may be missing (in this case $s = 1, l > 0$).

If v_1' is a nonempty word, then $v_1' < v_1 < w_1 \leq w_s$ because v_1 is standard. The inequality $v_1' < w_s$ implies $av_1'b < aw_sc$ for all words a, b, c because w_s is not a beginning of v_1'. Taking $a = (w_1^{k_1}w_2^{k_2}\cdots w_{s-1}^{k_{s-1}})w_s^l$ and suitable b, c, we obtain $v < w$.

Let v_1' is the empty word. If $l > 0$, then the word v_1 should be greater than its end w_s. Therefore, $w_1 > v_1 > w_s$, which contradicts the fact that $w_1 \leq w_s$ is valid for all $s \geq 1$. If $l = 0$, then $s > 1$ because v_1 begins with w_1. It follows that v_1 is greater than its end w_{s-1}, which is again a contradiction with $w_1 > v_1 > w_{s-1}$.

The second part of the lemma follows from Lemma 2.3 and the fact that the leading word of a product of homogeneous polynomials equals the product of leading words of the factors. □

Remark 2.1 We stress that the above lemma cannot be extended to all super-words, for example if $x_1 > x_2 > x_3$, then $[x_1] \cdot [x_3] > [x_1x_2]$ and $x_1x_3 < x_1x_2$.

Lemma 2.5 *Let u, u_1 be standard words and $u > u_1$. The polynomial $[[u], [u_1]]$ is a linear combination of super-words in the super-letters $[w]$ such that $uu_1 \geq w > u_1$, in which case the constitution of the super-words equals the constitution of uu_1.*

Proof If the nonassociative word $[[u][u_1]]$ is standard then it defines a super-letter $[w]$ and $uu_1 = w > u_1$ by Lemma 1.4. In particular, the lemma is valid if u and u_1 are letters. We can therefore proceed by induction on the length of uu_1.

Suppose that the lemma is true if the length of uu_1 is less than m. Choose a pair u, u_1 with a greatest word u, so that the polynomial $[[u], [u_1]]$ does not enjoy the required decomposition and the length of uu_1 equals m. Then the nonassociative word $[[u][u_1]]$ is not standard. By Lemma 1.10, we have $[u] = [[u_3][u_2]]$ with $u_2 > u_1$.

We fix the notation for super-letters $U_i = [u_i]$, $i = 1, 2, 3$. By Jacobi identity (2.1), we can write

$$[[U_3, U_2], U_1] = [U_3, [U_2, U_1]] + p_{u_1,u_2}^{-1}[[U_3, U_1], U_2] \\ +(p_{u_2,u_1} - p_{u_1,u_2}^{-1})[U_3, U_1] \cdot U_2. \tag{2.12}$$

We have $u_3 > u > u_2 > u_1$. By the inductive hypothesis, $[U_3, U_1]$ can be represented as $\sum_i \alpha_i \prod_k [w_{ik}]$, where $u_3 > u_3u_1 \geq w_{ik} > u_1$. Using Lemma 1.7, we obtain $u > uu_1 > u_3u_1 \geq w_{ik}$; that is, all super-letters $[w_{ik}]$ satisfy the requirements of the present lemma. Furthermore, the word u cannot be the beginning of u_2, and so $u > u_2$ implies $uu_1 > u_2$. Thus, the super-letter U_2, too, satisfies the requirements. Consequently, the second [in view of (2.6)] and third summands of (2.12) have the required decomposition.

Using the inductive hypothesis, for the first summand we obtain

$$[U_2, U_1] = \sum_i \beta_i \prod_k [v_{ik}], \tag{2.13}$$

where $u_2u_1 \geq v_{ik} > u_1$. By Lemma 1.7, $uu_1 > u_2u_1 \geq v_{ik}$; that is, the super-letters $[v_{ik}]$ satisfy the conditions of the lemma. Rewrite the first summand using skew-derivation formula (2.8), with the first factor replaced by (2.13). In this way, the first summand turns into a linear combination of words in the super-letters $[v_{ik}]$ and skew commutators $[[u_3], [v_{ik}]]$. Because $u_3 > u > u_2 > v_{ik}$ and the length of v_{ik} does not exceed that of u_2u_1, the inductive hypothesis applies to yield

$$[[u_3], [v_{ik}]] = \sum_j \gamma_j \prod_t [w_{jt}], \tag{2.14}$$

where $u_3 > u_3v_{ik} \geq w_{jt} > v_{ik}$. In this case $u_2u_1 \geq v_{ik}$ implies

$$uu_1 = u_3u_2u_1 \geq u_3v_{ik} \geq w_{jt};$$

in addition, $w_{jt} > v_{ik} > u_1$, i.e., the super-letters $[w_{jt}]$ also satisfy the conditions. □

Lemma 2.6 *Every nonincreasing super-word W is a linear combination of lesser increasing super-words of the same constitution whose super-letters all lie* (*not strictly*) *between the greatest and the least super-letters of W.*

Proof We proceed by induction on the length of the super-word. Assume that the lemma is true for super-words of length $\leq t$, and let $W = UU_1 \cdots U_t$ be a least super-word of length $t + 1$ for which our lemma fails.

If the super-word $U_1 \cdots U_t$ is not increasing, then by the inductive hypothesis it is a linear combination of lesser increasing super-words W_i. In this case $UW_i < W$, and according to the choice of W, all super-words UW_i have the required representation.

Let

$$W = UU_1^{k_1} \cdots U_t^{k_t}, \quad U_1 < U_2 < \ldots < U_t. \tag{2.15}$$

If $U \le U_1$, then W is increasing, and there is nothing to prove. Let $U > U_1$. Then

$$W = [U, U_1]U_1^{k_1-1} \cdots U_t^{k_t} + p_{u,u_1} U_1 U U_1^{k_1-1} \cdots U_t^{k_t}. \tag{2.16}$$

The second summand is less than W as a super-word, and so we can write it in the required form. By Lemma 2.5, the factor $[U, U_1]$ in the first term can be represented as $\sum_i \alpha_i \prod_s [w_{is}]$, where the super-letters $[w_{is}]$ are less than U. Consequently, the super-words $\prod_s [w_{is}] U_1^{k_1-1} \cdots U_t^{k_t}$ are less than W; that is, the first term has the required representation too. □

Theorem 2.1 *The set of all super-words*

$$[u_1]^{n_1}[u_2]^{n_2} \cdots [u_k]^{n_k}, \tag{2.17}$$

where $u_1 < u_2 < \ldots < u_k$ *are standard words, forms a basis of* $\mathbf{k}\langle X \rangle$.

Proof Since by definition all words of length one are standard, the letters $x_i = [x_i]$ are super-letters. Hence, by Lemma 2.6, every polynomial is a linear combination of increasing super-words. It remains to prove that the set of all increasing super-words is linearly independent. Let

$$\sum_i \alpha_i W_i = 0 \tag{2.18}$$

and assume that $W = [w_1]^{k_1}[w_2]^{k_2} \cdots [w_m]^{k_m}$ is a leading super-word in (2.18). By Lemma 2.4, the leading word of W equals $w = w_1^{k_1} w_2^{k_2} \cdots w_m^{k_m}$. This word occurs exactly once in (2.18). Suppose, to the contrary, that W does also occur in the decomposition of $V = [v_1]^{m_1}[v_2]^{m_2} \cdots [v_k]^{m_k}$. Then the word w is less than or equal to the leading word $v = v_1^{m_1} v_2^{m_2} \cdots v_k^{m_k}$ in the decomposition of V, which contradicts the fact that $W > V$ by Lemma 2.4. □

2.2 Coproduct on Super-Letters

Theorem 2.1 demonstrates that the super-letters are PBW generators of infinite height for the free character Hopf algebra $G\langle X \rangle$. Our next goal is to describe properties of the coproduct of these PBW generators.

Lemma 2.7 *The coproduct of a super-letter* $W = [w]$ *has a representation*

$$\Delta([w]) = [w] \otimes 1 + g_w \otimes [w] + \sum_i \alpha_i g(W_i'')W_i' \otimes W_i'', \tag{2.19}$$

where W_i' *are nonempty words in less super-letters than is* $[w]$. *Moreover, the sum of constitutions of* W_i' *and* W_i'' *equals the constitution of* V. *Here* $g(u)$ *denotes the group-like element* g_u.

Proof We use induction on the length of a word w. For letters, there is nothing to prove. Let $W = [U, V]$, $U = [u]$, and $V = [v]$. Assume that the decompositions

$$\Delta(U) = U \otimes 1 + g_u \otimes U + \sum_i \alpha_i g(U_i'')U_i' \otimes U_i'', \tag{2.20}$$

and

$$\Delta(V) = V \otimes 1 + g_v \otimes V + \sum_j \beta_j g(V_j'')V_j' \otimes V_j'' \tag{2.21}$$

satisfy the requirements of the lemma. Using (2.6) and properties of p, we can write

$$\begin{aligned}\Delta(W) = {}& \Delta(U)\Delta(V) - p_{u,v}\Delta(V)\Delta(U) = W \otimes 1 + g_w \otimes W \\ & +(1 - p_{u,v}p_{v,u})g_u V \otimes U + \sum \beta_j p(U, V_j'')g(V_j'')[U, V_j'] \otimes V_j'' \\ & + \sum \beta_j g_u g(V_j'')V_j' \otimes (UV_j'' - p_{u,v}p(V_j', U)V_j''U) \\ & + \sum \alpha_i g(U_i'')(U_i' \cdot V - p_{u,v}p(V, U_i'')V \cdot U_i') \otimes U_i'' \\ & + \sum \alpha_i p(U_i', V)g_v g(U_i'')U_i' \otimes [U_i'', V] \\ & + \sum \alpha_i \beta_j g(U_i''V_j'')(p(U_i', V_j'')U_i'V_j' \otimes U_i''V_j'' \\ & - p_{u,v}p(V_j', U_i'')V_j'U_i' \otimes V_j''U_i'').\end{aligned} \tag{2.22}$$

Collecting similar terms in this formula was result in the canceling of terms of the form $g_v U \otimes V$ only. We claim that all left parts of the remaining tensors in (2.22) admit the required decomposition. First, in view of the inductive hypothesis, all super-letters of all super-words V_j' are less than V, which are in turn less than W because v is the end of a standard word w. Moreover, by the inductive hypothesis again, u cannot be the beginning of any word u' such that the super-letter $[u']$ would occur in super-words U_i'. Therefore, $u > u'$ implies $uv > u'$ and $W > [u']$. Thus, all but the first and fourth super-words on the left-hand sides of all tensors depend only on super-letters which are less than W.

We want to apply Lemma 2.5 to the fourth tensor. Let $V'_j = \prod_k V_{ik}$, where $V_{ik} = [v_{ik}]$ are less than V. By Eq. (2.8), the polynomial $[U, V'_j]$ is a linear combination of words in the super-letters V_{ik} and skew commutators $[U, V_{ik}]$. By Lemma 2.5, each of these commutators is a linear combination of words in the super-letters $[v']$ such that $v' \leq uv_{ik}$. In view of $v_{ik} < v$, we obtain $v' < uv = w$.

The statement concerning the constitutions follows immediately from formula (2.22) and the inductive hypothesis. □

Lemma 2.8 *The coproduct of a super-word W has a decomposition*

$$\Delta(W) = W \otimes 1 + g(W) \otimes W + \sum_i \alpha_i g(W''_i) W'_i \otimes W''_i, \tag{2.23}$$

where the sum of constitutions of W'_i and W''_i equals the constitution of W.

Proof It suffices to observe that Δ is an homomorphism of algebras. Here, we can no longer assert that $W'_i < W$. □

Lemma 2.9 *If $[w]$ is a super-letter, then*

$$\Delta([w]^m) = \sum_{j=0}^{m} \begin{bmatrix} m \\ j \end{bmatrix}_q g_w^{m-j} [w]^j \otimes [w]^{m-j} + \sum_i \alpha_i g(V_i) U_i \otimes V_i, \tag{2.24}$$

where $\begin{bmatrix} m \\ j \end{bmatrix}_q$ are the Gauss polynomials considered in Sect. 1.1 with $q = p(w, w)$, whereas the super-words U_i are less than $[w]^m$ with respect to the lexicographical ordering of words in super-letters.

Proof After developing of the product, the mth power of the right hand side of (2.19) takes the form (2.24), where each of U_i is a product of m super-words some of whom equal to $[w]$ (but not all of them!) and others equal to some of the W'_i's. By Lemma 2.7, all super-letters that occur in W_i are less than $[w]$. Hence, the super-word U_i is less than $[w]^m$ with respect to the lexicographical ordering of words in super-letters. □

2.3 Hard Super-Letters

Consider a character Hopf algebra H. By definition H is generated over $\mathbf{k}[G]$ by skew-primitive semi-invariants $b_i, i \in I$:

$$\Delta(b_i) = b_i \otimes h_i + f_i \otimes b_i,\ h_i, f_i \in G, \quad b_i g = \chi^{b_i}(g) \cdot g b_i,\ g \in G,\ i \in I. \tag{2.25}$$

As the skew-primitive elements are closed with respect to the multiplication by group-like elements, we may normalize the generators, $a_i = h_i^{-1} b_i$, diminishing the number of group-like elements related to them:

$$\Delta(h_i^{-1}b_i) = h_i^{-1}u \otimes 1 + h_i^{-1}f_i \otimes h_i^{-1}b_i.$$

In what follows, we fix a set of *normalized skew-primitive* generators $\{a_i\}$, so that

$$\Delta(a_i) = a_i \otimes 1 + g_i \otimes a_i, \ \ \Delta(g_i) = g_i \otimes g_i, \ \ a_i g = \chi^{a_i}(g) \cdot g a_i, \ g \in G, \ i \in I. \tag{2.26}$$

Let $G\langle X\rangle, \ X = \{x_i \,|\, i \in I\}$ be the free character Hopf algebra such that $\chi^i = \chi^{a_i}$ and $g_i = g_{a_i}$, $i \in I$. Then there exists a natural homomorphism of Hopf algebras

$$\varphi : G\langle X\rangle \to H, \tag{2.27}$$

which maps x_i to $a_i, \ i \in I$.

Definition 2.4 Let Γ be a well-ordered additive (commutative) monoid. With each $x_i, \ i \in I$ we associate a nonzero element $d_i \in \Gamma$. The *D-degree* of a word, a super-letter, a super-word, or more generally, a homogeneous polynomial f in X of a constitution $\{m_i \,|\, i \in I\}$ is

$$D(f) = \sum_i m_i d_i = \sum_i d_i \deg_i(f). \tag{2.28}$$

In what follows, we fix a well-ordered monoid Γ and elements $d_i = D(x_i)$. For example, Γ may be the monoid related to the constitution given in the construction after Definition 1.3. For the first reading, one may suppose that $\Gamma = Z^+$ is the monoid of nonnegative integer numbers, whereas $d_i = 1$. However, we should stress that the resulting set of PBW generators and its properties essentially depend on the chosen D-degree function.

Lemma 2.10 *The set X_m^* of all words of a fixed D-degree m is well-ordered with respect to the lexicographical order.*

Proof We note, first, that Γ has no negative elements: if $a < 0$, then there appears an infinite descending chain $0 > a > 2a > 3a > \dots$. Additionally, Γ has the cancelation property, $a + x = a + y$ implies $x = y$: if $x > y$, then $a + x > a + y$.

Let F be a subset of X_m^*. As $\langle X, <\rangle$ is well-ordered, the set A of all first letters of words from F has a least element, say, $x_1 \in X$. If $x_1 u, \ x_1 v \in F$, then $D(x_1) + D(u) = D(x_1) + D(v) = m$. Hence, $D(u) = D(v) < m$ because $D(v) \geq m$ and $D(x_1) > 0$ would imply $D(x_1) + D(v) > m$. By these reasons, we may apply the induction supposition to the set $B = \{u \in X^* \,|\, x_1 u \in F\}$. If u_0 is a least element of B, then $x_1 u_0$ is a least element of F. □

Definition 2.5 A *G-super-word* is a product of the form gW, where $g \in G$ and W is a super-word. The degree, constitution, length, and other concepts which apply with G-super-words are defined by the super-word W. In other words, we assume that the D-degree and the constitution of $g \in G$ are equal to zero. In view of (2.26), every product of super-letters and group-like elements equals a linear combination of G-super-words of the same constitution.

Definition 2.6 A super-letter $[u]$ is said to be *hard* if its value $\varphi([u])$ in H is not a linear combination of values of words of the same D-degree in less super-letters than is $[u]$ and of G-super-words of a lesser D-degree.

We are remanded that a primitive tth root of 1 is an element $\alpha \in \mathbf{k}$ such that $\alpha^t = 1$ and $\alpha^r \neq 1$ for all $r,\ 1 \leq r < t$. In particular, 1 is the 1st primitive root of 1.

Definition 2.7 We say that the *height* of a super-letter $[u]$ of D-degree $d \in \Gamma$ equals $h = h([u])$ if h is the smallest natural number such that:

(1) $p_{u,u}$ is a primitive tth root of 1 and either $h = t$ or $h = tl^r$, where l is the characteristic of $\mathbf{k}$.
(2) the value in H of $[u]^h$ is a linear combination of values of super-words of D-degree hd in less super-letters than is $[u]$ and of G-super-words of a lesser D-degree.

If, for the super-letter $[u]$, the number h with the above properties does not exist, then we say that the height of $[u]$ is infinite.

Theorem 2.2 *The set of values in H of all G-super-words W in the hard super-letters $[u_i]$,*

$$W = g[u_1]^{n_1}[u_2]^{n_2}\cdots[u_k]^{n_k}, \tag{2.29}$$

where $g \in G$, $u_1 < u_2 < \ldots < u_k$, $n_i < h([u_i])$, forms a basis of H.

The proof will proceed through a number of lemmas. For brevity, we call a G-super-word (2.29) *restricted* if each of the numbers n_i is less than the height of $[u_i]$. A super-word (a G-super-word) is said to be *admissible* if it is increasing restricted and is a word in hard super-letters only.

First of all, we have to demonstrate that every element of H is a linear combination of values of admissible G-super-words. Clearly, every element is a linear combination of values of not necessarily admissible G-super-words because each variable x_i is a super-letter, $x_i = [x_i]$. In fact, there exist a natural diminishing procedure, based on Lemma 2.5 and on the definitions of hard super-letters and their heights, that allows one to find the required linear combination.

Lemma 2.11 *The value of each non-admissible super-word of D-degree d is a linear combination of values of lesser admissible super-words of D-degree d and of admissible G-super-words of a lesser D-degree. Also, all super-letters occurring in the super-words of D-degree d of this linear combination are less than or equal to a greatest super-letter of the super-word given.*

Proof Assume that the lemma is valid for super-words of D-degree $< m$. Let W be a least super-word of D-degree m for which the required representation fails. By Lemma 2.6, the super-word W is increasing. If it has a non-hard super-letter, by definition, we can replace it with a linear combination of G-super-words of a lesser D-degree and of words in less super-letters of the same D-degree. Developing the product turns W into a linear combination of G-super-words of a lesser D-degree and of lesser super-words of the same D-degree, a contradiction with the choice of W. If W contains a subword $[u]^k$, where k equals the height of $[u]$, then we can replace it as is specified above, which gives us a contradiction again. Thus the W is itself increasing restricted and is a word in hard super-letters only. □

In order to prove Theorem 2.2, it remains to show that admissible G-super-words are linearly independent. Consider an arbitrary linear combination $\mathbf{T}$ of admissible G-super-words and let $U = V_1^{n_1} V_2^{n_2} \cdots V_k^{n_k}$ be its leading (maximal) super-word of D-degree m. Multiplying, if necessary, that combination by a group-like element, we can assume that U occurs once without a group-like element:

$$\mathbf{T} = U + \sum_{j=1}^{r} \alpha_j g_j U + \sum_{\mathbf{i}=(i1,i2,\dots,is)} \alpha_{\mathbf{i}}\, g_{\mathbf{i}}\, W_{\mathbf{i}}, \quad W_{\mathbf{i}} = V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}. \tag{2.30}$$

In the next three lemmas, we accept the following assumptions on $m,\ U$ and r :

1. The admissible G-super-words of D-degree $< m$ are linearly independent;
2. The admissible G-super-words of D-degree m which are less than U are linearly independent modulo the space spanned by G-super-words mentioned in 1;
   and, if $r > 0$, then
3. The super-words $g_j U,\ 1 \le j \le r$ are linearly independent modulo the space spanned by G-super-words mentioned in 1 and 2.

In view of these assumptions and Lemma 2.11, every super-word of D-degree m which is less than U, and every super-word of D-degree $< m$, can be *uniquely* decomposed into a linear combination of admissible G-super-words. For brevity, such will be referred to as a *basis* decomposition.

Lemma 2.12 *Under the assumptions 1, 2, 3, if the value of* $\mathbf{T}$ *in* H *is a skew-primitive element, then* $r = 0$ *and* $g_{\mathbf{i}} = 1$ *for all* $\mathbf{i}$ *such that* $D(W_{\mathbf{i}}) = m$.

Proof Rewrite the linear combination $\mathbf{T}$ as follows:

$$\mathbf{T} = U + \sum_{\mathbf{i}\in I} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}} + W', \tag{2.31}$$

where $g_{\mathbf{i}} W_{\mathbf{i}}$ are distinct G-super-words of D-degree m in (2.30) (including $\alpha_j\, g_j\, U$) and W' is a linear combination of G-super-words of D-degree $< m$. In the expression

$$\Delta(\mathbf{T}) - \mathbf{T} \otimes h_t - f_t \otimes \mathbf{T}, \quad h_t,\, f_t \in G \tag{2.32}$$

consider all tensors of the form $gW \otimes \dots$, where $D(W) = m$. By Lemma 2.8, the sum of all such tensors equals

$$\sum_{\mathbf{i}\in I} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}} \otimes g_{\mathbf{i}} - \sum_{\mathbf{i}\in I} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}} \otimes 1 = \sum_{\mathbf{i}\in I} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}} \otimes (g_i - 1). \tag{2.33}$$

By assumptions 1, 2, 3, the elements $g_{\mathbf{i}} W_{\mathbf{i}}$, $\mathbf{i} \in I$ are linearly independent modulo all left parts of tensors of D-degree $< m$ in (2.32). Therefore, if (2.32) vanishes in H, then either $\alpha_{\mathbf{i}} = 0$ or $g_{\mathbf{i}} = 1$ for every $\mathbf{i} \in I$, as required. □

Lemma 2.13 *Under the assumptions 1, 2, 3, if* $\mathbf{T}$ *is a skew-primitive element, then* $U = [u]^h$ *and all super-words of D-degree m except U are words in less super-letters than* $[u]$ *is.*

Proof By the preceding lemma, we can assume that

$$\mathbf{T} = \sum_{\mathbf{i}=(i1,i2,\dots,is)} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}}, \; W_{\mathbf{i}} = V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}, \tag{2.34}$$

where one of the $W_{\mathbf{i}}$'s is U, whereas $V_{ij} = [v_{ij}]$ are hard super-letters, $\alpha_{\mathbf{i}}$ are nonzero coefficients, and $g_{\mathbf{i}} = 1$ if $W_{\mathbf{i}}$ is of D-degree m. By Lemma 2.7, we have

$$\Delta(g_{\mathbf{i}} W_{\mathbf{i}}) = (g_{\mathbf{i}} \otimes g_{\mathbf{i}}) \prod_{j=1}^{s} (V_{ij} \otimes 1 + g_{ij} \otimes V_{ij} + \sum_{\theta} g_{ij\theta} V'_{ij\theta} \otimes V''_{ij\theta})^{n_{ij}}, \tag{2.35}$$

where $V'_{ij\theta} < V_{ij}$ and $\deg V'_{ij\theta} + \deg V''_{ij\theta} = \deg V_{ij}$.

Let $[u]$ be the greatest super-letter occurring in super-words of D-degree m in (2.34). Because all super-words of (2.34) are increasing, this super-letter stands at the end of some super-words $W_{\mathbf{i}}$, i.e., $[u] = V_{is}$. If one of these super-words depends only on $[u]$; that is, $W_{\mathbf{i}} = [u]^h$, then $W_{\mathbf{i}}$ is a leading super-word, $W_{\mathbf{i}} = U$ as required. Therefore, we assume that every super-word of D-degree m ending with $[u]$ is a word in more than one different super-letters.

Let $h = n_{is}$ be the largest exponent of $[u]$ in (2.34). Consider all tensors of the form $g[u]^k \otimes \dots$ obtained in (2.35) by removing the parentheses and applying the basis decomposition to all left parts of tensors in all terms except $\mathbf{T} \otimes 1$ (all of these terms are of D-degree $< m$).

All left parts of tensors which appear in (2.35) removing the parentheses arise from the G-super-word $g_i V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}$ by replacing some of the super-letters V_{ij} either with group-like element g_{ij} or with G-super-word $g_{ij\theta} V'_{ij\theta}$ of a lesser D-degree in less super-letters. The right parts are, respectively, products obtained by replacing super-letters V_{ij} with super-words $V''_{ij\theta}$ multiplied from the left by g_i.

Let $gR \otimes g'S$ be a resulting tensor under the replacements above and followed then basis decomposition.

If $D(R) < hD(u)$, then its basis decomposition may give rise to terms of the form $g[u]^k \otimes \ldots$. In this case, however, $D(S) < (m-h)D(u)$ because the sum of D-degrees of both parts of the tensors either remains equal to m or decreases.

If $D(R) < hD(u)$, or R is itself less than $[u]^h$ as a super-word, then the basis decomposition of R have no terms of the form $g[u]^h$; see Lemma 2.9.

If $D(R) = hD(u)$, while $D(W_{\mathbf{i}}) < m$, then R can be greater than or equal to $[u]^h$, but in this case $D(S) < (m-h)D(u)$ because $D(R) + D(S) \le D(W_{\mathbf{i}}) < m$.

If $D(R) = hD(u)$, while $D(W_{\mathbf{i}})$ does not end with $[u]^h$; that is, $W_{\mathbf{i}} = W'_{\mathbf{i}}[u]^r$, $0 \le r < h$ and $W'_{\mathbf{i}}$ ends with a lesser than $[u]$ supper-letter, then S is less than $[u]^h$ because, due to Lemma 2.7, its first super-letter is less than $[u]$: if all super-letters of $W'_{\mathbf{i}}$ are replaced with group-like elements, then $D(R) \le D([u]^r) < hD(u)$.

Finally, if $W_{\mathbf{i}} = W'_{\mathbf{i}}[u]^h$, then a super-word R of D-degree $hD(u)$, which is greater than or equal to $[u]^h$, may appear only if all super-letters of the super-word $W'_{\mathbf{i}}$ are replaced with group-like elements, but $[u]$ is not. Here, the resulting tensor is of the form $g_{\mathbf{i}}\, g(W'_{\mathbf{i}})[u]^h \otimes g_{\mathbf{i}}\, W'_{\mathbf{i}}$.

We fix an index $\mathbf{i}$ such that $W_{\mathbf{i}}$ ends with $[u]^h$. Then the sum of all tensors of the form $g_{\mathbf{i}}\, g(W'_{\mathbf{i}})[u]^h \otimes \ldots$ in $\Delta(\mathbf{T}) - \mathbf{T} \otimes h_t$ is equal to

$$g_{\mathbf{i}} g(W'_{\mathbf{i}})[u]^h \otimes \Big(\sum_{\mathbf{j}} \alpha_{\mathbf{j}}\, g_{\mathbf{j}}\, W'_{\mathbf{j}} + \mathbf{W}''\Big), \tag{2.36}$$

where $\mathbf{W}''$ is a linear combination of basis elements of D-degree less than $(m-h)D(u)$, and $\mathbf{j}$ runs through the set of all indices such that $W_{\mathbf{j}} = W'_{\mathbf{j}}[u]^h$, $g_{\mathbf{j}}\, g(W'_{\mathbf{j}}) = g_{\mathbf{i}}\, g(W'_{\mathbf{i}})$, and $D(W_{\mathbf{j}}) = (m-h)D([u])$.

Because $W'_{\mathbf{j}}$ are distinct nonempty basis super-words of D-degree $(m-h)D(u)$, the value of tensor (2.36) in H is nonzero. A contradiction. □

Lemma 2.14 *Under the conditions of the above lemma, $p_{u,u}$ is a tth primitive root of* 1 *with* $t \ge 1$ *and* $h = t$, *or the characteristic of* $\mathbf{k}$ *equals* $l > 0$ *and* $h = tl^k$.

Proof By Lemma 2.13, the linear combination $\mathbf{T}$ can be written in the form

$$\mathbf{T} = [u]^h + \sum_{\mathbf{i}=(i1,i2,\ldots,is)} \alpha_{\mathbf{i}} g_{\mathbf{i}} W_{\mathbf{i}},\ W_{\mathbf{i}} = V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}, \tag{2.37}$$

where $[u]$ is greater than all super-letters V_{ij} for $W_{\mathbf{i}}$ of D-degree m. First let $\xi = 1 + p_{uu} + p_{uu}^2 + \ldots + p_{uu}^{h-1} \neq 0$ and assume $h > 1$.

In the basis decomposition of $\Delta(\mathbf{T}) - \mathbf{T} \otimes 1$, consider tensors of the form $[u]^{h-1} \otimes \ldots$. All super-letters V_{ij} in super-words of D-degree m are less than or equal to $[u]$; therefore, tensors of this form may appear under the basis decomposition of a tensor of $\Delta(W_{\mathbf{i}}) - W_{\mathbf{i}} \otimes 1$, $V_i = V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}$, only if either the left part of that tensor is of D-degree greater than $(h-1)D(u)$ or $W_{\mathbf{i}}$ is of D-degree less than m. In either case, the right part is of less D-degree than is $[u]$. As above, if we remove the parentheses in

$$\Delta([u]^h) = ([u] \otimes 1 + g_u \otimes [u] + \sum_{\tau} g_\tau U'_\tau \otimes U''_\tau)^h, \tag{2.38}$$

we see that the left parts of the resulting tensors arise from the super-word $[u]^h$ by replacing some super-letters $[u]$ either with g_u or with G-super-words $g_\tau U'_\tau$ of a lesser D-degree in less super-letters than is $[u]$. It follows that a super-word of D-degree $(h-1)D(u)$ which is greater than or equal to $[u]^{h-1}$ appears only if exactly one super-letter is replaced with a group element. Using the commutation rule $[u]^s g_u = p^s_{u,u} g_u [u]^s$, we see that the sum of all tensors of the form $g_u[u]^{k-1} \otimes \dots$ equals

$$g_u[u]^{k-1} \otimes (\xi[u] + F + \mathbf{W}), \tag{2.39}$$

where F is a linear combination of super-words in less than $[u]$ super-letters, and $\mathbf{W}$ is a linear combination of basis G-super-words of D-degree less than $D(u)$. Consequently, (2.32) is nonzero provided that $\xi \neq 0$.

Now let $\xi = 0$. In this case $p^h_{u,u} = 1$. Therefore, $p_{u,u}$ is a tth primitive root of 1, and $h = t \cdot q$ or, if $\mathbf{k}$ has a characteristic $l > 0$, then $h = tl^r \cdot q$ with $q, t \neq 0 \pmod{l}$. Our aim is to demonstrate that $q = 1$. Let $h' = h/q$.

The commutation rule $([u] \otimes 1) \cdot (g_u \otimes [u]) = p_{u,u}(g_u \otimes [u]) \cdot ([u] \otimes 1)$ implies

$$([u] \otimes 1 + g_u \otimes [u])^{h'} = [u]^{h'} \otimes 1 + g_u^{h'} \otimes [u]^{h'}. \tag{2.40}$$

If we remove the parentheses in

$$\Delta([u]^{h'}) = (([u] \otimes 1 + g_u \otimes [u]) + \sum_i g(U''_i)U'_i \otimes U''_i)^{h'}, \tag{2.41}$$

then Lemma 2.9 implies

$$\Delta([u]^{h'}) = [u]^{h'} \otimes 1 + g_u^{h'} \otimes [u]^{h'} + \sum_\theta g(U''_\theta)U'_\theta \otimes U''_\theta, \tag{2.42}$$

where all super-words U'_θ are less than $[u]^{h'}$ (in particular, $U'_\theta \neq [u]^d,\ d < h'$) and $D(U'_\theta) < h' \cdot D(u)$.

This allows us to treat $[u]^{h'}$ in (2.37) as a single block, or as a new formal super-letter $\{[u]^{h'}\}$ such that $\{[u]^{h'}\} < [u]$, and $\{[u]^{h'}\} > [v_{ij}]$ if $u^{h'} > v_{ij}$ (the latter inequality is equivalent to $u > v_{ij}$ by Lemma 1.5):

$$\mathbf{T} = \{[u]^{h'}\}^q + \sum_i \alpha_i g_i V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}}. \tag{2.43}$$

Considering that $p([u]^{h'}, [u]^{h'}) = p_{u,u}^{h'\cdot h'} = 1$, we have

$$\xi_1 = 1 + p([u]^{h'}, [u]^{h'}) + \ldots + p([u]^{h'}, [u]^{h'})^{q-1} = q \neq 0 \pmod{l}.$$

As in the case above, assuming that $\{[u]^{h'}\}$ is a single block, we can compute the sum of all tensors of the form $g_u^{h'}\{[u]^{h'}\}^{q-1} \otimes \ldots$ in the basis decomposition of $\Delta(\mathbf{T}) - \mathbf{T} \otimes 1$ (provided that $q > 1$):

$$g_u^{h'}\{[u]^{h'}\}^{q-1} \otimes (q \cdot \{[u]^{h'}\} + F + \mathbf{W}), \tag{2.44}$$

where F is a linear combination of super-words in less than $[u]^{h'}$ super-letters, and $\mathbf{W}$ is a linear combination of basis G-super-words of less D-degree than is $[u]^{h'}$. By the induction hypothesis, tensor (2.44) is nonzero in $H \otimes H$, and so is (2.32). □

Now we are ready to complete the proof of Theorem 2.2 by induction on m, U, and r. The least super-word of the minimal D-degree is a least variable x_i with minimal d_i. In (2.30), the minimal value of r is zero. For these values of the induction parameters, we have $\mathbf{T} = x_i$. If $x_i = 0$ in H then $U = [x_i]$ is not a hard super-letter.

If under the induction assumptions 1, 2, 3, we have $\mathbf{T} = 0$ in H, then value of $\mathbf{T}$ is a skew-primitive element. By Lemmas 2.13, 2.14, the equality $\mathbf{T} = 0$ takes the form

$$[u]^h = -\sum_{\mathbf{i}=(i1,i2,\ldots,is)} \alpha_{\mathbf{i}}\, g_{\mathbf{i}}\, W_{\mathbf{i}}, \quad W_{\mathbf{i}} = V_{i1}^{n_{i1}} V_{i2}^{n_{i2}} \cdots V_{is}^{n_{is}},$$

where $V_{ij} < [v]$ if $D(W_{\mathbf{i}}) = D([u]^h)$, whereas for h there are just the following options: $h = 1$; or $p_{u,u}$ is a primitive tth root of 1, and either $h = t$ or, in case when the characteristic l is positive, $h = tl^k$

If $h = 1$, then Definition 2.6 implies that $[u]$ is not hard. In other cases, Definition 2.7 implies that the height of $[u]$ is less than h. Theorem 2.2 is proved.

The skew-primitive elements in character Hopf algebras have a special form in the basis decomposition related to hard super-letters. We are remanded that if $a \in \mathbf{k}[G]$ is a skew-primitive element, then a is proportional to $h - f$, see Lemma 1.19.

Theorem 2.3 *If $a \notin \mathbf{k}[G]$ is a skew-primitive element, then $a = \alpha g\, \varphi(\mathbf{T})$, where $0 \neq \alpha \in \mathbf{k}$, $g \in G$, and $\mathbf{T}$ has the following expansion:*

$$\mathbf{T} = [u]^h + \sum \alpha_i W_i + \sum \beta_j\, g_j\, W_j'. \tag{2.45}$$

Here, $[u]$ is a hard super-letter, W_i are basis super-words in super-letters less than $[u]$, $D(W_i) = hD([u])$, and $D(W_j') < hD([u])$. Moreover, if $p_{u,u}$ is not a root of 1, then $h = 1$; if $p_{u,u}$ is a primitive tth root of 1, then $h = 1$, or $h = t$, or (in case of characteristic $l > 0$) $h = tl^k$.

Proof By Theorem 2.2, the element a is a linear combination of values of increasing restricted G-super-words, $a = \varphi(\mathbf{T}')$,

$$\mathbf{T}' = \alpha g U + \sum_{i=1}^{k} \gamma_i g_i W_i + W', \quad \alpha \neq 0, \tag{2.46}$$

where gU, g_iW_i are admissible G-super-words of maximal degree, and either $U > W_i$ or $U = W_i$ but $g_i \neq g$. Considering that, due to Theorem 2.2, assumptions 1, 2, 3 are universally true, we may apply Lemmas 2.12–2.14 to $\mathbf{T} = \alpha^{-1} g^{-1}\mathbf{T}'$. □

2.4 Monomial PBW Basis

In this section, we prove that values of standard words corresponding to hard super-letters form a set of *PBW* generators for H also. Additionally we find some criterion for a super-letter $[u]$ to be hard in terms of the values of monomials. This criterion allows one to forget about skew brackets while computing the hard super-letters.

We keep the notations of the above section. In particular, H is a Hopf algebra generated by an Abelian group G of all group-like elements and by skew-primitive semi-invariants $a_1, \ldots, a_n$ with which degrees $d_1, \ldots, d_n$ are associated. We fix the homomorphism of Hopf algebras $\varphi : G\langle X\rangle \to H,\ x_i \mapsto a_i,\ 1 \le i \le n$.

Let w be an arbitrary word. By Theorem 1.1, there exists a unique decomposition of the word w in the product: $w = w_1^{n_1} \cdot w_2^{n_2} \cdot \ldots \cdot w_m^{n_m}$, where $w_i,\ 1 \le i \le m$ are standard words such that $w_1 < w_2 < \ldots < w_m$. Let $W = [w_1]^{n_1} \cdot [w_2]^{n_2} \cdot \ldots \cdot [w_m]^{n_m}$.

Lemma 2.15 *If the super-word W is admissible, then the leading super-word of the basis decomposition of $\varphi(w)$ is precisely W and it occurs with the coefficient 1 only. If W is not admissible, then each super-word of the basis decomposition of $\varphi(w)$ either is less than W or is of a lesser D-degree.*

Proof Lemma 2.4 implies that the leading word of the polynomial W is precisely w. Hence, $W - w$ is a linear combination of words that are less than w.

If W is admissible, then the decomposition $w = W + (w - W)$ allows one to perform the evident induction.

If W is not admissible, then by Lemma 2.9, there is a decomposition $\varphi(W) = \sum_j \alpha_j\, g_j\, \varphi(W_j)$, where W_j are admissible super-words and for each j either $W_j < W$ or $D(W_j) < D(w)$. Let $W_j = [w_{1j}]^{n_1} \cdot [w_{2j}]^{n_2} \cdot \ldots \cdot [w_{mj}]^{n_{mj}}$ and $w_j = w_{1j}^{n_1} \cdot \ldots \cdot w_{mj}^{n_{mj}}$. Lemma 2.4 implies that $w_j < w$ provided that $D(w_j) = D(w)$. Thus, we have a representation of $\varphi(w)$ as a linear combination of lesser words of the same D-degree and G-words of lesser D-degree:

$$\varphi(w) = \varphi(w - W) + \sum_j \alpha_j\, g_j\, \varphi(w_j) - \sum_j \alpha_j\, g_j\, \varphi(W_j - w_j). \tag{2.47}$$

The induction applies. □

Theorem 2.4 *The set of values in H of all G-words*

$$gu_1^{n_1} \cdot u_2^{n_2} \cdot \ldots \cdot u_k^{n_k}, \tag{2.48}$$

where $g \in G$, $u_1 < u_2 < \ldots < u_k$ are standard words such that $[u_i]$ are hard super-letters, $n_i < h([u_i])$ forms a basis of H.

Proof Suppose that values of all words of degree $< m$ belong to the space H_0 spanned by (2.48). Among the words of D-degree m, let w be the minimal one with respect to the lexicographic order, such that $\varphi(w) \notin H_0$. If W is admissible, then w itself has the form (2.48). If W is not admissible, than by induction (2.47) implies that $\varphi(w) \in H_0$. Hence, $H_0 = H$.

Let w_j, $j \in J$ be different words of the type (2.48); that is, $w_j = w_{1j}^{n_1} \cdot \ldots \cdot w_{mj}^{n_{mj}}$, whereas $W_j = [w_{1j}]^{n_1} \cdot [w_{2j}]^{n_2} \cdot \ldots \cdot [w_{mj}]^{n_{mj}}$ are admissible super-words. By Lemma 2.15, the super-word W_j is a leading super-word of the PBW decomposition $w_j = W_j + \sum_i \alpha_{ij} W_{ij}$. Let W_k is the maximal super-word among the W_j's of maximal D-degree. Considering that different W_j, W_{ij}, $j \in J$ are linearly independent in H, we obtain that a linear dependence

$$\sum_{j \in J,\ t \in T} \alpha_{jt} h_{jt} \varphi(w_j) = 0,\ 0 \neq \alpha_{jt} \in \mathbf{k},\ h_{jt} \in G, \tag{2.49}$$

would imply $\sum_{t \in T} \alpha_{kt} g_{kt} \varphi(W_k) = 0$. This contradicts to Theorem 2.2. □

Corollary 2.1 *A super-letter $[u]$ is hard if and only if the value of u is not a linear combination of values of lesser words of D-degree $D(u)$ and of G-words of a lesser D-degree.*

Proof Let $\varphi(u) = \sum_i \alpha_i \varphi(w_i) + u_0$, $\alpha_i \in \mathbf{k}$, where $w_i < u$, $D(w_i) = D(u)$ and $D(u_0) < D(u)$. By Lemma 2.15, we obtain $u = [u] + \sum_j \beta_j U_j$ where the super-words U_j are less than $[u]$.

Let $w_i = w_{1i}^{n_1} \cdot w_{2i}^{n_2} \cdot \ldots \cdot w_{mi}^{n_{mi}}$, where w_{ki}, $1 \leq k \leq mi$ are standard words such that $w_{1i} < w_{2i} < \ldots < w_{mi}$, and let $W_i = [w_{1i}]^{n_1} \cdot [w_{2i}]^{n_2} \cdot \ldots \cdot [w_{mi}]^{n_{mi}}$. Lemma 2.15 demonstrates that all super-words V of the basis decomposition of w_i are less than or equal to W_i unless $D(V) < D(w_i)$. Because $u > w_i$, by Lemma 2.4, we have $[u] > W_i$, for all i.

Therefore $[u]$ is greater than all super-words of degree $D(u)$ in the basis decomposition of $\sum_i \alpha_i \varphi(w_i)$. Thus, Theorem 2.2 implies that $\varphi(u) \neq \sum_i \alpha_i \varphi(w_i) + u_0$.

Conversely, if $\varphi([u]) = \sum \alpha_i \varphi(W_i) + U_0$, where W_i depends on super-letters less than $[u]$ only, and $D(U_0) < D(u)$, then

$$\varphi(u) = \varphi([u]) + \varphi(u - [u]) = \sum \alpha_i \varphi(W_i) + U_0 + \varphi(u - [u]).$$

Due to Lemma 2.4, the latter polynomial has no one monomial whose D-degree equals $D(u)$ and which is greater than or equal to u. □

2.5 Serre Skew-Primitive Polynomials

In this section, using Theorem 2.3, we shall describe all skew-primitive polynomials in two variables linear in one of them. We keep notation of Sect. 1.5.3:

$$\Delta(y_i) = y_i \otimes h_i + f_i \otimes y_i, \quad y_i g = \chi^i(g) g y_i, \qquad h_i, f_i, g \in G, \quad i = 1, 2.$$

We know that $G\langle y_1, y_2\rangle$ as a Hopf algebra with group G of group-like elements is completely defined by the following four parameters

$$p_{ik} = q_{ik}^{-1} q'_{ik} = \chi^i(h_k^{-1} f_k), \quad 1 \leq i, k \leq 2 \tag{2.50}$$

related to the normalized skew-primitive generators $x_1 = h_1^{-1} y_1, \ x_2 = h_2^{-1} y_2$ because $G\langle y_1, y_2\rangle = G\langle x_1, x_2\rangle$.

Theorem 2.5 *There exists a nonzero linear in y_1 skew-primitive element W of degree n in y_2 if and only if either*

$$p_{12} p_{21} = p_{22}^{1-n} \tag{2.51}$$

or p_{22} is a primitive mth root of $1, \ m|n$, *and*

$$p_{12}^m p_{21}^m = 1. \tag{2.52}$$

If one (*or both*) *of these conditions is satisfied, then*

$$W = \alpha g\, [\ldots [[y_1, y_2], y_2], \ldots, y_2], \quad \alpha \in \mathbf{k}, \ g \in G, \tag{2.53}$$

where the brackets are defined in (1.67).

Proof Let W be a skew-primitive element of constitution $(1, n)$. By Theorem 2.3 the element W has a representation (2.45) up to a factor αg. Considering that the free character Hopf algebra is homogeneous in each variable, there are no terms W'_s in that representation. There exist only one standard word of constitution $(1, n)$: this is $x_1 x_2^n$. The standard alignment of brackets is precisely $[x_1 x_2^n] = [[\ldots [[x_1 x_2] x_2], \ldots] x_2]$. Hence, (2.45) reduces to $W = \alpha g\, [x_1 x_2^n]$. Due to Lemma 1.21, the G-super-word $h_1 h_2^n [x_1 x_2^n]$ becomes $[y_1 y_2^n]$ up to a scalar factor if we distribute the group-like factors among the variables using the commutation rules (1.62):

$$h_1 h_2^n [[\ldots [[x_1, x_2], x_2], \ldots], x_2] \sim [[\ldots [[y_1, y_2], y_2], \ldots], y_2]. \tag{2.54}$$

This proportion proves (2.53).

It remains to analyze when $[x_1x_2^n]$ is skew-primitive. By induction on n we shall prove the following explicit coproduct formula

$$\Delta([x_1x_2^n]) = [x_1x_2^n] \otimes 1 + \sum_{k=0}^{n} \alpha_k^{(n)} g_1 g_2^{n-k} x_2^k \otimes [x_1x_2^{n-k}], \tag{2.55}$$

$$\alpha_k^{(n)} = \begin{bmatrix} n \\ k \end{bmatrix}_{p_{22}} \cdot \prod_{s=n-k}^{n-1} (1 - p_{12}p_{21}p_{22}^s). \tag{2.56}$$

If $n = 0$, then the equality reduces to $\Delta(x_1) = x_1 \otimes 1 + g_1 \otimes x_1$, whereas $\alpha_0^{(0)} = 1$. Moreover, it is clear that $\alpha_0^{(n)} = 1$ for all n. We have,

$$\Delta([x_1x_2^n]) \cdot (x_2 \otimes 1) = [x_1x_2^n]x_2 \otimes 1 + \sum_{k=0}^{n} \alpha_k^{(n)} g_1 g_2^{n-k} x_2^{k+1} \otimes [x_1x_2^{n-k}], \tag{2.57}$$

$$\Delta([x_1x_2^n]) \cdot (g_2 \otimes x_2) = [x_1x_2^n]\, g_2 \otimes x_2 + \sum_{k=0}^{n} \alpha_k^{(n)} g_1 g_2^{n-k} x_2^k\, g_2 \otimes [x_1x_2^{n-k}]x_2, \tag{2.58}$$

$$(x_2 \otimes 1) \cdot \Delta([x_1x_2^n]) = x_2[x_1x_2^n] \otimes 1 + \sum_{k=0}^{n} \alpha_k^{(n)} x_2\, g_1 g_2^{n-k} x_2^k \otimes [x_1x_2^{n-k}], \tag{2.59}$$

$$(g_2 \otimes x_2) \cdot \Delta([x_1x_2^n]) = g_2[x_1x_2^n] \otimes x_2 + \sum_{k=0}^{n} \alpha_k^{(n)} g_1 g_2^{n-k+1} x_2^k \otimes x_2[x_1x_2^{n-k}]. \tag{2.60}$$

In the second and third relations we may move the group-like factors to the left:

$$[x_1x_2^n]g_2 = p_{12}p_{22}^n\, g_2[x_1x_2^n], \quad x_2^k\, g_2 = p_{22}^k\, g_2\, x_2^k, \quad x_2\, g_1 g_2^{n-k}\, x_2^k$$
$$= p_{21}p_{22}^{n-k}\, g_1 g_2^{n-k+1}\, x_2^{k+1}.$$

Using all that relations, we develop the coproduct of

$$[x_1x_2^{n+1}] = [x_1x_2^n]x_2 - p_{12}p_{22}^n\, x_2[x_1x_2^n]$$

taking into account that $\Delta(x_2) = x_2 \otimes 1 + g_2 \otimes x_2$. The sums of (2.57) and (2.59) provide the tensors

$$\sum_{k=0}^{n} \alpha_k^{(n)} (1 - p_{12}p_{21}p_{22}^{2n-k}) g_1 g_2^{n-k}\, x_2^{k+1} \otimes [x_1x_2^{n-k}],$$

whereas the sums of (2.57) and (2.59) produce the following ones:

$$\sum_{k=0}^{n} \alpha_k^{(n)} p_{22}^k \, g_1 g_2^{n-k+1} \, x_2^k \otimes [x_1 x_2^{n-k+1}].$$

The first term of (2.58) cancels with the first term of (2.60). Finally, we arrive to a formula (2.55) with $n \leftarrow n+1$ and coefficients

$$\alpha_k^{(n+1)} = \alpha_{k-1}^{(n)} \, (1 - p_{12} p_{21} p_{22}^{2n-k+1}) + \alpha_k^{(n)} \, p_{22}^k, \;\; k \geq 1, \;\; \alpha_0^{(n+1)} = 1. \qquad (2.61)$$

To prove the coproduct formula (2.55), it remains to check that values (2.56) satisfy the above recurrence relations. To this end, we shall check the equality of the following two polynomials in commutative variables λ, q :

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q \cdot (1 - \lambda q^n) = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \cdot (1 - \lambda q^{2n-k+1}) + \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot (1 - \lambda q^{n-k}) \cdot q^k. \qquad (2.62)$$

If $\lambda = 0$, then the equality reduces to the first q-Pascal identity (1.2). Let us compare the coefficients at λ,

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q \cdot q^n = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \cdot q^{2n-k+1} + \begin{bmatrix} n \\ k \end{bmatrix}_q \cdot q^{n-k} \cdot q^k.$$

This equality differs from the second q-Pascal identity (1.3) just by a common factor q^n. Hence, the equality (2.62) is valid.

If we multiply both sides of (2.62) by $\prod_{s=n-k+1}^{n-1}(1 - \lambda q^s)$ and next replace the variables $q \leftarrow p_{22}, \; \lambda \leftarrow p_{12}p_{21}$, then we obtain precisely (2.61) for values (2.56). The proof of (2.55) is complete.

Each $\alpha_k^{(n)}, \; 1 \leq k \leq n$ defined by (2.56) has a factor $1 - p_{12}p_{21}p_{22}^{n-1}$. In particular, if $p_{12}p_{21} = p_{22}^{1-n}$, then all of these coefficients are zero, whence $[x_1 x_2^n]$ is a skew-primitive polynomial.

If p_{22} is a primitive mth root of 1, $m|n$, and $p_{12}^m p_{21}^m = 1$, then $p_{12}p_{21}$ is a power of p_{22}; that is, $p_{12}p_{21}p_{22}^s = 1$ for some $s, \; 0 \leq s < m$. This implies that the product $\prod_{s=n-k}^{n-1}(1 - p_{12}p_{21}p_{22}^s)$ equals zero provided that $k \geq m$. If $k < m$, then Lemma 1.1 applies.

Conversely, suppose that all coefficients $\alpha_k^{(n)}, \; 1 \leq k \leq n$ are zero. In particular, $\alpha_1^{(n)} = (1 - p_{12}p_{21}p_{22}^{n-1})p_{22}^{[n]} = 0$. Therefore, if $p_{12}p_{21} \neq p_{22}^{1-n}$, then $p_{22}^{[n]} = 0$. This implies $p_{22}^n = 1$; that is, p_{22} is a primitive mth root of 1 and $m|n$. In this case, the equality $\alpha_n^{(n)} = \prod_{s=0}^{n-1}(1 - p_{12}p_{21}p_{22}^s) = 0$ implies that $1 - p_{12}p_{21}p_{22}^s = 0$ for some $s, \; 0 \leq s < n$. Hence, $(p_{12}p_{21})^m = p_{22}^{-sm} = 1$ which is required. □

Corollary 2.2 *If one of the existence conditions of the above theorem holds then*

$$[\dots[[y_1, y_2], y_2], \dots, y_2] \sim [y_2, [y_2, \dots, [y_2, y_1]\dots]]. \tag{2.63}$$

Proof By Lemma 1.21, we have

$$[y_2, [y_2, \dots, [y_2, y_1]\dots]] \sim h_1 h_2^n [x_2, [x_2, \dots, [x_2, x_1]\dots]]. \tag{2.64}$$

This lemma and (2.54) imply that it suffices to demonstrate (2.63) under the substitution $y_i \leftarrow x_i$.

Let us introduce the opposite order, $x_2 > x_1$. There exist only one standard word of constitution $(1, n)$ with respect to this ordering of variables, $x_2^n x_1$, whereas the standard alignment of brackets is $[x_2[x_2 \dots [x_2, x_1]\dots]]$. As $[\dots[[x_1, x_2], x_2]\dots, x_2]$ is skew-primitive, it has a representation (2.45) where all summands have the same constitution, $(1, n)$. By definition of the lexicographical order $x_2 > x_2^n x_1$. Hence, x_2 does not occur in (2.45) as a super-letter. Since every addend has degree 1 in x_1, it follows that (2.45) reduces to $\mathbf{T} = \alpha[x_2^n x_1]$. □

2.5.1 Examples

In this subsection, we consider in more detail the above-described binary skew-primitive polynomials with $n \leq 3$ and study the Hopf algebras set up by those polynomials (as defining relations).

We fix two normalized skew-primitive variables x_1, x_2 such that

$$\Delta(x_i) = x_i \otimes 1 + g_i \otimes x_i, \quad i = 1, 2.$$

Respectively, we put $p_{is} = \chi^i(g_s),\ i, s = 1, 2$ so that

$$x_1 g_1 = p_{11} g_1 x_1, \quad x_1 g_2 = p_{12} g_2 x_1, \quad x_2 g_1 = p_{21} g_1 x_2, \quad x_2 g_2 = p_{22} g_2 x_2.$$

We always suppose that the variables are ordered so that $x_1 > x_2$.

Example 2.1 If $n = 1$, then the existence condition of Theorem 2.53 reduces to $p_{12} p_{21} = 1$. Under that condition the skew commutator $[x_1, x_2] = x_1 x_2 - p_{12} x_2 x_1$ is a skew primitive element. We have $[x_1, x_2] = -p_{12}[x_2, x_1]$, which is the particular case of the general formula (2.63). The Hopf algebra H defined by the relation $[x_1, x_2] = 0$ is the skew group ring $R * G$, where G is the group generated by $g_1,\ g_2$ and R is the so-called algebra of quantum polynomials

$$R = \{\sum_{m,n} \alpha_{m,n} x_2^m x_1^n \mid x_1 x_2 = p_{12} x_2 x_1\}.$$

Obviously, x_1 and x_2 are the PBW-generators of H. To see this formally, we may apply Composition Lemma (Theorem 1.2). Indeed, $[x_1, x_2] = 0$ is a Gröbner-Shirshov system of relations because there are no compositions at all. Hence, by Composition Lemma, the set Σ of all words without subword x_1x_2 is a basis of R. Of course, $\Sigma = \{x_2^m x_1^n \mid m, n \geq 0\}$.

Example 2.2 If $n = 2$, then the existence condition of Theorem 2.53 reduces to

$$(p_{12}p_{21} = p_{22}^{-1}) \vee (p_{12}p_{21} = 1 \;\&\; p_{22} = -1). \tag{2.65}$$

Under that condition, the polynomial

$$[[x_1, x_2], x_2] = x_1x_2^2 - p_{12}(1 + p_{22})x_2x_1x_2 + p_{12}^2 p_{22} x_2^2 x_1$$

is a skew primitive element. In this case, the general formula (2.63) takes the form $[x_2, [x_2, x_1]] = p_{12}^2 p_{22}[[x_1, x_2], x_2]$. Similarly, condition

$$(p_{12}p_{21} = p_{11}^{-1}) \vee (p_{12}p_{21} = 1 \;\&\; p_{11} = -1) \tag{2.66}$$

implies that

$$[x_1, [x_1, x_2]] = x_1^2 x_2 - p_{12}(1 + p_{11})x_1x_2x_1 + p_{12}^2 p_{11} x_2 x_1^2$$

is a skew-primitive element and $[x_1, [x_1, x_2]] = p_{12}^2 p_{11}[[x_2, x_1], x_1]$.

If both polynomials are skew-primitive, then we may consider the Hopf algebra H defined by relations $[[x_1, x_2], x_2] = 0$ and $[x_1, [x_1, x_2]] = 0$. Of course, $H = R * G$, where R is the algebra defined by the same relations, and G, as above, is the group generated by g_1, g_2.

If $p_{11} = p_{22}$, then the algebra R is precisely the algebra A_2^+ considered in Example 1.1, where $\alpha = -p_{12}(1 + p_{22})$, $\beta = p_{12}^2 p_{22}$. In Example 1.1, we have seen that the system of relations

$$[[x_1, x_2], x_2] = 0, \quad [x_1, [x_1, x_2]] = 0$$

is closed with respect to the compositions, and

$$\Sigma = \{x_2^m (x_1x_2)^n x_1^k \mid m, n, k \geq 0\}$$

is a basis of R. In other words, the elements x_2, x_1x_2, x_1 form a set of PBW generators for H over G. Corollary 2.1 implies that all hard super-letters are precisely $x_2, [x_1x_2], x_1$, and they form a set of PBW generators for H over G as well.

We stress that the existence conditions (2.65), (2.66) imply $p_{11} = p_{22}$ unless $p_{22} = p_{12}p_{21} = 1, p_{11} = -1$ or $p_{22} = -1, p_{12}p_{21} = p_{11} = 1$.

Example 2.3 Note that $[[[x_1, x_2], x_2], x_2]$ is precisely the Lyndon–Shirshov standard word $[x_1x_2^3]$ with the standard alignment of brackets. Due to Theorem 2.53 the polynomial $[x_1x_2^3]$ is skew-primitive if either $p_{12}p_{21} = p_{22}^{-2}$ or $p_{22} = \zeta$ is a primitive third root of 1 and $p_{12}p_{21} \in \{1, \zeta^2\}$. Under that condition the polynomial

$$[x_1x_2^3] = x_1x_2^3 - p(1 + q + q^2)x_2x_1x_2^2 + p^2(q + q^2 + q^3)x_2^2x_1x_2 - p^3q^3x_2^3x_1,$$

where $p = p_{12},\ q = p_{22}$ is skew-primitive, and (2.63) takes the form

$$[x_1x_2^3] = -p^3q^3[x_2, [x_2, [x_2, x_1]]].$$

If $p_{11}^{-1} = p_{12}p_{21} = p_{22}^{-2}$, then both $[x_1x_2^3]$ and $[x_1^2x_2]$ are skew-primitive polynomials. Consider the Hopf algebra H defined by two relations: $[x_1x_2^3] = 0$, and $[x_1^2x_2] = 0$. These relations have the form (1.22) considered in Example 1.2 with

$$\alpha = -p(1+q^2),\ \beta = p^2q^2,\ \gamma = -p(1+q+q^2),\ \delta = p^2(q+q^2+q^3),\ \varepsilon = -p^3q^3,$$

whereas before, we put for short $p = p_{12},\ q = p_{22}$. If we define $\mu = -pq$, then these parameters satisfy the following relations (1.23):

$$\beta = \mu^2,\ \ \gamma = \alpha + \mu,\ \ \delta = \gamma\mu,\ \ \varepsilon = \mu^3.$$

In Example 1.2, we observed that the system of relations $[x_1x_2^3] = 0$ and $[x_1^2x_2] = 0$ becomes closed with respect to the compositions if we add one new relation, (1.27), which is a consequence of the two initial ones. Hence the set

$$\Sigma = \{x_2^m(x_1x_2x_2)^n(x_1x_2)^kx_1^s \mid m, n, k, s \geq 0\}$$

is a basis of R. In other words, the elements $x_2,\ x_1x_2^2,\ x_1x_2,\ x_1$ form a set of PBW-genrators for H over G. Respectively, Corollary 2.1 implies that all hard super-letters are precisely x_2, $[x_1x_2^2]$, $[x_1x_2], x_1$, and they form a set of PBW-generators of H over G also.

Interestingly, by Proposition 1.3 we may replace the very new relation with any other relation with the same leading word. The leading word, $x_1x_2x_1x_2^2$, is standard, and one may show (here we omit the detailed calculations) that $[x_1x_2x_1x_2^2] = 0$ is a relation for R. Therefore the three relations $[x_1x_2^3] = 0$, $[x_1^2x_2] = 0$, and $[x_1x_2x_1x_2^2] = 0$ is a Gröbner–Shirshov system of defining relations for R. Here $[x_1x_2x_1x_2^2] = [[x_1x_2][[x_1x_2]x_2]]$ has the standard alignment of brackets.

There exist five exceptional cases, when $[x_1x_2^3]$, $[x_1^2x_2]$ are still skew-primitive but $p_{11} \neq p_{22}^2$. They are: $p_{11} = p_{12}p_{21} = 1,\ p_{22} = \zeta;\ p_{11} = p_{22} = \zeta,\ p_{12}p_{21} = \zeta^2$; and $p_{11} = -1,\ p_{12}p_{21} = 1,\ p_{22} \in \{1, -1, \zeta\}$; here, ζ is the third primitive root of 1. The analysis of each one of these cases is much easier than that of Example 1.2, and we let the reader find the PBW-generators and Gröbner-Shirshov systems of relations as an exercise.

2.6 Chapter Notes

Examples 2.2 and 2.3 above are particular cases of quantizations of Lie algebras. Gröbner-Shirshov systems of defining relations for quantizations of Lie algebras of infinite series $A_n,\ B_n,\ C_n,\ D_n$ were found by the author [128] using as a basic tool the PBW theorem proved in this chapter. Interestingly, all relations in those systems have the form $[u] = 0$, where $[u]$ is a standard word with standard alignment of brackets. Independently, Chen et al. [48] found the Gröbner-Shirshov systems for quantizations $U_q(\mathfrak{sl}_n)$ of type A_n by means of the specific PBW basis constructed by Rosso [195] and Yamane [234].

There are many publications on the construction of a PBW basis for Hopf algebras. The first PBW-type theorem for *Drinfeld-Jimbo quantizations* (see the next chapter) appeared in the pioneering paper by Jimbo [106], which discusses $U_q(\mathfrak{sl}_2)$ in detail. Rosso [195] and Yamane [234] independently constructed the PBW basis for Drinfeld–Jimbo algebras $U_q(\mathfrak{sl}_n)$ of type $A_n,\ n > 2$. Thereafter, G. Lusztig, in his fundamental works [151–153], determined the PBW bases for arbitrary Drinfeld-Jimbo and Lusztig quantum enveloping algebras. These bases and their modifications have been considered in a number of subsequent papers, e.g., Kashiwara [119], Concini et al. [58], Berger [28], Towber [224], Bautista [21], Gavarini [84], Chari and Xi [47], Reineke [192], Leclerc [146], Bai and Hu [19]. An original approach based on the Ringel-Hall algebras was also advanced in [59, 60, 194].

The general statement given in Theorem 2.2 can be attributed to the author [124]. This PBW-type theorem was found to be essential in the construction of the *Weyl groupoid* by Heckenberger [91] corresponding to a *Nichols algebra* (see Sect. 6.7 below) of diagonal type. This groupoid was crucial in classifying such Nichols algebras [90]. In turn, knowledge of these Nichols algebras is important to perform the lifting method developed by N. Andruskiewitsch and H.-J. Schneider for classifying pointed Hopf algebras [4] .

Theorem 2.2 was generalized in two different directions by Ufer [225], and by Graña and Heckenberger [87] using similar methods. Instead of character Hopf algebras, S. Ufer considered *braided Hopf algebras* (see Chap. 6 below) with "triangular" braidings, whereas M. Graña and I. Heckenberger replaced the skew-primitive generators with irreducible Yetter–Drinfeld modules and obtained a factorization of the Hilbert series for a wide class of graded Hopf algebras, where the factors are parametrized by Lyndon–Shirshov words in a manner similar to how the PBW generators are parametrized in Theorem 2.2. In [97], I. Heckenberger and H. Yamane modified Theorem 2.2 based on the work of G. Lusztig by using the concept of the Weyl groupoid.

Returning to the main idea of the proof of Theorem 2.2, the right and left sides of the tensors in (2.2) were used differently, although we required detailed information (given in Lemma 2.9) about the left sides only. This information provides a noteworthy idea for applying the method to subalgebras R of H such that $\Delta(R) \subseteq R \otimes H$. A subspace that obeys the latter property is known as a *right coideal*.The author developed this idea in [133] by proving the following statement:

Theorem 2.6 *Every right coideal subalgebra of a character Hopf algebra H that contains all group-like elements of H has a PBW basis that can be extended up to a PBW basis of H.*

One reason that one-sided coideal subalgebras are important is that Hopf algebras do not have a sufficient number of Hopf subalgebras. The straightforward idea to consider Hopf subalgebras as "quantum subgroups" appeared to be inappropriate, whereas the one-sided coideal subalgebras are more precise. The one-sided comodule subalgebras, not the Hopf subalgebras, are found to be the Galois objects in the Galois theory for Hopf algebra actions (Milinski [173, 174], see also a detailed survey by Yanai [235]). In particular, the Galois correspondence theorem for the actions on free algebra establishes a one-to-one correspondence between right coideal subalgebras and intermediate free subalgebras (see Ferreira et al. [73]). In a detailed survey [147], G. Letzter provides a panorama of the use of one-sided coideal subalgebras in constructing quantum symmetric pairs to form Harish-Chandra modules and produce quantum symmetric spaces.

The importance of this concept led to a project to classify one-sided coideal subalgebras of Drinfeld–Jimbo quantizations. In fact, the proof of Theorem 2.6 yields sufficient additional information to try to attempt this classification for the subalgebras containing all group-like elements.

In a series of papers by Lara Sagahón, Garza Rivera and the author [134, 135, 139, 140], using the parallelization technique for supercomputers, this program was developed for a multiparameter version of the Drinfeld–Jimbo and Lusztig quantizations of types A_n and B_n. It was found in [135, 139] that in these cases the number of right coideal subalgebras of the positive Borel part $U_q^+(\mathfrak{g})$ coincides with the order of the Weyl group.

The latter statement was extended to arbitrary quantizations of finite type by Heckenberger and Schneider [96]. The right coideal subalgebras in that case are the well-known spaces $U^+[w]$ defined by the elements w of the Weyl group, which was used by Lusztig [153] to establish a PBW basis for $U_q^+(\mathfrak{g})$. This establishment represents an outstanding achievement of a general theory developed by N. Andruskiewitsch, I. Heckenberger, and H.-J. Schneider in a number of papers [5, 92, 95, 96]. Generally, this theory is a categorical version of the fundamental theory of Lusztig's automorphisms. More precisely, instead of the skew-primitive generators $x_1, \ldots, x_n$ the authors consider irreducible finite-dimensional Yetter–Drinfeld modules $V_1, \ldots, V_n$ over a Hopf algebra H with bijective antipode, and in place of the Weyl group is the Weyl groupoid theorized by I. Heckenberger. The theory includes a PBW theorem for the related Nichols algebras and their right coideal subalgebras.

Using these results as a starting point, Heckenberger and Kolb [94] classified all homogeneous right coideal subalgebras for a quantized enveloping algebra $U_q^+(\mathfrak{g})$ of a complex semisimple Lie algebra $\mathfrak{g}$ with deformation parameter q not a root of unity.

Using the computer algebra program to compute the commutative and non-commutative rings and modules FELIX [6, 72], they determined the number of different right coideal subalgebras when the order $|W|$ of the Weyl group was less than one million, thus confirming results of [139] for the case A_n and reducing the error in the explicit computer calculations for the case B_n presented in [140]. These numbers $|Co|$ are given in the tables below.

Type	A_2	A_3	A_4	A_5	A_6	A_7	A_8	E_6	F_4	G_2
$\|W\|$	6	24	120	720	5040	40,320	362,880	51,840	1152	12
$\|Co\|$	26	252	3368	58,810	1,290,930	34,604,844	1,107,490,596	38,305,190	91,244	68

B_2	B_3	B_4, C_4	B_5, C_5	B_6, C_6	B_7, C_7	D_4	D_5	D_6	D_7
8	48	384	38,400	46,080	645,120	192	1920	23,040	322,560
38	664	17,848	672,004	33,369,560	2,094,849,020	6512	238,720	11,633,624	720,453,984

It is likely that the same numbers remain true for multiparameter and "small" versions of the quantizations. Heckenberger and Kolb [93] recently extended their work on classification problem by considering right coideal subalgebras that do not contain all group-like elements.

http://www.springer.com/978-3-319-22703-0

Quantum Lie Theory
A Multilinear Approach
Kharchenko, V.
2015, XIII, 302 p., Softcover
ISBN: 978-3-319-22703-0