HOPF ALGEBRAS IN COMBINATORICS

DARIJ GRINBERG AND VICTOR REINER

Contents

Introduction 3
1. What is a Hopf algebra? 6
1.1. Algebras 6
1.2. Coalgebras 7
1.3. Morphisms, tensor products, and bialgebras 9
1.4. Antipodes and Hopf algebras 15
1.5. Commutativity, cocommutativity 25
1.6. Duals 27
1.7. Infinite sums and Leray's theorem 32
2. Review of symmetric functions Λ as Hopf algebra 40
2.1. Definition of Λ 40
2.2. Other Bases 43
2.3. Comultiplications 51
2.4. The antipode, the involution ω, and algebra generators 53
2.5. Cauchy product, Hall inner product, self-duality 56
2.6. Bialternants, Littlewood-Richardson: Stembridge's concise proof 67
2.7. The Pieri and Assaf-McNamara skew Pieri rule 72
2.8. Skewing and Lam's proof of the skew Pieri rule 76
2.9. Assorted exercises on symmetric functions 80
3. Zelevinsky's structure theory of positive self-dual Hopf algebras 94
3.1. Self-duality implies polynomiality 94
3.2. The decomposition theorem 97
3.3. Λ is the unique indecomposable PSH 100
4. Complex representations for $\mathfrak{S}_n$, wreath products, $GL_n(\mathbb{F}_q)$ 107
4.1. Review of complex character theory 107
4.2. Three towers of groups 115
4.3. Bialgebra and double cosets 117
4.4. Symmetric groups 125
4.5. Wreath products 128
4.6. General linear groups 130
4.7. Steinberg's unipotent characters 131
4.8. Examples: $GL_2(\mathbb{F}_2)$ and $GL_3(\mathbb{F}_2)$ 132
4.9. The Hall algebra 134
5. Quasisymmetric functions and P-partitions 140
5.1. Definitions, and Hopf structure 140
5.2. The fundamental basis and P-partitions 146
5.3. Standardization of n-tuples and the fundamental basis 155
5.4. The Hopf algebra NSym dual to QSym 156
6. Polynomial generators for QSym and Lyndon words 163
6.1. Lyndon words 163
6.2. Shuffles and Lyndon words 177

Date: July 27, 2020 (with minor corrections November 17, 2020).
Key words and phrases. Hopf algebra, combinatorics, symmetric functions, quasisymmetric functions.

6.3. Radford's theorem on the shuffle algebra 190
6.4. Polynomial freeness of QSym: statement and easy parts 193
6.5. Polynomial freeness of QSym: the general case 196
6.6. The Gessel-Reutenauer bijection and symmetric functions 204
7. Aguiar-Bergeron-Sottile character theory Part I: QSym as a terminal object 215
7.1. Characters and the universal property 215
7.2. Example: Ehrenborg's quasisymmetric function of a ranked poset 218
7.3. Example: Stanley's chromatic symmetric function of a graph 222
7.4. Example: The quasisymmetric function of a matroid 228
8. The Malvenuto-Reutenauer Hopf algebra of permutations 237
8.1. Definition and Hopf structure 237
9. Further topics 246
10. Some open problems and conjectures 247
11. Appendix: Some basics 248
11.1. Linear expansions and triangularity 248
12. Further hints to the exercises (work in progress) 253
12.1. Hints for Chapter 1 253
Acknowledgements 268
References 268

Introduction

The concept of a Hopf algebra crystallized out of algebraic topology and the study of algebraic groups in the 1940s and 1950s (see [8] and [35] for its history). Being a fairly elementary algebraic notion itself, it subsequently found applications in other mathematical disciplines, and is now particularly commonplace in representation theory[1].

These notes concern themselves (after a brief introduction into the algebraic foundations of Hopf algebra theory in Chapter 1) with the Hopf algebras that appear in combinatorics. These Hopf algebras tend to have bases naturally parametrized by combinatorial objects (partitions, compositions, permutations, tableaux, graphs, trees, posets, polytopes, etc.), and their Hopf-algebraic operations often encode basic operations on these objects[2]. Combinatorial results can then be seen as particular cases of general algebraic properties of Hopf algebras (e.g., the multiplicativity of the Möbius function can be recovered from the fact that the antipode of a Hopf algebra is an algebra anti-endomorphism), and many interesting invariants of combinatorial objects turn out to be evaluations of Hopf morphisms. In some cases (particularly that of symmetric functions), the rigidity in the structure of a Hopf algebra can lead to enlightening proofs.

One of the most elementary interesting examples of a combinatorial Hopf algebra is that of the symmetric functions. We will devote all of Chapter 2 to studying it, deviating from the usual treatments (such as in Stanley [206, Ch. 7], Sagan [186] and Macdonald [142]) by introducing the Hopf-algebraic structure early on and using it to obtain combinatorial results. Chapter 3 will underpin the importance of this algebra by proving Zelevinsky's main theorem of PSH theory, which (roughly) claims that a Hopf algebra over $\mathbb{Z}$ satisfying a certain set of axioms must be a tensor product of copies of the Hopf algebra of symmetric functions. These axioms are fairly restrictive, so this result is far from curtailing the diversity of combinatorial Hopf algebras; but they are natural enough that, as we will see in Chapter 4, they are satisfied for a Hopf algebra of representations of symmetric groups. As a consequence, this Hopf algebra will be revealed isomorphic to the symmetric functions – this is the famous Frobenius correspondence between symmetric functions and characters of symmetric groups, usually obtained through other ways ([73, §7.3], [186, §4.7]). We will further elaborate on the representation theories of wreath products and general linear groups over finite fields; while Zelevinsky's PSH theory does not fully explain the latter, it illuminates it significantly.

In the next chapters, we will study further examples of combinatorial Hopf algebras: the quasisymmetric functions and the noncommutative symmetric functions in Chapter 5, various other algebras (of graphs, posets, matroids, etc.) in Chapter 7, and the Malvenuto-Reutenauer Hopf algebra of permutations in Chapter 8.

The main prerequisite for reading these notes is a good understanding of graduate algebra[3], in particular multilinear algebra (tensor products, symmetric powers and exterior powers)[4] and basic categorical language[5]. In Chapter 4, familiarity with representation theory of finite groups (over $\mathbb{C}$) is assumed, along with the theory of finite fields and (at some places) the rational canonical form of a matrix. Only basic knowledge of combinatorics is required (except for a few spots in Chapter 7), and familiarity with geometry and topology is needed only to understand some tangential remarks. The concepts of Hopf algebras and coalgebras and the basics of symmetric function theory will be introduced as needed. We will work over a commutative base ring most of the time, but no commutative algebra (besides, occasionally, properties of modules over a PID) will be used.

These notes began as an accompanying text for Fall 2012 Math 8680 Topics in Combinatorics, a graduate class taught by the second author at the University of Minnesota. The first author has since added many

[1] where it provides explanations for similarities between group representations and Lie algebra representations

[2] such as concatenating two compositions, or taking the disjoint union of two graphs – but, more often, operations which return a multiset of results, such as cutting a composition into two pieces at all possible places, or partitioning a poset into two subposets in every way that satisfies a certain axiom

[3] William Schmitt's expositions [193] are tailored to a reader interested in combinatorial Hopf algebras; his notes on modules and algebras cover a significant part of what we need from abstract algebra, whereas those on categories cover all category theory we will use and much more.

[4] Keith Conrad's expository notes [40] are useful, even if not comprehensive, sources for the latter.

[5] We also will use a few nonstandard notions from linear algebra that are explained in the Appendix (Chapter 11).

exercises (and solutions[6]), as well as Chapter 6 on Lyndon words and the polynomiality of QSym. The notes might still grow, and any comments, corrections and complaints are welcome!

The course was an attempt to focus on examples that we find interesting, but which are hard to find fully explained currently in books or in one paper. Much of the subject of combinatorial Hopf algebras is fairly recent (1990s onwards) and still spread over research papers, although sets of lecture notes do exist, such as Foissy's [70]. A reference which we discovered late, having a great deal of overlap with these notes is Hazewinkel, Gubareni, and Kirichenko [93]. References for the purely algebraic theory of Hopf algebras are much more frequent (see the beginning of Chapter 1 for a list). Another recent text that has a significant amount of material in common with ours (but focuses on representation theory and probability applications) is Méliot's [153].

Be warned that our notes are highly idiosyncratic in choice of topics, and they steal heavily from the sources in the bibliography.

Warnings: Unless otherwise specified ...

- $\mathbf{k}$ here usually denotes a commutative ring[7].
- all maps between $\mathbf{k}$-modules are $\mathbf{k}$-linear.
- every ring or $\mathbf{k}$-algebra is associative and has a 1, and every ring morphism or $\mathbf{k}$-algebra morphism preserves the 1's.
- all $\mathbf{k}$-algebras A have the property that $(\lambda 1_A)\, a = a\, (\lambda 1_A) = \lambda a$ for all $\lambda \in \mathbf{k}$ and $a \in A$.
- all tensor products are over $\mathbf{k}$ (unless a subscript specifies a different base ring).
- 1 will denote the multiplicative identity in some ring like $\mathbf{k}$ or in some $\mathbf{k}$-algebra (sometimes also the identity of a group written multiplicatively).
- for any set S, we denote by id_S (or by id) the identity map on S.
- The symbols $\subset$ (for "subset") and $<$ (for "subgroup") don't imply properness (so $\mathbb{Z} \subset \mathbb{Z}$ and $\mathbb{Z} < \mathbb{Z}$).
- the n-th symmetric group (i.e., the group of all permutations of $\{1, 2, \ldots, n\}$) is denoted $\mathfrak{S}_n$.
- A permutation $\sigma \in \mathfrak{S}_n$ will often be identified with the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$, which will occasionally be written without commas and parentheses (i.e., as follows: $\sigma(1)\,\sigma(2)\cdots\sigma(n)$). This is called the *one-line notation* for permutations.
- The product of permutations $a \in \mathfrak{S}_n$ and $b \in \mathfrak{S}_n$ is defined by $(ab)(i) = a(b(i))$ for all i.
- *Words* over (or in) an *alphabet* I simply mean finite tuples of elements of a set I. It is customary to write such a word $(a_1, a_2, \ldots, a_k)$ as $a_1 a_2 \ldots a_k$ when this is not likely to be confused for multiplication.
- $\mathbb{N} := \{0, 1, 2, \ldots\}$.
- if i and j are any two objects, then $\delta_{i,j}$ denotes the *Kronecker delta* of i and j; this is the integer 1 if $i = j$ and 0 otherwise.
- a *family* of objects indexed by a set I means a choice of an object f_i for each element $i \in I$; this family will be denoted either by $(f_i)_{i \in I}$ or by $\{f_i\}_{i \in I}$ (and sometimes the "$i \in I$" will be omitted when the context makes it obvious – so we just write $\{f_i\}$).
- several objects $s_1, s_2, \ldots, s_k$ are said to be *distinct* if every $i \neq j$ satisfy $s_i \neq s_j$.
- similarly, several sets $S_1, S_2, \ldots, S_k$ are said to be *disjoint* if every $i \neq j$ satisfy $S_i \cap S_j = \varnothing$.
- the symbol $\sqcup$ (and the corresponding quantifier $\bigsqcup$) denotes a disjoint union of sets or posets. For example, if $S_1, S_2, \ldots, S_k$ are k sets, then $\bigsqcup_{i=1}^{k} S_i$ is their disjoint union. This disjoint union can mean either of the following two things:
  - It can mean the union $\bigcup_{i=1}^{k} S_i$ in the case when the sets $S_1, S_2, \ldots, S_k$ are disjoint. This is called an "internal disjoint union", and is simply a way to refer to the union of sets while simultaneously claiming that these sets are disjoint. Thus, of course, it is only well-defined if the sets are disjoint.
  - It can also mean the union $\bigcup_{i=1}^{k} \{i\} \times S_i$. This is called an "external disjoint union", and is well-defined whether or not the sets $S_1, S_2, \ldots, S_k$ are disjoint; it is a way to assemble the sets

[6]The version of the notes you are reading does not contain said solutions. The version that does can be downloaded from http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf or compiled from the sourcecode.

[7]As explained below, "ring" means "associative ring with 1". The most important cases are when $\mathbf{k}$ is a field or when $\mathbf{k} = \mathbb{Z}$.

$S_1, S_2, \ldots, S_k$ into a larger set which contains a copy of each of their elements that "remembers" which set this element comes from.

The two meanings are different, but in the case when $S_1, S_2, \ldots, S_k$ are disjoint, they are isomorphic. We hope the reader will not have a hard time telling which of them we are trying to evoke.

Similarly, the notion of a direct sum of $\mathbf{k}$-modules has two meanings ("internal direct sum" and "external direct sum").

- A sequence $(w_1, w_2, \ldots, w_k)$ of numbers (or, more generally, of elements of a poset) is said to be *strictly increasing* (or, for short, *increasing*) if it satisfies $w_1 < w_2 < \cdots < w_k$. A sequence $(w_1, w_2, \ldots, w_k)$ of numbers (or, more generally, of elements of a poset) is said to be *weakly increasing* (or *nondecreasing*) if it satisfies $w_1 \leq w_2 \leq \cdots \leq w_k$. Reversing the inequalities, we obtain the definitions of a *strictly decreasing* (a.k.a. *decreasing*) and of a *weakly decreasing* (a.k.a. *nonincreasing*) sequence. All these definitions extend in an obvious way to infinite sequences. Note that "nondecreasing" is not the same as "not decreasing"; for example, any sequence having at most one entry is both decreasing and nondecreasing, whereas the sequence $(1, 3, 1)$ is neither.

Hopefully context will resolve some of the ambiguities.

1. What is a Hopf algebra?

The standard references for Hopf algebras are Abe [1] and Sweedler [213], and some other good ones are [33, 36, 47, 93, 107, 118, 157, 176, 196, 225]. See also Foissy [70] and Manchon [149] for introductions to Hopf algebras tailored to combinatorial applications. Most texts only study Hopf algebras over fields (with exceptions such as [36, 33, 225]). We will work over arbitrary commutative rings[8], which requires some more care at certain points (but we will not go deep enough into the algebraic theory to witness the situation over commutative rings diverge seriously from that over fields).

Let's build up the definition of Hopf algebra structure bit-by-bit, starting with the more familiar definition of algebras.

1.1. **Algebras.** Recall that an *associative* $\mathbf{k}$*-algebra* is defined to be a $\mathbf{k}$-module A equipped with an associative $\mathbf{k}$-bilinear map $\mathrm{mult} : A \times A \to A$ (the *multiplication map* of A) and an element $1 \in A$ (the *(multiplicative) unity* or *identity* of A) that is neutral for this map mult (that is, it satisfies $\mathrm{mult}\,(a, 1) = \mathrm{mult}\,(1, a) = a$ for all $a \in A$). If we recall that

- $\mathbf{k}$-bilinear maps $A \times A \to A$ are in 1-to-1 correspondence with $\mathbf{k}$-linear maps $A \otimes A \to A$ (by the universal property of the tensor product), and
- elements of A are in 1-to-1 correspondence with $\mathbf{k}$-linear maps $\mathbf{k} \to A$,

then we can restate this classical definition of associative $\mathbf{k}$-algebras as follows in terms of $\mathbf{k}$-linear maps[9]:

Definition 1.1.1. An *associative* $\mathbf{k}$*-algebra* is a $\mathbf{k}$-module A equipped with a $\mathbf{k}$-linear *associative operation* $A \otimes A \xrightarrow{m} A$, and a $\mathbf{k}$-linear *unit* $\mathbf{k} \xrightarrow{u} A$, for which the following two diagrams are commutative:

(1.1.1)
$$\begin{array}{ccccc} & & A \otimes A \otimes A & & \\ & \swarrow^{m \otimes \mathrm{id}} & & \searrow^{\mathrm{id} \otimes m} & \\ A \otimes A & & & & A \otimes A \\ & \searrow_{m} & & \swarrow_{m} & \\ & & A & & \end{array}$$

(1.1.2)
$$\begin{array}{ccccc} A \otimes \mathbf{k} & \longleftarrow & A & \longrightarrow & \mathbf{k} \otimes A \\ \downarrow{\scriptstyle \mathrm{id} \otimes u} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle u \otimes \mathrm{id}} \\ A \otimes A & \xrightarrow{m} & A & \xleftarrow{m} & A \otimes A \end{array}$$

where the maps $A \to A \otimes \mathbf{k}$ and $A \to \mathbf{k} \otimes A$ are the isomorphisms sending $a \mapsto a \otimes 1$ and $a \mapsto 1 \otimes a$.

We abbreviate "associative $\mathbf{k}$-algebra" as "$\mathbf{k}$-algebra" (associativity is assumed unless otherwise specified) or as "algebra" (when $\mathbf{k}$ is clear from the context). We sometimes refer to m as the "multiplication map" of A as well.

As we said, the multiplication map $m : A \otimes A \to A$ sends each $a \otimes b$ to the product ab, and the unit map $u : \mathbf{k} \to A$ sends the identity $1_{\mathbf{k}}$ of $\mathbf{k}$ to the identity 1_A of A.

Well-known examples of $\mathbf{k}$-algebras are *tensor* and *symmetric algebras*, which we can think of as algebras of *words* and *multisets*, respectively.

Example 1.1.2. If V is a $\mathbf{k}$-module and $n \in \mathbb{N}$, then the *n-fold tensor power* $V^{\otimes n}$ of V is the $\mathbf{k}$-module $\underbrace{V \otimes V \otimes \cdots \otimes V}_{n \text{ times}}$. (For $n = 0$, this is the $\mathbf{k}$-module $\mathbf{k}$, spanned by the "empty tensor" $1_{\mathbf{k}}$.)

The *tensor algebra* $T(V) = \bigoplus_{n \geq 0} V^{\otimes n}$ on a $\mathbf{k}$-module V is an associative $\mathbf{k}$-algebra spanned (as $\mathbf{k}$-module) by decomposable tensors $v_1 v_2 \cdots v_k := v_1 \otimes v_2 \otimes \cdots \otimes v_k$ with $k \in \mathbb{N}$ and $v_1, v_2, \ldots, v_k \in V$. Its multiplication

[8] and we will profit from this generality in Chapters 3 and 4, where we will be applying the theory of Hopf algebras to $\mathbf{k} = \mathbb{Z}$ in a way that would not be possible over $\mathbf{k} = \mathbb{Q}$

[9] Explicitly speaking, we are replacing the $\mathbf{k}$-bilinear multiplication map $\mathrm{mult} : A \times A \to A$ by the $\mathbf{k}$-linear map $m : A \otimes A \to A,\ a \otimes b \mapsto \mathrm{mult}\,(a, b)$, and we are replacing the element $1 \in A$ by the $\mathbf{k}$-linear map $u : \mathbf{k} \to A,\ 1_{\mathbf{k}} \mapsto 1$.

is defined $\mathbf{k}$-linearly by

$$m\left(v_1 v_2 \cdots v_k \otimes w_1 w_2 \cdots w_\ell\right) := v_1 v_2 \cdots v_k w_1 w_2 \cdots w_\ell$$

[10] for all $k, \ell \in \mathbb{N}$ and $v_1, v_2, \ldots, v_k, w_1, w_2, \ldots, w_\ell$ in V. The unit map $u : \mathbf{k} \to T(V)$ sends $1_{\mathbf{k}}$ to the empty tensor $1_{T(V)} = 1_{\mathbf{k}} \in \mathbf{k} = V^{\otimes 0}$.

If V is a free $\mathbf{k}$-module, say with $\mathbf{k}$-basis $\{x_i\}_{i \in I}$, then $T(V)$ has a $\mathbf{k}$-basis of decomposable tensors $x_{i_1} \cdots x_{i_k} := x_{i_1} \otimes \cdots \otimes x_{i_k}$ indexed by *words* $(i_1, \ldots, i_k)$ in the alphabet I, and the multiplication on this basis is given by concatenation of words:

$$m(x_{i_1} \cdots x_{i_k} \otimes x_{j_1} \cdots x_{j_\ell}) = x_{i_1} \cdots x_{i_k} x_{j_1} \cdots x_{j_\ell}.$$

Recall that a *two-sided ideal* of a $\mathbf{k}$-algebra A is defined to be a $\mathbf{k}$-submodule J of A such that all $j \in J$ and $a \in A$ satisfy $ja \in J$ and $aj \in J$. Using tensors, we can restate this as follows: A *two-sided ideal* of a $\mathbf{k}$-algebra A means a $\mathbf{k}$-submodule J of A satisfying $m(J \otimes A) \subset J$ and $m(A \otimes J) \subset J$. Often, the word "two-sided" is omitted and one just speaks of an ideal.

It is well-known that if J is a two-sided ideal of a $\mathbf{k}$-algebra A, then one can form a *quotient algebra* A/J.

Example 1.1.3. Let V be a $\mathbf{k}$-module. The *symmetric algebra* $\mathrm{Sym}(V) = \bigoplus_{n \geq 0} \mathrm{Sym}^n(V)$ is the quotient of $T(V)$ by the two-sided ideal generated by all elements $xy - yx$ with x, y in V. When V is a free $\mathbf{k}$-module with basis $\{x_i\}_{i \in I}$, this symmetric algebra $S(V)$ can be identified with a (commutative) polynomial algebra $\mathbf{k}[x_i]_{i \in I}$, having a $\mathbf{k}$-basis of (commutative) monomials $x_{i_1} \cdots x_{i_k}$ as $\{i_1, \ldots, i_k\}_{\text{multiset}}$ runs through all finite multisubsets[11] of I, and with multiplication defined $\mathbf{k}$-linearly via multiset union[12].

Note that the $\mathbf{k}$-module $\mathbf{k}$ itself canonically becomes a $\mathbf{k}$-algebra. Its associative operation $m : \mathbf{k} \otimes \mathbf{k} \to \mathbf{k}$ is the canonical isomorphism $\mathbf{k} \otimes \mathbf{k} \to \mathbf{k}$, and its unit $u : \mathbf{k} \to \mathbf{k}$ is the identity map.

Topology and group theory give more examples.

Example 1.1.4. The *cohomology algebra* $H^*(X; \mathbf{k}) = \bigoplus_{i \geq 0} H^i(X; \mathbf{k})$ with coefficients in $\mathbf{k}$ for a topological space X has an associative *cup product*. Its unit $\mathbf{k} = H^*(\mathbf{pt}; \mathbf{k}) \xrightarrow{u} H^*(X; \mathbf{k})$ is induced from the unique (continuous) map $X \to \mathbf{pt}$, where $\mathbf{pt}$ is a one-point space.

Example 1.1.5. For a group G, the *group algebra* $\mathbf{k}G$ has $\mathbf{k}$-basis $\{t_g\}_{g \in G}$ and multiplication defined $\mathbf{k}$-linearly by $t_g t_h = t_{gh}$, and unit defined by $u(1) = t_e$, where e is the identity element of G.

1.2. **Coalgebras.** In Definition 1.1.1, we have defined the notion of an algebra entirely in terms of linear maps; thus, by reversing all arrows, we can define a dual notion, which is called a *coalgebra*. If we are to think of the multiplication $A \otimes A \to A$ in an algebra as *putting together* two basis elements of A to get a sum of basis elements of A, then coalgebra structure should be thought of as *taking basis elements apart*.

Definition 1.2.1. A *co-associative* $\mathbf{k}$-*coalgebra* is a $\mathbf{k}$-module C equipped with a *comultiplication*, that is, a $\mathbf{k}$-linear map $C \xrightarrow{\Delta} C \otimes C$, and a $\mathbf{k}$-linear *counit* $C \xrightarrow{\epsilon} \mathbf{k}$ for which the following diagrams (which are exactly the diagrams in (1.1.1) and (1.1.2) but with *all arrows reversed*) are commutative:

---

[10] Some remarks about our notation (which we are using here and throughout these notes) are in order.

Since we are working with tensor products of $\mathbf{k}$-modules like $T(V)$ – which themselves are made of tensors – here, we must specify what the $\otimes$ sign means in expressions like $a \otimes b$ where a and b are elements of $T(V)$. Our convention is the following: When a and b are elements of a tensor algebra $T(V)$, we always understand $a \otimes b$ to mean the pure tensor $a \otimes b \in T(V) \otimes T(V)$ rather than the product of a and b inside the tensor algebra $T(V)$. The latter product will plainly be written ab.

The operator precedence between $\otimes$ and multiplication in $T(V)$ is such that multiplication in $T(V)$ binds more tightly than the $\otimes$ sign; e.g., the term $ab \otimes cd$ means $(ab) \otimes (cd)$. The same convention applies to any algebra instead of $T(V)$.

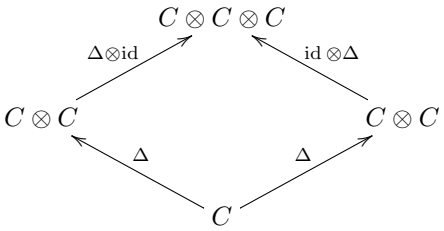
[11] By a *multisubset* of a set S, we mean a multiset each of whose elements belongs to S (but can appear arbitrarily often).

[12] The *multiset union* of two finite multisets A and B is defined to be the multiset C with the property that every x satisfies

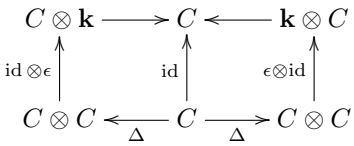
$$(\text{multiplicity of } x \text{ in } C) = (\text{multiplicity of } x \text{ in } A) + (\text{multiplicity of } x \text{ in } B).$$

Equivalently, the multiset union of $\{a_1, a_2, \ldots, a_k\}_{\text{multiset}}$ and $\{b_1, b_2, \ldots, b_\ell\}_{\text{multiset}}$ is $\{a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell\}_{\text{multiset}}$. The multiset union is also known as the *disjoint union* of multisets.

(1.2.1)



(1.2.2)



Here the maps $C \otimes \mathbf{k} \to C$ and $\mathbf{k} \otimes C \to C$ are the isomorphisms sending $c \otimes 1 \mapsto c$ and $1 \otimes c \mapsto c$.

We abbreviate "co-associative $\mathbf{k}$-coalgebra" as "$\mathbf{k}$-coalgebra" (co-associativity, i.e., the commutativity of the diagram (1.2.1), is assumed unless otherwise specified) or as "coalgebra" (when $\mathbf{k}$ is clear from the context).

Sometimes, the word "coproduct" is used as a synonym for "comultiplication"[13].

One often uses the *Sweedler notation*

$$\Delta(c) = \sum_{(c)} c_1 \otimes c_2 = \sum c_1 \otimes c_2 \tag{1.2.3}$$

to abbreviate formulas involving Δ. This means that an expression of the form $\sum_{(c)} f(c_1, c_2)$ (where $f : C \times C \to M$ is some $\mathbf{k}$-bilinear map from $C \times C$ to some $\mathbf{k}$-module M) has to be understood to mean $\sum_{k=1}^{m} f(d_k, e_k)$, where $k \in \mathbb{N}$ and $d_1, d_2, \ldots, d_k \in C$ and $e_1, e_2, \ldots, e_k \in C$ are chosen such that $\Delta(c) = \sum_{k=1}^{m} d_k \otimes e_k$. (There are many ways to choose such k, d_i and e_i, but they all produce the same result $\sum_{k=1}^{m} f(d_k, e_k)$. Indeed, the result they produce is $F(\Delta(c))$, where $F : C \otimes C \to M$ is the $\mathbf{k}$-linear map induced by the bilinear map f.) For example, commutativity of the left square in (1.2.2) asserts that $\sum_{(c)} c_1 \epsilon(c_2) = c$ for each $c \in C$. Likewise, commutativity of the right square in (1.2.2) asserts that $\sum_{(c)} \epsilon(c_1) c_2 = c$ for each $c \in C$. The commutativity of (1.2.1) can be written as $\sum_{(c)} \Delta(c_1) \otimes c_2 = \sum_{(c)} c_1 \otimes \Delta(c_2)$, or (using nested Sweedler notation to unravel the two remaining Δ's) as

$$\sum_{(c)} \sum_{(c_1)} (c_1)_1 \otimes (c_1)_2 \otimes c_2 = \sum_{(c)} \sum_{(c_2)} c_1 \otimes (c_2)_1 \otimes (c_2)_2.$$

The $\mathbf{k}$-module $\mathbf{k}$ itself canonically becomes a $\mathbf{k}$-coalgebra, with its comultiplication $\Delta : \mathbf{k} \to \mathbf{k} \otimes \mathbf{k}$ being the canonical isomorphism $\mathbf{k} \to \mathbf{k} \otimes \mathbf{k}$, and its counit $\epsilon : \mathbf{k} \to \mathbf{k}$ being the identity map.

Example 1.2.2. Let $\mathbf{k}$ be a field. The *homology* $H_*(X; \mathbf{k}) = \bigoplus_{i \geq 0} H_i(X; \mathbf{k})$ for a topological space X is naturally a coalgebra: the (continuous) *diagonal embedding* $X \to X \times X$ sending $x \mapsto (x, x)$ induces a coassociative map

$$H_*(X; \mathbf{k}) \to H_*(X \times X; \mathbf{k}) \cong H_*(X; \mathbf{k}) \otimes H_*(X; \mathbf{k})$$

in which the last isomorphism comes from the *Künneth theorem* with field coefficients $\mathbf{k}$. As before, the unique (continuous) map $X \to \mathbf{pt}$ induces the counit $H_*(X; \mathbf{k}) \xrightarrow{\epsilon} H_*(\mathbf{pt}; \mathbf{k}) \cong \mathbf{k}$.

Exercise 1.2.3. Let C be a $\mathbf{k}$-module, and let $\Delta : C \to C \otimes C$ be a $\mathbf{k}$-linear map. Prove that there exists *at most one* $\mathbf{k}$-linear map $\epsilon : C \to \mathbf{k}$ such that the diagram (1.2.2) commutes.

For us, the notion of a coalgebra serves mostly as a stepping stone towards that of a Hopf algebra, which will be the focus of these notes. However, coalgebras have interesting properties of their own (see, e.g., [150]).

[13] although the word "coproduct" already has a different meaning in algebra

1.3. **Morphisms, tensor products, and bialgebras.** Just as we rewrote the definition of an algebra in terms of linear maps (in Definition 1.1.1), we can likewise rephrase the standard definition of a morphism of algebras:

Definition 1.3.1. A *morphism of algebras* is a $\mathbf{k}$-linear map $A \xrightarrow{\varphi} B$ between two $\mathbf{k}$-algebras A and B that makes the following two diagrams commute:

(1.3.1)
$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle m_A}\uparrow & & \uparrow{\scriptstyle m_B} \\ A \otimes A & \xrightarrow{\varphi\otimes\varphi} & B \otimes B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ & {\scriptstyle u_A}\nwarrow \quad \nearrow{\scriptstyle u_B} & \\ & \mathbf{k} & \end{array}$$

Here the subscripts on m_A, m_B, u_A, u_B indicate for which algebra they are part of the structure (e.g., the map u_A is the map u of the algebra A); we will occasionally use such conventions from now on.

Similarly, a *morphism of coalgebras* is a $\mathbf{k}$-linear map $C \xrightarrow{\varphi} D$ between two $\mathbf{k}$-coalgebras C and D that makes the reverse diagrams commute:

(1.3.2)
$$\begin{array}{ccc} C & \xrightarrow{\varphi} & D \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_D} \\ C \otimes C & \xrightarrow{\varphi\otimes\varphi} & D \otimes D \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{\varphi} & D \\ & {\scriptstyle \epsilon_C}\searrow \quad \swarrow{\scriptstyle \epsilon_D} & \\ & \mathbf{k} & \end{array}$$

As usual, we shall use the word "*homomorphism*" as a synonym for "morphism", and we will say "$\mathbf{k}$-coalgebra homomorphism" for "homomorphism of coalgebras" (and similarly for algebras and other structures).

As usual, the word "*isomorphism*" (of algebras, of coalgebras, or of other structures that we will define further below) means "invertible morphism whose inverse is a morphism as well". Two algebras (or coalgebras, or other structures) are said to be *isomorphic* if there exists an isomorphism between them.

Example 1.3.2. Let $\mathbf{k}$ be a field. Continuous maps $X \xrightarrow{f} Y$ of topological spaces induce algebra morphisms $H^*(Y;\mathbf{k}) \to H^*(X;\mathbf{k})$, and coalgebra morphisms $H_*(X;\mathbf{k}) \to H_*(Y;\mathbf{k})$.

Coalgebra morphisms behave similarly to algebra morphisms in many regards: For example, the inverse of an invertible coalgebra morphism is again a coalgebra morphism[14]. Thus, the invertible coalgebra morphisms are precisely the coalgebra isomorphisms.

Definition 1.3.3. Given two $\mathbf{k}$-algebras A, B, their tensor product $A \otimes B$ also becomes a $\mathbf{k}$-algebra defining the multiplication bilinearly via

$$m((a \otimes b) \otimes (a' \otimes b')) := aa' \otimes bb',$$

or, in other words, $m_{A\otimes B}$ is the composite map

$$A \otimes B \otimes A \otimes B \xrightarrow{\mathrm{id}\otimes T\otimes \mathrm{id}} A \otimes A \otimes B \otimes B \xrightarrow{m_A \otimes m_B} A \otimes B$$

where T is the *twist map* $B \otimes A \to A \otimes B$ that sends $b \otimes a \mapsto a \otimes b$. (See Exercise 1.3.4(a) below for a proof that this $\mathbf{k}$-algebra $A \otimes B$ is well-defined.)

Here we are omitting the topologist's sign in the twist map which should be present for graded algebras and coalgebras that come from cohomology and homology: For homogeneous elements a and b of two graded modules A and B, the topologist's twist map $T : B \otimes A \to A \otimes B$ sends

$$b \otimes a \longmapsto (-1)^{\deg(b)\deg(a)} a \otimes b \tag{1.3.3}$$

instead of $b \otimes a \mapsto a \otimes b$. This means that, if one is using the topologists' convention, most of our examples which we later call *graded* should actually be considered to live in only *even* degrees (which can be achieved, e.g., by artificially doubling all degrees in their grading). We will, however, keep to our own definitions (so that our twist map T will always send $b \otimes a \mapsto a \otimes b$) unless otherwise noted. Only in parts of Exercise 1.6.5 will we use the topologist's sign. Readers interested in the wide world of algebras defined using the topologist's

[14] The easy proof of this fact is left to the reader.

sign convention (which is also known as the *Koszul sign rule*) can consult [65, Appendix A2]; see also [87] for applications to algebraic combinatorics[15].

The unit element of $A \otimes B$ is $1_A \otimes 1_B$, meaning that the unit map $\mathbf{k} \xrightarrow{u_{A\otimes B}} A \otimes B$ is the composite

$$\mathbf{k} \longrightarrow \mathbf{k} \otimes \mathbf{k} \xrightarrow{u_A \otimes u_B} A \otimes B \, .$$

Similarly, given two coalgebras C, D, one can make $C \otimes D$ a coalgebra in which the comultiplication and counit maps are the composites of

$$C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes D \otimes D \xrightarrow{\mathrm{id} \otimes T \otimes \mathrm{id}} C \otimes D \otimes C \otimes D$$

and

$$C \otimes D \xrightarrow{\epsilon_C \otimes \epsilon_D} \mathbf{k} \otimes \mathbf{k} \longrightarrow \mathbf{k} \, .$$

(See Exercise 1.3.4(b) below for a proof that this $\mathbf{k}$-coalgebra $C \otimes D$ is well-defined.)

Exercise 1.3.4. (a) Let A and B be two $\mathbf{k}$-algebras. Show that the $\mathbf{k}$-algebra $A \otimes B$ introduced in Definition 1.3.3 is actually well-defined (i.e., its multiplication and unit satisfy the axioms of a $\mathbf{k}$-algebra).

(b) Let C and D be two $\mathbf{k}$-coalgebras. Show that the $\mathbf{k}$-coalgebra $C \otimes D$ introduced in Definition 1.3.3 is actually well-defined (i.e., its comultiplication and counit satisfy the axioms of a $\mathbf{k}$-coalgebra).

It is straightforward to show that the concept of tensor products of algebras and of coalgebras satisfy the properties one would expect:

- For any three $\mathbf{k}$-coalgebras C, D and E, the $\mathbf{k}$-linear map
$$(C \otimes D) \otimes E \to C \otimes (D \otimes E) \, , \qquad (c \otimes d) \otimes e \mapsto c \otimes (d \otimes e)$$
is a coalgebra isomorphism. This allows us to speak of the $\mathbf{k}$-coalgebra $C \otimes D \otimes E$ without worrying about the parenthesization.
- For any two $\mathbf{k}$-coalgebras C and D, the $\mathbf{k}$-linear map
$$T : C \otimes D \to D \otimes C, \qquad c \otimes d \mapsto d \otimes c$$
is a coalgebra isomorphism.
- For any $\mathbf{k}$-coalgebra C, the $\mathbf{k}$-linear maps
$$C \to \mathbf{k} \otimes C, \qquad c \mapsto 1 \otimes c \qquad \text{and}$$
$$C \to C \otimes \mathbf{k}, \qquad c \mapsto c \otimes 1$$
are coalgebra isomorphisms.
- Similar properties hold for algebras instead of coalgebras.

One of the first signs that these definitions interact nicely is the following straightforward proposition.

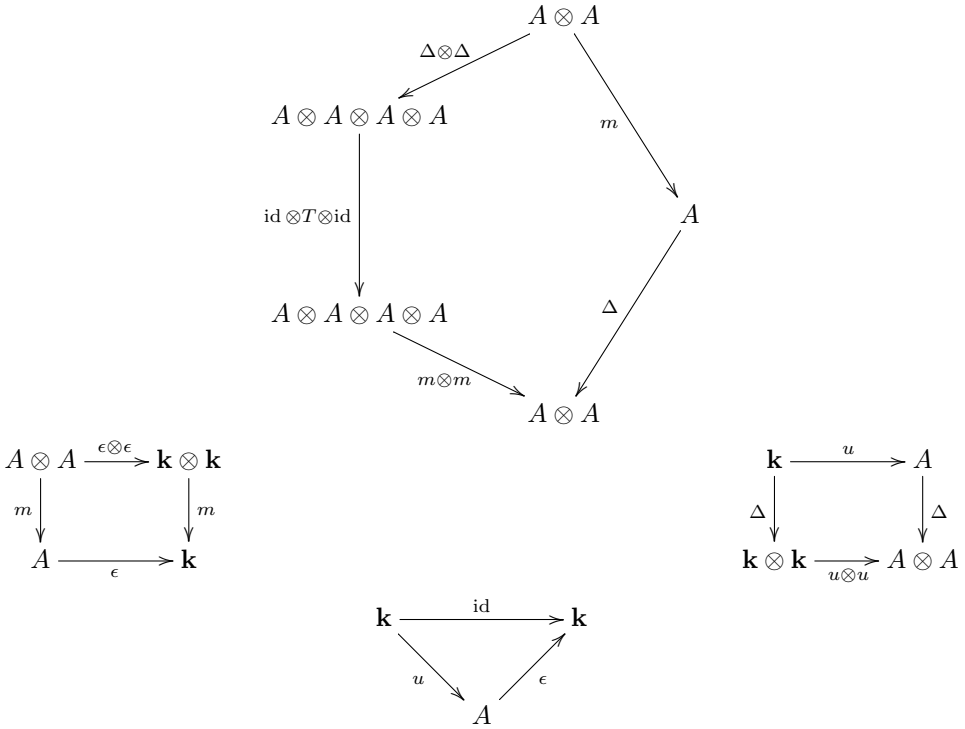
Proposition 1.3.5. *When A is both a $\mathbf{k}$-algebra and a $\mathbf{k}$-coalgebra, the following are equivalent:*

- *The maps Δ and ϵ are morphisms for the algebra structure (A, m, u).*
- *The maps m and u are morphisms for the coalgebra structure (A, Δ, ϵ).*

[15]To be precise, [87] works with the related concept of *superalgebras*, which are graded by elements of $\mathbb{Z}/2\mathbb{Z}$ rather than $\mathbb{N}$ but use the same sign convention as the topologists have for algebras.

- *These four diagrams commute:*

(1.3.4)

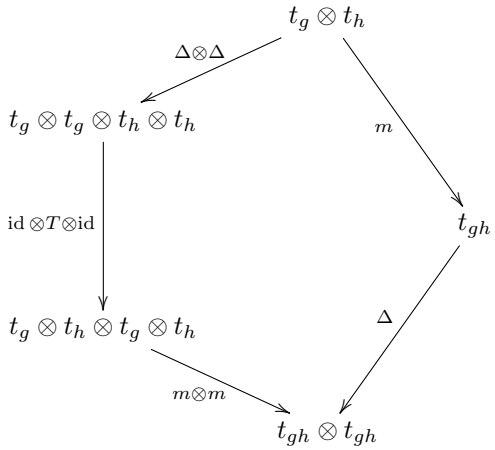


Exercise 1.3.6. (a) If A, A', B and B' are four $\mathbf{k}$-algebras, and $f : A \to A'$ and $g : B \to B'$ are two $\mathbf{k}$-algebra homomorphisms, then show that $f \otimes g : A \otimes B \to A' \otimes B'$ is a $\mathbf{k}$-algebra homomorphism.

(b) If C, C', D and D' are four $\mathbf{k}$-coalgebras, and $f : C \to C'$ and $g : D \to D'$ are two $\mathbf{k}$-coalgebra homomorphisms, then show that $f \otimes g : C \otimes D \to C' \otimes D'$ is a $\mathbf{k}$-coalgebra homomorphism.

Definition 1.3.7. Call the $\mathbf{k}$-module A a $\mathbf{k}$-*bialgebra* if it is a $\mathbf{k}$-algebra and $\mathbf{k}$-coalgebra satisfying the three equivalent conditions in Proposition 1.3.5.

Example 1.3.8. For a group G, one can make the group algebra $\mathbf{k}G$ a coalgebra with counit $\mathbf{k}G \xrightarrow{\epsilon} \mathbf{k}$ mapping $t_g \mapsto 1$ for all g in G, and with comultiplication $\mathbf{k}G \xrightarrow{\Delta} \mathbf{k}G \otimes \mathbf{k}G$ given by $\Delta(t_g) := t_g \otimes t_g$. Checking the various diagrams in (1.3.4) commute is easy. For example, one can check the pentagonal diagram on each basis element $t_g \otimes t_h$:



Remark 1.3.9. In fact, one can think of adding a bialgebra structure to a $\mathbf{k}$-algebra A as a way of making A-modules M, N have an A-module structure on their tensor product $M \otimes N$: the algebra $A \otimes A$ already acts naturally on $M \otimes N$, so one can let a in A act via $\Delta(a)$ in $A \otimes A$. In the theory of group representations

over $\mathbf{k}$, that is, $\mathbf{k}G$-modules M, this is how one defines the *diagonal action* of G on $M \otimes N$, namely t_g acts as $t_g \otimes t_g$.

Definition 1.3.10. An element x in a coalgebra for which $\Delta(x) = x \otimes x$ and $\epsilon(x) = 1$ is called *group-like*.

An element x in a bialgebra for which $\Delta(x) = 1 \otimes x + x \otimes 1$ is called *primitive*. We shall also sometimes abbreviate "primitive element" as "primitive".

Example 1.3.11. Let V be a $\mathbf{k}$-module. The *tensor algebra* $T(V) = \bigoplus_{n \geq 0} V^{\otimes n}$ is a coalgebra, with counit ϵ equal to the identity on $V^{\otimes 0} = \mathbf{k}$ and the zero map on $V^{\otimes n}$ for $n > 0$, and with comultiplication defined to make the elements x in $V^{\otimes 1} = V$ all primitive:

$$\Delta(x) := 1 \otimes x + x \otimes 1 \text{ for } x \in V^{\otimes 1}.$$

Since the elements of V generate $T(V)$ as a $\mathbf{k}$-algebra, and since $T(V) \otimes T(V)$ is also an associative $\mathbf{k}$-algebra, the universal property of $T(V)$ as the free associative $\mathbf{k}$-algebra on the generators V allows one to define $T(V) \xrightarrow{\Delta} T(V) \otimes T(V)$ arbitrarily on V, and extend it as an algebra morphism.

It may not be obvious that this Δ is coassociative, but one can prove this as follows. Note that

$$((\mathrm{id} \otimes \Delta) \circ \Delta)(x) = x \otimes 1 \otimes 1 + 1 \otimes x \otimes 1 + 1 \otimes 1 \otimes x = ((\Delta \otimes \mathrm{id}) \circ \Delta)(x)$$

for every x in V. Hence the two maps $(\mathrm{id} \otimes \Delta) \circ \Delta$ and $(\Delta \otimes \mathrm{id}) \circ \Delta$, considered as algebra morphisms $T(V) \to T(V) \otimes T(V) \otimes T(V)$, must coincide on every element of $T(V)$ since they coincide on V. We leave it as an exercise to check the map ϵ defined as above satisfies the counit axioms (1.2.2).

Here is a sample calculation in $T(V)$ when x, y, z are three elements of V:

$$\begin{aligned}
\Delta(xyz) &= \Delta(x)\Delta(y)\Delta(z) \\
&= (1 \otimes x + x \otimes 1)(1 \otimes y + y \otimes 1)(1 \otimes z + z \otimes 1) \\
&= (1 \otimes xy + x \otimes y + y \otimes x + xy \otimes 1)(1 \otimes z + z \otimes 1) \\
&= 1 \otimes xyz + x \otimes yz + y \otimes xz + z \otimes xy \\
&\qquad + xy \otimes z + xz \otimes y + yz \otimes x + xyz \otimes 1.
\end{aligned}$$

This illustrates the idea that comultiplication "takes basis elements apart" (and, in the case of $T(V)$, not just basis elements, but any decomposable tensors). Here for any $v_1, v_2, \ldots, v_n$ in V one has

$$\Delta(v_1 v_2 \cdots v_n) = \sum v_{j_1} \cdots v_{j_r} \otimes v_{k_1} \cdots v_{k_{n-r}}$$

where the sum is over ordered pairs $(j_1, j_2, \ldots, j_r), (k_1, k_2, \ldots, k_{n-r})$ of complementary subwords of the word $(1, 2, \ldots, n)$. [16] Equivalently (and in a more familiar language),

$$\Delta(v_1 v_2 \cdots v_n) = \sum_{I \subset \{1,2,\ldots,n\}} v_I \otimes v_{\{1,2,\ldots,n\} \setminus I}, \tag{1.3.5}$$

where v_J (for J a subset of $\{1, 2, \ldots, n\}$) denotes the product of all v_j with $j \in J$ in the order of increasing j.

We can rewrite the axioms of a $\mathbf{k}$-bialgebra A using Sweedler notation. Indeed, asking for $\Delta : A \to A \otimes A$ to be a $\mathbf{k}$-algebra morphism is equivalent to requiring that

$$\sum_{(ab)} (ab)_1 \otimes (ab)_2 = \sum_{(a)} \sum_{(b)} a_1 b_1 \otimes a_2 b_2 \qquad \text{for all } a, b \in A \tag{1.3.6}$$

and $\sum_{(1)} 1_1 \otimes 1_2 = 1_A \otimes 1_A$. (The other axioms have already been rewritten or don't need Sweedler notation.)

Recall one can quotient a $\mathbf{k}$-algebra A by a two-sided ideal J to obtain a quotient algebra A/J. An analogous construction can be done for coalgebras using the following concept, which is dual to that of a two-sided ideal:

[16] More formally speaking, the sum is over all permutations $(j_1, j_2, \ldots, j_r, k_1, k_2, \ldots, k_{n-r})$ of $(1, 2, \ldots, n)$ satisfying $j_1 < j_2 < \cdots < j_r$ and $k_1 < k_2 < \cdots < k_{n-r}$.

Definition 1.3.12. In a coalgebra C, a *two-sided coideal* is a $\mathbf{k}$-submodule $J \subset C$ for which

$$\Delta(J) \subset J \otimes C + C \otimes J,$$
$$\epsilon(J) = 0.$$

The quotient $\mathbf{k}$-module C/J then inherits a coalgebra structure[17]. Similarly, in a bialgebra A, a subset $J \subset A$ which is both a two-sided ideal and two-sided coideal gives rise to a quotient bialgebra A/J.

Exercise 1.3.13. Let A and C be two $\mathbf{k}$-coalgebras, and $f : A \to C$ a surjective coalgebra homomorphism.

(a) If f is surjective, then show that $\ker f$ is a two-sided coideal of A.
(b) If $\mathbf{k}$ is a field, then show that $\ker f$ is a two-sided coideal of A.

Example 1.3.14. Let V be a $\mathbf{k}$-module. The *symmetric algebra* $\mathrm{Sym}(V)$ was defined as the quotient of the tensor algebra $T(V)$ by the two-sided ideal J generated by all *commutators* $[x, y] = xy - yx$ for x, y in V (see Example 1.1.3). Note that x, y are primitive elements in $T(V)$, and the following very reusable calculation shows that *the commutator of two primitives is primitive*:

$$\begin{aligned}
\Delta[x,y] &= \Delta(xy-yx) = \Delta(x)\,\Delta(y) - \Delta(y)\,\Delta(x) \\
&\qquad \text{(since } \Delta \text{ is an algebra homomorphism)} \\
&= (1\otimes x + x\otimes 1)(1\otimes y + y\otimes 1) - (1\otimes y + y\otimes 1)(1\otimes x + x\otimes 1) \\
&= 1\otimes xy - 1\otimes yx + xy\otimes 1 - yx\otimes 1 \\
&\qquad + x\otimes y + y\otimes x - x\otimes y - y\otimes x \\
&= 1\otimes(xy-yx) + (xy-yx)\otimes 1 \\
&= 1\otimes[x,y] + [x,y]\otimes 1. \qquad (1.3.7)
\end{aligned}$$

In particular, the commutators $[x, y]$ have $\Delta[x, y]$ in $J \otimes T(V) + T(V) \otimes J$. They also satisfy $\epsilon([x, y]) = 0$. Since they are generators for J as a two-sided ideal, it is not hard to see this implies $\Delta(J) \subset J \otimes T(V) + T(V) \otimes J$, and $\epsilon(J) = 0$. Thus J is also a two-sided coideal, and $\mathrm{Sym}(V) = T(V)/J$ inherits a bialgebra structure.

In fact we will see in Section 3.1 that symmetric algebras are the universal example of bialgebras which are *graded, connected, commutative, cocommutative*. But first we should define some of these concepts.

Definition 1.3.15. (a) A *graded* $\mathbf{k}$*-module*[18] is a $\mathbf{k}$-module V equipped with a $\mathbf{k}$-module direct sum decomposition $V = \bigoplus_{n\geq 0} V_n$. In this case, the addend V_n (for any given $n \in \mathbb{N}$) is called the *n-th homogeneous component* (or the *n-th graded component*) of the graded $\mathbf{k}$-module V. Furthermore, elements x in V_n are said to be *homogeneous* of degree n; occasionally, the notation $\deg(x) = n$ is used to signify this[19]. The decomposition $\bigoplus_{n\geq 0} V_n$ of V (that is, the family of submodules $(V_n)_{n\in\mathbb{N}}$) is called the *grading* of V.

(b) The tensor product $V \otimes W$ of two graded $\mathbf{k}$-modules V and W is, by default, endowed with the graded module structure in which

$$(V\otimes W)_n := \bigoplus_{i+j=n} V_i \otimes W_j.$$

(c) A $\mathbf{k}$-linear map $V \xrightarrow{\varphi} W$ between two graded $\mathbf{k}$-modules is called *graded* if $\varphi(V_n) \subset W_n$ for all n. Graded $\mathbf{k}$-linear maps are also called *homomorphisms of graded* $\mathbf{k}$*-modules*. An *isomorphism of graded* $\mathbf{k}$*-modules* means an invertible graded $\mathbf{k}$-linear map whose inverse is also graded.[20]

---

[17] Indeed, $J \otimes C + C \otimes J$ is contained in the kernel of the canonical map $C \otimes C \to (C/J) \otimes (C/J)$; therefore, the condition $\Delta(J) \subset J \otimes C + C \otimes J$ shows that the map $C \xrightarrow{\Delta} C \otimes C \twoheadrightarrow (C/J) \otimes (C/J)$ factors through a map $\overline{\Delta} : C/J \to (C/J) \otimes (C/J)$. Likewise, $\epsilon(J) = 0$ shows that the map $\epsilon : C \to \mathbf{k}$ factors through a map $\overline{\epsilon} : C/J \to \mathbf{k}$. Equipping C/J with these maps $\overline{\Delta}$ and $\overline{\epsilon}$, we obtain a coalgebra (as the commutativity of the required diagrams follows from the corresponding property of C).

[18] also known as an "$\mathbb{N}$*-graded* $\mathbf{k}$*-module*"

[19] This notation should not be taken too literally, as it would absurdly imply that $\deg(0)$ "equals" every $n \in \mathbb{N}$ at the same time, since $0 \in V_n$ for all n.

[20] We shall see in Exercise 1.3.18 that the "whose inverse is also graded" requirement is actually superfluous (i.e., it is automatically satisfied for an invertible graded $\mathbf{k}$-linear map); we are imposing it only in order to stick to our tradition of defining "isomorphisms" as invertible morphisms whose inverses are morphisms as well.

(d) Say that a $\mathbf{k}$-algebra (or coalgebra, or bialgebra) is *graded* if it is a graded $\mathbf{k}$-module and all of the relevant structure maps (u, ϵ, m, Δ) are graded.
(e) Say that a graded $\mathbf{k}$-module V is *connected* if $V_0 \cong \mathbf{k}$.
(f) Let V be a graded $\mathbf{k}$-module. Then, a *graded $\mathbf{k}$-submodule of V* (sometimes also called a *homogeneous $\mathbf{k}$-submodule of V*) means a graded $\mathbf{k}$-module W such that $W \subset V$ as sets, and such that the inclusion map $W \hookrightarrow V$ is a graded $\mathbf{k}$-linear map.
Note that if W is a graded $\mathbf{k}$-submodule of V, then the grading of W is uniquely determined by the underlying set of W and the grading of V – namely, the n-th graded component W_n of W is $W_n = W \cap V_n$ for each $n \in \mathbb{N}$. Thus, we can specify a graded $\mathbf{k}$-submodule of V without explicitly specifying its grading. From this point of view, a graded $\mathbf{k}$-submodule of V can also be defined as a $\mathbf{k}$-submodule W of V satisfying $W = \sum_{n \in \mathbb{N}} (W \cap V_n)$. (This sum is automatically a direct sum, and thus defines a grading on W.)

Example 1.3.16. Let $\mathbf{k}$ be a field. A path-connected space X has its homology and cohomology

$$H_*(X; \mathbf{k}) = \bigoplus_{i \geq 0} H_i(X; \mathbf{k}),$$
$$H^*(X; \mathbf{k}) = \bigoplus_{i \geq 0} H^i(X; \mathbf{k})$$

carrying the structure of connected graded coalgebras and algebras, respectively. If in addition, X is a topological group, or even less strongly, a *homotopy-associative H-space* (e.g. the *loop space* ΩY on some other space Y), the continuous multiplication map $X \times X \to X$ induces an algebra structure on $H_*(X; \mathbf{k})$ and a coalgebra structure on $H^*(X; \mathbf{k})$, so that each become bialgebras in the topologist's sense (i.e., with the twist as in (1.3.3)), and these bialgebras are dual to each other in a sense soon to be discussed. This was Hopf's motivation: the (co-)homology of a compact Lie group carries bialgebra structure that explains why it takes a certain form; see Cartier [35, §2].

Example 1.3.17. Let V be a graded $\mathbf{k}$-module. Then, its tensor algebra $T(V)$ and its symmetric algebra $\mathrm{Sym}(V)$ are graded Hopf algebras. The grading is given as follows: If $v_1, v_2, \ldots, v_k$ are homogeneous elements of V having degrees $i_1, i_2, \ldots, i_k$, respectively, then the elements $v_1 v_2 \cdots v_k$ of $T(V)$ and $\mathrm{Sym}(V)$ are homogeneous of degree $i_1 + i_2 + \cdots + i_k$. That is, we have

$$\deg(v_1 v_2 \cdots v_k) = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_k)$$

for any homogeneous elements $v_1, v_2, \ldots, v_k$ of V.

Assuming that $V_0 = 0$, the graded algebras $T(V)$ and $\mathrm{Sym}(V)$ are connected. This is a fairly common situation in combinatorics. For example, we will often turn a (non-graded) $\mathbf{k}$-module V into a graded $\mathbf{k}$-module by declaring that all elements of V are homogeneous of degree 1, but at other times, it will make sense to have V live in different (positive) degrees.

Exercise 1.3.18. Let V and W be two graded $\mathbf{k}$-modules. Prove that if $f : V \to W$ is an invertible graded $\mathbf{k}$-linear map, then its inverse $f^{-1} : W \to V$ is also graded.

Exercise 1.3.19. Let $A = \bigoplus_{n \geq 0} A_n$ be a graded $\mathbf{k}$-bialgebra. We denote by $\mathfrak{p}$ the set of all primitive elements of A.

(a) Show that $\mathfrak{p}$ is a graded $\mathbf{k}$-submodule of A (that is, we have $\mathfrak{p} = \bigoplus_{n \geq 0} (\mathfrak{p} \cap A_n)$).
(b) Show that $\mathfrak{p}$ is a two-sided coideal of A.

Exercise 1.3.20. Let A be a connected graded $\mathbf{k}$-bialgebra. Show the following:

(a) The $\mathbf{k}$-submodule $\mathbf{k} = \mathbf{k} \cdot 1_A$ of A lies in A_0.
(b) The map u is an isomorphism $\mathbf{k} \xrightarrow{u} A_0$.
(c) We have $A_0 = \mathbf{k} \cdot 1_A$.
(d) The two-sided ideal $\ker \epsilon$ is the $\mathbf{k}$-module of positive degree elements $I = \bigoplus_{n > 0} A_n$.
(e) The map ϵ restricted to A_0 is the inverse isomorphism $A_0 \xrightarrow{\epsilon} \mathbf{k}$ to u.
(f) For every $x \in A$, we have

$$\Delta(x) \in x \otimes 1 + A \otimes I.$$

(g) Every x in I satisfies

$$\Delta(x) = 1 \otimes x + x \otimes 1 + \Delta_+(x), \qquad \text{where } \Delta_+(x) \text{ lies in } I \otimes I.$$

(h) Every $n > 0$ and every $x \in A_n$ satisfy

$$\Delta(x) = 1 \otimes x + x \otimes 1 + \Delta_+(x), \qquad \text{where } \Delta_+(x) \text{ lies in } \sum_{k=1}^{n-1} A_k \otimes A_{n-k}.$$

(Use only the gradedness of the unit u and counit ϵ maps, along with commutativity of diagrams (1.2.2), and (1.3.4) and the connectedness of A.)

Having discussed graded $\mathbf{k}$-modules, let us also define the concept of a *graded basis*, which is the analogue of the notion of a basis in the graded context. Roughly speaking, a graded basis of a graded $\mathbf{k}$-module is a basis that comprises bases of all its homogeneous components. More formally:

Definition 1.3.21. Let $V = \bigoplus_{n \geq 0} V_n$ be a graded $\mathbf{k}$-module. A *graded basis* of the graded $\mathbf{k}$-module V means a basis $\{v_i\}_{i \in I}$ of the $\mathbf{k}$-module V whose indexing set I is partitioned into subsets $I_0, I_1, I_2, \ldots$ (which are allowed to be empty) with the property that, for every $n \in \mathbb{N}$, the subfamily $\{v_i\}_{i \in I_n}$ is a basis of the $\mathbf{k}$-module V_n.

Example 1.3.22. Consider the polynomial ring $\mathbf{k}[x]$ in one variable x over $\mathbf{k}$. This is a graded $\mathbf{k}$-module (graded by the degree of a polynomial; thus, each x^n is homogeneous of degree n). Then, the family $(x^n)_{n \in \mathbb{N}} = \left(x^0, x^1, x^2, \ldots\right)$ is a graded basis of $\mathbf{k}[x]$ (presuming that its indexing set $\mathbb{N}$ is partitioned into the one-element subsets $\{0\}, \{1\}, \{2\}, \ldots$). The family $((-x)^n)_{n \in \mathbb{N}} = \left(x^0, -x^1, x^2, -x^3, \ldots\right)$ is a graded basis of $\mathbf{k}[x]$ as well. But the family $((1+x)^n)_{n \in \mathbb{N}}$ is not, since it contains non-homogeneous elements.

We end this section by discussing morphisms between bialgebras. They are defined as one would expect:

Definition 1.3.23. A *morphism of bialgebras* (also known as a $\mathbf{k}$-*bialgebra homomorphism*) is a $\mathbf{k}$-linear map $A \xrightarrow{\varphi} B$ between two $\mathbf{k}$-bialgebras A and B that is simultaneously a $\mathbf{k}$-algebra homomorphism and a $\mathbf{k}$-coalgebra homomorphism.

For example, any $\mathbf{k}$-linear map $f : V \to W$ between two $\mathbf{k}$-modules V and W induces a $\mathbf{k}$-linear map $T(f) : T(V) \to T(W)$ between their tensor algebras (which sends each $v_1 v_2 \cdots v_k \in T(V)$ to $f(v_1) f(v_2) \cdots f(v_k) \in T(W)$) as well as a $\mathbf{k}$-linear map $\operatorname{Sym}(f) : \operatorname{Sym}(V) \to \operatorname{Sym}(W)$ between their symmetric algebras; both of these maps $T(f)$ and $\operatorname{Sym}(f)$ are morphisms of bialgebras.

Graded bialgebras come with a special family of endomorphisms, as the following exercise shows:

Exercise 1.3.24. Fix $q \in \mathbf{k}$. Let $A = \bigoplus_{n \in \mathbb{N}} A_n$ be a graded $\mathbf{k}$-bialgebra (where the A_n are the homogeneous components of A). Let $D_q : A \to A$ be the $\mathbf{k}$-module endomorphism of A defined by setting

$$D_q(a) = q^n a \qquad \text{for each } n \in \mathbb{N} \text{ and each } a \in A_n.$$

(It is easy to see that this is well-defined; equivalently, D_q could be defined as the direct sum $\bigoplus_{n \in \mathbb{N}} (q^n \cdot \mathrm{id}_{A_n}) : \bigoplus_{n \in \mathbb{N}} A_n \to \bigoplus_{n \in \mathbb{N}} A_n$ of the maps $q^n \cdot \mathrm{id}_{A_n} : A_n \to A_n$.)

Prove that D_q is a $\mathbf{k}$-bialgebra homomorphism.

The tensor product of two bialgebras is canonically a bialgebra, as the following proposition shows:

Proposition 1.3.25. *Let A and B be two $\mathbf{k}$-bialgebras. Then, $A \otimes B$ is both a $\mathbf{k}$-algebra and a $\mathbf{k}$-coalgebra (by Definition 1.3.3). These two structures, combined, turn $A \otimes B$ into a $\mathbf{k}$-bialgebra.*

Exercise 1.3.26. (a) Prove Proposition 1.3.25.

(b) Let G and H be two groups. Show that the $\mathbf{k}$-bialgebra $\mathbf{k}G \otimes \mathbf{k}H$ (defined as in Proposition 1.3.25) is isomorphic to the $\mathbf{k}$-bialgebra $\mathbf{k}[G \times H]$. (The notation $\mathbf{k}[S]$ is a synonym for $\mathbf{k}S$.)

1.4. **Antipodes and Hopf algebras.** There is one more piece of structure needed to make a bialgebra a Hopf algebra, although it will come for free in the connected graded case.

Definition 1.4.1. For any coalgebra C and algebra A, one can endow the $\mathbf{k}$-module $\operatorname{Hom}(C, A)$ (which consists of all $\mathbf{k}$-linear maps from C to A) with an associative algebra structure called the *convolution*

algebra: Define the product $f \star g$ of two maps f, g in $\mathrm{Hom}(C, A)$ by $(f \star g)(c) = \sum f(c_1) g(c_2)$, using the Sweedler notation[21] $\Delta(c) = \sum c_1 \otimes c_2$. Equivalently, $f \star g$ is the composite

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{m} A \,.$$

The associativity of this multiplication $\star$ is easy to check (see Exercise 1.4.2 below).

The map $u \circ \epsilon$ is a two-sided identity element for $\star$, meaning that every $f \in \mathrm{Hom}(C, A)$ satisfies

$$\sum f(c_1)\epsilon(c_2) = f(c) = \sum \epsilon(c_1) f(c_2)$$

for all $c \in C$. One sees this by adding a top row to (1.2.2):

(1.4.1)
$$\begin{array}{ccccc}
A \otimes \mathbf{k} & \longrightarrow & A & \longleftarrow & \mathbf{k} \otimes A \\
{\scriptstyle f\otimes \mathrm{id}}\uparrow & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle \mathrm{id}\otimes f} \\
C \otimes \mathbf{k} & \longrightarrow & C & \longleftarrow & \mathbf{k} \otimes C \\
{\scriptstyle \mathrm{id}\otimes \epsilon}\uparrow & & \uparrow{\scriptstyle \mathrm{id}} & & \uparrow{\scriptstyle \epsilon\otimes \mathrm{id}} \\
C \otimes C & \xleftarrow[\Delta]{} & C & \xrightarrow[\Delta]{} & C \otimes C
\end{array}$$

In particular, when one has a bialgebra A, the convolution product $\star$ gives an associative algebra structure on $\mathrm{End}(A) := \mathrm{Hom}(A, A)$.

Exercise 1.4.2. Let C be a $\mathbf{k}$-coalgebra and A be a $\mathbf{k}$-algebra. Show that the binary operation $\star$ on $\mathrm{Hom}\,(C, A)$ is associative.

The product $f \star g$ of two elements f and g in a convolution algebra $\mathrm{Hom}(C, A)$ is often called their *convolution*.

The following simple (but useful) property of convolution algebras says essentially that the $\mathbf{k}$-algebra $(\mathrm{Hom}\,(C, A), \star)$ is a covariant functor in A and a contravariant functor in C, acting on morphisms by pre- and post-composition:

Proposition 1.4.3. *Let C and C' be two $\mathbf{k}$-coalgebras, and let A and A' be two $\mathbf{k}$-algebras. Let $\gamma : C \to C'$ be a $\mathbf{k}$-coalgebra morphism. Let $\alpha : A \to A'$ be a $\mathbf{k}$-algebra morphism.*

The map

$$\mathrm{Hom}\,(C', A) \to \mathrm{Hom}\,(C, A')\,, \qquad f \mapsto \alpha \circ f \circ \gamma$$

is a $\mathbf{k}$-algebra homomorphism from the convolution algebra $(\mathrm{Hom}\,(C', A), \star)$ to the convolution algebra $(\mathrm{Hom}\,(C, A'), \star)$.

Proof of Proposition 1.4.3. Denote this map by φ. We must show that φ is a $\mathbf{k}$-algebra homomorphism.

Recall that α is an algebra morphism; thus, $\alpha \circ m_A = m_{A'} \circ (\alpha \otimes \alpha)$ and $\alpha \circ u_A = u_{A'}$. Also, γ is a coalgebra morphism; thus, $\Delta_{C'} \circ \gamma = (\gamma \otimes \gamma) \circ \Delta_C$ and $\epsilon_{C'} \circ \gamma = \epsilon_C$.

Now, the definition of φ yields $\varphi(u_A \circ \epsilon_{C'}) = \underbrace{\alpha \circ u_A}_{=u_{A'}} \circ \underbrace{\epsilon_{C'} \circ \gamma}_{=\epsilon_C} = u_{A'} \circ \epsilon_C$; in other words, φ sends the unity of the algebra $(\mathrm{Hom}\,(C', A), \star)$ to the unity of the algebra $(\mathrm{Hom}\,(C, A'), \star)$.

[21] See the paragraph around (1.2.3) for the meaning of this notation.

Furthermore, every $f \in \operatorname{Hom}(C', A)$ and $g \in \operatorname{Hom}(C', A)$ satisfy

$$\begin{aligned}
\varphi(f \star g) &= \alpha \circ \underbrace{(f \star g)}_{=m_A \circ (f \otimes g) \circ \Delta_{C'}} \circ \gamma \\
&= \underbrace{\alpha \circ m_A}_{=m_{A'} \circ (\alpha \otimes \alpha)} \circ (f \otimes g) \circ \underbrace{\Delta_{C'} \circ \gamma}_{=(\gamma \otimes \gamma) \circ \Delta_C} \\
&= m_{A'} \circ \underbrace{(\alpha \otimes \alpha) \circ (f \otimes g) \circ (\gamma \otimes \gamma)}_{=(\alpha \circ f \circ \gamma) \otimes (\alpha \circ g \circ \gamma)} \circ \Delta_C \\
&= m_{A'} \circ ((\alpha \circ f \circ \gamma) \otimes (\alpha \circ g \circ \gamma)) \circ \Delta_C \\
&= \underbrace{(\alpha \circ f \circ \gamma)}_{=\varphi(f)} \star \underbrace{(\alpha \circ g \circ \gamma)}_{=\varphi(g)} = \varphi(f) \star \varphi(g). \qquad (1.4.2)
\end{aligned}$$

Thus, φ is a $\mathbf{k}$-algebra homomorphism (since φ is a $\mathbf{k}$-linear map and sends the unity of the algebra $(\operatorname{Hom}(C', A), \star)$ to the unity of the algebra $(\operatorname{Hom}(C, A'), \star)$). □

Exercise 1.4.4. Let C and D be two $\mathbf{k}$-coalgebras, and let A and B be two $\mathbf{k}$-algebras. Prove that:

(a) If $f : C \to A$, $f' : C \to A$, $g : D \to B$ and $g' : D \to B$ are four $\mathbf{k}$-linear maps, then
$$(f \otimes g) \star (f' \otimes g') = (f \star f') \otimes (g \star g')$$
in the convolution algebra $\operatorname{Hom}(C \otimes D, A \otimes B)$.

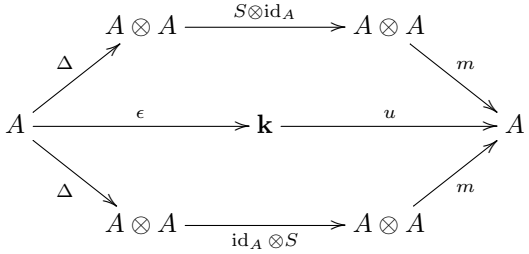
(b) Let R be the $\mathbf{k}$-linear map $(\operatorname{Hom}(C, A), \star) \otimes (\operatorname{Hom}(D, B), \star) \to (\operatorname{Hom}(C \otimes D, A \otimes B), \star)$ which sends every tensor $f \otimes g \in (\operatorname{Hom}(C, A), \star) \otimes (\operatorname{Hom}(D, B), \star)$ to the map $f \otimes g : C \otimes D \to A \otimes B$. (Notice that the tensor $f \otimes g$ and the map $f \otimes g$ are different things which happen to be written in the same way.) Then, R is a $\mathbf{k}$-algebra homomorphism.

Exercise 1.4.5. Let C and D be two $\mathbf{k}$-coalgebras. Let A be a $\mathbf{k}$-algebra. Let Φ be the canonical $\mathbf{k}$-module isomorphism $\operatorname{Hom}(C \otimes D, A) \to \operatorname{Hom}(C, \operatorname{Hom}(D, A))$ (defined by $((\Phi(f))(c))(d) = f(c \otimes d)$ for all $f \in \operatorname{Hom}(C \otimes D, A)$, $c \in C$ and $d \in D$). Prove that Φ is a $\mathbf{k}$-algebra isomorphism

$$(\operatorname{Hom}(C \otimes D, A), \star) \to (\operatorname{Hom}(C, (\operatorname{Hom}(D, A), \star)), \star).$$

Definition 1.4.6. A bialgebra A is called a *Hopf algebra* if there is an element S (called an *antipode* for A) in $\operatorname{End}(A)$ which is a 2-sided inverse under $\star$ for the identity map id_A. In other words, this diagram commutes:

(1.4.3)



Or equivalently, if we follow the Sweedler notation in writing $\Delta(a) = \sum a_1 \otimes a_2$, then

$$\sum_{(a)} S(a_1) a_2 = u(\epsilon(a)) = \sum_{(a)} a_1 S(a_2). \qquad (1.4.4)$$

Example 1.4.7. For a group algebra $\mathbf{k}G$, one can define an antipode $\mathbf{k}$-linearly via $S(t_g) = t_{g^{-1}}$. The top pentagon in the above diagram commutes because

$$(S \star \mathrm{id})(t_g) = m((S \otimes \mathrm{id})(t_g \otimes t_g)) = S(t_g) t_g = t_{g^{-1}} t_g = t_e = (u \circ \epsilon)(t_g).$$

Note that when it exists, the antipode S is unique, as with all 2-sided inverses in associative algebras: if S, S' are both 2-sided $\star$-inverses to id_A then

$$S' = (u \circ \epsilon) \star S' = (S \star \mathrm{id}_A) \star S' = S \star (\mathrm{id}_A \star S') = S \star (u \circ \epsilon) = S.$$

Thus, we can speak of "*the antipode*" of a Hopf algebra.

Unlike the comultiplication Δ, the antipode S of a Hopf algebra is not always an algebra homomorphism. It is instead an algebra *anti-homomorphism*, a notion we shall now introduce:

Definition 1.4.8. (a) For any two $\mathbf{k}$-modules U and V, we let $T_{U,V} : U \otimes V \to V \otimes U$ be the $\mathbf{k}$-linear map $U \otimes V \to V \otimes U$ sending every $u \otimes v$ to $v \otimes u$. This map $T_{U,V}$ is called the *twist map* for U and V.

(b) A $\mathbf{k}$-*algebra anti-homomorphism* means a $\mathbf{k}$-linear map $f : A \to B$ between two $\mathbf{k}$-algebras A and B which satisfies $f \circ m_A = m_B \circ (f \otimes f) \circ T_{A,A}$ and $f \circ u_A = u_B$.

(c) A $\mathbf{k}$-*coalgebra anti-homomorphism* means a $\mathbf{k}$-linear map $f : C \to D$ between two $\mathbf{k}$-coalgebras C and D which satisfies $\Delta_D \circ f = T_{D,D} \circ (f \otimes f) \circ \Delta_C$ and $\epsilon_D \circ f = \epsilon_C$.

(d) A $\mathbf{k}$-*algebra anti-endomorphism* of a $\mathbf{k}$-algebra A means a $\mathbf{k}$-algebra anti-homomorphism from A to A.

(e) A $\mathbf{k}$-*coalgebra anti-endomorphism* of a $\mathbf{k}$-coalgebra C means a $\mathbf{k}$-coalgebra anti-homomorphism from C to C.

Parts (b) and (c) of Definition 1.4.8 can be restated in terms of elements:

- A $\mathbf{k}$-linear map $f : A \to B$ between two $\mathbf{k}$-algebras A and B is a $\mathbf{k}$-algebra anti-homomorphism if and only if it satisfies $f(ab) = f(b) f(a)$ for all $a, b \in A$ as well as $f(1) = 1$.
- A $\mathbf{k}$-linear map $f : C \to D$ between two $\mathbf{k}$-coalgebras C and D is a $\mathbf{k}$-coalgebra anti-homomorphism if and only if it satisfies $\sum_{(f(c))} (f(c))_1 \otimes (f(c))_2 = \sum_{(c)} f(c_2) \otimes f(c_1)$ and $\epsilon(f(c)) = \epsilon(c)$ for all $c \in C$.

Example 1.4.9. Let $n \in \mathbb{N}$, and consider the $\mathbf{k}$-algebra $\mathbf{k}^{n \times n}$ of $n \times n$-matrices over $\mathbf{k}$. The map $\mathbf{k}^{n \times n} \to \mathbf{k}^{n \times n}$ that sends each matrix A to its transpose A^T is a $\mathbf{k}$-algebra anti-endomorphism of $\mathbf{k}^{n \times n}$.

We warn the reader that the composition of two $\mathbf{k}$-algebra anti-homomorphisms is not generally a $\mathbf{k}$-algebra anti-homomorphism again, but rather a $\mathbf{k}$-algebra homomorphism. The same applies to coalgebra anti-homomorphisms. Other than that, however, anti-homomorphisms share many of the helpful properties of homomorphisms. In particular, two $\mathbf{k}$-algebra anti-homomorphisms are identical if they agree on a generating set of their domain. Thus, the next proposition is useful when one wants to check that a certain map *is* the antipode in a particular Hopf algebra, by checking it on an algebra generating set.

Proposition 1.4.10. *The antipode S in a Hopf algebra A is an algebra anti-endomorphism: $S(1) = 1$, and $S(ab) = S(b)S(a)$ for all a, b in A.*

Proof. This is surprisingly nontrivial; the following argument comes from [213, proof of Proposition 4.0.1].

Since Δ is an algebra morphism, one has $\Delta(1) = 1 \otimes 1$, and therefore $1 = u\epsilon(1) = S(1) \cdot 1 = S(1)$.

To show $S(ab) = S(b)S(a)$, consider $A \otimes A$ as a coalgebra and A as an algebra. Then $\mathrm{Hom}(A \otimes A, A)$ is an associative algebra with a convolution product $\circledast$ (to be distinguished from the convolution $\star$ on $\mathrm{End}(A)$), having two-sided identity element $u_A \epsilon_{A \otimes A}$. We define three elements f, g, h of $\mathrm{Hom}(A \otimes A, A)$ by

$$\begin{aligned} f(a \otimes b) &= ab, \\ g(a \otimes b) &= S(b)S(a), \\ h(a \otimes b) &= S(ab). \end{aligned}$$

We will show that these three elements have the property that

$$h \circledast f = u_A \epsilon_{A \otimes A} = f \circledast g, \tag{1.4.5}$$

which would then show the desired equality $h = g$ via associativity:

$$h = h \circledast (u_A \epsilon_{A \otimes A}) = h \circledast (f \circledast g) = (h \circledast f) \circledast g = (u_A \epsilon_{A \otimes A}) \circledast g = g.$$

So we evaluate the three elements in (1.4.5) on $a \otimes b$. To do so, we use Sweedler notation – i.e., we assume $\Delta(a) = \sum_{(a)} a_1 \otimes a_2$ and $\Delta(b) = \sum_{(b)} b_1 \otimes b_2$, and hence $\Delta(ab) = \sum_{(a),(b)} a_1 b_1 \otimes a_2 b_2$ (by (1.3.6)); then,

$$(u_A \epsilon_{A\otimes A})(a \otimes b) = u_A(\epsilon_A(a)\epsilon_A(b)) = u_A(\epsilon_A(ab)).$$

$$\begin{aligned}(h \circledast f)(a \otimes b) &= \sum_{(a),(b)} h(a_1 \otimes b_1) f(a_2 \otimes b_2) \\ &= \sum_{(a),(b)} S(a_1 b_1) a_2 b_2 \\ &= (S \star \mathrm{id}_A)(ab) = u_A(\epsilon_A(ab)).\end{aligned}$$

$$\begin{aligned}(f \circledast g)(a \otimes b) &= \sum_{(a),(b)} f(a_1 \otimes b_1) g(a_2 \otimes b_2) \\ &= \sum_{(a),(b)} a_1 b_1 S(b_2) S(a_2) \\ &= \sum_{(a)} a_1 \cdot (\mathrm{id}_A \star S)(b) \cdot S(a_2) \\ &= u_A(\epsilon_A(b)) \sum_{(a)} a_1 S(a_2) = u_A(\epsilon_A(b)) u_A(\epsilon_A(a)) = u_A(\epsilon_A(ab)).\end{aligned}$$

These results are equal, so that (1.4.5) holds, and we conclude that $h = g$ as explained above. □

Remark 1.4.11. Recall from Remark 1.3.9 that the comultiplication on a bialgebra A allows one to define an A-module structure on the tensor product $M \otimes N$ of two A-modules M, N. Similarly, the anti-endomorphism S in a Hopf algebra allows one to turn *left* A-modules into *right* A-modules, or vice-versa.[22] E.g., left A-modules M naturally have a right A-module structure on the dual $\mathbf{k}$-module $M^* := \mathrm{Hom}(M, \mathbf{k})$, defined via $(fa)(m) := f(am)$ for f in M^* and a in A. The antipode S can be used to turn this back into a left A-module M^*, via $(af)(m) = f(S(a)m)$.

For groups G and left $\mathbf{k}G$-modules (group representations) M, this is how one defines the *contragredient action* of G on M^*, namely t_g acts as $(t_g f)(m) = f(t_{g^{-1}} m)$.

More generally, if A is a Hopf algebra and M and N are two left A-modules, then $\mathrm{Hom}\,(M, N)$ (the Hom here means $\mathrm{Hom}_{\mathbf{k}}$, not Hom_A) canonically becomes a left A-module by setting

$$(af)(m) = \sum_{(a)} a_1 f(S(a_2) m) \qquad \text{for all } a \in A,\ f \in \mathrm{Hom}\,(M, N) \text{ and } m \in M.$$

[23] When A is the group algebra $\mathbf{k}G$ of a group G, this leads to

$$(t_g f)(m) = t_g f\left(t_{g^{-1}} m\right) \qquad \text{for all } g \in G,\ f \in \mathrm{Hom}\,(M, N) \text{ and } m \in M.$$

This is precisely how one commonly makes $\mathrm{Hom}\,(M, N)$ a representation of G for two representations M and N.

---

[22] Be warned that these two transformations are not mutually inverse! Turning a left A-module into a right one and then again into a left one using the antipode might lead to a non-isomorphic A-module, unless the antipode S satisfies $S^2 = \mathrm{id}$.

[23] In more abstract terms, this A-module structure is given by the composition

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{\mathrm{id}_A \otimes S} A \otimes A^{\mathrm{op}} \longrightarrow \mathrm{End}\,(\mathrm{Hom}\,(M, N))\,,$$

where the last arrow is the morphism

$$\begin{aligned}A \otimes A^{\mathrm{op}} &\longrightarrow \mathrm{End}\,(\mathrm{Hom}\,(M, N))\,, \\ a \otimes b &\longmapsto (f \mapsto (M \to N,\ m \mapsto af(bm)))\,.\end{aligned}$$

Here, A^{op} denotes the *opposite algebra* of A, which is the $\mathbf{k}$-algebra differing from A only in the multiplication being twisted (the product of a and b in A^{op} is defined to be the product of b and a in A). As $\mathbf{k}$-modules, $A^{\mathrm{op}} = A$, but we prefer to use A^{op} instead of A here to ensure that all morphisms in the above composition are algebra morphisms.

Along the same lines, whenever A is a $\mathbf{k}$-bialgebra, we are supposed to think of the counit $A \xrightarrow{\epsilon} \mathbf{k}$ as giving a way to make $\mathbf{k}$ into a *trivial* A-module. This A-module $\mathbf{k}$ behaves as one would expect: the canonical isomorphisms $\mathbf{k} \otimes M \to M$, $M \otimes \mathbf{k} \to M$ and (if A is a Hopf algebra) $\operatorname{Hom}(M, \mathbf{k}) \to M^*$ are A-module isomorphisms for any A-module M.

Corollary 1.4.12. *Let A be a commutative Hopf algebra. Then, its antipode is an involution: $S^2 = \mathrm{id}_A$.*

Proof. One checks that $S^2 = S \circ S$ is a right $\star$-inverse to S, as follows:

$$\begin{aligned}
(S \star S^2)(a) &= \sum_{(a)} S(a_1) S^2(a_2) \\
&= S\left(\sum_{(a)} S(a_2) a_1 \right) \qquad \text{(by Proposition 1.4.10)} \\
&= S\left(\sum_{(a)} a_1 S(a_2) \right) \qquad \text{(by commutativity of } A\text{)} \\
&= S\left(u(\epsilon(a)) \right) \\
&= u(\epsilon(a)) \qquad \text{(since } S(1) = 1 \text{ by Proposition 1.4.10)}.
\end{aligned}$$

Since S itself is the $\star$-inverse to id_A, this shows that $S^2 = \mathrm{id}_A$. □

Remark 1.4.13. We won't need it, but it is easy to adapt the above proof to show that $S^2 = \mathrm{id}_A$ also holds for *cocommutative* Hopf algebras (the dual notion to commutativity; see Definition 1.5.2 below for the precise definition); see [157, Corollary 1.5.12] or [213, Proposition 4.0.1 6)] or Exercise 1.5.13 below. For a general Hopf algebra which is not finite-dimensional over a field $\mathbf{k}$, the antipode S may not even have finite order, even in the connected graded setting. E.g., Aguiar and Sottile [7] show that the Malvenuto-Reutenauer Hopf algebra of permutations has antipode of infinite order. In general, antipodes need not even be invertible [214].

Proposition 1.4.14. *Let A and B be two Hopf algebras. Then, the $\mathbf{k}$-bialgebra $A \otimes B$ (defined as in Proposition 1.3.25) is a Hopf algebra. The antipode of this Hopf algebra $A \otimes B$ is the map $S_A \otimes S_B : A \otimes B \to A \otimes B$, where S_A and S_B are the antipodes of the Hopf algebras A and B.*

Exercise 1.4.15. Prove Proposition 1.4.14.

In our frequent setting of connected graded bialgebras, antipodes come for free.

Proposition 1.4.16. *A connected graded bialgebra A has a unique antipode S, which is a graded map $A \xrightarrow{S} A$, endowing it with a Hopf structure.*

Proof. Let us try to define a ($\mathbf{k}$-linear) left $\star$-inverse S to id_A on each homogeneous component A_n, via induction on n.

In the base case $n = 0$, Proposition 1.4.10 and its proof show that one must define $S(1) = 1$ so S is the identity on $A_0 = \mathbf{k}$.

In the inductive step, recall from Exercise 1.3.20(h) that a homogeneous element a of degree $n > 0$ has $\Delta(a) = a \otimes 1 + \sum a'_1 \otimes a'_2$, with each $\deg(a'_1) < n$. (Here $\sum a'_1 \otimes a'_2$ stands for a sum of tensors $a'_{1,k} \otimes a'_{2,k}$, with each $a'_{1,k}$ being homogeneous of degree $\deg(a'_{1,k}) < n$. This is a slight variation on Sweedler notation.) Hence in order to have $S \star \mathrm{id}_A = u\epsilon$, one must define $S(a)$ in such a way that $S(a) \cdot 1 + \sum S(a'_1) a'_2 = u\epsilon(a) = 0$ and hence $S(a) := -\sum S(a'_1) a'_2$, where $S(a'_1)$ have already been uniquely defined by induction (since $\deg(a'_{1,k}) < n$). This does indeed define such a left $\star$-inverse S to id_A, by induction. It is also a graded map by induction.

The same argument shows how to define a right $\star$-inverse S' to id_A. Then $S = S'$ is a two-sided $\star$-inverse to id_A by the associativity of $\star$. □

Here is another consequence of the fact that $S(1) = 1$.

Proposition 1.4.17. *In bialgebras, primitive elements x have $\epsilon(x) = 0$, and in Hopf algebras, they have $S(x) = -x$.*

Proof. In a bialgebra, $\epsilon(1) = 1$. Hence $\Delta(x) = 1 \otimes x + x \otimes 1$ implies via (1.2.2) that $1 \cdot \epsilon(x) + \epsilon(1)x = x$, so $\epsilon(x) = 0$. It also implies via (1.4.3) that $S(x)1 + S(1)x = u\epsilon(x) = u(0) = 0$, so $S(x) = -x$. □

Thus, whenever A is a Hopf algebra generated as an algebra by its primitive elements, S is its unique $\mathbf{k}$-algebra anti-endomorphism that negates all primitive elements.

Example 1.4.18. The tensor and symmetric algebras $T(V)$ and $\mathrm{Sym}(V)$ are each generated by V, and each element of V is primitive when regarded as an element of either of them. Hence one has in $T(V)$ that

$$S(x_{i_1}x_{i_2}\cdots x_{i_k}) = (-x_{i_k})\cdots(-x_{i_2})(-x_{i_1}) = (-1)^k x_{i_k}\cdots x_{i_2}x_{i_1} \tag{1.4.6}$$

for each word $(i_1, \ldots, i_k)$ in the alphabet I if V is a free $\mathbf{k}$-module with basis $\{x_i\}_{i\in I}$. The same holds in $\mathrm{Sym}(V)$ for each multiset $\{i_1, \ldots, i_k\}_{\text{multiset}}$, recalling that the monomials are now commutative. In other words, for a commutative polynomial $f(x_1, x_2, \ldots, x_n)$ in $\mathrm{Sym}(V)$, the antipode S sends $f(x_1, x_2, \ldots, x_n)$ to $f(-x_1, -x_2, \ldots, -x_n)$, negating all the variables.

The antipode for a connected graded Hopf algebra has an interesting formula due to Takeuchi [214], reminiscent of P. Hall's formula for the Möbius function of a poset[24]. For the sake of stating this, consider (for every $k \in \mathbb{N}$) the k-fold *tensor power* $A^{\otimes k} = A \otimes \cdots \otimes A$ (defined in Example 1.1.2) and define *iterated multiplication and comultiplication* maps

$$A^{\otimes k} \xrightarrow{m^{(k-1)}} A \qquad \text{and} \qquad A \xrightarrow{\Delta^{(k-1)}} A^{\otimes k}$$

by induction over k, setting $m^{(-1)} = u$, $\Delta^{(-1)} = \epsilon$, $m^{(0)} = \Delta^{(0)} = \mathrm{id}_A$, and

$$\begin{aligned} m^{(k)} &= m \circ (\mathrm{id}_A \otimes m^{(k-1)}) && \text{for every } k \geq 1; \\ \Delta^{(k)} &= (\mathrm{id}_A \otimes \Delta^{(k-1)}) \circ \Delta && \text{for every } k \geq 1. \end{aligned}$$

Using associativity and coassociativity, one can see that for $k \geq 1$ these maps also satisfy

$$\begin{aligned} m^{(k)} &= m \circ (m^{(k-1)} \otimes \mathrm{id}_A) && \text{for every } k \geq 1; \\ \Delta^{(k)} &= (\Delta^{(k-1)} \otimes \mathrm{id}_A) \circ \Delta && \text{for every } k \geq 1 \end{aligned}$$

(so we could just as well have used $\mathrm{id}_A \otimes m^{(k-1)}$ instead of $m^{(k-1)} \otimes \mathrm{id}_A$ in defining them) and further symmetry properties (see Exercise 1.4.19 and Exercise 1.4.20). They are how one gives meaning to the right sides of these equations:

$$m^{(k)}(a^{(1)} \otimes \cdots \otimes a^{(k+1)}) = a^{(1)} \cdots a^{(k+1)};$$

$$\Delta^{(k)}(b) = \sum b_1 \otimes \cdots \otimes b_{k+1} \text{ in Sweedler notation.}$$

Exercise 1.4.19. Let A be a $\mathbf{k}$-algebra. Let us define, for every $k \in \mathbb{N}$, a $\mathbf{k}$-linear map $m^{(k)} : A^{\otimes(k+1)} \to A$. Namely, we define these maps by induction over k, with the induction base $m^{(0)} = \mathrm{id}_A$, and with the induction step $m^{(k)} = m \circ \left(\mathrm{id}_A \otimes m^{(k-1)}\right)$ for every $k \geq 1$. (This generalizes our definition of $m^{(k)}$ for Hopf algebras A given above, except for $m^{(-1)}$ which we have omitted.)

(a) Show that $m^{(k)} = m \circ \left(m^{(i)} \otimes m^{(k-1-i)}\right)$ for every $k \geq 0$ and $0 \leq i \leq k-1$.
(b) Show that $m^{(k)} = m \circ \left(m^{(k-1)} \otimes \mathrm{id}_A\right)$ for every $k \geq 1$.
(c) Show that $m^{(k)} = m^{(k-1)} \circ \left(\mathrm{id}_{A^{\otimes i}} \otimes m \otimes \mathrm{id}_{A^{\otimes(k-1-i)}}\right)$ for every $k \geq 0$ and $0 \leq i \leq k-1$.
(d) Show that $m^{(k)} = m^{(k-1)} \circ \left(\mathrm{id}_{A^{\otimes(k-1)}} \otimes m\right) = m^{(k-1)} \circ \left(m \otimes \mathrm{id}_{A^{\otimes(k-1)}}\right)$ for every $k \geq 1$.

Exercise 1.4.20. Let C be a $\mathbf{k}$-coalgebra. Let us define, for every $k \in \mathbb{N}$, a $\mathbf{k}$-linear map $\Delta^{(k)} : C \to C^{\otimes(k+1)}$. Namely, we define these maps by induction over k, with the induction base $\Delta^{(0)} = \mathrm{id}_C$, and with the induction step $\Delta^{(k)} = \left(\mathrm{id}_C \otimes \Delta^{(k-1)}\right) \circ \Delta$ for every $k \geq 1$. (This generalizes our definition of $\Delta^{(k)}$ for Hopf algebras A given above, except for $\Delta^{(-1)}$ which we have omitted.)

(a) Show that $\Delta^{(k)} = \left(\Delta^{(i)} \otimes \Delta^{(k-1-i)}\right) \circ \Delta$ for every $k \geq 0$ and $0 \leq i \leq k-1$.
(b) Show that $\Delta^{(k)} = \left(\Delta^{(k-1)} \otimes \mathrm{id}_C\right) \circ \Delta$ for every $k \geq 1$.
(c) Show that $\Delta^{(k)} = (\mathrm{id}_{C^{\otimes i}} \otimes \Delta \otimes \mathrm{id}_{C^{\otimes(k-1-i)}}) \circ \Delta^{(k-1)}$ for every $k \geq 0$ and $0 \leq i \leq k-1$.
(d) Show that $\Delta^{(k)} = (\mathrm{id}_{C^{\otimes(k-1)}} \otimes \Delta) \circ \Delta^{(k-1)} = (\Delta \otimes \mathrm{id}_{C^{\otimes(k-1)}}) \circ \Delta^{(k-1)}$ for every $k \geq 1$.

[24] In fact, for incidence Hopf algebras, Takeuchi's formula generalizes Hall's formula– see Corollary 7.2.3.

Remark 1.4.21. Exercise 1.4.19 holds more generally for nonunital associative algebras A (that is, $\mathbf{k}$-modules A equipped with a $\mathbf{k}$-linear map $m : A \otimes A \to A$ such that the diagram (1.1.1) is commutative, but not necessarily admitting a unit map u). Similarly, Exercise 1.4.20 holds for non-counital coassociative coalgebras C. The existence of a unit in A, respectively a counit in C, allows slightly extending these two exercises by additionally introducing maps $m^{(-1)} = u : \mathbf{k} \to A$ and $\Delta^{(-1)} = \epsilon : C \to \mathbf{k}$; however, not much is gained from this extension.[25]

Exercise 1.4.22. For every $k \in \mathbb{N}$ and every $\mathbf{k}$-bialgebra H, consider the map $\Delta_H^{(k)} : H \to H^{\otimes(k+1)}$ (this is the map $\Delta^{(k)}$ defined as in Exercise 1.4.20 for $C = H$), and the map $m_H^{(k)} : H^{\otimes(k+1)} \to H$ (this is the map $m^{(k)}$ defined as in Exercise 1.4.19 for $A = H$).

Let H be a $\mathbf{k}$-bialgebra. Let $k \in \mathbb{N}$. Show that:[26]

(a) The map $m_H^{(k)} : H^{\otimes(k+1)} \to H$ is a $\mathbf{k}$-coalgebra homomorphism.

(b) The map $\Delta_H^{(k)} : H \to H^{\otimes(k+1)}$ is a $\mathbf{k}$-algebra homomorphism.

(c) We have $m_{H^{\otimes(k+1)}}^{(\ell)} \circ \left(\Delta_H^{(k)}\right)^{\otimes(\ell+1)} = \Delta_H^{(k)} \circ m_H^{(\ell)}$ for every $\ell \in \mathbb{N}$.

(d) We have $\left(m_H^{(\ell)}\right)^{\otimes(k+1)} \circ \Delta_{H^{\otimes(\ell+1)}}^{(k)} = \Delta_H^{(k)} \circ m_H^{(\ell)}$ for every $\ell \in \mathbb{N}$.

The iterated multiplication and comultiplication maps allow explicitly computing the convolution of multiple maps; the following formula will often be used without explicit mention:

Exercise 1.4.23. Let C be a $\mathbf{k}$-coalgebra, and A be a $\mathbf{k}$-algebra. Let $k \in \mathbb{N}$. Let $f_1, f_2, \ldots, f_k$ be k elements of $\mathrm{Hom}(C, A)$. Show that

$$f_1 \star f_2 \star \cdots \star f_k = m_A^{(k-1)} \circ (f_1 \otimes f_2 \otimes \cdots \otimes f_k) \circ \Delta_C^{(k-1)}.$$

We are now ready to state Takeuchi's formula for the antipode:

Proposition 1.4.24. *In a connected graded Hopf algebra A, the antipode has formula*

$$\begin{aligned} S &= \sum_{k \geq 0} (-1)^k m^{(k-1)} f^{\otimes k} \Delta^{(k-1)} \\ &= u\epsilon - f + m \circ f^{\otimes 2} \circ \Delta - m^{(2)} \circ f^{\otimes 3} \circ \Delta^{(2)} + \cdots \end{aligned} \tag{1.4.7}$$

where $f := \mathrm{id}_A - u\epsilon$ in $\mathrm{End}(A)$.

Proof. We argue as in [214, proof of Lemma 14] or [7, §5]. For any f in $\mathrm{End}(A)$, the following explicit formula expresses its k-fold convolution power $f^{\star k} := f \star \cdots \star f$ in terms of its tensor powers $f^{\otimes k} := f \otimes \cdots \otimes f$ (according to Exercise 1.4.23):

$$f^{\star k} = m^{(k-1)} \circ f^{\otimes k} \circ \Delta^{(k-1)}.$$

Therefore any f annihilating A_0 will be *locally $\star$-nilpotent* on A, meaning that for each n one has that A_n is annihilated by $f^{\star m}$ for every $m > n$: homogeneity forces that for a in A_n, every summand of $\Delta^{(m-1)}(a)$ must contain among its m tensor factors at least one factor lying in A_0, so each summand is annihilated by $f^{\otimes m}$, and $f^{\star m}(a) = 0$.

In particular such f have the property that $u\epsilon + f$ has as two-sided $\star$-inverse

$$\begin{aligned} (u\epsilon + f)^{\star(-1)} &= u\epsilon - f + f \star f - f \star f \star f + \cdots \\ &= \sum_{k \geq 0} (-1)^k f^{\star k} = \sum_{k \geq 0} (-1)^k m^{(k-1)} \circ f^{\otimes k} \circ \Delta^{(k-1)}. \end{aligned}$$

The proposition follows upon taking $f := \mathrm{id}_A - u\epsilon$, which annihilates A_0. □

Remark 1.4.25. In fact, one can see that Takeuchi's formula applies more generally to define an antipode $A \xrightarrow{S} A$ in any (not necessarily graded) bialgebra A where the map $\mathrm{id}_A - u\epsilon$ is locally $\star$-nilpotent.

It is also worth noting that the proof of Proposition 1.4.24 gives an alternate proof of Proposition 1.4.16.

[25] The identity $m^{(k)} = m \circ \left(\mathrm{id}_A \otimes m^{(k-1)}\right)$ for a $\mathbf{k}$-algebra A still holds when $k = 0$ if it is interpreted in the right way (viz., if A is identified with $A \otimes \mathbf{k}$ using the canonical homomorphism).

[26] The following statements are taken from [167]; specifically, part (c) is [167, Lem. 1.8].

To finish our discussion of antipodes, we mention some properties (taken from [213, Lemma 4.0.3]) relating antipodes to convolutional inverses.

Proposition 1.4.26. *Let H be a Hopf algebra with antipode S.*

(a) *For any algebra A and algebra morphism $H \xrightarrow{\alpha} A$, one has $\alpha \circ S = \alpha^{\star -1}$, the convolutional inverse to α in* $\mathrm{Hom}(H, A)$.

(b) *For any coalgebra C and coalgebra morphism $C \xrightarrow{\gamma} H$, one has $S \circ \gamma = \gamma^{\star -1}$, the convolutional inverse to γ in* $\mathrm{Hom}(C, H)$.

Proof. We prove (a); the proof of (b) is similar.

For assertion (a), note that Proposition 1.4.3 (applied to H, H, H, A, id_H and α instead of C, C', A, A', γ and α) shows that the map

$$\mathrm{Hom}\left(H, H\right) \to \mathrm{Hom}\left(H, A\right), \qquad f \mapsto \alpha \circ f$$

is a $\mathbf{k}$-algebra homomorphism from the convolution algebra $\left(\mathrm{Hom}\left(H, H\right), \star\right)$ to the convolution algebra $\left(\mathrm{Hom}\left(H, A\right), \star\right)$. Denoting this homomorphism by φ, we thus have $\varphi\left(\left(\mathrm{id}_H\right)^{\star -1}\right) = \left(\varphi(\mathrm{id}_H)\right)^{\star -1}$ (since $\mathbf{k}$-algebra homomorphisms preserve inverses). Now,

$$\alpha \circ S = \varphi(S) = \varphi\left(\left(\mathrm{id}_H\right)^{\star -1}\right) = \left(\varphi(\mathrm{id}_H)\right)^{\star -1} = \left(\alpha \circ \mathrm{id}_H\right)^{\star -1} = \alpha^{\star -1}.$$

□

A rather useful consequence of Proposition 1.4.26 is the fact ([213, Lemma 4.0.4]) that a bialgebra morphism between Hopf algebras automatically respects the antipodes:

Corollary 1.4.27. *Let H_1 and H_2 be Hopf algebras with antipodes S_1 and S_2, respectively. Then, any bialgebra morphism $H_1 \xrightarrow{\beta} H_2$ is a Hopf morphism*[27]*, that is, it commutes with the antipodes (i.e., we have $\beta \circ S_1 = S_2 \circ \beta$).*

Proof. Proposition 1.4.26(a) (applied to $H = H_1$, $S = S_1$, $A = H_2$ and $\alpha = \beta$) yields $\beta \circ S_1 = \beta^{\star -1}$. Proposition 1.4.26(b) (applied to $H = H_2$, $S = S_2$, $C = H_1$ and $\gamma = \beta$) yields $S_2 \circ \beta = \beta^{\star -1}$. Comparing these equalities shows that $\beta \circ S_1 = S_2 \circ \beta$, qed. □

Exercise 1.4.28. Prove that the antipode S of a Hopf algebra A is a coalgebra anti-endomorphism, i.e., that it satisfies $\epsilon \circ S = \epsilon$ and $\Delta \circ S = T \circ (S \otimes S) \circ \Delta$, where $T : A \otimes A \to A \otimes A$ is the twist map sending every $a \otimes b$ to $b \otimes a$.

Exercise 1.4.29. If C is a $\mathbf{k}$-coalgebra and if A is a $\mathbf{k}$-algebra, then a $\mathbf{k}$-linear map $f : C \to A$ is said to be *$\star$-invertible* if it is invertible as an element of the $\mathbf{k}$-algebra $\left(\mathrm{Hom}\left(C, A\right), \star\right)$. In this case, the multiplicative inverse $f^{\star(-1)}$ of f in $\left(\mathrm{Hom}\left(C, A\right), \star\right)$ is called the *$\star$-inverse* of f.

Recall the concepts introduced in Definition 1.4.8.

(a) If C is a $\mathbf{k}$-bialgebra, if A is a $\mathbf{k}$-algebra, and if $r : C \to A$ is a $\star$-invertible $\mathbf{k}$-algebra homomorphism, then prove that the $\star$-inverse $r^{\star(-1)}$ of r is a $\mathbf{k}$-algebra anti-homomorphism.

(b) If C is a $\mathbf{k}$-bialgebra, if A is a $\mathbf{k}$-coalgebra, and if $r : A \to C$ is a $\star$-invertible $\mathbf{k}$-coalgebra homomorphism, then prove that the $\star$-inverse $r^{\star(-1)}$ of r is a $\mathbf{k}$-coalgebra anti-homomorphism.

(c) Derive Proposition 1.4.10 from Exercise 1.4.29(a), and derive Exercise 1.4.28 from Exercise 1.4.29(b).

(d) Prove Corollary 1.4.12 again using Proposition 1.4.26.

(e) If C is a graded $\mathbf{k}$-coalgebra, if A is a graded $\mathbf{k}$-algebra, and if $r : C \to A$ is a $\star$-invertible $\mathbf{k}$-linear map that is graded, then prove that the $\star$-inverse $r^{\star(-1)}$ of r is also graded.

Exercise 1.4.30. (a) Let A be a Hopf algebra. If $P : A \to A$ is a $\mathbf{k}$-linear map such that every $a \in A$ satisfies

$$\sum_{(a)} P\left(a_2\right) \cdot a_1 = u\left(\epsilon\left(a\right)\right),$$

then prove that the antipode S of A is invertible and its inverse is P.

[27] A *Hopf morphism* (or, more officially, a *Hopf algebra morphism*, or *homomorphism of Hopf algebras*) between two Hopf algebras A and B is defined to be a bialgebra morphism $f : A \to B$ that satisfies $f \circ S_A = S_B \circ f$.

(b) Let A be a Hopf algebra. If $P : A \to A$ is a $\mathbf{k}$-linear map such that every $a \in A$ satisfies

$$\sum_{(a)} a_2 \cdot P(a_1) = u(\epsilon(a)),$$

then prove that the antipode S of A is invertible and its inverse is P.

(c) Show that the antipode of a connected graded Hopf algebra is invertible.

(Compare this exercise to [157, Lemma 1.5.11].)

Definition 1.4.31. Let C be a $\mathbf{k}$-coalgebra. A *subcoalgebra* of C means a $\mathbf{k}$-coalgebra D such that $D \subset C$ and such that the canonical inclusion map $D \to C$ is a $\mathbf{k}$-coalgebra homomorphism[28]. When $\mathbf{k}$ is a field, we can equivalently define a subcoalgebra of C as a $\mathbf{k}$-submodule D of C such that $\Delta_C(D)$ is a subset of the $\mathbf{k}$-submodule $D \otimes D$ of $C \otimes C$; however, this might no longer be equivalent when $\mathbf{k}$ is not a field[29].

Similarly, a *subbialgebra* of a bialgebra C is a $\mathbf{k}$-bialgebra D such that $D \subset C$ and such that the canonical inclusion map $D \to C$ is a $\mathbf{k}$-bialgebra homomorphism. Also, a *Hopf subalgebra* of a Hopf algebra C is a $\mathbf{k}$-Hopf algebra D such that $D \subset C$ and such that the canonical inclusion map $D \to C$ is a $\mathbf{k}$-Hopf algebra homomorphism.[30]

Exercise 1.4.32. Let C be a $\mathbf{k}$-coalgebra. Let D be a $\mathbf{k}$-submodule of C such that D is a direct summand of C as a $\mathbf{k}$-module (i.e., there exists a $\mathbf{k}$-submodule E of C such that $C = D \oplus E$). (This is automatically satisfied if $\mathbf{k}$ is a field.) Assume that $\Delta(D) \subset C \otimes D$ and $\Delta(D) \subset D \otimes C$. (Here, we are abusing the notation $C \otimes D$ to denote the $\mathbf{k}$-submodule of $C \otimes C$ spanned by tensors of the form $c \otimes d$ with $c \in C$ and $d \in D$; similarly, $D \otimes C$ should be understood.) Show that there is a canonically defined $\mathbf{k}$-coalgebra structure on D which makes D a subcoalgebra of C.

The next exercise is implicit in [4, §5]:

Exercise 1.4.33. Let $\mathbf{k}$ be a field. Let C be a $\mathbf{k}$-coalgebra, and let U be any $\mathbf{k}$-module. Let $f : C \to U$ be a $\mathbf{k}$-linear map. Recall the map $\Delta^{(2)} : C \to C^{\otimes 3}$ from Exercise 1.4.20. Let $K = \ker\left((\mathrm{id}_C \otimes f \otimes \mathrm{id}_C) \circ \Delta^{(2)}\right)$.

(a) Show that K is a $\mathbf{k}$-subcoalgebra of C.

(b) Show that every $\mathbf{k}$-subcoalgebra of C which is a subset of $\ker f$ must be a subset of K.

Exercise 1.4.34. (a) Let $C = \bigoplus_{n \geq 0} C_n$ be a graded $\mathbf{k}$-coalgebra, and A be any $\mathbf{k}$-algebra. Notice that C_0 itself is a $\mathbf{k}$-subcoalgebra of C. Let $h : C \to A$ be a $\mathbf{k}$-linear map such that the restriction $h\mid_{C_0}$ is a $\star$-invertible map in $\mathrm{Hom}(C_0, A)$. Prove that h is a $\star$-invertible map in $\mathrm{Hom}(C, A)$. (This is a weaker version of Takeuchi's [214, Lemma 14].)

(b) Let $A = \bigoplus_{n \geq 0} A_n$ be a graded $\mathbf{k}$-bialgebra. Notice that A_0 is a subbialgebra of A. Assume that A_0 is a Hopf algebra. Show that A is a Hopf algebra.

(c) Obtain yet another proof of Proposition 1.4.16.

Exercise 1.4.35. Let $A = \bigoplus_{n \geq 0} A_n$ be a connected graded $\mathbf{k}$-bialgebra. Let $\mathfrak{p}$ be the $\mathbf{k}$-submodule of A consisting of the primitive elements of A.

(a) If I is a two-sided coideal of A such that $I \cap \mathfrak{p} = 0$ and such that $I = \bigoplus_{n \geq 0} (I \cap A_n)$, then prove that $I = 0$.

(b) Let $f : A \to C$ be a graded surjective coalgebra homomorphism from A to a graded $\mathbf{k}$-coalgebra C. If $f\mid_{\mathfrak{p}}$ is injective, then prove that f is injective.

(c) Assume that $\mathbf{k}$ is a field. Show that the claim of Exercise 1.4.35(b) is valid even without requiring f to be surjective.

Remark 1.4.36. Exercise 1.4.35 (b) and (c) are often used in order to prove that certain coalgebra homomorphisms are injective.

The word "bialgebra" can be replaced by "coalgebra" in Exercise 1.4.35, provided that the notion of a connected graded coalgebra is defined correctly (namely, as a graded coalgebra such that the restriction of

[28] In this definition, we follow [162, p. 55] and [225, §6.7]; other authors may use other definitions.

[29] This is because the $\mathbf{k}$-submodule $D \otimes D$ of $C \otimes C$ is generally not isomorphic to the $\mathbf{k}$-module $D \otimes D$. See [162, p. 56] for specific counterexamples for the non-equivalence of the two notions of a subcoalgebra. Notice that the equivalence is salvaged if D is a direct summand of C as a $\mathbf{k}$-module (see Exercise 1.4.32 for this).

[30] By Corollary 1.4.27, we can also define it as a subbialgebra of C that happens to be a Hopf algebra.

ϵ to the 0-th graded component is an isomorphism), and the notion of the element 1 of a connected graded coalgebra is defined accordingly (namely, as the preimage of $1 \in \mathbf{k}$ under the restriction of ϵ to the 0-th graded component).

1.5. **Commutativity, cocommutativity.** Recall that a $\mathbf{k}$-algebra A is *commutative* if and only if all $a, b \in A$ satisfy $ab = ba$. Here is a way to restate this classical definition using tensors instead of pairs of elements:

Definition 1.5.1. A $\mathbf{k}$-algebra A is said to be *commutative* if the following diagram commutes:

(1.5.1)
$$\begin{array}{ccc} A \otimes A & \xrightarrow{T} & A \otimes A \\ & {\scriptstyle m} \searrow \quad \swarrow {\scriptstyle m} & \\ & A & \end{array}$$

where T is the twist map $T_{A,A}$ (see Definition 1.4.8(a) for its definition).

Having thus redefined commutative algebras in terms of tensors and linear maps, we can dualize this definition (reversing all arrows) and obtain the notion of *cocommutative coalgebras*:

Definition 1.5.2. A $\mathbf{k}$-coalgebra C is said to be *cocommutative* if the following diagram commutes:

(1.5.2)
$$\begin{array}{ccc} C \otimes C & \xrightarrow{T} & C \otimes C \\ & {\scriptstyle \Delta} \nwarrow \quad \nearrow {\scriptstyle \Delta} & \\ & C & \end{array}$$

where T is the twist map $T_{C,C}$ (see Definition 1.4.8(a) for its definition).

Example 1.5.3. Group algebras $\mathbf{k}G$ are always cocommutative. They are commutative if and only if G is abelian or $\mathbf{k} = 0$.

Tensor algebras $T(V)$ are always cocommutative, but not generally commutative[31].

Symmetric algebras $\mathrm{Sym}(V)$ are always cocommutative and commutative.

Homology and cohomology of H-spaces are always cocommutative and commutative *in the topologist's sense* where one reinterprets that twist map $A \otimes A \xrightarrow{T} A \otimes A$ to have the extra sign as in (1.3.3).

Note how the cocommutative Hopf algebras $T(V), \mathrm{Sym}(V)$ have much of their structure controlled by their $\mathbf{k}$-submodules V, which consist of primitive elements only (although, in general, not of all their primitive elements). This is not far from the truth in general, and closely related to Lie algebras.

Exercise 1.5.4. Recall that a *Lie algebra* over $\mathbf{k}$ is a $\mathbf{k}$-module $\mathfrak{g}$ with a $\mathbf{k}$-bilinear map $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that satisfies $[x, x] = 0$ for x in $\mathfrak{g}$, and the *Jacobi identity*

$$[x,[y,z]] = [[x,y],z] + [y,[x,z]], \text{ or equivalently}$$
$$[x,[y,z]] + [z,[x,y]] + [y,[z,x]] = 0$$

for all $x, y, z \in \mathfrak{g}$. This $\mathbf{k}$-bilinear map $[\cdot,\cdot]$ is called the *Lie bracket* of $\mathfrak{g}$.

(a) Check that any associative algebra A gives rise to a Lie algebra by means of the commutator operation $[a, b] := ab - ba$.

(b) If A is also a bialgebra, show that the $\mathbf{k}$-submodule of primitive elements $\mathfrak{p} \subset A$ is closed under the Lie bracket, that is, $[\mathfrak{p}, \mathfrak{p}] \subset \mathfrak{p}$, and hence forms a Lie subalgebra.

Conversely, given a Lie algebra $\mathfrak{p}$, one constructs the *universal enveloping algebra* $\mathcal{U}(\mathfrak{p}) := T(\mathfrak{p})/J$ as the quotient of the tensor algebra $T(\mathfrak{p})$ by the two-sided ideal J generated by all elements $xy - yx - [x, y]$ for x, y in $\mathfrak{p}$.

(c) Show that J is also a two-sided coideal in $T(\mathfrak{p})$ for its usual coalgebra structure, and hence the quotient $\mathcal{U}(\mathfrak{p})$ inherits the structure of a cocommutative bialgebra.

(d) Show that the antipode S on $T(\mathfrak{p})$ preserves J, meaning that $S(J) \subset J$, and hence $\mathcal{U}(\mathfrak{p})$ inherits the structure of a (cocommutative) Hopf algebra.

[31] If $\mathbf{k}$ is a field, then $T(V)$ is commutative if and only if $\dim_{\mathbf{k}} V \leq 1$.

There are theorems, discussed in [35, §3.8], [157, Chap. 5], [60, §3.2] giving various mild hypotheses in addition to cocommutativity which imply that the inclusion of the $\mathbf{k}$-module $\mathfrak{p}$ of primitives in a Hopf algebra A extends to a Hopf isomorphism $\mathcal{U}(\mathfrak{p}) \cong A$.

Exercise 1.5.5. Let C be a cocommutative $\mathbf{k}$-coalgebra. Let A be a commutative $\mathbf{k}$-algebra. Show that the convolution algebra $(\mathrm{Hom}(C, A), \star)$ is commutative (i.e., every $f, g \in \mathrm{Hom}(C, A)$ satisfy $f \star g = g \star f$).

Exercise 1.5.6. (a) Let C be a $\mathbf{k}$-coalgebra. Show that C is cocommutative if and only if its comultiplication $\Delta_C : C \to C \otimes C$ is a $\mathbf{k}$-coalgebra homomorphism.

(b) Let A be a $\mathbf{k}$-algebra. Show that A is commutative if and only if its multiplication $m_A : A \otimes A \to A$ is a $\mathbf{k}$-algebra homomorphism.

Remark 1.5.7. If C is a $\mathbf{k}$-coalgebra, then $\epsilon_C : C \to \mathbf{k}$ is always a $\mathbf{k}$-coalgebra homomorphism. Similarly, $u_A : \mathbf{k} \to A$ is a $\mathbf{k}$-algebra homomorphism whenever A is a $\mathbf{k}$-algebra.

Exercise 1.5.8. (a) Let A and B be two $\mathbf{k}$-algebras, at least one of which is commutative. Prove that the $\mathbf{k}$-algebra anti-homomorphisms from A to B are the same as the $\mathbf{k}$-algebra homomorphisms from A to B.

(b) State and prove the dual of this result.

Exercise 1.5.9. Let A be a commutative $\mathbf{k}$-algebra, and let $k \in \mathbb{N}$. The symmetric group $\mathfrak{S}_k$ acts on the k-fold tensor power $A^{\otimes k}$ by permuting the tensor factors: $\sigma(v_1 \otimes v_2 \otimes \cdots \otimes v_k) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(k)}$ for all $v_1, v_2, \ldots, v_k \in A$ and $\sigma \in \mathfrak{S}_k$. For every $\pi \in \mathfrak{S}_k$, denote by $\rho(\pi)$ the action of π on $A^{\otimes k}$ (this is an endomorphism of $A^{\otimes k}$). Show that every $\pi \in \mathfrak{S}_k$ satisfies $m^{(k-1)} \circ (\rho(\pi)) = m^{(k-1)}$. (Recall that $m^{(k-1)} : A^{\otimes k} \to A$ is defined as in Exercise 1.4.19 for $k \geq 1$, and by $m^{(-1)} = u : \mathbf{k} \to A$ for $k = 0$.)

Exercise 1.5.10. State and solve the analogue of Exercise 1.5.9 for cocommutative $\mathbf{k}$-coalgebras.

Exercise 1.5.11. (a) If H is a $\mathbf{k}$-bialgebra and A is a commutative $\mathbf{k}$-algebra, and if f and g are two $\mathbf{k}$-algebra homomorphisms $H \to A$, then prove that $f \star g$ also is a $\mathbf{k}$-algebra homomorphism $H \to A$.

(b) If H is a $\mathbf{k}$-bialgebra and A is a commutative $\mathbf{k}$-algebra, and if $f_1, f_2, \ldots, f_k$ are several $\mathbf{k}$-algebra homomorphisms $H \to A$, then prove that $f_1 \star f_2 \star \cdots \star f_k$ also is a $\mathbf{k}$-algebra homomorphism $H \to A$.

(c) If H is a Hopf algebra and A is a commutative $\mathbf{k}$-algebra, and if $f : H \to A$ is a $\mathbf{k}$-algebra homomorphism, then prove that $f \circ S : H \to A$ (where S is the antipode of H) is again a $\mathbf{k}$-algebra homomorphism, and is a $\star$-inverse to f.

(d) If A is a commutative $\mathbf{k}$-algebra, then show that $m^{(k)}$ is a $\mathbf{k}$-algebra homomorphism for every $k \in \mathbb{N}$. (The map $m^{(k)} : A^{\otimes(k+1)} \to A$ is defined as in Exercise 1.4.19.)

(e) If C' and C are two $\mathbf{k}$-coalgebras, if $\gamma : C \to C'$ is a $\mathbf{k}$-coalgebra homomorphism, if A and A' are two $\mathbf{k}$-algebras, if $\alpha : A \to A'$ is a $\mathbf{k}$-algebra homomorphism, and if $f_1, f_2, \ldots, f_k$ are several $\mathbf{k}$-linear maps $C' \to A$, then prove that

$$\alpha \circ (f_1 \star f_2 \star \cdots \star f_k) \circ \gamma = (\alpha \circ f_1 \circ \gamma) \star (\alpha \circ f_2 \circ \gamma) \star \cdots \star (\alpha \circ f_k \circ \gamma).$$

(f) If H is a commutative $\mathbf{k}$-bialgebra, and k and ℓ are two nonnegative integers, then prove that $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star (k\ell)}$.

(g) If H is a commutative $\mathbf{k}$-Hopf algebra, and k and ℓ are two integers, then prove that $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star (k\ell)}$. (These powers $\mathrm{id}_H^{\star k}$, $\mathrm{id}_H^{\star \ell}$ and $\mathrm{id}_H^{\star (k\ell)}$ are well-defined since id_H is $\star$-invertible.)

(h) State and prove the duals of parts (a)–(g) of this exercise.

Remark 1.5.12. The maps $\mathrm{id}_H^{\star k}$ for $k \in \mathbb{N}$ are known as the *Adams operators* of the bialgebra H; they are studied, inter alia, in [5]. Particular cases (and variants) of Exercise 1.5.11(f) appear in [167, Corollaire II.9] and [78, Theorem 1]. Exercise 1.5.11(f) and its dual are [135, Prop. 1.6].

Exercise 1.5.13. Prove that the antipode S of a cocommutative Hopf algebra A satisfies $S^2 = \mathrm{id}_A$. (This was a statement made in Remark 1.4.13.)

Exercise 1.5.14. Let A be a cocommutative graded Hopf algebra with antipode S. Define a $\mathbf{k}$-linear map $E : A \to A$ by having $E(a) = (\deg a) \cdot a$ for every homogeneous element a of A.

(a) Prove that for every $a \in A$, the elements $(S \star E)(a)$ and $(E \star S)(a)$ (where $\star$ denotes convolution in $\mathrm{Hom}(A, A)$) are primitive.

(b) Prove that for every primitive $p \in A$, we have $(S \star E)(p) = (E \star S)(p) = E(p)$.
(c) Prove that for every $a \in A$ and every primitive $p \in A$, we have $(S \star E)(ap) = [(S \star E)(a), p] + \epsilon(a) E(p)$, where $[u, v]$ denotes the commutator $uv - vu$ of u and v.
(d) If A is connected and $\mathbb{Q}$ is a subring of $\mathbf{k}$, prove that the $\mathbf{k}$-algebra A is generated by the $\mathbf{k}$-submodule $\mathfrak{p}$ consisting of the primitive elements of A.
(e) Assume that A is the tensor algebra $T(V)$ of a $\mathbf{k}$-module V, and that the $\mathbf{k}$-submodule $V = V^{\otimes 1}$ of $T(V)$ is the degree-1 homogeneous component of A. Show that $(S \star E)(x_1 x_2 \ldots x_n) = [\ldots[[x_1, x_2], x_3], \ldots, x_n]$ for any $n \geq 1$ and any $x_1, x_2, \ldots, x_n \in V$.

Remark 1.5.15. Exercise 1.5.14 gives rise to a certain idempotent map $A \to A$ when $\mathbf{k}$ is a commutative $\mathbb{Q}$-algebra and A is a cocommutative connected graded $\mathbf{k}$-Hopf algebra. Namely, the $\mathbf{k}$-linear map $A \to A$ sending every homogeneous $a \in A$ to $\frac{1}{\deg a}(S \star E)(a)$ (or 0 if $\deg a = 0$) is idempotent and is a projection on the $\mathbf{k}$-module of primitive elements of A. It is called the *Dynkin idempotent*; see [168] for more of its properties.[32] Part (c) of the exercise is more or less Baker's identity.

1.6. **Duals.** Recall that for $\mathbf{k}$-modules V, taking the dual $\mathbf{k}$-module $V^* := \operatorname{Hom}(V, \mathbf{k})$ reverses $\mathbf{k}$-linear maps. That is, every $\mathbf{k}$-linear map $V \xrightarrow{\varphi} W$ induces an *adjoint map* $W^* \xrightarrow{\varphi^*} V^*$ defined uniquely by

$$(f, \varphi(v)) = (\varphi^*(f), v)$$

in which (f, v) is the bilinear pairing $V^* \times V \to \mathbf{k}$ sending $(f, v) \mapsto f(v)$. If V and W are finite free $\mathbf{k}$-modules[33], more can be said: When φ is expressed in terms of a basis $\{v_i\}_{i \in I}$ for V and a basis $\{w_j\}_{j \in J}$ for W by some matrix, the map φ^* is expressed by the transpose matrix in terms of the dual bases of these two bases[34].

The correspondence $\varphi \mapsto \varphi^*$ between $\mathbf{k}$-linear maps $V \xrightarrow{\varphi} W$ and $\mathbf{k}$-linear maps $W^* \xrightarrow{\varphi^*} V^*$ is one-to-one when W is finite free. However, this is not the case in many combinatorial situations (in which W is usually free but not finite free). Fortunately, many of the good properties of finite free modules carry over to a certain class of graded modules as long as the dual V^* is replaced by a smaller module V^o called the graded dual. Let us first introduce the latter:

When $V = \bigoplus_{n \geq 0} V_n$ is a graded $\mathbf{k}$-module, note that the dual $V^* = \prod_{n \geq 0} (V_n)^*$ can contain functionals f supported on infinitely many V_n. However, we can consider the $\mathbf{k}$-submodule $V^o := \bigoplus_{n \geq 0} (V_n)^* \subset \prod_{n \geq 0} (V_n)^* = V^*$, sometimes called the *graded dual*[35], consisting of the functions f that vanish on all but finitely many V_n. Notice that V^o is graded, whereas V^* (in general) is not. If $V \xrightarrow{\varphi} W$ is a graded $\mathbf{k}$-linear map, then the adjoint map $W^* \xrightarrow{\varphi^*} V^*$ restricts to a graded $\mathbf{k}$-linear map $W^o \to V^o$, which we (abusively) still denote by φ^*.

A graded $\mathbf{k}$-module $V = \bigoplus_{n \geq 0} V_n$ is said to be *of finite type* if each V_n is a finite free $\mathbf{k}$-module[36]. When the graded $\mathbf{k}$-module V is of finite type, the graded $\mathbf{k}$-module V^o is again of finite type[37] and satisfies $(V^o)^o \cong V$. Many other properties of finite free modules are salvaged in this situation; most importantly: The correspondence $\varphi \mapsto \varphi^*$ between graded $\mathbf{k}$-linear maps $V \to W$ and graded $\mathbf{k}$-linear maps $W^o \to V^o$ is one-to-one when W is of finite type[38].

Reversing the diagrams should then make it clear that, in the finite free or finite-type situation, duals of algebras are coalgebras, and vice-versa, and duals of bialgebras or Hopf algebras are bialgebras or Hopf

[32] We will see another such idempotent in Exercise 5.4.6.

[33] A $\mathbf{k}$-module is said to be *finite free* if it has a finite basis. If $\mathbf{k}$ is a field, then a finite free $\mathbf{k}$-module is the same as a finite-dimensional $\mathbf{k}$-vector space.

[34] If $\{v_i\}_{i \in I}$ is a basis of a finite free $\mathbf{k}$-module V, then the *dual basis* of this basis is defined as the basis $\{f_i\}_{i \in I}$ of V^* that satisfies $(f_i, v_j) = \delta_{i,j}$ for all i and j. (Recall that $\delta_{i,j}$ is the Kronecker delta: $\delta_{i,j} = 1$ if $i = j$ and 0 else.)

[35] Do not mistake this for the coalgebraic restricted dual A° of [213, §6.0].

[36] This meaning of "finite type" can differ from the standard one.

[37] More precisely: Let $V = \bigoplus_{n \geq 0} V_n$ be of finite type, and let $\{v_i\}_{i \in I}$ be a *graded basis* of V, that is, a basis of the $\mathbf{k}$-module V such that the indexing set I is partitioned into subsets $I_0, I_1, I_2, \ldots$ (which are allowed to be empty) with the property that, for every $n \in \mathbb{N}$, the subfamily $\{v_i\}_{i \in I_n}$ is a basis of the $\mathbf{k}$-module V_n. Then, we can define a family $\{f_i\}_{i \in I}$ of elements of V^o by setting $(f_i, v_j) = \delta_{i,j}$ for all $i, j \in I$. This family $\{f_i\}_{i \in I}$ is a graded basis of the graded $\mathbf{k}$-module V^o. (Actually, for every $n \in \mathbb{N}$, the subfamily $\{f_i\}_{i \in I_n}$ is a basis of the $\mathbf{k}$-submodule $(V_n)^*$ of V^o – indeed the dual basis to the basis $\{v_i\}_{i \in I_n}$ of V_n.) This basis $\{f_i\}_{i \in I}$ is said to be the *dual basis* to the basis $\{v_i\}_{i \in I}$ of V.

[38] Only W has to be of finite type here; V can be any graded $\mathbf{k}$-module.

algebras. For example, the product in a Hopf algebra A of finite type uniquely defines the coproduct of A^o via adjointness:

$$(\Delta_{A^o}(f), a \otimes b)_{A \otimes A} = (f, ab)_A.$$

Thus if A has a basis $\{a_i\}_{i \in I}$ with *product structure constants* $\{c_{j,k}^i\}$, meaning

$$a_j a_k = \sum_{i \in I} c_{j,k}^i a_i,$$

then the dual basis $\{f_i\}_{i \in I}$ has the same $\{c_{j,k}^i\}$ as its *coproduct structure constants*:

$$\Delta_{A^o}(f_i) = \sum_{(j,k) \in I \times I} c_{j,k}^i f_j \otimes f_k.$$

The assumption that A be of finite type was indispensable here; in general, the dual of a $\mathbf{k}$-algebra does not become a $\mathbf{k}$-coalgebra. However, the dual of a $\mathbf{k}$-coalgebra still becomes a $\mathbf{k}$-algebra, as shown in the following exercise:

Exercise 1.6.1. For any two $\mathbf{k}$-modules U and V, let $\rho_{U,V} : U^* \otimes V^* \to (U \otimes V)^*$ be the $\mathbf{k}$-linear map which sends every tensor $f \otimes g \in U^* \otimes V^*$ to the composition $U \otimes V \xrightarrow{f \otimes g} \mathbf{k} \otimes \mathbf{k} \xrightarrow{m_{\mathbf{k}}} \mathbf{k}$ of the map[39] $f \otimes g$ with the canonical isomorphism $\mathbf{k} \otimes \mathbf{k} \xrightarrow{m_{\mathbf{k}}} \mathbf{k}$. When $\mathbf{k}$ is a field and U is finite-dimensional, this map $\rho_{U,V}$ is a $\mathbf{k}$-vector space isomorphism (and usually regarded as the identity); more generally, it is injective whenever $\mathbf{k}$ is a field[40]. Also, let $s : \mathbf{k} \to \mathbf{k}^*$ be the canonical isomorphism. Prove that:

(a) If C is a $\mathbf{k}$-coalgebra, then C^* becomes a $\mathbf{k}$-algebra if we define its associative operation by $m_{C^*} = \Delta_C^* \circ \rho_{C,C} : C^* \otimes C^* \to C^*$ and its unit map to be $\epsilon_C^* \circ s : \mathbf{k} \to C^*$. [41]

(b) The $\mathbf{k}$-algebra structure defined on C^* in part (a) is precisely the one defined on $\operatorname{Hom}(C, \mathbf{k}) = C^*$ in Definition 1.4.1 applied to $A = \mathbf{k}$.

(c) If C is a graded $\mathbf{k}$-coalgebra, then C^o is a $\mathbf{k}$-subalgebra of the $\mathbf{k}$-algebra C^* defined in part (a).

(d) If $f : C \to D$ is a homomorphism of $\mathbf{k}$-coalgebras, then $f^* : D^* \to C^*$ is a homomorphism of $\mathbf{k}$-algebras.

(e) Let U be a graded $\mathbf{k}$-module (not necessarily of finite type), and let V be a graded $\mathbf{k}$-module of finite type. Then, there is a 1-to-1 correspondence between graded $\mathbf{k}$-linear maps $U \to V$ and graded $\mathbf{k}$-linear maps $V^o \to U^o$ given by $f \mapsto f^*$.

(f) Let C be a graded $\mathbf{k}$-coalgebra (not necessarily of finite type), and let D be a graded $\mathbf{k}$-coalgebra of finite type. Part (e) of this exercise shows that there is a 1-to-1 correspondence between graded $\mathbf{k}$-linear maps $C \to D$ and graded $\mathbf{k}$-linear maps $D^o \to C^o$ given by $f \mapsto f^*$. This correspondence has the property that a given graded $\mathbf{k}$-linear map $f : C \to D$ is a $\mathbf{k}$-coalgebra morphism if and only if $f^* : D^o \to C^o$ is a $\mathbf{k}$-algebra morphism.

Another example of a Hopf algebra is provided by the so-called shuffle algebra. Before we introduce it, let us define the *shuffles* of two words:

Definition 1.6.2. Given two words $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_m)$, the *multiset of shuffles of a and b* is defined as the multiset

$$\left\{ \left(c_{w(1)}, c_{w(2)}, \ldots, c_{w(n+m)}\right) \ : \ w \in \mathrm{Sh}_{n,m} \right\}_{\text{multiset}},$$

where $(c_1, c_2, \ldots, c_{n+m})$ is the concatenation $a \cdot b = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m)$, and where $\mathrm{Sh}_{n,m}$ is the subset[42]

$$\left\{ w \in \mathfrak{S}_{n+m} \ : \ w^{-1}(1) < w^{-1}(2) < \cdots < w^{-1}(n) ; \ w^{-1}(n+1) < w^{-1}(n+2) < \cdots < w^{-1}(n+m) \right\}$$

of the symmetric group $\mathfrak{S}_{n+m}$. Informally speaking, the shuffles of the two words a and b are the words obtained by overlaying the words a and b, after first moving their letters apart so that no letters get

[39] Keep in mind that the *tensor* $f \otimes g \in U^* \otimes V^*$ is not the same as the *map* $U \otimes V \xrightarrow{f \otimes g} \mathbf{k} \otimes \mathbf{k}$.

[40] Over arbitrary rings it does not have to be even that!

[41] If C is a finite free $\mathbf{k}$-module, then this $\mathbf{k}$-algebra structure is the same as the one defined above by adjointness. But the advantage of the new definition is that it works even if C is not a finite free $\mathbf{k}$-module.

[42] **Warning:** This definition of $\mathrm{Sh}_{n,m}$ is highly nonstandard, and many authors define $\mathrm{Sh}_{n,m}$ to be the set of the inverses of the permutations belonging to what we call $\mathrm{Sh}_{n,m}$.

superimposed when the words are overlayed[43]. In particular, any shuffle of a and b contains a and b as subsequences. The multiset of shuffles of a and b has $\binom{m+n}{n}$ elements (counted with multiplicity) and is denoted by $a \sqcup\!\sqcup b$. For instance, the shuffles of $(1,2,1)$ and $(3,2)$ are

$$(\underline{1},\underline{2},\underline{1},3,2),(\underline{1},\underline{2},3,\underline{1},2),(\underline{1},\underline{2},3,2,\underline{1}),(\underline{1},3,\underline{2},\underline{1},2),(\underline{1},3,\underline{2},2,\underline{1}),$$
$$(\underline{1},3,2,\underline{2},\underline{1}),(3,\underline{1},\underline{2},\underline{1},2),(3,\underline{1},\underline{2},2,\underline{1}),(3,\underline{1},2,\underline{2},\underline{1}),(3,2,\underline{1},\underline{2},\underline{1}),$$

listed here as often as they appear in the multiset $(1,2,1) \sqcup\!\sqcup (3,2)$. Here we have underlined the letters taken from a – that is, the letters at positions $w^{-1}(1)$, $w^{-1}(2)$, ..., $w^{-1}(n)$.

Example 1.6.3. When $A = T(V)$ is the tensor algebra for a finite free $\mathbf{k}$-module V, having $\mathbf{k}$-basis $\{x_i\}_{i\in I}$, its graded dual A^o is another Hopf algebra whose basis $\left\{y_{(i_1,\ldots,i_\ell)}\right\}$ (the dual basis of the basis $\{x_{i_1}\cdots x_{i_\ell}\}$ of $A = T(V)$) is indexed by words in the alphabet I. This Hopf algebra A^o could be called the *shuffle algebra* of V^*. (To be more precise, it is isomorphic to the shuffle algebra of V^* introduced in Proposition 1.6.7 further below; we prefer not to call A^o itself the shuffle algebra of V^*, since A^o has several disadvantages[44].) Duality shows that the *cut* coproduct in A^o is defined by

$$\Delta y_{(i_1,\ldots,i_\ell)} = \sum_{j=0}^{\ell} y_{(i_1,\ldots,i_j)} \otimes y_{(i_{j+1},i_{j+2},\ldots,i_\ell)}. \tag{1.6.1}$$

For example,

$$\Delta y_{abcb} = y_{\varnothing}\otimes y_{abcb} + y_a \otimes y_{bcb} + y_{ab}\otimes y_{cb} + y_{abc}\otimes y_b + y_{abcb}\otimes y_{\varnothing}.$$

Duality also shows that the *shuffle* product in A^o will be given by

$$y_{(i_1,\ldots,i_\ell)} y_{(j_1,\ldots,j_m)} = \sum_{\mathbf{k}=(k_1,\ldots,k_{\ell+m})\in \mathbf{i}\sqcup\!\sqcup\mathbf{j}} y_{(k_1,\ldots,k_{\ell+m})} \tag{1.6.2}$$

where $\mathbf{i}\sqcup\!\sqcup\mathbf{j}$ (as in Definition 1.6.2) denotes the multiset of the $\binom{\ell+m}{\ell}$ words obtained as *shuffles* of the two words $\mathbf{i} = (i_1,\ldots,i_\ell)$ and $\mathbf{j} = (j_1,\ldots,j_m)$. For example,

$$\begin{aligned} y_{ab}y_{cb} &= y_{abcb} + y_{acbb} + y_{cabb} + y_{cabb} + y_{acbb} + y_{cbab} \\ &= y_{abcb} + 2y_{acbb} + 2y_{cabb} + y_{cbab}. \end{aligned}$$

Equivalently, one has

$$y_{(i_1,i_2,\ldots,i_\ell)} y_{(i_{\ell+1},i_{\ell+2},\ldots,i_{\ell+m})} = \sum_{\substack{w\in\mathfrak{S}_{\ell+m}:\\ w(1)<\cdots<w(\ell),\\ w(\ell+1)<\cdots<w(\ell+m)}} y_{\left(i_{w^{-1}(1)},i_{w^{-1}(2)},\ldots,i_{w^{-1}(\ell+m)}\right)} \tag{1.6.3}$$

$$= \sum_{\sigma\in \mathrm{Sh}_{\ell,m}} y_{\left(i_{\sigma(1)},i_{\sigma(2)},\ldots,i_{\sigma(\ell+m)}\right)} \tag{1.6.4}$$

(using the notations of Definition 1.6.2 again). Lastly, the antipode S of A^o is the adjoint of the antipode of $A = T(V)$ described in (1.4.6):

$$S y_{(i_1,i_2,\ldots,i_\ell)} = (-1)^\ell y_{(i_\ell,\ldots,i_2,i_1)}.$$

Since the coalgebra $T(V)$ is cocommutative, its graded dual $T(V)^o$ is commutative.

Exercise 1.6.4. Let V be a 1-dimensional free $\mathbf{k}$-module with basis element x, so $\mathrm{Sym}(V) \cong \mathbf{k}[x]$, with $\mathbf{k}$-basis $\{1 = x^0, x^1, x^2, \ldots\}$.

---

[43] For instance, if $a = (1,3,2,1)$ and $b = (2,4)$, then the shuffle $(1,2,3,2,4,1)$ of a and b can be obtained by moving the letters of a and b apart as follows:

$$\begin{array}{lcccccc} a = & 1 & & 3 & 2 & & 1 \\ b = & & 2 & & & 4 & \end{array}$$

and then overlaying them to obtain $\begin{array}{cccccc} 1 & 2 & 3 & 2 & 4 & 1 \end{array}$. Other ways of moving letters apart lead to further shuffles (not always distinct).

[44] Specifically, A^o has the disadvantages of being defined only when V^* is the dual of a finite free $\mathbf{k}$-module V, and depending on a choice of basis, whereas Proposition 1.6.7 will define shuffle algebras in full generality and canonically.

(a) Check that the powers x^i satisfy

$$\begin{aligned} x^i \cdot x^j &= x^{i+j}, \\ \Delta(x^n) &= \sum_{i+j=n} \binom{n}{i} x^i \otimes x^j, \\ S(x^n) &= (-1)^n x^n. \end{aligned}$$

(b) Check that the dual basis elements $\{f^{(0)}, f^{(1)}, f^{(2)}, \ldots\}$ for $\mathrm{Sym}(V)^o$, defined by $f^{(i)}(x^j) = \delta_{i,j}$, satisfy

$$\begin{aligned} f^{(i)} f^{(j)} &= \binom{i+j}{i} f^{(i+j)}, \\ \Delta(f^{(n)}) &= \sum_{i+j=n} f^{(i)} \otimes f^{(j)}, \\ S(f^{(n)}) &= (-1)^n f^{(n)}. \end{aligned}$$

(c) Show that if $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the $\mathbf{k}$-linear map $\mathrm{Sym}(V)^o \to \mathrm{Sym}(V)$ sending $f^{(n)} \mapsto \frac{x^n}{n!}$ is a graded Hopf isomorphism.

For this reason, the Hopf structure on $\mathrm{Sym}(V)^o$ is called a *divided power algebra*.

(d) Show that when $\mathbf{k}$ is a field of characteristic $p > 0$, one has $(f^{(1)})^p = 0$, and hence why there can be no Hopf isomorphism $\mathrm{Sym}(V)^o \to \mathrm{Sym}(V)$.

Exercise 1.6.5. Let V have $\mathbf{k}$-basis $\{x_1, \ldots, x_n\}$, and let $V \oplus V$ have $\mathbf{k}$-basis $\{x_1, \ldots, x_n, y_1, \ldots, y_n\}$, so that one has isomorphisms

$$\mathrm{Sym}(V \oplus V) \cong \mathbf{k}[\mathbf{x}, \mathbf{y}] \cong \mathbf{k}[\mathbf{x}] \otimes \mathbf{k}[\mathbf{y}] \cong \mathrm{Sym}(V) \otimes \mathrm{Sym}(V).$$

Here we are using the abbreviations $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_n)$.

(a) Show that our usual coproduct on $\mathrm{Sym}(V)$ can be re-expressed as follows:

$$\begin{array}{ccc} \mathrm{Sym}(V) & & \mathrm{Sym}(V) \otimes \mathrm{Sym}(V) \\ \| & & \| \\ \mathbf{k}[\mathbf{x}] & \xrightarrow{\Delta} & \mathbf{k}[\mathbf{x}, \mathbf{y}], \\ f(x_1, \ldots, x_n) & \longmapsto & f(x_1 + y_1, \ldots, x_n + y_n). \end{array}$$

In other words, it is induced from the diagonal map

$$\begin{array}{ccc} V & \longrightarrow & V \oplus V, \\ x_i & \longmapsto & x_i + y_i. \end{array} \tag{1.6.5}$$

(b) One can similarly define a coproduct on the *exterior algebra* $\wedge V$, which is the quotient $T(V)/J$ where J is the two-sided ideal generated by the elements $\{x^2 (= x \otimes x)\}_{x \in V}$ in $T^2(V)$. The ideal J is a graded $\mathbf{k}$-submodule of $T(V)$ (this is not obvious!), and the quotient $T(V)/J$ becomes a graded commutative algebra

$$\wedge V = \bigoplus_{d=0}^{n} \wedge^d V \left(= \bigoplus_{d=0}^{\infty} \wedge^d V \right),$$

if one views the elements of $V = \wedge^1 V$ as having *odd* degree, and uses the topologist's sign convention (as in (1.3.3)). One again has $\wedge(V \oplus V) = \wedge V \otimes \wedge V$ as graded algebras. Show that one can again let the diagonal map (1.6.5) induce a map

$$\begin{array}{ccc} \wedge(V) & \xrightarrow{\Delta} & \wedge V \otimes \wedge V, \\ f(x_1, \ldots, x_n) & \longmapsto & f(x_1 + y_1, \ldots, x_n + y_n) \\ \| & & \| \\ \sum c_{i_1, \ldots, i_d} \cdot x_{i_1} \wedge \cdots \wedge x_{i_d} & & \sum c_{i_1, \ldots, i_d} \cdot (x_{i_1} + y_{i_1}) \wedge \cdots \wedge (x_{i_d} + y_{i_d}), \end{array} \tag{1.6.6}$$

which makes $\wedge V$ into a connected graded Hopf algebra.

(c) Show that in the tensor algebra $T(V)$, if one views the elements of $V = V^{\otimes 1}$ as having odd degree, and uses the topologist's sign convention (1.3.3) in the twist map when defining $T(V)$, then for any x in V one has $\Delta(x^2) = 1 \otimes x^2 + x^2 \otimes 1$.

(d) Let us use the convention (1.3.3) as in part (c). Show that the two-sided ideal $J \subset T(V)$ generated by $\{x^2\}_{x \in V}$ is also a two-sided coideal and a graded $\mathbf{k}$-submodule of $T(V)$, and hence the quotient $\wedge V = T(V)/J$ inherits the structure of a graded bialgebra. Check that the coproduct on $\wedge V$ inherited from $T(V)$ is the same as the one defined in part (b).

[**Hint:** The ideal J in part (b) is a graded $\mathbf{k}$-submodule of $T(V)$, but this is not completely obvious (not all elements of V have to be homogeneous!).]

Exercise 1.6.6. Let C be a $\mathbf{k}$-coalgebra. As we know from Exercise 1.6.1(a), this makes C^* into a $\mathbf{k}$-algebra.
Let A be a $\mathbf{k}$-algebra which is finite free as $\mathbf{k}$-module. This makes A^* into a $\mathbf{k}$-coalgebra.
Let $f : C \to A$ and $g : C \to A$ be two $\mathbf{k}$-linear maps. Show that $f^* \star g^* = (f \star g)^*$.

The above arguments might have created the impression that duals of bialgebras have good properties only under certain restrictive conditions (e.g., the dual of a bialgebra H does not generally become a bialgebra unless H is of finite type), and so they cannot be used in proofs and constructions unless one is willing to sacrifice some generality (e.g., we had to require V to be finite free in Example 1.6.3). While the first part of this impression is true, the second is not always; often there is a way to gain back the generality lost from using duals. As an example of this, let us define the shuffle algebra of an arbitrary $\mathbf{k}$-module (not just of a dual of a finite free $\mathbf{k}$-module as in Example 1.6.3):

Proposition 1.6.7. *Let V be a $\mathbf{k}$-module. Define a $\mathbf{k}$-linear map $\Delta_{\sqcup\!\sqcup} : T(V) \to T(V) \otimes T(V)$ by setting*

$$\Delta_{\sqcup\!\sqcup}(v_1 v_2 \cdots v_n) = \sum_{k=0}^{n} (v_1 v_2 \cdots v_k) \otimes (v_{k+1} v_{k+2} \cdots v_n) \qquad \text{for all } n \in \mathbb{N} \text{ and } v_1, v_2, \ldots, v_n \in V.$$

[45] *Define a $\mathbf{k}$-bilinear map $\mathbin{\underline{\sqcup\!\sqcup}} : T(V) \times T(V) \to T(V)$, which will be written in infix notation (that is, we will write $a \mathbin{\underline{\sqcup\!\sqcup}} b$ instead of $\mathbin{\underline{\sqcup\!\sqcup}}(a, b)$), by setting*[46]

$$(v_1 v_2 \cdots v_\ell) \mathbin{\underline{\sqcup\!\sqcup}} (v_{\ell+1} v_{\ell+2} \cdots v_{\ell+m}) = \sum_{\sigma \in \mathrm{Sh}_{\ell,m}} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(\ell+m)}$$
$$\text{for all } \ell, m \in \mathbb{N} \text{ and } v_1, v_2, \ldots, v_{\ell+m} \in V.$$

[47] *Consider also the comultiplication ϵ of the Hopf algebra $T(V)$.*

Then, the $\mathbf{k}$-module $T(V)$, endowed with the multiplication $\mathbin{\underline{\sqcup\!\sqcup}}$, the unit $1_{T(V)} \in V^{\otimes 0} \subset T(V)$, the comultiplication $\Delta_{\sqcup\!\sqcup}$ and the counit ϵ, becomes a commutative Hopf algebra. This Hopf algebra is called the shuffle algebra *of V, and denoted by $\mathrm{Sh}(V)$. The antipode of the Hopf algebra $\mathrm{Sh}(V)$ is precisely the antipode S of $T(V)$.*

Exercise 1.6.8. Prove Proposition 1.6.7.

[**Hint:** When V is a finite free $\mathbf{k}$-module, Proposition 1.6.7 follows from Example 1.6.3. The trick is to derive the general case from this specific one. Every $\mathbf{k}$-linear map $f : W \to V$ between two $\mathbf{k}$-modules W and V induces a map $T(f) : T(W) \to T(V)$ which preserves $\Delta_{\sqcup\!\sqcup}$, $\mathbin{\underline{\sqcup\!\sqcup}}$, $1_{T(W)}$, ϵ and S (in the appropriate meanings – e.g., preserving $\Delta_{\sqcup\!\sqcup}$ means $\Delta_{\sqcup\!\sqcup} \circ T(f) = (T(f) \otimes T(f)) \circ \Delta_{\sqcup\!\sqcup}$). Show that each of the equalities that need to be proven in order to verify Proposition 1.6.7 can be "transported" along such a map $T(f)$ from a $T(W)$ for a suitably chosen finite free $\mathbf{k}$-module W.]

It is also possible to prove Proposition 1.6.7 "by foot", as long as one is ready to make combinatorial arguments about cutting shuffles.

Remark 1.6.9. (a) Let V be a finite free $\mathbf{k}$-module. The Hopf algebra $T(V)^o$ (studied in Example 1.6.3) is naturally isomorphic to the shuffle algebra $\mathrm{Sh}(V^*)$ (defined as in Proposition 1.6.7 but for V^* instead of V) as Hopf algebras, by the obvious isomorphism (namely, the direct sum of the isomorphisms $(V^{\otimes n})^* \to (V^*)^{\otimes n}$ over all $n \in \mathbb{N}$). [48]

[45] This is well-defined, because the right hand side is n-multilinear in $v_1, v_2, \ldots, v_n$, and because any n-multilinear map $V^{\times n} \to M$ into a $\mathbf{k}$-module M gives rise to a unique $\mathbf{k}$-linear map $V^{\otimes n} \to M$.

[46] Many authors use the symbol $\sqcup\!\sqcup$ instead of $\mathbin{\underline{\sqcup\!\sqcup}}$ here, but we prefer to reserve the former notation for the shuffle product of words.

[47] Again, this is well-defined by the $\ell + m$-multilinearity of the right hand side.

[48] This can be verified by comparing (1.6.1) with the definition of $\Delta_{\sqcup\!\sqcup}$, and comparing (1.6.4) with the definition of $\mathbin{\underline{\sqcup\!\sqcup}}$.

(b) The same statement applies to the case when V is a graded $\mathbf{k}$-module of finite type satisfying $V_0 = 0$ rather than a finite free $\mathbf{k}$-module, provided that V^* and $(V^{\otimes n})^*$ are replaced by V^o and $(V^{\otimes n})^o$.

We shall return to shuffle algebras in Section 6.3, where we will show that under certain conditions ($\mathbb{Q}$ being a subring of $\mathbf{k}$, and V being a free $\mathbf{k}$-module) the algebra structure on a shuffle algebra $\mathrm{Sh}(V)$ is a polynomial algebra in an appropriately chosen set of generators[49].

1.7. **Infinite sums and Leray's theorem.** In this section (which can be skipped, as it will not be used except in a few exercises), we will see how a Hopf algebra structure on a $\mathbf{k}$-algebra reveals knowledge about the $\mathbf{k}$-algebra itself. Specifically, we will show that if $\mathbf{k}$ is a commutative $\mathbb{Q}$-algebra, and if A is any commutative connected graded $\mathbf{k}$-Hopf algebra, then A as a $\mathbf{k}$-algebra must be (isomorphic to) a symmetric algebra of a $\mathbf{k}$-module[50]. This is a specimen of a class of facts which are commonly called *Leray theorems*; for different specimens, see [156, Theorem 7.5] or [35, p. 17, "Hopf's theorem"] or [35, §2.5, A, B, C] or [35, Theorem 3.8.3].[51] In a sense, these facts foreshadow Zelevinsky's theory of positive self-dual Hopf algebras, which we shall encounter in Chapter 3; however, the latter theory works in a much less general setting (and makes much stronger claims).

We shall first explore the possibilities of applying a formal power series v to a linear map $f : C \to A$ from a coalgebra C to an algebra A. We have already seen an example of this in the proof of Proposition 1.4.7 above (where the power series $\sum_{k \geq 0} (-1)^k T^k \in \mathbf{k}[[T]]$ was applied to the locally $\star$-nilpotent map $\mathrm{id}_A - u_A \epsilon_A : A \to A$); we shall now take a more systematic approach and establish general criteria for when such applications are possible. First, we will have to make sense of infinite sums of maps from a coalgebra to an algebra. This is somewhat technical, but the effort will pay off.

Definition 1.7.1. Let A be an abelian group (written additively).

We say that a family $(a_q)_{q \in Q} \in A^Q$ of elements of A is *finitely supported* if all but finitely many $q \in Q$ satisfy $a_q = 0$. Clearly, if $(a_q)_{q \in Q} \in A^Q$ is a finitely supported family, then the sum $\sum_{q \in Q} a_q$ is well-defined (since all but finitely many of its addends are 0). Sums like this satisfy the usual rules for sums, even though their indexing set Q may be infinite. (For example, if $(a_q)_{q \in Q}$ and $(b_q)_{q \in Q}$ are two finitely supported families in A^Q, then the family $(a_q + b_q)_{q \in Q}$ is also finitely supported, and we have $\sum_{q \in Q} a_q + \sum_{q \in Q} b_q = \sum_{q \in Q} (a_q + b_q)$.)

Definition 1.7.2. Let C and A be two $\mathbf{k}$-modules.

We say that a family $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ of maps $f_q \in \mathrm{Hom}(C, A)$ is *pointwise finitely supported* if for each $x \in C$, the family $(f_q(x))_{q \in Q} \in A^Q$ of elements of A is finitely supported.[52] If $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is a pointwise finitely supported family, then the sum $\sum_{q \in Q} f_q$ is defined to be the map $C \to A$ sending each $x \in C$ to $\sum_{q \in Q} f_q(x)$. [53]

Note that the concept of a "pointwise finitely supported" family $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is precisely the concept of a "summable" family in [60, Definition 1].

Definition 1.7.3. For the rest of Section 1.7, we shall use the following conventions:

- Let C be a $\mathbf{k}$-coalgebra. Let A be a $\mathbf{k}$-algebra.

[49] This says nothing about the coalgebra structure on $\mathrm{Sh}(V)$ – which is much more complicated in these generators.

[50] If $\mathbf{k}$ is a field, then this simply means that A as a $\mathbf{k}$-algebra must be a polynomial ring over $\mathbf{k}$.

[51] Notice that many of these sources assume $\mathbf{k}$ to be a field; some of their proofs rely on this assumption.

[52] Here are some examples of pointwise finitely supported families:

- If Q is a finite set, then any family $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is pointwise finitely supported.
- More generally, any finitely supported family $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is pointwise finitely supported.
- If C is a graded $\mathbf{k}$-module, and if $(f_n)_{n \in \mathbb{N}} \in (\mathrm{Hom}(C, A))^{\mathbb{N}}$ is a family of maps such that $f_n(C_m) = 0$ whenever $n \neq m$, then the family $(f_n)_{n \in \mathbb{N}}$ is pointwise finitely supported.
- If C is a graded $\mathbf{k}$-coalgebra and A is any $\mathbf{k}$-algebra, and if $f \in \mathrm{Hom}(C, A)$ satisfies $f(C_0) = 0$, then the family $(f^{\star n})_{n \in \mathbb{N}} \in (\mathrm{Hom}(C, A))^{\mathbb{N}}$ is pointwise finitely supported. (This will be proven in Proposition 1.7.11(h).)

[53] This definition of $\sum_{q \in Q} f_q$ generalizes the usual definition of $\sum_{q \in Q} f_q$ when Q is a finite set (because if Q is a finite set, then any family $(f_q)_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is pointwise finitely supported).

- We shall avoid our standard practice of denoting the unit map $u_A : \mathbf{k} \to A$ of a $\mathbf{k}$-algebra A by u; instead, we will use the letter u (without the subscript A) for other purposes.

Definition 1.7.2 allows us to work with infinite sums in $\operatorname{Hom}(C, A)$, provided that we are summing a pointwise finitely supported family. We shall next state some properties of such sums:[54]

Proposition 1.7.4. *Let $(f_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ be a pointwise finitely supported family. Then, the map $\sum_{q\in Q} f_q$ belongs to $\operatorname{Hom}(C, A)$.*

Proposition 1.7.5. *Let $(f_q)_{q\in Q}$ and $(g_q)_{q\in Q}$ be two pointwise finitely supported families in $(\operatorname{Hom}(C, A))^Q$. Then, the family $(f_q + g_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ is also pointwise finitely supported, and satisfies*

$$\sum_{q\in Q} f_q + \sum_{q\in Q} g_q = \sum_{q\in Q} (f_q + g_q).$$

Proposition 1.7.6. *Let $(f_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ and $(g_r)_{r\in R} \in (\operatorname{Hom}(C, A))^R$ be two pointwise finitely supported families. Then, the family $(f_q \star g_r)_{(q,r)\in Q\times R} \in (\operatorname{Hom}(C, A))^{Q\times R}$ is pointwise finitely supported, and satisfies*

$$\sum_{(q,r)\in Q\times R} (f_q \star g_r) = \left(\sum_{q\in Q} f_q\right) \star \left(\sum_{r\in R} g_r\right).$$

Roughly speaking, the above three propositions say that sums of the form $\sum_{q\in Q} f_q$ (where $(f_q)_{q\in Q}$ is a pointwise finitely supported family) satisfy the usual rules for finite sums. Furthermore, the following properties of pointwise finitely supported families hold:

Proposition 1.7.7. *Let $(f_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ be a pointwise finitely supported family. Let $(\lambda_q)_{q\in Q} \in \mathbf{k}^Q$ be any family of elements of $\mathbf{k}$. Then, the family $(\lambda_q f_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ is pointwise finitely supported.*

Proposition 1.7.8. *Let $(f_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ and $(g_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ be two families such that $(f_q)_{q\in Q}$ is pointwise finitely supported. Then, the family $(f_q \star g_q)_{q\in Q} \in (\operatorname{Hom}(C, A))^Q$ is also pointwise finitely supported.*

Exercise 1.7.9. Prove Propositions 1.7.4, 1.7.5, 1.7.6, 1.7.7 and 1.7.8.

We can now define the notion of a "pointwise $\star$-nilpotent" map. Roughly speaking, this will mean an element of $(\operatorname{Hom}(C, A), \star)$ that can be substituted into any power series because its powers (with respect to the convolution $\star$) form a pointwise finitely supported family. Here is the definition:

Definition 1.7.10. (a) A map $f \in \operatorname{Hom}(C, A)$ is said to be *pointwise $\star$-nilpotent* if and only if the family $(f^{\star n})_{n\in\mathbb{N}} \in (\operatorname{Hom}(C, A))^{\mathbb{N}}$ is pointwise finitely supported. Equivalently, a map $f \in \operatorname{Hom}(C, A)$ is pointwise $\star$-nilpotent if and only if for each $x \in C$, the family $(f^{\star n}(x))_{n\in\mathbb{N}}$ of elements of A is finitely supported.

(b) If $f \in \operatorname{Hom}(C, A)$ is a pointwise $\star$-nilpotent map, and if $(\lambda_n)_{n\in\mathbb{N}} \in \mathbf{k}^{\mathbb{N}}$ is any family of scalars, then the family $(\lambda_n f^{\star n})_{n\in\mathbb{N}} \in (\operatorname{Hom}(C, A))^{\mathbb{N}}$ is pointwise finitely supported[55], and thus the infinite sum $\sum_{n\geq 0} \lambda_n f^{\star n} = \sum_{n\in\mathbb{N}} \lambda_n f^{\star n}$ is well-defined and belongs to $\operatorname{Hom}(C, A)$ (by Proposition 1.7.4).[56]

[54] See Exercise 1.7.9 below for the proofs of these properties.

[55] This follows easily from Proposition 1.7.7 above. (In fact, the map f is pointwise $\star$-nilpotent, and thus the family $(f^{\star n})_{n\in\mathbb{N}} \in (\operatorname{Hom}(C, A))^{\mathbb{N}}$ is pointwise finitely supported (by the definition of "pointwise $\star$-nilpotent"). Hence, Proposition 1.7.7 (applied to $Q = \mathbb{N}$ and $(f_q)_{q\in Q} = (f^{\star n})_{n\in\mathbb{N}}$ and $(\lambda_q)_{q\in Q} = (\lambda_n)_{n\in\mathbb{N}}$) shows that the family $(\lambda_n f^{\star n})_{n\in\mathbb{N}} \in (\operatorname{Hom}(C, A))^{\mathbb{N}}$ is pointwise finitely supported.)

[56] Notice that the concept of "local $\star$-nilpotence" we used in the proof of Proposition 1.4.24 serves the same function (viz., ensuring that the sum $\sum_{n\in\mathbb{N}} \lambda_n f^{\star n}$ is well-defined). But local $\star$-nilpotence is only defined when a grading is present, whereas pointwise $\star$-nilpotence is defined in the general case. Also, local $\star$-nilpotence is more restrictive (i.e., a locally $\star$-nilpotent map is always pointwise $\star$-nilpotent, but the converse does not always hold).

(c) We let $\mathfrak{n}(C,A)$ be the set of all pointwise $\star$-nilpotent maps $f \in \mathrm{Hom}(C,A)$. Note that this is not necessarily a $\mathbf{k}$-submodule of $\mathrm{Hom}(C,A)$.

(d) Consider the ring $\mathbf{k}[[T]]$ of formal power series in an indeterminate T over $\mathbf{k}$. For any power series $u \in \mathbf{k}[[T]]$ and any $f \in \mathfrak{n}(C,A)$, we define a map $u^\star(f) \in \mathrm{Hom}(C,A)$ by $u^\star(f) = \sum_{n\geq 0} u_n f^{\star n}$, where u is written in the form $u = \sum_{n\geq 0} u_n T^n$ with $(u_n)_{n\geq 0} \in \mathbf{k}^{\mathbb{N}}$. (This sum $\sum_{n\geq 0} u_n f^{\star n}$ is well-defined in $\mathrm{Hom}(C,A)$, since f is pointwise $\star$-nilpotent.)

The following proposition gathers some properties of pointwise $\star$-nilpotent maps[57]:

Proposition 1.7.11. (a) *For any $f \in \mathfrak{n}(C,A)$ and $k \in \mathbb{N}$, we have*

$$\left(T^k\right)^\star(f) = f^{\star k}. \tag{1.7.1}$$

(b) *For any $f \in \mathfrak{n}(C,A)$ and $u, v \in \mathbf{k}[[T]]$, we have*

$$(u+v)^\star(f) = u^\star(f) + v^\star(f) \qquad \text{and} \tag{1.7.2}$$

$$(uv)^\star(f) = u^\star(f) \star v^\star(f). \tag{1.7.3}$$

Also, for any $f \in \mathfrak{n}(C,A)$ and $u \in \mathbf{k}[[T]]$ and $\lambda \in \mathbf{k}$, we have

$$(\lambda u)^\star(f) = \lambda u^\star(f). \tag{1.7.4}$$

Also, for any $f \in \mathfrak{n}(C,A)$, we have

$$0^\star(f) = 0 \qquad \text{and} \tag{1.7.5}$$

$$1^\star(f) = u_A \epsilon_C. \tag{1.7.6}$$

(c) *If $f, g \in \mathfrak{n}(C,A)$ satisfy $f \star g = g \star f$, then $f+g \in \mathfrak{n}(C,A)$.*

(d) *For any $\lambda \in \mathbf{k}$ and $f \in \mathfrak{n}(C,A)$, we have $\lambda f \in \mathfrak{n}(C,A)$.*

(e) *If $f \in \mathfrak{n}(C,A)$ and $g \in \mathrm{Hom}(C,A)$ satisfy $f \star g = g \star f$, then $f \star g \in \mathfrak{n}(C,A)$.*

(f) *If $v \in \mathbf{k}[[T]]$ is a power series whose constant term is 0, then $v^\star(f) \in \mathfrak{n}(C,A)$ for each $f \in \mathfrak{n}(C,A)$.*

(g) *If $u, v \in \mathbf{k}[[T]]$ are two power series such that the constant term of v is 0, and if $f \in \mathfrak{n}(C,A)$ is arbitrary, then*

$$(u[v])^\star(f) = u^\star(v^\star(f)). \tag{1.7.7}$$

Here, $u[v]$ denotes the composition *of u with v; this is the power series obtained by substituting v for T in u. (This power series is well-defined, since v has constant term 0.) Furthermore, notice that the right hand side of (1.7.7) is well-defined, since Proposition 1.7.11(f) shows that $v^\star(f) \in \mathfrak{n}(C,A)$.*

(h) *If C is a graded $\mathbf{k}$-coalgebra, and if $f \in \mathrm{Hom}(C,A)$ satisfies $f(C_0) = 0$, then $f \in \mathfrak{n}(C,A)$.*

(i) *If B is any $\mathbf{k}$-algebra, and if $s : A \to B$ is any $\mathbf{k}$-algebra homomorphism, then every $u \in \mathbf{k}[[T]]$ and $f \in \mathfrak{n}(C,A)$ satisfy*

$$s \circ f \in \mathfrak{n}(C,B) \qquad \text{and} \qquad u^\star(s \circ f) = s \circ (u^\star(f)).$$

(j) *If C is a connected graded $\mathbf{k}$-bialgebra, and if $F : C \to A$ is a $\mathbf{k}$-algebra homomorphism, then $F - u_A \epsilon_C \in \mathfrak{n}(C,A)$.*

Example 1.7.12. Let C be a graded $\mathbf{k}$-coalgebra. Let $f \in \mathrm{Hom}(C,A)$ be such that $f(C_0) = 0$. Then, we claim that the map $u_A\epsilon_C + f : C \to A$ is $\star$-invertible. (This observation has already been made in the proof of Proposition 1.4.24, at least in the particular case when $C = A$.)

Let us see how this claim follows from Proposition 1.7.11. First, Proposition 1.7.11(h) shows that $f \in \mathfrak{n}(C,A)$. Now, define a power series $u \in \mathbf{k}[[T]]$ by $u = 1 + T$. Then, the power series u has constant term 1, and thus has a multiplicative inverse $v = u^{-1} \in \mathbf{k}[[T]]$. Consider this v. (Explicitly, $v = \sum_{n\geq 0} (-1)^n T^n$, but this does not matter for us.) Now, (1.7.3) yields $(uv)^\star(f) = u^\star(f) \star v^\star(f)$. Since $uv = 1$ (because $v = u^{-1}$), we have $(uv)^\star(f) = 1^\star(f) = u_A\epsilon_C$ (by (1.7.6)). Thus, $u^\star(f) \star v^\star(f) = (uv)^\star(f) = u_A\epsilon_C$. Hence, the map $u^\star(f)$ has a right $\star$-inverse.

[57] See Exercise 1.7.13 below for the proofs of these properties.

Also, from $u = 1 + T$, we obtain

$$u^\star(f) = (1+T)^\star(f) = \underbrace{1^\star(f)}_{=u_A\epsilon_C} + \underbrace{T^\star(f)}_{=f^{\star 1}} \qquad \text{(by (1.7.2))}$$
$$\text{(by (1.7.1), applied to } k\text{=1)}$$
$$= u_A\epsilon_C + \underbrace{f^{\star 1}}_{=f} = u_A\epsilon_C + f.$$

Thus, the map $u_A\epsilon_C + f$ has a right $\star$-inverse (since the map $u^\star(f)$ has a right $\star$-inverse). A similar argument shows that this map $u_A\epsilon_C + f$ has a left $\star$-inverse. Consequently, the map $u_A\epsilon_C + f$ is $\star$-invertible.

Exercise 1.7.13. Prove Proposition 1.7.11.

Definition 1.7.14. (a) For the rest of Section 1.7, we assume that $\mathbf{k}$ is a commutative $\mathbb{Q}$-algebra. Thus, the two formal power series $\exp = \sum_{n\geq 0} \frac{1}{n!} T^n \in \mathbf{k}[[T]]$ and $\log(1+T) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} T^n \in \mathbf{k}[[T]]$ are well-defined.

(b) Define two power series $\overline{\exp} \in \mathbf{k}[[T]]$ and $\overline{\log} \in \mathbf{k}[[T]]$ by $\overline{\exp} = \exp - 1$ and $\overline{\log} = \log(1+T)$.

(c) If u and v are two power series in $\mathbf{k}[[T]]$ such that v has constant term 0, then $u[v]$ denotes the *composition* of u with v; this is the power series obtained by substituting v for T in u.

The following proposition is just a formal analogue of the well-known fact that the exponential function and the logarithm are mutually inverse (on their domains of definition):[58]

Proposition 1.7.15. *Both power series $\overline{\exp}$ and $\overline{\log}$ have constant term 0 and satisfy $\overline{\exp}\left[\overline{\log}\right] = T$ and $\overline{\log}\left[\overline{\exp}\right] = T$.*

For any map $f \in \mathfrak{n}(C, A)$, the power series exp, $\overline{\exp}$ and $\overline{\log}$ give rise to three further maps $\exp^\star f$, $\overline{\exp}^\star f$ and $\overline{\log}^\star f$. We can also define a map $\log^\star g$ whenever g is a map in $\mathrm{Hom}(C, A)$ satisfying $g - u_A\epsilon_C \in \mathfrak{n}(C, A)$ (but we cannot define $\log^\star f$ for $f \in \mathfrak{n}(C, A)$, since log is not per se a power series); in order to do this, we need a simple lemma:

Lemma 1.7.16. *Let $g \in \mathrm{Hom}(C, A)$ be such that $g - u_A\epsilon_C \in \mathfrak{n}(C, A)$. Then, $\overline{\log}^\star(g - u_A\epsilon_C)$ is a well-defined element of $\mathfrak{n}(C, A)$.*

Definition 1.7.17. If $g \in \mathrm{Hom}(C, A)$ is a map satisfying $g - u_A\epsilon_C \in \mathfrak{n}(C, A)$, then we define a map $\log^\star g \in \mathfrak{n}(C, A)$ by $\log^\star g = \overline{\log}^\star(g - u_A\epsilon_C)$. (This is well-defined, according to Lemma 1.7.16.)

Proposition 1.7.18. (a) *Each $f \in \mathfrak{n}(C, A)$ satisfies $\exp^\star f - u_A\epsilon_C \in \mathfrak{n}(C, A)$ and*

$$\log^\star(\exp^\star f) = f.$$

(b) *Each $g \in \mathrm{Hom}(C, A)$ satisfying $g - u_A\epsilon_C \in \mathfrak{n}(C, A)$ satisfies*

$$\exp^\star(\log^\star g) = g.$$

(c) *If $f, g \in \mathfrak{n}(C, A)$ satisfy $f \star g = g \star f$, then $f + g \in \mathfrak{n}(C, A)$ and $\exp^\star(f+g) = (\exp^\star f) \star (\exp^\star g)$.*

(d) *The $\mathbf{k}$-linear map $0 : C \to A$ satisfies $0 \in \mathfrak{n}(C, A)$ and $\exp^\star 0 = u_A\epsilon_C$.*

(e) *If $f \in \mathfrak{n}(C, A)$ and $n \in \mathbb{N}$, then $nf \in \mathfrak{n}(C, A)$ and $\exp^\star(nf) = (\exp^\star f)^{\star n}$.*

(f) *If $f \in \mathfrak{n}(C, A)$, then*

$$\log^\star(f + u_A\epsilon_C) = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} f^{\star n}. \tag{1.7.8}$$

Example 1.7.19. Consider again the Hopf algebra $\mathbf{k}[x]$ from Exercise 1.6.4. Let $c_1 : \mathbf{k}[x] \to \mathbf{k}$ be the $\mathbf{k}$-linear map sending each polynomial $p \in \mathbf{k}[x]$ to the coefficient of x^1 in p. (In other words, c_1 sends each polynomial $p \in \mathbf{k}[x]$ to its derivative at 0.)

Then, $c_1((\mathbf{k}[x])_0) = 0$ (as can easily be seen). Hence, Proposition 1.7.11(h) shows that $c_1 \in \mathfrak{n}(\mathbf{k}[x], \mathbf{k})$. Thus, a map $\exp^\star(c_1) : \mathbf{k}[x] \to \mathbf{k}$ is well-defined. It is not hard to see that this map is explicitly given by

$$(\exp^\star(c_1))(p) = p(1) \qquad \text{for every } p \in \mathbf{k}[x].$$

[58] See Exercise 1.7.20 below for the proof of this proposition, as well as of the lemma and proposition that follow afterwards.

(In fact, this follows easily after showing that each $n \in \mathbb{N}$ satisfies

$$(c_1)^{\star n}(p) = n! \cdot (\text{the coefficient of } x^n \text{ in } p) \qquad \text{for every } p \in \mathbf{k}[x],$$

which in turn is easily seen by induction.)

Note that the equality $(\exp^\star(c_1))(p) = p(1)$ shows that the map $\exp^\star(c_1)$ is a $\mathbf{k}$-algebra homomorphism. This is a particular case of a fact that we will soon see (Proposition 1.7.23).

Exercise 1.7.20. Prove Proposition 1.7.15, Lemma 1.7.16 and Proposition 1.7.18.

Next, we state another sequence of facts (some of which have nothing to do with Hopf algebras), beginning with a fact about convolutions which is similar to Proposition 1.4.3:[59]

Proposition 1.7.21. *Let C and C' be two $\mathbf{k}$-coalgebras, and let A and A' be two $\mathbf{k}$-algebras. Let $\gamma : C \to C'$ be a $\mathbf{k}$-coalgebra morphism. Let $\alpha : A \to A'$ be a $\mathbf{k}$-algebra morphism.*

(a) *If $f \in \operatorname{Hom}(C, A)$, $g \in \operatorname{Hom}(C, A)$, $f' \in \operatorname{Hom}(C', A')$ and $g' \in \operatorname{Hom}(C', A')$ satisfy $f' \circ \gamma = \alpha \circ f$ and $g' \circ \gamma = \alpha \circ g$, then $(f' \star g') \circ \gamma = \alpha \circ (f \star g)$.*

(b) *If $f \in \operatorname{Hom}(C, A)$ and $f' \in \operatorname{Hom}(C', A')$ satisfy $f' \circ \gamma = \alpha \circ f$, then each $n \in \mathbb{N}$ satisfies $(f')^{\star n} \circ \gamma = \alpha \circ f^{\star n}$.*

Proposition 1.7.22. *Let C be a $\mathbf{k}$-bialgebra. Let A be a commutative $\mathbf{k}$-algebra. Let $f \in \operatorname{Hom}(C, A)$ be such that $f\left((\ker\epsilon)^2\right) = 0$ and $f(1) = 0$. Then, any $x, y \in C$ and $n \in \mathbb{N}$ satisfy*

$$f^{\star n}(xy) = \sum_{i=0}^{n} \binom{n}{i} f^{\star i}(x)\, f^{\star(n-i)}(y).$$

Proposition 1.7.23. *Let C be a $\mathbf{k}$-bialgebra. Let A be a commutative $\mathbf{k}$-algebra. Let $f \in \mathfrak{n}(C, A)$ be such that $f\left((\ker\epsilon)^2\right) = 0$ and $f(1) = 0$. Then, $\exp^\star f : C \to A$ is a $\mathbf{k}$-algebra homomorphism.*

Lemma 1.7.24. *Let V be any torsionfree abelian group (written additively). Let $N \in \mathbb{N}$. For every $k \in \{0, 1, \ldots, N\}$, let w_k be an element of V. Assume that*

$$\sum_{k=0}^{N} w_k n^k = 0 \qquad \text{for all } n \in \mathbb{N}. \tag{1.7.9}$$

Then, $w_k = 0$ for every $k \in \{0, 1, \ldots, N\}$.

Lemma 1.7.25. *Let V be a torsionfree abelian group (written additively). Let $(w_k)_{k\in\mathbb{N}} \in V^{\mathbb{N}}$ be a finitely supported family of elements of V. Assume that*

$$\sum_{k\in\mathbb{N}} w_k n^k = 0 \qquad \text{for all } n \in \mathbb{N}.$$

Then, $w_k = 0$ for every $k \in \mathbb{N}$.

Proposition 1.7.26. *Let C be a graded $\mathbf{k}$-bialgebra. Let A be a commutative $\mathbf{k}$-algebra. Let $f \in \operatorname{Hom}(C, A)$ be such that $f(C_0) = 0$. Assume that[60] $\exp^\star f : C \to A$ is a $\mathbf{k}$-algebra homomorphism. Then, $f\left((\ker\epsilon)^2\right) = 0$.*

Proposition 1.7.27. *Let C be a connected graded $\mathbf{k}$-bialgebra. Let A be a commutative $\mathbf{k}$-algebra. Let $f \in \mathfrak{n}(C, A)$ be such that $f\left((\ker\epsilon)^2\right) = 0$ and $f(1) = 0$. Assume further that $f(C)$ generates the $\mathbf{k}$-algebra A. Then, $\exp^\star f : C \to A$ is a surjective $\mathbf{k}$-algebra homomorphism.*

Exercise 1.7.28. Prove Lemmas 1.7.24 and 1.7.25 and Propositions 1.7.21, 1.7.22, 1.7.23, 1.7.26 and 1.7.27.

[**Hint:** For Proposition 1.7.26, show first that $\exp^\star(nf) = (\exp^\star f)^{\star n}$ is a $\mathbf{k}$-algebra homomorphism for each $n \in \mathbb{N}$. Turn this into an equality between polynomials in n, and use Lemma 1.7.25.]

With these preparations, we can state our version of Leray's theorem:

[59] See Exercise 1.7.28 below for their proofs.

[60] Notice that $\exp^\star f$ is well-defined, since Proposition 1.7.11(h) yields $f \in \mathfrak{n}(C, A)$.

Theorem 1.7.29. *Let A be a commutative connected graded $\mathbf{k}$-bialgebra.*[61]

(a) *We have $\mathrm{id}_A - u_A \epsilon_A \in \mathfrak{n}(A, A)$; thus, the map $\log^\star(\mathrm{id}_A) \in \mathfrak{n}(A, A)$ is well-defined. We denote this map $\log^\star(\mathrm{id}_A)$ by $\mathfrak{e}$.*

(b) *We have $\ker \mathfrak{e} = \mathbf{k} \cdot 1_A + (\ker \epsilon)^2$ and $\mathfrak{e}(A) \cong (\ker \epsilon) / (\ker \epsilon)^2$ (as $\mathbf{k}$-modules).*

(c) *For each $\mathbf{k}$-module V, let ι_V be the canonical inclusion $V \to \operatorname{Sym} V$. Let $\mathfrak{q}$ be the map*

$$A \xrightarrow{\mathfrak{e}} \mathfrak{e}(A) \xrightarrow{\iota_{\mathfrak{e}(A)}} \operatorname{Sym}(\mathfrak{e}(A)).$$

Then, $\mathfrak{q} \in \mathfrak{n}(A, \operatorname{Sym}(\mathfrak{e}(A)))$ [62].

(d) *Let $\mathbf{i}$ be the canonical inclusion $\mathfrak{e}(A) \to A$. Recall the universal property of the symmetric algebra: If V is a $\mathbf{k}$-module, if W is a commutative $\mathbf{k}$-algebra, and if $\varphi : V \to W$ is any $\mathbf{k}$-linear map, then there exists a unique $\mathbf{k}$-algebra homomorphism $\Phi : \operatorname{Sym} V \to W$ satisfying $\varphi = \Phi \circ \iota_V$. Applying this to $V = \mathfrak{e}(A)$, $W = A$ and $\varphi = \mathbf{i}$, we conclude that there exists a unique $\mathbf{k}$-algebra homomorphism $\Phi : \operatorname{Sym}(\mathfrak{e}(A)) \to A$ satisfying $\mathbf{i} = \Phi \circ \iota_{\mathfrak{e}(A)}$. Denote this Φ by $\mathfrak{s}$. Then, the maps $\exp^\star \mathfrak{q} : A \to \operatorname{Sym}(\mathfrak{e}(A))$ and $\mathfrak{s} : \operatorname{Sym}(\mathfrak{e}(A)) \to A$ are mutually inverse $\mathbf{k}$-algebra isomorphisms.*

(e) *We have $A \cong \operatorname{Sym}\left((\ker \epsilon) / (\ker \epsilon)^2\right)$ as $\mathbf{k}$-algebras.*

(f) *The map $\mathfrak{e} : A \to A$ is a projection (i.e., it satisfies $\mathfrak{e} \circ \mathfrak{e} = \mathfrak{e}$).*

Remark 1.7.30. (a) The main upshot of Theorem 1.7.29 is that any commutative connected graded $\mathbf{k}$-bialgebra A (where $\mathbf{k}$ is a commutative $\mathbb{Q}$-algebra) is isomorphic **as a k-algebra** to the symmetric algebra $\operatorname{Sym} W$ of some $\mathbf{k}$-module W. (Specifically, Theorem 1.7.29(e) claims this for $W = (\ker \epsilon) / (\ker \epsilon)^2$, whereas Theorem 1.7.29(d) claims this for $W = \mathfrak{e}(A)$; these two modules W are isomorphic by Theorem 1.7.29(b).) This is a useful statement even without any specific knowledge about W, since symmetric algebras are a far tamer class of algebras than arbitrary commutative algebras. For example, if $\mathbf{k}$ is a field, then symmetric algebras are just polynomial algebras (up to isomorphism). This can be applied, for example, to the case of the shuffle algebra $\operatorname{Sh}(V)$ of a $\mathbf{k}$-module V. The consequence is that the shuffle algebra $\operatorname{Sh}(V)$ of any $\mathbf{k}$-module V (where $\mathbf{k}$ is a commutative $\mathbb{Q}$-algebra) is isomorphic **as a k-algebra** to a symmetric algebra $\operatorname{Sym} W$. When V is a free $\mathbf{k}$-module, one can actually show that $\operatorname{Sh}(V)$ is isomorphic **as a k-algebra** to the symmetric algebra of a **free** $\mathbf{k}$-module W (that is, to a polynomial ring over $\mathbf{k}$); however, this W is not easy to characterize. Such a characterization is given by *Radford's theorem* (Theorem 6.3.4 below) using the concept of *Lyndon words*. Notice that if V has rank ≥ 2, then W is not finitely generated.

(b) The isomorphism in Theorem 1.7.29(e) is generally not an isomorphism of Hopf algebras. However, with a little (rather straightforward) work, it reveals to be an isomorphism of **graded** $\mathbf{k}$-algebras. Actually, all maps mentioned in Theorem 1.7.29 are graded, provided that we use the appropriate gradings for $\mathfrak{e}(A)$ and $\operatorname{Sym}(\mathfrak{e}(A))$. (To define the appropriate grading for $\mathfrak{e}(A)$, we must show that $\mathfrak{e}$ is a graded map, whence $\mathfrak{e}(A)$ is a homogeneous submodule of A; this provides $\mathfrak{e}(A)$ with the grading we seek. The grading on $\operatorname{Sym}(\mathfrak{e}(A))$ then follows from the usual definition of the grading on the symmetric algebra $\operatorname{Sym} V$ of a graded $\mathbf{k}$-module V: Namely, if V is a graded $\mathbf{k}$-module, then the n-th graded component of $\operatorname{Sym} V$ is defined to be the span of all products of the form $v_1 v_2 \cdots v_k \in \operatorname{Sym} V$, where $v_1, v_2, \ldots, v_k \in V$ are homogeneous elements satisfying $\deg(v_1) + \deg(v_2) + \cdots + \deg(v_k) = n$.)

(c) The map $\mathfrak{e} : A \to A$ from Theorem 1.7.29 is called the *Eulerian idempotent* of A.

(d) Theorem 1.7.29 is concerned with commutative bialgebras. Most of its claims have a "dual version", concerning cocommutative bialgebras. Again, the Eulerian idempotent plays a crucial role; but the result characterizes not the $\mathbf{k}$-algebra structure on A, but the $\mathbf{k}$-coalgebra structure on A. This leads to the Cartier-Milnor-Moore theorem; see [35, §3.8] and [60, §3.2]. We shall say a bit about the Eulerian idempotent for a cocommutative bialgebra in Exercises 5.4.6 and 5.4.8.

Example 1.7.31. Consider the symmetric algebra $\operatorname{Sym} V$ of a $\mathbf{k}$-module V. Then, $\operatorname{Sym} V$ is a commutative connected graded $\mathbf{k}$-bialgebra, and thus Theorem 1.7.29 can be applied to $A = \operatorname{Sym} V$. What is the projection $\mathfrak{e} : A \to A$ obtained in this case?

[61] Keep in mind that $\mathbf{k}$ is assumed to be a commutative $\mathbb{Q}$-algebra.

[62] Do not mistake the map $\mathfrak{q}$ for $\mathfrak{e}$. While every $a \in A$ satisfies $\mathfrak{q}(a) = \mathfrak{e}(a)$, the two maps $\mathfrak{q}$ and $\mathfrak{e}$ have different target sets, and thus we do **not** have $(\exp^\star \mathfrak{q})(a) = (\exp^\star \mathfrak{e})(a)$ for every $a \in A$.

Theorem 1.7.29(b) shows that its kernel is

$$\operatorname{Ker}\mathfrak{e} = \underbrace{\mathbf{k}\cdot 1_A}_{=\operatorname{Sym}^0 V} + \underbrace{(\ker\epsilon)^2}_{=\sum_{n\geq 2}\operatorname{Sym}^n V} = \operatorname{Sym}^0 V + \sum_{n\geq 2}\operatorname{Sym}^n V = \sum_{n\neq 1}\operatorname{Sym}^n V. \tag{1.7.10}$$

This does not yet characterize $\mathfrak{e}$ completely, because we have yet to determine the action of $\mathfrak{e}$ on $\operatorname{Sym}^1 V$. Fortunately, the elements of $\operatorname{Sym}^1 V$ are all primitive (recall that $\Delta_{\operatorname{Sym} V}(v) = 1\otimes v + v\otimes 1$ for each $v\in V$), and it can easily be shown that the map $\mathfrak{e}$ fixes any primitive element of A [63]. Therefore, the map $\mathfrak{e}$ fixes all elements of $\operatorname{Sym}^1 V$. Since we also know that $\mathfrak{e}$ annihilates all elements of $\sum_{n\neq 1}\operatorname{Sym}^n V$ (by (1.7.10)), we thus conclude that $\mathfrak{e}$ is the canonical projection from the direct sum $\operatorname{Sym} V = \bigoplus_{n\in\mathbb{N}}\operatorname{Sym}^n V$ onto its addend $\operatorname{Sym}^1 V$.

Example 1.7.32. For this example, let A be the shuffle algebra $\operatorname{Sh}(V)$ of a $\mathbf{k}$-module V. (See Proposition 1.6.7 for its definition, and keep in mind that its product is being denoted by $\sqcup\!\sqcup$, whereas the notation uv is still being used for the product of two elements u and v in the **tensor** algebra $T(V)$.)

Theorem 1.7.29 can be applied to $A = \operatorname{Sh}(V)$. What is the projection $\mathfrak{e}: A\to A$ obtained in this case?

Let us compute $\mathfrak{e}(v_1v_2)$ for two elements $v_1, v_2\in V$. Indeed, define a map $\widetilde{\mathrm{id}}: A\to A$ by $\widetilde{\mathrm{id}} = \mathrm{id}_A - u_A\epsilon_A$. Then, $\widetilde{\mathrm{id}}\in\mathfrak{n}(A,A)$ and $\log^\star\left(\underbrace{\widetilde{\mathrm{id}}+u_A\epsilon_A}_{=\mathrm{id}_A}\right) = \log^\star(\mathrm{id}_A) = \mathfrak{e}$. Hence, (1.7.8) (applied to $C=A$ and $f=\widetilde{\mathrm{id}}$) shows that

$$\mathfrak{e} = \sum_{n\geq 1}\frac{(-1)^{n-1}}{n}\widetilde{\mathrm{id}}^{\star n}. \tag{1.7.11}$$

Thus, we need to compute $\widetilde{\mathrm{id}}^{\star n}(v_1v_2)$ for each $n\geq 1$.

Notice that the map $\widetilde{\mathrm{id}}$ annihilates A_0, but fixes any element of A_k for $k>0$. Thus,

$$\widetilde{\mathrm{id}}(w_1w_2\cdots w_k) = \begin{cases} w_1w_2\cdots w_k, & \text{if } k>0;\\ 0, & \text{if } k=0\end{cases} \qquad \text{for any } w_1,w_2,\ldots,w_k\in V.$$

But it is easy to see that the map $\widetilde{\mathrm{id}}^{\star n}: A\to A$ annihilates A_k whenever $n>k$. In particular, for every $n>2$, the map $\widetilde{\mathrm{id}}^{\star n}: A\to A$ annihilates A_2, and therefore satisfies

$$\widetilde{\mathrm{id}}^{\star n}(v_1v_2) = 0 \qquad (\text{since } v_1v_2\in A_2). \tag{1.7.12}$$

It remains to find $\widetilde{\mathrm{id}}^{\star n}(v_1v_2)$ for $n\in\{1,2\}$.

We have $\widetilde{\mathrm{id}}^{\star 1} = \widetilde{\mathrm{id}}$ and thus

$$\widetilde{\mathrm{id}}^{\star 1}(v_1v_2) = \widetilde{\mathrm{id}}(v_1v_2) = v_1v_2$$

and

$$\begin{aligned}\widetilde{\mathrm{id}}^{\star 2}(v_1v_2) &= \underbrace{\widetilde{\mathrm{id}}(1)}_{=0}\sqcup\!\sqcup\underbrace{\widetilde{\mathrm{id}}(v_1v_2)}_{=v_1v_2} + \underbrace{\widetilde{\mathrm{id}}(v_1)}_{=v_1}\sqcup\!\sqcup\underbrace{\widetilde{\mathrm{id}}(v_2)}_{=v_2} + \underbrace{\widetilde{\mathrm{id}}(v_1v_2)}_{=v_1v_2}\sqcup\!\sqcup\underbrace{\widetilde{\mathrm{id}}(1)}_{=0}\\ &\qquad (\text{since } \Delta_{\operatorname{Sh}V}(v_1v_2) = 1\otimes v_1v_2 + v_1\otimes v_2 + v_1v_2\otimes 1)\\ &= \underbrace{0\sqcup\!\sqcup(v_1v_2)}_{=0} + \underbrace{v_1\sqcup\!\sqcup v_2}_{=v_1v_2+v_2v_1} + \underbrace{(v_1v_2)\sqcup\!\sqcup 0}_{=0}\\ &= v_1v_2 + v_2v_1.\end{aligned}$$

[63] See Exercise 5.4.6(f) further below for this proof. (While Exercise 5.4.6 requires A to be cocommutative, this requirement is not used in the solution to Exercise 5.4.6(f). That said, this requirement is actually satisfied for $A = \operatorname{Sym} V$, so we do not even need to avoid it here.)

Now, applying both sides of (1.7.11) to v_1v_2, we find

$$\begin{aligned}
&\mathfrak{e}(v_1v_2) \\
&= \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}(v_1v_2) = \underbrace{\frac{(-1)^{1-1}}{1}}_{=1} \underbrace{\widetilde{\mathrm{id}}^{\star 1}(v_1v_2)}_{=v_1v_2} + \underbrace{\frac{(-1)^{2-1}}{2}}_{=\frac{-1}{2}} \underbrace{\widetilde{\mathrm{id}}^{\star 2}(v_1v_2)}_{=v_1v_2+v_2v_1} + \sum_{n\geq 3} \frac{(-1)^{n-1}}{n} \underbrace{\widetilde{\mathrm{id}}^{\star n}(v_1v_2)}_{\substack{=0 \\ \text{(by (1.7.12))}}} \\
&= v_1v_2 + \frac{-1}{2}(v_1v_2+v_2v_1) + \underbrace{\sum_{n\geq 3} \frac{(-1)^{n-1}}{n} 0}_{=0} = \frac{1}{2}(v_1v_2 - v_2v_1).
\end{aligned}$$

This describes the action of $\mathfrak{e}$ on the graded component A_2 of $A = \mathrm{Sh}(V)$.

Similarly, we can describe $\mathfrak{e}$ acting on any other graded component:

$$\begin{aligned}
\mathfrak{e}(1) &= 0; \\
\mathfrak{e}(v_1) &= v_1 \qquad \text{for each } v_1 \in V; \\
\mathfrak{e}(v_1v_2) &= \frac{1}{2}(v_1v_2 - v_2v_1) \qquad \text{for any } v_1, v_2 \in V; \\
\mathfrak{e}(v_1v_2v_3) &= \frac{1}{6}(2v_1v_2v_3 - v_1v_3v_2 - v_2v_1v_3 - v_2v_3v_1 - v_3v_1v_2 + 2v_3v_2v_1) \qquad \text{for any } v_1, v_2, v_3 \in V, \\
&\cdots.
\end{aligned}$$

With some more work, one can show the following formula for the action of $\mathfrak{e}$ on any nontrivial pure tensor:

$$\begin{aligned}
\mathfrak{e}(v_1v_2\cdots v_n) &= \sum_{\sigma\in\mathfrak{S}_n} \left(\sum_{k=1+\mathrm{des}(\sigma^{-1})}^{n} \frac{(-1)^{k-1}}{k} \binom{n-1-\mathrm{des}(\sigma^{-1})}{k-1-\mathrm{des}(\sigma^{-1})} \right) v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \\
&= \sum_{\sigma\in\mathfrak{S}_n} \frac{(-1)^{\mathrm{des}(\sigma^{-1})}}{\mathrm{des}(\sigma^{-1})+1} \binom{n}{\mathrm{des}(\sigma^{-1})+1}^{-1} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \\
&\qquad \text{for any } n \geq 1 \text{ and } v_1, v_2, \ldots, v_n \in V,
\end{aligned}$$

where we use the notation $\mathrm{des}\,\pi$ for the number of descents[64] of any permutation $\pi \in \mathfrak{S}_n$. (A statement essentially dual to this appears in [191, Theorem 9.5].)

Theorem 1.7.29(b) yields $\ker\mathfrak{e} = \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. Notice, however, that $(\ker\epsilon)^2$ means the square of the ideal $\ker\epsilon$ with respect to the shuffle multiplication $\sqcup\!\sqcup$; thus, $(\ker\epsilon)^2$ is the $\mathbf{k}$-linear span of all shuffle products of the form $a \sqcup\!\sqcup b$ with $a \in \ker\epsilon$ and $b \in \ker\epsilon$.

Exercise 1.7.33. Prove Theorem 1.7.29.

[**Hint:** (a) is easy. For (b), define an element $\widetilde{\mathrm{id}}$ of $\mathfrak{n}(A,A)$ by $\widetilde{\mathrm{id}} = \mathrm{id}_A - u_A\epsilon_A$. Observe that $\mathfrak{e} = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}$, and draw the conclusions that $\mathfrak{e}(1_A) = 0$ and that each $x \in A$ satisfies $\widetilde{\mathrm{id}}(x) - \mathfrak{e}(x) \in (\ker\epsilon)^2$ (because $\widetilde{\mathrm{id}}^{\star n}(x) \in (\ker\epsilon)^2$ for every $n \geq 2$). Use this to prove $\ker\mathfrak{e} \subset \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. On the other hand, prove $\mathfrak{e}\left((\ker\epsilon)^2\right) = 0$ by applying Proposition 1.7.26. Combine to obtain $\ker\mathfrak{e} = \mathbf{k}\cdot 1_A + (\ker\epsilon)^2$. Finish (b) by showing that $A/\left(\mathbf{k}\cdot 1_A + (\ker\epsilon)^2\right) \cong (\ker\epsilon)/(\ker\epsilon)^2$ as $\mathbf{k}$-modules. Part (c) is easy again. For (d), first apply Proposition 1.7.11(i) to show that $\exp^\star(\mathfrak{s}\circ\mathfrak{q}) = \mathfrak{s}\circ(\exp^\star\mathfrak{q})$. In light of $\mathfrak{s}\circ\mathfrak{q} = \mathfrak{e}$ and $\exp^\star\mathfrak{e} = \mathrm{id}_A$, this becomes $\mathrm{id}_A = \mathfrak{s}\circ(\exp^\star\mathfrak{q})$. To obtain part (d), it remains to show that $\exp^\star\mathfrak{q}$ is a surjective $\mathbf{k}$-algebra homomorphism; but this follows from Proposition 1.7.27. For (e), combine (d) and (b). For (f), use once again the observation that each $x \in A$ satisfies $\widetilde{\mathrm{id}}(x) - \mathfrak{e}(x) \in (\ker\epsilon)^2$.]

[64] A *descent* of a permutation $\pi \in \mathfrak{S}_n$ means an $i \in \{1, 2, \ldots, n-1\}$ satisfying $\pi(i) > \pi(i+1)$.

2. Review of symmetric functions Λ as Hopf algebra

Here we review the ring of symmetric functions, borrowing heavily from standard treatments, such as Macdonald [142, Chap. I], Sagan [186, Chap. 4], Stanley [206, Chap. 7], and Mendes and Remmel [154], but emphasizing the Hopf structure early on. Other recent references for this subject are [224], [189], [63], [153, Chapters 2–3] and [187, Chapter 7].

2.1. **Definition of Λ.** As before, $\mathbf{k}$ here is a commutative ring (hence could be a field or the integers $\mathbb{Z}$; these are the usual choices).

Given an infinite variable set $\mathbf{x} = (x_1, x_2, \ldots)$, a monomial $\mathbf{x}^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots$ is indexed by a sequence $\alpha = (\alpha_1, \alpha_2, \ldots)$ in $\mathbb{N}^\infty$ having finite support[65]; such sequences α are called *weak compositions*. The nonzero entries of the sequence $\alpha = (\alpha_1, \alpha_2, \ldots)$ are called the *parts* of the weak composition α.

The sum $\alpha_1 + \alpha_2 + \alpha_3 + \cdots$ of all entries of a weak composition $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots)$ (or, equivalently, the sum of all parts of α) is called the *size* of α and denoted by $|\alpha|$.

Consider the $\mathbf{k}$-algebra $\mathbf{k}[[\mathbf{x}]] := \mathbf{k}[[x_1, x_2, x_3, \ldots]]$ of all formal power series in the indeterminates $x_1, x_2, x_3, \ldots$ over $\mathbf{k}$; these series are infinite $\mathbf{k}$-linear combinations $\sum_\alpha c_\alpha \mathbf{x}^\alpha$ (with c_α in $\mathbf{k}$) of the monomials $\mathbf{x}^\alpha$ where α ranges over all weak compositions. The product of two such formal power series is well-defined by the usual multiplication rule.

The *degree* of a monomial $\mathbf{x}^\alpha$ is defined to be the number $\deg(\mathbf{x}^\alpha) := \sum_i \alpha_i \in \mathbb{N}$. Given a number $d \in \mathbb{N}$, we say that a formal power series $f(\mathbf{x}) = \sum_\alpha c_\alpha \mathbf{x}^\alpha \in \mathbf{k}[[\mathbf{x}]]$ (with c_α in $\mathbf{k}$) is *homogeneous of degree d* if every weak composition α satisfying $\deg(\mathbf{x}^\alpha) \neq d$ must satisfy $c_\alpha = 0$. In other words, a formal power series is homogeneous of degree d if it is an infinite $\mathbf{k}$-linear combination of monomials of degree d. Every formal power series $f \in \mathbf{k}[[\mathbf{x}]]$ can be uniquely represented as an infinite sum $f_0 + f_1 + f_2 + \cdots$, where each f_d is homogeneous of degree d; in this case, we refer to each f_d as the *d-th homogeneous component of f*. Note that this does not make $\mathbf{k}[[\mathbf{x}]]$ into a graded $\mathbf{k}$-module, since these sums $f_0 + f_1 + f_2 + \cdots$ can have infinitely many nonzero addends. Nevertheless, if f and g are homogeneous power series of degrees d and e, then fg is homogeneous of degree $d + e$.

A formal power series $f(\mathbf{x}) = \sum_\alpha c_\alpha \mathbf{x}^\alpha \in \mathbf{k}[[\mathbf{x}]]$ (with c_α in $\mathbf{k}$) is said to be *of bounded degree* if there exists some bound $d = d(f) \in \mathbb{N}$ such that every weak composition $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots)$ satisfying $\deg(\mathbf{x}^\alpha) > d$ must satisfy $c_\alpha = 0$. Equivalently, a formal power series $f \in \mathbf{k}[[\mathbf{x}]]$ is of bounded degree if all but finitely many of its homogeneous components are zero. (For example, $x_1^2 + x_2^2 + x_3^2 + \cdots$ and $1 + x_1 + x_2 + x_3 + \cdots$ are of bounded degree, while $x_1 + x_1 x_2 + x_1 x_2 x_3 + \cdots$ and $1 + x_1 + x_1^2 + x_1^3 + \cdots$ are not.) It is easy to see that the sum and the product of two power series of bounded degree also have bounded degree. Thus, the formal power series of bounded degree form a $\mathbf{k}$-subalgebra of $\mathbf{k}[[\mathbf{x}]]$, which we call $R(\mathbf{x})$. This subalgebra $R(\mathbf{x})$ is graded (by degree).

The symmetric group $\mathfrak{S}_n$ permuting the first n variables $x_1, \ldots, x_n$ acts as a group of automorphisms on $R(\mathbf{x})$, as does the union $\mathfrak{S}_{(\infty)} = \bigcup_{n \geq 0} \mathfrak{S}_n$ of the infinite ascending chain $\mathfrak{S}_0 \subset \mathfrak{S}_1 \subset \mathfrak{S}_2 \subset \cdots$ of symmetric groups[66]. This group $\mathfrak{S}_{(\infty)}$ can also be described as the group of all permutations of the set $\{1, 2, 3, \ldots\}$ which leave all but finitely many elements invariant. It is known as the *finitary symmetric group* on $\{1, 2, 3, \ldots\}$.

The group $\mathfrak{S}_{(\infty)}$ also acts on the set of all weak compositions by permuting their entries:

$$\sigma(\alpha_1, \alpha_2, \alpha_3, \ldots) = \left(\alpha_{\sigma^{-1}(1)}, \alpha_{\sigma^{-1}(2)}, \alpha_{\sigma^{-1}(3)}, \ldots\right)$$
$$\text{for any weak composition } (\alpha_1, \alpha_2, \alpha_3, \ldots) \text{ and any } \sigma \in \mathfrak{S}_{(\infty)}.$$

These two actions are connected by the equality $\sigma(\mathbf{x}^\alpha) = \mathbf{x}^{\sigma\alpha}$ for any weak composition α and any $\sigma \in \mathfrak{S}_{(\infty)}$.

---

[65] The *support* of a sequence $\alpha = (\alpha_1, \alpha_2, \alpha_3, \ldots) \in \mathbb{N}^\infty$ is defined to be the set of all positive integers i for which $\alpha_i \neq 0$.

[66] This ascending chain is constructed as follows: For every $n \in \mathbb{N}$, there is an injective group homomorphism $\iota_n : \mathfrak{S}_n \to \mathfrak{S}_{n+1}$ which sends every permutation $\sigma \in \mathfrak{S}_n$ to the permutation $\iota_n(\sigma) = \tau \in \mathfrak{S}_{n+1}$ defined by

$$\tau(i) = \begin{cases} \sigma(i), & \text{if } i \leq n; \\ i, & \text{if } i = n+1 \end{cases} \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}.$$

These homomorphisms ι_n for all n form a chain $\mathfrak{S}_0 \xrightarrow{\iota_0} \mathfrak{S}_1 \xrightarrow{\iota_1} \mathfrak{S}_2 \xrightarrow{\iota_2} \cdots$, which is often regarded as a chain of inclusions.

Definition 2.1.1. The *ring of symmetric functions in* $\mathbf{x}$ *with coefficients in* $\mathbf{k}$, denoted $\Lambda = \Lambda_{\mathbf{k}} = \Lambda(\mathbf{x}) = \Lambda_{\mathbf{k}}(\mathbf{x})$, is the $\mathfrak{S}_{(\infty)}$-invariant subalgebra $R(\mathbf{x})^{\mathfrak{S}_{(\infty)}}$ of $R(\mathbf{x})$:

$$\begin{aligned}\Lambda &:= \left\{ f \in R(\mathbf{x}) : \sigma(f) = f \text{ for all } \sigma \in \mathfrak{S}_{(\infty)} \right\} \\ &= \left\{ f = \sum_{\alpha} c_\alpha \mathbf{x}^\alpha \in R(\mathbf{x}) : c_\alpha = c_\beta \text{ if } \alpha, \beta \text{ lie in the same } \mathfrak{S}_{(\infty)}\text{-orbit} \right\}.\end{aligned}$$

We refer to the elements of Λ as *symmetric functions* (over $\mathbf{k}$); however, despite this terminology, they are not functions in the usual sense.[67]

Note that Λ is a graded $\mathbf{k}$-algebra, since $\Lambda = \bigoplus_{n \geq 0} \Lambda_n$ where Λ_n are the symmetric functions $f = \sum_\alpha c_\alpha \mathbf{x}^\alpha$ which are *homogeneous of degree* n, meaning $\deg(\mathbf{x}^\alpha) = n$ for all $c_\alpha \neq 0$.

Exercise 2.1.2. Let $f \in R(\mathbf{x})$. Let A be a commutative $\mathbf{k}$-algebra, and $a_1, a_2, \ldots, a_k$ be finitely many elements of A. Show that substituting $a_1, a_2, \ldots, a_k, 0, 0, 0, \ldots$ for $x_1, x_2, x_3, \ldots$ in f yields an infinite sum in which all but finitely many addends are zero. Hence, this sum has a value in A, which is commonly denoted by $f(a_1, a_2, \ldots, a_k)$.

Definition 2.1.3. A *partition* $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell, 0, 0, \ldots)$ is a weak composition whose entries weakly decrease: $\lambda_1 \geq \cdots \geq \lambda_\ell > 0$. The (uniquely defined) ℓ is said to be the *length* of the partition λ and denoted by $\ell(\lambda)$. Thus, $\ell(\lambda)$ is the number of parts[68] of λ. One sometimes omits trailing zeroes from a partition: e.g., one can write the partition $(3, 1, 0, 0, 0, \ldots)$ as $(3, 1)$. We will often (but not always) write λ_i for the i-th entry of the partition λ (for instance, if $\lambda = (5, 3, 1, 1)$, then $\lambda_2 = 3$ and $\lambda_5 = 0$). If λ_i is nonzero, we will also call it the *i-th part* of λ. The sum $\lambda_1 + \lambda_2 + \cdots + \lambda_\ell = \lambda_1 + \lambda_2 + \cdots$ (where $\ell = \ell(\lambda)$) of all entries of λ (or, equivalently, of all parts of λ) is the size $|\lambda|$ of λ. For a given integer n, the partitions of size n are referred to as the *partitions of* n. The empty partition $() = (0, 0, 0, \ldots)$ is denoted by $\varnothing$.

Partitions (as defined above) are sometimes called *integer partitions* in order to distinguish them from set partitions.

Every weak composition α lies in the $\mathfrak{S}_{(\infty)}$-orbit of a unique partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell, 0, 0, \ldots)$ with $\lambda_1 \geq \cdots \geq \lambda_\ell > 0$. For any partition λ, define the *monomial symmetric function*

$$m_\lambda := \sum_{\alpha \in \mathfrak{S}_{(\infty)}\lambda} \mathbf{x}^\alpha. \tag{2.1.1}$$

Letting λ run through the set Par of all partitions, this gives the *monomial* $\mathbf{k}$*-basis* $\{m_\lambda\}$ of Λ. Letting λ run only through the set Par_n of partitions of n gives the monomial $\mathbf{k}$-basis for Λ_n.

Example 2.1.4. For $n = 3$, one has

$$\begin{aligned} m_{(3)} &= x_1^3 + x_2^3 + x_3^3 + \cdots, \\ m_{(2,1)} &= x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + \cdots, \\ m_{(1,1,1)} &= x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4 + x_1 x_2 x_5 + \cdots. \end{aligned}$$

The monomial basis $\{m_\lambda\}_{\lambda \in \mathrm{Par}}$ of Λ is thus a graded basis[69] of the graded $\mathbf{k}$-module Λ. (Here and in the following, when we say that a basis $\{u_\lambda\}_{\lambda \in \mathrm{Par}}$ indexed by Par is a graded basis of Λ, we tacitly understand that Par is partitioned into $\mathrm{Par}_0, \mathrm{Par}_1, \mathrm{Par}_2, \ldots$, so that for each $n \in \mathbb{N}$, the subfamily $\{u_\lambda\}_{\lambda \in \mathrm{Par}_n}$ should be a basis for Λ_n.)

Remark 2.1.5. We have defined the symmetric functions as the elements of $R(\mathbf{x})$ invariant under the group $\mathfrak{S}_{(\infty)}$. However, they also are the elements of $R(\mathbf{x})$ invariant under the group $\mathfrak{S}_\infty$ of *all* permutations of the set $\{1, 2, 3, \ldots\}$ (which acts on $R(\mathbf{x})$ in the same way as its subgroup $\mathfrak{S}_{(\infty)}$ does).[70]

---

[67] Being power series, they can be evaluated at appropriate families of variables. But this does not make them functions (no more than polynomials are functions). The terminology "symmetric function" is thus not well-chosen; but it is standard.

[68] Recall that a *part* of a partition means a nonzero entry of the partition.

[69] See Definition 1.3.21 for the meaning of "graded basis".

[70] *Proof.* We need to show that $\Lambda = R(\mathbf{x})^{\mathfrak{S}_\infty}$. Since

$$\Lambda = \left\{ f = \sum_{\alpha} c_\alpha \mathbf{x}^\alpha \in R(\mathbf{x}) : c_\alpha = c_\beta \text{ if } \alpha, \beta \text{ lie in the same } \mathfrak{S}_{(\infty)}\text{-orbit} \right\}$$

Remark 2.1.6. It is sometimes convenient to work with finite variable sets $x_1, \ldots, x_n$, which one justifies as follows. Note that the algebra homomorphism

$$R(\mathbf{x}) \to R(x_1, \ldots, x_n) = \mathbf{k}[x_1, \ldots, x_n]$$

which sends $x_{n+1}, x_{n+2}, \ldots$ to 0 restricts to an algebra homomorphism

$$\Lambda_{\mathbf{k}}(\mathbf{x}) \to \Lambda_{\mathbf{k}}(x_1, \ldots, x_n) = \mathbf{k}[x_1, \ldots, x_n]^{\mathfrak{S}_n}.$$

Furthermore, this last homomorphism is a $\mathbf{k}$-module isomorphism when restricted to Λ_i for $0 \leq i \leq n$, since it sends the monomial basis elements $m_\lambda(\mathbf{x})$ to the monomial basis elements $m_\lambda(x_1, \ldots, x_n)$. Thus, when one proves identities in $\Lambda_{\mathbf{k}}(x_1, \ldots, x_n)$ for all n, they are valid in Λ, that is, Λ is the inverse limit of the $\Lambda(x_1, \ldots, x_n)$ in the category of graded $\mathbf{k}$-algebras.[71]

This characterization of Λ as an inverse limit of the graded $\mathbf{k}$-algebras $\Lambda(x_1, \ldots, x_n)$ can be used as an alternative definition of Λ. The definitions used by Macdonald [142] and Wildon [224] are closely related (see [142, §1.2, p. 19, Remark 1], [90, §A.11] and [224, §1.7] for discussions of this definition). It also suggests that much of the theory of symmetric functions can be rewritten in terms of the $\Lambda(x_1, \ldots, x_n)$ (at the cost of extra complexity); and this indeed is possible[72].

One can also define a comultiplication on Λ as follows.

Consider the countably infinite set of variables $(\mathbf{x}, \mathbf{y}) = (x_1, x_2, \ldots, y_1, y_2, \ldots)$. Although it properly contains $\mathbf{x}$, there are nevertheless bijections between $\mathbf{x}$ and $(\mathbf{x}, \mathbf{y})$, since these two variable sets have the same cardinality.

Let $R(\mathbf{x}, \mathbf{y})$ denote the $\mathbf{k}$-algebra of formal power series in $(\mathbf{x}, \mathbf{y})$ of bounded degree. Let $\mathfrak{S}_{(\infty,\infty)}$ be the group of all permutations of $\{x_1, x_2, \ldots, y_1, y_2, \ldots\}$ leaving all but finitely many variables invariant. Then, $\mathfrak{S}_{(\infty,\infty)}$ acts on $R(\mathbf{x}, \mathbf{y})$ by permuting variables, in the same way as $\mathfrak{S}_{(\infty)}$ acts on $R(\mathbf{x})$. The fixed space $R(\mathbf{x}, \mathbf{y})^{\mathfrak{S}_{(\infty,\infty)}}$ is a $\mathbf{k}$-algebra, which we denote by $\Lambda(\mathbf{x}, \mathbf{y})$. This $\mathbf{k}$-algebra $\Lambda(\mathbf{x}, \mathbf{y})$ is isomorphic to $\Lambda = \Lambda(\mathbf{x})$, since there is a bijection between the two sets of variables $(\mathbf{x}, \mathbf{y})$ and $\mathbf{x}$. More explicitly: The map

$$\begin{array}{rcl} \Lambda = \Lambda(\mathbf{x}) & \stackrel{\Delta}{\longrightarrow} & \Lambda(\mathbf{x}, \mathbf{y}), \\ f(\mathbf{x}) = f(x_1, x_2, \ldots) & \longmapsto & f(\mathbf{x}, \mathbf{y}) = f(x_1, x_2, \ldots, y_1, y_2, \ldots) \end{array} \tag{2.1.2}$$

is a graded $\mathbf{k}$-algebra isomorphism. Here, $f(x_1, x_2, \ldots, y_1, y_2, \ldots)$ means the result of choosing some bijection $\phi : \{x_1, x_2, x_3, \ldots\} \to \{x_1, x_2, \ldots, y_1, y_2, \ldots\}$ and substituting $\phi(x_i)$ for every x_i in f. (The choice of ϕ is irrelevant since f is symmetric.[73])

The group $\mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}$ is a subgroup of the group $\mathfrak{S}_{(\infty,\infty)}$ (via the obvious injection, which lets each $(\sigma, \tau) \in \mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}$ act by separately permuting the $x_1, x_2, x_3, \ldots$ using σ and permuting the $y_1, y_2, y_3, \ldots$ using τ), and thus also acts on $R(\mathbf{x}, \mathbf{y})$. Hence, we have an inclusion of $\mathbf{k}$-algebras $\Lambda(\mathbf{x}, \mathbf{y}) = R(\mathbf{x}, \mathbf{y})^{\mathfrak{S}_{(\infty,\infty)}} \subset R(\mathbf{x}, \mathbf{y})^{\mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}} \subset R(\mathbf{x}, \mathbf{y})$. The $\mathbf{k}$-module $R(\mathbf{x}, \mathbf{y})^{\mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}}$ has $\mathbf{k}$-basis $\{m_\lambda(\mathbf{x}) m_\mu(\mathbf{y})\}_{\lambda,\mu \in \mathrm{Par}}$, since $m_\lambda(\mathbf{x}) m_\mu(\mathbf{y})$ is just the sum of all monomials in the $\mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}$-orbit of $\mathbf{x}^\lambda \mathbf{y}^\mu$ (and since any $\mathfrak{S}_{(\infty)} \times \mathfrak{S}_{(\infty)}$-orbit of monomials has exactly one representative of the form $\mathbf{x}^\lambda \mathbf{y}^\mu$ with $\lambda, \mu \in \mathrm{Par}$). Here, of course, $\mathbf{y}$ stands for the set of variables $(y_1, y_2, y_3, \ldots)$, and we define $\mathbf{y}^\mu$ to be $y_1^{\mu_1} y_2^{\mu_2} \cdots$.

On the other hand, the map

$$\begin{array}{rcl} R(\mathbf{x}) \otimes R(\mathbf{x}) & \longrightarrow & R(\mathbf{x}, \mathbf{y}), \\ f(\mathbf{x}) \otimes g(\mathbf{x}) & \longmapsto & f(\mathbf{x}) g(\mathbf{y}) \end{array}$$

---

and

$$R(\mathbf{x})^{\mathfrak{S}_\infty} = \left\{ f = \sum_\alpha c_\alpha \mathbf{x}^\alpha \in R(\mathbf{x}) : c_\alpha = c_\beta \text{ if } \alpha, \beta \text{ lie in the same } \mathfrak{S}_\infty\text{-orbit} \right\},$$

this will follow immediately if we can show that two weak compositions α and β lie in the same $\mathfrak{S}_{(\infty)}$-orbit if and only if they lie in the same $\mathfrak{S}_\infty$-orbit. But this is straightforward to check (in fact, two weak compositions α and β lie in the same orbit under either group if and only if they have the same multiset of nonzero entries).

[71] *Warning:* The word "graded" here is crucial. Indeed, Λ is **not** the inverse limit of the $\Lambda(x_1, \ldots, x_n)$ in the category of $\mathbf{k}$-algebras. In fact, the latter limit is the $\mathbf{k}$-algebra of all symmetric power series f in $\mathbf{k}[\mathbf{x}]$ with the following property: For each $g \in \mathbb{N}$, there exists a $d \in \mathbb{N}$ such that every monomial in f that involves exactly g distinct indeterminates has degree at most d. For example, the power series $(1 + x_1)(1 + x_2)(1 + x_3) \cdots$ and $m_{(1)} + m_{(2,2)} + m_{(3,3,3)} + \cdots$ satisfy this property, although they do not lie in Λ (unless $\mathbf{k}$ is a trivial ring).

[72] See, for example, [119, Chapter SYM], [174] and [138, Chapters 10–11] for various results of this present chapter rewritten in terms of symmetric polynomials in finitely many variables.

[73] To be more precise, the choice of ϕ is irrelevant because f is $\mathfrak{S}_\infty$-invariant, with the notations of Remark 2.1.5.

is a $\mathbf{k}$-algebra homomorphism. Restricting it to $R(\mathbf{x})^{\mathfrak{S}(\infty)} \otimes R(\mathbf{x})^{\mathfrak{S}(\infty)}$, we obtain a $\mathbf{k}$-algebra homomorphism

$$\Lambda \otimes \Lambda = R(\mathbf{x})^{\mathfrak{S}(\infty)} \otimes R(\mathbf{x})^{\mathfrak{S}(\infty)} \longrightarrow R(\mathbf{x},\mathbf{y})^{\mathfrak{S}(\infty)\times\mathfrak{S}(\infty)}, \tag{2.1.3}$$

which is an isomorphism because it sends the basis $\{m_\lambda \otimes m_\mu\}_{\lambda,\mu\in\mathrm{Par}}$ of the $\mathbf{k}$-module $\Lambda\otimes\Lambda$ to the basis $\{m_\lambda(\mathbf{x})m_\mu(\mathbf{y})\}_{\lambda,\mu\in\mathrm{Par}}$ of the $\mathbf{k}$-module $R(\mathbf{x},\mathbf{y})^{\mathfrak{S}(\infty)\times\mathfrak{S}(\infty)}$. Thus, we get an inclusion of graded $\mathbf{k}$-algebras

$$\Lambda(\mathbf{x},\mathbf{y}) = R(\mathbf{x},\mathbf{y})^{\mathfrak{S}(\infty,\infty)} \hookrightarrow R(\mathbf{x},\mathbf{y})^{\mathfrak{S}(\infty)\times\mathfrak{S}(\infty)} \cong \Lambda\otimes\Lambda$$

where the last isomorphism is the inverse of the one in (2.1.3). This gives a comultiplication

$$\begin{array}{rcl} \Lambda = \Lambda(\mathbf{x}) & \stackrel{\Delta}{\longrightarrow} & \Lambda(\mathbf{x},\mathbf{y}) \hookrightarrow \Lambda\otimes\Lambda, \\ f(\mathbf{x}) = f(x_1,x_2,\ldots) & \longmapsto & f(\mathbf{x},\mathbf{y}) = f(x_1,x_2,\ldots,y_1,y_2,\ldots). \end{array}$$

Here, $f(x_1,x_2,\ldots,y_1,y_2,\ldots)$ is understood as in (2.1.2).

Example 2.1.7. One has

$$\begin{aligned} \Delta m_{(2,1)} &= m_{(2,1)}(x_1,x_2,\ldots,y_1,y_2,\ldots) \\ &= x_1^2x_2 + x_1x_2^2 + \cdots \\ &\quad + x_1^2y_1 + x_1^2y_2 + \cdots \\ &\quad + x_1y_1^2 + x_1y_2^2 + \cdots \\ &\quad + y_1^2y_2 + y_1y_2^2 + \cdots \\ &= m_{(2,1)}(\mathbf{x}) + m_{(2)}(\mathbf{x})m_{(1)}(\mathbf{y}) + m_{(1)}(\mathbf{x})m_{(2)}(\mathbf{y}) + m_{(2,1)}(\mathbf{y}) \\ &= m_{(2,1)}\otimes 1 + m_{(2)}\otimes m_{(1)} + m_{(1)}\otimes m_{(2)} + 1\otimes m_{(2,1)}. \end{aligned}$$

This example generalizes easily to the following formula:

$$\Delta m_\lambda = \sum_{\substack{(\mu,\nu):\\ \mu\sqcup\nu=\lambda}} m_\mu \otimes m_\nu, \tag{2.1.4}$$

in which $\mu\sqcup\nu$ is the partition obtained by taking the multiset union of the parts of μ and ν, and then reordering them to make them weakly decreasing.

Checking that Δ is coassociative amounts to checking that

$$(\Delta\otimes\mathrm{id})\circ\Delta f = f(\mathbf{x},\mathbf{y},\mathbf{z}) = (\mathrm{id}\otimes\Delta)\circ\Delta f$$

inside $\Lambda(\mathbf{x},\mathbf{y},\mathbf{z})$ as a subring of $\Lambda\otimes\Lambda\otimes\Lambda$.

The counit $\Lambda \stackrel{\epsilon}{\to} \mathbf{k}$ is defined in the usual fashion for connected graded coalgebras, namely ϵ annihilates $I = \bigoplus_{n>0}\Lambda_n$, and ϵ is the identity on $\Lambda_0 = \mathbf{k}$; alternatively ϵ sends a symmetric function $f(\mathbf{x})$ to its constant term $f(0,0,\ldots)$.

Note that Δ is an algebra morphism $\Lambda\to\Lambda\otimes\Lambda$ because it is a composition of maps which are all algebra morphisms. As the unit and counit axioms are easily checked, Λ becomes a connected graded $\mathbf{k}$-bialgebra of finite type, and hence also a Hopf algebra by Proposition 1.4.16. We will identify its antipode more explicitly in Section 2.4 below.

2.2. **Other Bases.** We introduce the usual other bases of Λ, and explain their significance later.

Definition 2.2.1. Define the families of *power sum symmetric functions* p_n, *elementary symmetric functions* e_n, and *complete homogeneous symmetric functions* h_n, for $n = 1,2,3,\ldots$ by

$$p_n := x_1^n + x_2^n + \cdots = m_{(n)}, \tag{2.2.1}$$

$$e_n := \sum_{i_1<\cdots<i_n} x_{i_1}\cdots x_{i_n} = m_{(1^n)}, \tag{2.2.2}$$

$$h_n := \sum_{i_1\le\cdots\le i_n} x_{i_1}\cdots x_{i_n} = \sum_{\lambda\in\mathrm{Par}_n} m_\lambda. \tag{2.2.3}$$

Here, we are using the *multiplicative notation* for partitions: whenever $(m_1,m_2,m_3,\ldots)$ is a weak composition, $(1^{m_1}2^{m_2}3^{m_3}\cdots)$ denotes the partition λ such that for every i, the multiplicity of the part i in λ is m_i. The i^{m_i} satisfying $m_i = 0$ are often omitted from this notation, and so the (1^n) in (2.2.2) means

$\left(\underbrace{1,1,\ldots,1}_{n \text{ ones}}\right)$. (For another example, $\left(1^2 3^1 4^3\right) = \left(1^2 2^0 3^1 4^3 5^0 6^0 7^0 \cdots\right)$ means the partition $(4,4,4,3,1,1)$.)
By convention, also define $h_0 = e_0 = 1$, and $h_n = e_n = 0$ if $n < 0$. Extend these multiplicatively to partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ with $\lambda_1 \geq \cdots \geq \lambda_\ell > 0$ by setting

$$p_\lambda := p_{\lambda_1} p_{\lambda_2} \cdots p_{\lambda_\ell},$$
$$e_\lambda := e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_\ell},$$
$$h_\lambda := h_{\lambda_1} h_{\lambda_2} \cdots h_{\lambda_\ell}.$$

Also define the *Schur function*

$$s_\lambda := \sum_T \mathbf{x}^{\mathrm{cont}(T)} \tag{2.2.4}$$

where T runs through all *column-strict tableaux* of shape λ, that is, T is an assignment of entries in $\{1,2,3,\ldots\}$ to the cells of the *Ferrers diagram*[74] for λ, weakly increasing left-to-right in rows, and strictly increasing top-to-bottom in columns. Here $\mathrm{cont}(T)$ denotes the weak composition $\left(|T^{-1}(1)|, |T^{-1}(2)|, |T^{-1}(3)|, \ldots\right)$, so that $\mathbf{x}^{\mathrm{cont}(T)} = \prod_i x_i^{|T^{-1}(i)|}$. For example,[75]

$$T = \begin{array}{ccccc} 1 & 1 & 1 & 4 & 7 \\ 2 & 3 & 3 & & \\ 4 & 4 & 6 & & \\ 6 & 7 & & & \end{array}$$

is a column-strict tableau of shape $\lambda = (5,3,3,2)$ with $\mathbf{x}^{\mathrm{cont}(T)} = x_1^3 x_2^1 x_3^2 x_4^3 x_5^0 x_6^2 x_7^2$. If T is a column-strict tableau, then the weak composition $\mathrm{cont}(T)$ is called the *content* of T.

Column-strict tableaux are also known as *semistandard tableaux*, and some authors even omit the adjective and just call them *tableaux* (e.g., Fulton in [73], a book entirely devoted to them).

---

[74] The *Ferrers diagram* of a partition λ is defined as the set of all pairs $(i,j) \in \{1,2,3,\ldots\}^2$ satisfying $j \leq \lambda_i$. This is a set of cardinality $|\lambda|$. Usually, one visually represents a Ferrers diagram by drawing its elements (i,j) as points on the plane, although (unlike the standard convention for drawing points on the plane) one lets the x-axis go top-to-bottom (i.e., the point $(i+1,j)$ is one step below the point (i,j)), and the y-axis go left-to-right (i.e., the point $(i,j+1)$ is one step to the right of the point (i,j)). (This is the so-called *English notation*, also known as the *matrix notation* because it is precisely the way one labels the entries of a matrix. Other notations appear in literature, such as the French notation used, e.g., in Malvenuto's [145], and the Russian notation used, e.g., in parts of Kerov's [108].) These points are drawn either as dots or as square boxes; in the latter case, the boxes are centered at the points they represent, and they have sidelength 1 so that the boxes centered around (i,j) and $(i,j+1)$ touch each other along a sideline. For example, the Ferrers diagram of the partition $(3,2,2)$ is represented as


(using dots) or as (using boxes).

The Ferrers diagram of a partition λ uniquely determines λ. One refers to the elements of the Ferrers diagram of λ as the *cells* (or *boxes*) of this diagram (which is particularly natural when one represents them by boxes) or, briefly, as the cells of λ. Notation like "west", "north", "left", "right", "row" and "column" concerning cells of Ferrers diagrams normally refers to their visual representation.

Ferrers diagrams are also known as *Young diagrams*.

One can characterize the Ferrers diagrams of partitions as follows: A finite subset S of $\{1,2,3,\ldots\}^2$ is the Ferrers diagram of some partition if and only if for every $(i,j) \in S$ and every $(i',j') \in \{1,2,3,\ldots\}^2$ satisfying $i' \leq i$ and $j' \leq j$, we have $(i',j') \in S$. In other words, a finite subset S of $\{1,2,3,\ldots\}^2$ is the Ferrers diagram of some partition if and only if it is a lower set of the poset $\{1,2,3,\ldots\}^2$ with respect to the componentwise order.

[75] To visually represent a column-strict tableau T of shape λ, we draw the same picture as when representing the Ferrers diagram of λ, but with a little difference: a cell (i,j) is no longer represented by a dot or box, but instead is represented by the entry of T assigned to this cell. Accordingly, the entry of T assigned to a given cell c is often referred to as *the entry of T in c*.

Example 2.2.2. One has

$$\begin{aligned} m_{(1)} = p_{(1)} = e_{(1)} = h_{(1)} = s_{(1)} &= x_1 + x_2 + x_3 + \cdots, \\ s_{(n)} &= h_n, \\ s_{(1^n)} &= e_n. \end{aligned}$$

Example 2.2.3. One has for $\lambda = (2,1)$ that

$$\begin{aligned} p_{(2,1)} &= p_2 p_1 = (x_1^2 + x_2^2 + \cdots)(x_1 + x_2 + \cdots) \\ &= m_{(2,1)} + m_{(3)}, \\ e_{(2,1)} &= e_2 e_1 = (x_1x_2 + x_1x_3 + \cdots)(x_1 + x_2 + \cdots) \\ &= m_{(2,1)} + 3m_{(1,1,1)}, \\ h_{(2,1)} &= h_2 h_1 = (x_1^2 + x_2^2 + \cdots + x_1x_2 + x_1x_3 + \cdots)(x_1 + x_2 + \cdots) \\ &= m_{(3)} + 2m_{(2,1)} + 3m_{(1,1,1)}, \end{aligned}$$

and

$$\begin{aligned} s_{(2,1)} &= x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_1x_2x_3 + x_1x_2x_3 + x_1x_2x_4 + \cdots \\ &\quad\ 11 \quad\ 11 \quad\ 12 \quad\ 13 \quad\ 12 \quad\ 13 \quad\ 12 \\ &\quad\ 2 \quad\ 3 \quad\ 2 \quad\ 3 \quad\ 3 \quad\ 2 \quad\ 4 \\ &= m_{(2,1)} + 2m_{(1,1,1)}. \end{aligned}$$

In fact, one has these transition matrices for $n = 3$ expressing elements in terms of the monomial basis m_λ:

$$\begin{array}{c} \\ m_{(3)} \\ m_{(2,1)} \\ m_{(1,1,1)} \end{array} \begin{array}{c} \begin{array}{ccc} p_{(3)} & p_{(2,1)} & p_{(1,1,1)} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 6 \end{pmatrix} \end{array}, \qquad \begin{array}{c} \\ m_{(3)} \\ m_{(2,1)} \\ m_{(1,1,1)} \end{array} \begin{array}{c} \begin{array}{ccc} e_{(3)} & e_{(2,1)} & e_{(1,1,1)} \end{array} \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 3 \\ 1 & 3 & 6 \end{pmatrix} \end{array},$$

$$\begin{array}{c} \\ m_{(3)} \\ m_{(2,1)} \\ m_{(1,1,1)} \end{array} \begin{array}{c} \begin{array}{ccc} h_{(3)} & h_{(2,1)} & h_{(1,1,1)} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix} \end{array}, \qquad \begin{array}{c} \\ m_{(3)} \\ m_{(2,1)} \\ m_{(1,1,1)} \end{array} \begin{array}{c} \begin{array}{ccc} s_{(3)} & s_{(2,1)} & s_{(1,1,1)} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \end{array}.$$

Our next goal is to show that $e_\lambda, s_\lambda, h_\lambda$ (and, under some conditions, the p_λ as well) all give bases for Λ. However at the moment it is not yet even clear that s_λ are symmetric!

Proposition 2.2.4. *Schur functions s_λ are symmetric, that is, they lie in Λ.*

Proof. It suffices to show s_λ is symmetric under swapping the variables x_i, x_{i+1}, by providing an involution ι on the set of all column-strict tableaux T of shape λ which switches the $\mathrm{cont}(T)$ for $(i, i+1)\,\mathrm{cont}(T)$. Restrict attention to the entries $i, i+1$ in T, which must look something like this:

$$\begin{array}{ccccccccccccccc} & & & & & & & & & i & & i & & i & i & i+1 & i+1 \\ & & i & & i & i & i & i+1 & i+1 & i+1 & i+1 & i+1 & i+1 & & & & \\ i+1 & i+1 & i+1 & & & & & & & & & & & & & & \end{array}$$

One finds several vertically aligned pairs $\begin{matrix} i \\ i+1 \end{matrix}$. If one were to remove all such pairs, the remaining entries would be a sequence of rows, each looking like this:

$$\underbrace{i, i, \ldots, i}_{r \text{ occurrences}}, \underbrace{i+1, i+1, \ldots, i+1}_{s \text{ occurrences}}. \tag{2.2.5}$$

An involution due to Bender and Knuth tells us to leave fixed all the vertically aligned pairs $\begin{matrix} i \\ i+1 \end{matrix}$, but change each sequence of remaining entries as in (2.2.5) to this:

$$\underbrace{i, i, \ldots, i}_{s \text{ occurrences}}, \underbrace{i+1, i+1, \ldots, i+1}_{r \text{ occurrences}}.$$

For example, the above configuration in T would change to

$$\begin{array}{cccccccccccccc} & & & & & & & & i & & i & & i & i & i & i+1 \\ & & i & & i & & i & i & i+1 & i+1 & i+1 & i+1 & & & & \\ i & & i+1 & & i+1 & & & & & & & & & & & \end{array}$$

It is easily checked that this map is an involution, and that it has the effect of swapping $(i, i+1)$ in $\mathrm{cont}(T)$. □

Remark 2.2.5. The symmetry of Schur functions allows one to reformulate them via column-strict tableaux defined with respect to *any* total ordering $\mathcal{L}$ on the positive integers, rather than the usual $1 < 2 < 3 < \cdots$. For example, one can use the *reverse order*[76] $\cdots < 3 < 2 < 1$, or even more exotic orders, such as

$$1 < 3 < 5 < 7 < \cdots < 2 < 4 < 6 < 8 < \cdots .$$

Say that an assignment T of entries in $\{1, 2, 3, \ldots\}$ to the cells of the Ferrers diagram of λ is an *$\mathcal{L}$-column-strict tableau* if it is weakly $\mathcal{L}$-increasing left-to-right in rows, and strictly $\mathcal{L}$-increasing top-to-bottom in columns.

Proposition 2.2.6. *For any total order $\mathcal{L}$ on the positive integers,*

$$s_\lambda = \sum_T \mathbf{x}^{\mathrm{cont}(T)} \tag{2.2.6}$$

as T runs through all $\mathcal{L}$-column-strict tableaux of shape λ.

Proof. Given a weak composition $\alpha = (\alpha_1, \alpha_2, \ldots)$ with $\alpha_{n+1} = \alpha_{n+2} = \cdots = 0$, assume that the integers $1, 2, \ldots, n$ are totally ordered by $\mathcal{L}$ as $w(1) <_{\mathcal{L}} \cdots <_{\mathcal{L}} w(n)$ for some w in $\mathfrak{S}_n$. Then the coefficient of $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ on the right side of (2.2.6) is the same as the coefficient of $\mathbf{x}^{w^{-1}(\alpha)}$ on the right side of (2.2.4) defining s_λ, which by symmetry of s_λ is the same as the coefficient of $\mathbf{x}^\alpha$ on the right side of (2.2.4). □

It is now not hard to show that $p_\lambda, e_\lambda, s_\lambda$ give bases by a triangularity argument[77]. For this purpose, let us introduce a useful partial order on partitions.

Definition 2.2.7. The *dominance* or *majorization* order on Par_n is the partial order on the set Par_n whose greater-or-equal relation $\trianglerighteq$ is defined as follows: For two partitions λ and μ of n, we set $\lambda \trianglerighteq \mu$ (and say that λ *dominates*, or *majorizes*, μ) if and only if

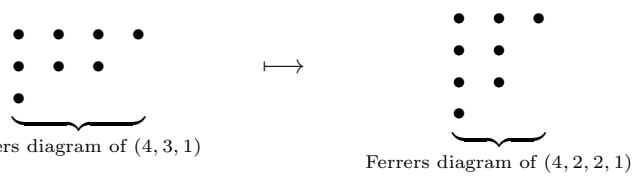
$$\lambda_1 + \lambda_2 + \cdots + \lambda_k \geq \mu_1 + \mu_2 + \cdots + \mu_k \quad \text{for } k = 1, 2, \ldots, n.$$

(The definition of dominance would not change if we would replace "for $k = 1, 2, \ldots, n$" by "for every positive integer k" or by "for every $k \in \mathbb{N}$".)

Definition 2.2.8. For a partition λ, its *conjugate* or *transpose* partition λ^t is the one whose Ferrers diagram is obtained from that of λ by exchanging rows for columns (i.e., by flipping the diagram across the "main", i.e., top-right-to-bottom-left, diagonal)[78]. Alternatively, one has this formula for its i-th entry:

$$(\lambda^t)_i := |\{j : \lambda_j \geq i\}|. \tag{2.2.7}$$

For example, $(4,3,1)^t = (3,2,2,1)$, which can be easily verified by flipping the Ferrers diagram of $(4,3,1)$ across the "main diagonal":



(or simply counting the boxes in each column of this diagram).

[76] This reverse order is what one uses when one defines a Schur function as a generating function for *reverse semistandard tableaux* or *column-strict plane partitions*; see Stanley [206, Proposition 7.10.4].

[77] See Section 11.1 for some notions and notations that will be used in this argument.

[78] In more rigorous terms: The cells of the Ferrers diagram of λ^t are the pairs (j, i), where (i, j) ranges over all cells of λ. It is easy to see that this indeed uniquely determines a partition λ^t.

Exercise 2.2.9. Let $\lambda, \mu \in \mathrm{Par}_n$. Show that $\lambda \rhd \mu$ if and only if $\mu^t \rhd \lambda^t$.

Proposition 2.2.10. *The families $\{e_\lambda\}$ and $\{s_\lambda\}$, as λ runs through all partitions, are graded bases for the graded $\mathbf{k}$-module $\Lambda_\mathbf{k}$ whenever $\mathbf{k}$ is a commutative ring. The same holds for the family $\{p_\lambda\}$ when $\mathbb{Q}$ is a subring of $\mathbf{k}$.*

Our proof of this proposition will involve three separate arguments, one for each of the three alleged bases $\{s_\lambda\}$, $\{e_\lambda\}$ and $\{p_\lambda\}$; however, all these three arguments fit the same mold: Each one shows that the alleged basis expands invertibly triangularly[79] in the basis $\{m_\lambda\}$ (possibly after reindexing), with an appropriately chosen partial order on the indexing set. We will simplify our life by restricting ourselves to Par_n for a given $n \in \mathbb{N}$, and by stating the common part of the three arguments in a greater generality (so that we won't have to repeat it thrice):

Lemma 2.2.11. *Let S be a finite poset. We write $\leq$ for the smaller-or-equal relation of S.*

Let M be a free $\mathbf{k}$-module with a basis $(b_\lambda)_{\lambda \in S}$. Let $(a_\lambda)_{\lambda \in S}$ be a further family of elements of M.

For each $\lambda \in S$, let $(g_{\lambda,\mu})_{\mu \in S}$ be the family of the coefficients in the expansion of $a_\lambda \in M$ in the basis $(b_\mu)_{\mu \in S}$; in other words, let $(g_{\lambda,\mu})_{\mu \in S} \in \mathbf{k}^S$ be such that $a_\lambda = \sum_{\mu \in S} g_{\lambda,\mu} b_\mu$. Assume that:

- *Assumption A1: Any $\lambda \in S$ and $\mu \in S$ satisfy $g_{\lambda,\mu} = 0$ unless $\mu \leq \lambda$.*
- *Assumption A2: For any $\lambda \in S$, the element $g_{\lambda,\lambda}$ of $\mathbf{k}$ is invertible.*

Then, the family $(a_\lambda)_{\lambda \in S}$ is a basis of the $\mathbf{k}$-module M.

Proof of Lemma 2.2.11. Use the notations of Section 11.1. Assumptions A1 and A2 yield that the $S \times S$-matrix $(g_{\lambda,\mu})_{(\lambda,\mu) \in S \times S} \in \mathbf{k}^{S \times S}$ is invertibly triangular. But the definition of the $g_{\lambda,\mu}$ yields that the family $(a_\lambda)_{\lambda \in S}$ expands in the family $(b_\lambda)_{\lambda \in S}$ through this matrix $(g_{\lambda,\mu})_{(\lambda,\mu) \in S \times S}$. Since the latter matrix is invertibly triangular, this shows that the family $(a_\lambda)_{\lambda \in S}$ expands invertibly triangularly in the family $(b_\lambda)_{\lambda \in S}$. Therefore, Corollary 11.1.19(e) (applied to $(e_s)_{s \in S} = (a_\lambda)_{\lambda \in S}$ and $(f_s)_{s \in S} = (b_\lambda)_{\lambda \in S}$) shows that $(a_\lambda)_{\lambda \in S}$ is a basis of the $\mathbf{k}$-module M (since $(b_\lambda)_{\lambda \in S}$ is a basis of the $\mathbf{k}$-module M). □

Proof of Proposition 2.2.10. We can restrict our attention to each homogeneous component Λ_n and partitions λ of n. Thus, we have to prove that, for each $n \in \mathbb{N}$, the families $(e_\lambda)_{\lambda \in \mathrm{Par}_n}$ and $(s_\lambda)_{\lambda \in \mathrm{Par}_n}$ are bases of the $\mathbf{k}$-module Λ_n, and that the same holds for $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ if $\mathbb{Q}$ is a subring of $\mathbf{k}$.

Fix $n \in \mathbb{N}$. We already know that $(m_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n.

1. We shall first show that the family $(s_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n.

   For every partition λ, we have $s_\lambda = \sum_{\mu \in \mathrm{Par}} K_{\lambda,\mu} m_\mu$, where the coefficient $K_{\lambda,\mu}$ is the *Kostka number* counting the column-strict tableaux T of shape λ having $\mathrm{cont}(T) = \mu$; this follows because both sides are symmetric functions, and $K_{\lambda,\mu}$ is the coefficient of $\mathbf{x}^\mu$ on both sides[80]. Thus, for every $\lambda \in \mathrm{Par}_n$, one has

$$s_\lambda = \sum_{\mu \in \mathrm{Par}_n} K_{\lambda,\mu} m_\mu \tag{2.2.8}$$

   (since s_λ is homogeneous of degree n). [81] But if λ and μ are partitions satisfying $K_{\lambda,\mu} \neq 0$, then there exists a column-strict tableau T of shape λ having $\mathrm{cont}(T) = \mu$ (since $K_{\lambda,\mu}$ counts such tableaux), and therefore we must have $\lambda_1 + \lambda_2 + \cdots + \lambda_k \geq \mu_1 + \mu_2 + \cdots + \mu_k$ for each positive integer k (since the entries $1, 2, \ldots, k$ in T must all lie within the first k rows of λ); in other words, $\lambda \rhd \mu$ (if $K_{\lambda,\mu} \neq 0$) [82]. In other words,

$$\text{any } \lambda \in \mathrm{Par}_n \text{ and } \mu \in \mathrm{Par}_n \text{ satisfy } K_{\lambda,\mu} = 0 \text{ unless } \lambda \rhd \mu. \tag{2.2.9}$$

[79] i.e., triangularly, with all diagonal coefficients being invertible

[80] In general, in order to prove that two symmetric functions f and g are equal, it suffices to show that, for every $\mu \in \mathrm{Par}$, the coefficients of $\mathbf{x}^\mu$ in f and in g are equal. (Indeed, all other coefficients are determined by these coefficients because of the symmetry.)

[81] See Exercise 2.2.13(c) below for a detailed proof of (2.2.8).

[82] See Exercise 2.2.13(d) below for a detailed proof of this fact.

One can also check that $K_{\lambda,\lambda} = 1$ for any $\lambda \in \mathrm{Par}_n$ [83]. Hence,

(2.2.10) for any $\lambda \in \mathrm{Par}_n$, the element $K_{\lambda,\lambda}$ of $\mathbf{k}$ is invertible.

Now, let us regard the set Par_n as a poset, whose greater-or-equal relation is $\triangleright$. Lemma 2.2.11 (applied to $S = \mathrm{Par}_n$, $M = \Lambda_n$, $a_\lambda = s_\lambda$, $b_\lambda = m_\lambda$ and $g_{\lambda,\mu} = K_{\lambda,\mu}$) shows that the family $(s_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n (because the Assumptions A1 and A2 of Lemma 2.2.11 are satisfied[84]).

2. Before we show that $(e_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis, we define a few notations regarding integer matrices. A $\{0,1\}$-*matrix* means a matrix whose entries belong to the set $\{0,1\}$. If $A \in \mathbb{N}^{\ell \times m}$ is a matrix, then the *row sums* of A means the ℓ-tuple $(r_1, r_2, \ldots, r_\ell)$, where each r_i is the sum of all entries in the i-th row of A; similarly, the *column sums* of A means the m-tuple $(c_1, c_2, \ldots, c_m)$, where each c_j is the sum of all entries in the j-th column of A. (For instance, the row sums of the $\{0,1\}$-matrix $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ is $(2,3)$, whereas its column sums is $(1,2,1,1,0)$.) We identify any k-tuple of nonnegative integers $(a_1, a_2, \ldots, a_k)$ with the weak composition $(a_1, a_2, \ldots, a_k, 0, 0, 0, \ldots)$; thus, the row sums and the column sums of a matrix in $\mathbb{N}^{\ell \times m}$ can be viewed as weak compositions. (For example, the column sums of the matrix $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$ is the 5-tuple $(1,2,1,1,0)$, and can be viewed as the weak composition $(1,2,1,1,0,0,0,\ldots)$.)

For every $\lambda \in \mathrm{Par}_n$, one has

$$e_\lambda = \sum_{\mu \in \mathrm{Par}_n} a_{\lambda,\mu} m_\mu, \tag{2.2.11}$$

where $a_{\lambda,\mu}$ counts $\{0,1\}$-matrices (of size $\ell(\lambda) \times \ell(\mu)$) having row sums λ and column sums μ: indeed, when one expands $e_{\lambda_1} e_{\lambda_2} \cdots$, choosing the monomial $x_{j_1} \ldots x_{j_{\lambda_i}}$ in the e_{λ_i} factor corresponds to putting 1's in the i-th row and columns $j_1, \ldots, j_{\lambda_i}$ of the $\{0,1\}$-matrix [85]. Applying (2.2.11) to λ^t instead of λ, we see that

$$e_{\lambda^t} = \sum_{\mu \in \mathrm{Par}_n} a_{\lambda^t,\mu} m_\mu \tag{2.2.12}$$

for every $\lambda \in \mathrm{Par}_n$.

It is not hard to check[86] that $a_{\lambda,\mu}$ vanishes unless $\lambda^t \triangleright \mu$. Applying this to λ^t instead of λ, we conclude that

(2.2.13) any $\lambda \in \mathrm{Par}_n$ and $\mu \in \mathrm{Par}_n$ satisfy $a_{\lambda^t,\mu} = 0$ unless $\lambda \triangleright \mu$.

Moreover, one can show that $a_{\lambda^t,\lambda} = 1$ for each $\lambda \in \mathrm{Par}_n$ [87]. Hence,

(2.2.14) for any $\lambda \in \mathrm{Par}_n$, the element $a_{\lambda^t,\lambda}$ of $\mathbf{k}$ is invertible.

Now, let us regard the set Par_n as a poset, whose greater-or-equal relation is $\triangleright$. Lemma 2.2.11 (applied to $S = \mathrm{Par}_n$, $M = \Lambda_n$, $a_\lambda = e_{\lambda^t}$, $b_\lambda = m_\lambda$ and $g_{\lambda,\mu} = a_{\lambda^t,\mu}$) shows that the family $(e_{\lambda^t})_{\lambda \in \mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n (because the Assumptions A1 and A2 of Lemma 2.2.11 are satisfied[88]). Hence, $(e_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis of Λ_n.

3. Assume now that $\mathbb{Q}$ is a subring of $\mathbf{k}$. For every $\lambda \in \mathrm{Par}_n$, one has

$$p_\lambda = \sum_{\mu \in \mathrm{Par}_n} b_{\lambda,\mu} m_\mu, \tag{2.2.15}$$

[83] See Exercise 2.2.13(e) below for a proof of this.

[84] Indeed, they follow from (2.2.9) and (2.2.10), respectively.

[85] See Exercise 2.2.13(g) below for a detailed proof of (2.2.11).

[86] See Exercise 2.2.13(h) below for a proof of this. This is the easy implication in the *Gale-Ryser Theorem*. (The hard implication is the converse: It says that if $\lambda, \mu \in \mathrm{Par}_n$ satisfy $\lambda^t \triangleright \mu$, then there exists a $\{0,1\}$-matrix having row sums λ and column sums μ, so that $a_{\lambda,\mu}$ is a positive integer. This is proven, e.g., in [114], in [46, Theorem 2.4] and in [224, Section 5.2].)

[87] See Exercise 2.2.13(i) below for a proof of this.

[88] Indeed, they follow from (2.2.13) and (2.2.14), respectively.

where $b_{\lambda,\mu}$ counts the ways to partition the nonzero parts $\lambda_1, \ldots, \lambda_\ell$ (where $\ell = \ell(\lambda)$) into blocks such that the sums of the blocks give μ; more formally, $b_{\lambda,\mu}$ is the number of maps $\varphi : \{1, 2, \ldots, \ell\} \to \{1, 2, 3, \ldots\}$ having

$$\mu_j = \sum_{i:\varphi(i)=j} \lambda_i \qquad \text{for all } j = 1, 2, \ldots$$

[89]. Again it is not hard to check that

$$\text{any } \lambda \in \mathrm{Par}_n \text{ and } \mu \in \mathrm{Par}_n \text{ satisfy } b_{\lambda,\mu} = 0 \text{ unless } \mu \trianglerighteq \lambda. \tag{2.2.16}$$

[90] Furthermore, for any $\lambda \in \mathrm{Par}_n$, the element $b_{\lambda,\lambda}$ is a positive integer[91], and thus invertible in $\mathbf{k}$ (since $\mathbb{Q}$ is a subring of $\mathbf{k}$). Thus,

$$\text{for any } \lambda \in \mathrm{Par}_n \text{, the element } b_{\lambda,\lambda} \text{ of } \mathbf{k} \text{ is invertible} \tag{2.2.17}$$

(although we don't always have $b_{\lambda,\lambda} = 1$ this time).

Now, let us regard the set Par_n as a poset, whose smaller-or-equal relation is $\trianglerighteq$. Lemma 2.2.11 (applied to $S = \mathrm{Par}_n$, $M = \Lambda_n$, $a_\lambda = p_\lambda$, $b_\lambda = m_\lambda$ and $g_{\lambda,\mu} = b_{\lambda,\mu}$) shows that the family $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n (because the Assumptions A1 and A2 of Lemma 2.2.11 are satisfied[92]). □

Remark 2.2.12. When $\mathbb{Q}$ is not a subring of $\mathbf{k}$, the family $\{p_\lambda\}$ is not (in general) a basis of $\Lambda_{\mathbf{k}}$; for instance, $e_2 = \frac{1}{2}\left(p_{(1,1)} - p_2\right) \in \Lambda_{\mathbb{Q}}$ is not in the $\mathbb{Z}$-span of this family. However, if we define $b_{\lambda,\mu}$ as in the above proof, then the $\mathbb{Z}$-linear span of all p_λ equals the $\mathbb{Z}$-linear span of all $b_{\lambda,\lambda} m_\lambda$. Indeed, if $\mu = (\mu_1, \mu_2, \ldots, \mu_k)$ with $k = \ell(\mu)$, then $b_{\mu,\mu}$ is the size of the subgroup of $\mathfrak{S}_k$ consisting of all permutations $\sigma \in \mathfrak{S}_k$ having each i satisfy $\mu_{\sigma(i)} = \mu_i$ [93]. As a consequence, $b_{\mu,\mu}$ divides $b_{\lambda,\mu}$ for every partition μ of the same size as λ (because this group acts[94] freely on the set which is enumerated by $b_{\lambda,\mu}$) [95]. Hence, the $\mathrm{Par}_n \times \mathrm{Par}_n$-matrix $\left(\dfrac{b_{\lambda,\mu}}{b_{\mu,\mu}}\right)_{(\lambda,\mu) \in \mathrm{Par}_n \times \mathrm{Par}_n}$ has integer entries. Furthermore, this matrix is unitriangular[96] (indeed, (2.2.16) shows that it is triangular, but its diagonal entries are clearly 1) and thus invertibly triangular. But (2.2.15) shows that the family $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ expands in the family $(b_{\lambda,\lambda} m_\lambda)_{\lambda \in \mathrm{Par}_n}$ through this matrix. Hence, the family $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ expands invertibly triangularly in the family $(b_{\lambda,\lambda} m_\lambda)_{\lambda \in \mathrm{Par}_n}$. Thus, Corollary 11.1.19(b) (applied to $\mathbb{Z}$, Λ_n, Par_n, $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ and $(b_{\lambda,\lambda} m_\lambda)_{\lambda \in \mathrm{Par}_n}$ instead of $\mathbf{k}$, M, S, $(e_s)_{s \in S}$ and $(f_s)_{s \in S}$) shows that the $\mathbb{Z}$-submodule of Λ_n spanned by $(p_\lambda)_{\lambda \in \mathrm{Par}_n}$ is the $\mathbb{Z}$-submodule of Λ_n spanned by $(b_{\lambda,\lambda} m_\lambda)_{\lambda \in \mathrm{Par}_n}$.

The purpose of the following exercise is to fill in some details omitted from the proof of Proposition 2.2.10.

Exercise 2.2.13. Let $n \in \mathbb{N}$.

(a) Show that every $f \in \Lambda_n$ satisfies

$$f = \sum_{\mu \in \mathrm{Par}_n} \left([\mathbf{x}^\mu] f\right) m_\mu.$$

Here, $[\mathbf{x}^\mu] f$ denotes the coefficient of the monomial $\mathbf{x}^\mu$ in the power series f.

Now, we introduce a notation (which generalizes the notation $K_{\lambda,\mu}$ from the proof of Proposition 2.2.10): For any partition λ and any weak composition μ, we let $K_{\lambda,\mu}$ denote the number of all column-strict tableaux T of shape λ having $\mathrm{cont}(T) = \mu$.

(b) Prove that this number $K_{\lambda,\mu}$ is well-defined (i.e., there are only finitely many column-strict tableaux T of shape λ having $\mathrm{cont}(T) = \mu$).

---

[89] See Exercise 2.2.13(k) below for a detailed proof of (2.2.15) (and see Exercise 2.2.13(j) for a proof that the numbers $b_{\lambda,\mu}$ are well-defined).

[90] See Exercise 2.2.13(l) below for a proof of this.

[91] This is proven in Exercise 2.2.13(m) below.

[92] Indeed, they follow from (2.2.16) and (2.2.17), respectively.

[93] See Exercise 2.2.13(n) below for a proof of this.

[94] Specifically, an element σ of the group takes $\varphi : \{1, 2, \ldots, \ell\} \to \{1, 2, 3, \ldots\}$ to $\sigma \circ \varphi$.

[95] See Exercise 2.2.13(o) below for a detailed proof of this.

[96] Here, we are using the terminology defined in Section 11.1, and we are regarding Par_n as a poset whose smaller-or-equal relation is $\trianglerighteq$.

(c) Show that $s_\lambda = \sum_{\mu \in \mathrm{Par}_n} K_{\lambda,\mu} m_\mu$ for every $\lambda \in \mathrm{Par}_n$.
(d) Show that $K_{\lambda,\mu} = 0$ for any partitions $\lambda \in \mathrm{Par}_n$ and $\mu \in \mathrm{Par}_n$ that don't satisfy $\lambda \rhd \mu$.
(e) Show that $K_{\lambda,\lambda} = 1$ for any $\lambda \in \mathrm{Par}_n$.

Next, we recall a further notation: For any two partitions λ and μ, we let $a_{\lambda,\mu}$ denote the number of all $\{0,1\}$-matrices of size $\ell(\lambda) \times \ell(\mu)$ having row sums λ and column sums μ. (See the proof of Proposition 2.2.10 for the concepts of $\{0,1\}$-matrices and of row sums and column sums.)

(f) Prove that this number $a_{\lambda,\mu}$ is well-defined (i.e., there are only finitely many $\{0,1\}$-matrices of size $\ell(\lambda) \times \ell(\mu)$ having row sums λ and column sums μ).
(g) Show that $e_\lambda = \sum_{\mu \in \mathrm{Par}_n} a_{\lambda,\mu} m_\mu$ for every $\lambda \in \mathrm{Par}_n$.
(h) Show that $a_{\lambda,\mu} = 0$ for any partitions $\lambda \in \mathrm{Par}_n$ and $\mu \in \mathrm{Par}_n$ that don't satisfy $\lambda^t \rhd \mu$.
(i) Show that $a_{\lambda^t,\lambda} = 1$ for any $\lambda \in \mathrm{Par}_n$.

Next, we introduce a further notation (which generalizes the notation $b_{\lambda,\mu}$ from the proof of Proposition 2.2.10): For any partition λ and any weak composition μ, we let $b_{\lambda,\mu}$ be the number of all maps $\varphi : \{1,2,\ldots,\ell\} \to \{1,2,3,\ldots\}$ satisfying $\left(\mu_j = \sum\limits_{\substack{i \in \{1,2,\ldots,\ell\}; \\ \varphi(i) = j}} \lambda_i \text{ for all } j \geq 1 \right)$, where $\ell = \ell(\lambda)$.

(j) Prove that this number $b_{\lambda,\mu}$ is well-defined (i.e., there are only finitely many maps $\varphi : \{1,2,\ldots,\ell\} \to \{1,2,3,\ldots\}$ satisfying $\left(\mu_j = \sum\limits_{\substack{i \in \{1,2,\ldots,\ell\}; \\ \varphi(i) = j}} \lambda_i \text{ for all } j \geq 1 \right)$).
(k) Show that $p_\lambda = \sum_{\mu \in \mathrm{Par}_n} b_{\lambda,\mu} m_\mu$ for every $\lambda \in \mathrm{Par}_n$.
(l) Show that $b_{\lambda,\mu} = 0$ for any partitions $\lambda \in \mathrm{Par}_n$ and $\mu \in \mathrm{Par}_n$ that don't satisfy $\mu \rhd \lambda$.
(m) Show that $b_{\lambda,\lambda}$ is a positive integer for any $\lambda \in \mathrm{Par}_n$.
(n) Show that for any partition $\mu = (\mu_1, \mu_2, \ldots, \mu_k) \in \mathrm{Par}_n$ with $k = \ell(\mu)$, the integer $b_{\mu,\mu}$ is the size of the subgroup of $\mathfrak{S}_k$ consisting of all permutations $\sigma \in \mathfrak{S}_k$ having each i satisfy $\mu_{\sigma(i)} = \mu_i$. (In particular, show that this subgroup is indeed a subgroup.)
(o) Show that $b_{\mu,\mu} \mid b_{\lambda,\mu}$ for every $\lambda \in \mathrm{Par}_n$ and $\mu \in \mathrm{Par}_n$.

The bases $\{p_\lambda\}$ and $\{e_\lambda\}$ of Λ are two examples of *multiplicative bases*: these are bases constructed from a sequence $v_1, v_2, v_3, \ldots$ of symmetric functions by taking all possible finite products. We will soon encounter another example. First, let us observe that the finite products of a sequence $v_1, v_2, v_3, \ldots$ of symmetric functions form a basis of Λ if and only if the sequence is an algebraically independent generating set of Λ. This holds more generally for any commutative algebra, as the following simple exercise shows:

Exercise 2.2.14. Let A be a commutative $\mathbf{k}$-algebra. Let $v_1, v_2, v_3, \ldots$ be some elements of A.

For every partition λ, define an element $v_\lambda \in A$ by $v_\lambda = v_{\lambda_1} v_{\lambda_2} \cdots v_{\lambda_{\ell(\lambda)}}$. Prove the following:

(a) The $\mathbf{k}$-subalgebra of A generated by $v_1, v_2, v_3, \ldots$ is the $\mathbf{k}$-submodule of A spanned by the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$.
(b) The elements $v_1, v_2, v_3, \ldots$ generate the $\mathbf{k}$-algebra A if and only if the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$ spans the $\mathbf{k}$-module A.
(c) The elements $v_1, v_2, v_3, \ldots$ are algebraically independent over $\mathbf{k}$ if and only if the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$ is $\mathbf{k}$-linearly independent.

The next exercise states two well-known identities for the *generating functions* of the sequences $(e_0, e_1, e_2, \ldots)$ and $(h_0, h_1, h_2, \ldots)$, which will be used several times further below:

Exercise 2.2.15. In the ring of formal power series $(\mathbf{k}[[\mathbf{x}]])[[t]]$, prove the two identities

$$\prod_{i=1}^{\infty} (1 - x_i t)^{-1} = 1 + h_1(\mathbf{x})\, t + h_2(\mathbf{x})\, t^2 + \cdots = \sum_{n \geq 0} h_n(\mathbf{x})\, t^n \tag{2.2.18}$$

and

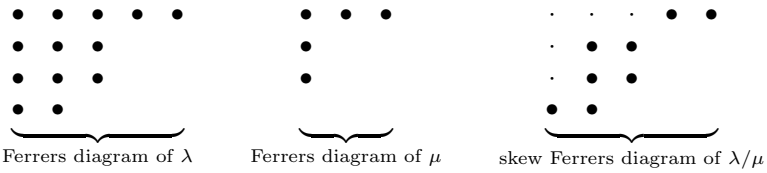
$$\prod_{i=1}^{\infty} (1 + x_i t) = 1 + e_1(\mathbf{x})\, t + e_2(\mathbf{x})\, t^2 + \cdots = \sum_{n \geq 0} e_n(\mathbf{x})\, t^n. \tag{2.2.19}$$

2.3. **Comultiplications.** Thinking about comultiplication $\Lambda \xrightarrow{\Delta} \Lambda \otimes \Lambda$ on Schur functions forces us to immediately confront the following.

Definition 2.3.1. For partitions μ and λ say that $\mu \subseteq \lambda$ if $\mu_i \leq \lambda_i$ for $i = 1, 2, \ldots$. In other words, two partitions μ and λ satisfy $\mu \subseteq \lambda$ if and only if the Ferrers diagram for μ is a subset of the Ferrers diagram of λ. In this case, define the *skew (Ferrers) diagram* λ/μ to be their set difference.[97]

Then define the *skew Schur function* $s_{\lambda/\mu}(\mathbf{x})$ to be the sum $s_{\lambda/\mu} := \sum_T \mathbf{x}^{\mathrm{cont}(T)}$, where the sum ranges over all *column-strict tableaux* T of shape λ/μ, that is, assignments of a value in $\{1, 2, 3, \ldots\}$ to each cell of λ/μ, weakly increasing left-to-right in rows, and strictly increasing top-to-bottom in columns.

Example 2.3.2. Let $\lambda = (5, 3, 3, 2)$ and $\mu = (3, 1, 1, 0)$. Then, $\mu \subseteq \lambda$. The Ferrers diagrams for λ and μ and the skew Ferrers diagram for λ/μ look as follows:



(where the small dots represent boxes removed from the diagram). The filling

$$T = \begin{array}{cccccc} \cdot & \cdot & \cdot & 2 & 5 \\ \cdot & 1 & 1 & & \\ 2 & 2 & 4 & & \\ 4 & 5 & & & \end{array}$$

is a column-strict tableau of shape $\lambda/\mu = (5, 3, 3, 2)/(3, 1, 0, 0)$ and it has $\mathbf{x}^{\mathrm{cont}(T)} = x_1^2 x_2^3 x_3^0 x_4^2 x_5^2$.

On the other hand, if we took $\lambda = (5, 3, 1)$ and $\mu = (1, 1, 1, 1)$, then we wouldn't have $\mu \subseteq \lambda$, since $\mu_4 = 1 > 0 = \lambda_4$.

Remark 2.3.3. If μ and λ are partitions such that $\mu \subseteq \lambda$, then $s_{\lambda/\mu} \in \Lambda$. (This is proven similarly as Proposition 2.2.4.) Actually, if $\mu \subseteq \lambda$, then $s_{\lambda/\mu} \in \Lambda_{|\lambda/\mu|}$, where $|\lambda/\mu|$ denotes the number of cells of the skew shape λ/μ (so $|\lambda/\mu| = |\lambda| - |\mu|$).

It is customary to define $s_{\lambda/\mu}$ to be 0 if we don't have $\mu \subseteq \lambda$. This can also be seen by a literal reading of the definition $s_{\lambda/\mu} := \sum_T \mathbf{x}^{\mathrm{cont}(T)}$, as long as we understand that there are no column-strict tableaux of shape λ/μ when λ/μ is not defined.

Clearly, every partition λ satisfies $s_\lambda = s_{\lambda/\varnothing}$.

It is easy to see that two partitions λ and μ satisfy $\mu \subseteq \lambda$ if and only if they satisfy $\mu^t \subseteq \lambda^t$.

Exercise 2.3.4. (a) State and prove an analogue of Proposition 2.2.6 for skew Schur functions.

(b) Let λ, μ, λ' and μ' be partitions such that $\mu \subseteq \lambda$ and $\mu' \subseteq \lambda'$. Assume that the skew Ferrers diagram λ'/μ' can be obtained from the skew Ferrers diagram λ/μ by a 180° rotation.[98] Prove that $s_{\lambda/\mu} = s_{\lambda'/\mu'}$.

Exercise 2.3.5. Let λ and μ be two partitions, and let $k \in \mathbb{N}$ be such that[99] $\mu_k \geq \lambda_{k+1}$. Let F be the skew Ferrers diagram λ/μ. Let $F_{\mathrm{rows} \leq k}$ denote the subset of F consisting of all $(i, j) \in F$ satisfying $i \leq k$. Let $F_{\mathrm{rows} > k}$ denote the subset of F consisting of all $(i, j) \in F$ satisfying $i > k$. Let α and β be two partitions such that $\beta \subseteq \alpha$ and such that the skew Ferrers diagram α/β can be obtained from $F_{\mathrm{rows} \leq k}$ by parallel

[97] In other words, the skew Ferrers diagram λ/μ is the set of all $(i, j) \in \{1, 2, 3, \ldots\}^2$ satisfying $\mu_i < j \leq \lambda_i$.

While the Ferrers diagram for a single partition λ uniquely determines λ, the skew Ferrers diagram λ/μ does not uniquely determine μ and λ. (For instance, it is empty whenever $\lambda = \mu$.) When one wants to keep μ and λ in memory, one speaks of the *skew shape* λ/μ; this simply means the pair (μ, λ). Every notion defined for skew Ferrers diagrams also makes sense for skew shapes, because to any skew shape λ/μ we can assign the skew Ferrers diagram λ/μ (even if not injectively). For instance, the *cells* of the skew shape λ/μ are the cells of the skew Ferrers diagram λ/μ.

One can characterize the skew Ferrers diagrams as follows: A finite subset S of $\{1, 2, 3, \ldots\}^2$ is a skew Ferrers diagram (i.e., there exist two partitions λ and μ such that $\mu \subseteq \lambda$ and such that S is the skew Ferrers diagram λ/μ) if and only if for every $(i, j) \in S$, every $(i', j') \in \{1, 2, 3, \ldots\}^2$ and every $(i'', j'') \in S$ satisfying $i'' \leq i' \leq i$ and $j'' \leq j' \leq j$, we have $(i', j') \in S$.

[98] For example, this happens when $\lambda = (3, 2)$, $\mu = (1)$, $\lambda' = (5, 4)$ and $\mu' = (3, 1)$.

[99] As usual, we write ν_k for the k-th entry of a partition ν.

translation. Let γ and δ be two partitions such that $\delta \subseteq \gamma$ and such that the skew Ferrers diagram γ/δ can be obtained from $F_{\text{rows}>k}$ by parallel translation.[100] Prove that $s_{\lambda/\mu} = s_{\alpha/\beta} s_{\gamma/\delta}$.

Proposition 2.3.6. *The comultiplication $\Lambda \xrightarrow{\Delta} \Lambda \otimes \Lambda$ has the following effect on the symmetric functions discussed so far*[101]*:*

(i) $\Delta p_n = 1 \otimes p_n + p_n \otimes 1$ *for every* $n \geq 1$, *that is, the power sums* p_n *are primitive.*
(ii) $\Delta e_n = \sum_{i+j=n} e_i \otimes e_j$ *for every* $n \in \mathbb{N}$.
(iii) $\Delta h_n = \sum_{i+j=n} h_i \otimes h_j$ *for every* $n \in \mathbb{N}$.
(iv) $\Delta s_\lambda = \sum_{\mu \subseteq \lambda} s_\mu \otimes s_{\lambda/\mu}$ *for any partition* λ.
(v) $\Delta s_{\lambda/\nu} = \sum\limits_{\substack{\mu \in \text{Par}: \\ \nu \subseteq \mu \subseteq \lambda}} s_{\mu/\nu} \otimes s_{\lambda/\mu}$ *for any partitions* λ *and* ν.

Proof. Recall that Δ sends $f(\mathbf{x}) \mapsto f(\mathbf{x}, \mathbf{y})$, and one can easily check that

(i) $p_n(\mathbf{x}, \mathbf{y}) = \sum_i x_i^n + \sum_i y_i^n = p_n(\mathbf{x}) \cdot 1 + 1 \cdot p_n(\mathbf{y})$ for every $n \geq 1$;
(ii) $e_n(\mathbf{x}, \mathbf{y}) = \sum_{i+j=n} e_i(\mathbf{x}) e_j(\mathbf{y})$ for every $n \in \mathbb{N}$;
(iii) $h_n(\mathbf{x}, \mathbf{y}) = \sum_{i+j=n} h_i(\mathbf{x}) h_j(\mathbf{y})$ for every $n \in \mathbb{N}$.

For assertion (iv), note that by (2.2.6), one has

$$s_\lambda(\mathbf{x}, \mathbf{y}) = \sum_T (\mathbf{x}, \mathbf{y})^{\text{cont}(T)}, \tag{2.3.1}$$

where the sum is over column-strict tableaux T of shape λ having entries in the linearly ordered alphabet

$$x_1 < x_2 < \cdots < y_1 < y_2 < \cdots . \tag{2.3.2}$$

[102] For example,

$$T = \begin{array}{lllll} x_1 & x_1 & x_1 & y_2 & y_5 \\ x_2 & y_1 & y_1 & & \\ y_2 & y_2 & y_4 & & \\ y_4 & y_5 & & & \end{array}$$

is such a tableau of shape $\lambda = (5,3,3,2)$. Note that the restriction of T to the alphabet $\mathbf{x}$ gives a column-strict tableau $T_\mathbf{x}$ of some shape $\mu \subseteq \lambda$, and the restriction of T to the alphabet $\mathbf{y}$ gives a column-strict tableau $T_\mathbf{y}$ of shape λ/μ (e.g. for T in the example above, the tableau $T_\mathbf{y}$ appeared in Example 2.3.2). Consequently, one has

$$\begin{aligned} s_\lambda(\mathbf{x}, \mathbf{y}) &= \sum_T \mathbf{x}^{\text{cont}(T_\mathbf{x})} \cdot \mathbf{y}^{\text{cont}(T_\mathbf{y})} \\ &= \sum_{\mu \subseteq \lambda} \left(\sum_{T_\mathbf{x}} \mathbf{x}^{\text{cont}(T_\mathbf{x})} \right) \left(\sum_{T_\mathbf{y}} \mathbf{y}^{\text{cont}(T_\mathbf{y})} \right) = \sum_{\mu \subseteq \lambda} s_\mu(\mathbf{x}) s_{\lambda/\mu}(\mathbf{y}). \end{aligned} \tag{2.3.3}$$

[100] Here is an example of the situation: $\lambda = (6,5,5,2,2)$, $\mu = (4,4,3,1)$, $k = 3$ (satisfying $\mu_k = \mu_3 = 3 \geq 2 = \lambda_4 = \lambda_{k+1}$), $\alpha = (3,2,2)$, $\beta = (1,1)$, $\gamma = (2,2)$, and $\delta = (1)$.

[101] The abbreviated summation indexing $\sum_{i+j=n} t_{i,j}$ used here is intended to mean

$$\sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}} t_{i,j}.$$

[102] Here, $(\mathbf{x}, \mathbf{y})^{\text{cont}(T)}$ means the monomial $\prod_{a \in \mathfrak{A}} a^{|T^{-1}(a)|}$, where $\mathfrak{A}$ denotes the totally ordered alphabet $x_1 < x_2 < \cdots < y_1 < y_2 < \cdots$. In other words, $(\mathbf{x}, \mathbf{y})^{\text{cont}(T)}$ is the product of all entries of the tableau T (which is a monomial, since the entries of T are not numbers but variables).

The following rather formal argument should allay any doubts as to why (2.3.1) holds: Let $\mathcal{L}$ denote the totally ordered set which is given by the set $\{1, 2, 3, \ldots\}$ of positive integers, equipped with the total order $1 <_\mathcal{L} 3 <_\mathcal{L} 5 <_\mathcal{L} 7 <_\mathcal{L} \cdots <_\mathcal{L} 2 <_\mathcal{L} 4 <_\mathcal{L} 6 <_\mathcal{L} 8 <_\mathcal{L} \cdots$. Then, (2.2.6) yields $s_\lambda = \sum_T \mathbf{x}^{\text{cont}(T)}$ as T runs through all $\mathcal{L}$-column-strict tableaux of shape λ. Substituting the variables $x_1, y_1, x_2, y_2, x_3, y_3, \ldots$ for $x_1, x_2, x_3, x_4, x_5, x_6, \ldots$ (that is, substituting x_i for x_{2i-1} and y_i for x_{2i}) in this equality, we obtain (2.3.1).

Assertion (v) is obvious in the case when we don't have $\nu \subseteq \lambda$ (in fact, in this case, both $s_{\lambda/\nu}$ and $\sum_{\substack{\mu\in\mathrm{Par}:\\ \nu\subseteq\mu\subseteq\lambda}} s_{\mu/\nu}\otimes s_{\lambda/\mu}$ are clearly zero). In the remaining case, the proof of assertion (v) is similar to that of (iv). (Of course, the tableaux T and $T_{\mathbf{x}}$ now have skew shapes λ/ν and μ/ν, and instead of (2.2.6), we need to use the answer to Exercise 2.3.4(a).) □

Notice that parts (ii) and (iii) of Proposition 2.3.6 are particular cases of part (iv), since $h_n = s_{(n)}$ and $e_n = s_{(1^n)}$.

Exercise 2.3.7. (a) Show that the Hopf algebra Λ is cocommutative.

(b) Show that $\Delta s_{\lambda/\nu} = \sum_{\substack{\mu\in\mathrm{Par}:\\ \nu\subseteq\mu\subseteq\lambda}} s_{\lambda/\mu}\otimes s_{\mu/\nu}$ for any partitions λ and ν.

Exercise 2.3.8. Let $n\in\mathbb{N}$. Consider the finite variable set $(x_1,x_2,\ldots,x_n)$ as a subset of $\mathbf{x}=(x_1,x_2,x_3,\ldots)$. Recall that $f(x_1,x_2,\ldots,x_n)$ is a well-defined element of $\mathbf{k}[x_1,x_2,\ldots,x_n]$ for every $f\in R(\mathbf{x})$ (and therefore also for every $f\in\Lambda$, since $\Lambda\subset R(\mathbf{x})$), according to Exercise 2.1.2.

(a) Show that any two partitions λ and μ satisfy

$$s_{\lambda/\mu}(x_1,x_2,\ldots,x_n) = \sum_{\substack{T \text{ is a column-strict}\\ \text{tableau of shape } \lambda/\mu;\\ \text{all entries of } T \text{ belong}\\ \text{to } \{1,2,\ldots,n\}}} \mathbf{x}^{\mathrm{cont}(T)}.$$

(b) If λ is a partition having more than n parts[103], then show that $s_\lambda(x_1,x_2,\ldots,x_n)=0$.

Remark 2.3.9. An analogue of Proposition 2.2.10 holds for symmetric polynomials in finitely many variables: Let $N\in\mathbb{N}$. Then, we have

(a) The family $\{m_\lambda(x_1,x_2,\ldots,x_N)\}$, as λ runs through all partitions having length $\leq N$, is a graded basis of the graded $\mathbf{k}$-module $\Lambda(x_1,x_2,\ldots,x_N)=\mathbf{k}[x_1,x_2,\ldots,x_N]^{\mathfrak{S}_N}$.

(b) For any partition λ having length $>N$, we have $m_\lambda(x_1,x_2,\ldots,x_N)=0$.

(c) The family $\{e_\lambda(x_1,x_2,\ldots,x_N)\}$, as λ runs through all partitions whose parts are all $\leq N$, is a graded basis of the graded $\mathbf{k}$-module $\Lambda(x_1,x_2,\ldots,x_N)$.

(d) The family $\{s_\lambda(x_1,x_2,\ldots,x_N)\}$, as λ runs through all partitions having length $\leq N$, is a graded basis of the graded $\mathbf{k}$-module $\Lambda(x_1,x_2,\ldots,x_N)$.

(e) If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the family $\{p_\lambda(x_1,x_2,\ldots,x_N)\}$, as λ runs through all partitions having length $\leq N$, is a graded basis of the graded $\mathbf{k}$-module $\Lambda(x_1,x_2,\ldots,x_N)$.

(f) If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the family $\{p_\lambda(x_1,x_2,\ldots,x_N)\}$, as λ runs through all partitions whose parts are all $\leq N$, is a graded basis of the graded $\mathbf{k}$-module $\Lambda(x_1,x_2,\ldots,x_N)$.

Indeed, the claims (a) and (b) are obvious, while the claims (c), (d) and (e) are proven similarly to our proof of Proposition 2.2.10. We leave the proof of (f) to the reader; this proof can also be found in [138, Theorem 10.86][104].

Claim (c) can be rewritten as follows: The elementary symmetric polynomials $e_i(x_1,x_2,\ldots,x_N)$, for $i\in\{1,2,\ldots,N\}$, form an algebraically independent generating set of $\Lambda(x_1,x_2,\ldots,x_N)$. This is precisely the well-known theorem (due to Gauss)[105] that every symmetric polynomial in N variables $x_1,x_2,\ldots,x_N$ can be written uniquely as a polynomial in the N elementary symmetric polynomials.

2.4. **The antipode, the involution ω, and algebra generators.** Since Λ is a connected graded $\mathbf{k}$-bialgebra, it will have an antipode $\Lambda\xrightarrow{S}\Lambda$ making it a Hopf algebra by Proposition 1.4.16. However, we can identify S more explicitly now.

Proposition 2.4.1. *Each of the families $\{e_n\}_{n=1,2,\ldots}$ and $\{h_n\}_{n=1,2,\ldots}$ are algebraically independent, and generate $\Lambda_{\mathbf{k}}$ as a polynomial algebra for any commutative ring $\mathbf{k}$. The same holds for $\{p_n\}_{n=1,2,\ldots}$ when $\mathbb{Q}$ is a subring of $\mathbf{k}$.*

Furthermore, the antipode S acts as follows:

[103] Recall that the *parts* of a partition are its nonzero entries.

[104] See [138, Remark 10.76] for why [138, Theorem 10.86] is equivalent to our claim (f).

[105] See, e.g., [40, *Symmetric Polynomials*, Theorem 5 and Remark 17] or [221, §5.3] or [26, Theorem 1]. In a slightly different form, it also appears in [119, Theorem (5.10)].

(i) $S(p_n) = -p_n$ *for every positive integer* n.
(ii) $S(e_n) = (-1)^n h_n$ *for every* $n \in \mathbb{N}$.
(iii) $S(h_n) = (-1)^n e_n$ *for every* $n \in \mathbb{N}$.

Proof. The assertion that $\{e_n\}_{n\geq 1}$ are algebraically independent and generate Λ is equivalent to Proposition 2.2.10 asserting that $\{e_\lambda\}_{\lambda\in \mathrm{Par}}$ is a basis for Λ. (Indeed, this equivalence follows from parts (b) and (c) of Exercise 2.2.14, applied to $v_n = e_n$ and $v_\lambda = e_\lambda$.) Thus, the former assertion is true. If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then a similar argument (using p_n and p_λ instead of e_n and e_λ) shows that $\{p_n\}_{n\geq 1}$ are algebraically independent and generate Λ.

The assertion $S(p_n) = -p_n$ follows from Proposition 1.4.17 since p_n is primitive by Proposition 2.3.6(i).

For the remaining assertions, start with the easy generating function identities[106]

$$H(t) := \prod_{i=1}^{\infty} (1 - x_i t)^{-1} = 1 + h_1(\mathbf{x})t + h_2(\mathbf{x})t^2 + \cdots = \sum_{n\geq 0} h_n(\mathbf{x})t^n; \tag{2.4.1}$$

$$E(t) := \prod_{i=1}^{\infty} (1 + x_i t) = 1 + e_1(\mathbf{x})t + e_2(\mathbf{x})t^2 + \cdots = \sum_{n\geq 0} e_n(\mathbf{x})t^n. \tag{2.4.2}$$

These show that

$$1 = E(-t)H(t) = \left(\sum_{n\geq 0} e_n(\mathbf{x})(-t)^n\right)\left(\sum_{n\geq 0} h_n(\mathbf{x})t^n\right). \tag{2.4.3}$$

Hence, equating coefficients of powers of t, we see that for $n = 0, 1, 2, \ldots$ we have

$$\sum_{i+j=n} (-1)^i e_i h_j = \delta_{0,n}. \tag{2.4.4}$$

This lets us recursively express the e_n in terms of h_n and vice-versa:

$$e_0 = 1 = h_0; \tag{2.4.5}$$

$$e_n = e_{n-1}h_1 - e_{n-2}h_2 + e_{n-3}h_3 - \cdots; \tag{2.4.6}$$

$$h_n = h_{n-1}e_1 - h_{n-2}e_2 + h_{n-3}e_3 - \cdots \tag{2.4.7}$$

for $n = 1, 2, 3, \ldots$ Now, let us use the algebraic independence of the generators $\{e_n\}$ for Λ to define a $\mathbf{k}$-algebra endomorphism

$$\begin{array}{ccc} \Lambda & \overset{\omega}{\to} & \Lambda, \\ e_n & \longmapsto & h_n \qquad \text{(for positive integers } n\text{)}. \end{array}$$

Then,

$$\omega(e_n) = h_n \qquad \text{for each } n \geq 0 \tag{2.4.8}$$

(indeed, this holds for $n > 0$ by definition, and for $n = 0$ because $\omega(e_0) = \omega(1) = 1 = h_0$). Hence, the identical form of the two recursions (2.4.6) and (2.4.7) shows that

$$\omega(h_n) = e_n \qquad \text{for each } n \geq 0 \tag{2.4.9}$$

[107]. Combining this with (2.4.8), we conclude that $(\omega \circ \omega)(e_n) = e_n$ for each $n \geq 0$. Therefore, the two $\mathbf{k}$-algebra homomorphisms $\omega \circ \omega : \Lambda \to \Lambda$ and $\mathrm{id} : \Lambda \to \Lambda$ agree on each element of the generating set

[106] See the solution to Exercise 2.2.15 for the proofs of the identities.

[107] Here is this argument in more detail: We must show that $\omega(h_n) = e_n$ for each $n \geq 0$. We shall prove this by strong induction on n. Thus, we fix an $n \geq 0$, and assume as induction hypothesis that $\omega(h_m) = e_m$ for each $m < n$. We must then prove that $\omega(h_n) = e_n$. If $n = 0$, then this is obvious; thus, assume WLOG that $n > 0$. Hence,

$$\begin{aligned} \omega(h_n) &= \omega(h_{n-1}e_1 - h_{n-2}e_2 + h_{n-3}e_3 - \cdots) \qquad \text{(by (2.4.7))} \\ &= \omega(h_{n-1})\omega(e_1) - \omega(h_{n-2})\omega(e_2) + \omega(h_{n-3})\omega(e_3) - \cdots \qquad \text{(since } \omega \text{ is a } \mathbf{k}\text{-algebra homomorphism)} \\ &= e_{n-1}\omega(e_1) - e_{n-2}\omega(e_2) + e_{n-3}\omega(e_3) - \cdots \qquad \text{(since } \omega(h_m) = e_m \text{ for each } m < n\text{)} \\ &= e_{n-1}h_1 - e_{n-2}h_2 + e_{n-3}h_3 - \cdots \qquad \text{(since (2.4.8) shows that } \omega(e_m) = h_m \text{ for each } m \geq 0\text{)} \\ &= e_n \qquad \text{(by (2.4.6))}, \end{aligned}$$

as desired. This completes the induction step.

$\{e_n\}$ of Λ. Hence, they are equal, i.e., we have $\omega \circ \omega = \mathrm{id}$. Therefore ω is an involution and therefore a $\mathbf{k}$-algebra automorphism of Λ. This, in turn, yields that the $\{h_n\}$ (being the images of the $\{e_n\}$ under this automorphism) are another algebraically independent generating set for Λ.

For the assertion about the antipode S applied to e_n or h_n, note that the coproduct formulas for e_n, h_n in Proposition 2.3.6(ii),(iii) show that the defining relations for their antipodes (1.4.4) will in this case be

$$\sum_{i+j=n} S(e_i)e_j = \delta_{0,n} = \sum_{i+j=n} e_i S(e_j),$$
$$\sum_{i+j=n} S(h_i)h_j = \delta_{0,n} = \sum_{i+j=n} h_i S(h_j)$$

because $u\epsilon(e_n) = u\epsilon(h_n) = \delta_{0,n}$. Comparing these to (2.4.4), one concludes via induction on n that $S(e_n) = (-1)^n h_n$ and $S(h_n) = (-1)^n e_n$. □

The $\mathbf{k}$-algebra endomorphism ω of Λ defined in the proof of Proposition 2.4.1 is sufficiently important that we record its definition and a selection of fundamental properties:

Definition 2.4.2. Let ω be the $\mathbf{k}$-algebra homomorphism

$$\begin{array}{ccc} \Lambda & \to & \Lambda, \\ e_n & \longmapsto & h_n \end{array} \qquad \text{(for positive integers } n\text{)}. \tag{2.4.10}$$

This homomorphism ω is known as the *fundamental involution* of Λ.

Proposition 2.4.3. *Consider the fundamental involution ω and the antipode S of the Hopf algebra Λ.*

(a) *We have*
$$\omega(e_n) = h_n \qquad \text{for each } n \in \mathbb{Z}.$$

(b) *We have*
$$\omega(h_n) = e_n \qquad \text{for each } n \in \mathbb{Z}.$$

(c) *We have*
$$\omega(p_n) = (-1)^{n-1} p_n \qquad \text{for each positive integer } n.$$

(d) *The map ω is a $\mathbf{k}$-algebra automorphism of Λ and an involution.*

(e) *If $n \in \mathbb{N}$, then*
$$S(f) = (-1)^n \omega(f) \qquad \text{for all } f \in \Lambda_n. \tag{2.4.11}$$

(f) *The map ω is a Hopf algebra automorphism of Λ.*

(g) *The map S is a Hopf algebra automorphism of Λ.*

(h) *Every partition λ satisfies the three equalities*
$$\omega(h_\lambda) = e_\lambda; \tag{2.4.12}$$
$$\omega(e_\lambda) = h_\lambda; \tag{2.4.13}$$
$$\omega(p_\lambda) = (-1)^{|\lambda| - \ell(\lambda)} p_\lambda. \tag{2.4.14}$$

(i) *The map ω is an isomorphism of graded $\mathbf{k}$-modules.*

(j) *The family $(h_\lambda)_{\lambda \in \mathrm{Par}}$ is a graded basis of the graded $\mathbf{k}$-module Λ.*

Exercise 2.4.4. Prove Proposition 2.4.3.

[**Hint:** Parts (a), (b) and (d) have been shown in the proof of Proposition 2.4.1 above. For part (e), let $D_{-1} : \Lambda \to \Lambda$ be the $\mathbf{k}$-algebra morphism sending each homogeneous $f \in \Lambda_n$ to $(-1)^n f$; then argue that $\omega \circ D_{-1}$ and S are two $\mathbf{k}$-algebra morphisms that agree on all elements of the generating set $\{e_n\}$. Derive part (c) from (d) and Proposition 2.4.1. Part (h) then follows by multiplicativity. For parts (f) and (g), check the coalgebra homomorphism axioms on the e_n. Parts (i) and (j) are easy consequences.]

Proposition 2.4.3(e) shows that the antipode S on Λ is, up to sign, the same as the fundamental involution ω. Thus, studying ω is essentially equivalent to studying S.

Remark 2.4.5. Up to now we have not yet derived how the involution ω and the antipode S act on (skew) Schur functions, which is quite beautiful: If λ and μ are partitions satisfying $\mu \subseteq \lambda$, then

$$\begin{aligned} \omega(s_{\lambda/\mu}) &= s_{\lambda^t/\mu^t}, \\ S(s_{\lambda/\mu}) &= (-1)^{|\lambda/\mu|} s_{\lambda^t/\mu^t} \end{aligned} \tag{2.4.15}$$

where recall that λ^t is the transpose or conjugate partition to λ, and $|\lambda/\mu|$ is the number of squares in the skew diagram λ/μ, that is, $|\lambda/\mu| = n - k$ if λ, μ lie in $\mathrm{Par}_n, \mathrm{Par}_k$ respectively.

We will deduce this later in three ways (once as an exercise using the Pieri rules in Exercise 2.7.11, once again using skewing operators in Exercise 2.8.7, and for the third time from the action of the antipode in QSym on P-partition enumerators in Corollary 5.2.22). However, one could also deduce it immediately from our knowledge of the action of ω and S on e_n, h_n, if we were to prove the following famous *Jacobi-Trudi* and *dual Jacobi-Trudi* formulas[108]:

Theorem 2.4.6. *Skew Schur functions are the following polynomials in* $\{h_n\}, \{e_n\}$*:*

$$s_{\lambda/\mu} = \det(h_{\lambda_i - \mu_j - i + j})_{i,j=1,2,\ldots,\ell}, \tag{2.4.16}$$

$$s_{\lambda^t/\mu^t} = \det(e_{\lambda_i - \mu_j - i + j})_{i,j=1,2,\ldots,\ell} \tag{2.4.17}$$

for any two partitions λ *and* μ *and any* $\ell \in \mathbb{N}$ *satisfying* $\ell(\lambda) \leq \ell$ *and* $\ell(\mu) \leq \ell$*.*

Since we appear not to need these formulas in the sequel, we will not prove them right away. However, a proof is sketched in the solution to Exercise 2.7.13, and various proofs are well-explained in [126, (39) and (41)], [142, §I.5], [184, Thm. 7.1], [186, §4.5], [206, §7.16], [220, Thms. 3.5 and 3.5*]; also, a simultaneous generalization of both formulas is shown in [83, Theorem 11], and three others in [181, 1.9], [88, Thm. 3.1] and [105]. An elegant treatment of Schur polynomials taking the Jacobi-Trudi formula (2.4.16) as the *definition* of s_λ is given by Tamvakis [215].

2.5. **Cauchy product, Hall inner product, self-duality.** The Schur functions, although a bit unmotivated right now, have special properties with regard to the Hopf structure. One property is intimately connected with the following *Cauchy identity*.

Theorem 2.5.1. *In the power series ring* $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] := \mathbf{k}[[x_1, x_2, \ldots, y_1, y_2, \ldots]]$*, one has the following expansion:*

$$\prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1} = \sum_{\lambda \in \mathrm{Par}} s_\lambda(\mathbf{x}) s_\lambda(\mathbf{y}). \tag{2.5.1}$$

Remark 2.5.2. The left hand side of (2.5.1) is known as the *Cauchy product*, or *Cauchy kernel*.

An equivalent version of the equality (2.5.1) is obtained by replacing each x_i by $x_i t$, and writing the resulting identity in the power series ring $R(\mathbf{x}, \mathbf{y})[[t]]$:

$$\prod_{i,j=1}^{\infty} (1 - t x_i y_j)^{-1} = \sum_{\lambda \in \mathrm{Par}} t^{|\lambda|} s_\lambda(\mathbf{x}) s_\lambda(\mathbf{y}). \tag{2.5.2}$$

(Recall that $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_\ell$ for any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$.)

Proof of Theorem 2.5.1. We follow the standard combinatorial proof (see [186, §4.8],[206, §7.11,7.12]), which rewrites the left and right sides of (2.5.2), and then compares them with the *Robinson-Schensted-Knuth* (RSK) bijection.[109] On the left side, expanding out each geometric series

$$(1 - t x_i y_j)^{-1} = 1 + t x_i y_j + (t x_i y_j)^2 + (t x_i y_j)^3 + \cdots$$

[108] The second of the following identities is also known as the *von Nägelsbach-Kostka identity*.

[109] The RSK bijection has been introduced by Knuth [111], where what we call "biletters" is referred to as "two-line arrays". The most important ingredient of this algorithm – the RS-insertion operation – however goes back to Schensted. The special case of the RSK algorithm where the biword has to be a permutation (written in two-line notation) and the two tableaux have to be *standard* (i.e., each of them has content (1^n), where n is the size of their shape) is the famous *Robinson-Schensted correspondence* [130]. More about these algorithms can be found in [186, Chapter 3], [154, Chapter 5], [206, §7.11-7.12], [138, Sections 10.9–10.22], [73, Chapters 1 and A], [28, §3, §6] and various other places.

and thinking of $(x_i y_j)^m$ as m occurrences of a *biletter*[110] $\binom{i}{j}$, we see that the left hand side can be rewritten as the sum of $t^\ell (x_{i_1} y_{j_1})(x_{i_2} y_{j_2}) \cdots (x_{i_\ell} y_{j_\ell})$ over all multisets $\left\{ \binom{i_1}{j_1}, \ldots, \binom{i_\ell}{j_\ell} \right\}_{\text{multiset}}$ of biletters. Order the biletters in such a multiset in the lexicographic order $\leq_{lex}$, which is the total order on the set of all biletters defined by

$$\binom{i_1}{j_1} \leq_{lex} \binom{i_2}{j_2} \quad \Longleftrightarrow \quad (\text{we have } i_1 \leq i_2, \text{ and if } i_1 = i_2, \text{ then } j_1 \leq j_2).$$

Defining a *biword* to be an array $\binom{\mathbf{i}}{\mathbf{j}} = \binom{i_1 \cdots i_\ell}{j_1 \cdots j_\ell}$ in which the biletters are ordered $\binom{i_1}{j_1} \leq_{lex} \cdots \leq_{lex} \binom{i_\ell}{j_\ell}$, then the left side of (2.5.2) is the sum $\sum t^\ell \mathbf{x}^{\mathrm{cont}(\mathbf{i})} \mathbf{y}^{\mathrm{cont}(\mathbf{j})}$ over all biwords $\binom{\mathbf{i}}{\mathbf{j}}$, where ℓ stands for the number of biletters in the biword. On the right side, expanding out the Schur functions as sums of tableaux gives $\sum_{(P,Q)} t^\ell \mathbf{x}^{\mathrm{cont}(Q)} \mathbf{y}^{\mathrm{cont}(P)}$ in which the sum is over all ordered pairs (P, Q) of column-strict tableaux *having the same shape*[111], with ℓ cells. (We shall refer to such pairs as *tableau pairs* from now on.)

The *Robinson-Schensted-Knuth algorithm* gives us a bijection between the biwords $\binom{\mathbf{i}}{\mathbf{j}}$ and the tableau pairs (P, Q), which has the property that

$$\mathrm{cont}(\mathbf{i}) = \mathrm{cont}(Q),$$
$$\mathrm{cont}(\mathbf{j}) = \mathrm{cont}(P)$$

(and that the length ℓ of the biword $\binom{\mathbf{i}}{\mathbf{j}}$ equals the size $|\lambda|$ of the common shape of P and Q; but this follows automatically from $\mathrm{cont}(\mathbf{i}) = \mathrm{cont}(Q)$). Clearly, once such a bijection is constructed, the equality (2.5.2) will follow.

Before we define this algorithm, we introduce a simpler operation known as *RS-insertion* (short for Robinson-Schensted insertion). RS-insertion takes as input a column-strict tableau P and a letter j, and returns a new column-strict tableau P' along with a corner cell[112] c of P', which is constructed as follows: Start out by setting $P' = P$. The letter j tries to insert itself into the first row of P' by either bumping out the leftmost letter in the first row strictly larger than j, or else placing itself at the right end of the row if no such larger letter exists. If a letter was bumped from the first row, this letter follows the same rules to insert itself into the second row, and so on[113]. This series of bumps must eventually come to an end[114]. At the end of the bumping, the tableau P' created has an extra corner cell not present in P. If we call this corner cell c, then P' (in its final form) and c are what the RS-insertion operation returns. One says that P' is the result of *inserting*[115] j into the tableau P. It is straightforward to see that this resulting filling P' is a column-strict tableau[116].

Example 2.5.3. To give an example of this operation, let us insert the letter $j = 3$ into the column-strict tableau $\begin{array}{llllll} 1 & 1 & 3 & 3 & 4 \\ 2 & 2 & 4 & 6 & \\ 3 & 4 & 7 & & \\ 5 & & & & \end{array}$ (we are showing all intermediate states of P'; the underlined letter is always the one

[110] A *biletter* here simply means a pair of letters, written as a column vector. A *letter* means a positive integer.

[111] And this shape should be the Ferrers diagram of a partition (not just a skew diagram).

[112] A *corner cell* of a tableau or of a Ferrers diagram is defined to be a cell c which belongs to the tableau (resp. diagram) but whose immediate neighbors to the east and to the south don't. For example, the cell $(3, 2)$ is a corner cell of the Ferrers diagram of the partition $(3, 2, 2, 1)$, and thus also of any tableau whose shape is this partition. But the cell $(2, 2)$ is not a corner cell of this Ferrers diagram, since its immediate neighbor to the south is still in the diagram.

[113] Here, rows are allowed to be empty – so it is possible that a letter is bumped from the last nonempty row of P' and settles in the next, initially empty, row.

[114] since we can only bump out entries from nonempty rows

[115] This terminology is reminiscent of insertion into binary search trees, a basic operation in theoretical computer science. This is more than superficial similarity; there are, in fact, various analogies between Ferrers diagrams (and their fillings) and unlabelled plane binary trees (resp. their labellings), and one of them is the analogy between RS-insertion and binary search tree insertion. See [97, §4.1].

[116] Indeed, the reader can check that P' remains a column-strict tableau throughout the algorithm that defines RS-insertion. (The only part of this that isn't obvious is showing that when a letter t bumped out of some row k is inserted into row $k+1$, the property that the letters increase strictly down columns is preserved. Argue that the bumping-out of t from row k was caused by the insertion of another letter $u < t$, and that the cell of row $k+1$ into which t is then being inserted is in the same column as this u, or in a column further left than it.)

that is going to be bumped out at the next step):

$$\begin{array}{llllll} 1 & 1 & 3 & 3 & \underline{4} \\ 2 & 2 & 4 & 6 & \\ 3 & 4 & 7 & & \\ 5 & & & & \end{array} \quad \begin{array}{c} \longmapsto \\ \text{insert 3;} \\ \text{bump out 4} \end{array} \quad \begin{array}{lllll} 1 & 1 & 3 & 3 & 3 \\ 2 & 2 & 4 & \underline{6} & \\ 3 & 4 & 7 & & \\ 5 & & & & \end{array} \quad \begin{array}{c} \longmapsto \\ \text{insert 4;} \\ \text{bump out 6} \end{array} \quad \begin{array}{lllll} 1 & 1 & 3 & 3 & 3 \\ 2 & 2 & 4 & 4 & \\ 3 & 4 & \underline{7} & & \\ 5 & & & & \end{array}$$

$$\begin{array}{c} \longmapsto \\ \text{insert 6;} \\ \text{bump out 7} \end{array} \quad \begin{array}{lllll} 1 & 1 & 3 & 3 & 3 \\ 2 & 2 & 4 & 4 & \\ 3 & 4 & 6 & & \\ 5 & & & & \end{array} \quad \begin{array}{c} \longmapsto \\ \text{insert 7;} \\ \text{done} \end{array} \quad \begin{array}{lllll} 1 & 1 & 3 & 3 & 3 \\ 2 & 2 & 4 & 4 & \\ 3 & 4 & 6 & & \\ 5 & 7 & & & \end{array} .$$

The last tableau in this sequence is the column-strict tableau that is returned. The corner cell that is returned is the second cell of the fourth row (the one containing 7).

RS-insertion will be used as a step in the RSK algorithm; the construction will rely on a simple fact known as the *row bumping lemma*. Let us first define the notion of a *bumping path* (or *bumping route*): If P is a column-strict tableau, and j is a letter, then some letters are inserted into some cells when RS-insertion is applied to P and j. The sequence of these cells (in the order in which they see letters inserted into them) is called the *bumping path* for P and j. This bumping path always ends with the corner cell c which is returned by RS-insertion. As an example, when $j = 1$ is inserted into the tableau P shown below, the result P' is shown with all entries on the bumping path underlined:

$$P = \begin{array}{llll} 1 & 1 & 2 & 2 & 3 \\ 2 & 2 & 4 & 4 & \\ 3 & 4 & 5 & & \\ 4 & 6 & 6 & & \end{array} \quad \begin{array}{c} \overset{\text{insert}}{\longmapsto} \\ j=1 \end{array} \quad P' = \begin{array}{llll} 1 & 1 & \underline{1} & 2 & 3 \\ 2 & 2 & \underline{2} & 4 & \\ 3 & 4 & \underline{4} & & \\ 4 & \underline{5} & 6 & & \\ \underline{6} & & & & \end{array}$$

A first simple observation about bumping paths is that bumping paths *trend weakly left* – that is, if the bumping path of P and j is $(c_1, c_2, \ldots, c_k)$, then, for each $1 \leq i < k$, the cell c_{i+1} lies in the same column as c_i or in a column further left.[117] A subtler property of bumping paths is the following *row bumping lemma* ([73, p. 9]):

> **Row bumping lemma:** Let P be a column-strict tableau, and let j and j' be two letters. Applying RS-insertion to the tableau P and the letter j yields a new column-strict tableau P' and a corner cell c. Applying RS-insertion to the tableau P' and the letter j' yields a new column-strict tableau P'' and a corner cell c'.
>
> (a) Assume that $j \leq j'$. Then, the bumping path for P' and j' stays strictly to the right, within each row, of the bumping path for P and j. The cell c' (in which the bumping path for P' and j' ends) is in the same row as the cell c (in which the bumping path for P and j ends) or in a row further up; it is also in a column further right than c.
>
> (b) Assume instead that $j > j'$. Then, the bumping path for P' and j' stays weakly to the left, within each row, of the bumping path for P and j. The cell c' (in which the bumping path for P' and j' ends) is in a row further down than the cell c (in which the bumping path for P and j ends); it is also in the same column as c or in a column further left.

This lemma can be easily proven by induction over the row.[118]

[117] This follows easily from the preservation of column-strictness during RS-insertion.

[118] We leave the details to the reader, only giving the main idea for (a) (the proof of (b) is similar). To prove the first claim of (a), it is enough to show that for every i, if any letter is inserted into row i during RS-insertion for P' and j', then some letter is also inserted into row i during RS-insertion for P and j, and the former insertion happens in a cell strictly to the right of the cell where the latter insertion happens. This follows by induction over i. In the induction step, we need to show that if, for a positive integer i, we try to consecutively insert two letters k and k', in this order, into the i-th row of a column-strict tableau, possibly bumping out existing letters in the process, and if we have $k \leq k'$, then the cell into which k is inserted is strictly to the left of the cell into which k' is inserted, and the letter bumped out by the insertion of k is $\leq$ to the letter bumped out by the insertion of k' (or else the insertion of k' bumps out no letter at all – but it cannot happen that k' bumps out a letter but k does not). This statement is completely straightforward to check (by only studying the i-th row). This way, the first claim of (a) is proven, and this entails that the cell c' (being the last cell of the bumping path for P' and j') is in the same row as the cell c or in a row further up. It only remains to show that c' is in a column further right than c. This follows by noticing

We can now define the actual RSK algorithm. Let $\binom{\mathbf{i}}{\mathbf{j}}$ be a biword. Starting with the pair $(P_0, Q_0) = (\varnothing, \varnothing)$ and $m = 0$, the algorithm applies the following steps (see Example 2.5.4 below):

- If i_{m+1} does not exist (that is, m is the length of $\mathbf{i}$), stop.
- Apply RS-insertion to the column-strict tableau P_m and the letter j_{m+1} (the bottom letter of $\binom{i_{m+1}}{j_{m+1}}$). Let P_{m+1} be the resulting column-strict tableau, and let c_{m+1} be the resulting corner cell.
- Create Q_{m+1} from Q_m by adding the top letter i_{m+1} of $\binom{i_{m+1}}{j_{m+1}}$ to Q_m in the cell c_{m+1} (which, as we recall, is the extra corner cell of P_{m+1} not present in P_m).
- Set m to $m+1$.

After all of the biletters have been thus processed, the result of the RSK algorithm is $(P_\ell, Q_\ell) =: (P, Q)$.

Example 2.5.4. The term in the expansion of the left side of (2.5.1) corresponding to

$$(x_1y_2)^1(x_1y_4)^1(x_2y_1)^1(x_4y_1)^1(x_4y_3)^2(x_5y_2)^1$$

is the biword $\binom{\mathbf{i}}{\mathbf{j}} = \binom{1124445}{2411332}$, whose RSK algorithm goes as follows:

$$\begin{array}{rcl|rcl}
P_0 & = & \varnothing & Q_0 & = & \varnothing \\
P_1 & = & 2 & Q_1 & = & 1 \\
P_2 & = & 2\ 4 & Q_2 & = & 1\ 1 \\
P_3 & = & \begin{array}{ll}1 & 4\\ 2 & \end{array} & Q_3 & = & \begin{array}{ll}1 & 1\\ 2 & \end{array} \\
P_4 & = & \begin{array}{ll}1 & 1\\ 2 & 4\end{array} & Q_4 & = & \begin{array}{ll}1 & 1\\ 2 & 4\end{array} \\
P_5 & = & \begin{array}{lll}1 & 1 & 3\\ 2 & 4 & \end{array} & Q_5 & = & \begin{array}{lll}1 & 1 & 4\\ 2 & 4 & \end{array} \\
P_6 & = & \begin{array}{llll}1 & 1 & 3 & 3\\ 2 & 4 & & \end{array} & Q_6 & = & \begin{array}{llll}1 & 1 & 4 & 4\\ 2 & 4 & & \end{array} \\
P := P_7 & = & \begin{array}{llll}1 & 1 & 2 & 3\\ 2 & 3 & & \\ 4 & & & \end{array} & Q := Q_7 & = & \begin{array}{llll}1 & 1 & 4 & 4\\ 2 & 4 & & \\ 5 & & & \end{array}
\end{array}$$

The bumping rule obviously maintains the property that P_m is a column-strict tableau of some Ferrers shape throughout. It should be clear that (P_m, Q_m) have the same shape at each stage. Also, the construction of Q_m shows that it is at least weakly increasing in rows and weakly increasing in columns throughout. What is perhaps least clear is that Q_m remains strictly increasing down columns. That is, when one has a string of equal letters on top $i_m = i_{m+1} = \cdots = i_{m+r}$, so that on bottom one bumps in $j_m \leq j_{m+1} \leq \cdots \leq j_{m+r}$, one needs to know that the new cells form a *horizontal strip*, that is, no two of them lie in the same column[119]. This follows from (the last claim of) part (a) of the row bumping lemma. Hence, the result (P, Q) of the RSK algorithm is a tableau pair.

To see that the RSK map is a bijection, we show how to recover $\binom{\mathbf{i}}{\mathbf{j}}$ from (P, Q). This is done by *reverse bumping* from (P_{m+1}, Q_{m+1}) to recover both the biletter $\binom{i_{m+1}}{j_{m+1}}$ and the tableaux (P_m, Q_m), as follows. Firstly, i_{m+1} is the maximum entry of Q_{m+1}, and Q_m is obtained by removing the rightmost occurrence of

that, if k is the row in which the cell c' lies, then c' is in a column further right than the entry of the bumping path for P and j in row k (by the first claim of (a)), and this latter entry is further right than or in the same column as the ultimate entry c of this bumping path (since bumping paths trend weakly left).

[119] Actually, each of these new cells (except for the first one) is in a column further right than the previous one. We will use this stronger fact further below.

this letter i_{m+1} from Q_{m+1}. [120] To produce P_m and j_{m+1}, find the position of the rightmost occurrence of i_{m+1} in Q_{m+1}, and start *reverse bumping* in P_{m+1} from the entry in this same position, where reverse bumping an entry means inserting it into one row higher by having it bump out the rightmost entry which is strictly smaller.[121] The entry bumped out of the first row is j_{m+1}, and the resulting tableau is P_m.

Finally, to see that the RSK map is surjective, one needs to show that the reverse bumping procedure can be applied to any pair (P, Q) of column-strict tableaux of the same shape, and will result in a (lexicographically ordered) biword $\left(\begin{smallmatrix}\mathbf{i}\\ \mathbf{j}\end{smallmatrix}\right)$. We leave this verification to the reader.[122] □

This is by far not the only known proof of Theorem 2.5.1. Two further proofs will be sketched in Exercise 2.7.10 and Exercise 2.7.8.

Before we move on to extracting identities in Λ from Theorem 2.5.1, let us state (as an exercise) a simple technical fact that will be useful:

Exercise 2.5.5. Let $(q_\lambda)_{\lambda\in\mathrm{Par}}$ be a basis of the $\mathbf{k}$-module Λ. Assume that for each partition λ, the element $q_\lambda \in \Lambda$ is homogeneous of degree $|\lambda|$.

(a) If two families $(a_\lambda)_{\lambda\in\mathrm{Par}} \in \mathbf{k}^{\mathrm{Par}}$ and $(b_\lambda)_{\lambda\in\mathrm{Par}} \in \mathbf{k}^{\mathrm{Par}}$ satisfy

$$\sum_{\lambda\in\mathrm{Par}} a_\lambda q_\lambda(\mathbf{x}) = \sum_{\lambda\in\mathrm{Par}} b_\lambda q_\lambda(\mathbf{x}) \tag{2.5.3}$$

in $\mathbf{k}[[\mathbf{x}]]$, then $(a_\lambda)_{\lambda\in\mathrm{Par}} = (b_\lambda)_{\lambda\in\mathrm{Par}}$. [123]

(b) Consider a further infinite family $\mathbf{y} = (y_1, y_2, y_3, \ldots)$ of indeterminates (disjoint from $\mathbf{x}$). If two families $(a_{\mu,\nu})_{(\mu,\nu)\in\mathrm{Par}^2} \in \mathbf{k}^{\mathrm{Par}^2}$ and $(b_{\mu,\nu})_{(\mu,\nu)\in\mathrm{Par}^2} \in \mathbf{k}^{\mathrm{Par}^2}$ satisfy

$$\sum_{(\mu,\nu)\in\mathrm{Par}^2} a_{\mu,\nu} q_\mu(\mathbf{x}) q_\nu(\mathbf{y}) = \sum_{(\mu,\nu)\in\mathrm{Par}^2} b_{\mu,\nu} q_\mu(\mathbf{x}) q_\nu(\mathbf{y}) \tag{2.5.4}$$

---

[120] It necessarily has to be the rightmost occurrence, since (according to the previous footnote) the cell into which i_{m+1} was filled at the step from Q_m to Q_{m+1} lies further right than any existing cell of Q_m containing the letter i_{m+1}.

[121] Let us give a few more details on this "reverse bumping" procedure. Reverse bumping (also known as *RS-deletion* or *reverse RS-insertion*) is an operation which takes a column-strict tableau P' and a corner cell c of P', and constructs a column-strict tableau P and a letter j such that RS-insertion for P and j yields P' and c. It starts by setting $P = P'$, and removing the entry in the cell c from P. This removed entry is then denoted by k, and is inserted into the row of P above c, bumping out the rightmost entry which is smaller than k. The letter which is bumped out – say, ℓ –, in turn, is inserted into the row above it, bumping out the rightmost entry which is smaller than ℓ. This procedure continues in the same way until an entry is bumped out of the first row (which will eventually happen). The reverse bumping operation returns the resulting tableau P and the entry which is bumped out of the first row.

It is straightforward to check that the reverse bumping operation is well-defined (i.e., P does stay a column-strict tableau throughout the procedure) and is the inverse of the RS-insertion operation. (In fact, these two operations undo each other step by step.)

[122] It is easy to see that repeatedly applying reverse bumping to (P, Q) will result in a sequence $\left(\begin{smallmatrix}i_\ell\\ j_\ell\end{smallmatrix}\right), \left(\begin{smallmatrix}i_{\ell-1}\\ j_{\ell-1}\end{smallmatrix}\right), \ldots, \left(\begin{smallmatrix}i_1\\ j_1\end{smallmatrix}\right)$ of biletters such that applying the RSK algorithm to $\left(\begin{smallmatrix}i_1\cdots i_\ell\\ j_1\cdots j_\ell\end{smallmatrix}\right)$ gives back (P, Q). The question is why we have $\left(\begin{smallmatrix}i_1\\ j_1\end{smallmatrix}\right) \leq_{lex} \cdots \leq_{lex} \left(\begin{smallmatrix}i_\ell\\ j_\ell\end{smallmatrix}\right)$. Since the chain of inequalities $i_1 \leq i_2 \leq \cdots \leq i_\ell$ is clear from the choice of entry to reverse-bump, it only remains to show that for every string $i_m = i_{m+1} = \cdots = i_{m+r}$ of equal top letters, the corresponding bottom letters weakly increase (that is, $j_m \leq j_{m+1} \leq \cdots \leq j_{m+r}$). One way to see this is the following:

Assume the contrary; i.e., assume that the bottom letters corresponding to some string $i_m = i_{m+1} = \cdots = i_{m+r}$ of equal top letters do not weakly increase. Thus, $j_{m+p} > j_{m+p+1}$ for some $p \in \{0, 1, \ldots, r-1\}$. Consider this p.

Let us consider the cells containing the equal letters $i_m = i_{m+1} = \cdots = i_{m+r}$ in the tableau Q_{m+r}. Label these cells as $c_m, c_{m+1}, \ldots, c_{m+r}$ from left to right (noticing that no two of them lie in the same column, since Q_{m+r} is column-strict). By the definition of reverse bumping, the first entry to be reverse bumped from P_{m+r} is the entry in position c_{m+r} (since this is the rightmost occurrence of the letter i_{m+r} in Q_{m+r}); then, the next entry to be reverse bumped is the one in position c_{m+r-1}, etc., moving further and further left. Thus, for each $q \in \{0, 1, \ldots, r\}$, the tableau P_{m+q-1} is obtained from P_{m+q} by reverse bumping the entry in position c_{m+q}. Hence, conversely, the tableau P_{m+q} is obtained from P_{m+q-1} by RS-inserting the entry j_{m+q}, which creates the corner cell c_{m+q}.

But recall that $j_{m+p} > j_{m+p+1}$. Hence, part (b) of the row bumping lemma (applied to P_{m+p-1}, j_{m+p}, j_{m+p+1}, P_{m+p}, c_{m+p}, P_{m+p+1} and c_{m+p+1} instead of P, j, j', P', c, P'' and c') shows that the cell c_{m+p+1} is in the same column as the cell c_{m+p} or in a column further left. But this contradicts the fact that the cell c_{m+p+1} is in a column further right than the cell c_{m+p} (since we have labeled our cells as $c_m, c_{m+1}, \ldots, c_{m+r}$ from left to right, and no two of them lied in the same column). This contradiction completes our proof.

[123] Note that this does not immediately follow from the linear independence of the basis $(q_\lambda)_{\lambda\in\mathrm{Par}}$. Indeed, linear independence would help if the sums in (2.5.3) were finite, but they are not. A subtler argument (involving the homogeneity of the q_λ) thus has to be used.

in $\mathbf{k}\left[\left[\mathbf{x},\mathbf{y}\right]\right]$, then $\left(a_{\mu,\nu}\right)_{(\mu,\nu)\in \mathrm{Par}^2} = \left(b_{\mu,\nu}\right)_{(\mu,\nu)\in \mathrm{Par}^2}$.

(c) Consider a further infinite family $\mathbf{z} = (z_1, z_2, z_3, \ldots)$ of indeterminates (disjoint from $\mathbf{x}$ and $\mathbf{y}$). If two families $\left(a_{\lambda,\mu,\nu}\right)_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} \in \mathbf{k}^{\mathrm{Par}^3}$ and $\left(b_{\lambda,\mu,\nu}\right)_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} \in \mathbf{k}^{\mathrm{Par}^3}$ satisfy

$$\sum_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} a_{\lambda,\mu,\nu} q_\mu\left(\mathbf{x}\right) q_\nu\left(\mathbf{y}\right) q_\lambda\left(\mathbf{z}\right) = \sum_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} b_{\lambda,\mu,\nu} q_\mu\left(\mathbf{x}\right) q_\nu\left(\mathbf{y}\right) q_\lambda\left(\mathbf{z}\right) \tag{2.5.5}$$

in $\mathbf{k}\left[\left[\mathbf{x},\mathbf{y},\mathbf{z}\right]\right]$, then $\left(a_{\lambda,\mu,\nu}\right)_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} = \left(b_{\lambda,\mu,\nu}\right)_{(\mu,\nu,\lambda)\in \mathrm{Par}^3}$.

Remark 2.5.6. Clearly, for any $n \in \mathbb{N}$, we can state an analogue of Exercise 2.5.5 for n infinite families $\mathbf{x}_i = (x_{i,1}, x_{i,2}, x_{i,3}, \ldots)$ of indeterminates (with $i \in \{1, 2, \ldots, n\}$). The three parts of Exercise 2.5.5 are the particular cases of this analogue for $n = 1$, for $n = 2$ and for $n = 3$. We have shied away from stating this analogue in full generality because these particular cases are the only ones we will need.

Corollary 2.5.7. *In the Schur function basis $\{s_\lambda\}$ for Λ, the structure constants for multiplication and comultiplication are the same, that is, if one defines scalars $c^\lambda_{\mu,\nu}, \hat{c}^\lambda_{\mu,\nu}$ via the unique expansions*

$$s_\mu s_\nu = \sum_\lambda c^\lambda_{\mu,\nu} s_\lambda, \tag{2.5.6}$$

$$\Delta(s_\lambda) = \sum_{\mu,\nu} \hat{c}^\lambda_{\mu,\nu} s_\mu \otimes s_\nu, \tag{2.5.7}$$

then $c^\lambda_{\mu,\nu} = \hat{c}^\lambda_{\mu,\nu}$.

Proof. Work in the ring $\mathbf{k}\left[\left[\mathbf{x},\mathbf{y},\mathbf{z}\right]\right]$, where $\mathbf{y} = (y_1, y_2, y_3, \ldots)$ and $\mathbf{z} = (z_1, z_2, z_3, \ldots)$ are two new sets of variables. The identity (2.5.1) lets one interpret both $c^\lambda_{\mu,\nu}, \hat{c}^\lambda_{\mu,\nu}$ as the coefficient[124] of $s_\mu(\mathbf{x}) s_\nu(\mathbf{y}) s_\lambda(\mathbf{z})$ in the product

$$\begin{aligned}
\prod_{i,j=1}^{\infty} \left(1 - x_i z_j\right)^{-1} \prod_{i,j=1}^{\infty} \left(1 - y_i z_j\right)^{-1} &\overset{(2.5.1)}{=} \left(\sum_\mu s_\mu(\mathbf{x}) s_\mu(\mathbf{z})\right) \left(\sum_\nu s_\nu(\mathbf{y}) s_\nu(\mathbf{z})\right) \\
&= \sum_{\mu,\nu} s_\mu(\mathbf{x}) s_\nu(\mathbf{y}) \cdot s_\mu(\mathbf{z}) s_\nu(\mathbf{z}) \\
&= \sum_{\mu,\nu} s_\mu(\mathbf{x}) s_\nu(\mathbf{y}) \left(\sum_\lambda c^\lambda_{\mu,\nu} s_\lambda(\mathbf{z})\right)
\end{aligned}$$

since, regarding $x_1, x_2, \ldots, y_1, y_2, \ldots$ as lying in a single variable set $(\mathbf{x}, \mathbf{y})$, separate from the variables $\mathbf{z}$, the Cauchy identity (2.5.1) expands the same product as

$$\begin{aligned}
\prod_{i,j=1}^{\infty} \left(1 - x_i z_j\right)^{-1} \prod_{i,j=1}^{\infty} \left(1 - y_i z_j\right)^{-1} &= \sum_\lambda s_\lambda(\mathbf{x},\mathbf{y}) s_\lambda(\mathbf{z}) \\
&= \sum_\lambda \left(\sum_{\mu,\nu} \hat{c}^\lambda_{\mu,\nu} s_\mu(\mathbf{x}) s_\nu(\mathbf{y})\right) s_\lambda(\mathbf{z}).
\end{aligned}$$

□

Definition 2.5.8. The coefficients $c^\lambda_{\mu,\nu} = \hat{c}^\lambda_{\mu,\nu}$ appearing in the expansions (2.5.6) and (2.5.7) are called *Littlewood-Richardson coefficients*.

Remark 2.5.9. We will interpret $c^\lambda_{\mu,\nu}$ combinatorially in Section 2.6. By now, however, we can already prove some properties of these coefficients:

We have

$$c^\lambda_{\mu,\nu} = c^\lambda_{\nu,\mu} \qquad \text{for all } \lambda, \mu, \nu \in \mathrm{Par} \tag{2.5.8}$$

[124] Let us explain why speaking of coefficients makes sense here:

We want to use the fact that if a power series $f \in \mathbf{k}\left[\left[\mathbf{x},\mathbf{y},\mathbf{z}\right]\right]$ is written in the form $f = \sum_{(\mu,\nu,\lambda)\in \mathrm{Par}^3} a_{\lambda,\mu,\nu} s_\mu\left(\mathbf{x}\right) s_\nu\left(\mathbf{y}\right) s_\lambda\left(\mathbf{z}\right)$ for some coefficients $a_{\lambda,\mu,\nu} \in \mathbf{k}$, then these coefficients $a_{\lambda,\mu,\nu}$ are uniquely determined by f. But this fact is precisely the claim of Exercise 2.5.5(c) above (applied to $q_\lambda = s_\lambda$).

(by comparing coefficients in $\sum_\lambda c^\lambda_{\mu,\nu} s_\lambda = s_\mu s_\nu = s_\nu s_\mu = \sum_\lambda c^\lambda_{\nu,\mu} s_\lambda$). Furthermore, let λ and μ be two partitions (not necessarily satisfying $\mu \subseteq \lambda$). Comparing the expansion

$$s_\lambda(\mathbf{x},\mathbf{y}) = \Delta(s_\lambda) = \sum_{\mu,\nu} c^\lambda_{\mu,\nu} s_\mu(\mathbf{x}) s_\nu(\mathbf{y}) = \sum_{\mu\in\mathrm{Par}} \left(\sum_{\nu\in\mathrm{Par}} c^\lambda_{\mu,\nu} s_\nu(\mathbf{y}) \right) s_\mu(\mathbf{x})$$

with

$$s_\lambda(\mathbf{x},\mathbf{y}) = \sum_{\mu\subseteq\lambda} s_\mu(\mathbf{x}) s_{\lambda/\mu}(\mathbf{y}) = \sum_{\mu\in\mathrm{Par}} s_\mu(\mathbf{x}) s_{\lambda/\mu}(\mathbf{y})$$

[125], one concludes that

$$\sum_{\mu\in\mathrm{Par}} \left(\sum_{\nu\in\mathrm{Par}} c^\lambda_{\mu,\nu} s_\nu(\mathbf{y}) \right) s_\mu(\mathbf{x}) = \sum_{\mu\in\mathrm{Par}} s_\mu(\mathbf{x}) s_{\lambda/\mu}(\mathbf{y}) = \sum_{\mu\in\mathrm{Par}} s_{\lambda/\mu}(\mathbf{y}) s_\mu(\mathbf{x}).$$

Treating the indeterminates $\mathbf{y}$ as constants, and comparing coefficients before $s_\mu(\mathbf{x})$ on both sides of this equality[126], we arrive at another standard interpretation for $c^\lambda_{\mu,\nu}$:

$$s_{\lambda/\mu} = \sum_\nu c^\lambda_{\mu,\nu} s_\nu.$$

In particular, $c^\lambda_{\mu,\nu}$ vanishes unless $\mu \subseteq \lambda$. Consequently, $c^\lambda_{\mu,\nu}$ vanishes unless $\nu \subseteq \lambda$ as well (since $c^\lambda_{\mu,\nu} = c^\lambda_{\nu,\mu}$) and furthermore vanishes unless the equality $|\mu| + |\nu| = |\lambda|$ holds[127]. Altogether, we conclude that $c^\lambda_{\mu,\nu}$ vanishes unless $\mu, \nu \subseteq \lambda$ and $|\mu| + |\nu| = |\lambda|$.

Exercise 2.5.10. Show that any four partitions κ, λ, φ and ψ satisfy

$$\sum_{\rho\in\mathrm{Par}} c^\rho_{\kappa,\lambda} c^\rho_{\varphi,\psi} = \sum_{(\alpha,\beta,\gamma,\delta)\in\mathrm{Par}^4} c^\lambda_{\beta,\delta} c^\varphi_{\alpha,\beta} c^\psi_{\gamma,\delta}.$$

Exercise 2.5.11. (a) For any partition μ, prove that

$$\sum_{\lambda\in\mathrm{Par}} s_\lambda(\mathbf{x}) s_{\lambda/\mu}(\mathbf{y}) = s_\mu(\mathbf{x}) \cdot \prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1}$$

in the power series ring $\mathbf{k}[[\mathbf{x},\mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$.

(b) Let α and β be two partitions. Show that

$$\sum_{\lambda\in\mathrm{Par}} s_{\lambda/\alpha}(\mathbf{x}) s_{\lambda/\beta}(\mathbf{y}) = \left(\sum_{\rho\in\mathrm{Par}} s_{\beta/\rho}(\mathbf{x}) s_{\alpha/\rho}(\mathbf{y}) \right) \cdot \prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1}$$

in the power series ring $\mathbf{k}[[\mathbf{x},\mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$.

[**Hint:** For (b), expand the product

$$\prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1} \prod_{i,j=1}^{\infty} (1 - x_i w_j)^{-1} \prod_{i,j=1}^{\infty} (1 - z_i y_j)^{-1} \prod_{i,j=1}^{\infty} (1 - z_i w_j)^{-1}$$

in the power series ring $\mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots, z_1, z_2, z_3, \ldots, w_1, w_2, w_3, \ldots]]$ in two ways: once by applying Theorem 2.5.1 to the two variable sets $(\mathbf{z},\mathbf{x})$ and $(\mathbf{w},\mathbf{y})$ and then using (2.3.3); once again by applying (2.5.1) to the two variable sets $\mathbf{z}$ and $\mathbf{w}$ and then applying Exercise 2.5.11(a) twice.]

The statement of Exercise 2.5.11(b) is known as the *skew Cauchy identity*, and appears in Sagan-Stanley [188, Cor. 6.12], Stanley [206, exercise 7.27(c)] and Macdonald [142, §I.5, example 26]; it seems to be due to Zelevinsky. It generalizes the statement of Exercise 2.5.11(a), which in turn is a generalization of Theorem 2.5.1.

[125] In the last equality, we removed the condition $\mu \subseteq \lambda$ on the addends of the sum; this does not change the value of the sum (because we have $s_{\lambda/\mu} = 0$ whenever we don't have $\mu \subseteq \lambda$).

[126] "Comparing coefficients" means applying Exercise 2.5.5(a) to $q_\lambda = s_\lambda$ in this case (although the base ring $\mathbf{k}$ is now replaced by $\mathbf{k}[[\mathbf{y}]]$, and the index μ is used instead of λ, since λ is already taken).

[127] In fact, this is clear when we don't have $\mu \subseteq \lambda$. When we do have $\mu \subseteq \lambda$, this follows from observing that $s_{\lambda/\mu} \in \Lambda_{|\lambda/\mu|}$ has zero coefficient before s_ν whenever $|\mu| + |\nu| \neq |\lambda|$.

Definition 2.5.12. Define the *Hall inner product* on Λ to be the $\mathbf{k}$-bilinear form $(\cdot,\cdot)$ which makes $\{s_\lambda\}$ an orthonormal basis, that is, $(s_\lambda, s_\nu) = \delta_{\lambda,\nu}$.

Exercise 2.5.13. (a) If n and m are two distinct nonnegative integers, and if $f \in \Lambda_n$ and $g \in \Lambda_m$, then show that $(f,g) = 0$.

(b) If $n \in \mathbb{N}$ and $f \in \Lambda_n$, then prove that $(h_n, f) = f(1)$ (where $f(1)$ is defined as in Exercise 2.1.2).

(c) Show that $(f,g) = (g,f)$ for all $f \in \Lambda$ and $g \in \Lambda$. (In other words, the Hall inner product is symmetric.)

The Hall inner product induces a $\mathbf{k}$-module homomorphism $\Lambda \to \Lambda^o$ (sending every $f \in \Lambda$ to the $\mathbf{k}$-linear map $\Lambda \to \mathbf{k},\ g \mapsto (f,g)$). This homomorphism is invertible (since the Hall inner product has an orthonormal basis), so that $\Lambda^o \cong \Lambda$ as $\mathbf{k}$-modules. But in fact, more can be said:

Corollary 2.5.14. *The isomorphism $\Lambda^o \cong \Lambda$ induced by the Hall inner product is an isomorphism of Hopf algebras.*

Proof. We have seen that the orthonormal basis $\{s_\lambda\}$ of Schur functions is *self-dual*, in the sense that its multiplication and comultiplication structure constants are the same. Thus the isomorphism $\Lambda^o \cong \Lambda$ induced by the Hall inner product is an isomorphism of bialgebras[128], and hence also a Hopf algebra isomorphism by Corollary 1.4.27. □

We next identify two other dual pairs of bases, by expanding the Cauchy product in two other ways.

Proposition 2.5.15. *One can also expand*

$$\prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1} = \sum_{\lambda \in \mathrm{Par}} h_\lambda(\mathbf{x}) m_\lambda(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} z_\lambda^{-1} p_\lambda(\mathbf{x}) p_\lambda(\mathbf{y}) \tag{2.5.11}$$

---

[128] Here are some details on the proof:

Let $\gamma : \Lambda \to \Lambda^o$ be the $\mathbf{k}$-module isomorphism $\Lambda \to \Lambda^o$ induced by the Hall inner product. We want to show that γ is an isomorphism of bialgebras.

Let $\{s_\lambda^*\}$ be the basis of Λ^o dual to the basis $\{s_\lambda\}$ of Λ. Thus, for any partition λ, we have

$$\gamma(s_\lambda) = s_\lambda^* \tag{2.5.9}$$

(since any partition μ satisfies $(\gamma(s_\lambda))(s_\mu) = (s_\lambda, s_\mu) = \delta_{\lambda,\mu} = s_\lambda^*(s_\mu)$, and thus the two $\mathbf{k}$-linear maps $\gamma(s_\lambda) : \Lambda \to \mathbf{k}$ and $s_\lambda^* : \Lambda \to \mathbf{k}$ are equal to each other on the basis $\{s_\mu\}$ of Λ, which forces them to be identical).

The coproduct structure constants of the basis $\{s_\lambda^*\}$ of Λ^o equal the product structure constants of the basis $\{s_\lambda\}$ of Λ (according to our discussion of duals in Section 1.6). Since the latter are the Littlewood-Richardson numbers $c_{\mu,\nu}^\lambda$ (because of (2.5.6)), we thus conclude that the former are $c_{\mu,\nu}^\lambda$ as well. In other words, every $\lambda \in \mathrm{Par}$ satisfies

$$\Delta_{\Lambda^o} s_\lambda^* = \sum_{\mu,\nu} c_{\mu,\nu}^\lambda s_\mu^* \otimes s_\nu^* \tag{2.5.10}$$

(where the sum is over all pairs (μ,ν) of partitions). On the other hand, applying the map $\gamma \otimes \gamma : \Lambda \otimes \Lambda \to \Lambda^o \otimes \Lambda^o$ to the equality (2.5.7) yields

$$\begin{aligned}
(\gamma\otimes\gamma)(\Delta(s_\lambda)) &= (\gamma\otimes\gamma)\left(\sum_{\mu,\nu} \hat{c}_{\mu,\nu}^\lambda s_\mu \otimes s_\nu\right) = \sum_{\mu,\nu} \underbrace{\hat{c}_{\mu,\nu}^\lambda}_{=c_{\mu,\nu}^\lambda} \underbrace{\gamma(s_\mu)}_{\substack{=s_\mu^* \\ \text{(by (2.5.9))}}} \otimes \underbrace{\gamma(s_\nu)}_{\substack{=s_\nu^* \\ \text{(by (2.5.9))}}} = \sum_{\mu,\nu} c_{\mu,\nu}^\lambda s_\mu^* \otimes s_\nu^* \\
&= \Delta_{\Lambda^o} \underbrace{s_\lambda^*}_{\substack{=\gamma(s_\lambda) \\ \text{(by (2.5.9))}}} \qquad \text{(by (2.5.10))} \\
&= \Delta_{\Lambda^o}(\gamma(s_\lambda))
\end{aligned}$$

for each $\lambda \in \mathrm{Par}$. In other words, the two $\mathbf{k}$-linear maps $(\gamma\otimes\gamma)\circ\Delta$ and $\Delta_{\Lambda^o}\circ\gamma$ are equal to each other on each s_λ with $\lambda \in \mathrm{Par}$. Hence, these two maps must be identical (since the s_λ form a basis of Λ). Hence, $\Delta_{\Lambda^o}\circ\gamma = (\gamma\otimes\gamma)\circ\Delta$.

Our next goal is to show that $\epsilon_{\Lambda^o}\circ\gamma = \epsilon$. Indeed, each $\lambda \in \mathrm{Par}$ satisfies

$$\begin{aligned}
(\epsilon_{\Lambda^o}\circ\gamma)(s_\lambda) &= \epsilon_{\Lambda^o}(\gamma(s_\lambda)) = (\gamma(s_\lambda))(1) \qquad \text{(by the definition of } \epsilon_{\Lambda^o}) \\
&= \left(s_\lambda, \underbrace{1}_{=s_\varnothing}\right) = (s_\lambda, s_\varnothing) = \delta_{\lambda,\varnothing} = \epsilon(s_\lambda).
\end{aligned}$$

Hence, $\epsilon_{\Lambda^o}\circ\gamma = \epsilon$. Combined with $\Delta_{\Lambda^o}\circ\gamma = (\gamma\otimes\gamma)\circ\Delta$, this shows that γ is a $\mathbf{k}$-coalgebra homomorphism. Similar reasoning can be used to prove that γ is a $\mathbf{k}$-algebra homomorphism. Altogether, we thus conclude that γ is a bialgebra homomorphism. Since γ is a $\mathbf{k}$-module isomorphism, this yields that γ is an isomorphism of bialgebras. Qed.

where $z_\lambda := m_1! \cdot 1^{m_1} \cdot m_2! \cdot 2^{m_2} \cdots$ *if* λ *is written in multiplicative notation as* $\lambda = (1^{m_1}, 2^{m_2}, \ldots)$ *with multiplicity* m_i *for the part* i*. (Here, we assume that* $\mathbb{Q}$ *is a subring of* $\mathbf{k}$ *for the last equality.)*

Remark 2.5.16. It is relevant later (and explains the notation) that z_λ is the size of the $\mathfrak{S}_n$-centralizer subgroup for a permutation having cycle type[129] λ with $|\lambda| = n$. This is a classical (and fairly easy) result (see, e.g., [186, Prop. 1.1.1] or [206, Prop. 7.7.3] for a proof).

Proof of Proposition 2.5.15. For the first expansion, note that (2.2.18) shows

$$\begin{aligned}
\prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1} &= \prod_{j=1}^{\infty} \sum_{n \geq 0} h_n(\mathbf{x}) y_j^n \\
&= \sum_{\substack{\text{weak} \\ \text{compositions} \\ (n_1, n_2, \ldots)}} (h_{n_1}(\mathbf{x}) h_{n_2}(\mathbf{x}) \cdots)(y_1^{n_1} y_2^{n_2} \cdots) \\
&= \sum_{\lambda \in \mathrm{Par}} \sum_{\substack{\text{weak} \\ \text{compositions} \\ (n_1, n_2, \ldots) \\ \text{satisfying} \\ (n_1, n_2, \ldots) \in \mathfrak{S}_{(\infty)} \lambda}} \underbrace{(h_{n_1}(\mathbf{x}) h_{n_2}(\mathbf{x}) \cdots)}_{\substack{= h_\lambda(\mathbf{x}) \\ (\text{since } (n_1, n_2, \ldots) \in \mathfrak{S}_{(\infty)} \lambda)}} \underbrace{(y_1^{n_1} y_2^{n_2} \cdots)}_{= \mathbf{y}^{(n_1, n_2, \ldots)}} \\
&= \sum_{\lambda \in \mathrm{Par}} h_\lambda(\mathbf{x}) \underbrace{\sum_{\substack{\text{weak} \\ \text{compositions} \\ (n_1, n_2, \ldots) \\ \text{satisfying} \\ (n_1, n_2, \ldots) \in \mathfrak{S}_{(\infty)} \lambda}} \mathbf{y}^{(n_1, n_2, \ldots)}}_{= m_\lambda(\mathbf{y})} \\
&= \sum_{\lambda \in \mathrm{Par}} h_\lambda(\mathbf{x}) m_\lambda(\mathbf{y}).
\end{aligned}$$

For the second expansion (and for later use in the proof of Theorem 4.9.5) note that

$$\log H(t) = \log \prod_{i=1}^{\infty} (1 - x_i t)^{-1} = \sum_{i=1}^{\infty} -\log(1 - x_i t) = \sum_{i=1}^{\infty} \sum_{m=1}^{\infty} \frac{(x_i t)^m}{m} = \sum_{m=1}^{\infty} \frac{1}{m} p_m(\mathbf{x}) t^m, \tag{2.5.12}$$

so that taking $\frac{d}{dt}$ then shows that

$$P(t) := \sum_{m \geq 0} p_{m+1} t^m = \frac{H'(t)}{H(t)} = H'(t) E(-t). \tag{2.5.13}$$

A similar calculation shows that

$$\log \prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1} = \sum_{m=1}^{\infty} \frac{1}{m} p_m(\mathbf{x}) p_m(\mathbf{y}) \tag{2.5.14}$$

[129] If σ is a permutation of a finite set X, then the *cycle type* of σ is defined as the list of the lengths of all cycles of σ (that is, of all orbits of σ acting on X) written in decreasing order. This is clearly a partition of $|X|$. (Some other authors write it in increasing order instead, or treat it as a multiset.)

For instance, the permutation of the set $\{0, 3, 6, 9, 12\}$ that sends 0 to 3, 3 to 9, 6 to 6, 9 to 0, and 12 to 12 has cycle type $(3, 1, 1)$, since the cycles of this permutation have lengths 3, 1 and 1.

It is known that two permutations in $\mathfrak{S}_n$ have the same cycle type if and only if they are conjugate. Thus, for a given partition λ with $|\lambda| = n$, any two permutations in $\mathfrak{S}_n$ having cycle type λ are conjugate and therefore their $\mathfrak{S}_n$-centralizer subgroups have the same size.

and hence

$$\prod_{i,j=1}^{\infty}\left(1-x_iy_j\right)^{-1}=\exp\left(\sum_{m=1}^{\infty}\frac{1}{m}p_m(\mathbf{x})p_m(\mathbf{y})\right)=\prod_{m=1}^{\infty}\exp\left(\frac{1}{m}p_m(\mathbf{x})p_m(\mathbf{y})\right)$$

$$=\prod_{m=1}^{\infty}\sum_{k=0}^{\infty}\frac{1}{k!}\left(\frac{1}{m}p_m(\mathbf{x})p_m(\mathbf{y})\right)^k=\sum_{\substack{\text{weak compositions}\\(k_1,k_2,k_3,\ldots)}}\prod_{m=1}^{\infty}\left(\frac{1}{k_m!}\left(\frac{1}{m}p_m(\mathbf{x})p_m(\mathbf{y})\right)^{k_m}\right)$$

(by the product rule)

$$=\sum_{\substack{\text{weak compositions}\\(k_1,k_2,k_3,\ldots)}}\prod_{m=1}^{\infty}\frac{\left(p_m(\mathbf{x})p_m(\mathbf{y})\right)^{k_m}}{k_m!m^{k_m}}=\sum_{\substack{\text{weak compositions}\\(k_1,k_2,k_3,\ldots)}}\frac{\prod_{m=1}^{\infty}\left(p_m(\mathbf{x})\right)^{k_m}\prod_{m=1}^{\infty}\left(p_m(\mathbf{y})\right)^{k_m}}{\prod_{m=1}^{\infty}\left(k_m!m^{k_m}\right)}$$

$$=\sum_{\substack{\text{weak compositions}\\(k_1,k_2,k_3,\ldots)}}\frac{p_{\left(1^{k_1}2^{k_2}3^{k_3}\cdots\right)}(\mathbf{x})\,p_{\left(1^{k_1}2^{k_2}3^{k_3}\cdots\right)}(\mathbf{y})}{z_{\left(1^{k_1}2^{k_2}3^{k_3}\cdots\right)}}=\sum_{\lambda\in\mathrm{Par}}\frac{p_\lambda(\mathbf{x})p_\lambda(\mathbf{y})}{z_\lambda}$$

due to the fact that every partition can be uniquely written in the form $\left(1^{k_1}2^{k_2}3^{k_3}\cdots\right)$ with $(k_1,k_2,k_3,\ldots)$ a weak composition. □

Corollary 2.5.17. (a) *With respect to the Hall inner product on Λ, one also has dual bases $\{h_\lambda\}$ and $\{m_\lambda\}$.*

(b) *If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then $\{p_\lambda\}$ and $\left\{z_\lambda^{-1}p_\lambda\right\}$ are also dual bases with respect to the Hall inner product on Λ.*

(c) *If $\mathbb{R}$ is a subring of $\mathbf{k}$, then $\left\{\dfrac{p_\lambda}{\sqrt{z_\lambda}}\right\}$ is an orthonormal basis of Λ with respect to the Hall inner product.*

Proof. Since (2.5.1) and (2.5.11) showed

$$\prod_{i,j=1}^{\infty}\left(1-x_iy_j\right)^{-1}=\sum_{\lambda\in\mathrm{Par}}s_\lambda(\mathbf{x})s_\lambda(\mathbf{y})=\sum_{\lambda\in\mathrm{Par}}h_\lambda(\mathbf{x})m_\lambda(\mathbf{y})=\sum_{\lambda\in\mathrm{Par}}p_\lambda(\mathbf{x})z_\lambda^{-1}p_\lambda(\mathbf{y})=\sum_{\lambda\in\mathrm{Par}}\frac{p_\lambda(\mathbf{x})}{\sqrt{z_\lambda}}\frac{p_\lambda(\mathbf{y})}{\sqrt{z_\lambda}},$$

it suffices to show that any pair of graded bases[130] $\{u_\lambda\},\{v_\lambda\}$ of Λ having

$$\sum_{\lambda\in\mathrm{Par}}s_\lambda(\mathbf{x})s_\lambda(\mathbf{y})=\sum_{\lambda\in\mathrm{Par}}u_\lambda(\mathbf{x})v_\lambda(\mathbf{y})$$

will be dual with respect to $(\cdot,\cdot)$. To show this, consider such a pair of graded bases. Write transition matrices $A=(a_{\nu,\lambda})_{(\nu,\lambda)\in\mathrm{Par}\times\mathrm{Par}}$ and $B=(b_{\nu,\lambda})_{(\nu,\lambda)\in\mathrm{Par}\times\mathrm{Par}}$ uniquely expressing

$$u_\lambda=\sum_\nu a_{\nu,\lambda}s_\nu, \tag{2.5.15}$$

$$v_\lambda=\sum_\nu b_{\nu,\lambda}s_\nu. \tag{2.5.16}$$

Recall that $\mathrm{Par}=\bigsqcup_{r\in\mathbb{N}}\mathrm{Par}_r$. Hence, we can view A as a block matrix, where the blocks are indexed by pairs of nonnegative integers, and the (r,s)-th block is $(a_{\nu,\lambda})_{(\nu,\lambda)\in\mathrm{Par}_r\times\mathrm{Par}_s}$. For reasons of homogeneity[131], we have $a_{\nu,\lambda}=0$ for any $(\nu,\lambda)\in\mathrm{Par}^2$ satisfying $|\nu|\neq|\lambda|$. Therefore, the (r,s)-th block of A is zero whenever $r\neq s$. In other words, the block matrix A is block-diagonal. Similarly, B can be viewed as a block-diagonal matrix. The diagonal blocks of A and B are finite square matrices (since Par_r is a finite set for each $r\in\mathbb{N}$); therefore, products such as A^tB, B^tA and AB^t are well-defined (since all sums involved in their definition have only finitely many nonzero addends) and subject to the law of associativity. Moreover, the matrix A is

[130] See Definition 1.3.21 for the concept of a "graded basis", and recall our convention that a graded basis of Λ is tacitly assumed to have its indexing set Par partitioned into $\mathrm{Par}_0,\mathrm{Par}_1,\mathrm{Par}_2,\ldots$. Thus, a graded basis of Λ means a basis $\{w_\lambda\}_{\lambda\in\mathrm{Par}}$ of the $\mathbf{k}$-module Λ (indexed by the partitions $\lambda\in\mathrm{Par}$) with the property that, for every $n\in\mathbb{N}$, the subfamily $\{w_\lambda\}_{\lambda\in\mathrm{Par}_n}$ is a basis of the $\mathbf{k}$-module Λ_n.

[131] More precisely: The power series u_λ is homogeneous of degree $|\lambda|$, and the power series s_ν is homogeneous of degree $|\nu|$.

invertible (being a transition matrix between two bases), and its inverse is again block-diagonal (because A is block-diagonal).

The equalities (2.5.15) and (2.5.16) show that $(u_\alpha, v_\beta) = \sum_\nu a_{\nu,\alpha} b_{\nu,\beta}$ (by the orthonormality of the s_λ). Hence, we want to prove that $\sum_\nu a_{\nu,\alpha} b_{\nu,\beta} = \delta_{\alpha,\beta}$. In other words, we want to prove that $A^t B = I$, that is, $B^{-1} = A^t$. On the other hand, one has

$$\sum_\lambda s_\lambda(\mathbf{x}) s_\lambda(\mathbf{y}) = \sum_\lambda u_\lambda(\mathbf{x}) v_\lambda(\mathbf{y}) = \sum_\lambda \sum_\nu a_{\nu,\lambda} s_\nu(\mathbf{x}) \sum_\rho b_{\rho,\lambda} s_\rho(\mathbf{y}).$$

Comparing coefficients[132] of $s_\nu(\mathbf{x}) s_\rho(\mathbf{y})$ forces $\sum_\lambda a_{\nu,\lambda} b_{\rho,\lambda} = \delta_{\nu,\rho}$, or in other words, $AB^t = I$. Since A is invertible, this yields $B^t A = I$, and hence $A^t B = I$, as desired.[133] □

Corollary 2.5.17 is a known and fundamental fact[134]. However, our definition of the Hall inner product is unusual; most authors (e.g., Macdonald in [142, §I.4, (4.5)], Hazewinkel/Gubareni/Kirichenko in [93, Def. 4.1.21], and Stanley in [206, (7.30)]) *define* the Hall inner product as the bilinear form satisfying $(h_\lambda, m_\mu) = \delta_{\lambda,\mu}$ (or, alternatively, $(m_\lambda, h_\mu) = \delta_{\lambda,\mu}$), and only later prove that the basis $\{s_\lambda\}$ is orthonormal with respect to this scalar product. (Of course, the fact that this definition is equivalent to our Definition 2.5.12 follows either from this orthonormality, or from our Corollary 2.5.17(a).)

The tactic applied in the proof of Corollary 2.5.17 can not only be used to show that certain bases of Λ are dual, but also, with a little help from linear algebra over rings (Exercise 2.5.18), it can be strengthened to show that certain families of symmetric functions are bases to begin with, as we will see in Exercise 2.5.19 and Exercise 2.5.20.

Exercise 2.5.18. (a) Prove that if an endomorphism of a finitely generated $\mathbf{k}$-module is surjective, then this endomorphism is a $\mathbf{k}$-module isomorphism.

(b) Let A be a finite free $\mathbf{k}$-module with finite basis $(\gamma_i)_{i \in I}$. Let $(\beta_i)_{i \in I}$ be a family of elements of A which spans the $\mathbf{k}$-module A. Prove that $(\beta_i)_{i \in I}$ is a $\mathbf{k}$-basis of A.

Exercise 2.5.19. For each partition λ, let v_λ be an element of $\Lambda_{|\lambda|}$. Assume that the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$ spans the $\mathbf{k}$-module Λ. Prove that the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$ is a graded basis of the graded $\mathbf{k}$-module Λ.

Exercise 2.5.20. (a) Assume that for every partition λ, two homogeneous elements u_λ and v_λ of Λ, both having degree $|\lambda|$, are given. Assume further that

$$\sum_{\lambda \in \mathrm{Par}} s_\lambda(\mathbf{x}) s_\lambda(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} u_\lambda(\mathbf{x}) v_\lambda(\mathbf{y})$$

in $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$. Show that $(u_\lambda)_{\lambda \in \mathrm{Par}}$ and $(v_\lambda)_{\lambda \in \mathrm{Par}}$ are $\mathbf{k}$-bases of Λ, and actually are dual bases with respect to the Hall inner product on Λ.

(b) Use this to give a new proof of the fact that $(h_\lambda)_{\lambda \in \mathrm{Par}}$ is a $\mathbf{k}$-basis of Λ.

Exercise 2.5.21. Prove that $\sum_{m \geq 0} p_{m+1} t^m = \dfrac{H'(t)}{H(t)}$. (This was proven in (2.5.13) in the case when $\mathbb{Q}$ is a subring of $\mathbf{k}$, but here we make no requirements on $\mathbf{k}$.)

The following exercises give some useful criteria for algebraic independence of families of symmetric functions:

---

[132] Comparing coefficients is legitimate because if a power series $f \in \mathbf{k}[[\mathbf{x}, \mathbf{y}]]$ is written in the form $f = \sum_{(\nu,\rho) \in \mathrm{Par}^2} a_{\rho,\nu} s_\nu(\mathbf{x}) s_\rho(\mathbf{y})$ for some coefficients $a_{\rho,\nu} \in \mathbf{k}$, then these coefficients $a_{\rho,\nu}$ are uniquely determined by f. This is just a restatement of Exercise 2.5.5(b).

[133] In our argument above, we have obtained the invertibility of A from the fact that A is a transition matrix between two bases. Here is an alternative way to prove that A is invertible:

Recall that A and B^t are block-diagonal matrices. Hence, the equality $AB^t = I$ rewrites as $A_{r,r} \left(B^t\right)_{r,r} = I$ for all $r \in \mathbb{N}$, where we are using the notation $C_{r,s}$ for the (r,s)-th block of a block matrix C. But this shows that each diagonal block $A_{r,r}$ of A is right-invertible. Therefore, each diagonal block $A_{r,r}$ of A is invertible (because $A_{r,r}$ is a square matrix of finite size, and such matrices are always invertible when they are right-invertible). Consequently, the block-diagonal matrix A is invertible, and its inverse is again a block-diagonal matrix (whose diagonal blocks are the inverses of the $A_{r,r}$).

[134] For example, Corollary 2.5.17(a) appears in [126, Corollary 3.3] (though the definition of Schur functions in [126] is different from ours; we will meet this alternative definition later on), and parts (b) and (c) of Corollary 2.5.17 are equivalent to [142, §I.4, (4.7)] (though Macdonald defines the Hall inner product using Corollary 2.5.17(a)).

Exercise 2.5.22. Let $v_1, v_2, v_3, \ldots$ be elements of Λ. Assume that $v_n \in \Lambda_n$ for each positive integer n. Assume further that $v_1, v_2, v_3, \ldots$ generate the $\mathbf{k}$-algebra Λ. Then:

(a) Prove that $v_1, v_2, v_3, \ldots$ are algebraically independent over $\mathbf{k}$.

(b) For every partition λ, define an element $v_\lambda \in \Lambda$ by $v_\lambda = v_{\lambda_1} v_{\lambda_2} \cdots v_{\lambda_{\ell(\lambda)}}$. Prove that the family $(v_\lambda)_{\lambda \in \mathrm{Par}}$ is a graded basis of the graded $\mathbf{k}$-module Λ.

Exercise 2.5.23. For each partition λ, let $a_\lambda \in \mathbf{k}$. Assume that the element $a_{(n)} \in \mathbf{k}$ is invertible for each positive integer n. Let $v_1, v_2, v_3, \ldots$ be elements of Λ such that each positive integer n satisfies $v_n = \sum_{\lambda \in \mathrm{Par}_n} a_\lambda h_\lambda$. Prove that the elements $v_1, v_2, v_3, \ldots$ generate the $\mathbf{k}$-algebra Λ and are algebraically independent over $\mathbf{k}$.

Exercise 2.5.24. Let $v_1, v_2, v_3, \ldots$ be elements of Λ. Assume that $v_n \in \Lambda_n$ for each positive integer n. Assume further that $(p_n, v_n) \in \mathbf{k}$ is invertible for each positive integer n. Prove that the elements $v_1, v_2, v_3, \ldots$ generate the $\mathbf{k}$-algebra Λ and are algebraically independent over $\mathbf{k}$.

Exercise 2.5.25. Let $f \in \Lambda$, and let β be a weak composition. Let $\mu \in \mathrm{Par}$ be the partition consisting of the nonzero entries of β (sorted in decreasing order).[135] Prove that

$$(f, h_\mu) = (h_\mu, f) = \left(\text{the coefficient of } \mathbf{x}^\beta \text{ in } f\right).$$

Exercise 2.5.26. Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Define a positive integer z_λ for each $\lambda \in \mathrm{Par}$ as in Proposition 2.5.15. Prove that every $n \in \mathbb{N}$ satisfies the two equalities

$$h_n = \sum_{\lambda \in \mathrm{Par}_n} z_\lambda^{-1} p_\lambda \tag{2.5.17}$$

and

$$e_n = \sum_{\lambda \in \mathrm{Par}_n} (-1)^{|\lambda| - \ell(\lambda)} z_\lambda^{-1} p_\lambda. \tag{2.5.18}$$

2.6. **Bialternants, Littlewood-Richardson: Stembridge's concise proof.** There is a more natural way in which Schur functions arise as a $\mathbf{k}$-basis for Λ, coming from consideration of polynomials in a finite variable set, and the relation between those which are symmetric and those which are *alternating*.

For the remainder of this section, fix a nonnegative integer n, and let $\mathbf{x} = (x_1, \ldots, x_n)$ be a finite variable set. This means that $s_{\lambda/\mu} = s_{\lambda/\mu}(\mathbf{x}) = \sum_T \mathbf{x}^{\mathrm{cont}(T)}$ is a generating function for column-strict tableaux T as in Definition 2.3.1, but with the extra condition that T have entries in $\{1, 2, \ldots, n\}$. [136] As a consequence, $s_{\lambda/\mu}$ is a polynomial in $\mathbf{k}[x_1, x_2, \ldots, x_n]$ (not just a power series), since there are only finitely many column-strict tableaux T of shape λ/μ having all their entries in $\{1, 2, \ldots, n\}$. We will assume without further mention that all partitions appearing in the section have at most n parts.

Definition 2.6.1. Let $\mathbf{k}$ be the ring $\mathbb{Z}$ or a field of characteristic not equal to 2. (We require this to avoid certain annoyances in the discussion of alternating polynomials in characteristic 2.)

Say that a polynomial $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ is *alternating* if for every permutation w in $\mathfrak{S}_n$ one has that

$$(wf)(\mathbf{x}) = f(x_{w(1)}, \ldots, x_{w(n)}) = \mathrm{sgn}(w) f(\mathbf{x}).$$

Let $\Lambda^{\mathrm{sgn}} \subset \mathbf{k}[x_1, \ldots, x_n]$ denote the subset of alternating polynomials[137].

As with Λ and its monomial basis $\{m_\lambda\}$, there is an obvious $\mathbf{k}$-basis for Λ^{sgn}, coming from the fact that a polynomial $f = \sum_\alpha c_\alpha \mathbf{x}^\alpha$ is alternating if and only if $c_{w(\alpha)} = \mathrm{sgn}(w) c_\alpha$ for every w in $\mathfrak{S}_n$ and every $\alpha \in \mathbb{N}^n$. This means that every alternating f is a $\mathbf{k}$-linear combination of the following elements.

Definition 2.6.2. For $\alpha = (\alpha_1, \ldots, \alpha_n)$ in $\mathbb{N}^n$, define the *alternant*

$$a_\alpha := \sum_{w \in \mathfrak{S}_n} \mathrm{sgn}(w) w(\mathbf{x}^\alpha) = \det \begin{bmatrix} x_1^{\alpha_1} & \cdots & x_1^{\alpha_n} \\ x_2^{\alpha_1} & \cdots & x_2^{\alpha_n} \\ \vdots & \ddots & \vdots \\ x_n^{\alpha_1} & \cdots & x_n^{\alpha_n} \end{bmatrix}.$$

[135] For example, if $\beta = (1, 0, 3, 1, 2, 3, 0, 0, 0, \ldots)$, then $\mu = (3, 3, 2, 1, 1)$.

[136] See Exercise 2.3.8(a) for this.

[137] When $\mathbf{k}$ has characteristic 2 (or, more generally, is an arbitrary commutative ring), it is probably best to define the alternating polynomials $\Lambda_{\mathbf{k}}^{\mathrm{sgn}}$ as the $\mathbf{k}$-submodule $\Lambda^{\mathrm{sgn}} \otimes_{\mathbb{Z}} \mathbf{k}$ of $\mathbb{Z}[x_1, \ldots, x_n] \otimes_{\mathbb{Z}} \mathbf{k} \cong \mathbf{k}[x_1, \ldots, x_n]$.

Example 2.6.3. One has

$$a_{(1,5,0)} = x_1^1 x_2^5 x_3^0 - x_1^5 x_2^1 x_3^0 - x_1^1 x_2^0 x_3^5 - x_1^0 x_2^5 x_3^1 + x_1^0 x_2^1 x_3^5 + x_1^5 x_2^0 x_3^1 = -a_{(5,1,0)}.$$

Similarly, $a_{w(\alpha)} = \operatorname{sgn}(w) a_\alpha$ for every $w \in \mathfrak{S}_n$ and every $\alpha \in \mathbb{N}^n$.

Meanwhile, $a_{(5,2,2)} = 0$ since the transposition $t = \binom{123}{132}$ fixes $(5,2,2)$ and hence

$$a_{(5,2,2)} = t(a_{(5,2,2)}) = \operatorname{sgn}(t) a_{(5,2,2)} = -a_{(5,2,2)}.$$

[138] Alternatively, $a_{(5,2,2)} = 0$ as it is a determinant of a matrix with two equal columns. Similarly, $a_\alpha = 0$ for every n-tuple $\alpha \in \mathbb{N}^n$ having two equal entries.

This example illustrates that, for a $\mathbf{k}$-basis for Λ^{sgn}, one can restrict attention to alternants a_α in which α is a *strict partition*, i.e., in which α satisfies $\alpha_1 > \alpha_2 > \cdots > \alpha_n$. One can therefore uniquely express $\alpha = \lambda + \rho$, where λ is a (weak) partition $\lambda_1 \geq \cdots \geq \lambda_n \geq 0$ and where $\rho := (n-1, n-2, \ldots, 2, 1, 0)$ is sometimes called the *staircase partition*[139]. For example $\alpha = (5,1,0) = (3,0,0) + (2,1,0) = \lambda + \rho$.

Proposition 2.6.4. *Let $\mathbf{k}$ be the ring $\mathbb{Z}$ or a field of characteristic not equal to 2.*

The alternants $\{a_{\lambda+\rho}\}$ as λ runs through the partitions with at most n parts form a $\mathbf{k}$-basis for Λ^{sgn}. In addition, the bialternants $\left\{\frac{a_{\lambda+\rho}}{a_\rho}\right\}$ *as λ runs through the same set form a $\mathbf{k}$-basis for $\Lambda(x_1, \ldots, x_n) = \mathbf{k}[x_1, \ldots, x_n]^{\mathfrak{S}_n}$.*

Proof. The first assertion should be clear from our previous discussion: the alternants $\{a_{\lambda+\rho}\}$ span Λ^{sgn} by definition, and they are $\mathbf{k}$-linearly independent because they are supported on disjoint sets of monomials $\mathbf{x}^\alpha$.

The second assertion follows from the first, after proving the following **Claim**: $f(\mathbf{x})$ lies in Λ^{sgn} if and only if $f(\mathbf{x}) = a_\rho \cdot g(\mathbf{x})$ where $g(\mathbf{x})$ lies in $\mathbf{k}[\mathbf{x}]^{\mathfrak{S}_n}$ and where

$$a_\rho = \det(x_i^{n-j})_{i,j=1,2,\ldots,n} = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

is the *Vandermonde determinant/product*. In other words,

$$\Lambda^{\mathrm{sgn}} = a_\rho \cdot \mathbf{k}[\mathbf{x}]^{\mathfrak{S}_n}$$

is a free $\mathbf{k}[\mathbf{x}]^{\mathfrak{S}_n}$-module of rank 1, with a_ρ as its $\mathbf{k}[\mathbf{x}]^{\mathfrak{S}_n}$-basis element.

To see the Claim, first note the inclusion

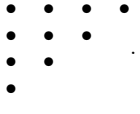
$$\Lambda^{\mathrm{sgn}} \supset a_\rho \cdot \mathbf{k}[\mathbf{x}]^{\mathfrak{S}_n}$$

since the product of a symmetric polynomial and an alternating polynomial is an alternating polynomial. For the reverse inclusion, note that since an alternating polynomial $f(\mathbf{x})$ changes sign whenever one exchanges two distinct variables x_i, x_j, it must vanish upon setting $x_i = x_j$, and therefore be divisible by $x_i - x_j$, so divisible by the entire product $\prod_{1 \leq i < j \leq n} (x_i - x_j) = a_\rho$. But then the quotient $g(\mathbf{x}) = \frac{f(\mathbf{x})}{a_\rho}$ is symmetric, as it is a quotient of two alternating polynomials. □

Let us now return to the general setting, where $\mathbf{k}$ is an arbitrary commutative ring. We are not requiring that the assumptions of Proposition 2.6.4 be valid; we can still study the a_α of Definition 2.6.2, but we cannot use Proposition 2.6.4 anymore. We will show that the fraction $\frac{a_{\lambda+\rho}}{a_\rho}$ is nevertheless a well-defined polynomial in $\Lambda(x_1, \ldots, x_n)$ whenever λ is a partition[140], and in fact equals the Schur function $s_\lambda(\mathbf{x})$. As a consequence, the mysterious bialternant basis $\left\{\frac{a_{\lambda+\rho}}{a_\rho}\right\}$ of $\Lambda(x_1, \ldots, x_n)$ defined in Proposition 2.6.4 still

[138] One subtlety should be addressed: We want to prove that $a_{(5,2,2)} = 0$ in $\mathbf{k}[x_1, \ldots, x_n]$ for every commutative ring $\mathbf{k}$. It is clearly enough to prove that $a_{(5,2,2)} = 0$ in $\mathbb{Z}[x_1, \ldots, x_n]$. Since 2 is not a zero-divisor in $\mathbb{Z}[x_1, \ldots, x_n]$, we can achieve this by showing that $a_{(5,2,2)} = -a_{(5,2,2)}$. We would not be able to make this argument directly over an arbitrary commutative ring $\mathbf{k}$.

[139] The name is owed to its Ferrers shape. For instance, if $n = 5$, then the Ferrers diagram of ρ (represented using dots) has the form



[140] This can also be deduced by base change from the $\mathbf{k} = \mathbb{Z}$ case of Proposition 2.6.4.

exists in the general setting, and is plainly the Schur functions $\{s_\lambda(\mathbf{x})\}$. Stembridge [210] noted that one could give a remarkably concise proof of an even stronger assertion, which simultaneously gives one of the standard combinatorial interpretations for the Littlewood-Richardson coefficients $c^\lambda_{\mu,\nu}$. For the purposes of stating it, we introduce for a tableau T the notation $T|_{\text{cols}\geq j}$ (resp. $T|_{\text{cols}\leq j}$) to indicate the subtableau which is the restriction of T to the union of its columns $j, j+1, j+2, \ldots$ (resp. columns $1, 2, \ldots, j$).

Example 2.6.5. If $T = \begin{array}{cc} & \\ 2 & 2 \\ 3 & 5 \end{array}\begin{array}{cc} 1 & 2 \\ 2 & 3 \\ & \end{array}$, then

$$T|_{\text{cols}\geq 3} = \begin{array}{cc} 1 & 2 \\ 2 & 3 \end{array} \qquad \text{and} \qquad T|_{\text{cols}\leq 2} = \begin{array}{cc} & 2 \\ 3 & 5 \end{array}$$

(note that $T|_{\text{cols}\leq 2}$ has an empty first row).

Theorem 2.6.6. *For partitions λ, μ, ν with $\mu \subseteq \lambda$, one has*[141]

$$a_{\nu+\rho} s_{\lambda/\mu} = \sum_T a_{\nu+\text{cont}(T)+\rho}$$

where T runs through all column-strict tableaux with entries in $\{1, 2, \ldots, n\}$ of shape λ/μ with the property that for each $j = 1, 2, 3, \ldots$, the weak composition $\nu + \text{cont}(T|_{\text{cols}\geq j})$ is a partition.

Before proving Theorem 2.6.6, let us see some of its consequences.

Corollary 2.6.7. *For any partition λ, we have*[142]

$$s_\lambda(\mathbf{x}) = \frac{a_{\lambda+\rho}}{a_\rho}.$$

Proof. Fix a partition λ. Take $\nu = \mu = \varnothing$ in Theorem 2.6.6. Note that there is only one column-strict tableau T of shape λ such that each $\text{cont}(T|_{\text{cols}\geq j})$ is a partition, namely the tableau having every entry in row i equal to i:

$$\begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & & \\ 3 & 3 & 3 & & \\ 4 & 4 & & & \end{array}$$

[143]. Furthermore, this T has $\text{cont}(T) = \lambda$, so the theorem says $a_\rho s_\lambda = a_{\lambda+\rho}$. □

[141] Again, we can drop the requirement that $\mu \subseteq \lambda$, provided that we understand that there are no column-strict tableaux of shape λ/μ unless $\mu \subseteq \lambda$.

[142] Notice that division by a_ρ is unambiguous in the ring $\mathbf{k}[x_1, \ldots, x_n]$, since a_ρ is not a zero-divisor (in fact, $a_\rho = \prod_{1\leq i<j\leq n}(x_i - x_j)$ is the product of the binomials $x_i - x_j$, none of which is a zero-divisor).

[143] *Proof.* It is clear that the tableau having every entry in row i equal to i indeed satisfies the condition that each $\text{cont}(T|_{\text{cols}\geq j})$ is a partition. It remains to show that it is the only column-strict tableau (of shape λ) satisfying this condition.

Let T be a column-strict tableau of shape λ satisfying the condition that each $\text{cont}(T|_{\text{cols}\geq j})$ is a partition. We must show that for each i, every entry in row i of T is equal to i. Assume the contrary. Thus, there exists some i such that row i of T contains an entry distinct from i. Consider the smallest such i. Hence, rows $1, 2, \ldots, i-1$ of T are filled with entries $1, 2, \ldots, i-1$, whereas row i has some entry distinct from i. Choose some j such that the j-th entry of row i of T is distinct from i. This entry cannot be smaller than i (since it has $i-1$ entries above it in its column, and the entries of T increase strictly down columns); thus, it has to be larger than i. Therefore, all entries in rows $i, i+1, i+2, \ldots$ of $T|_{\text{cols}\geq j}$ are larger than i as well (since they lie southeast of this entry). Hence, each entry of $T|_{\text{cols}\geq j}$ is either smaller than i (if it is in one of rows $1, 2, \ldots, i-1$) or larger than i (if it is in row i or further down). Thus, i is not an entry of $T|_{\text{cols}\geq j}$. In other words, $\text{cont}_i(T|_{\text{cols}\geq j}) = 0$. Since $\text{cont}(T|_{\text{cols}\geq j})$ is a partition, we thus conclude that $\text{cont}_k(T|_{\text{cols}\geq j}) = 0$ for all $k > i$. In other words, $T|_{\text{cols}\geq j}$ has no entries larger than i. But this contradicts the fact that the j-th entry of row i of T is larger than i. This contradiction completes our proof.

Example 2.6.8. For $n = 2$, so that $\rho = (1, 0)$, if we take $\lambda = (4, 2)$, then one has

$$\begin{aligned}\frac{a_{\lambda+\rho}}{a_\rho} &= \frac{a_{(4,2)+(1,0)}}{a_{(1,0)}} = \frac{a_{(5,2)}}{a_{(1,0)}} \\ &= \frac{x_1^5 x_2^2 - x_1^2 x_2^5}{x_1 - x_2} \\ &= x_1^4 x_2^2 + x_1^3 x_2^3 + x_1^2 x_2^4 \\ &= \mathbf{x}^{\operatorname{cont}\binom{1111}{22}} + \mathbf{x}^{\operatorname{cont}\binom{1112}{22}} + \mathbf{x}^{\operatorname{cont}\binom{1122}{22}} \\ &= s_{(4,2)} = s_\lambda.\end{aligned}$$

Some authors use the equality in Corollary 2.6.7 to *define* the Schur polynomial $s_\lambda(x_1, x_2, \ldots, x_n)$ in n variables; this definition, however, has the drawback of not generalizing easily to infinitely many variables or to skew Schur functions[144].

Next divide through by a_ρ on both sides of Theorem 2.6.6 (and use Corollary 2.6.7) to give the following.

Corollary 2.6.9. *For partitions λ, μ, ν having at most n parts, one has*

$$s_\nu s_{\lambda/\mu} = \sum_T s_{\nu+\operatorname{cont}(T)} \tag{2.6.1}$$

where T runs through the same set as in Theorem 2.6.6. In particular, taking $\nu = \varnothing$, we obtain

$$s_{\lambda/\mu} = \sum_T s_{\operatorname{cont}(T)} \tag{2.6.2}$$

where in the sum T runs through all column-strict tableaux of shape λ/μ for which each $\operatorname{cont}(T|_{\text{cols}\geq j})$ is a partition.

Proof of Theorem 2.6.6. Start by rewriting the left side of the theorem:

$$\begin{aligned}a_{\nu+\rho} s_{\lambda/\mu} &= \sum_{w\in\mathfrak{S}_n} \operatorname{sgn}(w)\mathbf{x}^{w(\nu+\rho)} s_{\lambda/\mu} = \sum_{w\in\mathfrak{S}_n} \operatorname{sgn}(w)\mathbf{x}^{w(\nu+\rho)} w(s_{\lambda/\mu}) \\ &\qquad \left(\text{since } w(s_{\lambda/\mu}) = s_{\lambda/\mu} \text{ for any } w \in \mathfrak{S}_n\right) \\ &= \sum_{w\in\mathfrak{S}_n} \operatorname{sgn}(w)\mathbf{x}^{w(\nu+\rho)} \sum_{\substack{\text{column-strict } T \\ \text{of shape } \lambda/\mu}} \mathbf{x}^{w(\operatorname{cont}(T))} \\ &= \sum_{\substack{\text{column-strict } T \\ \text{of shape } \lambda/\mu}} \sum_{w\in\mathfrak{S}_n} \operatorname{sgn}(w)\mathbf{x}^{w(\nu+\operatorname{cont}(T)+\rho)} \\ &= \sum_{\substack{\text{column-strict } T \\ \text{of shape } \lambda/\mu}} a_{\nu+\operatorname{cont}(T)+\rho}.\end{aligned}$$

We wish to cancel out all the summands indexed by column-strict tableaux T which fail any of the conditions that $\nu + \operatorname{cont}(T|_{\text{cols}\geq j})$ be a partition. Given such a T, find the maximal j for which it fails this condition[145], and then find the minimal k for which

$$\nu_k + \operatorname{cont}_k(T|_{\text{cols}\geq j}) < \nu_{k+1} + \operatorname{cont}_{k+1}(T|_{\text{cols}\geq j}).$$

Maximality of j forces

$$\nu_k + \operatorname{cont}_k(T|_{\text{cols}\geq j+1}) \geq \nu_{k+1} + \operatorname{cont}_{k+1}(T|_{\text{cols}\geq j+1}).$$

[144]With some effort, it is possible to use Corollary 2.6.7 in order to define the Schur function s_λ in infinitely many variables. Indeed, one can define this Schur function as the unique element of Λ whose evaluation at $(x_1, x_2, \ldots, x_n)$ equals $\frac{a_{\lambda+\rho}}{a_\rho}$ for every $n \in \mathbb{N}$. If one wants to use such a definition, however, one needs to check that such an element exists. This is the approach to defining s_λ taken in [126, Definition 1.4.2] and in [142, §I.3].

[145]Such a j exists because $\nu + \operatorname{cont}(T|_{\text{cols}\geq j})$ is a partition for all sufficiently high j (in fact, ν itself is a partition).

Since column-strictness implies that column j of T can contain at most one occurrence of k or of $k+1$ (or neither or both), the previous two inequalities imply that column j must contain an occurrence of $k+1$ and no occurrence of k, so that

$$\nu_k + \operatorname{cont}_k(T|_{\text{cols}\geq j}) + 1 = \nu_{k+1} + \operatorname{cont}_{k+1}(T|_{\text{cols}\geq j}).$$

This implies that the adjacent transposition $t_{k,k+1}$ swapping k and $k+1$ fixes the vector $\nu+\operatorname{cont}(T|_{\text{cols}\geq j})+\rho$.

Now create a new tableau T^* from T by applying the Bender-Knuth involution (from the proof of Proposition 2.2.4) on letters $k, k+1$, but *only to columns* $1, 2, \ldots, j-1$ of T, leaving columns $j, j+1, j+2, \ldots$ unchanged.[146] One should check that T^* is still column-strict, but this holds because column j of T has no occurrences of letter k. Note that

$$t_{k,k+1} \operatorname{cont}(T|_{\text{cols}\leq j-1}) = \operatorname{cont}(T^*|_{\text{cols}\leq j-1})$$

and hence

$$t_{k,k+1}(\nu + \operatorname{cont}(T) + \rho) = \nu + \operatorname{cont}(T^*) + \rho,$$

so that $a_{\nu+\operatorname{cont}(T)+\rho} = -a_{\nu+\operatorname{cont}(T^*)+\rho}$.

Because T and T^* have exactly the same columns $j, j+1, j+2, \ldots$, the tableau T^* is also a violator of at least one of the conditions that $\nu + \operatorname{cont}(T^*|_{\text{cols}\geq j})$ be a partition, and has the same choice of maximal j and minimal k as did T. Hence the map $T \mapsto T^*$ is an involution on the violators that lets one cancel their summands $a_{\nu+\operatorname{cont}(T)+\rho}$ and $a_{\nu+\operatorname{cont}(T^*)+\rho}$ in pairs.[147] □

Example 2.6.10. Here is an example of the construction of T^* in the above proof. Let $n = 6$ and $\lambda = (5,4,4)$ and $\mu = (2,2)$ and $\nu = (1)$. Let T be the column-strict tableau

$$\begin{array}{cccccc} & & & 1 & 2 & 2 \\ & & & 2 & 3 & \\ 2 & 2 & 3 & 4 & & \end{array} \quad \text{of shape } \lambda/\mu.$$

Then,

$$\operatorname{cont}(T|_{\text{cols}\geq 5}) = (0,1,0,0,0,\ldots) \quad (\text{since } T|_{\text{cols}\geq 5} \text{ has a single entry, which is 2}),$$
$$\text{so that} \quad \nu + \operatorname{cont}(T|_{\text{cols}\geq 5}) = (1,1,0,0,0,\ldots) \text{ is a partition.}$$

But

$$\operatorname{cont}(T|_{\text{cols}\geq 4}) = (0,2,1,1,0,0,0,\ldots),$$
$$\text{and thus} \quad \nu + \operatorname{cont}(T|_{\text{cols}\geq 4}) = (1,2,1,1,0,0,0,\ldots) \text{ is not a partition.}$$

Thus, the j in the above proof of Theorem 2.6.6 is 4. Furthermore, the k in the proof is 1, since $\nu_1 + \operatorname{cont}_1(T|_{\text{cols}\geq 4}) = 1+0 = 1 < 2 = 0+2 = \nu_2 + \operatorname{cont}_2(T|_{\text{cols}\geq 4})$. Thus, T^* is obtained from T by applying the Bender-Knuth involution on letters $1, 2$ to columns $1, 2, 3$ only, leaving columns $4, 5$ unchanged. The result is

$$T^* = \begin{array}{cccccc} & & & 1 & 2 & 2 \\ & & & 2 & 3 & \\ 1 & 1 & 3 & 4 & & \end{array}.$$

So far (in this section) we have worked with a finite set of variables $x_1, x_2, \ldots, x_n$ (where n is a fixed nonnegative integer) and with partitions having at most n parts. We now drop these conventions and restrictions; thus, partitions again mean arbitrary partitions, and $\mathbf{x}$ again means the infinite family $(x_1, x_2, x_3, \ldots)$ of variables. In this setting, we have the following analogue of Corollary 2.6.9:

---

[146] See Example 2.6.10 below for an example of this construction.

[147] One remark is in order: The tableaux T and T^* may be equal. In this case, the summands $a_{\nu+\operatorname{cont}(T)+\rho}$ and $a_{\nu+\operatorname{cont}(T^*)+\rho}$ do not cancel, as they are the same summand. However, this summand is zero (because $t_{k,k+1}(\nu+\operatorname{cont}(T)+\rho) = \nu+\operatorname{cont}\left(\underbrace{T^*}_{=T}\right)+\rho = \nu+\operatorname{cont}(T)+\rho$ shows that the n-tuple $\nu+\operatorname{cont}(T)+\rho$ has two equal entries, and thus $a_{\nu+\operatorname{cont}(T)+\rho} = 0$), and thus does not affect the sum.

Corollary 2.6.11. *For partitions λ, μ, ν (of any lengths), one has*

$$s_\nu s_{\lambda/\mu} = \sum_T s_{\nu+\mathrm{cont}(T)} \tag{2.6.3}$$

where T runs through all column-strict tableaux of shape λ/μ with the property that for each $j = 1, 2, 3, \ldots$, the weak composition $\nu + \mathrm{cont}(T|_{\mathrm{cols}\geq j})$ is a partition. In particular, taking $\nu = \varnothing$, we obtain

$$s_{\lambda/\mu} = \sum_T s_{\mathrm{cont}(T)} \tag{2.6.4}$$

where in the sum T runs through all column-strict tableaux of shape λ/μ for which each $\mathrm{cont}(T|_{\mathrm{cols}\geq j})$ is a partition.

Proof of Corollary 2.6.11. Essentially, Corollary 2.6.11 is obtained from Corollary 2.6.9 by "letting n (that is, the number of variables) tend to ∞". This can be formalized in different ways: One way is to endow the ring of power series $\mathbf{k}[[\mathbf{x}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots]]$ with the coefficientwise topology[148], and to show that the left hand side of (2.6.1) tends to the left hand side of (2.6.3) when $n \to \infty$, and the same holds for the right hand sides. A different approach proceeds by regarding Λ as the inverse limit of the $\Lambda(x_1, x_2, \ldots, x_n)$. □

Comparing coefficients of a given Schur function s_ν in (2.6.4), we obtain the following version of the Littlewood-Richardson rule.

Corollary 2.6.12. *For partitions λ, μ, ν (of any lengths), the Littlewood-Richardson coefficient $c^\lambda_{\mu,\nu}$ counts column-strict tableaux T of shape λ/μ with $\mathrm{cont}(T) = \nu$ having the property that each $\mathrm{cont}(T|_{\mathrm{cols}\geq j})$ is a partition.*

2.7. **The Pieri and Assaf-McNamara skew Pieri rule.** The classical *Pieri rule* refers to two special cases of the Littlewood-Richardson rule. To state them, recall that a skew shape is called a *horizontal (resp. vertical) strip* if no two of its cells lie in the same column (resp. row). A *horizontal (resp. vertical) n-strip* (for $n \in \mathbb{N}$) shall mean a horizontal (resp. vertical) strip of size n (that is, having exactly n cells).

Theorem 2.7.1. *For every partition λ and any $n \in \mathbb{N}$, we have*

$$s_\lambda h_n = \sum_{\substack{\lambda^+ : \lambda^+/\lambda \text{ is a} \\ \text{horizontal } n\text{-strip}}} s_{\lambda^+}; \tag{2.7.1}$$

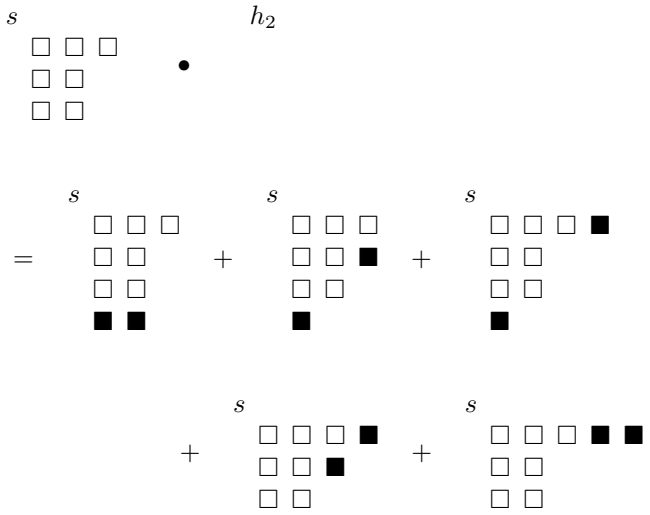
$$s_\lambda e_n = \sum_{\substack{\lambda^+ : \lambda^+/\lambda \text{ is a} \\ \text{vertical } n\text{-strip}}} s_{\lambda^+}. \tag{2.7.2}$$

[148]This topology is defined as follows:

We endow the ring $\mathbf{k}$ with the discrete topology. Then, we can regard the $\mathbf{k}$-module $\mathbf{k}[[\mathbf{x}]]$ as a direct product of infinitely many copies of $\mathbf{k}$ (by identifying every power series in $\mathbf{k}[[\mathbf{x}]]$ with the family of its coefficients). Hence, the product topology is a well-defined topology on $\mathbf{k}[[\mathbf{x}]]$; this topology is denoted as the *coefficientwise topology*. Its name is due to the fact that a sequence $(a_n)_{n\in\mathbb{N}}$ of power series converges to a power series a with respect to this topology if and only if for every monomial $\mathfrak{m}$, all sufficiently high $n \in \mathbb{N}$ satisfy

$$(\text{the coefficient of } \mathfrak{m} \text{ in } a_n) = (\text{the coefficient of } \mathfrak{m} \text{ in } a).$$

Example 2.7.2. In the following equality, we are representing each partition by its Ferrers diagram[149].



If λ is the partition $(3,2,2)$ on the left hand side, then all partitions λ^+ on the right hand side visibly have the property that λ^+/λ is a horizontal 2-strip[150], as (2.7.1) predicts.

Proof of Theorem 2.7.1. For the first Pieri formula involving h_n, as $h_n = s_{(n)}$ one has

$$s_\lambda h_n = \sum_{\lambda^+} c^{\lambda^+}_{\lambda,(n)} s_{\lambda^+}.$$

Corollary 2.6.12 says $c^{\lambda^+}_{\lambda,(n)}$ counts column-strict tableaux T of shape λ^+/λ having $\mathrm{cont}(T) = (n)$ (i.e. all entries of T are 1's), with an extra condition. Since its entries are all equal, such a T must certainly have shape being a horizontal strip, and more precisely a horizontal n-strip (since it has n cells). Conversely, for any horizontal n-strip, there is a unique such filling, and it will trivially satisfy the extra condition that $\mathrm{cont}(T|_{\mathrm{cols}\geq j})$ is a partition for each j. Hence $c^{\lambda^+}_{\lambda,(n)}$ is 1 if λ^+/λ is a horizontal n-strip, and 0 else.

For the second Pieri formula involving e_n, using $e_n = s_{(1^n)}$ one has

$$s_\lambda e_n = \sum_{\lambda^+} c^{\lambda^+}_{\lambda,(1^n)} s_{\lambda^+}.$$

Corollary 2.6.12 says $c^{\lambda^+}_{\lambda,(1^n)}$ counts column-strict tableaux T of shape λ^+/λ having $\mathrm{cont}(T) = (1^n)$, so its entries are $1, 2, \ldots, n$ each occurring once, with the extra condition that $1, 2, \ldots, n$ appear from right to left. Together with the tableau condition, this forces at most one entry in each row, that is λ^+/λ is a vertical strip, and then there is a unique way to fill it (maintaining column-strictness and the extra condition that $1, 2, \ldots, n$ appear from right to left). Thus $c^{\lambda^+}_{\lambda,(1^n)}$ is 1 if λ^+/λ is a vertical n-strip, and 0 else. □

In 2009, Assaf and McNamara [9] proved an elegant generalization.

[149] And we are drawing each Ferrers diagram with its boxes spaced out, in order to facilitate counting the boxes.

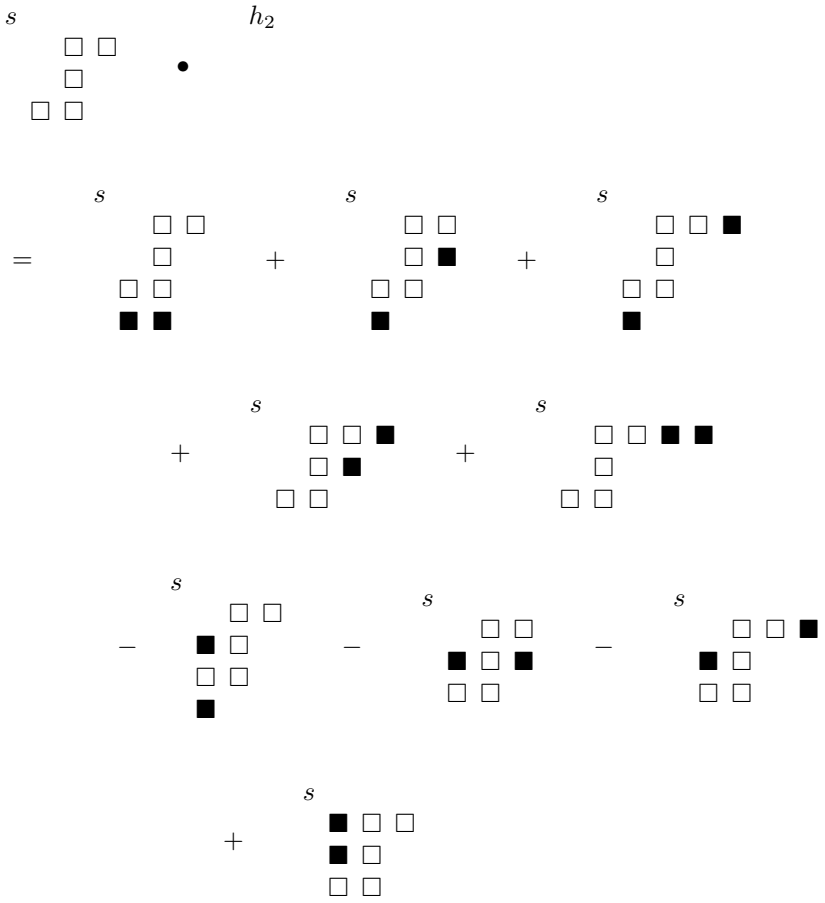
[150] We have colored the boxes of λ^+/λ black.

Theorem 2.7.3. *For any partitions λ and μ and any $n \in \mathbb{N}$, we have*[151]

$$s_{\lambda/\mu} h_n = \sum_{\substack{\lambda^+, \mu^-: \\ \lambda^+/\lambda \text{ a horizontal strip;} \\ \mu/\mu^- \text{ a vertical strip;} \\ |\lambda^+/\lambda| + |\mu/\mu^-| = n}} (-1)^{|\mu/\mu^-|} s_{\lambda^+/\mu^-}; \tag{2.7.3}$$

$$s_{\lambda/\mu} e_n = \sum_{\substack{\lambda^+, \mu^-: \\ \lambda^+/\lambda \text{ a vertical strip;} \\ \mu/\mu^- \text{ a horizontal strip;} \\ |\lambda^+/\lambda| + |\mu/\mu^-| = n}} (-1)^{|\mu/\mu^-|} s_{\lambda^+/\mu^-}. \tag{2.7.4}$$

Example 2.7.4. With the same conventions as in Example 2.7.2[152], we have



which illustrates the first equality of Theorem 2.7.3.

Theorem 2.7.3 is proven in the next section, using an important Hopf algebra tool.

Exercise 2.7.5. Let $\lambda = (\lambda_1, \lambda_2, \lambda_3, \ldots)$ and $\mu = (\mu_1, \mu_2, \mu_3, \ldots)$ be two partitions such that $\mu \subseteq \lambda$.

(a) Show that λ/μ is a horizontal strip if and only if every $i \in \{1, 2, 3, \ldots\}$ satisfies $\mu_i \geq \lambda_{i+1}$. [153]

(b) Show that λ/μ is a vertical strip if and only if every $i \in \{1, 2, 3, \ldots\}$ satisfies $\lambda_i \leq \mu_i + 1$.

Exercise 2.7.6. (a) Let λ and μ be two partitions such that $\mu \subseteq \lambda$. Let $n \in \mathbb{N}$. Show that $\left(h_n, s_{\lambda/\mu}\right)$ equals 1 if λ/μ is a horizontal n-strip, and equals 0 otherwise.

[151] Note that $\mu \subseteq \lambda$ is not required. (The left hand sides are 0 otherwise, but this does not trivialize the equalities.)

[152] but this time coloring both the boxes in λ^+/λ and the boxes in μ/μ^- black

[153] In other words, λ/μ is a horizontal strip if and only if $(\lambda_2, \lambda_3, \lambda_4, \ldots) \subseteq \mu$. This simple observation has been used by Pak and Postnikov [165, §10] for a new approach to RSK-type algorithms.

(b) Use part (a) to give a new proof of (2.7.1).

Exercise 2.7.7. Prove Theorem 2.7.1 again using the ideas of the proof of Theorem 2.5.1.

Exercise 2.7.8. Let A be a commutative ring, and $n \in \mathbb{N}$.

(a) Let $a_1, a_2, \ldots, a_n$ be n elements of A. Let $b_1, b_2, \ldots, b_n$ be n further elements of A. If $a_i - b_j$ is an invertible element of A for every $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$, then prove that

$$\det\left(\left(\frac{1}{a_i - b_j}\right)_{i,j=1,2,\ldots,n}\right) = \frac{\prod_{1 \leq j < i \leq n} \left(\left(a_i - a_j\right)\left(b_j - b_i\right)\right)}{\prod_{(i,j) \in \{1,2,\ldots,n\}^2} \left(a_i - b_j\right)}.$$

(b) Let $a_1, a_2, \ldots, a_n$ be n elements of A. Let $b_1, b_2, \ldots, b_n$ be n further elements of A. If $1 - a_i b_j$ is an invertible element of A for every $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$, then prove that

$$\det\left(\left(\frac{1}{1 - a_i b_j}\right)_{i,j=1,2,\ldots,n}\right) = \frac{\prod_{1 \leq j < i \leq n} \left(\left(a_i - a_j\right)\left(b_i - b_j\right)\right)}{\prod_{(i,j) \in \{1,2,\ldots,n\}^2} \left(1 - a_i b_j\right)}.$$

(c) Use the result of part (b) to give a new proof for Theorem 2.5.1.[154]

The determinant on the left hand side of Exercise 2.7.8(a) is known as the *Cauchy determinant*.

Exercise 2.7.9. Prove that $s_{(a,b)} = h_a h_b - h_{a+1} h_{b-1}$ for any two integers $a \geq b \geq 0$ (where we set $h_{-1} = 0$ as usual).

(Note that this is precisely the Jacobi-Trudi formula (2.4.16) in the case when $\lambda = (a, b)$ is a partition with at most two entries and $\mu = \varnothing$.)

Exercise 2.7.10. If λ is a partition and μ is a weak composition, let $K_{\lambda,\mu}$ denote the number of column-strict tableaux T of shape λ having $\operatorname{cont}(T) = \mu$. (This $K_{\lambda,\mu}$ is called the (λ, μ)-*Kostka number*.)

(a) Use Theorem 2.7.1 to show that every partition μ satisfies $h_\mu = \sum_\lambda K_{\lambda,\mu} s_\lambda$, where the sum ranges over all partitions λ.

(b) Use this to give a new proof for Theorem 2.5.1.[155]

(c) Give a new proof of the fact (previously shown as Proposition 2.4.3(j)) that $(h_\lambda)_{\lambda \in \mathrm{Par}}$ is a graded basis of the graded $\mathbf{k}$-module Λ.

Exercise 2.7.11. (a) Define a $\mathbf{k}$-linear map $\mathfrak{Z} : \Lambda \to \Lambda$ by having it send s_λ to s_{λ^t} for every partition λ. (This is clearly well-defined, since $(s_\lambda)_{\lambda \in \mathrm{Par}}$ is a $\mathbf{k}$-basis of Λ.) Show that

$$\mathfrak{Z}(f h_n) = \mathfrak{Z}(f) \cdot \mathfrak{Z}(h_n) \qquad \text{for every } f \in \Lambda \text{ and every } n \in \mathbb{N}.$$

(b) Show that $\mathfrak{Z} = \omega$.

(c) Show that $c^\lambda_{\mu,\nu} = c^{\lambda^t}_{\mu^t,\nu^t}$ for any three partitions λ, μ and ν.

(d) Use this to prove (2.4.15).[156]

Exercise 2.7.12. (a) Show that

$$\prod_{i,j=1}^{\infty} (1 + x_i y_j) = \sum_{\lambda \in \mathrm{Par}} s_\lambda(\mathbf{x}) s_{\lambda^t}(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} e_\lambda(\mathbf{x}) m_\lambda(\mathbf{y})$$

in the power series ring $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$.

(b) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Show that

$$\prod_{i,j=1}^{\infty} (1 + x_i y_j) = \sum_{\lambda \in \mathrm{Par}} (-1)^{|\lambda| - \ell(\lambda)} z_\lambda^{-1} p_\lambda(\mathbf{x}) p_\lambda(\mathbf{y})$$

in the power series ring $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$, where z_λ is defined as in Proposition 2.5.15.

[154] This approach to Theorem 2.5.1 is taken in [44, §4] (except that [44] only works with finitely many variables).

[155] Of course, this gives a new proof of Theorem 2.5.1 only when coupled with a proof of Theorem 2.7.1 which does not rely on Theorem 2.5.1. The proof of Theorem 2.7.1 we gave in the text above did not rely on Theorem 2.5.1, whereas the proof of (2.7.1) given in Exercise 2.7.6(b) did.

[156] The first author learned this approach to (2.4.15) from Alexander Postnikov.

The first equality of Exercise 2.7.12(a) appears in [206, Thm. 7.14.3], [186, Thm. 4.8.6] and several other references under the name of the *dual Cauchy identity*, and is commonly proven using a "dual" analogue of the Robinson-Schensted-Knuth algorithm.

Exercise 2.7.13. Prove Theorem 2.4.6.

[**Hint:**[157] Switch $\mathbf{x}$ and $\mathbf{y}$ in the formula of Exercise 2.5.11(a), and specialize the resulting equality by replacing $\mathbf{y}$ by a finite set of variables $(y_1, y_2, \ldots, y_\ell)$; then, set $n = \ell$ and $\rho = (n-1, n-2, \ldots, 0)$, and multiply with the alternant $a_\rho(y_1, y_2, \ldots, y_\ell)$, using Corollary 2.6.7 to simplify the result; finally, extract the coefficient of $\mathbf{y}^{\lambda+\rho}$.]

Exercise 2.7.14. Prove the following:

(a) We have $(S(f), S(g)) = (f, g)$ for all $f \in \Lambda$ and $g \in \Lambda$.

(b) We have $(e_n, f) = (-1)^n \cdot (S(f))(1)$ for any $n \in \mathbb{N}$ and $f \in \Lambda_n$. (See Exercise 2.1.2 for the meaning of $(S(f))(1)$.)

2.8. **Skewing and Lam's proof of the skew Pieri rule.** We codify here the operation $s_\mu^\perp$ of *skewing by* s_μ, acting on Schur functions via

$$s_\mu^\perp(s_\lambda) = s_{\lambda/\mu}$$

(where, as before, one defines $s_{\lambda/\mu} = 0$ if $\mu \not\subseteq \lambda$). These operations play a crucial role

- in Lam's proof of the skew Pieri rule,
- in Lam, Lauve, and Sottile's proof [120] of a more general skew Littlewood-Richardson rule that had been conjectured by Assaf and McNamara, and
- in Zelevinsky's structure theory of PSH's to be developed in the next chapter.

We are going to define them in the general setting of any graded Hopf algebra.

Definition 2.8.1. Given a graded Hopf algebra A, and its (graded) dual A^o, let $(\cdot,\cdot) = (\cdot,\cdot)_A : A^o \times A \to \mathbf{k}$ be the pairing defined by $(f, a) := f(a)$ for f in A^o and a in A. Then define for each f in A^o an operator $A \xrightarrow{f^\perp} A$ as follows[158]: for a in A with $\Delta(a) = \sum a_1 \otimes a_2$, let

$$f^\perp(a) = \sum (f, a_1) a_2.$$

In other words, $f^\perp$ is the composition

$$A \xrightarrow{\Delta} A \otimes A \xrightarrow{f \otimes \mathrm{id}} \mathbf{k} \otimes A \xrightarrow{\cong} A,$$

where the rightmost arrow is the canonical isomorphism $\mathbf{k} \otimes A \to A$. This operator $f^\perp$ is called *skewing by* f.

Now, recall that the Hall inner product induces an isomorphism $\Lambda^o \cong \Lambda$ (by Corollary 2.5.14). Hence, we can regard any element $f \in \Lambda$ as an element of Λ^o; this allows us to define an operator $f^\perp : \Lambda \to \Lambda$ for each $f \in \Lambda$ (by regarding f as an element of Λ^o, and applying Definition 2.8.1 to $A = \Lambda$). Explicitly, this operator is given by

$$f^\perp(a) = \sum (f, a_1) a_2 \qquad \text{whenever} \qquad \Delta(a) = \sum a_1 \otimes a_2, \tag{2.8.1}$$

where the inner product (f, a_1) is now understood as a Hall inner product.

Recall that each partition λ satisfies

$$\Delta s_\lambda = \sum_{\mu \subseteq \lambda} s_\mu \otimes s_{\lambda/\mu} = \sum_{\nu \subseteq \lambda} s_\nu \otimes s_{\lambda/\nu} = \sum_\nu s_\nu \otimes s_{\lambda/\nu}$$

(since $s_{\lambda/\nu} = 0$ unless $\nu \subseteq \lambda$). Hence, for any two partitions λ and μ, we have

$$s_\mu^\perp(s_\lambda) = \sum_\nu \underbrace{(s_\mu, s_\nu)}_{=\delta_{\mu,\nu}} s_{\lambda/\nu} \qquad \text{(by (2.8.1), applied to } f = s_\mu \text{ and } a = s_\lambda\text{)}$$

$$= \sum_\nu \delta_{\mu,\nu} s_{\lambda/\nu} = s_{\lambda/\mu}. \tag{2.8.2}$$

[157] This is the proof given in Stanley [206, §7.16, Second Proof of Thm. 7.16.1] and Macdonald [142, proof of (5.4)].

[158] This $f^\perp(a)$ is called $a \leftharpoonup f$ in Montgomery [157, Example 1.6.5].

Thus, skewing acts on the Schur functions exactly as desired.

Proposition 2.8.2. *Let A be a graded Hopf algebra. The $f^\perp$ operators $A \to A$ have the following properties.*

(i) *For every $f \in A^o$, the map $f^\perp$ is adjoint to left multiplication $A^o \xrightarrow{f\cdot} A^o$ in the sense that*

$$(g, f^\perp(a)) = (fg, a).$$

(ii) *For every $f, g \in A^o$, we have $(fg)^\perp(a) = g^\perp(f^\perp(a))$, that is, A becomes a right A^o-module via the $f^\perp$ action.*[159]

(iii) *The unity 1_{A^o} of the $\mathbf{k}$-algebra A^o satisfies $(1_{A^o})^\perp = \mathrm{id}_A$.*

(iv) *Assume that A is of finite type (so A^o becomes a Hopf algebra, not just an algebra). If an $f \in A^o$ satisfies $\Delta(f) = \sum f_1 \otimes f_2$, then*

$$f^\perp(ab) = \sum f_1^\perp(a) f_2^\perp(b).$$

In particular, if f is primitive in A^o, so that $\Delta(f) = f \otimes 1 + 1 \otimes f$, then $f^\perp$ is a derivation*:*

$$f^\perp(ab) = f^\perp(a) \cdot b + a \cdot f^\perp(b).$$

Proof. For (i), note that

$$(g, f^\perp(a)) = \sum (f, a_1)(g, a_2) = (f \otimes g, \Delta_A(a)) = (m_{A^o}(f \otimes g), a) = (fg, a).$$

For (ii), using (i) and considering any h in A^o, one has that

$$(h, (fg)^\perp(a)) = (fgh, a) = (gh, f^\perp(a)) = (h, g^\perp(f^\perp(a))).$$

For (iii), we recall that the unity 1_{A^o} of A^o is the counit ϵ of A, and thus every $a \in A$ satisfies

$$\begin{aligned}(1_{A^o})^\perp(a) = \epsilon^\perp(a) &= \sum_{(a)} \underbrace{(\epsilon, a_1)}_{=\epsilon(a_1)} a_2 \qquad \left(\text{by the definition of } \epsilon^\perp\right) \\ &= \sum_{(a)} \epsilon(a_1)\, a_2 = a \qquad (\text{by the axioms of a coalgebra}),\end{aligned}$$

so that $(1_{A^o})^\perp = \mathrm{id}_A$.

For (iv), noting that

$$\Delta(ab) = \Delta(a)\Delta(b) = \left(\sum_{(a)} a_1 \otimes a_2\right)\left(\sum_{(b)} b_1 \otimes b_2\right) = \sum_{(a),(b)} a_1 b_1 \otimes a_2 b_2,$$

one has that

$$\begin{aligned}f^\perp(ab) &= \sum_{(a),(b)} (f, a_1 b_1)_A \; a_2 b_2 = \sum_{(a),(b)} (\Delta(f), a_1 \otimes b_1)_{A\otimes A} \; a_2 b_2 \\ &= \sum_{(f),(a),(b)} (f_1, a_1)_A (f_2, b_1)_A \; a_2 b_2 \\ &= \sum_{(f)} \left(\sum_{(a)} (f_1, a_1)_A a_2\right)\left(\sum_{(b)} (f_2, b_1)_A b_2\right) = \sum_{(f)} f_1^\perp(a) f_2^\perp(b).\end{aligned}$$

□

The Pieri rules (Theorem 2.7.1) expressed multiplication by h_n or by e_n in the basis $(s_\lambda)_{\lambda \in \mathrm{Par}}$ of Λ. We can similarly express skewing by h_n or by e_n:

[159] This makes sense, since A^o is a $\mathbf{k}$-algebra (by Exercise 1.6.1(c), applied to $C = A$).

Proposition 2.8.3. *For every partition λ and any $n \in \mathbb{N}$, we have*

$$h_n^\perp s_\lambda = \sum_{\substack{\lambda^- : \lambda/\lambda^- \text{ is a} \\ \text{horizontal } n\text{-strip}}} s_{\lambda^-}; \tag{2.8.3}$$

$$e_n^\perp s_\lambda = \sum_{\substack{\lambda^- : \lambda/\lambda^- \text{ is a} \\ \text{vertical } n\text{-strip}}} s_{\lambda^-}. \tag{2.8.4}$$

Exercise 2.8.4. Prove Proposition 2.8.3.
[**Hint:** Use Theorem 2.7.1 and $(s_{\mu^-}, e_n^\perp s_\mu) = (e_n s_{\mu^-}, s_\mu)$.]

The following interaction between multiplication and $h^\perp$ is the key to deducing the skew Pieri formula from the usual Pieri formulas.

Lemma 2.8.5. *For any f, g in Λ and any $n \in \mathbb{N}$, one has*

$$f \cdot h_n^\perp(g) = \sum_{k=0}^{n} (-1)^k h_{n-k}^\perp(e_k^\perp(f) \cdot g).$$

Proof. Starting with the right side, first apply Proposition 2.8.2(iv):

$$\begin{aligned}
&\sum_{k=0}^{n} (-1)^k \underbrace{h_{n-k}^\perp(e_k^\perp(f) \cdot g)}_{\substack{= \sum_{j=0}^{n-k} h_j^\perp(e_k^\perp(f)) \cdot h_{n-k-j}^\perp(g) \\ \text{(by Proposition 2.8.2(iv), applied} \\ \text{to } h_{n-k},\ e_k^\perp(f) \text{ and } g \text{ instead of } f,\ a \text{ and } b)}} \\
&= \sum_{k=0}^{n} (-1)^k \sum_{j=0}^{n-k} h_j^\perp(e_k^\perp(f)) \cdot h_{n-k-j}^\perp(g) \\
&= \sum_{j=0}^{n} \sum_{k=0}^{n-j} (-1)^k h_j^\perp(e_k^\perp(f)) \cdot h_{n-k-j}^\perp(g) \\
&= \sum_{j=0}^{n} \sum_{i=0}^{n-j} (-1)^{n-i-j} h_j^\perp(e_{n-i-j}^\perp(f)) \cdot h_i^\perp(g) \qquad \text{(reindexing } i := n-k-j \text{ in the inner sum)} \\
&= \sum_{i=0}^{n} (-1)^{n-i} \left(\sum_{j=0}^{n-i} (-1)^j h_j^\perp(e_{n-i-j}^\perp(f)) \right) \cdot h_i^\perp(g) \\
&= \sum_{i=0}^{n} (-1)^{n-i} \left(\sum_{j=0}^{n-i} (-1)^j e_{n-i-j} h_j \right)^\perp (f) \cdot h_i^\perp(g) \qquad \text{(by Proposition 2.8.2(ii))} \\
&= 1^\perp(f) \cdot h_n^\perp(g) = f \cdot h_n^\perp(g)
\end{aligned}$$

where the second-to-last equality used (2.4.4). □

Proof of Theorem 2.7.3. We prove (2.7.3); the equality (2.7.4) is analogous, swapping $h_i \leftrightarrow e_i$ and swapping the words "vertical" $\leftrightarrow$ "horizontal". For any $f \in \Lambda$, we have

$$\begin{aligned}
\left(s_{\lambda/\mu}, f\right) &= \left(s_\mu^\perp(s_\lambda), f\right) && \text{(by (2.8.2))} \\
&= \left(f, s_\mu^\perp(s_\lambda)\right) && \text{(by symmetry of } (\cdot,\cdot)_\Lambda) \\
&= (s_\mu f, s_\lambda) && \text{(by Proposition 2.8.2(i))} \\
&= (s_\lambda, s_\mu f) && \text{(by symmetry of } (\cdot,\cdot)_\Lambda). \qquad (2.8.5)
\end{aligned}$$

Hence for any g in Λ, one can compute that

$$\begin{aligned}(h_n s_{\lambda/\mu}\ ,\ g) &\overset{\text{Prop. 2.8.2}(i)}{=} (s_{\lambda/\mu}\ ,\ h_n^{\perp} g) \overset{(2.8.5)}{=} (s_\lambda\ ,\ s_\mu \cdot h_n^{\perp} g) \\ &\overset{\text{Lemma 2.8.5}}{=} \sum_{k=0}^{n} (-1)^k (s_\lambda\ ,\ h_{n-k}^{\perp}(e_k^{\perp}(s_\mu)\cdot g)) \\ &\overset{\text{Prop. 2.8.2}(i)}{=} \sum_{k=0}^{n} (-1)^k (h_{n-k} s_\lambda\ , e_k^{\perp}(s_\mu)\cdot g). \end{aligned} \tag{2.8.6}$$

The first Pieri rule in Theorem 2.7.1 lets one rewrite $h_{n-k}s_\lambda = \sum_{\lambda^+} s_{\lambda^+}$, with the sum running through λ^+ for which λ^+/λ is a horizontal $(n-k)$-strip. Meanwhile, (2.8.4) lets one rewrite $e_k^{\perp} s_\mu = \sum_{\mu^-} s_{\mu^-}$, with the sum running through μ^- for which μ/μ^- is a vertical k-strip. Thus the right hand side of (2.8.6) becomes

$$\sum_{k=0}^{n} (-1)^k \left(\sum_{\lambda^+} s_{\lambda^+}\ ,\ \sum_{\mu^-} s_{\mu^-}\cdot g \right) \overset{(2.8.5)}{=} \left(\sum_{k=0}^{n} (-1)^k \sum_{(\lambda^+,\mu^-)} s_{\lambda^+/\mu^-}, g \right)$$

where the sum is over the pairs (λ^+, μ^-) for which λ^+/λ is a horizontal $(n-k)$-strip and μ/μ^- is a vertical k-strip. This proves (2.7.3). □

Exercise 2.8.6. Let $n \in \mathbb{N}$.

(a) For every $k \in \mathbb{N}$, let $p(n,k)$ denote the number of partitions of n of length k. Let $c(n)$ denote the number of *self-conjugate* partitions of n (that is, partitions λ of n satisfying $\lambda^t = \lambda$). Show that

$$(-1)^n c(n) = \sum_{k=0}^{n} (-1)^k p(n,k).$$

(This application of Hopf algebras was found by Aguiar and Lauve, [5, §5.1]. See also [206, Chapter 1, Exercise 22(b)] for an elementary proof.)

(b) For every partition λ, let $C(\lambda)$ denote the number of corner cells of the Ferrers diagram of λ (these are the cells of the Ferrers diagram whose neighbors to the east and to the south both lie outside of the Ferrers diagram). For every partition λ, let $\mu_1(\lambda)$ denote the number of parts of λ equal to 1. Show that

$$\sum_{\lambda \in \mathrm{Par}_n} C(\lambda) = \sum_{\lambda \in \mathrm{Par}_n} \mu_1(\lambda).$$

(This is also due to Stanley.)

Exercise 2.8.7. The goal of this exercise is to prove (2.4.15) using the skewing operators that we have developed.[160] Recall the involution $\omega : \Lambda \to \Lambda$ defined in (2.4.10).

(a) Show that $\omega(p_\lambda) = (-1)^{|\lambda|-\ell(\lambda)} p_\lambda$ for any $\lambda \in \mathrm{Par}$, where $\ell(\lambda)$ denotes the length of the partition λ.

(b) Show that ω is an isometry.

(c) Show that this same map $\omega : \Lambda \to \Lambda$ is a Hopf automorphism.

(d) Prove that $\omega\left(a^{\perp} b\right) = (\omega(a))^{\perp}(\omega(b))$ for every $a \in \Lambda$ and $b \in \Lambda$.

(e) For any partition $\lambda = (\lambda_1, \ldots, \lambda_\ell)$ with length $\ell(\lambda) = \ell$, prove that

$$e_\ell^{\perp} s_\lambda = s_{(\lambda_1 - 1, \lambda_2 - 1, \ldots, \lambda_\ell - 1)}.$$

(f) For any partition $\lambda = (\lambda_1, \lambda_2, \ldots)$, prove that

$$h_{\lambda_1}^{\perp} s_\lambda = s_{(\lambda_2, \lambda_3, \lambda_4, \ldots)}.$$

(g) Prove (2.4.15).

Exercise 2.8.8. Let n be a positive integer. Prove the following:

(a) We have $(e_n, p_n) = (-1)^{n-1}$.

(b) We have $(e_m, p_n) = 0$ for each $m \in \mathbb{N}$ satisfying $m \neq n$.

[160] Make sure not to use the results of Exercise 2.7.11 or Exercise 2.7.12 or Exercise 2.7.14 here, or anything else that relied on (2.4.15), in order to avoid circular reasoning.

(c) We have $e_n^\perp p_n = (-1)^{n-1}$.
(d) We have $e_m^\perp p_n = 0$ for each positive integer m satisfying $m \neq n$.

2.9. **Assorted exercises on symmetric functions.** Over a hundred exercises on symmetric functions are collected in Stanley's [206, chapter 7], and even more (but without any hints or references) on his website[161]. Further sources for results related to symmetric functions are Macdonald's work, including his monograph [142] and his expository [143]. In this section, we gather a few exercises that are not too difficult to handle with the material given above.

Exercise 2.9.1. (a) Let $m \in \mathbb{Z}$. Prove that, for every $f \in \Lambda$, the infinite sum $\sum_{i \in \mathbb{N}} (-1)^i h_{m+i} e_i^\perp f$ is convergent in the discrete topology (i.e., all but finitely many addends of this sum are zero). Hence, we can define a map $\mathbf{B}_m : \Lambda \to \Lambda$ by setting

$$\mathbf{B}_m(f) = \sum_{i \in \mathbb{N}} (-1)^i h_{m+i} e_i^\perp f \qquad \text{for all } f \in \Lambda.$$

Show that this map $\mathbf{B}_m$ is $\mathbf{k}$-linear.

(b) Let $\lambda = (\lambda_1, \lambda_2, \lambda_3, \ldots)$ be a partition, and let $m \in \mathbb{Z}$ be such that $m \geq \lambda_1$. Show that

$$\sum_{i \in \mathbb{N}} (-1)^i h_{m+i} e_i^\perp s_\lambda = s_{(m, \lambda_1, \lambda_2, \lambda_3, \ldots)}.$$

(c) Let $n \in \mathbb{N}$. For every n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$, we define an element $\overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} \in \Lambda$ by

$$\overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} = \det\left(\left(h_{\alpha_i - i + j} \right)_{i,j=1,2,\ldots,n} \right).$$

Show that

$$s_\lambda = \overline{s}_{(\lambda_1, \lambda_2, \ldots, \lambda_n)} \tag{2.9.1}$$

for every partition $\lambda = (\lambda_1, \lambda_2, \lambda_3, \ldots)$ having at most n parts[162].

Furthermore, show that for every n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$, the symmetric function $\overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)}$ either is 0 or equals $\pm s_\nu$ for some partition ν having at most n parts.

Finally, show that for any n-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$ and $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, we have

$$\overline{s}^\perp_{(\beta_1, \beta_2, \ldots, \beta_n)} \overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} = \det\left(\left(h_{\alpha_i - \beta_j - i + j} \right)_{i,j=1,2,\ldots,n} \right). \tag{2.9.2}$$

(d) For every $n \in \mathbb{N}$, every $m \in \mathbb{Z}$ and every n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$, prove that

$$\sum_{i \in \mathbb{N}} (-1)^i h_{m+i} e_i^\perp \overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} = \overline{s}_{(m, \alpha_1, \alpha_2, \ldots, \alpha_n)}, \tag{2.9.3}$$

where we are using the notations of Exercise 2.9.1(c).

(e) For every $n \in \mathbb{N}$ and every n-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}^n$, prove that

$$\overline{s}_{(\alpha_1, \alpha_2, \ldots, \alpha_n)} = \left(\mathbf{B}_{\alpha_1} \circ \mathbf{B}_{\alpha_2} \circ \cdots \circ \mathbf{B}_{\alpha_n} \right)(1),$$

where we are using the notations of Exercise 2.9.1(c) and Exercise 2.9.1(a).

(f) For every $m \in \mathbb{Z}$ and every positive integer n, prove that $\mathbf{B}_m(p_n) = h_m p_n - h_{m+n}$. Here, we are using the notations of Exercise 2.9.1(a).

Remark 2.9.2. The map $\mathbf{B}_m$ defined in Exercise 2.9.1(a) is the so-called *m-th Bernstein creation operator*; it appears in Zelevinsky [227, §4.20(a)] and has been introduced by J.N. Bernstein, who found the result of Exercise 2.9.1(b). It is called a "Schur row adder" in [74]. Exercise 2.9.1(e) appears in Berg/Bergeron/Saliola/Serrano/Zabrocki [17, Theorem 2.3], where it is used as a prototype for defining *noncommutative* analogues of Schur functions, the so-called *immaculate functions*. The particular case of Exercise 2.9.1(e) for $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a partition of length n (a restatement of Exercise 2.9.1(b)) is proven in [142, §I.5, example 29].

[161] http://math.mit.edu/~rstan/ec/ch7supp.pdf
[162] Recall that a *part* of a partition means a nonzero entry of the partition.

Exercise 2.9.3. (a) Prove that there exists a unique family $(x_n)_{n\geq 1}$ of elements of Λ such that

$$H(t) = \prod_{n=1}^{\infty} (1 - x_n t^n)^{-1}.$$

Denote this family $(x_n)_{n\geq 1}$ by $(w_n)_{n\geq 1}$. For instance,

$$w_1 = s_{(1)}, \qquad w_2 = -s_{(1,1)}, \qquad w_3 = -s_{(2,1)},$$
$$w_4 = -s_{(1,1,1,1)} - s_{(2,1,1)} - s_{(2,2)} - s_{(3,1)}, \qquad w_5 = -s_{(2,1,1,1)} - s_{(2,2,1)} - s_{(3,1,1)} - s_{(3,2)} - s_{(4,1)}.$$

(b) Show that w_n is homogeneous of degree n for every positive integer n.

(c) For every partition λ, define $w_\lambda \in \Lambda$ by $w_\lambda = w_{\lambda_1} w_{\lambda_2} \cdots w_{\lambda_\ell}$ (where $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ with $\ell = \ell(\lambda)$). Notice that w_λ is homogeneous of degree $|\lambda|$. Prove that $\sum_{\lambda \in \mathrm{Par}_n} w_\lambda = h_n$ for every $n \in \mathbb{N}$.

(d) Show that $\{w_\lambda\}_{\lambda \in \mathrm{Par}}$ is a $\mathbf{k}$-basis of Λ. (This basis is called the *Witt basis*[163]; it is studied in [90, §9-§10].[164])

(e) Prove that $p_n = \sum_{d|n} d w_d^{n/d}$ for every positive integer n. (Here, the summation sign $\sum_{d|n}$ means a sum over all positive divisors d of n.)

(f) We are going to show that $-w_n$ is a sum of Schur functions (possibly with repetitions, but without signs!) for every $n \geq 2$. (For $n = 1$, the opposite is true: w_1 is a single Schur function.) This proof goes back to Doran [55][165].

For any positive integers n and k, define $f_{n,k} \in \Lambda$ by $f_{n,k} = \sum_{\substack{\lambda \in \mathrm{Par}_n, \\ \min \lambda \geq k}} w_\lambda$, where $\min \lambda$ denotes the smallest part[166] of λ. Show that

$$-f_{n,k} = s_{(n-1,1)} + \sum_{i=2}^{k-1} f_{i,i} f_{n-i,i} \qquad \text{for every } n \geq k \geq 2.$$

Conclude that $-f_{n,k}$ is a sum of Schur functions for every $n \in \mathbb{N}$ and $k \geq 2$. Conclude that $-w_n$ is a sum of Schur functions for every $n \geq 2$.

(g) For every partition λ, define $r_\lambda \in \Lambda$ by $r_\lambda = \prod_{i \geq 1} h_{v_i}\left(x_1^i, x_2^i, x_3^i, \ldots\right)$, where v_i is the number of occurrences of i in λ. Show that $\sum_{\lambda \in \mathrm{Par}} w_\lambda(\mathbf{x}) r_\lambda(\mathbf{y}) = \prod_{i,j=1}^{\infty} (1 - x_i y_j)^{-1}$.

(h) Show that $\{r_\lambda\}_{\lambda \in \mathrm{Par}}$ and $\{w_\lambda\}_{\lambda \in \mathrm{Par}}$ are dual bases of Λ.

Exercise 2.9.4. For this exercise, set $\mathbf{k} = \mathbb{Z}$, and consider $\Lambda = \Lambda_{\mathbb{Z}}$ as a subring of $\Lambda_{\mathbb{Q}}$. Also, consider $\Lambda \otimes_{\mathbb{Z}} \Lambda$ as a subring of $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}$. [167] Recall that the family $(p_n)_{n\geq 1}$ generates the $\mathbb{Q}$-algebra $\Lambda_{\mathbb{Q}}$, but does not generate the $\mathbb{Z}$-algebra Λ.

(a) Define a $\mathbb{Q}$-linear map $Z : \Lambda_{\mathbb{Q}} \to \Lambda_{\mathbb{Q}}$ by setting

$$Z(p_\lambda) = z_\lambda p_\lambda \qquad \text{for every partition } \lambda,$$

where z_λ is defined as in Proposition 2.5.15.[168] Show that $Z(\Lambda) \subset \Lambda$.

---

[163] This is due to its relation with Witt vectors in the appropriate sense. Most of the work on this basis has been done by Reutenauer and Hazewinkel.

[164] It also implicitly appears in [12, §5]. Indeed, the q_n of [12] are our w_n (for $\mathbf{k} = R$).

[165] See also Stanley [206, Exercise 7.46].

[166] Recall that a *part* of a partition means a nonzero entry of the partition.

[167] Here is how this works: We have $\Lambda_{\mathbb{Q}} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$. But fundamental properties of tensor products yield

$$\mathbb{Q} \otimes_{\mathbb{Z}} (\Lambda \otimes_{\mathbb{Z}} \Lambda) \cong \underbrace{(\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda)}_{\cong \Lambda_{\mathbb{Q}}} \otimes_{\mathbb{Q}} \underbrace{(\mathbb{Q} \otimes_{\mathbb{Z}} \Lambda)}_{\cong \Lambda_{\mathbb{Q}}} \cong \Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}} \tag{2.9.4}$$

as $\mathbb{Q}$-algebras. But $\Lambda \otimes_{\mathbb{Z}} \Lambda$ is a free $\mathbb{Z}$-module (since Λ is a free $\mathbb{Z}$-module), and so the canonical ring homomorphism $\Lambda \otimes_{\mathbb{Z}} \Lambda \to \mathbb{Q} \otimes_{\mathbb{Z}} (\Lambda \otimes_{\mathbb{Z}} \Lambda)$ sending every u to $1_{\mathbb{Q}} \otimes_{\mathbb{Z}} u$ is injective. Composing this ring homomorphism with the $\mathbb{Q}$-algebra isomorphism of (2.9.4) gives an injective ring homomorphism $\Lambda \otimes_{\mathbb{Z}} \Lambda \to \Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}$. We use this latter homomorphism to identify $\Lambda \otimes_{\mathbb{Z}} \Lambda$ with a subring of $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}$.

[168] This is well-defined, since $(p_\lambda)_{\lambda \in \mathrm{Par}}$ is a $\mathbb{Q}$-module basis of $\Lambda_{\mathbb{Q}}$.

(b) Define a $\mathbb{Q}$-algebra homomorphism $\Delta_\times : \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q} \otimes_\mathbb{Q} \Lambda_\mathbb{Q}$ by setting

$$\Delta_\times(p_n) = p_n \otimes p_n \qquad \text{for every positive integer } n.$$

[169] Show that $\Delta_\times(\Lambda) \subset \Lambda \otimes_\mathbb{Z} \Lambda$.

(c) Let $r \in \mathbb{Z}$. Define a $\mathbb{Q}$-algebra homomorphism $\epsilon_r : \Lambda_\mathbb{Q} \to \mathbb{Q}$ by setting

$$\epsilon_r(p_n) = r \qquad \text{for every positive integer } n.$$

[170] Show that $\epsilon_r(\Lambda) \subset \mathbb{Z}$.

(d) Let $r \in \mathbb{Z}$. Define a $\mathbb{Q}$-algebra homomorphism $\mathbf{i}_r : \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q}$ by setting

$$\mathbf{i}_r(p_n) = rp_n \qquad \text{for every positive integer } n.$$

[171] Show that $\mathbf{i}_r(\Lambda) \subset \Lambda$.

(e) Define a $\mathbb{Q}$-linear map $\mathrm{Sq} : \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q}$ by setting

$$\mathrm{Sq}(p_\lambda) = p_\lambda^2 \qquad \text{for every partition } \lambda.$$

[172] Show that $\mathrm{Sq}(\Lambda) \subset \Lambda$.

(f) Let $r \in \mathbb{Z}$. Define a $\mathbb{Q}$-algebra homomorphism $\Delta_r : \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q} \otimes_\mathbb{Q} \Lambda_\mathbb{Q}$ by setting

$$\Delta_r(p_n) = \sum_{i=1}^{n-1} \binom{n}{i} p_i \otimes p_{n-i} + r \otimes p_n + p_n \otimes r \qquad \text{for every positive integer } n.$$

[173] Show that $\Delta_r(\Lambda) \subset \Lambda \otimes_\mathbb{Z} \Lambda$.

(g) Consider the map $\Delta_\times$ introduced in Exercise 2.9.4(b) and the map ϵ_1 introduced in Exercise 2.9.4(c). Show that the $\mathbb{Q}$-algebra $\Lambda_\mathbb{Q}$, endowed with the comultiplication $\Delta_\times$ and the counit ϵ_1, becomes a cocommutative $\mathbb{Q}$-bialgebra.[174]

(h) Define a $\mathbb{Q}$-bilinear map $* : \Lambda_\mathbb{Q} \times \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q}$, which will be written in infix notation (that is, we will write $a * b$ instead of $*(a, b)$), by setting

$$p_\lambda * p_\mu = \delta_{\lambda,\mu} z_\lambda p_\lambda \qquad \text{for any partitions } \lambda \text{ and } \mu$$

(where z_λ is defined as in Proposition 2.5.15). [175] Show that $f * g \in \Lambda$ for any $f \in \Lambda$ and $g \in \Lambda$.

(i) Show that $\epsilon_1(f) = f(1)$ for every $f \in \Lambda_\mathbb{Q}$ (where we are using the notation ϵ_r defined in Exercise 2.9.4(c)).

[**Hint:**

- For (b), show that, for every $f \in \Lambda_\mathbb{Q}$, the tensor $\Delta_\times(f)$ is the preimage of $f\left((x_i y_j)_{(i,j)\in\{1,2,3,\ldots\}^2}\right) = f(x_1y_1, x_1y_2, x_1y_3, \ldots, x_2y_1, x_2y_2, x_2y_3, \ldots, \ldots) \in \mathbb{Q}[[\mathbf{x}, \mathbf{y}]]$ under the canonical injection $\Lambda_\mathbb{Q} \otimes_\mathbb{Q} \Lambda_\mathbb{Q} \to \mathbb{Q}[[\mathbf{x}, \mathbf{y}]]$ which maps every $f \otimes g$ to $f(\mathbf{x})\, g(\mathbf{y})$. (This requires making sure that the evaluation $f\left((x_i y_j)_{(i,j)\in\{1,2,3,\ldots\}^2}\right)$ is well-defined to begin with, i.e., converges as a formal power series.)
  For an alternative solution to (b), compute $\Delta_\times(h_n)$ or $\Delta_\times(e_n)$.
- For (c), compute $\epsilon_r(e_n)$ or $\epsilon_r(h_n)$.
- Reduce (d) to (b) and (c) using Exercise 1.3.6.
- Reduce (e) to (b).
- (f) is the hardest part. It is tempting to try and interpret the definition of Δ_r as a convoluted way of saying that $\Delta_r(f)$ is the preimage of $f\left((x_i + y_j)_{(i,j)\in\{1,2,3,\ldots\}^2}\right)$ under the canonical injection $\Lambda_\mathbb{Q} \otimes_\mathbb{Q} \Lambda_\mathbb{Q} \to \mathbb{Q}[[\mathbf{x}, \mathbf{y}]]$ which maps every $f \otimes g$ to $f(\mathbf{x})\, g(\mathbf{y})$. However, this does not make sense since the evaluation $f\left((x_i + y_j)_{(i,j)\in\{1,2,3,\ldots\}^2}\right)$ is (in general) not well-defined[176] (and even if it was, it would fail to explain the r). So we need to get down to finitely many variables. For every $N \in \mathbb{N}$, define a

[169] This is well-defined, since the family $(p_n)_{n\geq 1}$ generates the $\mathbb{Q}$-algebra $\Lambda_\mathbb{Q}$ and is algebraically independent.
[170] This is well-defined, since the family $(p_n)_{n\geq 1}$ generates the $\mathbb{Q}$-algebra $\Lambda_\mathbb{Q}$ and is algebraically independent.
[171] This is well-defined, since the family $(p_n)_{n\geq 1}$ generates the $\mathbb{Q}$-algebra $\Lambda_\mathbb{Q}$ and is algebraically independent.
[172] This is well-defined, since $(p_\lambda)_{\lambda\in\mathrm{Par}}$ is a $\mathbb{Q}$-module basis of $\Lambda_\mathbb{Q}$.
[173] This is well-defined, since the family $(p_n)_{n\geq 1}$ generates the $\mathbb{Q}$-algebra $\Lambda_\mathbb{Q}$ and is algebraically independent.
[174] But unlike $\Lambda_\mathbb{Q}$ with the usual coalgebra structure, it is neither graded nor a Hopf algebra.
[175] This is well-defined, since $(p_\lambda)_{\lambda\in\mathrm{Par}}$ is a $\mathbb{Q}$-module basis of $\Lambda_\mathbb{Q}$.
[176] e.g., it involves summing infinitely many x_1's if $f = e_1$

$\mathbb{Q}$-algebra homomorphism $\mathcal{E}_N : \Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}} \to \mathbb{Q}[x_1, x_2, \ldots, x_N, y_1, y_2, \ldots, y_N]$ by sending each $f \otimes g$ to $f(x_1, x_2, \ldots, x_N)\, g(y_1, y_2, \ldots, y_N)$. Show that $\Delta_N(\Lambda) \subset \mathcal{E}_N^{-1}(\mathbb{Z}[x_1, x_2, \ldots, x_N, y_1, y_2, \ldots, y_N])$. This shows that, at least, the coefficients of $\Delta_r(f)$ in front of the $m_\lambda \otimes m_\mu$ with $\ell(\lambda) \leq r$ and $\ell(\mu) \leq r$ (in the $\mathbb{Q}$-basis $(m_\lambda \otimes m_\mu)_{\lambda,\mu \in \mathrm{Par}}$ of $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}$) are integral for $f \in \Lambda$. Of course, we want all coefficients. Show that $\Delta_a = \Delta_b \star \left(\Delta_{\Lambda_{\mathbb{Q}}} \circ \mathbf{i}_{a-b}\right)$ in $\mathrm{Hom}(\Lambda_{\mathbb{Q}}, \Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}})$ for any integers a and b. This allows "moving" the r. This approach to (f) was partly suggested to the first author by Richard Stanley.

- For (h), notice that Definition 3.1.1(b) (below) allows us to construct a bilinear form $(\cdot,\cdot)_{\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}} : (\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}) \times (\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}) \to \mathbb{Q}$ from the Hall inner product $(\cdot,\cdot) : \Lambda_{\mathbb{Q}} \times \Lambda_{\mathbb{Q}} \to \mathbb{Q}$. Show that

$$(a * b, c) = (a \otimes b, \Delta_\times(c))_{\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Q}} \Lambda_{\mathbb{Q}}} \qquad \text{for all } a, b, c \in \Lambda_{\mathbb{Q}}, \tag{2.9.5}$$

and then use (b).

]

Remark 2.9.5. The map $\Delta_\times$ defined in Exercise 2.9.4(b) is known as the *internal comultiplication* (or *Kronecker comultiplication*) on $\Lambda_{\mathbb{Q}}$. Unlike the standard comultiplication $\Delta_{\Lambda_{\mathbb{Q}}}$, it is not a graded map, but rather sends every homogeneous component $(\Lambda_{\mathbb{Q}})_n$ into $(\Lambda_{\mathbb{Q}})_n \otimes (\Lambda_{\mathbb{Q}})_n$. The bilinear map $*$ from Exercise 2.9.4(h) is the so-called *internal multiplication* (or *Kronecker multiplication*), and is similarly not graded but rather takes $(\Lambda_{\mathbb{Q}})_n \times (\Lambda_{\mathbb{Q}})_m$ to $(\Lambda_{\mathbb{Q}})_n$ if $n = m$ and to 0 otherwise.

The analogy between the two internal structures is not perfect: While we saw in Exercise 2.9.4(g) how the internal comultiplication yields another bialgebra structure on $\Lambda_{\mathbb{Q}}$, it is not true that the internal multiplication (combined with the usual coalgebra structure of $\Lambda_{\mathbb{Q}}$) forms a bialgebra structure as well. What is missing is a multiplicative unity; if we would take the closure of $\Lambda_{\mathbb{Q}}$ with respect to the grading, then $1 + h_1 + h_2 + h_3 + \cdots$ would be such a unity.

The structure constants of the internal comultiplication on the Schur basis $(s_\lambda)_{\lambda \in \mathrm{Par}}$ are equal to the structure constants of the internal multiplication on the Schur basis[177], and are commonly referred to as the *Kronecker coefficients*. They are known to be nonnegative integers (this follows from Exercise 4.4.8(c)[178]), but no combinatorial proof is known for their nonnegativity. Combinatorial interpretations for these coefficients akin to the Littlewood-Richardson rule have been found only in special cases (cf., e.g., [183] and [23] and [132]).

The map Δ_r of Exercise 2.9.4(f) also has some classical theory behind it, relating to Chern classes of tensor products ([151], [142, §I.4, example 5]).

Parts (b), (c), (d), (e) and (f) of Exercise 2.9.4 are instances of a general phenomenon: Many $\mathbb{Z}$-algebra homomorphisms $\Lambda \to A$ (with A a commutative ring, usually torsionfree) are easiest to define by first defining a $\mathbb{Q}$-algebra homomorphism $\Lambda_{\mathbb{Q}} \to A \otimes \mathbb{Q}$ and then showing that this homomorphism restricts to a $\mathbb{Z}$-algebra homomorphism $\Lambda \to A$. One might ask for general criteria when this is possible; specifically, for what choices of $(b_n)_{n \geq 1} \in A^{\{1,2,3,\ldots\}}$ does there exist a $\mathbb{Z}$-algebra homomorphism $\Lambda \to A$ sending the p_n to b_n ? Such choices are called *ghost-Witt vectors* in Hazewinkel [90], and we can give various equivalent conditions for a family $(b_n)_{n \geq 1}$ to be a ghost-Witt vector:

Exercise 2.9.6. Let A be a commutative ring.

For every $n \in \{1, 2, 3, \ldots\}$, let $\varphi_n : A \to A$ be a ring endomorphism of A. Assume that the following properties hold:

- We have $\varphi_n \circ \varphi_m = \varphi_{nm}$ for any two positive integers n and m.
- We have $\varphi_1 = \mathrm{id}$.
- We have $\varphi_p(a) \equiv a^p \bmod pA$ for every $a \in A$ and every prime number p.

(For example, when $A = \mathbb{Z}$, one can set $\varphi_n = \mathrm{id}$ for all n; this simplifies the exercise somewhat. More generally, setting $\varphi_n = \mathrm{id}$ works whenever A is a binomial ring[179]. However, the results of this exercise are at their most useful when A is a multivariate polynomial ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]$ over $\mathbb{Z}$ and the homomorphism φ_n sends every $P \in A$ to $P(x_1^n, x_2^n, x_3^n, \ldots)$.)

[177] This can be obtained, e.g., from (2.9.5).

[178] Their integrality can also be easily deduced from Exercise 2.9.4(b).

[179] A *binomial ring* is defined to be a torsionfree (as an additive group) commutative ring A which has one of the following equivalent properties:

Let μ denote the *number-theoretic Möbius function*; this is the function $\{1,2,3,\ldots\} \to \mathbb{Z}$ defined by

$$\mu(m) = \begin{cases} 0, & \text{if } m \text{ is not squarefree;} \\ (-1)^{(\text{number of prime factors of } m)}, & \text{if } m \text{ is squarefree} \end{cases} \qquad \text{for every positive integer } m.$$

Let ϕ denote the *Euler totient function*; this is the function $\{1,2,3,\ldots\} \to \mathbb{N}$ which sends every positive integer m to the number of elements of $\{1,2,\ldots,m\}$ coprime to m.

Let $(b_n)_{n\geq 1} \in A^{\{1,2,3,\ldots\}}$ be a family of elements of A. Prove that the following seven assertions are equivalent:

- *Assertion $\mathcal{C}$:* For every positive integer n and every prime factor p of n, we have
$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod p^{v_p(n)} A.$$
Here, $v_p(n)$ denotes the exponent of p in the prime factorization of n.
- *Assertion $\mathcal{D}$:* There exists a family $(\alpha_n)_{n\geq 1} \in A^{\{1,2,3,\ldots\}}$ of elements of A such that every positive integer n satisfies
$$b_n = \sum_{d|n} d\alpha_d^{n/d}.$$
[180]
- *Assertion $\mathcal{E}$:* There exists a family $(\beta_n)_{n\geq 1} \in A^{\{1,2,3,\ldots\}}$ of elements of A such that every positive integer n satisfies
$$b_n = \sum_{d|n} d\varphi_{n/d}(\beta_d).$$
- *Assertion $\mathcal{F}$:* Every positive integer n satisfies
$$\sum_{d|n} \mu(d)\, \varphi_d\left(b_{n/d}\right) \in nA.$$
- *Assertion $\mathcal{G}$:* Every positive integer n satisfies
$$\sum_{d|n} \phi(d)\, \varphi_d\left(b_{n/d}\right) \in nA.$$
- *Assertion $\mathcal{H}$:* Every positive integer n satisfies
$$\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA.$$
- *Assertion $\mathcal{J}$:* There exists a ring homomorphism $\Lambda_{\mathbb{Z}} \to A$ which, for every positive integer n, sends p_n to b_n.

- For every $n \in \mathbb{N}$ and $a \in A$, we have $a(a-1)\cdots(a-n+1) \in n! \cdot A$. (That is, binomial coefficients $\binom{a}{n}$ with $a \in A$ and $n \in \mathbb{N}$ are defined in A.)
- We have $a^p \equiv a \bmod pA$ for every $a \in A$ and every prime number p.

See [226] and the references therein for studies of these rings. It is not hard to check that $\mathbb{Z}$ and every localization of $\mathbb{Z}$ are binomial rings, and so is any commutative $\mathbb{Q}$-algebra as well as the ring

$$\{P \in \mathbb{Q}[X] \mid P(n) \in \mathbb{Z} \text{ for every } n \in \mathbb{Z}\}$$

(but not the ring $\mathbb{Z}[X]$ itself).

[180] Here and in the following, summations of the form $\sum_{d|n}$ range over all **positive** divisors of n.

[**Hint:** The following identities hold for every positive integer n:

$$\sum_{d\mid n}\phi\left(d\right)=n; \tag{2.9.6}$$

$$\sum_{d\mid n}\mu\left(d\right)=\delta_{n,1}; \tag{2.9.7}$$

$$\sum_{d\mid n}\mu\left(d\right)\frac{n}{d}=\phi\left(n\right); \tag{2.9.8}$$

$$\sum_{d\mid n}d\mu\left(d\right)\phi\left(\frac{n}{d}\right)=\mu\left(n\right). \tag{2.9.9}$$

Furthermore, the following simple lemma is useful: If k is a positive integer, and if $p\in\mathbb{N}$, $a\in A$ and $b\in A$ are such that $a\equiv b \bmod p^k A$, then $a^{p^\ell}\equiv b^{p^\ell} \bmod p^{k+\ell}A$ for every $\ell\in\mathbb{N}$.]

Remark 2.9.7. Much of Exercise 2.9.6 is folklore, but it is hard to pinpoint concrete appearances in literature. The equivalence $\mathcal{C}\iff\mathcal{D}$ appears in Hesselholt [95, Lemma 1] and [96, Lemma 1.1] (in slightly greater generality), where it is referred to as Dwork's lemma and used in the construction of the Witt vector functor. This equivalence is also [90, Lemma 9.93]. The equivalence $\mathcal{D}\iff\mathcal{F}\iff\mathcal{G}\iff\mathcal{H}$ in the case $A=\mathbb{Z}$ is [57, Corollary on p. 10], where it is put into the context of Burnside rings and necklace counting. The equivalence $\mathcal{C}\iff\mathcal{F}$ for finite families $\left(b_n\right)_{n\in\{1,2,\ldots,m\}}$ in lieu of $\left(b_n\right)_{n\geq 1}$ is [206, Exercise 5.2 **a**]. One of the likely oldest relevant sources is Schur's [195], which proves the equivalence $\mathcal{C}\iff\mathcal{D}\iff\mathcal{F}$ for finite families $\left(b_n\right)_{n\in\{1,2,\ldots,m\}}$, as well as a "finite version" of $\mathcal{C}\iff\mathcal{J}$ (Schur did not have Λ, but was working with actual power sums of roots of polynomials).

Exercise 2.9.8. Let A denote the ring $\mathbb{Z}$. For every $n\in\{1,2,3,\ldots\}$, let φ_n denote the identity endomorphism id of A. Prove that the seven equivalent assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$ and $\mathcal{J}$ of Exercise 2.9.6 are satisfied for each of the following families $\left(b_n\right)_{n\geq 1}\in\mathbb{Z}^{\{1,2,3,\ldots\}}$:

- the family $\left(b_n\right)_{n\geq 1}=\left(q^n\right)_{n\geq 1}$, where q is a given integer.
- the family $\left(b_n\right)_{n\geq 1}=\left(q\right)_{n\geq 1}$, where q is a given integer.
- the family $\left(b_n\right)_{n\geq 1}=\left(\binom{qn}{rn}\right)_{n\geq 1}$, where $r\in\mathbb{Q}$ and $q\in\mathbb{Z}$ are given. (Here, a binomial coefficient $\binom{a}{b}$ has to be interpreted as 0 when $b\notin\mathbb{N}$.)
- the family $\left(b_n\right)_{n\geq 1}=\left(\binom{qn-1}{rn-1}\right)_{n\geq 1}$, where $r\in\mathbb{Z}$ and $q\in\mathbb{Z}$ are given.

Exercise 2.9.9. For every $n\in\{1,2,3,\ldots\}$, define a map $\mathbf{f}_n:\Lambda\to\Lambda$ by setting

$$\mathbf{f}_n\left(a\right)=a\left(x_1^n,x_2^n,x_3^n,\ldots\right)\qquad\text{for every } a\in\Lambda.$$

(So what $\mathbf{f}_n$ does to a symmetric function is replacing all variables $x_1,x_2,x_3,\ldots$ by their n-th powers.)

(a) Show that $\mathbf{f}_n:\Lambda\to\Lambda$ is a $\mathbf{k}$-algebra homomorphism for every $n\in\{1,2,3,\ldots\}$.
(b) Show that $\mathbf{f}_n\circ\mathbf{f}_m=\mathbf{f}_{nm}$ for any two positive integers n and m.
(c) Show that $\mathbf{f}_1=\mathrm{id}$.
(d) Prove that $\mathbf{f}_n:\Lambda\to\Lambda$ is a Hopf algebra homomorphism for every $n\in\{1,2,3,\ldots\}$.
(e) Prove that $\mathbf{f}_2\left(h_m\right)=\sum_{i=0}^{2m}\left(-1\right)^i h_i h_{2m-i}$ for every $m\in\mathbb{N}$.
(f) Assume that $\mathbf{k}=\mathbb{Z}$. Prove that $\mathbf{f}_p\left(a\right)\equiv a^p \bmod p\Lambda$ for every $a\in\Lambda$ and every prime number p.
(g) Use Exercise 2.9.6 to obtain new solutions to parts (b), (c), (d), (e) and (f) of Exercise 2.9.4.

The maps $\mathbf{f}_n$ constructed in Exercise 2.9.9 are known as the *Frobenius endomorphisms* of Λ. They are a (deceptively) simple particular case of the notion of *plethysm* ([206, Chapter 7, Appendix 2] and [142, Section I.8]), and are often used as intermediate steps in computing more complicated plethysms[181].

[181] In the notations of [206, (A2.160)], the value $\mathbf{f}_n\left(a\right)$ for an $a\in\Lambda$ can be written as $a\left[p_n\right]$ or (when $\mathbf{k}=\mathbb{Z}$) as $p_n\left[a\right]$.

Exercise 2.9.10. For every $n \in \{1,2,3,\ldots\}$, define a $\mathbf{k}$-algebra homomorphism $\mathbf{v}_n : \Lambda \to \Lambda$ by

$$\mathbf{v}_n(h_m) = \begin{cases} h_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases} \qquad \text{for every positive integer } m$$

[182].

(a) Show that any positive integers n and m satisfy

$$\mathbf{v}_n(p_m) = \begin{cases} np_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases}.$$

(b) Show that any positive integers n and m satisfy

$$\mathbf{v}_n(e_m) = \begin{cases} (-1)^{m-m/n} e_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases}.$$

(c) Prove that $\mathbf{v}_n \circ \mathbf{v}_m = \mathbf{v}_{nm}$ for any two positive integers n and m.
(d) Prove that $\mathbf{v}_1 = \mathrm{id}$.
(e) Prove that $\mathbf{v}_n : \Lambda \to \Lambda$ is a Hopf algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.

Now, consider also the maps $\mathbf{f}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.9. Fix a positive integer n.

(f) Prove that the maps $\mathbf{f}_n : \Lambda \to \Lambda$ and $\mathbf{v}_n : \Lambda \to \Lambda$ are adjoint with respect to the Hall inner product on Λ.
(g) Show that $\mathbf{v}_n \circ \mathbf{f}_n = \mathrm{id}_\Lambda^{\star n}$.
(h) Prove that $\mathbf{f}_n \circ \mathbf{v}_m = \mathbf{v}_m \circ \mathbf{f}_n$ whenever m is a positive integer coprime to n.

Finally, recall the $w_m \in \Lambda$ defined in Exercise 2.9.3.

(i) Show that any positive integer m satisfies

$$\mathbf{v}_n(w_m) = \begin{cases} w_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases}.$$

The homomorphisms $\mathbf{v}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.10 are called the *Verschiebung endomorphisms* of Λ; this name comes from German, where "Verschiebung" means "shift". This terminology, as well as that of Frobenius endomorphisms, originates in the theory of Witt vectors, and the connection between the Frobenius and Verschiebung endomorphisms of Λ and the identically named operators on Witt vectors is elucidated in [90, Chapter 13][183].

Exercise 2.9.11. Fix $n \in \mathbb{N}$. For any n-tuple $w = (w_1, w_2, \ldots, w_n)$ of integers, define the *descent set* $\mathrm{Des}(w)$ of w to be the set $\{i \in \{1,2,\ldots,n-1\} : w_i > w_{i+1}\}$.

(a) We say that an n-tuple $(w_1, w_2, \ldots, w_n)$ is *Smirnov* if every $i \in \{1,2,\ldots,n-1\}$ satisfies $w_i \neq w_{i+1}$.
Fix $k \in \mathbb{N}$, and let $X_{n,k} \in \mathbf{k}[[\mathbf{x}]]$ denote the sum of the monomials $x_{w_1} x_{w_2} \cdots x_{w_n}$ over all Smirnov n-tuples $w = (w_1, w_2, \ldots, w_n) \in \{1,2,3,\ldots\}^n$ satisfying $|\mathrm{Des}(w)| = k$. Prove that $X_{n,k} \in \Lambda$.
(b) For any n-tuple $w = (w_1, w_2, \ldots, w_n)$, define the *stagnation set* $\mathrm{Stag}(w)$ of w to be the set $\{i \in \{1,2,\ldots,n-1\} : w_i = w_{i+1}\}$. (Thus, an n-tuple is Smirnov if and only if its stagnation set is empty.)
For any $d \in \mathbb{N}$ and $s \in \mathbb{N}$, define a power series $X_{n,d,s} \in \mathbf{k}[[\mathbf{x}]]$ as the sum of the monomials $x_{w_1} x_{w_2} \cdots x_{w_n}$ over all n-tuples $w = (w_1, w_2, \ldots, w_n) \in \{1,2,3,\ldots\}^n$ satisfying $|\mathrm{Des}(w)| = d$ and $|\mathrm{Stag}(w)| = s$. Prove that $X_{n,d,s} \in \Lambda$ for any nonnegative integers d and s.

[182] This is well-defined, since the family $(h_m)_{m \geq 1}$ generates the $\mathbf{k}$-algebra Λ and is algebraically independent.
[183] which is also where most of the statements of Exercises 2.9.9 and 2.9.10 come from

(c) Assume that n is positive. For any $d \in \mathbb{N}$ and $s \in \mathbb{N}$, define three further power series $U_{n,d,s}$, $V_{n,d,s}$ and $W_{n,d,s}$ in $\mathbf{k}[[\mathbf{x}]]$ by the following formulas:

$$U_{n,d,s} = \sum_{\substack{w=(w_1,w_2,\ldots,w_n)\in\{1,2,3,\ldots\}^n; \\ |\mathrm{Des}(w)|=d;\ |\mathrm{Stag}(w)|=s; \\ w_1<w_n}} x_{w_1}x_{w_2}\cdots x_{w_n}; \tag{2.9.10}$$

$$V_{n,d,s} = \sum_{\substack{w=(w_1,w_2,\ldots,w_n)\in\{1,2,3,\ldots\}^n; \\ |\mathrm{Des}(w)|=d;\ |\mathrm{Stag}(w)|=s; \\ w_1=w_n}} x_{w_1}x_{w_2}\cdots x_{w_n}; \tag{2.9.11}$$

$$W_{n,d,s} = \sum_{\substack{w=(w_1,w_2,\ldots,w_n)\in\{1,2,3,\ldots\}^n; \\ |\mathrm{Des}(w)|=d;\ |\mathrm{Stag}(w)|=s; \\ w_1>w_n}} x_{w_1}x_{w_2}\cdots x_{w_n}. \tag{2.9.12}$$

Prove that these three power series $U_{n,d,s}$, $V_{n,d,s}$ and $W_{n,d,s}$ belong to Λ.

Remark 2.9.12. The function $X_{n,k}$ in Exercise 2.9.11(a) is a simple example ([199, Example 2.5, Theorem C.3]) of a chromatic quasisymmetric function that happens to be symmetric. See Shareshian/Wachs [199] for more general criteria for such functions to be symmetric, as well as deeper results. For example, [199, Theorem 6.3] gives an expansion for a wide class of chromatic quasisymmetric functions in the Schur basis of Λ, which, in particular, shows that our $X_{n,k}$ satisfies

$$X_{n,k} = \sum_{\lambda\in\mathrm{Par}_n} a_{\lambda,k}s_\lambda,$$

where $a_{\lambda,k}$ is the number of all assignments T of entries in $\{1,2,\ldots,n\}$ to the cells of the Ferrers diagram of λ such that the following four conditions are satisfied:

- Every element of $\{1,2,\ldots,n\}$ is used precisely once in the assignment (i.e., we have $\mathrm{cont}(T) = (1^n)$).
- Whenever a cell y of the Ferrers diagram lies immediately to the right of a cell x, we have $T(y) - T(x) \geq 2$.
- Whenever a cell y of the Ferrers diagram lies immediately below a cell x, we have $T(y) - T(x) \geq -1$.
- There exist precisely k elements $i \in \{1,2,\ldots,n-1\}$ such that the cell $T^{-1}(i)$ lies in a row below $T^{-1}(i+1)$.

Are there any such rules for the $X_{n,d,s}$ of part (b)?

Smirnov n-tuples are more usually called Smirnov words, or (occasionally) Carlitz words.

See [68, Chapter 6] for further properties of the symmetric functions $U_{n,d,0}$, $V_{n,d,0}$ and $W_{n,d,0}$ from Exercise 2.9.11(c) (or, more precisely, of their generating functions $\sum_d U_{n,d,0}t^d$ etc.).

Exercise 2.9.13. (a) Let $n \in \mathbb{N}$. Define a matrix $A_n = (a_{i,j})_{i,j=1,2,\ldots,n} \in \Lambda^{n\times n}$ by

$$a_{i,j} = \begin{cases} p_{i-j+1}, & \text{if } i \geq j; \\ i, & \text{if } i = j-1; \\ 0, & \text{if } i < j-1 \end{cases} \qquad \text{for all } (i,j) \in \{1,2,\ldots,n\}^2.$$

This matrix A_n looks as follows:

$$A_n = \begin{pmatrix} p_1 & 1 & 0 & \cdots & 0 & 0 \\ p_2 & p_1 & 2 & \cdots & 0 & 0 \\ p_3 & p_2 & p_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ p_{n-1} & p_{n-2} & p_{n-3} & \cdots & p_1 & n-1 \\ p_n & p_{n-1} & p_{n-2} & \cdots & p_2 & p_1 \end{pmatrix}.$$

Show that $\det(A_n) = n!e_n$.

(b) Let n be a positive integer. Define a matrix $B_n = (b_{i,j})_{i,j=1,2,\ldots,n} \in \Lambda^{n\times n}$ by

$$b_{i,j} = \begin{cases} ie_i, & \text{if } j = 1; \\ e_{i-j+1}, & \text{if } j > 1 \end{cases} \qquad \text{for all } (i,j) \in \{1,2,\ldots,n\}^2.$$

The matrix B_n looks as follows:

$$B_n = \begin{pmatrix} e_1 & e_0 & e_{-1} & \cdots & e_{-n+3} & e_{-n+2} \\ 2e_2 & e_1 & e_0 & \cdots & e_{-n+4} & e_{-n+3} \\ 3e_3 & e_2 & e_1 & \cdots & e_{-n+5} & e_{-n+4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\,e_{n-1} & e_{n-2} & e_{n-3} & \cdots & e_1 & e_0 \\ ne_n & e_{n-1} & e_{n-2} & \cdots & e_2 & e_1 \end{pmatrix}$$

$$= \begin{pmatrix} e_1 & 1 & 0 & \cdots & 0 & 0 \\ 2e_2 & e_1 & 1 & \cdots & 0 & 0 \\ 3e_3 & e_2 & e_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\,e_{n-1} & e_{n-2} & e_{n-3} & \cdots & e_1 & 1 \\ ne_n & e_{n-1} & e_{n-2} & \cdots & e_2 & e_1 \end{pmatrix}.$$

Show that $\det(B_n) = p_n$.

The formulas of Exercise 2.9.13, for finitely many variables, appear in Prasolov's [171, §4.1][184]. In [171, §4.2], Prasolov gives four more formulas, which express e_n as a polynomial in the $h_1, h_2, h_3, \ldots$, or h_n as a polynomial in the $e_1, e_2, e_3, \ldots$, or p_n as a polynomial in the $h_1, h_2, h_3, \ldots$, or $n!h_n$ as a polynomial in the $p_1, p_2, p_3, \ldots$. These are not novel for us, since the first two of them are particular cases of Theorem 2.4.6, whereas the latter two can be derived from Exercise 2.9.13 by applying ω. (Note that ω is only well-defined on symmetric functions in infinitely many indeterminates, so we need to apply ω **before** evaluating at finitely many indeterminates; this explains why Prasolov has to prove the latter two identities separately.)

Exercise 2.9.14. In the following, if $k \in \mathbb{N}$, we shall use the notation 1^k for $\underbrace{1, 1, \ldots, 1}_{k \text{ times}}$ (in contexts such as $(n, 1^m)$). So, for example, $\left(3, 1^4\right)$ is the partition $(3, 1, 1, 1, 1)$.

(a) Show that $e_n h_m = s_{(m+1,1^{n-1})} + s_{(m,1^n)}$ for any two positive integers n and m.

(b) Show that

$$\sum_{i=0}^{b} (-1)^i h_{a+i+1} e_{b-i} = s_{(a+1,1^b)}$$

for any $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(c) Show that

$$\sum_{i=0}^{b} (-1)^i h_{a+i+1} e_{b-i} = (-1)^b \delta_{a+b,-1}$$

for any negative integer a and every $b \in \mathbb{N}$. (As usual, we set $h_j = 0$ for $j < 0$ here.)

(d) Show that

$$\Delta s_{(a+1,1^b)} = 1 \otimes s_{(a+1,1^b)} + s_{(a+1,1^b)} \otimes 1 + \sum_{\substack{(c,d,e,f) \in \mathbb{N}^4; \\ c+e=a-1; \\ d+f=b}} s_{(c+1,1^d)} \otimes s_{(e+1,1^f)} + \sum_{\substack{(c,d,e,f) \in \mathbb{N}^4; \\ c+e=a; \\ d+f=b-1}} s_{(c+1,1^d)} \otimes s_{(e+1,1^f)}$$

for any $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

Our next few exercises survey some results on Littlewood-Richardson coefficients.

Exercise 2.9.15. Let $m \in \mathbb{N}$ and $k \in \mathbb{N}$. Let λ and μ be two partitions such that $\ell(\lambda) \leq k$ and $\ell(\mu) \leq k$. Assume that all parts of λ and all parts of μ are $\leq m$. (It is easy to see that this assumption is equivalent to requiring $\lambda_i \leq m$ and $\mu_i \leq m$ for every positive integer i. [185]). Let $\lambda^\vee$ and $\mu^\vee$ denote the k-tuples $(m - \lambda_k, m - \lambda_{k-1}, \ldots, m - \lambda_1)$ and $(m - \mu_k, m - \mu_{k-1}, \ldots, m - \mu_1)$, respectively.

[184] where our symmetric functions e_k, h_k, p_k, evaluated in finitely many indeterminates, are denoted σ_k, p_k, s_k, respectively

[185] As usual, we are denoting by ν_i the i-th entry of a partition ν here.

(a) Show that $\lambda^\vee$ and $\mu^\vee$ are partitions, and that $s_{\lambda/\mu} = s_{\mu^\vee/\lambda^\vee}$.

(b) Show that $c^\lambda_{\mu,\nu} = c^{\mu^\vee}_{\lambda^\vee,\nu}$ for any partition ν.

(c) Let ν be a partition such that $\ell(\nu) \leq k$, and such that all parts of ν are $\leq m$. Let $\nu^\vee$ denote the k-tuple $(m-\nu_k, m-\nu_{k-1}, \ldots, m-\nu_1)$. Show that $\nu^\vee$ is a partition, and satisfies

$$c^\lambda_{\mu,\nu} = c^\lambda_{\nu,\mu} = c^{\mu^\vee}_{\lambda^\vee,\nu} = c^{\mu^\vee}_{\nu,\lambda^\vee} = c^{\nu^\vee}_{\mu,\lambda^\vee} = c^{\nu^\vee}_{\lambda^\vee,\mu}.$$

(d) Show that

$$s_{\lambda^\vee}(x_1, x_2, \ldots, x_k) = (x_1 x_2 \cdots x_k)^m \cdot s_\lambda\left(x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}\right)$$

in the Laurent polynomial ring $\mathbf{k}\left[x_1, x_2, \ldots, x_k, x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1}\right]$.

(e) Let r be a nonnegative integer. Show that $(r+\lambda_1, r+\lambda_2, \ldots, r+\lambda_k)$ is a partition and satisfies

$$s_{(r+\lambda_1, r+\lambda_2, \ldots, r+\lambda_k)}(x_1, x_2, \ldots, x_k) = (x_1 x_2 \cdots x_k)^r \cdot s_\lambda(x_1, x_2, \ldots, x_k)$$

in the polynomial ring $\mathbf{k}[x_1, x_2, \ldots, x_k]$.

Exercise 2.9.16. Let $m \in \mathbb{N}$, $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Let μ and ν be two partitions such that $\ell(\mu) \leq k$ and $\ell(\nu) \leq k$. Assume that all parts of μ are $\leq m$ (that is, $\mu_i \leq m$ for every positive integer i) [186], and that all parts of ν are $\leq n$ (that is, $\nu_i \leq n$ for every positive integer i). Let $\mu^{\vee\{m\}}$ denote the k-tuple $(m-\mu_k, m-\mu_{k-1}, \ldots, m-\mu_1)$, and let $\nu^{\vee\{n\}}$ denote the k-tuple $(n-\nu_k, n-\nu_{k-1}, \ldots, n-\nu_1)$.

(a) Show that $\mu^{\vee\{m\}}$ and $\nu^{\vee\{n\}}$ are partitions.

Now, let λ be a further partition such that $\ell(\lambda) \leq k$.

(b) If not all parts of λ are $\leq m+n$, then show that $c^\lambda_{\mu,\nu} = 0$.

(c) If all parts of λ are $\leq m+n$, then show that $c^\lambda_{\mu,\nu} = c^{\lambda^{\vee\{m+n\}}}_{\mu^{\vee\{m\}},\nu^{\vee\{n\}}}$, where $\lambda^{\vee\{m+n\}}$ denotes the k-tuple $(m+n-\lambda_k, m+n-\lambda_{k-1}, \ldots, m+n-\lambda_1)$.

The results of Exercise 2.7.11(c) and Exercise 2.9.15(c) are two *symmetries of Littlewood-Richardson coefficients*[187]; combining them yields further such symmetries. While these symmetries were relatively easy consequences of our algebraic definition of the Littlewood-Richardson coefficients, it is a much more challenging task to derive them bijectively from a combinatorial definition of these coefficients (such as the one given in Corollary 2.6.12). Some such derivations appear in [218], in [11], in [16, Example 3.6, Proposition 5.11 and references therein], [73, §5.1, §A.1, §A.4] and [109, (2.12)] (though a different combinatorial interpretation of $c^\lambda_{\mu,\nu}$ is used in the latter three).

Exercise 2.9.17. Recall our usual notations: For every partition λ and every positive integer i, the i-th entry of λ is denoted by λ_i. The sign $\triangleright$ stands for dominance order. We let λ^t denote the conjugate partition of a partition λ.

For any two partitions μ and ν, we define two new partitions $\mu+\nu$ and $\mu \sqcup \nu$ of $|\mu|+|\nu|$ as follows:

- The partition $\mu+\nu$ is defined as $(\mu_1+\nu_1, \mu_2+\nu_2, \mu_3+\nu_3, \ldots)$.
- The partition $\mu \sqcup \nu$ is defined as the result of sorting the list $\left(\mu_1, \mu_2, \ldots, \mu_{\ell(\mu)}, \nu_1, \nu_2, \ldots, \nu_{\ell(\nu)}\right)$ in decreasing order.

(a) Show that any two partitions μ and ν satisfy $(\mu+\nu)^t = \mu^t \sqcup \nu^t$ and $(\mu \sqcup \nu)^t = \mu^t + \nu^t$.

(b) Show that any two partitions μ and ν satisfy $c^{\mu+\nu}_{\mu,\nu} = 1$ and $c^{\mu\sqcup\nu}_{\mu,\nu} = 1$.

(c) If $k \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfy $k \leq n$, and if $\mu \in \mathrm{Par}_k$, $\nu \in \mathrm{Par}_{n-k}$ and $\lambda \in \mathrm{Par}_n$ are such that $c^\lambda_{\mu,\nu} \neq 0$, then prove that $\mu+\nu \triangleright \lambda \triangleright \mu \sqcup \nu$.

(d) If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ and $\alpha, \beta \in \mathrm{Par}_n$ and $\gamma, \delta \in \mathrm{Par}_m$ are such that $\alpha \triangleright \beta$ and $\gamma \triangleright \delta$, then show that $\alpha+\gamma \triangleright \beta+\delta$ and $\alpha \sqcup \gamma \triangleright \beta \sqcup \delta$.

(e) Let $m \in \mathbb{N}$ and $k \in \mathbb{N}$, and let λ be the partition $\left(m^k\right) = \left(\underbrace{m, m, \ldots, m}_{k \text{ times}}\right)$. Show that any two partitions μ and ν satisfy $c^\lambda_{\mu,\nu} \in \{0,1\}$.

(f) Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$, and let λ be the partition $\left(a+1, 1^b\right)$ (using the notation of Exercise 2.9.14). Show that any two partitions μ and ν satisfy $c^\lambda_{\mu,\nu} \in \{0,1\}$.

[186] As usual, we are denoting by ν_i the i-th entry of a partition ν here.

[187] The result of Exercise 2.9.16(c) can also be regarded as a symmetry of Littlewood-Richardson coefficients; see [10, §3.3].

(g) If λ is any partition, and if μ and ν are two rectangular partitions[188], then show that $c_{\mu,\nu}^{\lambda} \in \{0,1\}$.

Exercise 2.9.17(g) is part of Stembridge's [211, Thm. 2.1]; we refer to that article for further results of its kind.

The Littlewood-Richardson rule comes in many different forms, whose equivalence is not always immediate. Our version (Corollary 2.6.12) has the advantage of being the simplest to prove and one of the simplest to state. Other versions can be found in [206, appendix 1 to Ch. 7], Fulton's [73, Ch. 5] and van Leeuwen's [129]. We restrict ourselves to proving some very basic equivalences that allow us to restate parts of Corollary 2.6.12:

Exercise 2.9.18. We shall use the following notations:

- If T is a column-strict tableau and j is a positive integer, then we use the notation $T|_{\text{cols}\geq j}$ for the restriction of T to the union of its columns $j, j+1, j+2, \ldots$. (This notation has already been used in Section 2.6.)
- If T is a column-strict tableau and S is a set of cells of T, then we write $T|_S$ for the restriction of T to the set S of cells.[189]
- If T is a column-strict tableau, then an *NE-set* of T means a set S of cells of T such that whenever $s \in S$, every cell of T which lies northeast[190] of s must also belong to S.
- The *Semitic reading word*[191] of a column-strict tableau T is the concatenation[192] $r_1 r_2 r_3 \cdots$, where r_i is the word obtained by reading the i-th row of T from right to left.[193]
- If $w = (w_1, w_2, \ldots, w_n)$ is a word, then a *prefix* of w means a word of the form $(w_1, w_2, \ldots, w_i)$ for some $i \in \{0, 1, \ldots, n\}$. (In particular, both w and the empty word are prefixes of w.)

  A word w over the set of positive integers is said to be *Yamanouchi* if for any prefix v of w and any positive integer i, there are at least as many i's among the letters of v as there are $(i+1)$'s among them.[194]

Prove the following two statements:

(a) Let μ be a partition. Let $b_{i,j}$ be a nonnegative integer for every two positive integers i and j. Assume that $b_{i,j} = 0$ for all but finitely many pairs (i,j).

The following two assertions are equivalent:

– *Assertion $\mathcal{A}$:* There exist a partition λ and a column-strict tableau T of shape λ/μ such that all $(i,j) \in \{1,2,3,\ldots\}^2$ satisfy

$$b_{i,j} = (\text{the number of all entries } i \text{ in the } j\text{-th row of } T)\,. \tag{2.9.13}$$

– *Assertion $\mathcal{B}$:* The inequality

$$\mu_{j+1} + (b_{1,j+1} + b_{2,j+1} + \cdots + b_{i+1,j+1}) \leq \mu_j + (b_{1,j} + b_{2,j} + \cdots + b_{i,j}) \tag{2.9.14}$$

holds for all $(i,j) \in \mathbb{N} \times \{1,2,3,\ldots\}$.

---

[188] A partition is called *rectangular* if it has the form $(m^k) = \left(\underbrace{m, m, \ldots, m}_{k \text{ times}}\right)$ for some $m \in \mathbb{N}$ and $k \in \mathbb{N}$.

[189] This restriction $T|_S$ is not necessarily a tableau of skew shape; it is just a map from S to $\{1,2,3,\ldots\}$. The content $\operatorname{cont}(T|_S)$ is nevertheless well-defined (in the usual way: $(\operatorname{cont}(T|_S))_i = \left|(T|_S)^{-1}(i)\right|$).

[190] A cell (r,c) is said to lie *northeast* of a cell (r',c') if and only if we have $r \leq r'$ and $c \geq c'$.

[191] The notation comes from [129] and is a reference to the Arabic and Hebrew way of writing.

[192] If $s_1, s_2, s_3, \ldots$ are several words (finitely or infinitely many), then the *concatenation* $s_1 s_2 s_3 \cdots$ is defined as the word which is obtained by starting with the empty word, then appending s_1 to its end, then appending s_2 to the end of the result, then appending s_3 to the end of the result, etc.

[193] For example, the Semitic reading word of the tableau

$$\begin{array}{cccccc} & & 3 & 4 & 4 & 5 \\ 1 & 4 & 6 & & & \\ 3 & 5 & & & & \end{array}$$

is 544364153.

The Semitic reading word of a tableau T is what is called the *reverse reading word* of T in [206, §A.1.3].

[194] For instance, the words 11213223132 and 1213 are Yamanouchi, while the words 132, 21 and 1121322332111 are not. The Dyck words (defined as in [206, Example 6.6.6], and written using 1's and 2's instead of x's and y's) are precisely the Yamanouchi words whose letters are 1's and 2's and in which the letter 1 appears as often as the letter 2.

Yamanouchi words are often called lattice permutations.

(b) Let λ and μ be two partitions, and let T be a column-strict tableau of shape λ/μ. Then, the following five assertions are equivalent:
- *Assertion $\mathcal{C}$:* For every positive integer j, the weak composition $\operatorname{cont}\left(T|_{\text{cols}\geq j}\right)$ is a partition.
- *Assertion $\mathcal{D}$:* For every positive integers j and i, the number of entries $i+1$ in the first j rows[195] of T is $\leq$ to the number of entries i in the first $j-1$ rows of T.
- *Assertion $\mathcal{E}$:* For every NE-set S of T, the weak composition $\operatorname{cont}\left(T|_S\right)$ is a partition.
- *Assertion $\mathcal{F}$:* The Semitic reading word of T is Yamanouchi.
- *Assertion $\mathcal{G}$:* There exists a column-strict tableau S whose shape is a partition and which satisfies the following property: For any positive integers i and j, the number of entries i in the j-th row of T equals the number of entries j in the i-th row of S.

Remark 2.9.19. The equivalence of Assertions $\mathcal{C}$ and $\mathcal{F}$ in Exercise 2.9.18(b) is the "not-too-difficult exercise" mentioned in [210]. It yields the equivalence between our version of the Littlewood-Richardson rule (Corollary 2.6.12) and that in [206, A1.3.3].

In the next exercises, we shall restate Corollary 2.6.11 in a different form. While Corollary 2.6.11 provided a decomposition of the product of a skew Schur function with a Schur function into a sum of Schur functions, the different form that we will encounter in Exercise 2.9.21(b) will give a combinatorial interpretation for the Hall inner product between two skew Schur functions. Let us first generalize Exercise 2.9.18(b):

Exercise 2.9.20. Let us use the notations of Exercise 2.9.18. Let κ, λ and μ be three partitions, and let T be a column-strict tableau of shape λ/μ.

(a) Prove that the following five assertions are equivalent:
- *Assertion $\mathcal{C}^{(\kappa)}$:* For every positive integer j, the weak composition $\kappa + \operatorname{cont}\left(T|_{\text{cols}\geq j}\right)$ is a partition.
- *Assertion $\mathcal{D}^{(\kappa)}$:* For every positive integers j and i, we have
$$\kappa_{i+1} + (\text{the number of entries } i+1 \text{ in the first } j \text{ rows of } T)$$
$$\leq \kappa_i + (\text{the number of entries } i \text{ in the first } j-1 \text{ rows of } T)\,.$$
- *Assertion $\mathcal{E}^{(\kappa)}$:* For every NE-set S of T, the weak composition $\kappa + \operatorname{cont}\left(T|_S\right)$ is a partition.
- *Assertion $\mathcal{F}^{(\kappa)}$:* For every prefix v of the Semitic reading word of T, and for every positive integer i, we have
$$\kappa_i + (\text{the number of } i\text{'s among the letters of } v)$$
$$\geq \kappa_{i+1} + (\text{the number of } (i+1)\text{'s among the letters of } v)\,.$$
- *Assertion $\mathcal{G}^{(\kappa)}$:* There exist a partition ζ and a column-strict tableau S of shape ζ/κ which satisfies the following property: For any positive integers i and j, the number of entries i in the j-th row of T equals the number of entries j in the i-th row of S.

(b) Let τ be a partition such that $\tau = \kappa + \operatorname{cont} T$. Consider the five assertions $\mathcal{C}^{(\kappa)}$, $\mathcal{D}^{(\kappa)}$, $\mathcal{E}^{(\kappa)}$, $\mathcal{F}^{(\kappa)}$ and $\mathcal{G}^{(\kappa)}$ introduced in Exercise 2.9.20(a). Let us also consider the following assertion:
- *Assertion $\mathcal{H}^{(\kappa)}$:* There exists a column-strict tableau S of shape τ/κ which satisfies the following property: For any positive integers i and j, the number of entries i in the j-th row of T equals the number of entries j in the i-th row of S.

Prove that the six assertions $\mathcal{C}^{(\kappa)}$, $\mathcal{D}^{(\kappa)}$, $\mathcal{E}^{(\kappa)}$, $\mathcal{F}^{(\kappa)}$, $\mathcal{G}^{(\kappa)}$ and $\mathcal{H}^{(\kappa)}$ are equivalent.

Clearly, Exercise 2.9.18(b) is the particular case of Exercise 2.9.20 when $\kappa = \varnothing$.

Using Exercise 2.9.20, we can restate Corollary 2.6.11 in several ways:

Exercise 2.9.21. Let λ, μ and κ be three partitions.

(a) Show that
$$s_\kappa s_{\lambda/\mu} = \sum_T s_{\kappa+\operatorname{cont} T},$$
where the sum ranges over all column-strict tableaux T of shape λ/μ satisfying the five equivalent assertions $\mathcal{C}^{(\kappa)}$, $\mathcal{D}^{(\kappa)}$, $\mathcal{E}^{(\kappa)}$, $\mathcal{F}^{(\kappa)}$ and $\mathcal{G}^{(\kappa)}$ introduced in Exercise 2.9.20(a).

[195] The "first j rows" mean the 1-st row, the 2-nd row, etc., the j-th row (even if some of these rows are empty).

(b) Let τ be a partition. Show that $\left(s_{\lambda/\mu}, s_{\tau/\kappa}\right)_\Lambda$ is the number of all column-strict tableaux T of shape λ/μ satisfying $\tau = \kappa + \operatorname{cont} T$ and also satisfying the six equivalent assertions $\mathcal{C}^{(\kappa)}$, $\mathcal{D}^{(\kappa)}$, $\mathcal{E}^{(\kappa)}$, $\mathcal{F}^{(\kappa)}$, $\mathcal{G}^{(\kappa)}$ and $\mathcal{H}^{(\kappa)}$ introduced in Exercise 2.9.20.

Exercise 2.9.21(a) is merely Corollary 2.6.11, rewritten in light of Exercise 2.9.20. Various parts of it appear in the literature. For instance, [126, (53)] easily reveals to be a restatement of the fact that $s_\kappa s_{\lambda/\mu} = \sum_T s_{\nu+\operatorname{cont} T}$, where the sum ranges over all column-strict tableaux T of shape λ/μ satisfying Assertion $\mathcal{D}^{(\kappa)}$.

Exercise 2.9.21(b) is one version of a "skew Littlewood-Richardson rule" that goes back to Zelevinsky [228] (although Zelevinsky's version uses both a different language and a combinatorial interpretation which is not obviously equivalent to ours). It appears in various sources; for instance, [126, Theorem 5.2, second formula] says that $\left(s_{\lambda/\mu}, s_{\tau/\kappa}\right)_\Lambda$ is the number of all column-strict tableaux T of shape λ/μ satisfying $\tau = \kappa + \operatorname{cont} T$ and the assertion $\mathcal{H}^{(\kappa)}$, whereas [75, Theorem 1.2] says that $\left(s_{\lambda/\mu}, s_{\tau/\kappa}\right)_\Lambda$ is the number of all all column-strict tableaux T of shape λ/μ satisfying $\tau = \kappa + \operatorname{cont} T$ and the assertion $\mathcal{F}^{(\kappa)}$. (Notice that Gasharov's proof of [75, Theorem 1.2] uses the same involutions as Stembridge's proof of Theorem 2.6.6; it can thus be regarded as a close precursor to Stembridge's proof. However, it uses the Jacobi-Trudi identities, while Stembridge's does not.)

Exercise 2.9.22. Let $\mathbb{K}$ be a field.[196] If $N \in \mathbb{K}^{n\times n}$ is a nilpotent matrix, then the *Jordan type* of N is defined to be the list of the sizes of the Jordan blocks in the Jordan normal form of N, sorted in decreasing order[197]. This Jordan type is a partition of n, and uniquely determines N up to similarity (i.e., two nilpotent $n\times n$-matrices N and N' are similar if and only if the Jordan types of N and N' are equal). If f is a nilpotent endomorphism of a finite-dimensional $\mathbb{K}$-vector space V, then we define the *Jordan type* of f as the Jordan type of any matrix representing f (the choice of the matrix does not matter, since the Jordan type of a matrix remains unchanged under conjugation).

(a) Let $n \in \mathbb{N}$. Let $N \in \mathbb{K}^{n\times n}$ be a nilpotent matrix. Let $\lambda \in \operatorname{Par}_n$. Show that the matrix N has Jordan type λ if and only if every $k \in \mathbb{N}$ satisfies

$$\dim\left(\ker\left(N^k\right)\right) = \left(\lambda^t\right)_1 + \left(\lambda^t\right)_2 + \ldots + \left(\lambda^t\right)_k.$$

(Here, we are using the notation λ^t for the transpose of a partition λ, and the notation ν_i for the i-th entry of a partition ν.)

(b) Let f be a nilpotent endomorphism of a finite-dimensional $\mathbb{K}$-vector space V. Let U be an f-stable $\mathbb{K}$-vector subspace of V (that is, a $\mathbb{K}$-vector subspace of V satisfying $f(U) \subset U$). Then, restricting f to U gives a nilpotent endomorphism $f \mid U$ of U, and the endomorphism f also induces a nilpotent endomorphism $\overline{f}$ of the quotient space V/U. Let λ, μ and ν be the Jordan types of f, $f \mid U$ and $\overline{f}$, respectively. Show that $c^\lambda_{\mu,\nu} \neq 0$ (if $\mathbb{Z}$ is a subring of $\mathbf{k}$).

[**Hint:** For (b), Exercise 2.7.11(c) shows that it is enough to prove that $c^{\lambda^t}_{\mu^t,\nu^t} \neq 0$. Due to Corollary 2.6.12, this only requires constructing a column-strict tableau T of shape λ^t/μ^t with $\operatorname{cont} T = \nu^t$ which has the property that each $\operatorname{cont}\left(T|_{\text{cols}\geq j}\right)$ is a partition. Construct this tableau by defining $a_{i,j} = \dim\left(\left(f^i\right)^{-1}(U) \cap \ker\left(f^j\right)\right)$ for all $(i,j) \in \mathbb{N}^2$, and requiring that the number of entries i in the j-th row of T be $a_{i,j} - a_{i,j-1} - a_{i-1,j} + a_{i-1,j-1}$ for all $(i,j) \in \{1,2,3,\ldots\}^2$. Use Exercise 2.9.18(a) to prove that this indeed defines a column-strict tableau, and Exercise 2.9.18(b) to verify that it satisfies the condition on $\operatorname{cont}\left(T|_{\text{cols}\geq j}\right)$.]

Remark 2.9.23. Exercise 2.9.22 is a taste of the connections between the combinatorics of partitions and the Jordan normal form. Much more can, and has, been said. Marc van Leeuwen's [127] is dedicated to some of these connections; in particular, our Exercise 2.9.22(a) is [127, Proposition 1.1], and a far stronger version of Exercise 2.9.22(b) appears in [127, Theorem 4.3 (2)], albeit only for the case of an infinite $\mathbb{K}$. One can prove a converse to Exercise 2.9.22(b) as well: If $c^\lambda_{\mu,\nu} \neq 0$, then there exist V, f and U satisfying the premises of Exercise 2.9.22(b). When $\mathbb{K}$ is a finite field, we can ask enumerative questions, such as how many U's are

[196] This field has no relation to the ring $\mathbf{k}$, over which our symmetric functions are defined.

[197] The Jordan normal form of N is well-defined even if $\mathbb{K}$ is not algebraically closed, because N is nilpotent (so the characteristic polynomial of N is X^n).

there for given V, f, λ, μ and ν; we will see a few answers in Section 4.9 (specifically, Proposition 4.9.4), and a more detailed treatment is given in [142, Ch. 2].

The relationship between partitions and Jordan normal forms can be exploited to provide linear-algebraic proofs of purely combinatorial facts. See [28, Sections 6 and 9] for some examples. Note that [28, Lemma 9.10] is the statement that, under the conditions of Exercise 2.9.22(b), we have $\nu \subseteq \lambda$. This is a direct consequence of Exercise 2.9.22(b) (since $c^{\lambda}_{\mu,\nu} \neq 0$ can happen only if $\nu \subseteq \lambda$).

Exercise 2.9.24. Let $a \in \Lambda$. Prove the following:

(a) The set $\left\{ g \in \Lambda \mid g^{\perp} a = (\omega(g))^{\perp} a \right\}$ is a $\mathbf{k}$-subalgebra of Λ.

(b) Assume that $e_k^{\perp} a = h_k^{\perp} a$ for each positive integer k. Then, $g^{\perp} a = (\omega(g))^{\perp} a$ for each $g \in \Lambda$.

Exercise 2.9.25. Let $n \in \mathbb{N}$. Let ρ be the partition $(n-1, n-2, \ldots, 1)$. Prove that $s_{\rho/\mu} = s_{\rho/\mu^t}$ for every $\mu \in \mathrm{Par}$.

Remark 2.9.26. Exercise 2.9.25 appears in [180, Corollary 7.32], and is due to John Stembridge. Using Remark 2.5.9, we can rewrite it as yet another equality between Littlewood-Richardson coefficients: Namely, $c^{\rho}_{\mu,\nu} = c^{\rho}_{\mu^t,\nu}$ for any $\mu \in \mathrm{Par}$ and $\nu \in \mathrm{Par}$.

3. Zelevinsky's structure theory of positive self-dual Hopf algebras

Chapter 2 showed that, as a $\mathbb{Z}$-basis for the Hopf algebra $\Lambda = \Lambda_{\mathbb{Z}}$, the Schur functions $\{s_\lambda\}$ have two special properties: they have the *same* structure constants $c^\lambda_{\mu,\nu}$ for their multiplication as for their comultiplication (Corollary 2.5.7), and these structure constants are all *nonnegative* integers (Corollary 2.6.12). Zelevinsky [227, §2,3] isolated these two properties as crucial.

Definition 3.0.1. Say that a connected graded Hopf algebra A over $\mathbf{k} = \mathbb{Z}$ with a distinguished $\mathbb{Z}$-basis $\{\sigma_\lambda\}$ consisting of homogeneous elements[198] is a *positive self-dual Hopf algebra* (or *PSH*) if it satisfies the two further axioms

- **(self-duality)** The same structure constants $a^\lambda_{\mu,\nu}$ appear for the product $\sigma_\mu\sigma_\nu = \sum_\lambda a^\lambda_{\mu,\nu}\sigma_\lambda$ and the coproduct $\Delta\sigma_\lambda = \sum_{\mu,\nu} a^\lambda_{\mu,\nu}\sigma_\mu \otimes \sigma_\nu$.
- **(positivity)** The $a^\lambda_{\mu,\nu}$ are all nonnegative (integers).

Call $\{\sigma_\lambda\}$ the *PSH-basis* of A.

He then developed a beautiful structure theory for PSH's, explaining how they can be uniquely expressed as tensor products of copies of PSH's each isomorphic to Λ after rescaling their grading. The next few sections explain this, following his exposition closely.

3.1. **Self-duality implies polynomiality.** We begin with a property that forces a Hopf algebra to have algebra structure which is a *polynomial* algebra, specifically the symmetric algebra $\mathrm{Sym}(\mathfrak{p})$, where $\mathfrak{p}$ is the $\mathbf{k}$-submodule of primitive elements.

Recall from Exercise 1.3.20(g) that for a connected graded Hopf algebra $A = \bigoplus_{n=0}^\infty A_n$, every x in the two-sided ideal $I := \ker\epsilon = \bigoplus_{n>0} A_n$ has the property that its comultiplication takes the form

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

where $\Delta_+(x)$ lies in $I \otimes I$. Recall also that the elements x for which $\Delta_+(x) = 0$ are called the *primitives*. Denote by $\mathfrak{p}$ the $\mathbf{k}$-submodule of primitive elements inside A.

Given a PSH A (over $\mathbf{k} = \mathbb{Z}$) with a PSH-basis $\{\sigma_\lambda\}$, we consider the bilinear form $(\cdot,\cdot)_A : A \times A \to \mathbb{Z}$ on A that makes this basis orthonormal. Similarly, the elements $\{\sigma_\lambda \otimes \sigma_\mu\}$ give an orthonormal basis for a form $(\cdot,\cdot)_{A\otimes A}$ on $A \otimes A$. The bilinear form $(\cdot,\cdot)_A$ on the PSH A gives rise to a $\mathbb{Z}$-linear map $A \to A^o$, which is easily seen to be injective and a $\mathbb{Z}$-algebra homomorphism. We thus identify A with a subalgebra of A^o. When A is of finite type, this map is a Hopf algebra isomorphism, thus allowing us to identify A with A^o. This is an instance of the following notion of self-duality.

Definition 3.1.1. (a) If $(\cdot,\cdot) : V \times W \to \mathbf{k}$ is a bilinear form on the product $V \times W$ of two graded $\mathbf{k}$-modules $V = \bigoplus_{n\geq 0} V_n$ and $W = \bigoplus_{n\geq 0} W_n$, then we say that this form $(\cdot,\cdot)$ is *graded* if every two distinct nonnegative integers n and m satisfy $(V_n, W_m) = 0$ (that is, if every two homogeneous elements $v \in V$ and $w \in W$ having distinct degrees satisfy $(v, w) = 0$).

(b) If $(\cdot,\cdot)_V : V \times V \to \mathbf{k}$ and $(\cdot,\cdot)_W : W \times W \to \mathbf{k}$ are two symmetric bilinear forms on some $\mathbf{k}$-modules V and W, then we can canonically define a symmetric bilinear form $(\cdot,\cdot)_{V\otimes W}$ on the $\mathbf{k}$-module $V \otimes W$ by letting

$$(v \otimes w, v' \otimes w')_{V\otimes W} = (v, v')_V (w, w')_W \qquad \text{for all } v, v' \in V \text{ and } w, w' \in W.$$

This new bilinear form is graded if the original two forms $(\cdot,\cdot)_V$ and $(\cdot,\cdot)_W$ were graded (presuming that V and W are graded).

(c) Say that a bialgebra A is *self-dual* with respect to a given symmetric bilinear form $(\cdot,\cdot) : A \times A \to \mathbf{k}$ if one has $(a, m(b \otimes c))_A = (\Delta(a), b \otimes c)_{A\otimes A}$ and $(1_A, a) = \epsilon(a)$ for a, b, c in A. If A is a graded Hopf algebra of finite type, and this form $(\cdot,\cdot)$ is graded, then this is equivalent to the $\mathbf{k}$-module map $A \to A^o$ induced by $(\cdot,\cdot)_A$ giving a Hopf algebra homomorphism.

Thus, any PSH A is self-dual with respect to the bilinear form $(\cdot,\cdot)_A$ that makes its PSH-basis orthonormal.

Notice also that the injective $\mathbb{Z}$-algebra homomorphism $A \to A^o$ obtained from the bilinear form $(\cdot,\cdot)_A$ on a PSH A allows us to regard each $f \in A$ as an element of A^o. Thus, for any PSH A and any $f \in A$, an operator $f^\perp : A \to A$ is well-defined (indeed, regard f as an element of A^o, and apply Definition 2.8.1).

[198] not necessarily indexed by partitions

Proposition 3.1.2. *Let A be a Hopf algebra over $\mathbf{k} = \mathbb{Z}$ or $\mathbf{k} = \mathbb{Q}$ which is graded, connected, and self-dual with respect to a positive definite graded*[199] *bilinear form. Then:*

(a) *Within the ideal I, the $\mathbf{k}$-submodule of primitives $\mathfrak{p}$ is the orthogonal complement to the $\mathbf{k}$-submodule I^2.*
(b) *In particular, $\mathfrak{p} \cap I^2 = 0$.*
(c) *When $\mathbf{k} = \mathbb{Q}$, one has $I = \mathfrak{p} \oplus I^2$.*

Proof. (a) Note that $I^2 = m(I \otimes I)$. Hence an element x in I lies in the perpendicular space to I^2 if and only if one has for all y in $I \otimes I$ that

$$0 = (x, m(y))_A = (\Delta(x), y)_{A \otimes A} = (\Delta_+(x), y)_{A \otimes A}$$

where the second equality uses self-duality, while the third equality uses the fact that y lies in $I \otimes I$ and the form $(\cdot, \cdot)_{A \otimes A}$ makes distinct homogeneous components orthogonal. Since y was arbitrary, this means x is perpendicular to I^2 if and only if $\Delta_+(x) = 0$, that is, x lies in $\mathfrak{p}$.

(b) This follows from (a), since the form $(\cdot, \cdot)_A$ is positive definite.

(c) This follows from (a) using some basic linear algebra[200] when A is of finite type (which is the only case we will ever encounter in practice). See Exercise 3.1.6 for the general proof. □

Remark 3.1.3. One might wonder why we didn't just say $I = \mathfrak{p} \oplus I^2$ even when $\mathbf{k} = \mathbb{Z}$ in Proposition 3.1.2(c). However, this is false even for $A = \Lambda_{\mathbb{Z}}$: the second homogeneous component $(\mathfrak{p} \oplus I^2)_2$ is the index 2 sublattice of Λ_2 which is $\mathbb{Z}$-spanned by $\{p_2, e_1^2\}$, containing $2e_2$, but not containing e_2 itself.

Already the fact that $\mathfrak{p} \cap I^2 = 0$ has a strong implication.

Lemma 3.1.4. *A connected graded Hopf algebra A over any ring $\mathbf{k}$ having $\mathfrak{p} \cap I^2 = 0$ must necessarily be commutative (as an algebra).*

Proof. The component $A_0 = \mathbf{k}$ commutes with all of A. This forms the base case for an induction on $i + j$ in which one shows that any elements x in A_i and y in A_j with $i, j > 0$ will have $[x, y] := xy - yx = 0$. Since $[x, y]$ lies in I^2, it suffices to show that $[x, y]$ also lies in $\mathfrak{p}$:

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

showing that $[x, y]$ lies in $\mathfrak{p}$. Here the second-to-last equality used the inductive hypotheses: homogeneity implies that $\Delta_+(x)$ is a sum of homogeneous tensors of the form $z_1 \otimes z_2$ satisfying $\deg(z_1), \deg(z_2) < i$, so that by induction they will commute with $1 \otimes y, y \otimes 1$, thus proving that $[\Delta_+(x), 1 \otimes y + y \otimes 1] = 0$; a symmetric argument shows $[1 \otimes x + x \otimes 1, \Delta_+(y)] = 0$, and a similar argument shows $[\Delta_+(x), \Delta_+(y)] = 0$. The last equality is an easy calculation, and was done already in the process of proving (1.3.7). □

Remark 3.1.5. Zelevinsky actually shows [227, Proof of A.1.3, p. 150] that the assumption of $\mathfrak{p} \cap I^2 = 0$ (along with hypotheses of unit, counit, graded, connected, and Δ being a morphism for multiplication) already implies the *associativity* of the multiplication in A ! One shows by induction on $i + j + k$ that any x, y, z in A_i, A_j, A_k with $i, j, k > 0$ have vanishing *associator* $\mathrm{assoc}(x, y, z) := x(yz) - (xy)z$. In the inductive step, one first notes that $\mathrm{assoc}(x, y, z)$ lies in I^2, and then checks that $\mathrm{assoc}(x, y, z)$ also lies in $\mathfrak{p}$, by a calculation very similar to the one above, repeatedly using the fact that $\mathrm{assoc}(x, y, z)$ is multilinear in its three arguments.

Exercise 3.1.6. Prove Proposition 3.1.2(c) in the general case.

[199] That is, $(A_i, A_j) = 0$ for $i \neq j$.

[200] Specifically, either the existence of an orthogonal projection on a subspace of a finite-dimensional inner-product space over $\mathbb{Q}$, or the fact that $\dim\left(W^{\perp}\right) = \dim V - \dim W$ for a subspace W of a finite-dimensional inner-product space V over $\mathbb{Q}$ can be used.

This leads to a general structure theorem.

Theorem 3.1.7. *If a connected graded Hopf algebra A over a field $\mathbf{k}$ of characteristic zero has $I = \mathfrak{p} \oplus I^2$, then the inclusion $\mathfrak{p} \hookrightarrow A$ extends to a Hopf algebra isomorphism from the symmetric algebra $\mathrm{Sym}_{\mathbf{k}}(\mathfrak{p}) \to A$. In particular, A is both commutative and cocommutative.*

Note that the hypotheses of Theorem 3.1.7 are valid, using Proposition 3.1.2(c), whenever A is obtained from a PSH (over $\mathbb{Z}$) by tensoring with $\mathbb{Q}$.

Proof of Theorem 3.1.7. Since Lemma 3.1.4 implies that A is commutative, the universal property of $\mathrm{Sym}_{\mathbf{k}}(\mathfrak{p})$ as a free commutative algebra on generators $\mathfrak{p}$ shows that the inclusion $\mathfrak{p} \hookrightarrow A$ at least extends to an algebra morphism $\mathrm{Sym}_{\mathbf{k}}(\mathfrak{p}) \xrightarrow{\varphi} A$. Since the Hopf structure on $\mathrm{Sym}_{\mathbf{k}}(\mathfrak{p})$ makes the elements of $\mathfrak{p}$ primitive (see Example 1.3.14), this φ is actually a coalgebra morphism (since $\Delta \circ \varphi = (\varphi \otimes \varphi) \circ \Delta$ and $\epsilon \circ \varphi = \epsilon$ need only to be checked on algebra generators), hence a bialgebra morphism, hence a Hopf algebra morphism (by Corollary 1.4.27). It remains to show that φ is surjective, and injective.

For the surjectivity of φ, note that the hypothesis $I = \mathfrak{p} \oplus I^2$ implies that the composite $\mathfrak{p} \hookrightarrow I \to I/I^2$ gives a $\mathbf{k}$-vector space isomorphism. What follows is a standard argument to deduce that $\mathfrak{p}$ generates A as a commutative graded $\mathbf{k}$-algebra. One shows by induction on n that any homogeneous element a in A_n lies in the $\mathbf{k}$-subalgebra generated by $\mathfrak{p}$. The base case $n = 0$ is trivial as a lies in $A_0 = \mathbf{k} \cdot 1_A$. In the inductive step where a lies in I, write $a \equiv p \bmod I^2$ for some p in $\mathfrak{p}$. Thus $a = p + \sum_i b_i c_i$, where b_i, c_i lie in I but have strictly smaller degree, so that by induction they lie in the subalgebra generated by $\mathfrak{p}$, and hence so does a.

Note that the surjectivity argument did not use the assumption that $\mathbf{k}$ has characteristic zero, but we will now use it in the injectivity argument for φ, to establish the following

(3.1.1) **Claim:** Every primitive element of $\mathrm{Sym}(\mathfrak{p})$ lies in $\mathfrak{p} = \mathrm{Sym}^1(\mathfrak{p})$.

Note that this claim fails in positive characteristic, e.g. if $\mathbf{k}$ has characteristic 2 then x^2 lies in $\mathrm{Sym}^2(\mathfrak{p})$, however

$$\Delta(x^2) = 1 \otimes x^2 + 2x \otimes x + x^2 \otimes 1 = 1 \otimes x^2 + x^2 \otimes 1.$$

To prove the claim (3.1.1), assume not, so that by gradedness, there must exist some primitive element $y \neq 0$ lying in some $\mathrm{Sym}^n(\mathfrak{p})$ with $n \geq 2$. This would mean that $f(y) = 0$, where the map f is defined as the composition

$$\mathrm{Sym}^n(\mathfrak{p}) \xrightarrow{\Delta} \bigoplus_{i+j=n} \mathrm{Sym}^i(\mathfrak{p}) \otimes \mathrm{Sym}^j(\mathfrak{p}) \xrightarrow{\text{projection}} \mathrm{Sym}^1(\mathfrak{p}) \otimes \mathrm{Sym}^{n-1}(\mathfrak{p})$$

of the coproduct Δ with the component projection of $\bigoplus_{i+j=n} \mathrm{Sym}^i(\mathfrak{p}) \otimes \mathrm{Sym}^j(\mathfrak{p})$ onto $\mathrm{Sym}^1(\mathfrak{p}) \otimes \mathrm{Sym}^{n-1}(\mathfrak{p})$. However, one can check on a basis that the multiplication backward $\mathrm{Sym}^1(\mathfrak{p}) \otimes \mathrm{Sym}^{n-1}(\mathfrak{p}) \xrightarrow{m} \mathrm{Sym}^n(\mathfrak{p})$ has the property that $m \circ f = n \cdot \mathrm{id}_{\mathrm{Sym}^n(\mathfrak{p})}$: Indeed,

$$(m \circ f)(x_1 \cdots x_n) = m\left(\sum_{j=1}^{n} x_j \otimes x_1 \cdots \widehat{x_j} \cdots x_n\right) = n \cdot x_1 \cdots x_n$$

for $x_1, \ldots, x_n$ in $\mathfrak{p}$. Then $n \cdot y = m(f(y)) = m(0) = 0$ leads to the contradiction that $y = 0$, since $\mathbf{k}$ has characteristic zero. Thus, (3.1.1) is proven.

Now one can argue the injectivity of the (graded) map[201] φ by assuming that one has a nonzero homogeneous element u in $\ker(\varphi)$ of minimum degree. In particular, $\deg(u) \geq 1$. Also since $\mathfrak{p} \hookrightarrow A$, one has that u is not in $\mathrm{Sym}^1(\mathfrak{p}) = \mathfrak{p}$, and hence u is not primitive by (3.1.1). Consequently $\Delta_+(u) \neq 0$, and one can find a nonzero component $u^{(i,j)}$ of $\Delta_+(u)$ lying in $\mathrm{Sym}(\mathfrak{p})_i \otimes \mathrm{Sym}(\mathfrak{p})_j$ for some $i, j > 0$. Since this forces $i, j < \deg(u)$, one has that φ maps both $\mathrm{Sym}(\mathfrak{p})_i, \mathrm{Sym}(\mathfrak{p})_j$ injectively into A_i, A_j. Hence the tensor product map

$$\mathrm{Sym}(\mathfrak{p})_i \otimes \mathrm{Sym}(\mathfrak{p})_j \xrightarrow{\varphi \otimes \varphi} A_i \otimes A_j$$

[201] The grading on $\mathrm{Sym}(\mathfrak{p})$ is induced from the grading on $\mathfrak{p}$, a homogeneous subspace of $I \subset A$ as it is the kernel of the graded map $I \xrightarrow{\Delta_+} A \otimes A$.

is also injective[202]. This implies $(\varphi \otimes \varphi)(u^{(i,j)}) \neq 0$, giving the contradiction that

$$0 = \Delta_+^A(0) = \Delta_+^A(\varphi(u)) = (\varphi \otimes \varphi)(\Delta_+^{\mathrm{Sym}(\mathfrak{p})}(u))$$

contains the nonzero $A_i \otimes A_j$-component $(\varphi \otimes \varphi)(u^{(i,j)})$.

(An alternative proof of the injectivity of φ proceeds as follows: By (3.1.1), the subspace of primitive elements of $\mathrm{Sym}(\mathfrak{p})$ is $\mathfrak{p}$, and clearly $\varphi\,|_{\mathfrak{p}}$ is injective. Hence, Exercise 1.4.35(b) (applied to the homomorphism φ) shows that φ is injective.) □

Before closing this section, we mention one nonobvious corollary of the Claim (3.1.1), when applied to the ring of symmetric functions $\Lambda_{\mathbb{Q}}$ with $\mathbb{Q}$-coefficients, since Proposition 2.4.1 says that $\Lambda_{\mathbb{Q}} = \mathbb{Q}[p_1, p_2, \ldots] = \mathrm{Sym}(V)$ where $V = \mathbb{Q}\{p_1, p_2, \ldots\}$.

Corollary 3.1.8. *The subspace $\mathfrak{p}$ of primitives in $\Lambda_{\mathbb{Q}}$ is one-dimensional in each degree $n = 1, 2, \ldots$, and spanned by $\{p_1, p_2, \ldots\}$.*

We note in passing that this corollary can also be obtained in a simpler fashion and a greater generality:

Exercise 3.1.9. Let $\mathbf{k}$ be any commutative ring. Show that the primitive elements of Λ are precisely the elements of the $\mathbf{k}$-linear span of $p_1, p_2, p_3, \ldots$.

3.2. **The decomposition theorem.** Our goal here is Zelevinsky's theorem [227, Theorem 2.2] giving a canonical decomposition of any PSH as a tensor product into PSH's that each have only one primitive element in their PSH-basis. For the sake of stating it, we introduce some notation.

Definition 3.2.1. Given a PSH A with PSH-basis Σ, let $\mathcal{C} := \Sigma \cap \mathfrak{p}$ be the primitive elements in Σ. For each ρ in $\mathcal{C}$, let $A(\rho) \subset A$ be the $\mathbb{Z}$-span of

$$\Sigma(\rho) := \{\sigma \in \Sigma : \text{ there exists } n \geq 0 \text{ with } (\sigma, \rho^n) \neq 0\}.$$

Definition 3.2.2. The tensor product of two PSHs A_1 and A_2 with PSH-bases Σ_1 and Σ_2 is defined as the graded Hopf algebra $A_1 \otimes A_2$ with PSH-basis $\{\sigma_1 \otimes \sigma_2\}_{(\sigma_1,\sigma_2)\in\Sigma_1\times\Sigma_2}$. It is easy to see that this is again a PSH. The tensor product of any finite family of PSHs is defined similarly[203].

Theorem 3.2.3. *Any PSH A has a canonical tensor product decomposition*

$$A = \bigotimes_{\rho \in \mathcal{C}} A(\rho)$$

with $A(\rho)$ a PSH, and ρ the only primitive element in its PSH-basis $\Sigma(\rho)$.

Although in all the applications, $\mathcal{C}$ will be finite, when $\mathcal{C}$ is infinite one should interpret the tensor product in the theorem as the inductive limit of tensor products over finite subsets of $\mathcal{C}$, that is, linear combinations of basic tensors $\bigotimes_\rho a_\rho$ in which there are only finitely many factors $a_\rho \neq 1$.

The first step toward the theorem uses a certain unique factorization property.

Lemma 3.2.4. *Let $\mathcal{P}$ be a set of pairwise orthogonal primitives in a PSH A. Then,*

$$(\rho_1 \cdots \rho_r, \pi_1 \cdots \pi_s) = 0$$

for ρ_i, π_j in $\mathcal{P}$ unless $r = s$ and one can reindex so that $\rho_i = \pi_i$.

---

[202] One needs to know that for two injective maps $V_i \xrightarrow{\varphi_i} W_i$ of $\mathbf{k}$-vector spaces V_i, W_i with $i = 1, 2$, the tensor product $\varphi_1 \otimes \varphi_2$ is also injective. Factoring it as $\varphi_1 \otimes \varphi_2 = (\mathrm{id} \otimes \varphi_2) \circ (\varphi_1 \otimes \mathrm{id})$, one sees that it suffices to show that for an injective map $V \xrightarrow{\varphi} W$ of free $\mathbf{k}$-modules, and any free $\mathbf{k}$-module U, the map $V \otimes U \xrightarrow{\varphi\otimes\mathrm{id}} W \otimes U$ is also injective. Since tensor products commute with direct sums, and U is (isomorphic to) a direct sum of copies of $\mathbf{k}$, this reduces to the easy-to-check case where $U = \mathbf{k}$.

Note that some kind of freeness or flatness hypothesis on U is needed here since, e.g. the injective $\mathbb{Z}$-module maps $\mathbb{Z} \xrightarrow{\varphi_1=(\cdot\times 2)} \mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi_2=\mathrm{id}} \mathbb{Z}/2\mathbb{Z}$ have $\varphi_1 \otimes \varphi_2 = 0$ on $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \neq 0$.

[203] For the empty family, it is the connected graded Hopf algebra $\mathbb{Z}$ with PSH-basis $\{1\}$.

Proof. Induct on r. For $r > 0$, one has

$$\begin{aligned}(\rho_1 \cdots \rho_r, \pi_1 \cdots \pi_s) &= (\rho_2 \cdots \rho_r, \rho_1^{\perp}(\pi_1 \cdots \pi_s)) \\ &= (\rho_2 \cdots \rho_r, \sum_{j=1}^{s} (\pi_1 \cdots \pi_{j-1} \cdot \rho_1^{\perp}(\pi_j) \cdot \pi_{j+1} \cdots \pi_s))\end{aligned}$$

from Proposition 2.8.2(iv) because ρ_1 is primitive[204]. On the other hand, since each π_j is primitive, one has $\rho_1^{\perp}(\pi_j) = (\rho_1, 1) \cdot \pi_j + (\rho_1, \pi_j) \cdot 1 = (\rho_1, \pi_j)$ which vanishes unless $\rho_1 = \pi_j$. Hence $(\rho_1 \cdots \rho_r, \pi_1 \cdots \pi_s) = 0$ unless $\rho_1 \in \{\pi_1, \ldots, \pi_s\}$, in which case after reindexing so that $\pi_1 = \rho_1$, it equals

$$n \cdot (\rho_1, \rho_1) \cdot (\rho_2 \cdots \rho_r, \pi_2 \cdots \pi_s)$$

if there are exactly n occurrences of ρ_1 among $\pi_1, \ldots, \pi_s$. Now apply induction. □

So far the positivity hypothesis for a PSH has played little role. Now we use it to introduce a certain partial order on the PSH A, and then a semigroup grading.

Definition 3.2.5. For a subset S of an abelian group, let $\mathbb{Z}S$ (resp. $\mathbb{N}S$) denote the subgroup of $\mathbb{Z}$-linear combinations (resp. submonoid of $\mathbb{N}$-linear combinations[205]) of the elements of S.

In a PSH A with PSH-basis Σ, the subset $\mathbb{N}\Sigma$ forms a submonoid, and lets one define a partial order on A via $a \leq b$ if $b - a$ lies in $\mathbb{N}\Sigma$.

We note a few trivial properties of this partial order:

- The positivity hypothesis implies that $\mathbb{N}\Sigma \cdot \mathbb{N}\Sigma \subset \mathbb{N}\Sigma$.
- Hence multiplication by an element $c \geq 0$ (meaning c lies in $\mathbb{N}\Sigma$) preserves the order: $a \leq b$ implies $ac \leq bc$ since $(b - a)c$ lies in $\mathbb{N}\Sigma$.
- Thus $0 \leq c \leq d$ and $0 \leq a \leq b$ together imply $ac \leq bc \leq bd$.

This allows one to introduce a semigroup grading on A.

Definition 3.2.6. Let $\mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}$ denote the additive submonoid of $\mathbb{N}^{\mathcal{C}}$ consisting of those $\alpha = (\alpha_\rho)_{\rho \in \mathcal{C}}$ with finite support.

Note that for any α in $\mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}$, one has that the product $\prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho} \geq 0$. Define

$$\Sigma(\alpha) := \{\sigma \in \Sigma : \sigma \leq \prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho}\},$$

that is, the subset of Σ on which $\prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho}$ has support. Also define

$$A_{(\alpha)} := \mathbb{Z}\Sigma(\alpha) \subset A.$$

Proposition 3.2.7. *The PSH A has an $\mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}$-semigroup-grading: one has an orthogonal direct sum decomposition*

$$A = \bigoplus_{\alpha \in \mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}} A_{(\alpha)}$$

for which

$$A_{(\alpha)} A_{(\beta)} \subset A_{(\alpha+\beta)}, \tag{3.2.1}$$

$$\Delta A_{(\alpha)} \subset \bigoplus_{\alpha = \beta + \gamma} A_{(\beta)} \otimes A_{(\gamma)}. \tag{3.2.2}$$

Proof. We will make free use of the fact that a PSH A is commutative, since it embeds in $A \otimes_{\mathbb{Z}} \mathbb{Q}$, which is commutative by Theorem 3.1.7.

Note that the orthogonality $\left(A_{(\alpha)}, A_{(\beta)}\right) = 0$ for $\alpha \neq \beta$ is equivalent to the assertion that

$$\left(\prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho}, \prod_{\rho \in \mathcal{C}} \rho^{\beta_\rho}\right) = 0,$$

[204] Strictly speaking, this argument needs further justification since A might not be of finite type (and if it is not, Proposition 2.8.2(iv) cannot be applied). It is more adequate to refer to the proof of Proposition 2.8.2(iv), which indeed goes through with ρ_1 taking the role of f.

[205] Recall that $\mathbb{N} := \{0, 1, 2, \ldots\}$.

which follows from Lemma 3.2.4.

Next let us deal with the assertion (3.2.1). It suffices to check that when τ, ω in Σ lie in $A_{(\alpha)}, A_{(\beta)}$, respectively, then $\tau\omega$ lies in $A_{(\alpha+\beta)}$. But note that any σ in Σ having $\sigma \leq \tau\omega$ will then have

$$\sigma \leq \tau\omega \leq \prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho} \cdot \prod_{\rho \in \mathcal{C}} \rho^{\beta_\rho} = \prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho + \beta_\rho}$$

so that σ lies in $A_{(\alpha+\beta)}$. This means that $\tau\omega$ lies in $A_{(\alpha+\beta)}$.

This lets us check that $\bigoplus_{\alpha \in \mathbb{N}^{\mathcal{C}}_{\text{fin}}} A_{(\alpha)}$ exhaust A. It suffices to check that any σ in Σ lies in some $A_{(\alpha)}$. Proceed by induction on $\deg(\sigma)$, with the case $\sigma = 1$ being trivial; the element 1 always lies in Σ, and hence lies in $A_{(\alpha)}$ for $\alpha = 0$. For σ lying in I, one either has $(\sigma, a) \neq 0$ for some a in I^2, or else σ lies in $(I^2)^\perp = \mathfrak{p}$ (by Proposition 3.1.2(a)), so that σ is in $\mathcal{C}$ and we are done. If $(\sigma, a) \neq 0$ with a in I^2, then σ appears in the support of some $\mathbb{Z}$-linear combination of elements $\tau\omega$ where τ, ω lie in Σ and have strictly smaller degree than σ has. There exists at least one such pair τ, ω for which $(\sigma, \tau\omega) \neq 0$, and therefore $\sigma \leq \tau\omega$. Then by induction τ, ω lie in some $A_{(\alpha)}, A_{(\beta)}$, respectively, so $\tau\omega$ lies in $A_{(\alpha+\beta)}$, and hence σ lies in $A_{(\alpha+\beta)}$ also.

Self-duality shows that (3.2.1) implies (3.2.2): if a, b, c lie in $A_{(\alpha)}, A_{(\beta)}, A_{(\gamma)}$, respectively, then $(\Delta a, b \otimes c)_{A \otimes A} = (a, bc)_A = 0$ unless $\alpha = \beta + \gamma$. □

Proposition 3.2.8. *For α, β in $\mathbb{N}^{\mathcal{C}}_{\text{fin}}$ with disjoint support, one has a bijection*

$$\begin{array}{ccc} \Sigma(\alpha) \times \Sigma(\beta) & \longrightarrow & \Sigma(\alpha + \beta), \\ (\sigma, \tau) & \longmapsto & \sigma\tau. \end{array}$$

Thus, the multiplication map $A_{(\alpha)} \otimes A_{(\beta)} \to A_{(\alpha+\beta)}$ is an isomorphism.

Proof. We first check that for σ_1, σ_2 in $\Sigma(\alpha)$ and τ_1, τ_2 in $\Sigma(\beta)$, one has

$$(\sigma_1\tau_1, \sigma_2\tau_2) = \delta_{(\sigma_1,\tau_1),(\sigma_2,\tau_2)}. \tag{3.2.3}$$

Note that this is equivalent to showing both

- that $\sigma\tau$ lie in $\Sigma(\alpha + \beta)$ so that the map is well-defined, since it shows $(\sigma\tau, \sigma\tau) = 1$, and
- that the map is injective.

One calculates

$$\begin{aligned} (\sigma_1\tau_1, \sigma_2\tau_2)_A &= (\sigma_1\tau_1, m(\sigma_2 \otimes \tau_2))_A \\ &= (\Delta(\sigma_1\tau_1), \sigma_2 \otimes \tau_2)_{A \otimes A} \\ &= (\Delta(\sigma_1)\Delta(\tau_1), \sigma_2 \otimes \tau_2)_{A \otimes A}. \end{aligned}$$

Note that due to (3.2.2), $\Delta(\sigma_1)\Delta(\tau_1)$ lies in $\sum A_{(\alpha'+\beta')} \otimes A_{(\alpha''+\beta'')}$ where

$$\begin{aligned} \alpha' + \alpha'' &= \alpha, \\ \beta' + \beta'' &= \beta. \end{aligned}$$

Since $\sigma_2 \otimes \tau_2$ lies in $A_{(\alpha)} \otimes A_{(\beta)}$, the only nonvanishing terms in the inner product come from those with

$$\begin{aligned} \alpha' + \beta' &= \alpha, \\ \alpha'' + \beta'' &= \beta. \end{aligned}$$

As α, β have disjoint support, this can only happen if

$$\alpha' = \alpha,\ \alpha'' = 0,\ \beta' = 0,\ \beta'' = \beta;$$

that is, the only nonvanishing term comes from $(\sigma_1 \otimes 1)(1 \otimes \tau_1) = \sigma_1 \otimes \tau_1$. Hence

$$(\sigma_1\tau_1, \sigma_2\tau_2)_A = (\sigma_1 \otimes \tau_1, \sigma_2 \otimes \tau_2)_{A \otimes A} = \delta_{(\sigma_1,\tau_1),(\sigma_2,\tau_2)}.$$

To see that the map is surjective, express

$$\begin{aligned} \prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho} &= \sum_i \sigma_i, \\ \prod_{\rho \in \mathcal{C}} \rho^{\beta_\rho} &= \sum_j \tau_j \end{aligned}$$

with $\sigma_i \in \Sigma(\alpha)$ and $\tau_j \in \Sigma(\beta)$. Then each product $\sigma_i \tau_j$ is in $\Sigma(\alpha+\beta)$ by (3.2.3), and

$$\prod_{\rho \in \mathcal{C}} \rho^{\alpha_\rho + \beta_\rho} = \sum_{i,j} \sigma_i \tau_j$$

shows that $\{\sigma_i \tau_j\}$ exhausts $\Sigma(\alpha+\beta)$. This gives surjectivity. □

Proof of Theorem 3.2.3. Recall from Definition 3.2.1 that for each ρ in $\mathcal{C}$, one defines $A(\rho) \subset A$ to be the $\mathbb{Z}$-span of

$$\Sigma(\rho) := \{\sigma \in \Sigma : \text{ there exists } n \geq 0 \text{ with } (\sigma, \rho^n) \neq 0\}.$$

In other words, $A(\rho) := \bigoplus_{n \geq 0} A_{(n \cdot e_\rho)}$ where e_ρ in $\mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}$ is the standard basis element indexed by ρ. Proposition 3.2.7 then shows that $A(\rho)$ is a Hopf subalgebra of A. Since every α in $\mathbb{N}_{\mathrm{fin}}^{\mathcal{C}}$ can be expressed as the (finite) sum $\sum_\rho \alpha_\rho e_\rho$, and the e_ρ have disjoint support, iterating Proposition 3.2.8 shows that $A = \bigotimes_{\rho \in \mathcal{C}} A(\rho)$. Lastly, $\Sigma(\rho)$ is clearly a PSH-basis for $A(\rho)$, and if σ is any primitive element in $\Sigma(\rho)$ then $(\sigma, \rho^n) \neq 0$ lets one conclude via Lemma 3.2.4 that $\sigma = \rho$ (and $n = 1$). □

3.3. Λ **is the unique indecomposable PSH.** The goal here is to prove the rest of Zelevinsky's structure theory for PSH's. Namely, if A has only one primitive element ρ in its PSH-basis Σ, then A must be isomorphic as a PSH to the ring of symmetric functions Λ, after one rescales the grading of A. Note that every σ in Σ has $\sigma \leq \rho^n$ for some n, and hence has degree divisible by the degree of ρ. Thus one can divide all degrees by that of ρ and assume ρ has degree 1.

The idea is to find within A and Σ a set of elements that play the role of

$$\{h_n = s_{(n)}\}_{n=0,1,2,\ldots}, \qquad \{e_n = s_{(1^n)}\}_{n=0,1,2,\ldots}$$

within $A = \Lambda$ and its PSH-basis of Schur functions $\Sigma = \{s_\lambda\}$. Zelevinsky's argument does this by isolating some properties that turn out to characterize these elements:

(a) $h_0 = e_0 = 1$, and $h_1 = e_1 =: \rho$ has ρ^2 a sum of two elements of Σ, namely

$$\rho^2 = h_2 + e_2.$$

(b) For all $n = 0, 1, 2, \ldots$, there exist unique elements h_n, e_n in $A_n \cap \Sigma$ that satisfy

$$h_2^\perp e_n = 0,$$
$$e_2^\perp h_n = 0$$

with h_2, e_2 being the two elements of Σ introduced in (a).

(c) For $k = 0, 1, 2, \ldots, n$ one has

$$h_k^\perp h_n = h_{n-k} \text{ and } \sigma^\perp h_n = 0 \text{ for } \sigma \in \Sigma \setminus \{h_0, h_1, \ldots, h_n\},$$
$$e_k^\perp e_n = e_{n-k} \text{ and } \sigma^\perp e_n = 0 \text{ for } \sigma \in \Sigma \setminus \{e_0, e_1, \ldots, e_n\}.$$

In particular, $e_k^\perp h_n = 0 = h_k^\perp e_n$ for $k \geq 2$.

(d) Their coproducts are

$$\Delta(h_n) = \sum_{i+j=n} h_i \otimes h_j,$$
$$\Delta(e_n) = \sum_{i+j=n} e_i \otimes e_j.$$

We will prove Zelevinsky's result [227, Theorem 3.1] as a combination of the following two theorems.

Theorem 3.3.1. *Let A be a PSH with PSH-basis Σ containing only one primitive ρ, and assume that the grading has been rescaled so that ρ has degree 1. Then, after renaming $\rho = e_1 = h_1$, one can find unique sequences $\{h_n\}_{n=0,1,2,\ldots}, \{e_n\}_{n=0,1,2,\ldots}$ of elements of Σ having properties (a),(b),(c),(d) listed above.*

The second theorem uses the following notion.

Definition 3.3.2. A *PSH-morphism* $A \xrightarrow{\varphi} A'$ between two PSH's A, A' having PSH-bases Σ, Σ' is a graded Hopf algebra morphism for which $\varphi(\mathbb{N}\Sigma) \subset \mathbb{N}\Sigma'$. If $A = A'$ and $\Sigma = \Sigma'$ it will be called a *PSH-endomorphism*. If φ is an isomorphism and restricts to a bijection $\Sigma \to \Sigma'$, it will be called a *PSH-isomorphism*[206]; if it is both a PSH-isomorphism and an endomorphism, it is a *PSH-automorphism*.[207]

Theorem 3.3.3. *The elements $\{h_n\}_{n=0,1,2,\ldots}, \{e_n\}_{n=0,1,2,\ldots}$ in Theorem 3.3.1 also satisfy the following.*

(e) *The elements h_n, e_n in A satisfy the same relation (2.4.4)*

$$\sum_{i+j=n} (-1)^i e_i h_j = \delta_{0,n}$$

as their counterparts in Λ, along with the property that

$$A = \mathbb{Z}[h_1, h_2, \ldots] = \mathbb{Z}[e_1, e_2, \ldots].$$

(f) *There is exactly one nontrivial automorphism $A \xrightarrow{\omega} A$ as a PSH, swapping $h_n \leftrightarrow e_n$.*

(g) *There are exactly two PSH-isomorphisms $A \to \Lambda$:*
- *one sending h_n to the complete homogeneous symmetric functions $h_n(\mathbf{x})$, while sending e_n to the elementary symmetric functions $e_n(\mathbf{x})$,*
- *the second one (obtained by composing the first with ω) sending $h_n \mapsto e_n(\mathbf{x})$ and $e_n \mapsto h_n(\mathbf{x})$.*

Before embarking on the proof, we mention one more bit of convenient terminology: say that an element σ in Σ is a *constituent* of a in $\mathbb{N}\Sigma$ when $\sigma \leq a$, that is, σ appears with nonzero coefficient c_σ in the unique expansion $a = \sum_{\tau \in \Sigma} c_\tau \tau$.

Proof of Theorem 3.3.1. One fact that occurs frequently is this:

$$\text{Every } \sigma \text{ in } \Sigma \cap A_n \text{ is a constituent of } \rho^n. \tag{3.3.1}$$

This follows from Theorem 3.2.3, since ρ is the only primitive element of Σ: one has $A = A(\rho)$ and $\Sigma = \Sigma(\rho)$, so that σ is a constituent of some ρ^m, and homogeneity considerations force $m = n$.

Notice that A is of finite type (due to (3.3.1)). Thus, A^o is a graded Hopf algebra isomorphic to A.

Assertion (a). Note that

$$(\rho^2, \rho^2) = (\rho^\perp(\rho^2), \rho) = (2\rho, \rho) = 2$$

using the fact that $\rho^\perp$ is a derivation since ρ is primitive (Proposition 2.8.2(iv)). On the other hand, expressing $\rho^2 = \sum_{\sigma \in \Sigma} c_\sigma \sigma$ with c_σ in $\mathbb{N}$, one has $(\rho^2, \rho^2) = \sum_\sigma c_\sigma^2$. Hence exactly two of the $c_\sigma = 1$, so ρ^2 has exactly two distinct constituents. Denote them by h_2 and e_2. One concludes that $\Sigma \cap A_2 = \{h_2, e_2\}$ from (3.3.1).

Note also that the same argument shows $\Sigma \cap A_1 = \{\rho\}$, so that $A_1 = \mathbb{Z}\rho$. Since $\rho^\perp h_2$ lies in $A_1 = \mathbb{Z}\rho$ and $(\rho^\perp h_2, \rho) = (h_2, \rho^2) = 1$, we have $\rho^\perp h_2 = \rho$. Similarly $\rho^\perp e_2 = \rho$.

Assertion (b). We will show via induction on n the following three assertions for $n \geq 1$:

(3.3.2)
- There exists an element h_n in $\Sigma \cap A_n$ with $e_2^\perp h_n = 0$.
- This element h_n is unique.
- Furthermore $\rho^\perp h_n = h_{n-1}$.

In the base cases $n = 1, 2$, it is not hard to check that our previously labelled elements, h_1, h_2 (namely $h_1 := \rho$, and h_2 as named in part (a)) really *are* the unique elements satisfying these hypotheses.

---

[206] This definition is easily seen to be equivalent to saying that a PSH-isomorphism is an invertible PSH-morphism whose inverse is again a PSH-morphism.

[207] The reader should be warned that not every invertible PSH-endomorphism is necessarily a PSH-automorphism. For instance, it is an easy exercise to check that $\Lambda \otimes \Lambda \to \Lambda \otimes \Lambda$, $f \otimes g \mapsto \sum_{(f)} f_1 \otimes f_2 g$ is a well-defined invertible PSH-endomorphism of the PSH $\Lambda \otimes \Lambda$ with PSH-basis $(s_\lambda \otimes s_\mu)_{(\lambda,\mu) \in \mathrm{Par} \times \mathrm{Par}}$, but not a PSH-automorphism.

In the inductive step, it turns out that we will find h_n as a constituent of ρh_{n-1}. Thus we again use the derivation property of $\rho^\perp$ to compute that ρh_{n-1} has exactly two constituents:

$$\begin{aligned}(\rho h_{n-1}, \rho h_{n-1}) &= (\rho^\perp(\rho h_{n-1}), h_{n-1}) \\ &= (h_{n-1} + \rho \cdot \rho^\perp h_{n-1}, h_{n-1}) \\ &= (h_{n-1} + \rho h_{n-2}, h_{n-1}) \\ &= 1 + (h_{n-2}, \rho^\perp h_{n-1}) \\ &= 1 + (h_{n-2}, h_{n-2}) = 1 + 1 = 2\end{aligned}$$

where the inductive hypothesis $\rho^\perp h_{n-1} = h_{n-2}$ was used twice. We next show that exactly one of the two constituents of ρh_{n-1} is annihilated by $e_2^\perp$. Note that since e_2 lies in A_2, and A_1 has $\mathbb{Z}$-basis element ρ, there is a constant c in $\mathbb{Z}$ such that

$$\Delta(e_2) = e_2 \otimes 1 + c\rho \otimes \rho + 1 \otimes e_2. \tag{3.3.3}$$

On the other hand, (a) showed

$$1 = (e_2, \rho^2)_A = (\Delta(e_2), \rho \otimes \rho)_{A \otimes A}$$

so one must have $c = 1$. Therefore by Proposition 2.8.2(iv) again,

$$\begin{array}{rcccccc} e_2^\perp(\rho h_{n-1}) & = & e_2^\perp(\rho) h_{n-1} & + & \rho^\perp(\rho)\rho^\perp(h_{n-1}) & + & \rho e_2^\perp(h_{n-1}) \\ & = & 0 & + & h_{n-2} & + & 0 \\ & = & h_{n-2}, & & & & \end{array} \tag{3.3.4}$$

where the first term vanished due to degree considerations and the last term vanished by the inductive hypothesis. Bearing in mind that ρh_{n-1} lies in $\mathbb{N}\Sigma$, and in a PSH with PSH-basis Σ, any skewing operator $\sigma^\perp$ for σ in Σ will preserve $\mathbb{N}\Sigma$, one concludes from (3.3.4) that

- one of the two distinct constituents of the element ρh_{n-1} must be sent by $e_2^\perp$ to h_{n-2}, and
- the other constituent of ρh_{n-1} must be annihilated by $e_2^\perp$; call this second constituent h_n.

Lastly, to see that this h_n is unique, it suffices to show that any element σ of $\Sigma \cap A_n$ which is killed by $e_2^\perp$ must be a constituent of ρh_{n-1}. This holds for the following reason. We know $\sigma \leq \rho^n$ by (3.3.1), and hence $0 \neq (\rho^n, \sigma) = (\rho^{n-1}, \rho^\perp \sigma)$, implying that $\rho^\perp \sigma \neq 0$. On the other hand, since $0 = \rho^\perp e_2^\perp \sigma = e_2^\perp \rho^\perp \sigma$, one has that $\rho^\perp \sigma$ is annihilated by $e_2^\perp$, and hence $\rho^\perp \sigma$ must be a (positive) multiple of h_{n-1} by part of our inductive hypothesis. Therefore $(\sigma, \rho h_{n-1}) = (\rho^\perp \sigma, h_{n-1})$ is positive, that is, σ is a constituent of ρh_{n-1}.

The preceding argument, applied to $\sigma = h_n$, shows that $\rho^\perp h_n = c h_{n-1}$ for some c in $\{1, 2, \ldots\}$. Since $(\rho^\perp h_n, h_{n-1}) = (h_n, \rho h_{n-1}) = 1$, this c must be 1, so that $\rho^\perp h_n = h_{n-1}$. This completes the induction step in the proof of (3.3.2).

One can then argue, swapping the roles of e_n, h_n in the above argument, the existence and uniqueness of a sequence $\{e_n\}_{n=0}^\infty$ in Σ satisfying the properties analogous to (3.3.2), with $e_0 := 1, e_1 := \rho$.

Assertion (c). Iterating the property from (b) that $\rho^\perp h_n = h_{n-1}$ shows that $(\rho^k)^\perp h_n = h_{n-k}$ for $0 \leq k \leq n$. However one also has an expansion

$$\rho^k = c h_k + \sum_{\substack{\sigma \in \Sigma \cap A_k: \\ \sigma \neq h_k}} c_\sigma \sigma$$

for some integers $c, c_\sigma > 0$, since every σ in $\Sigma \cap A_k$ is a constituent of ρ^k. Hence

$$1 = (h_{n-k}, h_{n-k}) = ((\rho^k)^\perp h_n, (\rho^k)^\perp h_n) \geq c^2 (h_k^\perp h_n, h_k^\perp h_n)$$

using Proposition 2.8.2(ii). Hence if we knew that $h_k^\perp h_n \neq 0$ this would force

$$h_k^\perp h_n = (\rho^k)^\perp h_n = h_{n-k}$$

as well as $\sigma^\perp h_n = 0$ for all $\sigma \notin \{h_0, h_1, \ldots, h_n\}$. But

$$(\rho^{n-k})^\perp h_k^\perp h_n = h_k^\perp (\rho^{n-k})^\perp h_n = h_k^\perp h_k = 1 \neq 0$$

so $h_k^\perp h_n \neq 0$, as desired. The argument for $e_k^\perp e_n = e_{n-k}$ is symmetric.

The last assertion in (c) follows if one checks that $e_n \neq h_n$ for each $n \geq 2$, but this holds since $e_2^\perp(h_n) = 0$ but $e_2^\perp(e_n) = e_{n-2}$.

Assertion (d). Part (c) implies that

$$(\Delta h_n, \sigma \otimes \tau)_{A\otimes A} = (h_n, \sigma\tau)_A = (\sigma^\perp h_n, \tau)_A = 0$$

unless $\sigma = h_k$ for some $k = 0, 1, 2, \ldots, n$ and $\tau = h_{n-k}$. Also one can compute

$$(\Delta h_n, h_k \otimes h_{n-k}) = (h_n, h_k h_{n-k}) = (h_k^\perp h_n, h_{n-k}) \overset{(c)}{=} (h_{n-k}, h_{n-k}) = 1.$$

This is equivalent to the assertion for Δh_n in (d). The argument for Δe_n is symmetric. □

Before proving Theorem 3.3.3, we note some consequences of Theorem 3.3.1. Define for each partition $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell)$ the following two elements of A:

$$h_\lambda = h_{\lambda_1} h_{\lambda_2} \cdots h_{\lambda_\ell} = h_{\lambda_1} h_{\lambda_2} \cdots,$$
$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \cdots e_{\lambda_\ell} = e_{\lambda_1} e_{\lambda_2} \cdots.$$

Also, define the *lexicographic order* on Par_n by saying $\lambda <_{\mathrm{lex}} \mu$ if $\lambda \neq \mu$ and the smallest index i for which $\lambda_i \neq \mu_i$ has $\lambda_i < \mu_i$. Recall also that λ^t denotes the *conjugate* or *transpose* partition to λ, obtained by swapping rows and columns in the Ferrers diagram.

The following unitriangularity lemma will play a role in the proof of Theorem 3.3.3(e).

Lemma 3.3.4. *Under the hypotheses of Theorem 3.3.1, for λ, μ in Par_n, one has*

$$e_\mu^\perp h_\lambda = \begin{cases} 1, & \text{if } \mu = \lambda^t; \\ 0, & \text{if } \mu >_{\mathrm{lex}} \lambda^t. \end{cases} \tag{3.3.5}$$

Consequently

$$\det\left[(e_{\mu^t}, h_\lambda)\right]_{\lambda,\mu\in\mathrm{Par}_n} = 1. \tag{3.3.6}$$

Proof. Notice that A is of finite type (as shown in the proof of Theorem 3.3.1). Thus, A^o is a graded Hopf algebra isomorphic to A.

Also, notice that any $m \in \mathbb{N}$ and any $a_1, a_2, \ldots, a_\ell \in A$ satisfy

$$e_m^\perp(a_1 a_2 \cdots a_\ell) = \sum_{i_1+\cdots+i_\ell=m} e_{i_1}^\perp(a_1) \cdots e_{i_\ell}^\perp(a_\ell). \tag{3.3.7}$$

Indeed, this follows by induction over ℓ using Proposition 2.8.2(iv) (and the coproduct formula for $\Delta(e_n)$ in Theorem 3.3.1(d)).

In order to prove (3.3.5), induct on the length of μ. If λ has length ℓ, so that $\lambda_1^t = \ell$, then

$$\begin{aligned} e_\mu^\perp h_\lambda &= e_{(\mu_2,\mu_3,\ldots)}^\perp \left(e_{\mu_1}^\perp(h_{\lambda_1} \cdots h_{\lambda_\ell})\right) \qquad \left(\text{since } e_\mu = e_{\mu_1} e_{(\mu_2,\mu_3,\ldots)} \text{ and thus } e_\mu^\perp = e_{(\mu_2,\mu_3,\ldots)}^\perp \circ e_{\mu_1}^\perp\right) \\ &= e_{(\mu_2,\mu_3,\ldots)}^\perp \sum_{i_1+\cdots+i_\ell=\mu_1} e_{i_1}^\perp(h_{\lambda_1}) \cdots e_{i_\ell}^\perp(h_{\lambda_\ell}) \qquad \text{(by (3.3.7))} \\ &= e_{(\mu_2,\mu_3,\ldots)}^\perp \sum_{\substack{i_1+\cdots+i_\ell=\mu_1; \\ \text{each of } i_1,\ldots,i_\ell \text{ is } \leq 1}} e_{i_1}^\perp(h_{\lambda_1}) \cdots e_{i_\ell}^\perp(h_{\lambda_\ell}) \qquad \left(\text{since } e_k^\perp h_n = 0 \text{ for } k \geq 2\right) \\ &= \begin{cases} 0, & \text{if } \mu_1 > \ell = \lambda_1^t; \\ e_{(\mu_2,\mu_3,\ldots)}^\perp h_{(\lambda_1-1,\ldots,\lambda_\ell-1)}, & \text{if } \mu_1 = \ell = \lambda_1^t \end{cases} \end{aligned}$$

where the last equality used

$$e_k^\perp(h_n) = \begin{cases} h_{n-1}, & \text{if } k = 1; \\ 0, & \text{if } k \geq 2. \end{cases}$$

Now apply the induction hypothesis, since $(\lambda_1 - 1, \ldots, \lambda_\ell - 1)^t = (\lambda_2^t, \lambda_3^t, \ldots)$.

To prove (3.3.6), note that any λ, μ in Par_n satisfy $(e_{\mu^t}, h_\lambda) = (e_{\mu^t}^\perp(h_\lambda), 1) = e_{\mu^t}^\perp(h_\lambda)$ (since degree considerations enforce $e_{\mu^t}^\perp(h_\lambda) \in A_0 = \mathbf{k} \cdot 1$), and thus

$$(e_{\mu^t}, h_\lambda) = e_{\mu^t}^\perp(h_\lambda) = \begin{cases} 1, & \text{if } \mu^t = \lambda^t; \\ 0, & \text{if } \mu^t >_{\mathrm{lex}} \lambda^t \end{cases}$$

(by (3.3.5)). This means that the matrix $[(e_{\mu^t}, h_\lambda)]_{\lambda,\mu\in \mathrm{Par}_n}$ is unitriangular with respect to some total order on Par_n (namely, the lexicographic order on the conjugate partitions), and hence has determinant 1. □

The following proposition will be the crux of the proof of Theorem 3.3.3(f) and (g), and turns out to be closely related to Kerov's *asymptotic theory of characters of the symmetric groups* [108].

Proposition 3.3.5. *Given a PSH A with PSH-basis Σ containing only one primitive ρ, the two maps $A \to \mathbb{Z}$ defined on $A = \bigoplus_{n\geq 0} A_n$ via*

$$\delta_h = \bigoplus_n h_n^\perp,$$
$$\delta_e = \bigoplus_n e_n^\perp$$

are characterized as the only two $\mathbb{Z}$-linear maps $A \xrightarrow{\delta} \mathbb{Z}$ with the three properties of being

- ***positive**: $\delta(\mathbb{N}\Sigma) \subset \mathbb{N}$,*
- ***multiplicative**: $\delta(a_1a_2) = \delta(a_1)\delta(a_2)$ for all $a_1, a_2 \in A$, and*
- ***normalized**: $\delta(\rho) = 1$.*

Proof. Notice that A is of finite type (as shown in the proof of Theorem 3.3.1). Thus, A^o is a graded Hopf algebra isomorphic to A.

It should be clear from their definitions that δ_h, δ_e are $\mathbb{Z}$-linear, positive and normalized. To see that δ_h is multiplicative, by $\mathbb{Z}$-linearity, it suffices to check that for a_1, a_2 in A_{n_1}, A_{n_2} with $n_1 + n_2 = n$, one has

$$\delta_h(a_1a_2) = h_n^\perp(a_1a_2) = \sum_{i_1+i_2=n} h_{i_1}^\perp(a_1)h_{i_2}^\perp(a_2) = h_{n_1}^\perp(a_1)h_{n_2}^\perp(a_2) = \delta_h(a_1)\delta_h(a_2)$$

in which the second equality used Proposition 2.8.2(iv) and Theorem 3.3.1(d). The argument for δ_e is symmetric.

Conversely, given $A \xrightarrow{\delta} \mathbb{Z}$ which is $\mathbb{Z}$-linear, positive, multiplicative, and normalized, note that

$$\delta(h_2) + \delta(e_2) = \delta(h_2 + e_2) = \delta(\rho^2) = \delta(\rho)^2 = 1^2 = 1$$

and hence positivity implies that either $\delta(h_2) = 0$ or $\delta(e_2) = 0$. Assume the latter holds, and we will show that $\delta = \delta_h$.

Given any σ in $\Sigma \cap A_n \setminus \{h_n\}$, note that $e_2^\perp\sigma \neq 0$ by Theorem 3.3.1(b), and hence $0 \neq (e_2^\perp\sigma, \rho^{n-2}) = (\sigma, e_2\rho^{n-2})$. Thus σ is a constituent of $e_2\rho^{n-2}$, so positivity implies

$$0 \leq \delta(\sigma) \leq \delta(e_2\rho^{n-2}) = \delta(e_2)\delta(\rho^{n-2}) = 0.$$

Thus $\delta(\sigma) = 0$ for σ in $\Sigma \cap A_n \setminus \{h_n\}$. Since $\delta(\rho^n) = \delta(\rho)^n = 1^n = 1$, this forces $\delta(h_n) = 1$, for each $n \geq 0$ (including $n = 0$, as $1 = \delta(\rho) = \delta(\rho \cdot 1) = \delta(\rho)\delta(1) = 1 \cdot \delta(1) = \delta(1)$). Thus $\delta = \delta_h$. The argument when $\delta(h_2) = 0$ showing $\delta = \delta_e$ is symmetric. □

Proof of Theorem 3.3.3. Many of the assertions of parts (e) and (f) will come from constructing the unique nontrivial PSH-automorphism ω of A from the antipode S: for homogeneous a in A_n, define $\omega(a) := (-1)^n S(a)$. We now study some of the properties of S and ω.

Notice that A is of finite type (as shown in the proof of Theorem 3.3.1). Thus, A^o is a graded Hopf algebra isomorphic to A.

Since A is a PSH, it is commutative by Theorem 3.1.7 (applied to $A \otimes_{\mathbb{Z}} \mathbb{Q}$). This implies both that S is an algebra endomorphism by Proposition 1.4.10 (since Exercise 1.5.8(a) shows that the algebra anti-endomorphisms of a commutative algebra are the same as its algebra endomorphisms), and that $S^2 = \mathrm{id}_A$ by Corollary 1.4.12. Thus, ω is an algebra endomorphism and satisfies $\omega^2 = \mathrm{id}_A$.

Since A is self-dual and the defining diagram (1.4.3) satisfied by the antipode S is sent to itself when one replaces A by A^o and all maps by their adjoints, one concludes that $S = S^*$ (where S^* means the restricted adjoint $S^* : A^o \to A^o$), i.e., S is self-adjoint. Since S is an algebra endomorphism, and $S = S^*$, in fact S is also a coalgebra endomorphism, a bialgebra endomorphism, and a Hopf endomorphism (by Corollary 1.4.27). The same properties are shared by ω.

Since $\mathrm{id}_A = S^2 = SS^*$, one concludes that S is an isometry, and hence so is ω.

Since ρ is primitive, one has $S(\rho) = -\rho$ and $\omega(\rho) = \rho$. Therefore $\omega(\rho^n) = \rho^n$ for $n = 1, 2, \ldots$. Use this as follows to check that ω is a PSH-automorphism, which amounts to checking that every σ in Σ has $\omega(\sigma)$ in Σ:

$$(\omega(\sigma), \omega(\sigma)) = (\sigma, \sigma) = 1$$

so that $\pm\omega(\sigma)$ lies in Σ, but also if σ lies in A_n, then

$$(\omega(\sigma), \rho^n) = (\sigma, \omega(\rho^n)) = (\sigma, \rho^n) > 0.$$

In summary, ω is a PSH-automorphism of A, an isometry, and an involution.

Let us try to determine the action of ω on the $\{h_n\}$. By similar reasoning as in (3.3.3), one has

$$\Delta(h_2) = h_2 \otimes 1 + \rho \otimes \rho + 1 \otimes h_2.$$

Thus $0 = S(h_2) + S(\rho)\rho + h_2$, and combining this with $S(\rho) = -\rho$, one has $S(h_2) = e_2$. Thus also $\omega(h_2) = (-1)^2 S(h_2) = e_2$.

We claim that this forces $\omega(h_n) = e_n$, because $h_2^\perp \omega(h_n) = 0$ via the following calculation: for any a in A one has

$$\begin{aligned}(h_2^\perp \omega(h_n), a) &= (\omega(h_n), h_2 a) \\ &= (h_n, \omega(h_2 a)) \\ &= (h_n, e_2 \omega(a)) \\ &= (e_2^\perp h_n, \omega(a)) = (0, \omega(a)) = 0.\end{aligned}$$

Consequently the involution ω swaps h_n and e_n, while the antipode S has $S(h_n) = (-1)^n e_n$ and $S(e_n) = (-1)^n h_n$. Thus the coproduct formulas in (d) and definition of the antipode S imply the relation (2.4.4) between $\{h_n\}$ and $\{e_n\}$.

This relation (2.4.4) also lets one recursively express the h_n as polynomials with integer coefficients in the $\{e_n\}$, and vice-versa, so that $\{h_n\}$ and $\{e_n\}$ each generate the same $\mathbb{Z}$-subalgebra A' of A. We wish to show that A' exhausts A.

We argue that Lemma 3.3.4 implies that the *Gram matrix* $[(h_\mu, h_\lambda)]_{\mu,\lambda \in \mathrm{Par}_n}$ has determinant ± 1 as follows. Since $\{h_n\}$ and $\{e_n\}$ both generate A', there exists a $\mathbb{Z}$-matrix $(a_{\mu,\lambda})$ expressing $e_{\mu^t} = \sum_\lambda a_{\mu,\lambda} h_\lambda$, and one has

$$[(e_{\mu^t}, h_\lambda)] = [a_{\mu,\lambda}] \cdot [(h_\mu, h_\lambda)]\,.$$

Taking determinants of these three $\mathbb{Z}$-matrices, and using the fact that the determinant on the left is 1 (by (3.3.6)), both determinants on the right must also be ± 1.

Now we will show that every $\sigma \in \Sigma \cap A_n$ lies in A'_n. Uniquely express $\sigma = \sigma' + \sigma''$ in which σ' lies in the $\mathbb{R}$-span $\mathbb{R}A'_n$ and σ'' lies in the real perpendicular space $(\mathbb{R}A'_n)^\perp$ inside $\mathbb{R} \otimes_{\mathbb{Z}} A_n$. One can compute $\mathbb{R}$-coefficients $(c_\mu)_{\mu \in \mathrm{Par}_n}$ that express $\sigma' = \sum_\mu c_\mu h_\mu$ by solving the system

$$\left(\sum_\mu c_\mu h_\mu, h_\lambda \right) = (\sigma, h_\lambda) \text{ for } \lambda \in \mathrm{Par}_n\,.$$

This linear system is governed by the Gram matrix $[(h_\mu, h_\lambda)]_{\mu,\lambda \in \mathrm{Par}_n}$ with determinant ± 1, and its right side has $\mathbb{Z}$-entries since σ, h_λ lie in A. Hence the solution $(c_\mu)_{\mu \in \mathrm{Par}_n}$ will have $\mathbb{Z}$-entries, so σ' lies in A'. Furthermore, $\sigma'' = \sigma - \sigma'$ will lie in A, and hence by the orthogonality of σ', σ'',

$$1 = (\sigma, \sigma) = (\sigma', \sigma') + (\sigma'', \sigma'').$$

One concludes that either $\sigma'' = 0$, or $\sigma' = 0$. The latter cannot occur since it would mean that $\sigma = \sigma''$ is perpendicular to all of A'. But $\rho^n = h_1^n$ lies in A', and $(\sigma, \rho^n) \neq 0$. Thus $\sigma'' = 0$, meaning $\sigma = \sigma'$ lies in A'. This completes the proof of assertion (e). Note that in the process, having shown $\det(h_\mu, h_\lambda)_{\lambda,\mu \in \mathrm{Par}_n} = \pm 1$, one also knows that $\{h_\lambda\}_{\lambda \in \mathrm{Par}_n}$ are $\mathbb{Z}$-linearly independent, so that $\{h_1, h_2, \ldots\}$ are algebraically independent[208], and $A = \mathbb{Z}[h_1, h_2, \ldots]$ is the polynomial algebra generated by $\{h_1, h_2, \ldots\}$.

For assertion (f), we have seen that ω gives such a PSH-automorphism $A \to A$, swapping $h_n \leftrightarrow e_n$. Conversely, given a PSH-automorphism $A \xrightarrow{\varphi} A$, consider the positive, multiplicative, normalized $\mathbb{Z}$-linear map $\delta := \delta_h \circ \varphi : A \to \mathbb{Z}$. Proposition 3.3.5 shows that either

[208] by Exercise 2.2.14(c)

- $\delta = \delta_h$, which then forces $\varphi(h_n) = h_n$ for all n, so $\varphi = \mathrm{id}_A$, or
- $\delta = \delta_e$, which then forces $\varphi(e_n) = h_n$ for all n, so $\varphi = \omega$.

For assertion (g), given a PSH A with PSH-basis Σ having exactly one primitive ρ, since we have seen $A = \mathbb{Z}[h_1, h_2, \ldots]$, where h_n in A is as defined in Theorem 3.3.1, one can uniquely define an algebra morphism $A \xrightarrow{\varphi} \Lambda$ that sends the element h_n to the complete homogeneous symmetric function $h_n(\mathbf{x})$. Assertions (d) and (e) show that φ is a bialgebra isomorphism, and hence it is a Hopf isomorphism. To show that it is a PSH-isomorphism, we first note that it is an isometry because one can iterate Proposition 2.8.2(iv) together with assertions (c) and (d) to compute all inner products

$$(h_\mu, h_\lambda)_A = (1, h_\mu^\perp h_\lambda)_A = (1, h_{\mu_1}^\perp h_{\mu_2}^\perp \cdots (h_{\lambda_1} h_{\lambda_2} \cdots))_A$$

for μ, λ in Par_n. Hence

$$(h_\mu, h_\lambda)_A = (h_\mu(\mathbf{x}), h_\lambda(\mathbf{x}))_\Lambda = (\varphi(h_\mu), \varphi(h_\lambda))_\Lambda.$$

Once one knows φ is an isometry, then elements ω in $\Sigma \cap A_n$ are characterized in terms of the form $(\cdot, \cdot)$ by $(\omega, \omega) = 1$ and $(\omega, \rho^n) > 0$. Hence φ sends each σ in Σ to a Schur function s_λ, and is a PSH-isomorphism. $\square$

4. Complex representations for $\mathfrak{S}_n$, wreath products, $GL_n(\mathbb{F}_q)$

After reviewing the basics that we will need from representation and character theory of finite groups, we give Zelevinsky's three main examples of PSH's arising as spaces of virtual characters for three towers of finite groups:

- *symmetric* groups,
- their *wreath products* with any finite group, and
- the finite *general linear* groups.

Much in this chapter traces its roots to Zelevinsky's book [227]. The results concerning the symmetric groups, however, are significantly older and spread across the literature: see, e.g., [206, §7.18], [73, §7.3], [142, §I.7], [186, §4.7], [113], for proofs using different tools.

4.1. **Review of complex character theory.** We shall now briefly discuss some basics of representation (and character) theory that will be used below. A good source for this material, including the crucial Mackey formula, is Serre [197, Chaps. 1-7].[209]

4.1.1. *Basic definitions, Maschke, Schur.* For a group G, a *representation of* G is a homomorphism $G \xrightarrow{\varphi} GL(V)$ for some vector space V over a field. We will take the field to be $\mathbb{C}$ from now on, and we will also assume that V is finite-dimensional over $\mathbb{C}$. Thus a representation of G is the same as a finite-dimensional (left) $\mathbb{C}G$-module V. (We use the notations $\mathbb{C}G$ and $\mathbb{C}[G]$ synonymously for the group algebra of G over $\mathbb{C}$. More generally, if S is a set, then $\mathbb{C}S = \mathbb{C}[S]$ denotes the free $\mathbb{C}$-module with basis S.)

We also assume that G is finite, so that Maschke's Theorem[210] says that $\mathbb{C}G$ is semisimple, meaning that every $\mathbb{C}G$-module $U \subset V$ has a $\mathbb{C}G$-module complement U' with $V = U \oplus U'$. Equivalently, *indecomposable* $\mathbb{C}G$-modules are the same thing as *simple* (=*irreducible*) $\mathbb{C}G$-modules.

Schur's Lemma implies that for two simple $\mathbb{C}G$-modules V_1, V_2, one has

$$\mathrm{Hom}_{\mathbb{C}G}(V_1, V_2) \cong \begin{cases} \mathbb{C}, & \text{if } V_1 \cong V_2; \\ 0, & \text{if } V_1 \ncong V_2. \end{cases}$$

4.1.2. *Characters and Hom spaces.* A $\mathbb{C}G$-module V is completely determined up to isomorphism by its *character*

$$\begin{array}{ccc} G & \xrightarrow{\chi_V} & \mathbb{C}, \\ g & \longmapsto & \chi_V(g) := \mathrm{trace}(g : V \to V). \end{array}$$

This character χ_V is a *class function*, meaning it is constant on G-conjugacy classes. The space $R_{\mathbb{C}}(G)$ of class functions $G \to \mathbb{C}$ has a Hermitian, positive definite form

$$(f_1, f_2)_G := \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

For any two $\mathbb{C}G$-modules V_1, V_2,

$$(\chi_{V_1}, \chi_{V_2})_G = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}G}(V_1, V_2). \tag{4.1.1}$$

The set of all *irreducible characters*

$$\mathrm{Irr}(G) = \{\chi_V : V \text{ is a simple } \mathbb{C}G\text{-module}\}$$

forms an orthonormal basis of $R_{\mathbb{C}}(G)$ with respect to this form, and spans a $\mathbb{Z}$-sublattice

$$R(G) := \mathbb{Z}\,\mathrm{Irr}(G) \subset R_{\mathbb{C}}(G)$$

sometimes called the *virtual characters* of G. For every $\mathbb{C}G$-module V, the character χ_V belongs to $R(G)$.

Instead of working with the Hermitian form $(\cdot,\cdot)_G$ on G, we could also (and some authors do) define a $\mathbb{C}$-bilinear form $\langle \cdot, \cdot \rangle_G$ on $R_{\mathbb{C}}(G)$ by

$$\langle f_1, f_2 \rangle_G := \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1}).$$

---

[209] More advanced treatments of representation theory can be found in [222] and [69].

[210] ... which has a beautiful generalization to finite-dimensional Hopf algebras due to Larson and Sweedler; see Montgomery [157, §2.2].

This form is not identical with $(\cdot,\cdot)_G$ (indeed, $\langle\cdot,\cdot\rangle_G$ is bilinear while $(\cdot,\cdot)_G$ is Hermitian), but it still satisfies (4.1.1), and thus is identical with $(\cdot,\cdot)_G$ on $R(G)\times R(G)$. Hence, for all we are going to do until Section 4.9, we could just as well use the form $\langle\cdot,\cdot\rangle_G$ instead of $(\cdot,\cdot)_G$.

4.1.3. *Tensor products.* Given two groups G_1, G_2 and $\mathbb{C}G_i$-modules V_i for $i=1,2$, their tensor product $V_1\otimes_{\mathbb{C}} V_2$ becomes a $\mathbb{C}[G_1\times G_2]$-module via $(g_1,g_2)(v_1\otimes v_2)=g_1(v_1)\otimes g_2(v_2)$. This module is called the *(outer) tensor product* of V_1 and V_2. When V_1, V_2 are both simple, then so is $V_1\otimes V_2$, and every simple $\mathbb{C}[G_1\times G_2]$-module arises this way (with V_1 and V_2 determined uniquely up to isomorphism).[211] Thus one has identifications and isomorphisms

$$\begin{aligned}\operatorname{Irr}(G_1\times G_2)&=\operatorname{Irr}(G_1)\times\operatorname{Irr}(G_2),\\ R(G_1\times G_2)&\cong R(G_1)\otimes_{\mathbb{Z}} R(G_2);\end{aligned}$$

here, $\chi_{V_1}\otimes\chi_{V_2}\in R(G_1)\otimes_{\mathbb{Z}} R(G_2)$ is being identified with $\chi_{V_1\otimes V_2}\in R(G_1\times G_2)$ for all $\mathbb{C}G_1$-modules V_1 and all $\mathbb{C}G_2$-modules V_2. The latter isomorphism is actually a restriction of the isomorphism $R_{\mathbb{C}}(G_1\times G_2)\cong R_{\mathbb{C}}(G_1)\otimes_{\mathbb{C}} R_{\mathbb{C}}(G_2)$ under which every pure tensor $\phi_1\otimes\phi_2\in R_{\mathbb{C}}(G_1)\otimes_{\mathbb{C}} R_{\mathbb{C}}(G_2)$ corresponds to the class function $G_1\times G_2\to\mathbb{C},\ (g_1,g_2)\mapsto\phi_1(g_1)\otimes\phi_2(g_2)$.

Given two $\mathbb{C}G_1$-modules V_1 and W_1 and two $\mathbb{C}G_2$-modules V_2 and W_2, we have

$$(\chi_{V_1\otimes V_2},\chi_{W_1\otimes W_2})_{G_1\times G_2}=(\chi_{V_1},\chi_{W_1})_{G_1}(\chi_{V_2},\chi_{W_2})_{G_2}. \tag{4.1.2}$$

4.1.4. *Induction and restriction.* Given a subgroup $H<G$ and $\mathbb{C}H$-module U, one can use the fact that $\mathbb{C}G$ is a $(\mathbb{C}G,\mathbb{C}H)$-bimodule to form the *induced* $\mathbb{C}G$*-module*

$$\operatorname{Ind}_H^G U:=\mathbb{C}G\otimes_{\mathbb{C}H}U.$$

The fact that $\mathbb{C}G$ is free as a (right-)$\mathbb{C}H$-module[212] on basis elements $\{t_g\}_{gH\in G/H}$ makes this tensor product easy to analyze. For example one can compute its character

$$\chi_{\operatorname{Ind}_H^G U}(g)=\frac{1}{|H|}\sum_{\substack{k\in G:\\ kgk^{-1}\in H}}\chi_U(kgk^{-1}). \tag{4.1.3}$$

[213] One can also recognize when a $\mathbb{C}G$-module V is isomorphic to $\operatorname{Ind}_H^G U$ for some $\mathbb{C}H$-module U: this happens if and only if there is an H-stable subspace $U\subset V$ having the property that $V=\bigoplus_{gH\in G/H} gU$.

The above construction of a $\mathbb{C}G$-module $\operatorname{Ind}_H^G U$ corresponding to any $\mathbb{C}H$-module U is part of a functor Ind_H^G from the category of $\mathbb{C}H$-modules to the category of $\mathbb{C}G$-modules[214]; this functor is called *induction*.

Besides induction on $\mathbb{C}H$-modules, one can define induction on class functions of H:

Exercise 4.1.1. Let G be a finite group, and H a subgroup of G. Let $f\in R_{\mathbb{C}}(H)$ be a class function. We define the *induction* $\operatorname{Ind}_H^G f$ of f to be the function $G\to\mathbb{C}$ given by

$$\left(\operatorname{Ind}_H^G f\right)(g)=\frac{1}{|H|}\sum_{\substack{k\in G:\\ kgk^{-1}\in H}} f\left(kgk^{-1}\right)\qquad\text{for all } g\in G. \tag{4.1.4}$$

(a) Prove that this induction $\operatorname{Ind}_H^G f$ is a class function on G, hence belongs to $R_{\mathbb{C}}(G)$.

(b) Let J be a system of right coset[215] representatives for $H\backslash G$, so that $G=\bigsqcup_{j\in J} Hj$. Prove that

$$\left(\operatorname{Ind}_H^G f\right)(g)=\sum_{\substack{j\in J:\\ jgj^{-1}\in H}} f\left(jgj^{-1}\right)\qquad\text{for all } g\in G.$$

---

[211] This is proven in [197, §3.2, Thm. 10]. The fact that $\mathbb{C}$ is algebraically closed is essential for this!

[212] ... which also has a beautiful generalization to finite-dimensional Hopf algebras due to Nichols and Zoeller; see [157, §3.1].

[213] See [197, §7.2, Prop. 20(ii)] for the proof of this equality. (Another proof is given in [69, Remark 5.9.2 (the Remark after Theorem 4.32 in the arXiv version)], but [69] uses a different definition of $\operatorname{Ind}_H^G U$; see Remark 4.1.5 for why it is equivalent to ours. Yet another proof of (4.1.3) is given in Exercise 4.1.14(k).)

[214] On morphisms, it sends any $f: U\to U'$ to $\mathrm{id}_{\mathbb{C}G}\otimes_{\mathbb{C}H} f:\mathbb{C}G\otimes_{\mathbb{C}H}U\to\mathbb{C}G\otimes_{\mathbb{C}H}U'$.

[215] A *right coset* of a subgroup H in a group G is defined to be a subset of G having the form Hj for some $j\in G$. Similarly, a *left coset* has the form jH for some $j\in G$.

The induction Ind_H^G defined in Exercise 4.1.1 is a $\mathbb{C}$-linear map $R_{\mathbb{C}}(H) \to R_{\mathbb{C}}(G)$. Since every $\mathbb{C}H$-module U satisfies

$$\chi_{\operatorname{Ind}_H^G U} = \operatorname{Ind}_H^G(\chi_U) \tag{4.1.5}$$

[216], this $\mathbb{C}$-linear map Ind_H^G restricts to a $\mathbb{Z}$-linear map $R(H) \to R(G)$ (also denoted Ind_H^G) which sends the character χ_U of any $\mathbb{C}H$-module U to the character $\chi_{\operatorname{Ind}_H^G U}$ of the induced $\mathbb{C}G$-module $\operatorname{Ind}_H^G U$.

Exercise 4.1.2. Let G, H and I be three finite groups such that $I < H < G$. Let U be a $\mathbb{C}I$-module. Prove that $\operatorname{Ind}_H^G \operatorname{Ind}_I^H U \cong \operatorname{Ind}_I^G U$. (This fact is often referred to as the *transitivity of induction*.)

Exercise 4.1.3. Let G_1 and G_2 be two groups. Let $H_1 < G_1$ and $H_2 < G_2$ be two subgroups. Let U_1 be a $\mathbb{C}H_1$-module, and U_2 be a $\mathbb{C}H_2$-module. Show that

$$\operatorname{Ind}_{H_1 \times H_2}^{G_1 \times G_2}(U_1 \otimes U_2) \cong \left(\operatorname{Ind}_{H_1}^{G_1} U_1\right) \otimes \left(\operatorname{Ind}_{H_2}^{G_2} U_2\right) \tag{4.1.6}$$

as $\mathbb{C}[G_1 \times G_2]$-modules.

The *restriction* operation $V \mapsto \operatorname{Res}_H^G V$ restricts a $\mathbb{C}G$-module V to a $\mathbb{C}H$-module. *Frobenius reciprocity* asserts the adjointness between Ind_H^G and Res_H^G

$$\operatorname{Hom}_{\mathbb{C}G}(\operatorname{Ind}_H^G U, V) \cong \operatorname{Hom}_{\mathbb{C}H}(U, \operatorname{Res}_H^G V), \tag{4.1.7}$$

as a special case ($S = A = \mathbb{C}G, R = \mathbb{C}H, B = U, C = V$) of the general *adjoint associativity*

$$\operatorname{Hom}_S(A \otimes_R B, C) \cong \operatorname{Hom}_R(B, \operatorname{Hom}_S(A, C)) \tag{4.1.8}$$

for S, R two rings, A an (S, R)-bimodule, B a left R-module, C a left S-module.

We can define not just the restriction of a $\mathbb{C}G$-module, but also the *restriction of a class function* $f \in R_{\mathbb{C}}(G)$. When H is a subgroup of G, the restriction $\operatorname{Res}_H^G f$ of an $f \in R_{\mathbb{C}}(G)$ is defined as the result of restricting the map $f : G \to \mathbb{C}$ to H. This $\operatorname{Res}_H^G f$ is easily seen to belong to $R_{\mathbb{C}}(H)$, and so Res_H^G is a $\mathbb{C}$-linear map $R_{\mathbb{C}}(G) \to R_{\mathbb{C}}(H)$. This map restricts to a $\mathbb{Z}$-linear map $R(G) \to R(H)$, since we have $\operatorname{Res}_H^G \chi_V = \chi_{\operatorname{Res}_H^G V}$ for any $\mathbb{C}G$-module V. Taking characters in (4.1.7) (and recalling $\operatorname{Res}_H^G \chi_V = \chi_{\operatorname{Res}_H^G V}$ and (4.1.5)), we obtain

$$(\operatorname{Ind}_H^G \chi_U, \chi_V)_G = (\chi_U, \operatorname{Res}_H^G \chi_V)_H. \tag{4.1.9}$$

By bilinearity, this yields the equality

$$\left(\operatorname{Ind}_H^G \alpha, \beta\right)_G = \left(\alpha, \operatorname{Res}_H^G \beta\right)_H$$

for any class functions $\alpha \in R_{\mathbb{C}}(H)$ and $\beta \in R_{\mathbb{C}}(G)$ (since $R(G)$ spans $R_{\mathbb{C}}(G)$ as a $\mathbb{C}$-vector space).

Exercise 4.1.4. Let G be a finite group, and let $H < G$. Let U be a $\mathbb{C}H$-module. If A and B are two algebras, P is a (B, A)-bimodule and Q is a left B-module, then $\operatorname{Hom}_B(P, Q)$ is a left A-module (since $\mathbb{C}G$ is a $(\mathbb{C}H, \mathbb{C}G)$-bimodule). As a consequence, $\operatorname{Hom}_{\mathbb{C}H}(\mathbb{C}G, U)$ is a $\mathbb{C}G$-module. Prove that this $\mathbb{C}G$-module is isomorphic to $\operatorname{Ind}_H^G U$.

Remark 4.1.5. Some texts *define* the induction $\operatorname{Ind}_H^G U$ of a $\mathbb{C}H$-module U to be $\operatorname{Hom}_{\mathbb{C}H}(\mathbb{C}G, U)$ (rather than to be $\mathbb{C}G \otimes_{\mathbb{C}H} U$, as we did).[217] As Exercise 4.1.4 shows, this definition is equivalent to ours as long as G is finite (but not otherwise).

Exercise 4.1.4 yields the following "wrong-way" version of Frobenius reciprocity:

Exercise 4.1.6. Let G be a finite group; let $H < G$. Let U be a $\mathbb{C}G$-module, and let V be a $\mathbb{C}H$-module. Prove that $\operatorname{Hom}_{\mathbb{C}G}\left(U, \operatorname{Ind}_H^G V\right) \cong \operatorname{Hom}_{\mathbb{C}H}\left(\operatorname{Res}_H^G U, V\right)$.

[216] This follows by comparing the value of $\chi_{\operatorname{Ind}_H^G U}(g)$ obtained from (4.1.3) with the value of $\left(\operatorname{Ind}_H^G(\chi_U)\right)(g)$ found using (4.1.4).

[217] Or they define it as a set of morphisms of H-sets from G to U (this is how [69, Def. 5.8.1 (Def. 4.28 in the arXiv version)] defines it); this is easily seen to be equivalent to $\operatorname{Hom}_{\mathbb{C}H}(\mathbb{C}G, U)$.

4.1.5. *Mackey's formula.* Mackey gave an alternate description of a module which has been induced and then restricted. To state it, for a subgroup $H < G$ and g in G, let $H^g := g^{-1}Hg$ and ${}^gH := gHg^{-1}$. Given a $\mathbb{C}H$-module U, say defined by a homomorphism $H \xrightarrow{\varphi} GL(U)$, let U^g denote the $\mathbb{C}[gHg^{-1}]$-module on the same $\mathbb{C}$-vector space U defined by the composite homomorphism

$$\begin{array}{ccccc} {}^gH & \longrightarrow & H & \xrightarrow{\varphi} & GL(U), \\ h & \longmapsto & g^{-1}hg. & & \end{array}$$

Theorem 4.1.7. *(Mackey's formula) Consider subgroups $H, K < G$, and any $\mathbb{C}H$-module U. If $\{g_1, \ldots, g_t\}$ are double coset representatives for $K\backslash G/H$, then*

$$\mathrm{Res}^G_K \mathrm{Ind}^G_H U \cong \bigoplus_{i=1}^{t} \mathrm{Ind}^K_{{}^{g_i}H \cap K} \left(\left(\mathrm{Res}^H_{H \cap K^{g_i}} U \right)^{g_i} \right).$$

Proof. In this proof, all tensor product symbols $\otimes$ should be interpreted as $\otimes_{\mathbb{C}H}$. Recall $\mathbb{C}G$ has $\mathbb{C}$-basis $\{t_g\}_{g \in G}$. For subsets $S \subset G$, let $\mathbb{C}[S]$ denote the $\mathbb{C}$-span of $\{t_g\}_{g \in S}$ in $\mathbb{C}G$.

Note that each double coset KgH gives rise to a sub-(K, H)-bimodule $\mathbb{C}[KgH]$ within $\mathbb{C}G$, and one has a $\mathbb{C}K$-module direct sum decomposition

$$\mathrm{Ind}^G_H U = \mathbb{C}G \otimes U = \bigoplus_{i=1}^{t} \mathbb{C}[Kg_iH] \otimes U.$$

Hence it suffices to check for any element g in G that

$$\mathbb{C}[KgH] \otimes U \cong \mathrm{Ind}^K_{{}^gH \cap K} \left(\left(\mathrm{Res}^H_{H \cap K^g} U \right)^g \right).$$

Note that ${}^gH \cap K$ is the subgroup of K consisting of the elements k in K for which $kgH = gH$. Hence by picking $\{k_1, \ldots, k_s\}$ to be coset representatives for $K/({}^gH \cap K)$, one disjointly decomposes the double coset

$$KgH = \bigsqcup_{j=1}^{s} k_j({}^gH \cap K)gH,$$

giving a $\mathbb{C}$-vector space direct sum decomposition

$$\begin{aligned} \mathbb{C}[KgH] \otimes U &= \bigoplus_{j=1}^{s} \mathbb{C}\left[k_j \left({}^gH \cap K\right) gH\right] \otimes U \\ &\cong \mathrm{Ind}^K_{{}^gH \cap K} \left(\mathbb{C}[({}^gH \cap K)\, gH] \otimes U\right). \end{aligned}$$

So it remains to check that one has a $\mathbb{C}[{}^gH \cap K]$-module isomorphism

$$\mathbb{C}[({}^gH \cap K)\, gH] \otimes U \cong \left(\mathrm{Res}^H_{H \cap K^g} U\right)^g.$$

Bearing in mind that, for each k in ${}^gH \cap K$ and h in H, one has $g^{-1}kg$ in H and hence

$$t_{kgh} \otimes u = t_g \cdot t_{g^{-1}kg \cdot h} \otimes u = t_g \otimes g^{-1}kgh \cdot u,$$

one sees that this isomorphism can be defined by mapping

$$t_{kgh} \otimes u \longmapsto g^{-1}kgh \cdot u.$$

□

4.1.6. *Inflation and fixed points.* There are two (adjoint) constructions on representations that apply when one has a normal subgroup $K \triangleleft G$. Given a $\mathbb{C}[G/K]$-module U, say defined by the homomorphism $G/K \xrightarrow{\varphi} GL(U)$, the *inflation* of U to a $\mathbb{C}G$-module $\mathrm{Infl}^G_{G/K} U$ has the same underlying space U, and is defined by the composite homomorphism $G \to G/K \xrightarrow{\varphi} GL(U)$. We will later use the easily-checked fact that when $H < G$ is any other subgroup, one has

$$\mathrm{Res}^G_H \mathrm{Infl}^G_{G/K} U = \mathrm{Infl}^H_{H/H \cap K} \mathrm{Res}^{G/K}_{H/H \cap K} U. \tag{4.1.10}$$

(We regard $H/H \cap K$ as a subgroup of G/K, since the canonical homomorphism $H/H \cap K \to G/K$ is injective.)

Inflation turns out to be adjoint to the *K-fixed space construction* sending a $\mathbb{C}G$-module V to the $\mathbb{C}[G/K]$-module

$$V^K := \{v \in V : k(v) = v \text{ for } k \in K\}.$$

Note that V^K is indeed a G-stable subspace: for any v in V^K and g in G, one has that $g(v)$ lies in V^K since an element k in K satisfies $kg(v) = g \cdot g^{-1}kg(v) = g(v)$ as $g^{-1}kg$ lies in K. One has this adjointness

$$\operatorname{Hom}_{\mathbb{C}G}(\operatorname{Infl}_{G/K}^G U, V) = \operatorname{Hom}_{\mathbb{C}[G/K]}(U, V^K), \tag{4.1.11}$$

because any $\mathbb{C}G$-module homomorphism φ on the left must have the property that $k\varphi(u) = \varphi(k(u)) = \varphi(u)$ for all k in K, so that φ actually lies on the right.

We will also need the following formula for the character χ_{V^K} in terms of the character χ_V:

$$\chi_{V^K}(gK) = \frac{1}{|K|} \sum_{k \in K} \chi_V(gk). \tag{4.1.12}$$

To see this, note that when one has a $\mathbb{C}$-linear endomorphism φ on a space V that preserves some $\mathbb{C}$-subspace $W \subset V$, if $V \xrightarrow{\pi} W$ is any idempotent projection onto W, then the trace of the restriction $\varphi|_W$ equals the trace of $\varphi \circ \pi$ on V. Applying this to $W = V^K$ and $\varphi = g$, with $\pi = \frac{1}{|K|}\sum_{k \in K} k$, gives (4.1.12).[218]

Another way to restate (4.1.12) is:

$$\chi_{V^K}(gK) = \frac{1}{|K|} \sum_{h \in gK} \chi_V(h). \tag{4.1.13}$$

Inflation and K-fixed space construction can also be defined on class functions. For inflation, this is particularly easy: Inflation $\operatorname{Infl}_{G/K}^G f$ of an $f \in R_{\mathbb{C}}(G/K)$ is defined as the composition $G \twoheadrightarrow G/K \xrightarrow{f} \mathbb{C}$. This is a class function of G and thus lies in $R_{\mathbb{C}}(G)$. Thus, inflation $\operatorname{Infl}_{G/K}^G$ is a $\mathbb{C}$-linear map $R_{\mathbb{C}}(G/K) \to R_{\mathbb{C}}(G)$. It restricts to a $\mathbb{Z}$-linear map $R(G/K) \to R(G)$, since it is clear that every $\mathbb{C}(G/K)$-module U satisfies $\operatorname{Infl}_{G/K}^G \chi_U = \chi_{\operatorname{Infl}_{G/K}^G U}$.

We can also use (4.1.12) (or (4.1.13)) as inspiration for defining a "K-fixed space construction" on class functions. Explicitly, for every class function $f \in R_{\mathbb{C}}(G)$, we define a class function $f^K \in R_{\mathbb{C}}(G/K)$ by

$$f^K(gK) = \frac{1}{|K|} \sum_{k \in K} f(gk) = \frac{1}{|K|} \sum_{h \in gK} f(h).$$

The map $(\cdot)^K : R_{\mathbb{C}}(G) \to R_{\mathbb{C}}(G/K),\ f \mapsto f^K$ is $\mathbb{C}$-linear, and restricts to a $\mathbb{Z}$-linear map $R(G) \to R(G/K)$. Again, we have a compatibility with the K-fixed point construction on modules: We have $\chi_{V^K} = (\chi_V)^K$ for every $\mathbb{C}G$-module V.

Taking characters in (4.1.11), we obtain

$$(\operatorname{Infl}_{G/K}^G \chi_U, \chi_V)_G = (\chi_U, \chi_V^K)_{G/K} \tag{4.1.14}$$

for any $\mathbb{C}[G/K]$-module U and any $\mathbb{C}G$-module V (since $\chi_{\operatorname{Infl}_{G/K}^G U} = \operatorname{Infl}_{G/K}^G \chi_U$ and $\chi_{V^K} = (\chi_V)^K$). By $\mathbb{Z}$-linearity, this implies that

$$\left(\operatorname{Infl}_{G/K}^G \alpha, \beta\right)_G = \left(\alpha, \beta^K\right)_{G/K}$$

for any class functions $\alpha \in R_{\mathbb{C}}(G/K)$ and $\beta \in R_{\mathbb{C}}(G)$.

There is also an analogue of (4.1.6):

Lemma 4.1.8. *Let G_1 and G_2 be two groups, and $K_1 < G_1$ and $K_2 < G_2$ be two respective subgroups. Let U_i be a $\mathbb{C}G_i$-module for each $i \in \{1, 2\}$. Then,*

$$(U_1 \otimes U_2)^{K_1 \times K_2} = U_1^{K_1} \otimes U_2^{K_2} \tag{4.1.15}$$

(as subspaces of $U_1 \otimes U_2$).

[218] For another proof of (4.1.12), see Exercise 4.1.14(l).

Proof. The subgroup $K_1 = K_1 \times 1$ of $G_1 \times G_2$ acts on $U_1 \otimes U_2$, and its fixed points are $(U_1 \otimes U_2)^{K_1} = U_1^{K_1} \otimes U_2$ (because for a $\mathbb{C}K_1$-module, tensoring with U_2 is the same as taking a direct power, which clearly commutes with taking fixed points). Similarly, $(U_1 \otimes U_2)^{K_2} = U_1 \otimes U_2^{K_2}$. Now,

$$(U_1 \otimes U_2)^{K_1 \times K_2} = (U_1 \otimes U_2)^{K_1} \cap (U_1 \otimes U_2)^{K_2} = \left(U_1^{K_1} \otimes U_2\right) \cap \left(U_1 \otimes U_2^{K_2}\right) = U_1^{K_1} \otimes U_2^{K_2}$$

according to the known linear-algebraic fact stating that if P and Q are subspaces of two vector spaces U and V, respectively, then $(P \otimes V) \cap (U \otimes Q) = P \otimes Q$. □

Exercise 4.1.9. (a) Let G_1 and G_2 be two groups. Let V_i and W_i be finite-dimensional $\mathbb{C}G_i$-modules for every $i \in \{1, 2\}$. Prove that the $\mathbb{C}$-linear map

$$\operatorname{Hom}_{\mathbb{C}G_1}(V_1, W_1) \otimes \operatorname{Hom}_{\mathbb{C}G_2}(V_2, W_2) \to \operatorname{Hom}_{\mathbb{C}[G_1 \times G_2]}(V_1 \otimes V_2, W_1 \otimes W_2)$$

sending each tensor $f \otimes g$ to the tensor product $f \otimes g$ of homomorphisms is a vector space isomorphism.

(b) Use part (a) to give a new proof of (4.1.2).

As an aside, (4.1.10) has a "dual" analogue:

Exercise 4.1.10. Let G be a finite group, and let $K \lhd G$ and $H < G$. Let U be a $\mathbb{C}H$-module. As usual, regard $H/(H \cap K)$ as a subgroup of G/K. Show that $\left(\operatorname{Ind}_H^G U\right)^K \cong \operatorname{Ind}_{H/(H\cap K)}^{G/K}\left(U^{H\cap K}\right)$ as $\mathbb{C}[G/K]$-modules.

Inflation also "commutes" with induction:

Exercise 4.1.11. Let G be a finite group, and let $K < H < G$ be such that $K \lhd G$. Thus, automatically, $K \lhd H$, and we regard the quotient H/K as a subgroup of G/K. Let V be a $\mathbb{C}[H/K]$-module. Show that $\operatorname{Infl}_{G/K}^G \operatorname{Ind}_{H/K}^{G/K} V \cong \operatorname{Ind}_H^G \operatorname{Infl}_{H/K}^H V$ as $\mathbb{C}G$-modules.

Exercise 4.1.12. Let G be a finite group, and let $K \lhd G$. Let V be a $\mathbb{C}G$-module. Let $I_{V,K}$ denote the $\mathbb{C}$-vector subspace of V spanned by all elements of the form $v - kv$ for $k \in K$ and $v \in V$.

(a) Show that $I_{V,K}$ is a $\mathbb{C}G$-submodule of V.

(b) Let V_K denote the quotient $\mathbb{C}G$-module $V/I_{V,K}$. (This module is occasionally called the *K-coinvariant module of V*, a name it sadly shares with at least two other non-equivalent constructions in algebra.) Show that $V_K \cong \operatorname{Infl}_{G/K}^G\left(V^K\right)$ as $\mathbb{C}G$-modules. (Use $\operatorname{char}\mathbb{C} = 0$.)

In the remainder of this subsection, we shall briefly survey generalized notions of induction and restriction, defined in terms of a group homomorphism ρ rather than in terms of a group G and a subgroup H. These generalized notions (defined by van Leeuwen in [128, §2.2]) will not be used in the rest of these notes, but they shed some new light on the facts about induction, restriction, inflation and fixed point construction discussed above. (In particular, they reveal that some of said facts have common generalizations.)

The reader might have noticed that the definitions of inflation and of restriction (both for characters and for modules) are similar. In fact, they both are particular cases of the following construction:

Remark 4.1.13. Let G and H be two finite groups, and let $\rho : H \to G$ be a group homomorphism.

- If $f \in R_{\mathbb{C}}(G)$, then the *ρ-restriction* $\operatorname{Res}_\rho f$ of f is defined as the map $f \circ \rho : H \to \mathbb{C}$. This map is easily seen to belong to $R_{\mathbb{C}}(H)$.
- If V is a $\mathbb{C}G$-module, then the *ρ-restriction* $\operatorname{Res}_\rho V$ of V is the $\mathbb{C}H$-module with ground space V and action given by

$$h \cdot v = \rho(h) \cdot v \qquad \text{for every } h \in H \text{ and } v \in V.$$

This construction generalizes both inflation and restriction: If H is a subgroup of G, and if $\rho : H \to G$ is the inclusion map, then $\operatorname{Res}_\rho f = \operatorname{Res}_H^G f$ (for any $f \in R_{\mathbb{C}}(G)$) and $\operatorname{Res}_\rho V = \operatorname{Res}_H^G V$ (for any $\mathbb{C}G$-module V). If, instead, we have $G = H/K$ for a normal subgroup K of H, and if $\rho : H \to G$ is the projection map, then $\operatorname{Res}_\rho f = \operatorname{Infl}_{H/K}^H f$ (for any $f \in R_{\mathbb{C}}(H/K)$) and $\operatorname{Res}_\rho V = \operatorname{Infl}_{H/K}^H V$ (for any $\mathbb{C}[H/K]$-module V).

A subtler observation is that induction and fixed point construction can be generalized by a common notion. This is the subject of Exercise 4.1.14 below.

Exercise 4.1.14. Let G and H be two finite groups, and let $\rho : H \to G$ be a group homomorphism. We introduce the following notations:

- If $f \in R_{\mathbb{C}}(H)$, then the *ρ-induction* $\operatorname{Ind}_\rho f$ of f is a map $G \to \mathbb{C}$ which is defined as follows:

$$(\operatorname{Ind}_\rho f)(g) = \frac{1}{|H|} \sum_{\substack{(h,k) \in H \times G; \\ k\rho(h)k^{-1} = g}} f(h) \qquad \text{for every } g \in G.$$

- If U is a $\mathbb{C}H$-module, then the *ρ-induction* $\operatorname{Ind}_\rho U$ of U is defined as the $\mathbb{C}G$-module $\mathbb{C}G \otimes_{\mathbb{C}H} U$, where $\mathbb{C}G$ is regarded as a $(\mathbb{C}G, \mathbb{C}H)$-bimodule according to the following rule: The left $\mathbb{C}G$-module structure on $\mathbb{C}G$ is plain multiplication inside $\mathbb{C}G$; the right $\mathbb{C}H$-module structure on $\mathbb{C}G$ is induced by the $\mathbb{C}$-algebra homomorphism $\mathbb{C}[\rho] : \mathbb{C}H \to \mathbb{C}G$ (thus, it is explicitly given by $\gamma\eta = \gamma \cdot (\mathbb{C}[\rho])\,\eta$ for all $\gamma \in \mathbb{C}G$ and $\eta \in \mathbb{C}H$).

Prove the following properties of this construction:

(a) For every $f \in R_{\mathbb{C}}(H)$, we have $\operatorname{Ind}_\rho f \in R_{\mathbb{C}}(G)$.

(b) For any finite-dimensional $\mathbb{C}H$-module U, we have $\chi_{\operatorname{Ind}_\rho U} = \operatorname{Ind}_\rho \chi_U$.

(c) If H is a subgroup of G, and if $\rho : H \to G$ is the inclusion map, then $\operatorname{Ind}_\rho f = \operatorname{Ind}_H^G f$ for every $f \in R_{\mathbb{C}}(H)$.

(d) If H is a subgroup of G, and if $\rho : H \to G$ is the inclusion map, then $\operatorname{Ind}_\rho U = \operatorname{Ind}_H^G U$ for every $\mathbb{C}H$-module U.

(e) If $G = H/K$ for some normal subgroup K of H, and if $\rho : H \to G$ is the projection map, then $\operatorname{Ind}_\rho f = f^K$ for every $f \in R_{\mathbb{C}}(H)$.

(f) If $G = H/K$ for some normal subgroup K of H, and if $\rho : H \to G$ is the projection map, then $\operatorname{Ind}_\rho U \cong U^K$ for every $\mathbb{C}H$-module U.

(g) Any class functions $\alpha \in R_{\mathbb{C}}(H)$ and $\beta \in R_{\mathbb{C}}(G)$ satisfy

$$(\operatorname{Ind}_\rho \alpha, \beta)_G = (\alpha, \operatorname{Res}_\rho \beta)_H \tag{4.1.16}$$

and

$$\langle \operatorname{Ind}_\rho \alpha, \beta \rangle_G = \langle \alpha, \operatorname{Res}_\rho \beta \rangle_H . \tag{4.1.17}$$

(See Remark 4.1.13 for the definition of $\operatorname{Res}_\rho \beta$.)

(h) We have $\operatorname{Hom}_{\mathbb{C}G}(\operatorname{Ind}_\rho U, V) \cong \operatorname{Hom}_{\mathbb{C}H}(U, \operatorname{Res}_\rho V)$ for every $\mathbb{C}H$-module U and every $\mathbb{C}G$-module V. (See Remark 4.1.13 for the definition of $\operatorname{Res}_\rho V$.)

(i) Similarly to how we made $\mathbb{C}G$ into a $(\mathbb{C}G, \mathbb{C}H)$-bimodule, let us make $\mathbb{C}G$ into a $(\mathbb{C}H, \mathbb{C}G)$-bimodule (so the right $\mathbb{C}G$-module structure is plain multiplication inside $\mathbb{C}G$, whereas the left $\mathbb{C}H$-module structure is induced by the $\mathbb{C}$-algebra homomorphism $\mathbb{C}[\rho] : \mathbb{C}H \to \mathbb{C}G$). If U is any $\mathbb{C}H$-module, then the $\mathbb{C}G$-module $\operatorname{Hom}_{\mathbb{C}H}(\mathbb{C}G, U)$ (defined as in Exercise 4.1.4 using the $(\mathbb{C}H, \mathbb{C}G)$-bimodule structure on $\mathbb{C}G$) is isomorphic to $\operatorname{Ind}_\rho U$.

(j) We have $\operatorname{Hom}_{\mathbb{C}G}(U, \operatorname{Ind}_\rho V) \cong \operatorname{Hom}_{\mathbb{C}H}(\operatorname{Res}_\rho U, V)$ for every $\mathbb{C}G$-module U and every $\mathbb{C}H$-module V. (See Remark 4.1.13 for the definition of $\operatorname{Res}_\rho V$.)

Furthermore:

(k) Use the above to prove the formula (4.1.3).

(l) Use the above to prove the formula (4.1.12).

[**Hint:** Part (b) of this exercise is hard. To solve it, it is useful to have a way of computing the trace of a linear operator without knowing a basis of the vector space it is acting on. There is a way to do this using a "finite dual generating system", which is a somewhat less restricted notion than that of a basis[219]. Try to create a finite dual generating system for $\operatorname{Ind}_\rho U$ from one for U (and from the group G), and then use it to compute $\chi_{\operatorname{Ind}_\rho U}$.

[219] More precisely: Let $\mathbb{K}$ be a field, and V be a $\mathbb{K}$-vector space. A *finite dual generating system* for V means a triple $(I, (a_i)_{i \in I}, (f_i)_{i \in I})$, where

- I is a finite set;
- $(a_i)_{i \in I}$ is a family of elements of V;
- $(f_i)_{i \in I}$ is a family of elements of V^* (where V^* means $\operatorname{Hom}_{\mathbb{K}}(V, \mathbb{K})$)

such that every $v \in V$ satisfies $v = \sum_{i \in I} f_i(v)\, a_i$. For example, if $(e_j)_{j \in J}$ is a finite basis of the vector space V, and if $\left(e_j^*\right)_{j \in J}$ is the basis of V^* dual to this basis $(e_j)_{j \in J}$, then $\left(J, (e_j)_{j \in J}, \left(e_j^*\right)_{j \in J}\right)$ is a finite dual generating system for V; however, most finite dual generating systems are not obtained this way.

The solution of part (i) is a modification of the solution of Exercise 4.1.4, but complicated by the fact that H is no longer (necessarily) a subgroup of G. Part (f) can be solved by similar arguments, or using part (i), or using Exercise 4.1.12(b).]

The result of Exercise 4.1.14(h) generalizes (4.1.7) (because of Exercise 4.1.14(d)), but also generalizes (4.1.11) (due to Exercise 4.1.14(f)). Similarly, Exercise 4.1.14(g) generalizes both (4.1.9) and (4.1.14). Similarly, Exercise 4.1.14(i) generalizes Exercise 4.1.4, and Exercise 4.1.14(j) generalizes Exercise 4.1.6.

Similarly, Exercise 4.1.3 is generalized by the following exercise:

Exercise 4.1.15. Let G_1, G_2, H_1 and H_2 be four finite groups. Let $\rho_1 : H_1 \to G_1$ and $\rho_2 : H_2 \to G_2$ be two group homomorphisms. These two homomorphisms clearly induce a group homomorphism $\rho_1 \times \rho_2 : H_1 \times H_2 \to G_1 \times G_2$. Let U_1 be a $\mathbb{C}H_1$-module, and U_2 be a $\mathbb{C}H_2$-module. Show that

$$\operatorname{Ind}_{\rho_1 \times \rho_2} (U_1 \otimes U_2) \cong (\operatorname{Ind}_{\rho_1} U_1) \otimes (\operatorname{Ind}_{\rho_2} U_2)$$

as $\mathbb{C}[G_1 \times G_2]$-modules.

The Ind_ρ and Res_ρ operators behave "functorially" with respect to composition. Here is what this means:

Exercise 4.1.16. Let G, H and I be three finite groups. Let $\rho : H \to G$ and $\tau : I \to H$ be two group homomorphisms.

(a) We have $\operatorname{Ind}_\rho \operatorname{Ind}_\tau U \cong \operatorname{Ind}_{\rho\circ\tau} U$ for every $\mathbb{C}I$-module U.
(b) We have $\operatorname{Ind}_\rho \operatorname{Ind}_\tau f = \operatorname{Ind}_{\rho\circ\tau} f$ for every $f \in R_{\mathbb{C}}(I)$.
(c) We have $\operatorname{Res}_\tau \operatorname{Res}_\rho V = \operatorname{Res}_{\rho\circ\tau} V$ for every $\mathbb{C}G$-module V.
(d) We have $\operatorname{Res}_\tau \operatorname{Res}_\rho f = \operatorname{Res}_{\rho\circ\tau} f$ for every $f \in R_{\mathbb{C}}(G)$.

Exercise 4.1.16(a), of course, generalizes Exercise 4.1.2.

4.1.7. *Semidirect products.* Recall that a *semidirect product* is a group $G \ltimes K$ having two subgroups G, K with

- $K \lhd (G \ltimes K)$ is a normal subgroup,
- $G \ltimes K = GK = KG$, and
- $G \cap K = \{e\}$.

In this setting one has two interesting adjoint constructions, applied in Section 4.5.

Proposition 4.1.17. *Fix a $\mathbb{C}[G \ltimes K]$-module V.*

(i) *For any $\mathbb{C}G$-module U, one has $\mathbb{C}[G \ltimes K]$-module structure*

$$\Phi(U) := U \otimes V,$$

determined via

$$k(u \otimes v) = u \otimes k(v),$$
$$g(u \otimes v) = g(u) \otimes g(v).$$

(ii) *For any $\mathbb{C}[G \ltimes K]$-module W, one has $\mathbb{C}G$-module structure*

$$\Psi(W) := \operatorname{Hom}_{\mathbb{C}K}(\operatorname{Res}_K^{G\ltimes K} V, \operatorname{Res}_K^{G\ltimes K} W),$$

determined via $g(\varphi) = g \circ \varphi \circ g^{-1}$.

(iii) *The maps*

$$\mathbb{C}G - \text{mods} \underset{\Psi}{\overset{\Phi}{\rightleftharpoons}} \mathbb{C}[G \ltimes K] - \text{mods}$$

The crucial observation is now that if $\left(I, (a_i)_{i\in I}, (f_i)_{i\in I}\right)$ is a finite dual generating system for a vector space V, and if T is an endomorphism of V, then

$$\operatorname{trace} T = \sum_{i\in I} f_i(Ta_i).$$

Prove this!

are adjoint in the sense that one has an isomorphism

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{C}G}(U, \Psi(W)) & \longrightarrow & \mathrm{Hom}_{\mathbb{C}[G\ltimes K]}(\Phi(U), W) \\ \| & & \| \\ \mathrm{Hom}_{\mathbb{C}G}(U, \mathrm{Hom}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V, \mathrm{Res}^{G\ltimes K}_K W)) & & \mathrm{Hom}_{\mathbb{C}[G\ltimes K]}(U\otimes V, W), \\ \varphi & \longmapsto & \overline{\varphi}(u\otimes v) := \varphi(u)(v). \end{array}$$

(iv) *One has a $\mathbb{C}G$-module isomorphism*

$$(\Psi\circ\Phi)(U) \cong U \otimes \mathrm{End}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V).$$

In particular, if $\mathrm{Res}^{G\ltimes K}_K V$ is a simple $\mathbb{C}K$-module, then $(\Psi\circ\Phi)(U)\cong U$.

Proof. These are mostly straightforward exercises in the definitions. To check assertion (iv), for example, note that K acts only in the right tensor factor in $\mathrm{Res}^{G\ltimes K}_K(U\otimes V)$, and hence as $\mathbb{C}G$-modules one has

$$\begin{aligned} (\Psi\circ\Phi)(U) &= \mathrm{Hom}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V,\ \mathrm{Res}^{G\ltimes K}_K(U\otimes V)) \\ &= \mathrm{Hom}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V,\ U\otimes \mathrm{Res}^{G\ltimes K}_K V) \\ &= U\otimes \mathrm{Hom}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V,\ \mathrm{Res}^{G\ltimes K}_K V) \\ &= U\otimes \mathrm{End}_{\mathbb{C}K}(\mathrm{Res}^{G\ltimes K}_K V). \end{aligned}$$

□

4.2. **Three towers of groups.** Here we consider three towers of groups

$$G_* = (G_0 < G_1 < G_2 < G_3 < \cdots)$$

where either

- $G_n = \mathfrak{S}_n$, the *symmetric group*[220], or
- $G_n = \mathfrak{S}_n[\Gamma]$, the *wreath product* of the symmetric group with some arbitrary finite group Γ, or
- $G_n = GL_n(\mathbb{F}_q)$, the finite general linear group[221].

Here the wreath product $\mathfrak{S}_n[\Gamma]$ can be thought of informally as the group of *monomial* $n\times n$ matrices whose nonzero entries lie in Γ, that is, $n\times n$ matrices having exactly one nonzero entry in each row and column, and that entry is an element of Γ. E.g.

$$\begin{bmatrix} 0 & g_2 & 0 \\ g_1 & 0 & 0 \\ 0 & 0 & g_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & g_6 \\ 0 & g_5 & 0 \\ g_4 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & g_2g_5 & 0 \\ 0 & 0 & g_1g_6 \\ g_3g_4 & 0 & 0 \end{bmatrix}.$$

More formally, $\mathfrak{S}_n[\Gamma]$ is the semidirect product $\mathfrak{S}_n \ltimes \Gamma^n$ in which $\mathfrak{S}_n$ acts on Γ^n via $\sigma(\gamma_1,\ldots,\gamma_n) = (\gamma_{\sigma^{-1}(1)},\ldots,\gamma_{\sigma^{-1}(n)})$.

For each of the three towers G_*, there are embeddings $G_i\times G_j \hookrightarrow G_{i+j}$ and we introduce maps $\mathrm{ind}^{i+j}_{i,j}$ taking $\mathbb{C}[G_i\times G_j]$-modules to $\mathbb{C}G_{i+j}$-modules, as well as maps $\mathrm{res}^{i+j}_{i,j}$ carrying modules in the reverse direction which are adjoint:

$$\mathrm{Hom}_{\mathbb{C}G_{i+j}}(\mathrm{ind}^{i+j}_{i,j} U, V) = \mathrm{Hom}_{\mathbb{C}[G_i\times G_j]}(U, \mathrm{res}^{i+j}_{i,j} V). \tag{4.2.1}$$

Definition 4.2.1. For $G_n = \mathfrak{S}_n$, one embeds $\mathfrak{S}_i\times\mathfrak{S}_j$ into $\mathfrak{S}_{i+j}$ as the permutations that permute $\{1,2,\ldots,i\}$ and $\{i+1,i+2,\ldots,i+j\}$ separately. Here one defines

$$\begin{aligned} \mathrm{ind}^{i+j}_{i,j} &:= \mathrm{Ind}^{\mathfrak{S}_{i+j}}_{\mathfrak{S}_i\times\mathfrak{S}_j}, \\ \mathrm{res}^{i+j}_{i,j} &:= \mathrm{Res}^{\mathfrak{S}_{i+j}}_{\mathfrak{S}_i\times\mathfrak{S}_j}. \end{aligned}$$

[220]The symmetric group $\mathfrak{S}_0$ is the group of all permutations of the empty set $\{1,2,\ldots,0\} = \varnothing$. It is a trivial group. (Note that $\mathfrak{S}_1$ is also a trivial group.)

[221]The group $GL_0(\mathbb{F}_q)$ is a trivial group, consisting of the empty 0×0 matrix.

For $G_n = \mathfrak{S}_n[\Gamma]$, similarly embed $\mathfrak{S}_i[\Gamma] \times \mathfrak{S}_j[\Gamma]$ into $\mathfrak{S}_{i+j}[\Gamma]$ as block monomial matrices whose two diagonal blocks have sizes i, j respectively, and define

$$\begin{aligned} \mathrm{ind}_{i,j}^{i+j} &:= \mathrm{Ind}_{\mathfrak{S}_i[\Gamma]\times\mathfrak{S}_j[\Gamma]}^{\mathfrak{S}_{i+j}[\Gamma]}, \\ \mathrm{res}_{i,j}^{i+j} &:= \mathrm{Res}_{\mathfrak{S}_i[\Gamma]\times\mathfrak{S}_j[\Gamma]}^{\mathfrak{S}_{i+j}[\Gamma]}. \end{aligned}$$

For $G_n = GL_n(\mathbb{F}_q)$, which we will denote just GL_n, similarly embed $GL_i \times GL_j$ into GL_{i+j} as block diagonal matrices whose two diagonal blocks have sizes i, j respectively. However, one also introduces as an intermediate the *parabolic subgroup* $P_{i,j}$ consisting of the block upper-triangular matrices of the form

$$\begin{bmatrix} g_i & \ell \\ 0 & g_j \end{bmatrix}$$

where g_i, g_j lie in GL_i, GL_j, respectively, and ℓ in $\mathbb{F}_q^{i\times j}$ is arbitrary. One has a quotient map $P_{i,j} \to GL_i \times GL_j$ whose kernel $K_{i,j}$ is the set of matrices of the form

$$\begin{bmatrix} I_i & \ell \\ 0 & I_j \end{bmatrix}$$

with ℓ again arbitrary. Here one defines

$$\begin{aligned} \mathrm{ind}_{i,j}^{i+j} &:= \mathrm{Ind}_{P_{i,j}}^{GL_{i+j}} \mathrm{Infl}_{GL_i\times GL_j}^{P_{i,j}}, \\ \mathrm{res}_{i,j}^{i+j} &:= \left(\mathrm{Res}_{P_{i,j}}^{GL_{i+j}}(-)\right)^{K_{i,j}}. \end{aligned}$$

In the case $G_n = GL_n$, the operation $\mathrm{ind}_{i,j}^{i+j}$ is sometimes called *parabolic induction* or *Harish-Chandra induction*. The operation $\mathrm{res}_{i,j}^{i+j}$ is essentially just the $K_{i,j}$-fixed point construction $V \mapsto V^{K_{i,j}}$. However writing it as the above two-step composite makes it more obvious, (via (4.1.7) and (4.1.11)) that $\mathrm{res}_{i,j}^{i+j}$ is again adjoint to $\mathrm{ind}_{i,j}^{i+j}$.

Definition 4.2.2. For each of the three towers G_*, define a graded $\mathbb{Z}$-module

$$A := A(G_*) = \bigoplus_{n\geq 0} R(G_n)$$

with a bilinear form $(\cdot,\cdot)_A$ whose restriction to $A_n := R(G_n)$ is the usual form $(\cdot,\cdot)_{G_n}$, and such that $\Sigma := \bigsqcup_{n\geq 0} \mathrm{Irr}(G_n)$ gives an orthonormal $\mathbb{Z}$-basis. Notice that $A_0 = \mathbb{Z}$ has its basis element 1 equal to the unique irreducible character of the trivial group G_0.

Bearing in mind that $A_n = R(G_n)$ and

$$A_i \otimes A_j = R(G_i) \otimes R(G_j) \cong R(G_i \times G_j),$$

one then has candidates for product and coproduct defined by

$$\begin{aligned} m := \mathrm{ind}_{i,j}^{i+j} : \quad A_i \otimes A_j &\longrightarrow A_{i+j}, \\ \Delta := \textstyle\bigoplus_{i+j=n} \mathrm{res}_{i,j}^{i+j} : \quad A_n &\longrightarrow \textstyle\bigoplus_{i+j=n} A_i \otimes A_j. \end{aligned}$$

The coassociativity of Δ is an easy consequence of transitivity of the constructions of restriction and fixed points[222]. We could derive the associativity of m from the transitivity of induction and inflation, but this would be more complicated[223]; we will instead prove it differently.

[222] More precisely, using this transitivity, it is easily reduced to proving that $K_{i+j,k} \cdot (K_{i,j} \times \{I_k\}) = K_{i,j+k} \cdot (\{I_i\} \times K_{j,k})$ (an equality between subgroups of GL_{i+j+k}) for any three nonnegative integers i, j, k. But this equality can be proven by realizing that both of its sides equal the set of all block matrices of the form $\begin{pmatrix} I_i & \ell & \ell' \\ 0 & I_j & \ell'' \\ 0 & 0 & I_k \end{pmatrix}$ with ℓ, ℓ' and ℓ'' being matrices of sizes $i \times j$, $i \times k$ and $j \times k$, respectively.

[223] See Exercise 4.3.11(c) for such a derivation.

We first show that the maps m and Δ are adjoint with respect to the forms $(\cdot,\cdot)_A$ and $(\cdot,\cdot)_{A\otimes A}$. In fact, if U, V, W are modules over $\mathbb{C}G_i$, $\mathbb{C}G_j$, $\mathbb{C}G_{i+j}$, respectively, then we can write the $\mathbb{C}[G_i \times G_j]$-module $\operatorname{res}_{i,j}^{i+j} W$ as a direct sum $\bigoplus_k X_k \otimes Y_k$ with X_k being $\mathbb{C}G_i$-modules and Y_k being $\mathbb{C}G_j$-modules; we then have

$$\operatorname{res}_{i,j}^{i+j} \chi_W = \sum_k \chi_{X_k} \otimes \chi_{Y_k} \tag{4.2.2}$$

and

$$\begin{aligned}
(m(\chi_U \otimes \chi_V), \chi_W)_A &= \left(\operatorname{ind}_{i,j}^{i+j}(\chi_{U\otimes V}), \chi_W\right)_A = \left(\operatorname{ind}_{i,j}^{i+j}(\chi_{U\otimes V}), \chi_W\right)_{G_{i+j}} \\
&= \left(\chi_{U\otimes V}, \operatorname{res}_{i,j}^{i+j}\chi_W\right)_{G_i\times G_j} = \left(\chi_{U\otimes V}, \sum_k \chi_{X_k}\otimes\chi_{Y_k}\right)_{G_i\times G_j} \\
&= \sum_k (\chi_{U\otimes V}, \chi_{X_k\otimes Y_k})_{G_i\times G_j} = \sum_k (\chi_U, \chi_{X_k})_{G_i}(\chi_V, \chi_{Y_k})_{G_j}
\end{aligned}$$

(the third equality sign follows by taking dimensions in (4.2.1) and recalling (4.1.1); the fourth equality sign follows from (4.2.2); the sixth one follows from (4.1.2)) and

$$\begin{aligned}
(\chi_U \otimes \chi_V, \Delta(\chi_W))_{A\otimes A} &= \left(\chi_U\otimes\chi_V, \operatorname{res}_{i,j}^{i+j}\chi_W\right)_{A\otimes A} = \left(\chi_U\otimes\chi_V, \sum_k \chi_{X_k}\otimes\chi_{Y_k}\right)_{A\otimes A} \\
&= \sum_k (\chi_U, \chi_{X_k})_A (\chi_V, \chi_{Y_k})_A = \sum_k (\chi_U, \chi_{X_k})_{G_i}(\chi_V, \chi_{Y_k})_{G_j}
\end{aligned}$$

(the first equality sign follows by removing all terms in $\Delta(\chi_W)$ whose scalar product with $\chi_U \otimes \chi_V$ vanishes for reasons of gradedness; the second equality sign follows from (4.2.2)), which in comparison yield $(m(\chi_U \otimes \chi_V), \chi_W)_A = (\chi_U \otimes \chi_V, \Delta(\chi_W))_{A\otimes A}$, thus showing that m and Δ are adjoint maps. Therefore, m is associative (since Δ is coassociative).

Endowing $A = \bigoplus_{n\geq 0} R(G_n)$ with the obvious unit and counit maps, it thus becomes a graded, finite-type $\mathbb{Z}$-algebra and $\mathbb{Z}$-coalgebra.

The next section addresses the issue of why they form a bialgebra. However, assuming this for the moment, it should be clear that each of these algebras A is a PSH having $\Sigma = \bigsqcup_{n\geq 0} \operatorname{Irr}(G_n)$ as its PSH-basis. Σ is self-dual because m, Δ are defined by adjoint maps, and it is positive because m, Δ take irreducible representations to genuine representations not just virtual ones, and hence have characters which are nonnegative sums of irreducible characters.

Exercise 4.2.3. Let i, j and k be three nonnegative integers. Let U be a $\mathbb{C}\mathfrak{S}_i$-module, let V be a $\mathbb{C}\mathfrak{S}_j$-module, and let W be a $\mathbb{C}\mathfrak{S}_k$-module. Show that there are canonical $\mathbb{C}[\mathfrak{S}_i \times \mathfrak{S}_j \times \mathfrak{S}_k]$-module isomorphisms

$$\begin{aligned}
\operatorname{Ind}_{\mathfrak{S}_{i+j}\times\mathfrak{S}_k}^{\mathfrak{S}_{i+j+k}} \left(\operatorname{Ind}_{\mathfrak{S}_i\times\mathfrak{S}_j}^{\mathfrak{S}_{i+j}} (U\otimes V)\otimes W\right) &\cong \operatorname{Ind}_{\mathfrak{S}_i\times\mathfrak{S}_j\times\mathfrak{S}_k}^{\mathfrak{S}_{i+j+k}} (U\otimes V\otimes W) \\
&\cong \operatorname{Ind}_{\mathfrak{S}_i\times\mathfrak{S}_{j+k}}^{\mathfrak{S}_{i+j+k}} \left(U\otimes \operatorname{Ind}_{\mathfrak{S}_j\times\mathfrak{S}_k}^{\mathfrak{S}_{j+k}} (V\otimes W)\right).
\end{aligned}$$

(Similar statements hold for the other two towers of groups and their respective ind functors, although the one for the GL_* tower is harder to prove. See Exercise 4.3.11(a) for a more general result.)

4.3. **Bialgebra and double cosets.** To show that the algebra and coalgebras $A = A(G_*)$ are bialgebras, the central issue is checking the pentagonal diagram in (1.3.4), that is, as maps $A \otimes A \to A \otimes A$, one has

$$\Delta \circ m = (m\otimes m)\circ(\mathrm{id}\otimes T\otimes \mathrm{id})\circ(\Delta\otimes\Delta). \tag{4.3.1}$$

In checking this, it is convenient to have a lighter notation for various subgroups of the groups G_n corresponding to compositions α.

Definition 4.3.1. (a) An *almost-composition* is a (finite) tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ of nonnegative integers. Its *length* is defined to be ℓ and denoted by $\ell(\alpha)$; its *size* is defined to be $\alpha_1 + \alpha_2 + \cdots + \alpha_\ell$ and denoted by $|\alpha|$; its *parts* are its entries $\alpha_1, \alpha_2, \ldots, \alpha_\ell$. The almost-compositions of size n are called the *almost-compositions of* n.

(b) A *composition* is a finite tuple of positive integers. Of course, any composition is an almost-composition, and so all notions defined for almost-compositions (like size and length) make sense for compositions.

Note that any partition of n (written without trailing zeroes) is a composition of n. We write $\varnothing$ (and sometimes, sloppily, (0), when there is no danger of mistaking it for the almost-composition (0)) for the empty composition ().

Definition 4.3.2. Given an almost-composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ of n, define a subgroup

$$G_\alpha \cong G_{\alpha_1} \times \cdots \times G_{\alpha_\ell} < G_n$$

via the block-diagonal embedding with diagonal blocks of sizes $(\alpha_1, \ldots, \alpha_\ell)$. This G_α is called a *Young subgroup* $\mathfrak{S}_\alpha$ when $G_n = \mathfrak{S}_n$, and a *Levi subgroup* when $G_n = GL_n$. In the case when $G_n = \mathfrak{S}_n[\Gamma]$, we also denote G_α by $\mathfrak{S}_\alpha[\Gamma]$. In the case where $G_n = GL_n$, also define the *parabolic subgroup* P_α to be the subgroup of G_n consisting of block-upper triangular matrices whose diagonal blocks have sizes $(\alpha_1, \ldots, \alpha_\ell)$, and let K_α be the kernel of the obvious surjection $P_\alpha \to G_\alpha$ which sends a block upper-triangular matrix to the tuple of its diagonal blocks whose sizes are $\alpha_1, \alpha_2, \ldots, \alpha_\ell$. Notice that $P_{(i,j)} = P_{i,j}$ for any i and j with $i + j = n$; similarly, $K_{(i,j)} = K_{i,j}$ for any i and j with $i + j = n$. We will also abbreviate $G_{(i,j)} = G_i \times G_j$ by $G_{i,j}$.

When $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ is an almost-composition, we abbreviate $G_{(\alpha_1, \alpha_2, \ldots, \alpha_\ell)}$ by $G_{\alpha_1, \alpha_2, \ldots, \alpha_\ell}$ (and similarly for the P's).

Definition 4.3.3. Let K and H be two groups, $\tau : K \to H$ a group homomorphism, and U a $\mathbb{C}H$-module. Then, U^τ is defined as the $\mathbb{C}K$-module with ground space U and action given by $k \cdot u = \tau(k) \cdot u$ for all $k \in K$ and $u \in U$. [224] This very simple construction generalizes the definition of U^g for an element $g \in G$, where G is a group containing H as a subgroup; in fact, in this situation we have $U^g = U^\tau$, where $K = {}^gH$ and $\tau : K \to H$ is the map $k \mapsto g^{-1}kg$.

Using homogeneity, checking the bialgebra condition (4.3.1) in the homogeneous component $(A \otimes A)_n$ amounts to the following: for each pair of representations U_1, U_2 of G_{r_1}, G_{r_2} with $r_1 + r_2 = n$, and for each (c_1, c_2) with $c_1 + c_2 = n$, one must verify that

$$\begin{aligned} &\operatorname{res}^n_{c_1,c_2}\left(\operatorname{ind}^n_{r_1,r_2}(U_1 \otimes U_2)\right) \\ &\quad\cong \bigoplus_A \left(\operatorname{ind}^{c_1}_{a_{11},a_{21}} \otimes \operatorname{ind}^{c_2}_{a_{12},a_{22}}\right)\left(\left(\operatorname{res}^{r_1}_{a_{11},a_{12}} U_1 \otimes \operatorname{res}^{r_2}_{a_{21},a_{22}} U_2\right)^{\tau_A^{-1}}\right) \end{aligned} \tag{4.3.2}$$

where the direct sum is over all matrices $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ in $\mathbb{N}^{2\times 2}$ with row sums (r_1, r_2) and column sums (c_1, c_2), and where τ_A is the obvious isomorphism between the subgroups

$$\begin{aligned} &G_{a_{11},a_{12},a_{21},a_{22}} \quad (< G_{r_1,r_2}) \qquad \text{and} \\ &G_{a_{11},a_{21},a_{12},a_{22}} \quad (< G_{c_1,c_2}) \end{aligned} \tag{4.3.3}$$

(we are using the inverse τ_A^{-1} of this isomorphism τ_A to identify modules for the first subgroup with modules for the second subgroup, according to Definition 4.3.3).

As one might guess, (4.3.2) comes from the Mackey formula (Theorem 4.1.7), once one identifies the appropriate double coset representatives. This is just as easy to do in a slightly more general setting.

Definition 4.3.4. Given almost-compositions α, β of n having lengths ℓ, m and a matrix A in $\mathbb{N}^{\ell\times m}$ with row sums α and column sums β, define a permutation w_A in $\mathfrak{S}_n$ as follows. Disjointly decompose $[n] = \{1, 2, \ldots, n\}$ into consecutive intervals of numbers

$$[n] = I_1 \sqcup \cdots \sqcup I_\ell \qquad \text{such that } |I_i| = \alpha_i$$

(so the smallest α_1 elements of $[n]$ go into I_1, the next-smallest α_2 elements of $[n]$ go into I_2, and so on). Likewise, disjointly decompose $[n]$ into consecutive intervals of numbers

$$[n] = J_1 \sqcup \cdots \sqcup J_m \qquad \text{such that } |J_j| = \beta_j.$$

[224] We have already met this $\mathbb{C}K$-module U^τ in Remark 4.1.13, where it was called $\operatorname{Res}_\tau U$.

For every $j \in [m]$, disjointly decompose J_j into consecutive intervals of numbers $J_j = J_{j,1} \sqcup J_{j,2} \sqcup \cdots \sqcup J_{j,\ell}$ such that every $i \in [\ell]$ satisfies $|J_{j,i}| = a_{ij}$. For every $i \in [\ell]$, disjointly decompose I_i into consecutive intervals of numbers $I_i = I_{i,1} \sqcup I_{i,2} \sqcup \cdots \sqcup I_{i,m}$ such that every $j \in [m]$ satisfies $|I_{i,j}| = a_{ij}$. Now, for every $i \in [\ell]$ and $j \in [m]$, let $\pi_{i,j}$ be the increasing bijection from $J_{j,i}$ to $I_{i,j}$ (this is well-defined since these two sets both have cardinality a_{ij}). The disjoint union of these bijections $\pi_{i,j}$ over all i and j is a bijection $[n] \to [n]$ (since the disjoint union of the sets $J_{j,i}$ over all i and j is $[n]$, and so is the disjoint union of the sets $I_{i,j}$), that is, a permutation of $[n]$; this permutation is what we call w_A.

Example 4.3.5. Taking $n = 9$ and $\alpha = (4, 5), \beta = (3, 4, 2)$, one has

$$\begin{array}{ccc} I_1 = \{1,2,3,4\}, & I_2 = \{5,6,7,8,9\}, & \\ J_1 = \{1,2,3\}, & J_2 = \{4,5,6,7\}, & J_3 = \{8,9\}. \end{array}$$

Then one possible matrix A having row and column sums α, β is $A = \begin{bmatrix} 2 & 2 & 0 \\ 1 & 2 & 2 \end{bmatrix}$, and its associated permutation w_A written in two-line notation is

$$\begin{pmatrix} 1 & 2 & 3 & | & 4 & 5 & 6 & 7 & | & 8 & 9 \\ \underline{1} & \underline{2} & \underline{\underline{5}} & | & \underline{3} & \underline{4} & \underline{\underline{6}} & \underline{\underline{7}} & | & \underline{\underline{8}} & \underline{\underline{9}} \end{pmatrix}$$

with vertical lines dividing the sets J_j on top, and with elements of I_i underlined i times on the bottom.

Remark 4.3.6. Given almost-compositions α and β of n having lengths ℓ and m, and a permutation $w \in \mathfrak{S}_n$. It is easy to see that there exists a matrix $A \in \mathbb{N}^{\ell \times m}$ satisfying $w_A = w$ if and only if the restriction of w to each J_j and the restriction of w^{-1} to each I_i are increasing. In this case, the matrix A is determined by $a_{ij} = |w(J_j) \cap I_i|$.

Among our three towers G_* of groups, the symmetric group tower ($G_n = \mathfrak{S}_n$) is the simplest one. We will now see that it also embeds into the two others, in the sense that $\mathfrak{S}_n$ embeds into $\mathfrak{S}_n[\Gamma]$ for every Γ and into $GL_n(\mathbb{F}_q)$ for every q.

First, for every $n \in \mathbb{N}$ and any group Γ, we embed the group $\mathfrak{S}_n$ into $\mathfrak{S}_n[\Gamma]$ by means of the canonical embedding $\mathfrak{S}_n \to \mathfrak{S}_n \ltimes \Gamma^n = \mathfrak{S}_n[\Gamma]$. If we regard elements of $\mathfrak{S}_n[\Gamma]$ as $n \times n$ monomial matrices with nonzero entries in Γ, then this boils down to identifying every $\pi \in \mathfrak{S}_n$ with the permutation matrix of π (in which the 1's are read as the neutral element of Γ). If α is an almost-composition of n, then this embedding $\mathfrak{S}_n \to \mathfrak{S}_n[\Gamma]$ makes the subgroup $\mathfrak{S}_\alpha$ of $\mathfrak{S}_n$ become a subgroup of $\mathfrak{S}_n[\Gamma]$, more precisely a subgroup of $\mathfrak{S}_\alpha[\Gamma] < \mathfrak{S}_n[\Gamma]$.

For every $n \in \mathbb{N}$ and every q, we embed the group $\mathfrak{S}_n$ into $GL_n(\mathbb{F}_q)$ by identifying every permutation $\pi \in \mathfrak{S}_n$ with its permutation matrix in $GL_n(\mathbb{F}_q)$. If α is an almost-composition of n, then this embedding makes the subgroup $\mathfrak{S}_\alpha$ of $\mathfrak{S}_n$ become a subgroup of $GL_n(\mathbb{F}_q)$. If we let $G_n = GL_n(\mathbb{F}_q)$, then $\mathfrak{S}_\alpha < G_\alpha < P_\alpha$.

The embeddings we have just defined commute with the group embeddings $G_n < G_{n+1}$ on both sides.

Proposition 4.3.7. *The permutations $\{w_A\}$, as A runs over all matrices in $\mathbb{N}^{\ell \times m}$ having row sums α and column sums β, give*

(a) *a system of double coset representatives for $\mathfrak{S}_\alpha \backslash \mathfrak{S}_n / \mathfrak{S}_\beta$;*
(b) *a system of double coset representatives for $\mathfrak{S}_\alpha[\Gamma] \backslash \mathfrak{S}_n[\Gamma] / \mathfrak{S}_\beta[\Gamma]$;*
(c) *a system of double coset representatives for $P_\alpha \backslash GL_n / P_\beta$.*

Proof. (a) We give an algorithm to show that every double coset $\mathfrak{S}_\alpha w \mathfrak{S}_\beta$ contains some w_A. Start by altering w within its coset $w\mathfrak{S}_\beta$, that is, by permuting the *positions* within each set J_j, to obtain a representative w' for $w\mathfrak{S}_\beta$ in which each set $w'(J_j)$ appears in increasing order in the second line of the two-line notation for w'. Then alter w' within its coset $\mathfrak{S}_\alpha w'$, that is, by permuting the *values* within each set I_i, to obtain a representative w_A having the elements of each set I_i appearing in increasing order in the second line; because the values within each set I_i are consecutive, this alteration will not ruin the property that one had each set

$w'(J_j)$ appearing in increasing order. For example, one might have

$$w = \begin{pmatrix} 1 & 2 & 3 & | & 4 & 5 & 6 & 7 & | & 8 & 9 \\ \underline{4} & \underline{\underline{8}} & \underline{2} & | & \underline{\underline{5}} & \underline{3} & \underline{\underline{9}} & \underline{1} & | & \underline{\underline{7}} & \underline{\underline{6}} \end{pmatrix},$$

$$w' = \begin{pmatrix} 1 & 2 & 3 & | & 4 & 5 & 6 & 7 & | & 8 & 9 \\ \underline{2} & \underline{4} & \underline{\underline{8}} & | & \underline{1} & \underline{3} & \underline{\underline{5}} & \underline{\underline{9}} & | & \underline{\underline{6}} & \underline{\underline{7}} \end{pmatrix} \in w\mathfrak{S}_\beta,$$

$$w_A = \begin{pmatrix} 1 & 2 & 3 & | & 4 & 5 & 6 & 7 & | & 8 & 9 \\ \underline{1} & \underline{2} & \underline{\underline{5}} & | & \underline{3} & \underline{4} & \underline{\underline{6}} & \underline{\underline{7}} & | & \underline{\underline{8}} & \underline{\underline{9}} \end{pmatrix} \in \mathfrak{S}_\alpha w' \subset \mathfrak{S}_\alpha w' \mathfrak{S}_\beta = \mathfrak{S}_\alpha w \mathfrak{S}_\beta.$$

Next note that $\mathfrak{S}_\alpha w_A \mathfrak{S}_\beta = \mathfrak{S}_\alpha w_B \mathfrak{S}_\beta$ implies $A = B$, since the quantities

$$a_{i,j}(w) := |w(J_j) \cap I_i|$$

are easily seen to be constant on double cosets $\mathfrak{S}_\alpha w \mathfrak{S}_\beta$.

(b) Double coset representatives for $\mathfrak{S}_\alpha \backslash \mathfrak{S}_n / \mathfrak{S}_\beta$ should also provide double coset representatives for $\mathfrak{S}_\alpha[\Gamma] \backslash \mathfrak{S}_n[\Gamma] / \mathfrak{S}_\beta[\Gamma]$, since

$$\mathfrak{S}_\alpha[\Gamma] = \mathfrak{S}_\alpha \Gamma^n = \Gamma^n \mathfrak{S}_\alpha.$$

Thus, part (b) follows from part (a).

(c) In our proof of part (a) above, we showed that $\mathfrak{S}_\alpha w_A \mathfrak{S}_\beta = \mathfrak{S}_\alpha w_B \mathfrak{S}_\beta$ implies $A = B$. A similar argument shows that $P_\alpha w_A P_\beta = P_\alpha w_B P_\beta$ implies $A = B$: for g in GL_n, the rank $r_{ij}(g)$ of the matrix obtained by restricting g to rows $I_i \sqcup I_{i+1} \sqcup \cdots \sqcup I_\ell$ and columns $J_1 \sqcup J_2 \sqcup \cdots \sqcup J_j$ is constant on double cosets $P_\alpha g P_\beta$, and for a permutation matrix w one can recover $a_{i,j}(w)$ from the formula

$$a_{i,j}(w) = r_{i,j}(w) - r_{i,j-1}(w) - r_{i+1,j}(w) + r_{i+1,j-1}(w).$$

Thus it only remains to show that every double coset $P_\alpha g P_\beta$ contains some w_A. Since $\mathfrak{S}_\alpha < P_\alpha$, and we have seen already that every double coset $\mathfrak{S}_\alpha w \mathfrak{S}_\beta$ contains some w_A, it suffices to show that every double coset $P_\alpha g P_\beta$ contains some permutation w. However, we claim that this is already true for the smaller double cosets BgB where $B = P_{1^n}$ is the *Borel subgroup* of upper triangular invertible matrices, that is, one has the usual *Bruhat decomposition*

$$GL_n = \bigsqcup_{w \in \mathfrak{S}_n} BwB.$$

To prove this decomposition, we show how to find a permutation w in each double coset BgB. The freedom to alter g within its coset gB allows one to scale columns and add scalar multiples of earlier columns to later columns. We claim that using such column operations, one can always find a representative g' for coset gB in which

- the bottommost nonzero entry of each column is 1 (call this entry a *pivot*),
- the entries to right of each pivot within its row are all 0, and
- there is one pivot in each row and each column, so that their positions are the positions of the 1's in some permutation matrix w.

In fact, we will see below that $BgB = BwB$ in this case. The algorithm which produces g' from g is simple: starting with the leftmost column, find its bottommost nonzero entry, and scale the column to make this entry a 1, creating the pivot in this column. Now use this pivot to clear out all entries in its row to its right, using column operations that subtract multiples of this column from later columns. Having done this, move on to the next column to the right, and repeat, scaling to create a pivot, and using it to eliminate entries to its right.[225]

[225] To see that this works, we need to check three facts:

(a) We will find a nonzero entry in every column during our algorithm.
(b) Our column operations preserve the zeroes lying to the right of already existing pivots.
(c) Every row contains exactly one pivot at the end of the algorithm.

But fact **(a)** simply says that our matrix can never have an all-zero column during the algorithm; this is clear (since the rank of the matrix remains constant during the algorithm and was n at its beginning). Fact **(b)** holds because all our operations either scale columns (which clearly preserves zero entries) or subtract a multiple of the column c containing the current pivot from a later column d (which will preserve every zero lying to the right of an already existing pivot, because any already existing pivot must lie in a column $b < c$ and therefore both columns c and d have zeroes in its row). Fact **(c)** follows from noticing that

For example, the typical matrix g lying in the double coset BwB where

$$w = \begin{pmatrix} 1 & 2 & 3 & | & 4 & 5 & 6 & 7 & | & 8 & 9 \\ \underline{4} & \underline{\underline{8}} & \underline{2} & | & \underline{\underline{5}} & \underline{3} & \underline{\underline{9}} & \underline{1} & | & \underline{\underline{7}} & \underline{\underline{6}} \end{pmatrix}$$

from before is one that can be altered within its coset gB to look like this:

$$g' = \begin{bmatrix} * & * & * & * & * & * & 1 & 0 & 0 \\ * & * & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ * & * & 0 & * & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & * & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & * & 0 & 0 & 0 & * & 0 & * & 1 \\ 0 & * & 0 & 0 & 0 & * & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \in gB.$$

Having found this g' in gB, a similar algorithm using left multiplication by B shows that w lies in $Bg' \subset Bg'B = BgB$. This time no scalings are required to create the pivot entries: starting with the bottom row, one uses its pivot to eliminate all the entries above it in the same column (shown by stars $*$ above) by adding multiples of the bottom row to higher rows. Then do the same using the pivot in the next-to-bottom row, etc. The result is the permutation matrix for w. □

Remark 4.3.8. The Bruhat decomposition $GL_n = \bigsqcup_{w \in \mathfrak{S}_n} BwB$ is related to the so-called *LPU factorization* – one of a myriad of matrix factorizations appearing in linear algebra.[226] It is actually a fairly general phenomenon, and requires neither the finiteness of $\mathbb{F}$, nor the invertibility, nor even the squareness of the matrices (see Exercise 4.3.9(b) for an analogue holding in a more general setup).

Exercise 4.3.9. Let $\mathbb{F}$ be any field.

(a) For any $n \in \mathbb{N}$ and any $A \in GL_n(\mathbb{F})$, prove that there exist a lower-triangular matrix $L \in GL_n(\mathbb{F})$, an upper-triangular matrix $U \in GL_n(\mathbb{F})$ and a permutation matrix $P \in \mathfrak{S}_n \subset GL_n(\mathbb{F})$ (here, we identify permutations with the corresponding permutation matrices) such that $A = LPU$.

(b) Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $F_{n,m}$ denote the set of all $n \times m$-matrices $B \in \{0,1\}^{n \times m}$ such that each row of B contains at most one 1 and each column of B contains at most one 1. We regard $F_{n,m}$ as a subset of $\mathbb{F}^{n \times m}$ by means of regarding $\{0,1\}$ as a subset of $\mathbb{F}$.

For every $k \in \mathbb{N}$, we let B_k denote the subgroup of $GL_k(\mathbb{F})$ consisting of all upper-triangular matrices.

Prove that

$$\mathbb{F}^{n \times m} = \bigsqcup_{f \in F_{n,m}} B_n f B_m.$$

Corollary 4.3.10. *For each of the three towers of groups G_*, the product and coproduct structures on $A = A(G_*)$ endow it with a bialgebra structure, and hence they form PSH's.*

Proof. The first two towers $G_n = \mathfrak{S}_n$ and $G_n = \mathfrak{S}_n[\Gamma]$ have product, coproduct defined by induction, restriction along embeddings $G_i \times G_j < G_{i+j}$. Hence the desired bialgebra equality (4.3.2) follows from Mackey's Theorem 4.1.7, taking $G = G_n, H = G_{(r_1,r_2)}, K = G_{(c_1,c_2)}, U = U_1 \otimes U_2$ with double coset

there are n pivots altogether at the end of the algorithm, but no row can contain two of them (since the entries to the right of a pivot in its row are 0).

[226] Specifically, an *LPU factorization* of a matrix $A \in GL_n(\mathbb{F})$ (for an arbitrary field $\mathbb{F}$) means a way to write A as a product $A = LPU$ with $L \in GL_n(\mathbb{F})$ being lower-triangular, $U \in GL_n(\mathbb{F})$ being upper-triangular, and $P \in \mathfrak{S}_n \subset GL_n(\mathbb{F})$ being a permutation matrix. Such a factorization always exists (although it is generally not unique). This can be derived from the Bruhat decomposition (see Exercise 4.3.9(a) for a proof). See also [212] for related discussion.

representatives[227]

$$\{g_1, \ldots, g_t\} = \left\{ w_{A^t} \ : \ A \in \mathbb{N}^{2\times 2},\ A \text{ has row sums } (r_1, r_2) \text{ and column sums } (c_1, c_2) \right\}$$

and checking for a given double coset

$$KgH = (G_{c_1,c_2}) w_{A^t} (G_{r_1,r_2})$$

indexed by a matrix A in $\mathbb{N}^{2\times 2}$ with row sums (r_1, r_2) and column sums (c_1, c_2), that the two subgroups appearing on the left in (4.3.3) are exactly

$$H \cap K^{w_{A^t}} = G_{r_1,r_2} \cap (G_{c_1,c_2})^{w_{A^t}},$$
$$^{w_{A^t}}H \cap K = {}^{w_{A^t}}(G_{r_1,r_2}) \cap G_{c_1,c_2},$$

respectively. One should also apply (4.1.6) and check that the isomorphism τ_A between the two subgroups in (4.3.3) is the conjugation isomorphism by w_{A^t} (that is, $\tau_A(g) = w_{A^t} g w_{A^t}^{-1}$ for every $g \in H \cap K^{w_{A^t}}$). We leave all of these bookkeeping details to the reader to check. [228]

For the tower with $G_n = GL_n$, there is slightly more work to be done to check the equality (4.3.2). Via Mackey's Theorem 4.1.7 and Proposition 4.3.7(c), the left side is

$$\begin{aligned}
&\operatorname{res}^n_{c_1,c_2} \left(\operatorname{ind}^n_{r_1,r_2} (U_1 \otimes U_2) \right) \\
&= \left(\operatorname{Res}^{G_n}_{P_{c_1,c_2}} \operatorname{Ind}^{G_n}_{P_{r_1,r_2}} \operatorname{Infl}^{P_{r_1,r_2}}_{G_{r_1,r_2}} (U_1 \otimes U_2) \right)^{K_{c_1,c_2}} \\
&= \bigoplus_A \left(\operatorname{Ind}^{P_{c_1,c_2}}_{{}^{w_{A^t}}P_{r_1,r_2} \cap P_{c_1,c_2}} \left(\left(\operatorname{Res}^{P_{r_1,r_2}}_{P_{r_1,r_2} \cap P^{w_{A^t}}_{c_1,c_2}} \operatorname{Infl}^{P_{r_1,r_2}}_{G_{r_1,r_2}} (U_1 \otimes U_2) \right)^{\tau_A^{-1}} \right) \right)^{K_{c_1,c_2}} \qquad (4.3.4)
\end{aligned}$$

where A runs over the usual 2×2 matrices. The right side is a direct sum over this same set of matrices A:

$$\begin{aligned}
&\bigoplus_A \left(\operatorname{ind}^{c_1}_{a_{11},a_{21}} \otimes \operatorname{ind}^{c_2}_{a_{12},a_{22}} \right) \left(\left(\operatorname{res}^{r_1}_{a_{11},a_{12}} U_1 \otimes \operatorname{res}^{r_2}_{a_{21},a_{22}} U_2 \right)^{\tau_A^{-1}} \right) \\
&= \bigoplus_A \left(\operatorname{Ind}^{G_{c_1}}_{P_{a_{11},a_{21}}} \otimes \operatorname{Ind}^{G_{c_2}}_{P_{a_{12},a_{22}}} \right) \circ \left(\operatorname{Infl}^{P_{a_{11},a_{21}}}_{G_{a_{11},a_{21}}} \otimes \operatorname{Infl}^{P_{a_{12},a_{22}}}_{G_{a_{12},a_{22}}} \right) \\
&\qquad \left(\left(\left(\operatorname{Res}^{G_{r_1}}_{P_{a_{11},a_{12}}} U_1 \right)^{K_{a_{11},a_{12}}} \otimes \left(\operatorname{Res}^{G_{r_2}}_{P_{a_{21},a_{22}}} U_2 \right)^{K_{a_{21},a_{22}}} \right)^{\tau_A^{-1}} \right) \\
&= \bigoplus_A \operatorname{Ind}^{G_{c_1,c_2}}_{P_{a_{11},a_{21}} \times P_{a_{12},a_{22}}} \\
&\qquad \operatorname{Infl}^{P_{a_{11},a_{21}} \times P_{a_{12},a_{22}}}_{G_{a_{11},a_{21},a_{12},a_{22}}} \left(\left(\left(\operatorname{Res}^{G_{r_1,r_2}}_{P_{a_{11},a_{12}} \times P_{a_{21},a_{22}}} (U_1 \otimes U_2) \right)^{K_{a_{11},a_{12}} \times K_{a_{21},a_{22}}} \right)^{\tau_A^{-1}} \right) \qquad (4.3.5)
\end{aligned}$$

(by (4.1.6), (4.1.15) and their obvious analogues for restriction and inflation). Thus it suffices to check for each 2×2 matrix A that any $\mathbb{C}G_{c_1,c_2}$-module of the form $V_1 \otimes V_2$ has the same inner product with the A-summands of (4.3.4) and (4.3.5). Abbreviate $w := w_{A^t}$ and $\tau := \tau_A^{-1}$.

---

[227] Proposition 4.3.7 gives as a system of double coset representatives for $G_{(c_1,c_2)} \backslash G_n / G_{(r_1,r_2)}$ the elements

$$\begin{aligned}
&\left\{ w_A \ : \ A \in \mathbb{N}^{2\times 2},\ A \text{ has row sums } (c_1, c_2) \text{ and column sums } (r_1, r_2) \right\} \\
&= \left\{ w_{A^t} \ : \ A \in \mathbb{N}^{2\times 2},\ A \text{ has row sums } (r_1, r_2) \text{ and column sums } (c_1, c_2) \right\}
\end{aligned}$$

where A^t denotes the transpose matrix of A.

[228] It helps to recognize w_{A^t} as the permutation written in two-line notation as

$$\begin{pmatrix} 1 & 2 & \ldots & a_{11} & | & a_{11}+1 & a_{11}+2 & \ldots & r_1 & | & r_1+1 & r_1+2 & \ldots & a'_{22} & | & a'_{22}+1 & a'_{22}+2 & \ldots & n \\ 1 & 2 & \ldots & a_{11} & | & c_1+1 & c_1+2 & \ldots & a'_{22} & | & a_{11}+1 & a_{11}+2 & \ldots & c_1 & | & a'_{22}+1 & a'_{22}+2 & \ldots & n \end{pmatrix},$$

where $a'_{22} = r_1 + a_{21} = c_1 + a_{12} = n - a_{22}$. In matrix form, w_{A^t} is the block matrix $\begin{bmatrix} I_{a_{11}} & 0 & 0 & 0 \\ 0 & 0 & I_{a_{21}} & 0 \\ 0 & I_{a_{12}} & 0 & 0 \\ 0 & 0 & 0 & I_{a_{22}} \end{bmatrix}$.

Notice that ${}^{w}P_{r_1,r_2}$ is the group of all matrices having the block form

$$\begin{bmatrix} g_{11} & h & i & j \\ 0 & g_{21} & 0 & k \\ d & e & g_{12} & \ell \\ 0 & f & 0 & g_{22} \end{bmatrix} \tag{4.3.6}$$

in which the diagonal blocks g_{ij} for $i,j=1,2$ are invertible of size $a_{ij}\times a_{ij}$, while the blocks h,i,j,k,ℓ,d,e,f are all arbitrary matrices[229] of the appropriate (rectangular) block sizes. Hence, ${}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}$ is the group of all matrices having the block form

$$\begin{bmatrix} g_{11} & h & i & j \\ 0 & g_{21} & 0 & k \\ 0 & 0 & g_{12} & \ell \\ 0 & 0 & 0 & g_{22} \end{bmatrix} \tag{4.3.7}$$

in which the diagonal blocks g_{ij} for $i,j=1,2$ are invertible of size $a_{ij}\times a_{ij}$, while the blocks h,i,j,k,ℓ are all arbitrary matrices of the appropriate (rectangular) block sizes; then ${}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}$ is the subgroup where the blocks i,j,k all vanish. The canonical projection ${}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}\to {}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}$ (obtained by restricting the projection $P_{c_1,c_2}\to G_{c_1,c_2}$) has kernel ${}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}\cap K_{c_1,c_2}$. Consequently,

$$\left({}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}\right)/\left({}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}\cap K_{c_1,c_2}\right)={}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}. \tag{4.3.8}$$

Similarly,

$$\left(P_{r_1,r_2}\cap P^{w}_{c_1,c_2}\right)/\left(P_{r_1,r_2}\cap P^{w}_{c_1,c_2}\cap K_{r_1,r_2}\right)=G_{r_1,r_2}\cap P^{w}_{c_1,c_2}. \tag{4.3.9}$$

Computing first the inner product of $V_1\otimes V_2$ with the A-summand of (4.3.4), and using adjointness properties, one gets

$$\begin{aligned}
&\Big(\Big(\mathrm{Res}^{P_{r_1,r_2}}_{P_{r_1,r_2}\cap P^{w}_{c_1,c_2}}\,\mathrm{Infl}^{P_{r_1,r_2}}_{G_{r_1,r_2}}\,(U_1\otimes U_2)\Big)^{\tau},\\
&\qquad\qquad \mathrm{Res}^{P_{c_1,c_2}}_{{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}}\,\mathrm{Infl}^{P_{c_1,c_2}}_{G_{c_1,c_2}}\,(V_1\otimes V_2)\Big)_{{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}}\\
&\overset{(4.1.10)}{=}\Big(\Big(\mathrm{Infl}^{P_{r_1,r_2}\cap P^{w}_{c_1,c_2}}_{G_{r_1,r_2}\cap P^{w}_{c_1,c_2}}\,\mathrm{Res}^{G_{r_1,r_2}}_{G_{r_1,r_2}\cap P^{w}_{c_1,c_2}}\,(U_1\otimes U_2)\Big)^{\tau},\\
&\qquad\qquad \mathrm{Infl}^{{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}}_{{}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}}\,\mathrm{Res}^{G_{c_1,c_2}}_{{}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}}\,(V_1\otimes V_2)\Big)_{{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}}
\end{aligned}$$

(by (4.3.9) and (4.3.8)). One can compute this inner product by first recalling that ${}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}$ is the group of matrices having the block form (4.3.7) in which the diagonal blocks g_{ij} for $i,j=1,2$ are invertible of size $a_{ij}\times a_{ij}$, while the blocks h,i,j,k,ℓ are all arbitrary matrices of the appropriate (rectangular) block sizes; then ${}^{w}P_{r_1,r_2}\cap G_{c_1,c_2}$ is the subgroup where the blocks i,j,k all vanish. The inner product above then becomes

$$\begin{aligned}
\frac{1}{|{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}|}\sum_{\substack{(g_{ij})\\(h,i,j,k,\ell)}}&\chi_{U_1}\begin{pmatrix} g_{11} & i\\ 0 & g_{12}\end{pmatrix}\chi_{U_2}\begin{pmatrix} g_{21} & k\\ 0 & g_{22}\end{pmatrix}\\
&\overline{\chi}_{V_1}\begin{pmatrix} g_{11} & h\\ 0 & g_{21}\end{pmatrix}\overline{\chi}_{V_2}\begin{pmatrix} g_{12} & \ell\\ 0 & g_{22}\end{pmatrix}.
\end{aligned} \tag{4.3.10}$$

[229] The blocks i and j have nothing to do with the indices i,j in g_{ij}.

If one instead computes the inner product of $V_1 \otimes V_2$ with the A-summand of (4.3.5), using adjointness properties and (4.1.13) one gets

$$\begin{aligned}
&\Bigg(\Bigg(\left(\mathrm{Res}^{G_{r_1,r_2}}_{P_{a_{11},a_{12}}\times P_{a_{21},a_{22}}}(U_1\otimes U_2)\right)^{K_{a_{11},a_{12}}\times K_{a_{21},a_{22}}}\Bigg)^{\tau},\\
&\qquad\left(\mathrm{Res}^{G_{c_1,c_2}}_{P_{a_{11},a_{21}}\times P_{a_{12},a_{22}}}(V_1\otimes V_2)\right)^{K_{a_{11},a_{21}}\times K_{a_{12},a_{22}}}\Bigg)_{G_{a_{11},a_{21},a_{12},a_{22}}}\\
&=\frac{1}{|G_{a_{11},a_{21},a_{12},a_{22}}|}\sum_{(g_{ij})}\frac{1}{|K_{a_{11},a_{12}}\times K_{a_{21},a_{22}}|}\sum_{(i,k)}\chi_{U_1}\begin{pmatrix}g_{11}&i\\0&g_{12}\end{pmatrix}\chi_{U_2}\begin{pmatrix}g_{21}&k\\0&g_{22}\end{pmatrix}\\
&\qquad\frac{1}{|K_{a_{11},a_{21}}\times K_{a_{12},a_{22}}|}\sum_{(h,\ell)}\overline{\chi}_{V_1}\begin{pmatrix}g_{11}&h\\0&g_{21}\end{pmatrix}\overline{\chi}_{V_2}\begin{pmatrix}g_{12}&\ell\\0&g_{22}\end{pmatrix}.
\end{aligned}$$

But this right hand side can be seen to equal (4.3.10), after one notes that

$$|{}^{w}P_{r_1,r_2}\cap P_{c_1,c_2}| = |G_{a_{11},a_{21},a_{12},a_{22}}|\cdot|K_{a_{11},a_{12}}\times K_{a_{21},a_{22}}|\cdot|K_{a_{11},a_{21}}\times K_{a_{12},a_{22}}|\cdot\#\{j\in\mathbb{F}_q^{a_{11}\times a_{22}}\}$$

and that the summands in (4.3.10) are independent of the matrix j in the summation. □

We can also define a $\mathbb{C}$-vector space $A_{\mathbb{C}}$ as the direct sum $\bigoplus_{n\geq 0} R_{\mathbb{C}}(G_n)$. In the same way as we have made $A=\bigoplus_{n\geq 0}R(G_n)$ into a $\mathbb{Z}$-bialgebra, we can turn $A_{\mathbb{C}}=\bigoplus_{n\geq 0}R_{\mathbb{C}}(G_n)$ into a $\mathbb{C}$-bialgebra[230]. There is a $\mathbb{C}$-bilinear form $(\cdot,\cdot)_{A_{\mathbb{C}}}$ on $A_{\mathbb{C}}$ which can be defined either as the $\mathbb{C}$-bilinear extension of the $\mathbb{Z}$-bilinear form $(\cdot,\cdot)_A : A\times A\to\mathbb{Z}$ to $A_{\mathbb{C}}$, or (equivalently) as the $\mathbb{C}$-bilinear form on $A_{\mathbb{C}}$ which restricts to $\langle\cdot,\cdot\rangle_{\mathfrak{S}_n}$ on every homogeneous component $R_{\mathbb{C}}(G_n)$ and makes different homogeneous components mutually orthogonal. The obvious embedding of A into the $\mathbb{C}$-bialgebra $A_{\mathbb{C}}$ (obtained from the embeddings $R(G_n)\to R_{\mathbb{C}}(G_n)$ for all n) respects the bialgebra operations[231], and the $\mathbb{C}$-bialgebra $A_{\mathbb{C}}$ can be identified with $A\otimes_{\mathbb{Z}}\mathbb{C}$ (the result of extending scalars to $\mathbb{C}$ in A), because every finite group G satisfies $R_{\mathbb{C}}(G)\cong R(G)\otimes_{\mathbb{Z}}\mathbb{C}$. The embedding of A into $A_{\mathbb{C}}$ also respects the bilinear forms.

Exercise 4.3.11. Let G_* be one of the three towers.

For every almost-composition $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$ of $n\in\mathbb{N}$, let us define a map ind^n_α which takes $\mathbb{C}G_\alpha$-modules to $\mathbb{C}G_n$-modules as follows: If $G_*=\mathfrak{S}_*$ or $G_*=\mathfrak{S}_*[\Gamma]$, we set

$$\mathrm{ind}^n_\alpha := \mathrm{Ind}^{G_n}_{G_\alpha}.$$

If $G_*=GL_*$, then we set

$$\mathrm{ind}^n_\alpha := \mathrm{Ind}^{G_n}_{P_\alpha}\mathrm{Infl}^{P_\alpha}_{G_\alpha}.$$

(Note that $\mathrm{ind}^n_\alpha=\mathrm{ind}^n_{i,j}$ if α has the form (i,j).)

Similarly, for every almost-composition $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$ of $n\in\mathbb{N}$, let us define a map res^n_α which takes $\mathbb{C}G_n$-modules to $\mathbb{C}G_\alpha$-modules as follows: If $G_*=\mathfrak{S}_*$ or $G_*=\mathfrak{S}_*[\Gamma]$, we set

$$\mathrm{res}^n_\alpha := \mathrm{Res}^{G_n}_{G_\alpha}.$$

If $G_*=GL_*$, then we set

$$\mathrm{res}^n_\alpha := \left(\mathrm{Res}^{G_n}_{P_\alpha}(-)\right)^{K_\alpha}.$$

(Note that $\mathrm{res}^n_\alpha=\mathrm{res}^n_{i,j}$ if α has the form (i,j).)

---

[230] The definitions of m and Δ for this $\mathbb{C}$-bialgebra look the same as for A: For instance, m is still defined to be $\mathrm{ind}^{i+j}_{i,j}$ on $(A_{\mathbb{C}})_i\otimes(A_{\mathbb{C}})_j$, where $\mathrm{ind}^{i+j}_{i,j}$ is defined by the same formulas as in Definition 4.2.1. However, the operators of induction, restriction, inflation and K-fixed space construction appearing in these formulas now act on class functions as opposed to modules.

The fact that these maps m and Δ satisfy the axioms of a $\mathbb{C}$-bialgebra is easy to check: they are merely the $\mathbb{C}$-linear extensions of the maps m and Δ of the $\mathbb{Z}$-bialgebra A (this is because, for instance, induction of class functions and induction of modules are related by the identity (4.1.5)), and thus satisfy the same axioms as the latter.

[231] This is because, for example, induction of class functions harmonizes with induction of modules (i.e., the equality (4.1.5) holds).

(a) If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ is an almost-composition of an integer $n \in \mathbb{N}$ satisfying $\ell \geq 1$, and if V_i is a $\mathbb{C}G_{\alpha_i}$-module for every $i \in \{1, 2, \ldots, \ell\}$, then show that

$$\begin{aligned}
&\operatorname{ind}_{\alpha_1+\alpha_2+\cdots+\alpha_{\ell-1},\alpha_\ell}^{n} \left(\operatorname{ind}_{(\alpha_1,\alpha_2,\ldots,\alpha_{\ell-1})}^{\alpha_1+\alpha_2+\cdots+\alpha_{\ell-1}} (V_1 \otimes V_2 \otimes \cdots \otimes V_{\ell-1}) \otimes V_\ell \right) \\
&\cong \operatorname{ind}_{\alpha}^{n} (V_1 \otimes V_2 \otimes \cdots \otimes V_\ell) \\
&\cong \operatorname{ind}_{\alpha_1,\alpha_2+\alpha_3+\cdots+\alpha_\ell}^{n} \left(V_1 \otimes \operatorname{ind}_{(\alpha_2,\alpha_3,\ldots,\alpha_\ell)}^{\alpha_2+\alpha_3+\cdots+\alpha_\ell} (V_2 \otimes V_3 \otimes \cdots \otimes V_\ell) \right).
\end{aligned}$$

(b) Solve Exercise 4.2.3 again using Exercise 4.3.11(a).

(c) We proved above that the map $m : A \otimes A \to A$ (where $A = A(G_*)$) is associative, by using the adjointness of m and Δ. Give a new proof of this fact, which makes no use of Δ.

(d) If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ is an almost-composition of an $n \in \mathbb{N}$, and if $\chi_i \in R(G_{\alpha_i})$ for every $i \in \{1, 2, \ldots, \ell\}$, then show that

$$\chi_1 \chi_2 \cdots \chi_\ell = \operatorname{ind}_{\alpha}^{n} (\chi_1 \otimes \chi_2 \otimes \cdots \otimes \chi_\ell)$$

in $A = A(G_*)$.

(e) If $n \in \mathbb{N}$, $\ell \in \mathbb{N}$ and $\chi \in R(G_n)$, then show that

$$\Delta^{(\ell-1)} \chi = \sum \operatorname{res}_{\alpha}^{n} \chi$$

in $A^{\otimes \ell}$, where $A = A(G_*)$. Here, the sum on the right hand side runs over all almost-compositions α of n having length ℓ.

4.4. **Symmetric groups.** Finally, some payoff. Consider the tower of symmetric groups $G_n = \mathfrak{S}_n$, and $A = A(G_*) =: A(\mathfrak{S})$. Denote by $\underline{1}_{\mathfrak{S}_n}, \operatorname{sgn}_{\mathfrak{S}_n}$ the *trivial* and *sign* characters on $\mathfrak{S}_n$. For a partition λ of n, denote by $\underline{1}_{\mathfrak{S}_\lambda}, \operatorname{sgn}_{\mathfrak{S}_\lambda}$ the trivial and sign characters restricted to the Young subgroup $\mathfrak{S}_\lambda = \mathfrak{S}_{\lambda_1} \times \mathfrak{S}_{\lambda_2} \times \cdots$, and denote by $\underline{1}_\lambda$ the class function which is the characteristic function for the $\mathfrak{S}_n$-conjugacy class of permutations of cycle type λ.

Theorem 4.4.1. (a) *Irreducible complex characters $\{\chi^\lambda\}$ of $\mathfrak{S}_n$ are indexed by partitions λ in* Par_n, *and one has a PSH-isomorphism, the* Frobenius characteristic map[232],

$$A = A(\mathfrak{S}) \xrightarrow{\operatorname{ch}} \Lambda$$

that for $n \geq 0$ and $\lambda \in \operatorname{Par}_n$ sends

$$\begin{aligned}
\underline{1}_{\mathfrak{S}_n} &\longmapsto h_n, \\
\operatorname{sgn}_{\mathfrak{S}_n} &\longmapsto e_n, \\
\chi^\lambda &\longmapsto s_\lambda, \\
\operatorname{Ind}_{\mathfrak{S}_\lambda}^{\mathfrak{S}_n} \underline{1}_{\mathfrak{S}_\lambda} &\longmapsto h_\lambda, \\
\operatorname{Ind}_{\mathfrak{S}_\lambda}^{\mathfrak{S}_n} \operatorname{sgn}_{\mathfrak{S}_\lambda} &\longmapsto e_\lambda, \\
\underline{1}_\lambda &\longmapsto \tfrac{p_\lambda}{z_\lambda}
\end{aligned}$$

(where ch *is extended to a $\mathbb{C}$-linear map $A_{\mathbb{C}} \to \Lambda_{\mathbb{C}}$), and for $n \geq 1$ sends*

$$\underline{1}_{(n)} \longmapsto \tfrac{p_n}{n}.$$

Here, z_λ is defined as in Proposition 2.5.15.

(b) *For each $n \geq 0$, the involution on class functions $f : \mathfrak{S}_n \to \mathbb{C}$ sending $f \longmapsto \operatorname{sgn}_{\mathfrak{S}_n} * f$ where*

$$(\operatorname{sgn}_{\mathfrak{S}_n} * f)(g) := \operatorname{sgn}(g) f(g)$$

preserves the $\mathbb{Z}$-sublattice $R(\mathfrak{S}_n)$ of genuine characters. The direct sum of these involutions induces an involution on $A = A(\mathfrak{S}) = \bigoplus_{n \geq 0} R(\mathfrak{S}_n)$ that corresponds under ch *to the involution ω on Λ.*

[232] It is unrelated to the Frobenius endomorphisms from Exercise 2.9.9.

Proof. (a) Corollary 4.3.10 implies that the set $\Sigma = \bigsqcup_{n\geq 0} \operatorname{Irr}(\mathfrak{S}_n)$ gives a PSH-basis for A. Since a character χ of $\mathfrak{S}_n$ has

$$\Delta(\chi) = \bigoplus_{i+j=n} \operatorname{Res}^{\mathfrak{S}_n}_{\mathfrak{S}_i \times \mathfrak{S}_j} \chi, \tag{4.4.1}$$

such an element $\chi \in \Sigma \cap A_n$ is never primitive for $n \geq 2$. Hence the unique irreducible character $\rho = \underline{1}_{\mathfrak{S}_1}$ of $\mathfrak{S}_1$ is the only element of $\mathcal{C} = \Sigma \cap \mathfrak{p}$.

Thus Theorem 3.3.3(g) tells us that there are two PSH-isomorphisms $A \to \Lambda$, each of which sends Σ to the PSH-basis of Schur functions $\{s_\lambda\}$ for Λ. It also tells us that we can pin down one of the two isomorphisms to call ch, by insisting that it map the two characters $\underline{1}_{\mathfrak{S}_2}, \operatorname{sgn}_{\mathfrak{S}_2}$ in $\operatorname{Irr}(\mathfrak{S}_2)$ to h_2, e_2 (and not e_2, h_2).

Bearing in mind the coproduct formula (4.4.1), and the fact that $\underline{1}_{\mathfrak{S}_n}, \operatorname{sgn}_{\mathfrak{S}_n}$ restrict, respectively, to trivial and sign characters of $\mathfrak{S}_i \times \mathfrak{S}_j$ for $i+j=n$, one finds that for $n \geq 2$ one has $\operatorname{sgn}^{\perp}_{\mathfrak{S}_2}$ annihilating $\underline{1}_{\mathfrak{S}_n}$, and $\underline{1}^{\perp}_{\mathfrak{S}_2}$ annihilating $\operatorname{sgn}_{\mathfrak{S}_n}$. Therefore Theorem 3.3.1(b) (applied to Λ) implies $\underline{1}_{\mathfrak{S}_n}, \operatorname{sgn}_{\mathfrak{S}_n}$ are sent under ch to h_n, e_n. Then the fact that $\operatorname{Ind}^{\mathfrak{S}_n}_{\mathfrak{S}_\lambda} \underline{1}_{\mathfrak{S}_\lambda}, \operatorname{Ind}^{\mathfrak{S}_n}_{\mathfrak{S}_\lambda} \operatorname{sgn}_{\mathfrak{S}_\lambda}$ are sent to h_λ, e_λ follows via induction products.

Recall that the $\mathbb{C}$-vector space $A_{\mathbb{C}} = \bigoplus_{n\geq 0} R_{\mathbb{C}}(\mathfrak{S}_n)$ is a $\mathbb{C}$-bialgebra, and can be identified with $A \otimes_{\mathbb{Z}} \mathbb{C}$. The multiplication and the comultiplication of $A_{\mathbb{C}}$ are $\mathbb{C}$-linear extensions of those of A, and are still given by the same formulas $m = \operatorname{ind}^{i+j}_{i,j}$ and $\Delta = \bigoplus_{i+j=n} \operatorname{res}^{i+j}_{i,j}$ as those of A (but now, induction and restriction are defined for class functions, not just for representations). The $\mathbb{C}$-bilinear form $(\cdot,\cdot)_{A_{\mathbb{C}}}$ on $A_{\mathbb{C}}$ extends both the $\mathbb{Z}$-bilinear form $(\cdot,\cdot)_A$ on A and the $\mathbb{C}$-bilinear forms $\langle\cdot,\cdot\rangle_{\mathfrak{S}_n}$ on all $R_{\mathbb{C}}(\mathfrak{S}_n)$.

For the assertion about $\underline{1}_{(n)}$, note that it is primitive in $A_{\mathbb{C}}$ for $n \geq 1$, because as a class function, the indicator function of n-cycles vanishes upon restriction to $\mathfrak{S}_i \times \mathfrak{S}_j$ for $i+j=n$ if both $i,j \geq 1$; these subgroups contain no n-cycles. Hence Corollary 3.1.8 implies that $\operatorname{ch}(\underline{1}_{(n)})$ is a scalar multiple of p_n. To pin down the scalar, note $p_n = m_{(n)}$ so $(h_n, p_n)_\Lambda = (h_n, m_n)_\Lambda = 1$, while $\operatorname{ch}^{-1}(h_n) = \underline{1}_{\mathfrak{S}_n}$ has

$$(\underline{1}_{\mathfrak{S}_n}, \underline{1}_{(n)}) = \frac{1}{n!} \cdot (n-1)! = \frac{1}{n}.$$

[233] Thus $\operatorname{ch}(\underline{1}_{(n)}) = \frac{p_n}{n}$. The fact that $\operatorname{ch}(\underline{1}_\lambda) = \frac{p_\lambda}{z_\lambda}$ then follows via induction product calculations[234]. Part (b) follows from Exercise 4.4.4 below. □

Remark 4.4.2. The paper of Liulevicius [133] gives a very elegant alternate approach to the Frobenius map as a Hopf isomorphism $A(\mathfrak{S}) \xrightarrow{\text{ch}} \Lambda$, inspired by equivariant K-theory and vector bundles over spaces which are finite sets of points!

Exercise 4.4.3. If P is a subset of a group G, we denote by $\underline{1}_P$ the map $G \to \mathbb{C}$ which sends every element of P to 1 and all remaining elements of G to 0. [235] For any finite group G and any $h \in G$, we introduce the following notations:

- Let $Z_G(h)$ denote the centralizer of h in G.
- Let $\operatorname{Conj}_G(h)$ denote the conjugacy class of h in G.
- Define a map $\alpha_{G,h} : G \to \mathbb{C}$ by $\alpha_{G,h} = |Z_G(h)|\, \underline{1}_{\operatorname{Conj}_G(h)}$. This map $\alpha_{G,h}$ is a class function[236].

(a) Prove that $\alpha_{G,h}(g) = \sum_{k\in G} \left[khk^{-1} = g\right]$ for every finite group G and any $h \in G$ and $g \in G$. Here, we are using the Iverson bracket notation (that is, for any statement $\mathcal{A}$, we define $[\mathcal{A}]$ to be the integer 1 if $\mathcal{A}$ is true, and 0 otherwise).

(b) Prove that if H is a subgroup of a finite group G, and if $h \in H$, then $\operatorname{Ind}^G_H \alpha_{H,h} = \alpha_{G,h}$.

(c) Prove that if G_1 and G_2 are finite groups, and if $h_1 \in G_1$ and $h_2 \in G_2$, then the canonical isomorphism $R_{\mathbb{C}}(G_1) \otimes R_{\mathbb{C}}(G_2) \to R_{\mathbb{C}}(G_1 \times G_2)$ sends $\alpha_{G_1,h_1} \otimes \alpha_{G_2,h_2}$ to $\alpha_{G_1\times G_2,(h_1,h_2)}$.

---

[233] The first equality sign in this computation uses the fact that the number of all n-cycles in $\mathfrak{S}_n$ is $(n-1)!$. This is because any n-cycle in $\mathfrak{S}_n$ can be uniquely written in the form $(i_1, i_2, \ldots, i_{n-1}, n)$ (in cycle notation) with $(i_1, i_2, \ldots, i_{n-1})$ being a permutation in $\mathfrak{S}_{n-1}$ (written in one-line notation).

[234] For instance, one can use (4.1.3) to show that $z_\lambda \underline{1}_\lambda = \lambda_1\lambda_2\cdots\lambda_\ell \cdot \underline{1}_{(\lambda_1)}\underline{1}_{(\lambda_2)}\cdots\underline{1}_{(\lambda_\ell)}$ if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ with $\ell = \ell(\lambda)$. See Exercise 4.4.3(d) for the details.

[235] This is not in conflict with the notation $\underline{1}_G$ for the trivial character of G, since $\underline{1}_P = \underline{1}_G$ for $P = G$. Note that $\underline{1}_P$ is a class function when P is a union of conjugacy classes of G.

[236] In fact, $\underline{1}_{\operatorname{Conj}_G(h)}$ is a class function (since $\operatorname{Conj}_G(h)$ is a conjugacy class), and so $\alpha_{G,h}$ (being the scalar multiple $|Z_G(h)|\, \underline{1}_{\operatorname{Conj}_G(h)}$ of $\underline{1}_{\operatorname{Conj}_G(h)}$) must also be a class function.

(d) Fill in the details of the proof of $\operatorname{ch}(\underline{1}_\lambda) = \frac{p_\lambda}{z_\lambda}$ in the proof of Theorem 4.4.1.
(e) Obtain an alternative proof of Remark 2.5.16.
(f) If G and H are two finite groups, and if $\rho : H \to G$ is a group homomorphism, then prove that $\operatorname{Ind}_\rho \alpha_{H,h} = \alpha_{G,\rho(h)}$ for every $h \in H$, where $\operatorname{Ind}_\rho \alpha_{H,h}$ is defined as in Exercise 4.1.14.

Exercise 4.4.4. If G is a group and U_1 and U_2 are two $\mathbb{C}G$-modules, then the tensor product $U_1 \otimes U_2$ is a $\mathbb{C}[G \times G]$-module, which can be made into a $\mathbb{C}G$-module by letting $g \in G$ act as $(g, g) \in G \times G$. This $\mathbb{C}G$-module $U_1 \otimes U_2$ is called the *inner tensor product*[237] of U_1 and U_2, and is a restriction of the outer tensor product $U_1 \otimes U_2$ using the inclusion map $G \to G \times G,\ g \mapsto (g, g)$.

Let $n \geq 0$, and let $\operatorname{sgn}_{\mathfrak{S}_n}$ be the 1-dimensional $\mathbb{C}\mathfrak{S}_n$-module $\mathbb{C}$ on which every $g \in \mathfrak{S}_n$ acts as multiplication by $\operatorname{sgn}(g)$. If V is a $\mathbb{C}\mathfrak{S}_n$-module, show that the involution on $A(\mathfrak{S}) = \bigoplus_{n \geq 0} R(\mathfrak{S}_n)$ defined in Theorem 4.4.1(b) sends $\chi_V \mapsto \chi_{\operatorname{sgn}_{\mathfrak{S}_n} \otimes V}$ where $\operatorname{sgn}_{\mathfrak{S}_n} \otimes V$ is the inner tensor product of $\operatorname{sgn}_{\mathfrak{S}_n}$ and V. Use this to show that this involution is a nontrivial PSH-automorphism of $A(\mathfrak{S})$, and deduce Theorem 4.4.1(b).

Exercise 4.4.5. Let $n \in \mathbb{N}$. For every permutation $\sigma \in \mathfrak{S}_n$, we let $\operatorname{type}\sigma$ denote the cycle type of σ. Extend $\operatorname{ch} : A = A(\mathfrak{S}) \to \Lambda$ to a $\mathbb{C}$-linear map $A_\mathbb{C} \to \Lambda_\mathbb{C}$. We shall call the latter map ch, too.

(a) Prove that every class function $f \in R_\mathbb{C}(\mathfrak{S}_n)$ satisfies

$$\operatorname{ch}(f) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} f(\sigma)\, p_{\operatorname{type}\sigma}.$$

(b) Let H be a subgroup of $\mathfrak{S}_n$. Prove that every class function $f \in R_\mathbb{C}(H)$ satisfies

$$\operatorname{ch}\left(\operatorname{Ind}_H^{\mathfrak{S}_n} f\right) = \frac{1}{|H|} \sum_{h \in H} f(h)\, p_{\operatorname{type} h}.$$

Exercise 4.4.6. (a) Show that for every $n \geq 0$, every $g \in \mathfrak{S}_n$ and every finite-dimensional $\mathbb{C}\mathfrak{S}_n$-module V, we have $\chi_V(g) \in \mathbb{Z}$.
(b) Show that for every $n \geq 0$ and every finite-dimensional $\mathbb{C}\mathfrak{S}_n$-module V, there exists a $\mathbb{Q}\mathfrak{S}_n$-module W such that $V \cong \mathbb{C} \otimes_\mathbb{Q} W$. (In the representation theorists' parlance, this says that all representations of $\mathfrak{S}_n$ are *defined over* $\mathbb{Q}$. This part of the exercise requires some familiarity with representation theory.)

Remark 4.4.7. Parts (a) and (b) of Exercise 4.4.6 both follow from an even stronger result: For every $n \geq 0$ and every finite-dimensional $\mathbb{C}\mathfrak{S}_n$-module V, there exists a $\mathbb{Z}\mathfrak{S}_n$-module W which is finitely generated and free as a $\mathbb{Z}$-module and satisfies $V \cong \mathbb{C} \otimes_\mathbb{Z} W$ as $\mathbb{C}\mathfrak{S}_n$-modules. This follows from the combinatorial approach to the representation theory of $\mathfrak{S}_n$, in which the irreducible representations of $\mathbb{C}\mathfrak{S}_n$ (the *Specht modules*) are constructed using Young tableaux and tabloids. See the literature on the symmetric group, e.g., [186], [73, §7], [223] or [115, Section 2.2] for this approach.

The connection between Λ and $A(\mathfrak{S})$ as established in Theorem 4.4.1 benefits both the study of Λ and that of $A(\mathfrak{S})$. The following two exercises show some applications to Λ:

Exercise 4.4.8. If G is a group and U_1 and U_2 are two $\mathbb{C}G$-modules, then let $U_1 \boxtimes U_2$ denote the inner tensor product of U_1 and U_2 (as defined in Exercise 4.4.4). Consider also the binary operation $*$ on $\Lambda_\mathbb{Q}$ defined in Exercise 2.9.4(h).

(a) Show that $\operatorname{ch}(\chi_{U_1 \boxtimes U_2}) = \operatorname{ch}(\chi_{U_1}) * \operatorname{ch}(\chi_{U_2})$ for any $n \in \mathbb{N}$ and any two $\mathbb{C}\mathfrak{S}_n$-modules U_1 and U_2.
(b) Use this to obtain a new solution for Exercise 2.9.4(h).
(c) Show that $s_\mu * s_\nu \in \sum_{\lambda \in \operatorname{Par}} \mathbb{N} s_\lambda$ for any two partitions μ and ν.

[**Hint:** For any group G, introduce a binary operation $*$ on $R_\mathbb{C}(G)$ which satisfies $\chi_{U_1 \boxtimes U_2} = \chi_{U_1} * \chi_{U_2}$ for any two $\mathbb{C}G$-modules U_1 and U_2.]

Exercise 4.4.9. Define a $\mathbb{Q}$-bilinear map $\boxdot : \Lambda_\mathbb{Q} \times \Lambda_\mathbb{Q} \to \Lambda_\mathbb{Q}$, which will be written in infix notation (that is, we will write $a \boxdot b$ instead of $\boxdot(a, b)$), by setting

$$p_\lambda \boxdot p_\mu = \prod_{i=1}^{\ell(\lambda)} \prod_{j=1}^{\ell(\mu)} p_{\operatorname{lcm}(\lambda_i, \mu_j)}^{\gcd(\lambda_i, \mu_j)} \qquad \text{for any partitions } \lambda \text{ and } \mu.$$

[237] Do not confuse this with the inner product of characters.

238

(a) Show that $\Lambda_{\mathbb{Q}}$, equipped with the binary operation $\boxdot$, becomes a commutative $\mathbb{Q}$-algebra with unity p_1.
(b) For every $r \in \mathbb{Z}$, define the $\mathbb{Q}$-algebra homomorphism $\epsilon_r : \Lambda_{\mathbb{Q}} \to \mathbb{Q}$ as in Exercise 2.9.4(c). Show that $1 \boxdot f = \epsilon_1(f)\, 1$ for every $f \in \Lambda_{\mathbb{Q}}$ (where 1 denotes the unity of Λ).
(c) Show that $s_\mu \boxdot s_\nu \in \sum_{\lambda \in \mathrm{Par}} \mathbb{N} s_\lambda$ for any two partitions μ and ν.
(d) Show that $f \boxdot g \in \Lambda$ for any $f \in \Lambda$ and $g \in \Lambda$.

[**Hint:** For every set X, let $\mathfrak{S}_X$ denote the group of all permutations of X. For two sets X and Y, there is a canonical group homomorphism $\mathfrak{S}_X \times \mathfrak{S}_Y \to \mathfrak{S}_{X \times Y}$, which is injective if X and Y are nonempty. For positive integers n and m, this yields an embedding $\mathfrak{S}_n \times \mathfrak{S}_m \to \mathfrak{S}_{\{1,2,\ldots,n\} \times \{1,2,\ldots,m\}}$, which, once $\mathfrak{S}_{\{1,2,\ldots,n\} \times \{1,2,\ldots,m\}}$ is identified with $\mathfrak{S}_{nm}$ (using an arbitrary but fixed bijection $\{1,2,\ldots,n\} \times \{1,2,\ldots,m\} \to \{1,2,\ldots,nm\}$), can be regarded as an embedding $\mathfrak{S}_n \times \mathfrak{S}_m \to \mathfrak{S}_{nm}$ and thus allows defining a $\mathbb{C}\mathfrak{S}_{nm}$-module $\mathrm{Ind}_{\mathfrak{S}_n \times \mathfrak{S}_m}^{\mathfrak{S}_{nm}} (U \otimes V)$ for any $\mathbb{C}\mathfrak{S}_n$-module U and any $\mathbb{C}\mathfrak{S}_m$-module V. This gives a binary operation on $A(\mathfrak{S})$. Show that this operation corresponds to $\boxdot$ under the PSH-isomorphism $\mathrm{ch} : A(\mathfrak{S}) \to \Lambda$.]

Remark 4.4.10. The statements (and the idea of the solution) of Exercise 4.4.9 are due to Manuel Maia and Miguel Méndez (see [144] and, more explicitly, [155]), who call the operation $\boxdot$ the *arithmetic product*. Li [131, Thm. 3.5] denotes it by $\boxtimes$ and relates it to the enumeration of unlabelled graphs.

4.5. **Wreath products.** Next consider the tower of groups $G_n = \mathfrak{S}_n[\Gamma]$ for a finite group Γ, and the Hopf algebra $A = A(G_*) =: A(\mathfrak{S}[\Gamma])$. Recall (from Theorem 4.4.1) that irreducible complex representations χ^λ of $\mathfrak{S}_n$ are indexed by partitions λ in Par_n. Index the irreducible complex representations of Γ as $\mathrm{Irr}(\Gamma) = \{\rho_1, \ldots, \rho_d\}$.

Definition 4.5.1. Define for a partition λ in Par_n and ρ in $\mathrm{Irr}(\Gamma)$ a representation $\chi^{\lambda,\rho}$ of $\mathfrak{S}_n[\Gamma]$ in which σ in $\mathfrak{S}_n$ and $\gamma = (\gamma_1, \ldots, \gamma_n)$ in Γ^n act on the space $\chi^\lambda \otimes (\rho^{\otimes n})$ as follows:

$$\begin{aligned} \sigma(u \otimes (v_1 \otimes \cdots \otimes v_n)) &= \sigma(u) \otimes (v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(n)}); \\ \gamma(u \otimes (v_1 \otimes \cdots \otimes v_n)) &= u \otimes (\gamma_1 v_1 \otimes \cdots \otimes \gamma_n v_n). \end{aligned} \tag{4.5.1}$$

Theorem 4.5.2. *The irreducible $\mathbb{C}\mathfrak{S}_n[\Gamma]$-modules are the induced characters*

$$\chi^{\underline{\lambda}} := \mathrm{Ind}_{\mathfrak{S}_{\deg(\underline{\lambda})}[\Gamma]}^{\mathfrak{S}_n[\Gamma]} \left(\chi^{\lambda^{(1)},\rho_1} \otimes \cdots \otimes \chi^{\lambda^{(d)},\rho_d} \right)$$

as $\underline{\lambda}$ runs through all functions

$$\begin{array}{ccc} \mathrm{Irr}(\Gamma) & \xrightarrow{\underline{\lambda}} & \mathrm{Par}, \\ \rho_i & \longmapsto & \lambda^{(i)} \end{array}$$

with the property that $\sum_{i=1}^d |\lambda^{(i)}| = n$. Here, $\deg(\underline{\lambda})$ denotes the d-tuple $\left(\left|\lambda^{(1)}\right|, \left|\lambda^{(2)}\right|, \ldots, \left|\lambda^{(d)}\right|\right) \in \mathbb{N}^d$, and $\mathfrak{S}_{\deg(\underline{\lambda})}$ is defined as the subgroup $\mathfrak{S}_{\left|\lambda^{(1)}\right|} \times \mathfrak{S}_{\left|\lambda^{(2)}\right|} \times \cdots \times \mathfrak{S}_{\left|\lambda^{(d)}\right|}$ of $\mathfrak{S}_n$.

Furthermore, one has a PSH-isomorphism

$$\begin{array}{ccc} A(\mathfrak{S}[\Gamma]) & \longrightarrow & \Lambda^{\otimes d}, \\ \chi^{\underline{\lambda}} & \longmapsto & s_{\lambda^{(1)}} \otimes \cdots \otimes s_{\lambda^{(d)}}. \end{array}$$

Proof. We know from Corollary 4.3.10 that $A(\mathfrak{S}[\Gamma])$ is a PSH, with PSH-basis Σ given by the union of all irreducible characters of all groups $\mathfrak{S}_n[\Gamma]$. Therefore Theorem 3.2.3 tells us that $A(\mathfrak{S}[\Gamma]) \cong \bigotimes_{\rho \in \mathcal{C}} A(\mathfrak{S}[\Gamma])(\rho)$ where $\mathcal{C}$ is the set of irreducible characters which are also primitive. Just as in the case of $\mathfrak{S}_n$, it is clear from the definition of the coproduct that an irreducible character ρ of $\mathfrak{S}_n[\Gamma]$ is primitive if and only if $n = 1$, that in this case $\mathfrak{S}_n[\Gamma] = \Gamma$, and ρ lies in $\mathrm{Irr}(\Gamma) = \{\rho_1, \ldots, \rho_d\}$.

The remaining assertions of the theorem will then follow from the definition of the induction product algebra structure on $A(\mathfrak{S}[\Gamma])$, once we have shown that, for every $\rho \in \mathrm{Irr}(\Gamma)$, there is a PSH-isomorphism sending

$$\begin{array}{ccc} A(\mathfrak{S}) & \longrightarrow & A(\mathfrak{S}[\Gamma])(\rho), \\ \chi^\lambda & \longmapsto & \chi^{\lambda,\rho}. \end{array} \tag{4.5.2}$$

[238] This is well-defined, since $(p_\lambda)_{\lambda \in \mathrm{Par}}$ is a $\mathbb{Q}$-module basis of $\Lambda_{\mathbb{Q}}$.

Such an isomorphism comes from applying Proposition 4.1.17 to the semidirect product $\mathfrak{S}_n[\Gamma] = \mathfrak{S}_n \ltimes \Gamma^n$, so that $K = \Gamma^n, G = \mathfrak{S}_n$, and fixing $V = \rho^{\otimes n}$ as $\mathbb{C}\mathfrak{S}_n[\Gamma]$-module with structure as defined in (4.5.1) (but with λ set to (n), so that χ^λ is the trivial 1-dimensional $\mathbb{C}\mathfrak{S}_n$-module). One obtains for each n, maps

$$R(\mathfrak{S}_n) \underset{\Psi}{\overset{\Phi}{\rightleftharpoons}} R(\mathfrak{S}_n[\Gamma])$$

where

$$\begin{array}{rcl} \chi & \overset{\Phi}{\longmapsto} & \chi \otimes (\rho^{\otimes n}), \\ \alpha & \overset{\Psi}{\longmapsto} & \mathrm{Hom}_{\mathbb{C}\Gamma^n}(\rho^{\otimes n}, \alpha). \end{array}$$

Taking the direct sum of these maps for all n gives maps $A(\mathfrak{S}) \underset{\Psi}{\overset{\Phi}{\rightleftharpoons}} A(\mathfrak{S}[\Gamma])$.

These maps are coalgebra morphisms because of their interaction with restriction to $\mathfrak{S}_i \times \mathfrak{S}_j$. Since Proposition 4.1.17(iii) gives the adjointness property that

$$(\chi, \Psi(\alpha))_{A(\mathfrak{S})} = (\Phi(\chi), \alpha)_{A(\mathfrak{S}[\Gamma])},$$

one concludes from the self-duality of $A(\mathfrak{S}), A(\mathfrak{S}[\Gamma])$ that Φ, Ψ are also algebra morphisms. Since they take genuine characters to genuine characters, they are PSH-morphisms. Since ρ being a simple $\mathbb{C}\Gamma$-module implies that $V = \rho^{\otimes n}$ is a simple $\mathbb{C}\Gamma^n$-module, Proposition 4.1.17(iv) shows that

$$(\Psi \circ \Phi)(\chi) = \chi \tag{4.5.3}$$

for all $\mathfrak{S}_n$-characters χ. Hence Φ is an injective PSH-morphism. Using adjointness, (4.5.3) also shows that Φ sends $\mathbb{C}\mathfrak{S}_n$-simples χ to $\mathbb{C}[\mathfrak{S}_n[\Gamma]]$-simples $\Phi(\chi)$:

$$(\Phi(\chi), \Phi(\chi))_{A(\mathfrak{S}[\Gamma])} = ((\Psi \circ \Phi)(\chi), \chi)_{A(\mathfrak{S})} = (\chi, \chi)_{A(\mathfrak{S})} = 1.$$

Since $\Phi(\chi) = \chi \otimes (\rho^{\otimes n})$ has $V = \rho^{\otimes n}$ as a constituent upon restriction to Γ^n, Frobenius Reciprocity shows that the irreducible character $\Phi(\chi)$ is a constituent of $\mathrm{Ind}_{\Gamma^n}^{\mathfrak{S}_n[\Gamma]} \rho^{\otimes n} = \rho^n$. Hence the entire image of Φ lies in $A(\mathfrak{S}[\Gamma])(\rho)$ (due to how we defined $A(\rho)$ in the proof of Theorem 3.2.3), and so Φ must restrict to an isomorphism as desired in (4.5.2). □

One of Zelevinsky's sample applications of the theorem is this branching rule.

Corollary 4.5.3. *Given $\underline{\lambda} = (\lambda^{(1)}, \ldots, \lambda^{(d)})$ with $\sum_{i=1}^d |\lambda^{(i)}| = n$, one has*

$$\mathrm{Res}^{\mathfrak{S}_n[\Gamma]}_{\mathfrak{S}_{n-1}[\Gamma]\times\Gamma}\left(\chi^{\underline{\lambda}}\right) = \sum_{i=1}^{d} \sum_{\substack{\lambda_-^{(i)} \subseteq \lambda^{(i)}: \\ |\lambda^{(i)}/\lambda_-^{(i)}|=1}} \chi^{(\lambda^{(1)}, \ldots, \lambda_-^{(i)}, \ldots, \lambda^{(d)})} \otimes \rho_i.$$

(We are identifying functions $\underline{\lambda} : \mathrm{Irr}(\Gamma) \to \mathrm{Par}$ with the corresponding d-tuples $\left(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(d)}\right)$ here.)

Example 4.5.4. For Γ a two-element group, so $\mathrm{Irr}(\Gamma) = \{\rho_1, \rho_2\}$ and $d = 2$, then

$$\mathrm{Res}^{\mathfrak{S}_6[\Gamma]}_{\mathfrak{S}_5[\Gamma]\times\Gamma}\left(\chi^{((3,1),(1,1))}\right) = \chi^{((3),(1,1))} \otimes \rho_1 + \chi^{((2,1),(1,1))} \otimes \rho_1 + \chi^{((3,1),(1))} \otimes \rho_2.$$

Proof of Corollary 4.5.3. By Theorem 4.5.2, this is equivalent to computing in the Hopf algebra $A := \Lambda^{\otimes d}$ the component of the coproduct of $s_{\lambda^{(1)}} \otimes \cdots \otimes s_{\lambda^{(d)}}$ that lies in $A_{n-1} \otimes A_1$. Working within each tensor factor Λ, we conclude from Proposition 2.3.6(iv) that the $\Lambda_{|\lambda|-1} \otimes \Lambda_1$-component of $\Delta(s_\lambda)$ is

$$\sum_{\substack{\lambda_- \subseteq \lambda: \\ |\lambda/\lambda_-|=1}} s_{\lambda_-} \otimes \rho.$$

One must apply this in each of the d tensor factors of $A = \Lambda^{\otimes d}$, then sum on i. □

4.6. **General linear groups.** We now consider the tower of finite general linear groups $G_n = GL_n = GL_n(\mathbb{F}_q)$ and $A = A(G_*) =: A(GL)$. Corollary 4.3.10 tells us that $A(GL)$ is a PSH, with PSH-basis Σ given by the union of all irreducible characters of all groups GL_n. Therefore Theorem 3.2.3 tells us that

$$A(GL) \cong \bigotimes_{\rho \in \mathcal{C}} A(GL)(\rho) \tag{4.6.1}$$

where $\mathcal{C} = \Sigma \cap \mathfrak{p}$ is the set of primitive irreducible characters.

Definition 4.6.1. Call an irreducible representation ρ of GL_n *cuspidal* for $n \geq 1$ if it lies in $\mathcal{C}$, that is, its restriction to proper parabolic subgroups $P_{i,j}$ with $i+j = n$ and $i, j > 0$ contain no nonzero vectors which are $K_{i,j}$-invariant. Given an irreducible character σ of GL_n, say that $d(\sigma) = n$, and let $\mathcal{C}_n := \{\rho \in \mathcal{C} : d(\rho) = n\}$ for $n \geq 1$ denote the subset of cuspidal characters of GL_n.

Just as was the case for $\mathfrak{S}_1$ and $\mathfrak{S}_1[\Gamma] = \Gamma$, *every* irreducible character ρ of $GL_1(\mathbb{F}_q) = \mathbb{F}_q^\times$ is cuspidal. However, this does not exhaust the cuspidal characters. In fact, one can predict the number of cuspidal characters in $\mathcal{C}_n$, using knowledge of the number of conjugacy classes in GL_n. Let $\mathcal{F}$ denote the set of all nonconstant monic irreducible polynomials $f(x) \neq x$ in $\mathbb{F}_q[x]$. Let $\mathcal{F}_n := \{f \in \mathcal{F} : \deg(f) = n\}$ for $n \geq 1$.

Proposition 4.6.2. *The number $|\mathcal{C}_n|$ of cuspidal characters of $GL_n(\mathbb{F}_q)$ is the number of $|\mathcal{F}_n|$ of irreducible monic degree n polynomials $f(x) \neq x$ in $\mathbb{F}_q[x]$ with nonzero constant term.*

Proof. We show $|\mathcal{C}_n| = |\mathcal{F}_n|$ for $n \geq 1$ by strong induction on n. For the base case[239] $n = 1$, just as with the families $G_n = \mathfrak{S}_n$ and $G_n = \mathfrak{S}_n[\Gamma]$, when $n = 1$ any irreducible character χ of $G_1 = GL_1(\mathbb{F}_q)$ gives a primitive element of $A = A(GL)$, and hence is cuspidal. Since $GL_1(\mathbb{F}_q) = \mathbb{F}_q^\times$ is abelian, there are $|\mathbb{F}_q^\times| = q-1$ such cuspidal characters in $\mathcal{C}_1$, which agrees with the fact that there are $q-1$ monic (irreducible) linear polynomials $f(x) \neq x$ in $\mathbb{F}_q[x]$, namely $\mathcal{F}_1 := \{f(x) = x - c : c \in \mathbb{F}_q^\times\}$.

In the inductive step, use the fact that the number $|\Sigma_n|$ of irreducible complex characters χ of $GL_n(\mathbb{F}_q)$ equals its number of conjugacy classes. These conjugacy classes are uniquely represented by *rational canonical forms*, which are parametrized by functions $\underline{\lambda} : \mathcal{F} \to \mathrm{Par}$ with the property that $\sum_{f \in \mathcal{F}} \deg(f) |\underline{\lambda}(f)| = n$. On the other hand, (4.6.1) tells us that $|\Sigma_n|$ is similarly parametrized by the functions $\underline{\lambda} : \mathcal{C} \to \mathrm{Par}$ having the property that $\sum_{\rho \in \mathcal{C}} d(\rho) |\underline{\lambda}(\rho)| = n$. Thus we have parallel disjoint decompositions

$$\begin{aligned} \mathcal{C} &= \textstyle\bigsqcup_{n \geq 1} \mathcal{C}_n \quad \text{where } \mathcal{C}_n = \{\rho \in \mathcal{C} : d(\rho) = n\}, \\ \mathcal{F} &= \textstyle\bigsqcup_{n \geq 1} \mathcal{F}_n \quad \text{where } \mathcal{F}_n = \{f \in \mathcal{F} : \deg(f) = n\}, \end{aligned}$$

and hence an equality for all $n \geq 1$

$$\left| \left\{ \mathcal{C} \xrightarrow{\underline{\lambda}} \mathrm{Par} : \quad \sum_{\rho \in \mathcal{C}} d(\rho) |\underline{\lambda}(\rho)| = n \right\} \right| = |\Sigma_n| = \left| \left\{ \mathcal{F} \xrightarrow{\underline{\lambda}} \mathrm{Par} : \quad \sum_{f \in \mathcal{F}} \deg(f) |\underline{\lambda}(f)| = n \right\} \right|.$$

Since there is only one partition λ having $|\lambda| = 1$ (namely, $\lambda = (1)$), this leads to parallel recursions

$$\begin{aligned} |\mathcal{C}_n| &= |\Sigma_n| - \left| \left\{ \bigsqcup_{i=1}^{n-1} \mathcal{C}_i \xrightarrow{\underline{\lambda}} \mathrm{Par} : \quad \sum_{\rho \in \mathcal{C}} d(\rho) |\underline{\lambda}(\rho)| = n \right\} \right|, \\ |\mathcal{F}_n| &= |\Sigma_n| - \left| \left\{ \bigsqcup_{i=1}^{n-1} \mathcal{F}_i \xrightarrow{\underline{\lambda}} \mathrm{Par} : \quad \sum_{f \in \mathcal{F}} \deg(f) |\underline{\lambda}(f)| = n \right\} \right|, \end{aligned}$$

and induction implies that $|\mathcal{C}_n| = |\mathcal{F}_n|$. □

We shall use the notation $\underline{1}_H$ for the trivial character of a group H whenever H is a finite group. This generalizes the notations $\underline{1}_{\mathfrak{S}_n}$ and $\underline{1}_{\mathfrak{S}_\lambda}$ introduced above.

[239] Actually, we don't need any base case for our strong induction. We nevertheless handle the case $n = 1$ as a warmup.

Example 4.6.3. Taking $q = 2$, let us list the sets $\mathcal{F}_n$ of monic irreducible polynomials $f(x) \neq x$ in $\mathbb{F}_2[x]$ of degree n for $n \leq 3$, so that we know how many cuspidal characters of $GL_n(\mathbb{F}_q)$ in $\mathcal{C}_n$ to expect:

$$\mathcal{F}_1 = \{x+1\};$$
$$\mathcal{F}_2 = \{x^2+x+1\};$$
$$\mathcal{F}_3 = \{x^3+x+1, x^3+x^2+1\}.$$

Thus we expect

- one cuspidal character of $GL_1(\mathbb{F}_2)$, namely $\rho_1 (= \underline{1}_{GL_1(\mathbb{F}_2)})$,
- one cuspidal character ρ_2 of $GL_2(\mathbb{F}_2)$, and
- two cuspidal characters ρ_3, ρ_3' of $GL_3(\mathbb{F}_2)$.

We will say more about ρ_2, ρ_3, ρ_3' in the next section.

Exercise 4.6.4. Let $\mu : \{1,2,3,\ldots\} \to \mathbb{Z}$ denote the *number-theoretic Möbius function*, defined by setting $\mu(m) = (-1)^d$ if $m = p_1 \cdots p_d$ for d distinct primes $p_1, p_2, \ldots, p_d$, and $\mu(m) = 0$ if m is not squarefree.

(a) Show that for $n \geq 2$, we have

$$|\mathcal{C}_n| (= |\mathcal{F}_n|) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d. \tag{4.6.2}$$

(Here, the summation sign $\sum_{d|n}$ means a sum over all positive divisors d of n.)

(b) Show that (4.6.2) also counts the *necklaces* with n beads of q colors (= the equivalence classes under the $\mathbb{Z}/n\mathbb{Z}$-action of cyclic rotation on sequences $(a_1, \ldots, a_n)$ in $\mathbb{F}_q^n$) which are *primitive* in the sense that no nontrivial rotation fixes any of the sequences within the equivalence class. For example, when $q = 2$, here are systems of distinct representatives of these primitive necklaces for $n = 2, 3, 4$:

$$n = 2: \quad \{(0,1)\};$$
$$n = 3: \quad \{(0,0,1), (0,1,1)\};$$
$$n = 4: \quad \{(0,0,0,1), (0,0,1,1), (0,1,1,1)\}.$$

The result of Exercise 4.6.4(a) was stated by Gauss for prime q, and by Witt for general q; it is discussed in [37], [182, Section 7.6.2] and (for prime q) [84, (4.12.3)]. Exercise 4.6.4(b) is also well-known. See [182, Section 7.6.2] for a bijection explaining why the answers to both parts of Exercise 4.6.4 are the same.

4.7. **Steinberg's unipotent characters.** Not surprisingly, the (cuspidal) character $\iota := \underline{1}_{GL_1}$ of $GL_1(\mathbb{F}_q)$ plays a distinguished role. The parabolic subgroup $P_{(1^n)}$ of $GL_n(\mathbb{F}_q)$ is the Borel subgroup B of upper triangular matrices, and we have $\iota^n = \mathrm{Ind}_B^{GL_n} \underline{1}_B = \mathbb{C}[GL_n/B]$ (identifying representations with their characters as usual)[240]. The subalgebra $A(GL)(\iota)$ of $A(GL)$ is the $\mathbb{Z}$-span of the irreducible characters σ that appear as constituents of $\iota^n = \mathrm{Ind}_B^{GL_n} \underline{1}_B = \mathbb{C}[GL_n/B]$ for some n.

Definition 4.7.1. An irreducible character σ of GL_n appearing as a constituent of $\mathrm{Ind}_B^{GL_n} \underline{1}_B = \mathbb{C}[GL_n/B]$ is called a *unipotent character*. Equivalently, by Frobenius reciprocity, σ is unipotent if it contains a nonzero B-invariant vector.

In particular, $\underline{1}_{GL_n}$ is a unipotent character of GL_n for each n.

Proposition 4.7.2. *One can choose $\Lambda \cong A(GL)(\iota)$ in Theorem 3.3.3(g) so that $h_n \longmapsto \underline{1}_{GL_n}$.*

---

[240] *Proof.* Exercise 4.3.11(d) (applied to $G_* = GL_*$, $\ell = n$, $\alpha = (1^n) = \left(\underbrace{1,1,\ldots,1}_{n \text{ times}}\right)$ and $\chi_i = \iota$) gives

$$\iota^n = \mathrm{ind}_{(1^n)}^n \iota^{\otimes n} = \underbrace{\mathrm{Ind}_{P_{(1^n)}}^{G_n}}_{=\mathrm{Ind}_B^{GL_n}} \underbrace{\mathrm{Infl}_{G_{(1^n)}}^{P_{(1^n)}} \iota^{\otimes n}}_{=\underline{1}_{P_{(1^n)}} = \underline{1}_B} = \mathrm{Ind}_B^{GL_n} \underline{1}_B = \mathbb{C}\left[GL_n/B\right],$$

where the last equality follows from the general fact that if G is a finite group and H is a subgroup of G, then $\mathrm{Ind}_H^G \underline{1}_H \cong \mathbb{C}\left[G/H\right]$ as $\mathbb{C}G$-modules.

Proof. Theorem 3.3.1(a) tells us $\iota^2 = \mathrm{Ind}_B^{GL_2} \underline{1}_B$ must have exactly two irreducible constituents, one of which is $\underline{1}_{GL_2}$; call the other one St_2. Choose the isomorphism so as to send $h_2 \longmapsto \underline{1}_{GL_2}$. Then $h_n \mapsto \underline{1}_{GL_n}$ follows from the claim that $\mathrm{St}_2^{\perp}(\underline{1}_{GL_n}) = 0$ for $n \geq 2$: one has

$$\Delta(\underline{1}_{GL_n}) = \sum_{i+j=n} \left(\mathrm{Res}^{G_n}_{P_{i,j}} \underline{1}_{GL_n}\right)^{K_{i,j}} = \sum_{i+j=n} \underline{1}_{GL_i} \otimes \underline{1}_{GL_j}$$

so that $\mathrm{St}_2^{\perp}(\underline{1}_{GL_n}) = (\mathrm{St}_2, \underline{1}_{GL_2})\underline{1}_{GL_{n-2}} = 0$ since $\mathrm{St}_2 \neq \underline{1}_{GL_2}$.

□

This subalgebra $A(GL)(\iota)$, and the unipotent characters χ_q^λ corresponding under this isomorphism to the Schur functions s_λ, were introduced by Steinberg [208]. He wrote down χ_q^λ as a virtual sum of induced characters $\mathrm{Ind}_{P_\alpha}^{GL_n} \underline{1}_{P_\alpha} (= \underline{1}_{G_{\alpha_1}} \cdots \underline{1}_{G_{\alpha_\ell}})$, modelled on the Jacobi-Trudi determinantal expression for $s_\lambda = \det(h_{\lambda_i - i+j})$. Note that $\mathrm{Ind}_{P_\alpha}^{GL_n} \underline{1}_{P_\alpha}$ is the transitive permutation representation $\mathbb{C}[G/P_\alpha]$ for GL_n permuting the *finite partial flag variety* G/P_α, that is, the set of *α-flags of subspaces*

$$\{0\} \subset V_{\alpha_1} \subset V_{\alpha_1+\alpha_2} \subset \cdots \subset V_{\alpha_1+\alpha_2+\cdots+\alpha_{\ell-1}} \subset \mathbb{F}_q^n$$

where $\dim_{\mathbb{F}_q} V_d = d$ in each case. This character has dimension equal to $|G/P_\alpha|$, with formula given by the *q-multinomial coefficient* (see e.g. Stanley [206, §1.7]):

$$\begin{bmatrix} n \\ \alpha \end{bmatrix}_q = \frac{[n]!_q}{[\alpha_1]!_q \cdots [\alpha_\ell]!_q}$$

where $[n]!_q := [n]_q[n-1]_q \cdots [2]_q[1]_q$ and $[n]_q := 1 + q + \cdots + q^{n-1} = \frac{q^n-1}{q-1}$.

Our terminology St_2 is motivated by the $n = 2$ special case of the *Steinberg character* St_n, which is the unipotent character corresponding under the isomorphism in Proposition 4.7.2 to $e_n = s_{(1^n)}$. It can be defined by the virtual sum

$$\mathrm{St}_n := \chi_q^{(1^n)} = \sum_\alpha (-1)^{n-\ell(\alpha)} \mathrm{Ind}_{P_\alpha}^{GL_n} \underline{1}_{P_\alpha}$$

in which the sum runs through all compositions α of n. This turns out to be the genuine character for $GL_n(\mathbb{F}_q)$ acting on the top homology group of its *Tits building*: the simplicial complex whose vertices are nonzero proper subspaces V of $\mathbb{F}_q^n$, and whose simplices correspond to flags of nested subspaces. One needs to know that this Tits building has only top homology, so that one can deduce the above character formula from the Hopf trace formula; see Björner [22].

4.8. **Examples: $GL_2(\mathbb{F}_2)$ and $GL_3(\mathbb{F}_2)$.** Let's get our hands dirty.

Example 4.8.1. For $n = 2$, there are two unipotent characters, $\chi_q^{(2)} = \underline{1}_{GL_2}$ and

$$\mathrm{St}_2 := \chi_q^{(1,1)} = \underline{1}_{GL_1}^2 - \underline{1}_{GL_2} = \mathrm{Ind}_B^{GL_2} \underline{1}_B - \underline{1}_{GL_2} \tag{4.8.1}$$

since the Jacobi-Trudi formula (2.4.16) gives $s_{(1,1)} = \det \begin{bmatrix} h_1 & h_2 \\ 1 & h_1 \end{bmatrix} = h_1^2 - h_2$. The description (4.8.1) for this Steinberg character St_2 shows that it has dimension

$$|GL_2/B| - 1 = (q+1) - 1 = q$$

and that one can think of it as follows: consider the permutation action of GL_2 on the $q+1$ lines $\{\ell_0, \ell_1, \ldots, \ell_q\}$ in the projective space $\mathbb{P}^1_{\mathbb{F}_q} = GL_2(\mathbb{F}_q)/B$, and take the invariant subspace perpendicular to the sum of basis elements $e_{\ell_0} + \cdots + e_{\ell_q}$.

Example 4.8.2. Continuing the previous example, but taking $q = 2$, we find that we have constructed two unipotent characters: $\underline{1}_{GL_2} = \chi_{q=2}^{(2)}$ of dimension 1, and $\mathrm{St}_2 = \chi_{q=2}^{(1,1)}$ of dimension $q = 2$. This lets us identify the unique cuspidal character ρ_2 of $GL_2(\mathbb{F}_2)$, using knowledge of the character table of $GL_2(\mathbb{F}_2) \cong \mathfrak{S}_3$:

		$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	$\begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}1&0\\1&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}$	$\begin{bmatrix}1&1\\1&0\end{bmatrix}, \begin{bmatrix}0&1\\1&1\end{bmatrix}$
$\underline{1}_{GL_2} = \chi^{(2)}_{q=2}$	unipotent	1	1	1
$\mathrm{St}_2 = \chi^{(1,1)}_{q=2}$	unipotent	2	0	-1
ρ_2	cuspidal	1	-1	1

In other words, the cuspidal character ρ_2 of $GL_2(\mathbb{F}_2)$ corresponds under the isomorphism $GL_2(\mathbb{F}_2) \cong \mathfrak{S}_3$ to the sign character $\mathrm{sgn}_{\mathfrak{S}_3}$.

Example 4.8.3. Continuing the previous example to $q = 2$ and $n = 3$ lets us analyze the irreducible characters of $GL_3(\mathbb{F}_2)$. Recalling our labelling $\rho_1, \rho_2, \rho_3, \rho_3'$ from Example 4.6.3 of the cuspidal characters of $GL_n(\mathbb{F}_2)$ for $n = 1, 2, 3$, Zelevinsky's Theorem 3.2.3 tells us that the $GL_3(\mathbb{F}_2)$-irreducible characters should be labelled by functions $\{\rho_1, \rho_2, \rho_3, \rho_3'\} \xrightarrow{\underline{\lambda}} \mathrm{Par}$ for which

$$1 \cdot |\underline{\lambda}(\rho_1)| + 2 \cdot |\underline{\lambda}(\rho_2)| + 3 \cdot |\underline{\lambda}(\rho_3)| + 3 \cdot |\underline{\lambda}(\rho_3')| = 3.$$

We will label such an irreducible character $\chi^{\underline{\lambda}} = \chi^{(\underline{\lambda}(\rho_1), \underline{\lambda}(\rho_2), \underline{\lambda}(\rho_3), \underline{\lambda}(\rho_3'))}$.

Three of these irreducibles will be the unipotent characters, mapping under the isomorphism from Proposition 4.7.2 as follows:

- $s_{(3)} = h_3 \longmapsto \chi^{((3),\varnothing,\varnothing,\varnothing)} = \underline{1}_{GL_3}$ of dimension 1.
- $$s_{(2,1)} = \det \begin{bmatrix} h_2 & h_3 \\ 1 & h_1 \end{bmatrix} = h_2 h_1 - h_3 \longmapsto \chi^{((2,1),\varnothing,\varnothing,\varnothing)} = \mathrm{Ind}_{P_{2,1}}^{GL_3} \underline{1}_{P_{2,1}} - \underline{1}_{GL_3},$$
  of dimension $\begin{bmatrix} 3 \\ 2,1 \end{bmatrix}_q - \begin{bmatrix} 3 \\ 3 \end{bmatrix}_q = [3]_q - 1 = q^2 + q \overset{q=2}{\rightsquigarrow} 6.$
- Lastly,
$$s_{(1,1,1)} = \det \begin{bmatrix} h_1 & h_2 & h_3 \\ 1 & h_1 & h_2 \\ 0 & 1 & h_1 \end{bmatrix} = h_1^3 - h_2 h_1 - h_1 h_2 + h_3$$
$$\longmapsto \mathrm{St}_3 = \chi^{((1,1,1),\varnothing,\varnothing,\varnothing)} = \mathrm{Ind}_B^{GL_3} \underline{1}_B - \mathrm{Ind}_{P_{2,1}}^{GL_3} \underline{1}_{P_{2,1}} - \mathrm{Ind}_{P_{1,2}}^{GL_3} \underline{1}_{P_{1,2}} + \underline{1}_{GL_3}$$
  of dimension
$$\begin{bmatrix} 3 \\ 1,1,1 \end{bmatrix}_q - \begin{bmatrix} 3 \\ 2,1 \end{bmatrix}_q - \begin{bmatrix} 3 \\ 1,2 \end{bmatrix}_q + \begin{bmatrix} 3 \\ 3 \end{bmatrix}_q$$
$$= [3]!_q - [3]_q - [3]_q + 1 = q^3 \overset{q=2}{\rightsquigarrow} 8.$$

There should also be one non-unipotent, non-cuspidal character, namely

$$\chi^{((1),(1),\varnothing,\varnothing)} = \rho_1 \rho_2 = \mathrm{Ind}_{P_{1,2}}^{GL_3} \mathrm{Infl}_{GL_1 \times GL_2}^{P_{1,2}} \left(\underline{1}_{GL_1} \otimes \rho_2 \right)$$

having dimension $\begin{bmatrix} 3 \\ 1,2 \end{bmatrix}_q \cdot 1 \cdot 1 = [3]_q \overset{q=2}{\rightsquigarrow} 7.$

Finally, we expect cuspidal characters $\rho_3 = \chi^{(\varnothing,\varnothing,(1),\varnothing)}, \rho_3' = \chi^{(\varnothing,\varnothing,\varnothing,(1))}$, whose dimensions d_3, d_3' can be deduced from the equation

$$1^2 + 6^2 + 8^2 + 7^2 + d_3^2 + (d_3')^2 = |GL_3(\mathbb{F}_2)| = \left[(q^3 - q^0)(q^3 - q^1)(q^3 - q^2) \right]_{q=2} = 168.$$

This forces $d_3^2 + (d_3')^2 = 18$, whose only solution in positive integers is $d_3 = d_3' = 3$.

We can check our predictions of the dimensions for the various $GL_3(\mathbb{F}_2)$-irreducible characters since $GL_3(\mathbb{F}_2)$ is the finite simple group of order 168 (also isomorphic to $PSL_2(\mathbb{F}_7)$), with known character table (see James and Liebeck [104, p. 318]):

	centralizer order	168	8	4	3	7	7
	unipotent?/cuspidal?						
$\underline{1}_{GL_3} = \chi^{((3),\varnothing,\varnothing,\varnothing)}$	unipotent	1	1	1	1	1	1
$\chi^{((2,1),\varnothing,\varnothing,\varnothing)}$	unipotent	6	2	0	0	-1	-1
$\mathrm{St}_3 = \chi^{((1,1,1),\varnothing,\varnothing,\varnothing)}$	unipotent	8	0	0	-1	1	1
$\chi^{((1),(1),\varnothing,\varnothing)}$		7	-1	-1	1	0	0
$\rho_3 = \chi^{(\varnothing,\varnothing,(1),\varnothing)}$	cuspidal	3	-1	1	0	α	$\overline{\alpha}$
$\rho_3' = \chi^{(\varnothing,\varnothing,\varnothing,(1))}$	cuspidal	3	-1	1	0	$\overline{\alpha}$	α

Here $\alpha := -1/2 + i\sqrt{7}/2$.

Remark 4.8.4. It is known (see e.g. Bump [30, Cor. 7.4]) that, for $n \geq 2$, the dimension of any cuspidal irreducible character ρ of $GL_n(\mathbb{F}_q)$ is

$$(q^{n-1}-1)(q^{n-2}-1)\cdots(q^2-1)(q-1).$$

Note that when $q = 2$,

- for $n = 2$ this gives $2^1 - 1 = 1$ for the dimension of ρ_2, and
- for $n = 3$ it gives $(2^2-1)(2-1) = 3$ for the dimensions of ρ_3, ρ_3',

agreeing with our calculations above. Much more is known about the character table of $GL_n(\mathbb{F}_q)$; see Remark 4.9.14 below, Zelevinsky [227, Chap. 11], and Macdonald [142, Chap. IV].

4.9. **The Hall algebra.** There is another interesting Hopf subalgebra (and quotient Hopf algebra) of $A(GL)$, related to unipotent conjugacy classes in $GL_n(\mathbb{F}_q)$.

Definition 4.9.1. Say that an element g in $GL_n(\mathbb{F}_q)$ is *unipotent* if its eigenvalues are all equal to 1. Equivalently, $g \in GL_n(\mathbb{F}_q)$ is unipotent if and only if $g - \mathrm{id}_{\mathbb{F}_q^n}$ is nilpotent. A conjugacy class in $GL_n(\mathbb{F}_q)$ is *unipotent* if its elements are unipotent.

Denote by $\mathcal{H}_n$ the $\mathbb{C}$-subspace of $R_{\mathbb{C}}(GL_n)$ consisting of those class functions which are supported only on unipotent conjugacy classes, and let $\mathcal{H} = \bigoplus_{n\geq 0} \mathcal{H}_n$ as a $\mathbb{C}$-subspace of $A_{\mathbb{C}}(GL) = \bigoplus_{n\geq 0} R_{\mathbb{C}}(GL_n)$.

Proposition 4.9.2. *The subspace $\mathcal{H}$ is a Hopf subalgebra of $A_{\mathbb{C}}(GL)$, which is graded, connected, and of finite type, and self-dual with respect to the inner product on class functions inherited from $A_{\mathbb{C}}(GL)$. It is also a quotient Hopf algebra of $A_{\mathbb{C}}(GL)$, as the $\mathbb{C}$-linear surjection $A_{\mathbb{C}}(GL) \twoheadrightarrow \mathcal{H}$ restricting class functions to unipotent classes is a Hopf algebra homomorphism. This surjection has kernel $\mathcal{H}^{\perp}$, which is both an ideal and a two-sided coideal.*

Proof. It is immediately clear that $\mathcal{H}^{\perp}$ is a graded $\mathbb{C}$-vector subspace of $A_{\mathbb{C}}(GL)$, whose n-th homogeneous component consists of those class functions on GL_n whose values on all unipotent classes are 0. (This holds no matter whether the perpendicular space is taken with respect to the Hermitian form $(\cdot,\cdot)_G$ or with respect to the bilinear form $\langle\cdot,\cdot\rangle_G$.) In other words, $\mathcal{H}^{\perp}$ is the kernel of the surjection $A_{\mathbb{C}}(GL) \twoheadrightarrow \mathcal{H}$ defined in the proposition.

Given two class functions χ_i, χ_j on GL_i, GL_j and g in GL_{i+j}, one has

$$(\chi_i \cdot \chi_j)(g) = \frac{1}{|P_{i,j}|} \sum_{\substack{h \in GL_{i+j}: \\ h^{-1}gh = \begin{bmatrix} g_i & * \\ 0 & g_j \end{bmatrix} \in P_{i,j}}} \chi_i(g_i)\chi_j(g_j). \tag{4.9.1}$$

Since g is unipotent if and only if $h^{-1}gh$ is unipotent if and only if both g_i, g_j are unipotent, the formula (4.9.1) shows both that $\mathcal{H}$ is a subalgebra[241] and that $\mathcal{H}^{\perp}$ is a two-sided ideal[242]. It also shows that the surjection $A_{\mathbb{C}}(GL) \twoheadrightarrow \mathcal{H}$ restricting every class function to unipotent classes is an algebra homomorphism[243].

[241] Indeed, if χ_i and χ_j are both supported only on unipotent classes, then the same holds for $\chi_i \cdot \chi_j$.

[242] In fact, if one of χ_i and χ_j annihilates all unipotent classes, then so does $\chi_i \cdot \chi_j$.

[243] because if g is unipotent, then the only values of χ_i and χ_j appearing on the right hand side of (4.9.1) are those on unipotent elements

Similarly, for class functions χ on GL_n and (g_i, g_j) in $GL_{i,j} = GL_i \times GL_j$, one has

$$\Delta(\chi)(g_i, g_j) = \frac{1}{q^{ij}} \sum_{k \in \mathbb{F}_q^{i \times j}} \chi \begin{bmatrix} g_i & k \\ 0 & g_j \end{bmatrix}$$

using (4.1.13). This shows both that $\mathcal{H}$ is a sub-coalgebra of $A = A_{\mathbb{C}}(GL)$ (that is, it satisfies $\Delta\mathcal{H} \subset \mathcal{H} \otimes \mathcal{H}$) and that $\mathcal{H}^{\perp}$ is a two-sided coideal (that is, we have $\Delta(\mathcal{H}^{\perp}) \subset \mathcal{H}^{\perp} \otimes A + A \otimes \mathcal{H}^{\perp}$), since it shows that if χ is supported only on unipotent classes, then $\Delta(\chi)$ vanishes on (g_1, g_2) that have either g_1 or g_2 non-unipotent. It also shows that the surjection $A_{\mathbb{C}}(GL) \twoheadrightarrow \mathcal{H}$ restricting every class function to unipotent classes is a coalgebra homomorphism. The rest follows. □

The subspace $\mathcal{H}$ is called the *Hall algebra*. It has an obvious orthogonal $\mathbb{C}$-basis, with interesting structure constants.

Definition 4.9.3. Given a partition λ of n, let J_λ denote the GL_n-conjugacy class of unipotent matrices whose *Jordan type* (that is, the list of the sizes of the Jordan blocks, in decreasing order) is given by λ. Furthermore, let $z_\lambda(q)$ denote the size of the centralizer of any element of this conjugacy class J_λ.

The indicator class functions[244] $\{\underline{1}_{J_\lambda}\}_{\lambda \in \mathrm{Par}}$ form a $\mathbb{C}$-basis for $\mathcal{H}$ whose multiplicative structure constants are called the *Hall coefficients* $g^{\lambda}_{\mu,\nu}(q)$:

$$\underline{1}_{J_\mu} \underline{1}_{J_\nu} = \sum_{\lambda} g^{\lambda}_{\mu,\nu}(q)\ \underline{1}_{J_\lambda}.$$

Because the dual basis to $\{\underline{1}_{J_\lambda}\}$ is $\{z_\lambda(q)\underline{1}_{J_\lambda}\}$, self-duality of $\mathcal{H}$ shows that the Hall coefficients are (essentially) also structure constants for the comultiplication:

$$\Delta \underline{1}_{J_\lambda} = \sum_{\mu,\nu} g^{\lambda}_{\mu,\nu}(q) \frac{z_\mu(q) z_\nu(q)}{z_\lambda(q)} \cdot \underline{1}_{J_\mu} \otimes \underline{1}_{J_\nu}.$$

The Hall coefficient $g^{\lambda}_{\mu,\nu}(q)$ has the following interpretation.

Proposition 4.9.4. *Fix any g in $GL_n(\mathbb{F}_q)$ acting unipotently on $\mathbb{F}_q^n$ with Jordan type λ. Then $g^{\lambda}_{\mu,\nu}(q)$ counts the g-stable $\mathbb{F}_q$-subspaces $V \subset \mathbb{F}_q^n$ for which the restriction $g|V$ acts with Jordan type μ, and the induced map $\bar{g}$ on the quotient space $\mathbb{F}_q^n/V$ has Jordan type ν.*

Proof. Given μ, ν partitions of i, j with $i + j = n$, taking χ_i, χ_j equal to $\underline{1}_{J_\mu}, \underline{1}_{J_\nu}$ in (4.9.1) shows that for any g in GL_n, the value of $\left(\underline{1}_{J_\mu} \cdot \underline{1}_{J_\nu}\right)(g)$ is given by

$$\frac{1}{|P_{i,j}|} \left| \left\{ h \in GL_n : h^{-1} g h = \begin{bmatrix} g_i & * \\ 0 & g_j \end{bmatrix} \text{ with } g_i \in J_\mu, g_j \in J_\nu \right\} \right|. \tag{4.9.2}$$

Let S denote the set appearing in (4.9.2), and let $\mathbb{F}_q^i$ denote the i-dimensional subspace of $\mathbb{F}_q^n$ spanned by the first i standard basis vectors. Note that the condition on an element h in S saying that $h^{-1}gh$ is in block upper-triangular form can be re-expressed by saying that the subspace $V := h(\mathbb{F}_q^i)$ is g-stable. One then sees that the map $h \stackrel{\varphi}{\longmapsto} V = h(\mathbb{F}_q^i)$ surjects S onto the set of i-dimensional g-stable subspaces V of $\mathbb{F}_q^n$ for which $g|V$ and $\bar{g}$ are unipotent of types μ, ν, respectively. Furthermore, for any particular such V, its fiber $\varphi^{-1}(V)$ in S is a coset of the stabilizer within GL_n of V, which is conjugate to $P_{i,j}$, and hence has cardinality $|\varphi^{-1}(V)| = |P_{i,j}|$. This proves the assertion of the proposition. □

The Hall algebra $\mathcal{H}$ will turn out to be isomorphic to the ring $\Lambda_{\mathbb{C}}$ of symmetric functions with $\mathbb{C}$ coefficients, via a composite φ of three maps

$$\Lambda_{\mathbb{C}} \longrightarrow A(GL)(\iota)_{\mathbb{C}} \longrightarrow A(GL)_{\mathbb{C}} \longrightarrow \mathcal{H}$$

in which the first map is the isomorphism from Proposition 4.7.2, the second is inclusion, and the third is the quotient map from Proposition 4.9.2.

[244] Here we use the following notation: Whenever P is a subset of a group G, we denote by $\underline{1}_P$ the map $G \to \mathbb{C}$ which sends every element of P to 1 and all remaining elements of G to 0. This is not in conflict with the notation $\underline{1}_G$ for the trivial character of G, since $\underline{1}_P = \underline{1}_G$ for $P = G$. Note that $\underline{1}_P$ is a class function when P is a union of conjugacy classes of G.

Theorem 4.9.5. *The above composite φ is a Hopf algebra isomorphism, sending*

$$\begin{aligned} h_n &\longmapsto \sum_{\lambda\in \mathrm{Par}_n} \underline{1}_{J_\lambda}, \\ e_n &\longmapsto q^{\binom{n}{2}} \underline{1}_{J_{(1^n)}}, \\ p_n &\longmapsto \sum_{\lambda\in \mathrm{Par}_n} (q;q)_{\ell(\lambda)-1} \underline{1}_{J_\lambda} \qquad (\text{for } n>0), \end{aligned}$$

where we are using the notation

$$(x;q)_m := (1-x)(1-qx)(1-q^2x)\cdots(1-q^{m-1}x) \qquad \text{for all } m\in\mathbb{N} \text{ and } x \text{ in any ring.}$$

Proof. That φ is a graded Hopf morphism follows because it is a composite of three such morphisms. We claim that once one shows the formula for the (nonzero) image $\varphi(p_n)$ given above is correct, then this will already show φ is an isomorphism, by the following argument. Note first that $\Lambda_{\mathbb{C}}$ and $\mathcal{H}$ both have dimension $|\,\mathrm{Par}_n\,|$ for their n-th homogeneous components, so it suffices to show that the graded map φ is injective. On the other hand, both $\Lambda_{\mathbb{C}}$ and $\mathcal{H}$ are (graded, connected, finite type) *self-dual* Hopf algebras (although with respect to a sesquilinear form), so Theorem 3.1.7 says that each is the symmetric algebra on its space of primitive elements. Thus it suffices to check that φ is injective when restricted to their subspaces of primitives.[245] For $\Lambda_{\mathbb{C}}$, by Corollary 3.1.8 the primitives are spanned by $\{p_1, p_2, \ldots\}$, with only one basis element in each degree $n \geq 1$. Hence φ is injective on the subspace of primitives if and only if it does not annihilate any p_n.

Thus it only remains to show the above formulas for the images of h_n, e_n, p_n under φ. This is clear for h_n, since Proposition 4.7.2 shows that it maps under the first two composites to the indicator function $\underline{1}_{GL_n}$ which then restricts to the sum of indicators $\sum_{\lambda\in\mathrm{Par}_n} \underline{1}_{J_\lambda}$ in $\mathcal{H}$. For e_n, p_n, we resort to generating functions. Let $\tilde{h}_n, \tilde{e}_n, \tilde{p}_n$ denote the three putative images in $\mathcal{H}$ of h_n, e_n, p_n, appearing on the right side in the theorem, and define generating functions

$$\tilde{H}(t) := \sum_{n\geq 0} \tilde{h}_n t^n, \quad \tilde{E}(t) := \sum_{n\geq 0} \tilde{e}_n t^n, \quad \tilde{P}(t) := \sum_{n\geq 0} \tilde{p}_{n+1} t^n \qquad \text{in } \mathcal{H}[[t]].$$

We wish to show that the map $\varphi[[t]] : \Lambda_{\mathbb{C}}[[t]] \to \mathcal{H}[[t]]$ (induced by φ) maps $H(t), E(t), P(t)$ in $\Lambda[[t]]$ to these three generating functions[246]. Since we have already shown this is correct for $H(t)$, by (2.4.3), (2.5.13), it suffices to check that in $\mathcal{H}[[t]]$ one has

$$\begin{aligned} \tilde{H}(t)\tilde{E}(-t) = 1, \quad &\text{or equivalently,} \quad \textstyle\sum_{k=0}^{n} (-1)^k \tilde{e}_k \tilde{h}_{n-k} = \delta_{0,n}; \\ \tilde{H}'(t)\tilde{E}(-t) = \tilde{P}(t), \quad &\text{or equivalently,} \quad \textstyle\sum_{k=0}^{n} (-1)^k (n-k) \tilde{e}_k \tilde{h}_{n-k} = \tilde{p}_n. \end{aligned}$$

Thus it would be helpful to evaluate the class function $\tilde{e}_k \tilde{h}_{n-k}$. Note that a unipotent g in GL_n having ℓ Jordan blocks has an ℓ-dimensional 1-eigenspace, so that the number of k-dimensional g-stable $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$ on which g has Jordan type $\left(1^k\right)$ (that is, on which g acts as the identity) is the *q-binomial coefficient*

$$\begin{bmatrix} \ell \\ k \end{bmatrix}_q = \frac{(q;q)_\ell}{(q;q)_k (q;q)_{\ell-k}},$$

counting k-dimensional $\mathbb{F}_q$-subspaces V of an ℓ-dimensional $\mathbb{F}_q$-vector space; see, e.g., [206, §1.7]. Hence, for a unipotent g in GL_n having ℓ Jordan blocks, we have

$$(\tilde{e}_k \tilde{h}_{n-k})(g) = q^{\binom{k}{2}} \cdot \left(\underline{1}_{J_{(1^k)}} \cdot \tilde{h}_{n-k} \right)(g) = q^{\binom{k}{2}} \cdot \sum_{\nu\in\mathrm{Par}_{n-k}} \left(\underline{1}_{J_{(1^k)}} \cdot \underline{1}_{J_\nu} \right)(g) = q^{\binom{k}{2}} \begin{bmatrix} \ell \\ k \end{bmatrix}_q$$

(by Proposition 4.9.4). Thus one needs for $\ell \geq 1$ that

$$\sum_{k=0}^{\ell} (-1)^k q^{\binom{k}{2}} \begin{bmatrix} \ell \\ k \end{bmatrix}_q = 0, \tag{4.9.3}$$

$$\sum_{k=0}^{\ell} (-1)^k (n-k) q^{\binom{k}{2}} \begin{bmatrix} \ell \\ k \end{bmatrix}_q = (q;q)_{\ell-1}. \tag{4.9.4}$$

[245] An alternative way to see that it suffices to check this is by recalling Exercise 1.4.35(c).

[246] See (2.4.1), (2.4.2), (2.5.13) for the definitions of $H(t), E(t), P(t)$.

Identity (4.9.3) comes from setting $x = 1$ in the *q-binomial theorem* [206, Exer. 3.119]:

$$\sum_{k=0}^{\ell} (-1)^k q^{\binom{k}{2}} \begin{bmatrix} \ell \\ k \end{bmatrix}_q x^{\ell-k} = (x-1)(x-q)(x-q^2)\cdots(x-q^{\ell-1}). \tag{4.9.5}$$

Identity (4.9.4) comes from applying $\frac{d}{dx}$ to (4.9.5), then setting $x = 1$, and finally adding $(n-\ell)$ times (4.9.3). ☐

Exercise 4.9.6. Fix a prime power q. For any $k \in \mathbb{N}$, and any k partitions $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k)}$, we define a family $\left(g^{\lambda}_{\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)}}(q)\right)_{\lambda \in \mathrm{Par}}$ of elements of $\mathbb{C}$ by the equation

$$\underline{1}_{J_{\lambda^{(1)}}} \underline{1}_{J_{\lambda^{(2)}}} \cdots \underline{1}_{J_{\lambda^{(k)}}} = \sum_{\lambda \in \mathrm{Par}} g^{\lambda}_{\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)}}(q)\, \underline{1}_{J_\lambda}$$

in $\mathcal{H}$. This notation generalizes the notation $g^{\lambda}_{\mu,\nu}(q)$ we introduced in Definition 4.9.3. Note that $g^{\lambda}_{\mu}(q) = \delta_{\lambda,\mu}$ for any two partitions λ and μ, and that $g^{\lambda}(q) = \delta_{\lambda,\varnothing}$ for any partition λ (where $g^{\lambda}(q)$ is to be understood as $g^{\lambda}_{\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)}}(q)$ for $k = 0$).

(a) Let $\lambda \in \mathrm{Par}$, and let $n = |\lambda|$. Let V be an n-dimensional $\mathbb{F}_q$-vector space, and let g be a unipotent endomorphism of V having Jordan type λ. Let $k \in \mathbb{N}$, and let $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k)}$ be k partitions. A $\left(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k)}\right)$-*compatible* g-*flag* will mean a sequence $0 = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_k = V$ of g-invariant $\mathbb{F}_q$-vector subspaces V_i of V such that for every $i \in \{1, 2, \ldots, k\}$, the endomorphism of V_i/V_{i-1} induced by g [247] has Jordan type $\lambda^{(i)}$.
Show that $g^{\lambda}_{\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)}}(q)$ is the number of $\left(\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k)}\right)$-compatible g-flags.[248]

(b) Let $\lambda \in \mathrm{Par}$. Let $k \in \mathbb{N}$, and let $\lambda^{(1)}, \lambda^{(2)}, \ldots, \lambda^{(k)}$ be k partitions. Show that $g^{\lambda}_{\lambda^{(1)},\lambda^{(2)},\ldots,\lambda^{(k)}}(q) = 0$ unless $\left|\lambda^{(1)}\right| + \left|\lambda^{(2)}\right| + \cdots + \left|\lambda^{(k)}\right| = |\lambda|$ and $\lambda^{(1)} + \lambda^{(2)} + \cdots + \lambda^{(k)} \trianglerighteq \lambda$. (Here and in the following, we are using the notations of Exercise 2.9.17).

(c) Let $\lambda \in \mathrm{Par}$, and let us write the transpose partition λ^t as $\lambda^t = \left(\left(\lambda^t\right)_1, \left(\lambda^t\right)_2, \ldots, \left(\lambda^t\right)_\ell\right)$. Show that $g^{\lambda}_{\left(1^{(\lambda^t)_1}\right),\left(1^{(\lambda^t)_2}\right),\ldots,\left(1^{(\lambda^t)_\ell}\right)}(q) \neq 0$.

(d) Let $n \in \mathbb{N}$ and $\lambda \in \mathrm{Par}_n$. Show that

$$\varphi(e_\lambda) = \sum_{\mu \in \mathrm{Par}_n;\ \lambda^t \trianglerighteq \mu} \alpha_{\lambda,\mu} \underline{1}_{J_\mu}$$

for some coefficients $\alpha_{\lambda,\mu} \in \mathbb{C}$ satisfying $\alpha_{\lambda,\lambda^t} \neq 0$.

(e) Give another proof of the fact that the map φ is injective.

[**Hint:** For (b), use Exercise 2.9.22(b).]

We next indicate, without proof, how $\mathcal{H}$ relates to the classical Hall algebra.

Definition 4.9.7. Let p be a prime. The usual *Hall algebra*, or what Schiffmann [190, §2.3] calls *Steinitz's classical Hall algebra* (see also Macdonald [142, Chap. II]), has $\mathbb{Z}$-basis elements $\{u_\lambda\}_{\lambda \in \mathrm{Par}}$, with the multiplicative structure constants $g^{\lambda}_{\mu,\nu}(p)$ in

$$u_\mu u_\nu = \sum_\lambda g^{\lambda}_{\mu,\nu}(p)\ u_\lambda$$

defined as follows: fix a finite abelian p-group L of *type* λ, meaning that

$$L \cong \bigoplus_{i=1}^{\ell(\lambda)} \mathbb{Z}/p^{\lambda_i}\mathbb{Z},$$

[247] This is well-defined. In fact, both V_i and V_{i-1} are g-invariant, so that g restricts to an endomorphism of V_i, which further restricts to an endomorphism of V_{i-1}, and thus gives rise to an endomorphism of V_i/V_{i-1}.

[248] This can be seen as a generalization of Proposition 4.9.4. In fact, if μ and ν are two partitions, then a (μ,ν)-compatible g-flag is a sequence $0 = V_0 \subset V_1 \subset V_2 = V$ of g-invariant $\mathbb{F}_q$-vector subspaces V_i of V such that the endomorphism of $V_1/V_0 \cong V_1$ induced by g has Jordan type μ, and the endomorphism of $V_2/V_1 \cong V/V_1$ induced by g has Jordan type ν. Choosing such a sequence amounts to choosing V_1 (since there is only one choice for each of V_0 and V_2), and the conditions on this V_1 are precisely the conditions on V in Proposition 4.9.4.

and let $g^{\lambda}_{\mu,\nu}(p)$ be the number of subgroups M of L of type μ, for which the quotient $N := L/M$ is of type ν. In other words, $g^{\lambda}_{\mu,\nu}(p)$ counts, for a fixed abelian p-group L of type λ, the number of short exact sequences $0 \to M \to L \to N \to 0$ in which M, N have types μ, ν, respectively (modulo isomorphism of short exact sequences restricting to the identity on L).

We claim that when one takes the finite field $\mathbb{F}_q$ of order $q = p$ a *prime*, the $\mathbb{Z}$-linear map

$$u_\lambda \longmapsto \underline{1}_{J_\lambda} \tag{4.9.6}$$

gives an isomorphism from this classical Hall algebra to the $\mathbb{Z}$-algebra $\mathcal{H}_{\mathbb{Z}} \subset \mathcal{H}$. The key point is *Hall's Theorem*, a non-obvious statement for which Macdonald includes two proofs in [142, Chap. II], one of them due to Zelevinsky[249]. To state it, we first recall some notions about discrete valuation rings.

Definition 4.9.8. A *discrete valuation ring* (short *DVR*) $\mathfrak{o}$ is a principal ideal domain having only one maximal ideal $\mathfrak{m} \neq 0$, with quotient $k = \mathfrak{o}/\mathfrak{m}$ called its *residue field*.

The structure theorem for finitely generated modules over a PID implies that an $\mathfrak{o}$-module L with finite composition series of composition length n must have $L \cong \bigoplus_{i=1}^{\ell(\lambda)} \mathfrak{o}/\mathfrak{m}^{\lambda_i}$ for some partition λ of n; say L has *type* λ in this situation.

Here are the two crucial examples for us.

Example 4.9.9. For any field $\mathbb{F}$, the power series ring $\mathfrak{o} = \mathbb{F}[[t]]$ is a DVR with maximal ideal $\mathfrak{m} = (t)$ and residue field $k = \mathfrak{o}/\mathfrak{m} = \mathbb{F}[[t]]/(t) \cong \mathbb{F}$. An $\mathfrak{o}$-module L of type λ is an $\mathbb{F}$-vector space together with an $\mathbb{F}$-linear transformation $T \in \operatorname{End} L$ that acts on L nilpotently (so that $g := T + 1$ acts unipotently, where $1 = \mathrm{id}_L$) with Jordan blocks of sizes given by λ: each summand $\mathfrak{o}/\mathfrak{m}^{\lambda_i} = \mathbb{F}[[t]]/(t^{\lambda_i})$ of L has an $\mathbb{F}$-basis $\{1, t, t^2, \ldots, t^{\lambda_i - 1}\}$ on which the map T that multiplies by t acts as a nilpotent Jordan block of size λ_i. Note also that, in this setting, $\mathfrak{o}$-submodules are the same as T-stable (or g-stable) $\mathbb{F}$-subspaces.

Example 4.9.10. The ring of p-adic integers $\mathfrak{o} = \mathbb{Z}_p$ is a DVR with maximal ideal $\mathfrak{m} = (p)$ and residue field $k = \mathfrak{o}/\mathfrak{m} = \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$. An $\mathfrak{o}$-module L of type λ is an abelian p-group of type λ: for each summand, $\mathfrak{o}/\mathfrak{m}^{\lambda_i} = \mathbb{Z}_p/p^{\lambda_i}\mathbb{Z}_p \cong \mathbb{Z}/p^{\lambda_i}\mathbb{Z}$. Note also that, in this setting, $\mathfrak{o}$-submodules are the same as subgroups.

One last notation: $n(\lambda) := \sum_{i \geq 1} (i-1)\lambda_i$, for λ in Par. Hall's Theorem is as follows.

Theorem 4.9.11. *Assume $\mathfrak{o}$ is a DVR with maximal ideal $\mathfrak{m}$, and that its residue field $k = \mathfrak{o}/\mathfrak{m}$ is finite of cardinality q. Fix an $\mathfrak{o}$-module L of type λ. Then the number of $\mathfrak{o}$-submodules M of type μ for which the quotient $N = L/M$ is of type ν can be written as the specialization*

$$[g^{\lambda}_{\mu,\nu}(t)]_{t=q}$$

of a polynomial $g^{\lambda}_{\mu,\nu}(t)$ in $\mathbb{Z}[t]$, called the Hall polynomial.

Furthermore, the Hall polynomial $g^{\lambda}_{\mu,\nu}(t)$ has degree at most $n(\lambda) - (n(\mu) + n(\nu))$, and its coefficient of $t^{n(\lambda)-(n(\mu)+n(\nu))}$ is the Littlewood-Richardson coefficient $c^{\lambda}_{\mu,\nu}$.

Comparing what Hall's Theorem says in Examples 4.9.9 and 4.9.10, shows that the map (4.9.6) gives the desired isomorphism from the classical Hall algebra to $\mathcal{H}_{\mathbb{Z}}$.

We close this section with some remarks on the vast literature on Hall algebras that we will *not* discuss here.

Remark 4.9.12. Macdonald's version of Hall's Theorem [142, (4.3)] is stronger than Theorem 4.9.11, and useful for certain applications: he shows that $g^{\lambda}_{\mu,\nu}(t)$ is the zero polynomial whenever the Littlewood-Richardson coefficient $c^{\lambda}_{\mu,\nu}$ is zero.

Remark 4.9.13. In general, not all coefficients of the Hall polynomials $g^{\lambda}_{\mu,\nu}(t)$ are nonnegative (see Butler/Hales [32] for a study of when they are); it often happens that $g^{\lambda}_{\mu,\nu}(1) = 0$ despite $g^{\lambda}_{\mu,\nu}(t)$ not being the

[249] See also [190, Thm. 2.6, Prop. 2.7] for quick proofs of part of it, similar to Zelevinsky's. Another proof, based on a recent category-theoretical paradigm, can be found in [61, Theorem 3.53].

zero polynomial[250]. However, in [110, Thm. 4.2], Klein showed that the polynomial values $g^{\lambda}_{\mu,\nu}(p)$ for p prime are always positive when $c^{\lambda}_{\mu,\nu} \neq 0$. (This easily yields the same result for p a prime power.)

Remark 4.9.14. Zelevinsky in [227, Chaps 10, 11] uses the isomorphism $\Lambda_{\mathbb{C}} \to \mathcal{H}$ to derive J. Green's formula for the value of any irreducible character χ of GL_n on any unipotent class J_λ. The answer involves values of irreducible characters of $\mathfrak{S}_n$ along with *Green's polynomials* $Q^{\lambda}_{\mu}(q)$ (see Macdonald [142, §III.7]; they are denoted $Q(\lambda,\mu)$ by Zelevinsky), which express the images under the isomorphism of Theorem 4.9.5 of the symmetric function basis $\{p_\mu\}$ in terms of the basis $\{\underline{1}_{J_\lambda}\}$.

Remark 4.9.15. The Hall polynomials $g^{\lambda}_{\mu,\nu}(t)$ also essentially give the multiplicative structure constants for $\Lambda(\mathbf{x})[t]$ with respect to its basis of *Hall-Littlewood symmetric functions* $P_\lambda = P_\lambda(\mathbf{x};t)$:

$$P_\mu P_\nu = \sum_\lambda t^{n(\lambda)-(n(\mu)+n(\nu))} g^{\lambda}_{\mu,\nu}(t^{-1}) P_\lambda.$$

See Macdonald [142, §III.3].

Remark 4.9.16. Schiffmann [190] discusses self-dual Hopf algebras which vastly generalize the classical Hall algebra called *Ringel-Hall algebras*, associated to abelian categories which are hereditary. Examples come from categories of nilpotent representations of quivers; the quiver having exactly one node and one arc recovers the classical Hall algebra $\mathcal{H}_{\mathbb{Z}}$ discussed above.

Remark 4.9.17. The general linear groups $GL_n(\mathbb{F}_q)$ are one of four families of so-called *classical groups*. Progress has been made on extending Zelevinsky's PSH theory to the other families:

(a) Work of Thiem and Vinroot [217] shows that the tower $\{G_*\}$ of *finite unitary groups* $U_n(\mathbb{F}_{q^2})$ give rise to another positive self-dual Hopf algebra $A = \bigoplus_{n\geq 0} R(U_n(\mathbb{F}_{q^2}))$, in which the role of Harish-Chandra induction is played by *Deligne-Lusztig induction*. In this theory, character and degree formulas for $U_n(\mathbb{F}_{q^2})$ are related to those of $GL_n(\mathbb{F}_q)$ by substituting $q \mapsto -q$, along with appropriate scalings by ± 1, a phenomenon sometimes called *Ennola duality*. See also [207, §4].

(b) van Leeuwen [128] has studied $\bigoplus_{n\geq 0} R\left(Sp_{2n}\left(\mathbb{F}_q\right)\right)$, $\bigoplus_{n\geq 0} R\left(O_{2n}\left(\mathbb{F}_q\right)\right)$ and $\bigoplus_{n\geq 0} R\left(U_n\left(\mathbb{F}_{q^2}\right)\right)$ not as Hopf algebras, but rather as so-called *twisted PSH-modules* over the PSH $A(GL)$ (a "deformed" version of the older notion of Hopf modules). He classified these PSH-modules axiomatically similarly to Zelevinsky's above classification of PSH's.

(c) In a recent honors thesis [201], Shelley-Abrahamson defined yet another variation of the concept of Hopf modules, named 2-*compatible Hopf modules*, and identified $\bigoplus_{n\geq 0} R\left(Sp_{2n}\left(\mathbb{F}_q\right)\right)$ and $\bigoplus_{n\geq 0} R\left(O_{2n+1}\left(\mathbb{F}_q\right)\right)$ as such modules over $A(GL)$.

[250]Actually, Butler/Hales show in [32, proof of Prop. 2.4] that the values $g^{\lambda}_{\mu,\nu}(1)$ are the structure constants of the ring Λ with respect to its basis $(m_\lambda)_{\lambda\in \mathrm{Par}}$: we have

$$m_\mu m_\nu = \sum_{\lambda\in \mathrm{Par}} g^{\lambda}_{\mu,\nu}(1) m_\lambda$$

for all partitions μ and ν.

5. Quasisymmetric functions and P-partitions

We discuss here our next important example of a Hopf algebra arising in combinatorics: the *quasisymmetric functions* of Gessel [79], with roots in work of Stanley [203] on P-partitions. Other treatments of quasisymmetric functions can be found in [206, Section 7.19] and [187, Chapter 8] (with focus on their enumerative applications rather than on their Hopf structure) and in [153, Chapter 6] (with a focus on their representation-theoretical meaning). Quasisymmetric functions have found applications in combinatorial enumeration ([187, Chapter 8], [206, Section 7.19]), topology ([12]) and algebraic geometry ([158], [163]).

5.1. **Definitions, and Hopf structure.** The definitions of quasisymmetric functions require a totally ordered variable set. Usually we will use a variable set denoted $\mathbf{x} = (x_1, x_2, \ldots)$ with the usual ordering $x_1 < x_2 < \cdots$. However, it is good to have some flexibility in changing the ordering, which is why we make the following definition.

Definition 5.1.1. Given any totally ordered set I, create a totally ordered variable set $\{x_i\}_{i\in I}$, and then let $R(\{x_i\}_{i\in I})$ denote the power series of bounded degree in $\{x_i\}_{i\in I}$ having coefficients in $\mathbf{k}$.

The *ring of quasisymmetric functions* $\mathrm{QSym}(\{x_i\}_{i\in I})$ *over the alphabet* $\{x_i\}_{i\in I}$ will be the $\mathbf{k}$-submodule consisting of the elements f in $R(\{x_i\}_{i\in I})$ that have the same coefficient on the monomials $x_{i_1}^{\alpha_1}\cdots x_{i_\ell}^{\alpha_\ell}$ and $x_{j_1}^{\alpha_1}\cdots x_{j_\ell}^{\alpha_\ell}$ whenever both $i_1 < \cdots < i_\ell$ and $j_1 < \cdots < j_\ell$ in the total order on I. We write $\mathrm{QSym}_{\mathbf{k}}(\{x_i\}_{i\in I})$ instead of $\mathrm{QSym}(\{x_i\}_{i\in I})$ to stress the choice of base ring $\mathbf{k}$.

It immediately follows from this definition that $\mathrm{QSym}(\{x_i\}_{i\in I})$ is a free $\mathbf{k}$-submodule of $R(\{x_i\}_{i\in I})$, having as $\mathbf{k}$-basis elements the *monomial quasisymmetric functions*

$$M_\alpha(\{x_i\}_{i\in I}) := \sum_{i_1<\cdots<i_\ell \text{ in } I} x_{i_1}^{\alpha_1}\cdots x_{i_\ell}^{\alpha_\ell}$$

for all compositions[251] α satisfying $\ell(\alpha) \leq |I|$. When I is infinite, this means that the M_α for all compositions α form a basis of $\mathrm{QSym}(\{x_i\}_{i\in I})$.

Note that $\mathrm{QSym}(\{x_i\}_{i\in I}) = \bigoplus_{n\geq 0} \mathrm{QSym}_n(\{x_i\}_{i\in I})$ is a graded $\mathbf{k}$-module of finite type, where $\mathrm{QSym}_n(\{x_i\}_{i\in I})$ is the $\mathbf{k}$-submodule of quasisymmetric functions which are homogeneous of degree n. Letting Comp denote the set of all compositions α, and Comp_n the compositions α of n (that is, compositions whose parts sum to n), the subset $\{M_\alpha\}_{\alpha\in \mathrm{Comp}_n;\ \ell(\alpha)\leq |I|}$ gives a $\mathbf{k}$-basis for $\mathrm{QSym}_n(\{x_i\}_{i\in I})$.

Example 5.1.2. Taking the variable set $\mathbf{x} = (x_1 < x_2 < \cdots)$ to define $\mathrm{QSym}(\mathbf{x})$, for $n = 0, 1, 2, 3$, one has these basis elements in $\mathrm{QSym}_n(\mathbf{x})$:

$$\begin{aligned}
M_{()} = M_{\varnothing} &= 1,\\
M_{(1)} &= x_1 + x_2 + x_3 + \cdots && = m_{(1)} = s_{(1)} = e_1 = h_1 = p_1,\\
M_{(2)} &= x_1^2 + x_2^2 + x_3^2 + \cdots && = m_{(2)} = p_2,\\
M_{(1,1)} &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots && = m_{(1,1)} = e_2,\\
M_{(3)} &= x_1^3 + x_2^3 + x_3^3 + \cdots && = m_{(3)} = p_3,\\
M_{(2,1)} &= x_1^2x_2 + x_1^2x_3 + x_2^2x_3 + \cdots, &&\\
M_{(1,2)} &= x_1x_2^2 + x_1x_3^2 + x_2x_3^2 + \cdots, &&\\
M_{(1,1,1)} &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + \cdots && = m_{(1,1,1)} = e_3.
\end{aligned}$$

It is not obvious that $\mathrm{QSym}(\mathbf{x})$ is a subalgebra of $R(\mathbf{x})$, but we will show this momentarily. For example,

$$\begin{aligned}
M_{(a)}M_{(b,c)} &= (x_1^a + x_2^a + x_3^a + \cdots)(x_1^bx_2^c + x_1^bx_3^c + x_2^bx_3^c + \cdots)\\
&= x_1^{a+b}x_2^c + \cdots + x_1^bx_3^{a+c} + \cdots + x_1^ax_2^bx_3^c + \cdots + x_1^bx_2^ax_3^c + \cdots + x_1^bx_2^cx_3^a + \cdots\\
&= M_{(a+b,c)} + M_{(b,a+c)} + M_{(a,b,c)} + M_{(b,a,c)} + M_{(b,c,a)}.
\end{aligned}$$

Proposition 5.1.3. *For any infinite totally ordered set I, one has that $\mathrm{QSym}(\{x_i\}_{i\in I})$ is a $\mathbf{k}$-subalgebra of $R(\{x_i\}_{i\in I})$, with multiplication in the $\{M_\alpha\}$-basis as follows: Fix three disjoint chain posets $(i_1 < \cdots < i_\ell)$,*

[251] Recall that compositions were defined in Definition 4.3.1, along with related concepts such as length and size.

$(j_1 < \cdots < j_m)$ *and* $(k_1 < k_2 < \cdots)$. *Now, if* $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ *and* $\beta = (\beta_1, \ldots, \beta_m)$ *are two compositions, then*

$$M_\alpha M_\beta = \sum_f M_{\mathrm{wt}(f)} \tag{5.1.1}$$

in which the sum is over all $p \in \mathbb{N}$ *and all maps* f *from the disjoint union of two chains to a chain*

$$(i_1 < \cdots < i_\ell) \sqcup (j_1 < \cdots < j_m) \xrightarrow{f} (k_1 < \cdots < k_p) \tag{5.1.2}$$

which are both surjective and strictly order-preserving (that is, if x *and* y *are two elements in the domain satisfying* $x < y$, *then* $f(x) < f(y)$*), and where the composition* $\mathrm{wt}(f) := (\mathrm{wt}_1(f), \ldots, \mathrm{wt}_p(f))$ *is defined by* $\mathrm{wt}_s(f) := \sum_{i_u \in f^{-1}(k_s)} \alpha_u + \sum_{j_v \in f^{-1}(k_s)} \beta_v$.

Example 5.1.4. For this example, set $\alpha = (2,1)$ and $\beta = (3,4,2)$. Let us compute $M_\alpha M_\beta$ using (5.1.1). Indeed, the length of α is $\ell = 2$, and the length of β is $m = 3$, so the sum on the right hand side of (5.1.1) is a sum over all $p \in \mathbb{N}$ and all surjective strictly order-preserving maps f from the disjoint union $(i_1 < i_2) \sqcup (j_1 < j_2 < j_3)$ of two chains to the chain $(k_1 < k_2 < \cdots < k_p)$. Such maps can exist only when $p \leq 5$ (due to having to be surjective) and only for $p \geq 3$ (since, being strictly order-preserving, they have to be injective when restricted to $(j_1 < j_2 < j_3)$). Hence, enumerating them is a finite problem. The reader can check that the value obtained for $M_\alpha M_\beta$ is

$$\begin{aligned}
&M_{(2,1,3,4,2)} + M_{(2,3,1,4,2)} + M_{(2,3,4,1,2)} + M_{(2,3,4,2,1)} + M_{(3,2,1,4,2)} \\
&+ M_{(3,2,4,1,2)} + M_{(3,2,4,2,1)} + M_{(3,4,2,1,2)} + M_{(3,4,2,2,1)} + M_{(3,4,2,2,1)} \\
&+ M_{(2,3,4,3)} + M_{(2,3,5,2)} + M_{(2,4,4,2)} + M_{(3,2,4,3)} + M_{(3,2,5,2)} + M_{(3,4,2,3)} \\
&+ M_{(3,4,4,1)} + M_{(3,6,1,2)} + M_{(3,6,2,1)} + M_{(5,1,4,2)} + M_{(5,4,1,2)} + M_{(5,4,2,1)} \\
&+ M_{(5,4,3)} + M_{(5,5,2)} + M_{(3,6,3)}.
\end{aligned}$$

Here, we have listed the addends corresponding to $p = 5$ on the first two rows, the addends corresponding to $p = 4$ on the next two rows, and those corresponding to $p = 3$ on the fifth row. The reader might notice that the first two rows (i.e., the addends with $p = 5$) are basically a list of shuffles of α and β: In general, the maps (5.1.2) for $p = \ell + m$ are in bijection with the elements of $\mathrm{Sh}_{\ell,m}$ [252], and the corresponding compositions $\mathrm{wt}(f)$ are the shuffles of α and β. Therefore the name "overlapping shuffle product".

Proof of Proposition 5.1.3. It clearly suffices to prove the formula (5.1.1). Let $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_m)$ be two compositions. Fix three disjoint chain posets $(i_1 < \cdots < i_\ell)$, $(j_1 < \cdots < j_m)$ and $(k_1 < k_2 < \cdots)$.

Thus, multiplying $M_\alpha = \sum_{u_1 < \cdots < u_\ell} x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}$ with $M_\beta = \sum_{v_1 < \cdots < v_m} x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}$, we obtain

$$\begin{aligned}
M_\alpha M_\beta &= \sum_{u_1 < \cdots < u_\ell} \sum_{v_1 < \cdots < v_m} \left(x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}\right) \left(x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}\right) \\
&= \sum_{\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathrm{Comp}} \sum_{w_1 < \cdots < w_p \text{ in } I} N^\gamma_{w_1, \ldots, w_p} x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p},
\end{aligned} \tag{5.1.3}$$

where $N^\gamma_{w_1, \ldots, w_p}$ is the number of all pairs

$$((u_1 < \cdots < u_\ell), (v_1 < \cdots < v_m)) \in I^\ell \times I^m \tag{5.1.4}$$

of two strictly increasing tuples satisfying

$$\left(x_{u_1}^{\alpha_1} \cdots x_{u_\ell}^{\alpha_\ell}\right) \left(x_{v_1}^{\beta_1} \cdots x_{v_m}^{\beta_m}\right) = x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p}. \tag{5.1.5}$$

[253] Thus, we need to show that $N^\gamma_{w_1, \ldots, w_p}$ (for a given $\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathrm{Comp}$ and a given $(w_1 < \cdots < w_p) \in I^p$) is also the number of all surjective strictly order-preserving maps

$$(i_1 < \cdots < i_\ell) \sqcup (j_1 < \cdots < j_m) \xrightarrow{f} (k_1 < \cdots < k_p) \text{ satisfying } \mathrm{wt}(f) = \gamma \tag{5.1.6}$$

[252] The bijection takes a map f to the inverse of the permutation $\sigma \in \mathfrak{S}_p$ which sends every $x \in \{1, 2, \ldots, \ell\}$ to the index y satisfying $f(i_x) = k_y$, and sends every $x \in \{\ell + 1, \ell + 2, \ldots, \ell + m\}$ to the index y satisfying $f(j_{x-\ell}) = k_y$.

[253] In the second equality in (5.1.3), we have used the fact that each monomial can be uniquely written in the form $x_{w_1}^{\gamma_1} \cdots x_{w_p}^{\gamma_p}$ for some composition $\gamma = (\gamma_1, \ldots, \gamma_p) \in \mathrm{Comp}$ and some strictly increasing tuple $(w_1 < \cdots < w_p) \in I^p$.

(because then, (5.1.3) will simplify to (5.1.1)).

In order to show this, it suffices to construct a bijection from the set of all pairs (5.1.4) satisfying (5.1.5) to the set of all surjective strictly order-preserving maps (5.1.6). This bijection is easy to construct: Given a pair (5.1.4) satisfying (5.1.5), the bijection sends it to the map (5.1.6) determined by:

$$i_g \overset{f}{\mapsto} k_h, \text{ where } h \text{ is chosen such that } u_g = w_h;$$
$$j_g \overset{f}{\mapsto} k_h, \text{ where } h \text{ is chosen such that } v_g = w_h.$$

Proving that this bijection is well-defined and bijective is straightforward[254]. □

The multiplication rule (5.1.1) shows that the $\mathbf{k}$-algebra $\mathrm{QSym}(\{x_i\}_{i\in I})$ does not depend much on I, as long as I is infinite. More precisely, all such $\mathbf{k}$-algebras are mutually isomorphic. We can use this to define a $\mathbf{k}$-algebra of quasisymmetric functions without any reference to I:

Definition 5.1.5. Let QSym be the $\mathbf{k}$-algebra defined as having $\mathbf{k}$-basis $\{M_\alpha\}_{\alpha\in\mathrm{Comp}}$ and with multiplication defined $\mathbf{k}$-linearly by (5.1.1). This is called the $\mathbf{k}$-*algebra of quasisymmetric functions*. We write $\mathrm{QSym}_{\mathbf{k}}$ instead of QSym to stress the choice of base ring $\mathbf{k}$.

The $\mathbf{k}$-algebra QSym is graded, and its n-th graded component QSym_n has $\mathbf{k}$-basis $\{M_\alpha\}_{\alpha\in\mathrm{Comp}_n}$.

For every infinite totally ordered set I, the $\mathbf{k}$-algebra QSym is isomorphic to the $\mathbf{k}$-algebra $\mathrm{QSym}(\{x_i\}_{i\in I})$. The isomorphism sends $M_\alpha \longmapsto M_\alpha(\{x_i\}_{i\in I})$.

In particular, we obtain the isomorphism $\mathrm{QSym} \cong \mathrm{QSym}(\mathbf{x})$ for $\mathbf{x}$ being the infinite chain $(x_1 < x_2 < x_3 < \cdots)$. We will identify QSym with $\mathrm{QSym}(\mathbf{x})$ along this isomorphism. This allows us to regard quasisymmetric functions either as power series in a specific set of variables ("alphabet"), or as formal linear combinations of M_α's, whatever is more convenient.

For any infinite alphabet $\{x_i\}_{i\in I}$ and any $f \in \mathrm{QSym}$, we denote by $f\left(\{x_i\}_{i\in I}\right)$ the image of f under the algebra isomorphism $\mathrm{QSym} \to \mathrm{QSym}\left(\{x_i\}_{i\in I}\right)$ defined in Definition 5.1.5.

The comultiplication of QSym will extend the one that we defined for Λ, but we need to take care about the order of the variables this time. We consider the linear order from (2.3.2) on two sets of variables $(\mathbf{x},\mathbf{y}) = (x_1 < x_2 < \cdots < y_1 < y_2 < \cdots)$, and we embed the $\mathbf{k}$-algebra $\mathrm{QSym}(\mathbf{x}) \otimes \mathrm{QSym}(\mathbf{y})$ into the $\mathbf{k}$-algebra $R(\mathbf{x},\mathbf{y})$ by identifying every $f \otimes g \in \mathrm{QSym}(\mathbf{x}) \otimes \mathrm{QSym}(\mathbf{y})$ with $fg \in R(\mathbf{x},\mathbf{y})$ (this embedding is indeed injective[255]). It can then be seen that

$$\mathrm{QSym}(\mathbf{x},\mathbf{y}) \subset \mathrm{QSym}(\mathbf{x}) \otimes \mathrm{QSym}(\mathbf{y})$$

(where the right hand side is viewed as $\mathbf{k}$-subalgebra of $R(\mathbf{x},\mathbf{y})$ via said embedding)[256], so that one can define $\mathrm{QSym} \xrightarrow{\Delta} \mathrm{QSym} \otimes \mathrm{QSym}$ as the composite of the maps in the bottom row here:

(5.1.7)

$$\begin{array}{ccccccc} & & R(\mathbf{x},\mathbf{y}) & = & R(\mathbf{x},\mathbf{y}) & & \\ & & \cup & & \cup & & \\ \mathrm{QSym} & \cong & \mathrm{QSym}(\mathbf{x},\mathbf{y}) & \hookrightarrow & \mathrm{QSym}(\mathbf{x}) \otimes \mathrm{QSym}(\mathbf{y}) & \cong \mathrm{QSym} \otimes \mathrm{QSym}, & \\ f & \longmapsto & f(\mathbf{x},\mathbf{y}) = f(x_1,x_2,\ldots,y_1,y_2,\ldots). & & & & \end{array}$$

(Recall that $f(\mathbf{x},\mathbf{y})$ is formally defined as the image of f under the algebra isomorphism $\mathrm{QSym} \to \mathrm{QSym}(\mathbf{x},\mathbf{y})$ defined in Definition 5.1.5.)

[254] The inverse of this bijection sends each map (5.1.6) to the pair (5.1.4) determined by

$$u_g = w_h, \text{ where } h \text{ is chosen such that } f(i_g) = k_h;$$
$$v_g = w_h, \text{ where } h \text{ is chosen such that } f(j_g) = k_h.$$

[255] This is because it sends the basis elements $M_\beta(\mathbf{x}) \otimes M_\gamma(\mathbf{y})$ of the former $\mathbf{k}$-algebra to the linearly independent power series $M_\beta(\mathbf{x})M_\gamma(\mathbf{y})$.

[256] This is not completely obvious, but can be easily checked by verifying that $M_\alpha(\mathbf{x},\mathbf{y}) = \sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha}} M_\beta(\mathbf{x}) \otimes M_\gamma(\mathbf{y})$ for every composition α (see the proof of Proposition 5.1.7 for why this holds).

Example 5.1.6. For example,

$$\begin{aligned}
\Delta M_{(a,b,c)} &= M_{(a,b,c)}(x_1, x_2, \ldots, y_1, y_2, \ldots) \\
&= x_1^a x_2^b x_3^c + x_1^a x_2^b x_4^c + \cdots \\
&\quad + x_1^a x_2^b \cdot y_1^c + x_1^a x_2^b \cdot y_2^c + \cdots \\
&\quad + x_1^a \cdot y_1^b y_2^c + x_1^a \cdot y_1^b y_3^c + \cdots \\
&\quad + y_1^a y_2^b y_3^c + y_1^a y_2^b y_4^c + \cdots \\
&= M_{(a,b,c)}(\mathbf{x}) + M_{(a,b)}(\mathbf{x}) M_{(c)}(\mathbf{y}) + M_{(a)}(\mathbf{x}) M_{(b,c)}(\mathbf{y}) + M_{(a,b,c)}(\mathbf{y}) \\
&= M_{(a,b,c)} \otimes 1 + M_{(a,b)} \otimes M_{(c)} + M_{(a)} \otimes M_{(b,c)} + 1 \otimes M_{(a,b,c)}.
\end{aligned}$$

Defining the *concatenation* $\beta \cdot \gamma$ of two compositions $\beta = (\beta_1, \ldots, \beta_r), \gamma = (\gamma_1, \ldots, \gamma_s)$ to be the composition $(\beta_1, \ldots, \beta_r, \gamma_1, \ldots, \gamma_s)$, one has the following description of the coproduct in the $\{M_\alpha\}$ basis.

Proposition 5.1.7. *For a composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, one has*

$$\Delta M_\alpha = \sum_{k=0}^{\ell} M_{(\alpha_1, \ldots, \alpha_k)} \otimes M_{(\alpha_{k+1}, \ldots, \alpha_\ell)} = \sum_{\substack{(\beta,\gamma): \\ \beta \cdot \gamma = \alpha}} M_\beta \otimes M_\gamma.$$

Proof. We work with the infinite totally ordered set $I = \{1 < 2 < 3 < \cdots\}$. The definition of Δ yields

$$\Delta M_\alpha = M_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{p_1 < p_2 < \cdots < p_\ell \text{ in } (\mathbf{x},\mathbf{y})} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}, \tag{5.1.8}$$

where the sum runs over strictly increasing ℓ-tuples $(p_1 < p_2 < \cdots < p_\ell)$ of variables in the variable set $(\mathbf{x}, \mathbf{y})$. But every such ℓ-tuple $(p_1 < p_2 < \cdots < p_\ell)$ can be expressed uniquely in the form $\left(x_{i_1}, \ldots, x_{i_k}, y_{j_1}, \ldots, y_{j_{\ell-k}}\right)$ for some $k \in \{0, 1, \ldots, \ell\}$ and some subscripts $i_1 < \cdots < i_k$ and $j_1 < \cdots < j_{\ell-k}$ in I. The corresponding monomial $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$ then rewrites as $x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \cdot y_{j_1}^{\alpha_{k+1}} \cdots y_{j_{\ell-k}}^{\alpha_\ell}$. Thus, the sum on the right hand side of (5.1.8) rewrites as

$$\begin{aligned}
&\sum_{k=0}^{\ell} \sum_{i_1 < \cdots < i_k} \sum_{j_1 < \cdots < j_{\ell-k}} x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \cdot y_{j_1}^{\alpha_{k+1}} \cdots y_{j_{\ell-k}}^{\alpha_\ell} \\
&= \sum_{k=0}^{\ell} \underbrace{\left(\sum_{i_1 < \cdots < i_k} x_{i_1}^{\alpha_1} \cdots x_{i_k}^{\alpha_k} \right)}_{= M_{(\alpha_1, \ldots, \alpha_k)}(\mathbf{x})} \cdot \underbrace{\left(\sum_{j_1 < \cdots < j_{\ell-k}} y_{j_1}^{\alpha_{k+1}} \cdots y_{j_{\ell-k}}^{\alpha_\ell} \right)}_{= M_{(\alpha_{k+1}, \ldots, \alpha_\ell)}(\mathbf{y})} \\
&= \sum_{k=0}^{\ell} M_{(\alpha_1, \ldots, \alpha_k)}(\mathbf{x}) M_{(\alpha_{k+1}, \ldots, \alpha_\ell)}(\mathbf{y}).
\end{aligned}$$

Thus, (5.1.8) becomes

$$\begin{aligned}
\Delta M_\alpha = \sum_{p_1 < p_2 < \cdots < p_\ell \text{ in } (\mathbf{x},\mathbf{y})} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell} &= \sum_{k=0}^{\ell} M_{(\alpha_1, \ldots, \alpha_k)}(\mathbf{x}) M_{(\alpha_{k+1}, \ldots, \alpha_\ell)}(\mathbf{y}) \\
&= \sum_{k=0}^{\ell} M_{(\alpha_1, \ldots, \alpha_k)} \otimes M_{(\alpha_{k+1}, \ldots, \alpha_\ell)} = \sum_{\substack{(\beta,\gamma): \\ \beta \cdot \gamma = \alpha}} M_\beta \otimes M_\gamma.
\end{aligned}$$

□

Proposition 5.1.8. *The quasisymmetric functions* QSym *form a connected graded Hopf algebra of finite type, which is commutative, and contains the symmetric functions Λ as a Hopf subalgebra.*

Proof. To prove coassociativity of Δ, we need to be slightly careful. It seems reasonable to argue by $(\Delta \otimes \mathrm{id}) \circ \Delta f = f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (\mathrm{id} \otimes \Delta) \circ \Delta f$ as in the case of Λ, but this would now require further justification,

as terms like $f(\mathbf{x},\mathbf{y})$ and $f(\mathbf{x},\mathbf{y},\mathbf{z})$ are no longer directly defined as evaluations of f on some sequences (but rather are defined as images of f under certain homomorphisms). However, it is very easy to see that Δ is coassociative by checking $(\Delta\otimes \mathrm{id})\circ\Delta = (\mathrm{id}\otimes\Delta)\circ\Delta$ on the $\{M_\alpha\}$ basis: Proposition 5.1.7 yields

$$\begin{aligned}((\Delta\otimes \mathrm{id})\circ\Delta)\, M_\alpha &= \sum_{k=0}^{\ell} \Delta(M_{(\alpha_1,\ldots,\alpha_k)})\otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)}\\ &= \sum_{k=0}^{\ell}\left(\sum_{i=0}^{k} M_{(\alpha_1,\ldots,\alpha_i)}\otimes M_{(\alpha_{i+1},\ldots,\alpha_k)}\right)\otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)}\\ &= \sum_{k=0}^{\ell}\sum_{i=0}^{k} M_{(\alpha_1,\ldots,\alpha_i)}\otimes M_{(\alpha_{i+1},\ldots,\alpha_k)}\otimes M_{(\alpha_{k+1},\ldots,\alpha_\ell)}\end{aligned}$$

and the same expression for $((\mathrm{id}\otimes\Delta)\circ\Delta)\, M_\alpha$.

The coproduct Δ of QSym is an algebra morphism because it is defined as a composite of algebra morphisms in the bottom row of (5.1.7). To prove that the restriction of Δ to the subring Λ of QSym is the comultiplication of Λ, it thus is enough to check that it sends the elementary symmetric function e_n to $\sum_{i=0}^{n} e_i\otimes e_{n-i}$ for every $n\in\mathbb{N}$. This again follows from Proposition 5.1.7, since $e_n = M_{(1,1,\ldots,1)}$ (with n times 1).

The counit is as usual for a connected graded coalgebra, and just as in the case of Λ, sends a quasisymmetric function $f(\mathbf{x})$ to its constant term $f(0,0,\ldots)$. This is an evaluation, and hence an algebra morphism. Hence QSym forms a bialgebra, and as it is graded and connected, also a Hopf algebra by Proposition 1.4.16. It is clearly of finite type and contains Λ as a Hopf subalgebra. □

We will identify the antipode in QSym shortly, but we first deal with another slightly subtle issue. In addition to the counit evaluation $\epsilon(f) = f(0,0,\ldots)$, starting in Section 7.1, we will want to specialize elements in $\mathrm{QSym}(\mathbf{x})$ by making other variable substitutions, in which all but a finite list of variables are set to zero. We justify this here.

Proposition 5.1.9. *Fix a totally ordered set I, a commutative $\mathbf{k}$-algebra A, a finite list of variables $x_{i_1},\ldots,x_{i_m}$, say with $i_1<\cdots<i_m$ in I, and an ordered list of elements $(a_1,\ldots,a_m)\in A^m$.*

Then there is a well-defined evaluation homomorphism

$$\begin{array}{rcl}\mathrm{QSym}(\{x_i\}_{i\in I}) & \longrightarrow & A,\\ f & \longmapsto & [f]^{\,x_{i_1}=a_1,\ldots,x_{i_m}=a_m}_{x_j=0 \text{ for } j\notin\{i_1,\ldots,i_m\}}.\end{array}$$

Furthermore, this homomorphism depends only upon the list $(a_1,\ldots,a_m)$, as it coincides with the following:

$$\begin{array}{rcl}\mathrm{QSym}(\{x_i\}_{i\in I}) \cong \mathrm{QSym}(x_1,x_2,\ldots) & \longrightarrow & A,\\ f(x_1,x_2,\ldots) & \longmapsto & f(a_1,\ldots,a_m,0,0\ldots).\end{array}$$

(This latter statement is stated for the case when I is infinite; otherwise, read "$x_1,x_2,\ldots,x_{|I|}$" for "$x_1,x_2,\ldots$", and interpret $(a_1,\ldots,a_m,0,0\ldots)$ as an $|I|$-tuple.)

Proof. One already can make sense of evaluating $x_{i_1}=a_1,\ldots,x_{i_m}=a_m$ and $x_j=0$ for $j\notin\{i_1,\ldots,i_m\}$ in the ambient ring $R(\{x_i\}_{i\in I})$ containing $\mathrm{QSym}(\{x_i\}_{i\in I})$, since a power series f of bounded degree will have finitely many monomials that only involve the variables $x_{i_1},\ldots,x_{i_m}$. The last assertion follows from quasisymmetry of f, and is perhaps checked most easily when $f = M_\alpha(\{x_i\}_{i\in I})$ for some α. □

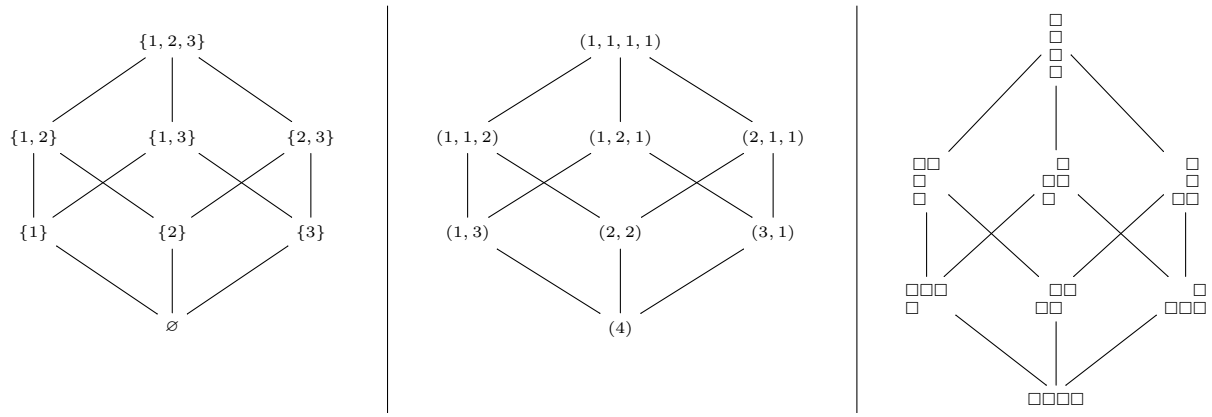
The antipode in QSym has a reasonably simple expression in the $\{M_\alpha\}$ basis, but requiring a definition.

Definition 5.1.10. For α,β in Comp_n, say that α *refines* β or β *coarsens* α if, informally, one can obtain β from α by combining some of its adjacent parts. Alternatively, this can be defined as follows: One has a bijection $\mathrm{Comp}_n\to 2^{[n-1]}$ where $[n-1]:=\{1,2,\ldots,n-1\}$ which sends $\alpha=(\alpha_1,\ldots,\alpha_\ell)$ having length $\ell(\alpha)=\ell$ to its subset of partial sums

$$D(\alpha) := \{\alpha_1,\alpha_1+\alpha_2,\ldots,\alpha_1+\cdots+\alpha_{\ell-1}\},$$

and this sends the refinement ordering to the inclusion ordering on the Boolean algebra $2^{[n-1]}$ (to be more precise: a composition $\alpha\in\mathrm{Comp}_n$ refines a composition $\beta\in\mathrm{Comp}_n$ if and only if $D(\alpha)\supset D(\beta)$).

There is also a bijection sending every composition α to its *ribbon* diagram $\mathrm{Rib}(\alpha)$: the skew diagram λ/μ having rows of sizes $\alpha_1, \ldots, \alpha_\ell$ read from bottom to top with exactly one column of overlap between adjacent rows. These bijections and the refinement partial order are illustrated here for $n = 4$:



(where we have drawn each ribbon diagram with its boxes spaced out).

Given $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, its *reverse* composition is $\mathrm{rev}(\alpha) = (\alpha_\ell, \alpha_{\ell-1}, \ldots, \alpha_2, \alpha_1)$. Note that $\alpha \mapsto \mathrm{rev}(\alpha)$ is a poset automorphism of Comp_n for the refinement ordering.

Theorem 5.1.11. *For any composition α in* Comp,

$$S(M_\alpha) = (-1)^{\ell(\alpha)} \sum_{\substack{\gamma \in \mathrm{Comp}: \\ \gamma \text{ coarsens } \mathrm{rev}(\alpha)}} M_\gamma.$$

For example,

$$S(M_{(a,b,c)}) = -\left(M_{(c,b,a)} + M_{(b+c,a)} + M_{(c,a+b)} + M_{(a+b+c)}\right).$$

Proof. We give Ehrenborg's proof[257] [64, Prop. 3.4] via induction on $\ell = \ell(\alpha)$. One has easy base cases when $\ell(\alpha) = 0$, where $S(M_\varnothing) = S(1) = 1 = (-1)^0 M_{\mathrm{rev}(\varnothing)}$, and when $\ell(\alpha) = 1$, where $M_{(n)}$ is primitive by Proposition 5.1.7, so Proposition 1.4.17 shows $S(M_{(n)}) = -M_{(n)} = (-1)^1 M_{\mathrm{rev}((n))}$.

For the inductive step, apply the inductive definition of S from the proof of Proposition 1.4.16:

$$\begin{aligned} S(M_{(\alpha_1,\ldots,\alpha_\ell)}) &= -\sum_{i=0}^{\ell-1} S(M_{(\alpha_1,\ldots,\alpha_i)}) M_{(\alpha_{i+1},\ldots,\alpha_\ell)} \\ &= \sum_{i=0}^{\ell-1} \sum_{\substack{\beta \text{ coarsening} \\ (\alpha_i,\alpha_{i-1},\ldots,\alpha_1)}} (-1)^{i+1} M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}. \end{aligned}$$

The idea will be to cancel terms of opposite sign that appear in the expansions of the products $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$. Note that each composition β appearing above has first part β_1 of the form $\alpha_i + \alpha_{i-1} + \cdots + \alpha_h$ for some $h \le i$ (unless $\beta = \varnothing$), and hence each term M_γ in the expansion of the product $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$ has γ_1 (that is, the first entry of γ) a sum that can take one of these three forms:

- $\alpha_i + \alpha_{i-1} + \cdots + \alpha_h$,
- $\alpha_{i+1} + (\alpha_i + \alpha_{i-1} + \cdots + \alpha_h)$,
- α_{i+1}.

Say that the *type* of γ is i in the first case, and $i+1$ in the second two cases[258]; in other words, the type is the largest subscript k on a part α_k which was combined in the sum γ_1. It is not hard to see that a given γ for which the type k is strictly smaller than ℓ arises from exactly two pairs $(\beta, \gamma), (\beta', \gamma)$, having opposite

[257] A different proof was given by Malvenuto and Reutenauer [146, Cor. 2.3], and is sketched in Remark 5.4.4 below.

[258] We imagine that we label the terms obtained by expanding $M_\beta M_{(\alpha_{i+1},\ldots,\alpha_\ell)}$ by distinct labels, so that each term knows how exactly it was created (i.e., which i, which β and which map f as in (5.1.2) gave rise to it). Strictly speaking, it is these triples (i, β, f) that we should be assigning types to, not terms.

signs $(-1)^k$ and $(-1)^{k+1}$ in the above sum[259]. For example, if $\alpha = (\alpha_1, \ldots, \alpha_8)$, then the composition $\gamma = (\alpha_6 + \alpha_5 + \alpha_4, \alpha_3, \alpha_7, \alpha_8 + \alpha_2 + \alpha_1)$ of type 6 can arise from either of

$$\beta = (\alpha_6 + \alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 6 \text{ and sign } (-1)^7,$$
$$\beta' = (\alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 5 \text{ and sign } (-1)^6.$$

Similarly, $\gamma = (\alpha_6, \alpha_5 + \alpha_4, \alpha_3, \alpha_7, \alpha_8 + \alpha_2 + \alpha_1)$ can arise from either of

$$\beta = (\alpha_6, \alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 6 \text{ and sign } (-1)^7,$$
$$\beta' = (\alpha_5 + \alpha_4, \alpha_3, \alpha_2 + \alpha_1) \text{ with } i = 5 \text{ and sign } (-1)^6.$$

Thus one can cancel almost all the terms, excepting those with γ of type ℓ among the terms M_γ in the expansion of the last $(i = \ell - 1)$ summand $M_\beta M_{(\alpha_\ell)}$. A bit of thought shows that these are the γ coarsening $\mathrm{rev}(\alpha)$, and all have sign $(-1)^\ell$. □

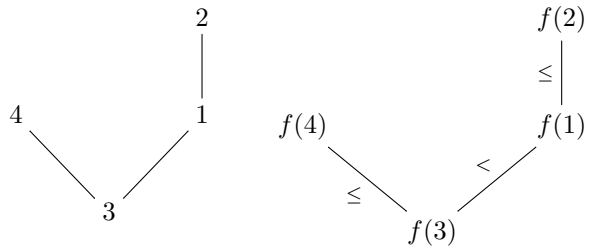
5.2. **The fundamental basis and P-partitions.** There is a second important basis for QSym which arose originally in Stanley's P-partition theory [203].[260]

Definition 5.2.1. A *labelled poset* will here mean a partially ordered set P whose underlying set is some finite subset of the integers. A *P-partition* is a function $P \xrightarrow{f} \{1, 2, \ldots\}$ with the following two properties:

- If $i \in P$ and $j \in P$ satisfy $i <_P j$ and $i <_{\mathbb{Z}} j$, then $f(i) \leq f(j)$.
- If $i \in P$ and $j \in P$ satisfy $i <_P j$ and $i >_{\mathbb{Z}} j$, then $f(i) < f(j)$.

Denote by $\mathcal{A}(P)$ the set of all P-partitions f, and let $F_P(\mathbf{x}) := \sum_{f \in \mathcal{A}(P)} \mathbf{x}_f$ where $\mathbf{x}_f := \prod_{i \in P} x_{f(i)}$. This $F_P(\mathbf{x})$ is an element of $\mathbf{k}[[\mathbf{x}]] := \mathbf{k}[[x_1, x_2, \ldots]]$.

Example 5.2.2. Depicted is a labelled poset P, along with the relations among the four values $f = (f(1), f(2), f(3), f(4))$ that define its P-partitions f:



Remark 5.2.3. Stanley's treatment of P-partitions in [206, §3.15 and §7.19] uses a language different from ours. First, Stanley works not with labelled posets P, but with pairs (P, ω) of a poset P and a bijective labelling $\omega : P \to [n]$. Thus, the relation $<_{\mathbb{Z}}$ is not given on P a priori, but has to be pulled back from $[n]$ using ω (and it depends on ω, whence Stanley speaks of "(P, ω)-partitions"). Furthermore, what we call "P-partition" is called a "reverse P-partition" in [206]. Finally, Stanley uses the notations F_P and $F_{P,\omega}$ for something different from what we denote by F_P, whereas what we call F_P is dubbed $K_{P,\omega}$ in [206, §7.19].

The so-called *fundamental quasisymmetric functions* are an important special case of the $F_P(\mathbf{x})$. We shall first define them directly and then see how they are obtained as P-partition enumerators $F_P(\mathbf{x})$ for some special labelled posets P.

Definition 5.2.4. Let $n \in \mathbb{N}$ and $\alpha \in \mathrm{Comp}_n$. We define the *fundamental quasisymmetric function* $L_\alpha = L_\alpha(\mathbf{x}) \in \mathrm{QSym}$ by

$$L_\alpha := \sum_{\substack{\beta \in \mathrm{Comp}_n: \\ \beta \text{ refines } \alpha}} M_\beta. \tag{5.2.1}$$

[259] Strictly speaking, this means that we have an involution on the set of our (i, β, f) triples having type smaller than ℓ, and this involution switches the sign of $(-1)^i M_{\mathrm{wt}(f)}$.

[260] See [80] for a history of P-partitions; our notations, however, strongly differ from those in [80].

Example 5.2.5. The extreme cases for α in Comp_n give quasisymmetric functions L_α which are symmetric:

$$L_{(1^n)} = M_{(1^n)} = e_n,$$
$$L_{(n)} = \sum_{\alpha \in \mathrm{Comp}_n} M_\alpha = h_n.$$

Before studying the L_α in earnest, we recall a basic fact about finite sets, which is sometimes known as the "principle of inclusion and exclusion" (although it is more general than the formula for the size of a union of sets that commonly goes by this name):

Lemma 5.2.6. *Let G be a finite set. Let V be a $\mathbf{k}$-module. For each subset A of G, we let f_A and g_A be two elements of V.*

(a) *If*

$$\text{every } A \subset G \text{ satisfies } g_A = \sum_{B \subset A} f_B,$$

then

$$\text{every } A \subset G \text{ satisfies } f_A = \sum_{B \subset A} (-1)^{|A \setminus B|} g_B.$$

(b) *If*

$$\text{every } A \subset G \text{ satisfies } g_A = \sum_{B \subset G;\ B \supset A} f_B,$$

then

$$\text{every } A \subset G \text{ satisfies } f_A = \sum_{B \subset G;\ B \supset A} (-1)^{|B \setminus A|} g_B.$$

Proof. This can be proven by elementary arguments (easy exercise). Alternatively, Lemma 5.2.6 can be viewed as a particular case of the Möbius inversion principle (see, e.g., [206, Propositions 3.7.1 and 3.7.2]) applied to the Boolean lattice 2^G (whose Möbius function is very simple: see [206, Example 3.8.3]). (This is spelled out in [138, Example 4.52], for example.) □

Lemma 5.2.6 can be translated into the language of compositions:

Lemma 5.2.7. *Let $n \in \mathbb{N}$. Let V be a $\mathbf{k}$-module. For each $\alpha \in \mathrm{Comp}_n$, we let f_α and g_α be two elements of V.*

(a) *If*

$$\text{every } \alpha \in \mathrm{Comp}_n \text{ satisfies } g_\alpha = \sum_{\beta \text{ coarsens } \alpha} f_\beta,$$

then

$$\text{every } \alpha \in \mathrm{Comp}_n \text{ satisfies } f_\alpha = \sum_{\beta \text{ coarsens } \alpha} (-1)^{\ell(\alpha)-\ell(\beta)} g_\beta.$$

(b) *If*

$$\text{every } \alpha \in \mathrm{Comp}_n \text{ satisfies } g_\alpha = \sum_{\beta \text{ refines } \alpha} f_\beta,$$

then

$$\text{every } \alpha \in \mathrm{Comp}_n \text{ satisfies } f_\alpha = \sum_{\beta \text{ refines } \alpha} (-1)^{\ell(\beta)-\ell(\alpha)} g_\beta.$$

Proof. Set $[n-1] = \{1, 2, \ldots, n-1\}$. Recall (from Definition 5.1.10) that there is a bijection $D : \mathrm{Comp}_n \to 2^{[n-1]}$ that sends each $\alpha \in \mathrm{Comp}_n$ to $D(\alpha) \subset [n-1]$. This bijection D has the properties that:

- a composition β refines a composition α if and only if $D(\beta) \supset D(\alpha)$;
- a composition β coarsens a composition α if and only if $D(\beta) \subset D(\alpha)$;
- any composition $\alpha \in \mathrm{Comp}_n$ satisfies $|D(\alpha)| = \ell(\alpha) - 1$ (unless $n = 0$), and thus
- any compositions α and β in Comp_n satisfy $|D(\alpha)| - |D(\beta)| = \ell(\alpha) - \ell(\beta)$.

This creates a dictionary between compositions in Comp_n and subsets of $[n-1]$. Now, apply Lemma 5.2.6 to $G = [n-1]$, $f_A = f_{D^{-1}(A)}$ and $g_A = g_{D^{-1}(A)}$, and translate using the dictionary. □

Now, we can see the following about the fundamental quasisymmetric functions:

Proposition 5.2.8. *The family $\{L_\alpha\}_{\alpha\in\mathrm{Comp}}$ is a* **k***-basis for* QSym*, and each $n \in \mathbb{N}$ and $\alpha \in \mathrm{Comp}_n$ satisfy*

$$M_\alpha = \sum_{\substack{\beta\in\mathrm{Comp}_n:\\ \beta \text{ refines } \alpha}} (-1)^{\ell(\beta)-\ell(\alpha)} L_\beta. \tag{5.2.2}$$

Proof. Fix $n \in \mathbb{N}$. Recall the equality (5.2.1). Thus, Lemma 5.2.7(b) (applied to $V = \mathrm{QSym}$, $f_\alpha = M_\alpha$ and $g_\alpha = L_\alpha$) yields (5.2.2).

Recall that the family $(M_\alpha)_{\alpha\in\mathrm{Comp}_n}$ is a basis of the **k**-module QSym_n. The equality (5.2.1) shows that the family $(L_\alpha)_{\alpha\in\mathrm{Comp}_n}$ expands invertibly triangularly[261] with respect to the family $(M_\alpha)_{\alpha\in\mathrm{Comp}_n}$ (where Comp_n is equipped with the refinement order).[262] Thus, Corollary 11.1.19(e) (applied to QSym_n, Comp_n, $(M_\alpha)_{\alpha\in\mathrm{Comp}_n}$ and $(L_\alpha)_{\alpha\in\mathrm{Comp}_n}$ instead of M, S, $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$) shows that the family $(L_\alpha)_{\alpha\in\mathrm{Comp}_n}$ is a basis of the **k**-module QSym_n. Combining this fact for all $n \in \mathbb{N}$, we conclude that the family $(L_\alpha)_{\alpha\in\mathrm{Comp}}$ is a basis of the **k**-module QSym. This completes the proof of Proposition 5.2.8. □

Proposition 5.2.9. *Let $n \in \mathbb{N}$. Let α be a composition of n. Let I be an infinite totally ordered set. Then,*

$$L_\alpha\left(\{x_i\}_{i\in I}\right) = \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n},$$

where $L_\alpha\left(\{x_i\}_{i\in I}\right)$ is defined as the image of L_α under the isomorphism $\mathrm{QSym} \to \mathrm{QSym}\left(\{x_i\}_{i\in I}\right)$ obtained in Definition 5.1.5. In particular, for the standard (totally ordered) variable set $\mathbf{x} = (x_1 < x_2 < \cdots)$, we obtain

$$L_\alpha = L_\alpha(\mathbf{x}) = \sum_{\substack{(1\le)i_1\le i_2\le\cdots\le i_n;\\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n}. \tag{5.2.3}$$

Proof. Every composition $\beta = (\beta_1, \ldots, \beta_\ell)$ of n satisfies

$$M_\beta\left(\{x_i\}_{i\in I}\right) = \sum_{k_1<\cdots<k_\ell \text{ in } I} x_{k_1}^{\beta_1}\cdots x_{k_\ell}^{\beta_\ell} = \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n}. \tag{5.2.4}$$

Applying the ring homomorphism $\mathrm{QSym} \to \mathrm{QSym}\left(\{x_i\}_{i\in I}\right)$ to (5.2.1), we obtain

$$\begin{aligned}
L_\alpha\left(\{x_i\}_{i\in I}\right) &= \sum_{\substack{\beta\in\mathrm{Comp}_n:\\ \beta \text{ refines } \alpha}} M_\beta\left(\{x_i\}_{i\in I}\right) \overset{(5.2.4)}{=} \sum_{\substack{\beta\in\mathrm{Comp}_n:\\ \beta \text{ refines } \alpha}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n} \\
&= \sum_{\substack{\beta\in\mathrm{Comp}_n:\\ D(\alpha)\subset D(\beta)}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in D(\beta)}} x_{i_1}x_{i_2}\cdots x_{i_n} \\
&= \sum_{\substack{Z\subset[n-1]:\\ D(\alpha)\subset Z}} \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if and only if } j\in Z}} x_{i_1}x_{i_2}\cdots x_{i_n} = \sum_{\substack{i_1\le i_2\le\cdots\le i_n \text{ in } I;\\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n}.
\end{aligned}$$

□

Proposition 5.2.10. *Assume that the labelled poset P is a total or linear order $w = (w_1 < \cdots < w_n)$ (that is, $P = \{w_1, w_2, \ldots, w_n\}$ as sets, and the order $<_P$ is given by $w_1 <_P w_2 <_P \cdots <_P w_n$). Let* $\mathrm{Des}(w)$ *be the* descent set *of w, defined by*

$$\mathrm{Des}(w) := \{i : w_i >_{\mathbb{Z}} w_{i+1}\} \subset \{1, 2, \ldots, n-1\}.$$

[261] See Section 11.1 for a definition of this concept.

[262] In fact, it expands unitriangularly with respect to the latter family.

Let $\alpha \in \mathrm{Comp}_n$ be the unique composition in Comp_n having partial sums $D(\alpha) = \mathrm{Des}(w)$. Then, the generating function $F_w(\mathbf{x})$ equals the fundamental quasisymmetric function L_α. In particular, $F_w(\mathbf{x})$ depends only upon the descent set $\mathrm{Des}(w)$.

E.g., total order $w = 35142$ has $\mathrm{Des}(w) = \{2, 4\}$ and composition $\alpha = (2, 2, 1)$, so

$$\begin{aligned} F_{35142}(\mathbf{x}) &= \sum_{f(3)\le f(5)<f(1)\le f(4)<f(2)} x_{f(3)}x_{f(5)}x_{f(1)}x_{f(4)}x_{f(2)} \\ &= \sum_{i_1\le i_2<i_3\le i_4<i_5} x_{i_1}x_{i_2}x_{i_3}x_{i_4}x_{i_5} \\ &= L_{(2,2,1)} = M_{(2,2,1)} + M_{(2,1,1,1)} + M_{(1,1,2,1)} + M_{(1,1,1,1,1)}. \end{aligned}$$

Proof of Proposition 5.2.10. Write $F_w(\mathbf{x})$ as a sum of monomials $x_{f(w_1)}\cdots x_{f(w_n)}$ over all w-partitions f. These w-partitions are exactly the maps $f : w \to \{1, 2, 3, \ldots\}$ satisfying $f(w_1) \le \cdots \le f(w_n)$ and having strict inequalities $f(w_i) < f(w_{i+1})$ whenever i is in $\mathrm{Des}(w)$ (because if two elements w_a and w_b of w satisfy $w_a <_w w_b$ and $w_a >_{\mathbb{Z}} w_b$, then they must satisfy $a < b$ and $i \in \mathrm{Des}(w)$ for some $i \in \{a, a+1, \ldots, b-1\}$; thus, the conditions "$f(w_1) \le \cdots \le f(w_n)$" and "$f(w_i) < f(w_{i+1})$ whenever i is in $\mathrm{Des}(w)$" ensure that $f(w_a) < f(w_b)$ in this case). Therefore, they are in bijection with the weakly increasing sequences $(i_1 \le i_2 \le \cdots \le i_n)$ of positive integers having strict inequalities $i_j < i_{j+1}$ whenever $i \in \mathrm{Des}(w)$ (namely, the bijection sends any w-partition f to the sequence $(f(w_1) \le f(w_2) \le \cdots \le f(w_n))$). Hence,

$$F_w(\mathbf{x}) = \sum_{f\in\mathcal{A}(w)} \mathbf{x}_f = \sum_{\substack{(1\le)i_1\le i_2\le\cdots\le i_n; \\ i_j<i_{j+1} \text{ if } j\in\mathrm{Des}(w)}} x_{i_1}x_{i_2}\cdots x_{i_n} = \sum_{\substack{(1\le)i_1\le i_2\le\cdots\le i_n; \\ i_j<i_{j+1} \text{ if } j\in D(\alpha)}} x_{i_1}x_{i_2}\cdots x_{i_n}$$

(since $\mathrm{Des}(w) = D(\alpha)$). Comparing this with (5.2.3), we conclude that $F_w(\mathbf{x}) = L_\alpha$. □

The next proposition ([206, Cor. 7.19.5], [140, Cor. 3.3.24]) is an algebraic shadow of Stanley's main lemma [206, Thm. 7.19.4] in P-partition theory. It expands any $F_P(\mathbf{x})$ in the $\{L_\alpha\}$ basis, as a sum over the set $\mathcal{L}(P)$ of all *linear extensions* w of P [263]. E.g., the poset P from Example 5.2.2 has $\mathcal{L}(P) = \{3124, 3142, 3412\}$.

Theorem 5.2.11. *For any labelled poset P,*

$$F_P(\mathbf{x}) = \sum_{w\in\mathcal{L}(P)} F_w(\mathbf{x}).$$

Proof. We give Gessel's proof [79, Thm. 1], via induction on the number of pairs i, j which are incomparable in P. When this quantity is 0, then P is itself a linear order w, so that $\mathcal{L}(P) = \{w\}$ and there is nothing to prove.

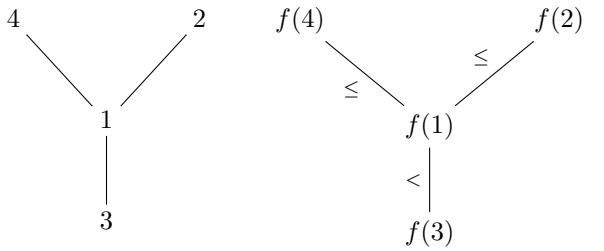
In the inductive step, let i, j be incomparable elements. Consider the two posets $P_{i<j}$ and $P_{j<i}$ which are obtained from P by adding in an order relation between i and j, and then taking the transitive closure; it is not hard to see that these transitive closures cannot contain a cycle, so that these really do define two posets. The result then follows by induction applied to $P_{i<j}, P_{j<i}$, once one notices that $\mathcal{L}(P) = \mathcal{L}(P_{i<j}) \sqcup \mathcal{L}(P_{j<i})$ since every linear extension w of P either has i before j or vice-versa, and $\mathcal{A}(P) = \mathcal{A}(P_{i<j}) \sqcup \mathcal{A}(P_{j<i})$ since, assuming that $i <_{\mathbb{Z}} j$ without loss of generality, every f in $\mathcal{A}(P)$ either satisfies $f(i) \le f(j)$ or $f(i) > f(j)$. □

[263] Let us explain what we mean by linear extensions and how we represent them.

If $\mathbf{P}$ is a finite poset, then a *linear extension* of $\mathbf{P}$ denotes a total order w on the set $\mathbf{P}$ having the property that every two elements i and j of $\mathbf{P}$ satisfying $i <_{\mathbf{P}} j$ satisfy $i <_w j$. (In other words, it is a linear order on the ground set $\mathbf{P}$ which extends $\mathbf{P}$ as a poset; therefore the name.) We identify such a total order w with the list $(\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_n)$ containing all elements of $\mathbf{P}$ in w-increasing order (that is, $\mathbf{p}_1 <_w \mathbf{p}_2 <_w \cdots <_w \mathbf{p}_n$).

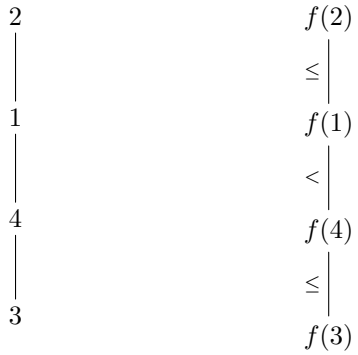
(Stanley, in [206, §3.5], defines linear extensions in a slightly different way: For him, a linear extension of a finite poset $\mathbf{P}$ is an order-preserving bijection from $\mathbf{P}$ to the subposet $\{1, 2, \ldots, |\mathbf{P}|\}$ of $\mathbb{Z}$. But this is equivalent to our definition, since a bijection like this can be used to transport the order relation of $\{1, 2, \ldots, |\mathbf{P}|\}$ back to $\mathbf{P}$, thus resulting in a total order on $\mathbf{P}$ which is a linear extension of $\mathbf{P}$ in our sense.)

Example 5.2.12. To illustrate the induction in the above proof, consider the poset P from Example 5.2.2, having $\mathcal{L}(P) = \{3124, 3142, 3412\}$. Then choosing as incomparable pair $(i, j) = (1, 4)$, one has

$P_{i<j} =$ 

, thus $\mathcal{L}(P_{i<j}) = \{3124, 3142\}$

and

$P_{j<i} =$ 

, thus $\mathcal{L}(P_{j<i}) = \{3412\}$.

Exercise 5.2.13. Give an alternative proof for Theorem 5.2.11.

[**Hint:** For every $f : P \to \{1, 2, 3, \ldots\}$, we can define a binary relation $\prec_f$ on the set P by letting $i \prec_f j$ hold if and only if

$$(f(i) < f(j) \text{ or } (f(i) = f(j) \text{ and } i <_{\mathbb{Z}} j)).$$

Show that this binary relation $\prec_f$ is (the smaller relation of) a total order. When f is a P-partition, then endowing the set P with this total order yields a linear extension of P. Use this to show that the set $\mathcal{A}(P)$ is the union of its disjoint subsets $\mathcal{A}(w)$ with $w \in \mathcal{L}(P)$.]

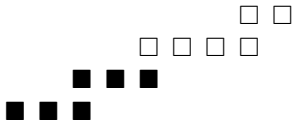
Various other properties of the quasisymmetric functions $F_P(\mathbf{x})$ are studied, e.g., in [152].

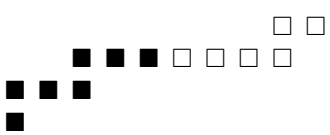
We next wish to describe the structure maps for the Hopf algebra QSym in the basis $\{L_\alpha\}$ of fundamental quasisymmetric functions. For this purpose, two more definitions are useful.

Definition 5.2.14. Given two nonempty compositions $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ and $\beta = (\beta_1, \ldots, \beta_m)$, their *near-concatenation* is

$$\alpha \odot \beta := (\alpha_1, \ldots, \alpha_{\ell-1}, \alpha_\ell + \beta_1, \beta_2, \ldots, \beta_m).$$

For example, the figure below depicts for $\alpha = (1, 3, 3)$ (black squares) and $\beta = (4, 2)$ (white squares) the concatenation and near-concatenation as ribbons:[264]

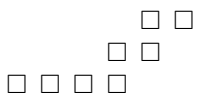
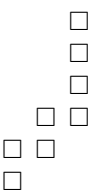
$\mathrm{Rib}(\alpha \cdot \beta) =$ 

$\mathrm{Rib}(\alpha \odot \beta) =$ 

Lastly, given α in Comp_n, let $\omega(\alpha)$ be the unique composition in Comp_n whose partial sums $D(\omega(\alpha))$ form the complementary set within $[n-1]$ to the partial sums $D(\mathrm{rev}(\alpha))$; alternatively, one can check this means that the ribbon for $\omega(\alpha)$ is obtained from that of α by conjugation or transposing, that is, if $\mathrm{Rib}(\alpha) = \lambda/\mu$

[264]The ribbons are drawn with their boxes spaced out in order to facilitate counting.

then $\mathrm{Rib}\,(\omega(\alpha)) = \lambda^t/\mu^t$. E.g. if $\alpha = (4,2,2)$ so that $n = 8$, then $\mathrm{rev}(\alpha) = (2,2,4)$ has $D(\mathrm{rev}(\alpha)) = \{2,4\} \subset [7]$, complementary to the set $\{1,3,5,6,7\}$ which are the partial sums for $\omega(\alpha) = (1,2,2,1,1,1)$, and the ribbon diagrams of α and $\omega(\alpha)$ are

$\mathrm{Rib}\,(\alpha) =$  and $\mathrm{Rib}\,(\omega(\alpha)) =$ 

Proposition 5.2.15. *The structure maps for the Hopf algebra* QSym *in the basis* $\{L_\alpha\}$ *of fundamental quasisymmetric functions are as follows:*

$$\Delta L_\alpha = \sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha \text{ or } \beta\odot\gamma=\alpha}} L_\beta \otimes L_\gamma, \tag{5.2.5}$$

$$L_\alpha L_\beta = \sum_{w \in w_\alpha \sqcup\!\sqcup\, w_\beta} L_{\gamma(w)}, \tag{5.2.6}$$

$$S(L_\alpha) = (-1)^{|\alpha|} L_{\omega(\alpha)}. \tag{5.2.7}$$

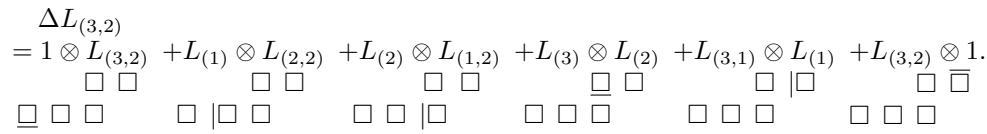
Here we are making use of the following notations in (5.2.6) *(recall also Definition 1.6.2):*

- *A* labelled linear order *will mean a labelled poset* P *whose order* $<_P$ *is a total order. We will identify any labelled linear order* P *with the word (over the alphabet* $\mathbb{Z}$*) obtained by writing down the elements of* P *in increasing order (with respect to the total order* $<_P$*). This way, every word (over the alphabet* $\mathbb{Z}$*) which has no two equal letters becomes identified with a labelled linear order.*
- w_α *is any labelled linear order with underlying set* $\{1,2,\ldots,|\alpha|\}$ *such that* $\mathrm{Des}\,(w_\alpha) = D\,(\alpha)$.
- w_β *is any labelled linear order with underlying set* $\{|\alpha|+1, |\alpha|+2, \ldots, |\alpha|+|\beta|\}$ *such that* $\mathrm{Des}\,(w_\beta) = D\,(\beta)$.
- $\gamma(w)$ *is the unique composition of* $|\alpha|+|\beta|$ *with* $D(\gamma(w)) = \mathrm{Des}(w)$.

(The right hand side of (5.2.6) *is to be read as a sum over all* w*, for a fixed choice of* w_α *and* w_β*.)*

At first glance the formula (5.2.5) for ΔL_α might seem more complicated than the formula of Proposition 5.1.7 for ΔM_α. However, it is equally simple when viewed in terms of ribbon diagrams: it cuts the ribbon diagram $\mathrm{Rib}\,(\alpha)$ into two smaller ribbons $\mathrm{Rib}\,(\beta)$ and $\mathrm{Rib}\,(\gamma)$, in all $|\alpha|+1$ possible ways, via *horizontal* cuts ($\beta\cdot\gamma = \alpha$) or *vertical* cuts ($\beta \odot \gamma = \alpha$). For example,

$$\begin{aligned}\Delta L_{(3,2)} &= 1 \otimes L_{(3,2)} + L_{(1)} \otimes L_{(2,2)} + L_{(2)} \otimes L_{(1,2)} + L_{(3)} \otimes L_{(2)} + L_{(3,1)} \otimes L_{(1)} + L_{(3,2)} \otimes 1.\end{aligned}$$



Example 5.2.16. To multiply $L_{(1,1)}L_{(2)}$, one could pick $w_\alpha = 21$ and $w_\beta = 34$, and then

$$\begin{aligned} L_{(1,1)}L_{(2)} = \sum_{w \in 21 \sqcup\!\sqcup\, 34} L_{\gamma(w)} &= L_{\gamma(2134)} + L_{\gamma(2314)} + L_{\gamma(3214)} + L_{\gamma(2341)} + L_{\gamma(3241)} + L_{\gamma(3421)} \\ &= L_{(1,3)} + L_{(2,2)} + L_{(1,1,2)} + L_{(3,1)} + L_{(1,2,1)} + L_{(2,1,1)}. \end{aligned}$$

Before we prove Proposition 5.2.15, we state a simple lemma:

Lemma 5.2.17. *Let* Q *and* R *be two labelled posets whose underlying sets are disjoint. Let* $Q \sqcup R$ *be the disjoint union of these posets* Q *and* R*; this is again a labelled poset. Then,*

$$F_Q\,(\mathbf{x})\, F_R\,(\mathbf{x}) = F_{Q\sqcup R}\,(\mathbf{x})\,.$$

Proof. We identify the underlying set of $Q \sqcup R$ with $Q \cup R$ (since the sets Q and R are already disjoint). If $f : Q \sqcup R \to \{1,2,3,\ldots\}$ is a $Q \sqcup R$-partition, then its restrictions $f\mid_Q$ and $f\mid_R$ are a Q-partition and an R-partition, respectively. Conversely, any pair of a Q-partition and an R-partition can be combined to form a $Q \sqcup R$-partition. Thus, there is a bijective correspondence between the addends in the expanded sum $F_Q\,(\mathbf{x})\, F_R\,(\mathbf{x})$ and the addends in $F_{Q\sqcup R}\,(\mathbf{x})$. ☐

Proof of Proposition 5.2.15. To prove formula (5.2.5) for α in Comp_n, note that

$$\Delta L_\alpha = L_\alpha(\mathbf{x},\mathbf{y}) = \sum_{k=0}^{n} \sum_{\substack{1\le i_1\le\cdots\le i_k,\\ 1\le i_{k+1}\le\cdots\le i_n:\\ i_r<i_{r+1} \text{ for } r\in D(\alpha)\setminus\{k\}}} x_{i_1}\cdots x_{i_k}\cdot y_{i_{k+1}}\cdots y_{i_n} \tag{5.2.8}$$

by Proposition 5.2.9 (where we identify $\mathrm{QSym}\otimes\mathrm{QSym}$ with a $\mathbf{k}$-subalgebra of $R(\mathbf{x},\mathbf{y})$ by means of the embedding $\mathrm{QSym}\otimes\mathrm{QSym} \xrightarrow{\cong} \mathrm{QSym}(\mathbf{x})\otimes\mathrm{QSym}(\mathbf{y}) \hookrightarrow R(\mathbf{x},\mathbf{y})$ as in the definition of the comultiplication on QSym). One then realizes that the inner sums corresponding to values of k that lie (resp. do not lie) in $D(\alpha)\cup\{0,n\}$ correspond to the terms $L_\beta(\mathbf{x})L_\gamma(\mathbf{y})$ for pairs (β,γ) in which $\beta\cdot\gamma=\alpha$ (resp. $\beta\odot\gamma=\alpha$).

For formula (5.2.6), let P be the labelled poset which is the disjoint union of linear orders w_α, w_β. Then

$$L_\alpha L_\beta = F_{w_\alpha}(\mathbf{x})F_{w_\beta}(\mathbf{x}) = F_P(\mathbf{x}) = \sum_{w\in\mathcal{L}(P)} F_w(\mathbf{x}) = \sum_{w\in w_\alpha \sqcup\!\sqcup w_\beta} L_{\gamma(w)}$$

where the first equality used Proposition 5.2.10, the second equality comes from Lemma 5.2.17, the third equality from Theorem 5.2.11, and the fourth from the equality $\mathcal{L}(P) = w_\alpha \sqcup\!\sqcup w_\beta$.

To prove formula (5.2.7), compute using Theorem 5.1.11 that

$$S(L_\alpha) = \sum_{\beta \text{ refining } \alpha} S(M_\beta) = \sum_{\substack{(\beta,\gamma):\\ \beta \text{ refines } \alpha,\\ \gamma \text{ coarsens } \mathrm{rev}(\beta)}} (-1)^{\ell(\beta)} M_\gamma = \sum_\gamma M_\gamma \sum_\beta (-1)^{\ell(\beta)}$$

in which the last inner sum is over β for which

$$D(\beta) \supset D(\alpha)\cup D(\mathrm{rev}(\gamma)).$$

The alternating signs make such inner sums vanish unless they have only the single term where $D(\beta)=[n-1]$ (that is, $\beta=(1^n)$). This happens exactly when $D(\mathrm{rev}(\gamma))\cup D(\alpha)=[n-1]$ or equivalently, when $D(\mathrm{rev}(\gamma))$ contains the complement of $D(\alpha)$, that is, when $D(\gamma)$ contains the complement of $D(\mathrm{rev}(\alpha))$, that is, when γ refines $\omega(\alpha)$. Thus

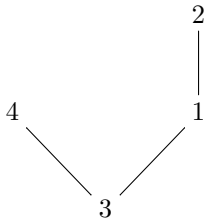
$$S(L_\alpha) = \sum_{\substack{\gamma\in\mathrm{Comp}_n:\\ \gamma \text{ refines } \omega(\alpha)}} M_\gamma\cdot(-1)^n = (-1)^{|\alpha|} L_{\omega(\alpha)}.$$

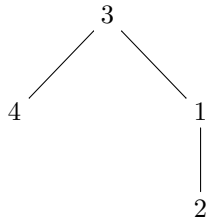
□

The antipode formula (5.2.7) for L_α leads to a general interpretation for the antipode of QSym acting on P-partition enumerators $F_P(\mathbf{x})$.

Definition 5.2.18. Given a labelled poset P on $\{1,2,\ldots,n\}$, let the *opposite* or *dual* labelled poset P^{opp} be the labelled poset on $\{1,2,\ldots,n\}$ that has $i <_{P^{\mathrm{opp}}} j$ if and only if $j <_P i$.

For example,

$P =$ 

$P^{\mathrm{opp}} =$ 

The following observation is straightforward.

Proposition 5.2.19. *When P is a linear order corresponding to some permutation $w=(w_1,\ldots,w_n)$ in $\mathfrak{S}_n$, then $w^{\mathrm{opp}} = ww_0$ where $w_0\in\mathfrak{S}_n$ is the permutation that swaps $i\leftrightarrow n+1-i$ (this is the so-called* longest permutation*, thus named due to it having the highest "Coxeter length" among all permutations in $\mathfrak{S}_n$). Furthermore, in this situation one has $F_w(\mathbf{x}) = L_\alpha$, that is, $\mathrm{Des}(w) = D(\alpha)$ if and only if $\mathrm{Des}(w^{\mathrm{opp}}) = D(\omega(\alpha))$, that is $F_{w^{\mathrm{opp}}}(\mathbf{x}) = L_{\omega(\alpha)}$. Thus,*

$$S(F_w(\mathbf{x})) = (-1)^n F_{w^{\mathrm{opp}}}(\mathbf{x}).$$

For example, given the compositions considered earlier:

$$\alpha = (4,2,2) = \ydiagram{2,2,4} \qquad \text{and} \qquad \omega(\alpha) = (1,2,2,1,1,1) = \ydiagram{3,2,1,1,1,1}$$

if one picks $w = 1235 \cdot 47 \cdot 68$ (with descent positions marked by dots) having $\mathrm{Des}(w) = \{4,6\} = D(\alpha)$, then $w^{\mathrm{opp}} = ww_0 = 8 \cdot 67 \cdot 45 \cdot 3 \cdot 2 \cdot 1$ has $\mathrm{Des}(w^{\mathrm{opp}}) = \{1,3,5,6,7\} = D(\omega(\alpha))$.

Corollary 5.2.20. *For any labelled poset P on $\{1,2,\ldots,n\}$, one has*

$$S\left(F_P(\mathbf{x})\right) = (-1)^n F_{P^{\mathrm{opp}}}(\mathbf{x}).$$

Proof. Since S is linear, one can apply Theorem 5.2.11 and Proposition 5.2.19, obtaining

$$S\left(F_P(\mathbf{x})\right) = \sum_{w \in \mathcal{L}(P)} S(F_w(\mathbf{x})) = \sum_{w \in \mathcal{L}(P)} (-1)^n F_{w^{\mathrm{opp}}}(\mathbf{x}) = (-1)^n F_{P^{\mathrm{opp}}}(\mathbf{x}),$$

as $\mathcal{L}(P^{\mathrm{opp}}) = \{w^{\mathrm{opp}} : w \in \mathcal{L}(P)\}$. □

Remark 5.2.21. Malvenuto and Reutenauer, in [147, Theorem 3.1], prove an even more general antipode formula, which encompasses our Corollary 5.2.20, Proposition 5.2.19, Theorem 5.1.11 and (5.2.7). See [85, Theorem 4.2] for a restatement and a self-contained proof of this theorem (and [85, Theorem 4.7] for an even further generalization).

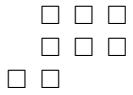
We remark on a special case of Corollary 5.2.20 to which we alluded earlier, related to skew Schur functions.

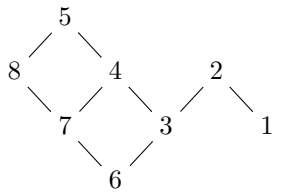
Corollary 5.2.22. *In Λ, the action of ω and the antipode S on skew Schur functions $s_{\lambda/\mu}$ are as follows:*

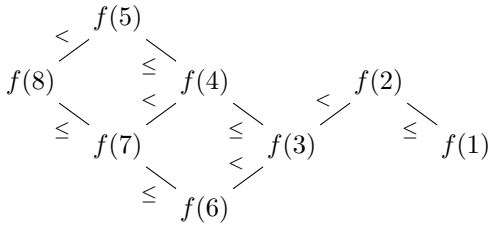
$$\omega(s_{\lambda/\mu}) = s_{\lambda^t/\mu^t}, \tag{5.2.9}$$

$$S(s_{\lambda/\mu}) = (-1)^{|\lambda/\mu|} s_{\lambda^t/\mu^t}. \tag{5.2.10}$$

Proof. Given a skew shape λ/μ, one can always create a labelled poset P which is its *skew Ferrers poset*, together with one of many *column-strict labellings*, in such a way that $F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x})$. An example is shown here for $\lambda/\mu = (4,4,2)/(1,1,0)$:

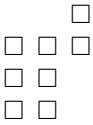
$\lambda/\mu =$ 

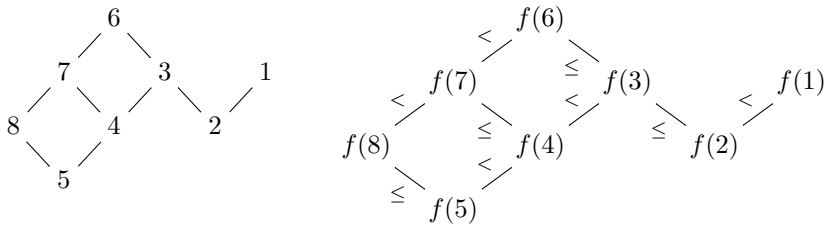
$P =$ 



The general definition is as follows: Let P be the set of all boxes of the skew diagram λ/μ. Label these boxes by the numbers $1,2,\ldots,n$ (where $n = |\lambda/\mu|$) row by row from bottom to top (reading every row from left to right), and then define an order relation $<_P$ on P by requiring that every box be smaller (in P) than its right neighbor and smaller (in P) than its lower neighbor. It is not hard to see that in this situation, $F_{P^{\mathrm{opp}}}(\mathbf{x}) = \sum_T \mathbf{x}^{\mathrm{cont}(T)}$ as T ranges over all *reverse semistandard tableaux* or *column-strict plane partitions*

of λ^t/μ^t:

$\lambda^t/\mu^t =$ 

$P^{\mathrm{opp}} =$ 

But this means that $F_{P^{\mathrm{opp}}}(\mathbf{x}) = s_{\lambda^t/\mu^t}(\mathbf{x})$, since the fact that skew Schur functions lie in Λ implies that they can be defined either as generating functions for column-strict tableaux or reverse semistandard tableaux; see Remark 2.2.5 above, or [206, Prop. 7.10.4].

Thus we have

$$F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x}),$$
$$F_{P^{\mathrm{opp}}}(\mathbf{x}) = s_{\lambda^t/\mu^t}(\mathbf{x}).$$

Corollary 1.4.27 tells us that the antipode for QSym must specialize to the antipode for Λ (see also Remark 5.4.11 below), so (5.2.10) is a special case of Corollary 5.2.20. Then (5.2.9) follows from the relation (2.4.11) that $S(f) = (-1)^n \omega(f)$ for f in Λ_n. □

Remark 5.2.23. Before leaving P-partitions temporarily, we mention two open questions about them.

The first is a conjecture of Stanley from his thesis [203]. As mentioned in the proof of Corollary 5.2.22, each skew Schur function $s_{\lambda/\mu}(\mathbf{x})$ is a special instance of P-partition enumerator $F_P(\mathbf{x})$.

Conjecture 5.2.24. *A labelled poset P has $F_P(\mathbf{x})$ symmetric, and not just quasisymmetric,* if and only if *P is a column-strict labelling of some skew Ferrers poset λ/μ.*

A somewhat weaker result in this direction was proven by Malvenuto in her thesis [145, Thm. 6.4], showing that if a labelled poset P has the stronger property that its set of linear extensions $\mathcal{L}(P)$ is a union of *plactic* or *Knuth equivalence classes*, then P must be a column-strict labelling of a skew Ferrers poset.

The next question is due to P. McNamara, and is suggested by the obvious factorizations of P-partition enumerators $F_{P_1 \sqcup P_2}(\mathbf{x}) = F_{P_1}(\mathbf{x}) F_{P_2}(\mathbf{x})$ (Lemma 5.2.17).

Question 5.2.25. If $\mathbf{k}$ is a field, does a *connected* labelled poset P always have $F_P(\mathbf{x})$ *irreducible* within the ring QSym?

The phrasing of this question requires further comment. It is assumed here that $\mathbf{x} = (x_1, x_2, \ldots)$ is infinite; for example when P is a 2-element chain labelled "against the grain" (i.e., the bigger element of the chain has the smaller label), then $F_P(\mathbf{x}) = e_2(\mathbf{x})$ is irreducible, but its specialization to two variables $\mathbf{x} = (x_1, x_2)$ is $e_2(x_1, x_2) = x_1 x_2$, which is reducible. If one wishes to work in finitely many variables $\mathbf{x} = (x_1, \ldots, x_m)$ one can perhaps assume that m is at least $|P| + 1$.

When working in QSym = QSym($\mathbf{x}$) in infinitely many variables, it is perhaps not so clear where factorizations occur. For example, if f lies in QSym and factors $f = g \cdot h$ with g, h in $R(\mathbf{x})$, does this imply that g, h also lie in QSym? The answer is "Yes" (for $\mathbf{k} = \mathbb{Z}$), but this is not obvious, and was proven by P. Pylyavskyy in [175, Chap. 11].

One also might wonder whether $\mathrm{QSym}_{\mathbb{Z}}$ is a unique factorization domain, but this follows from the result of M. Hazewinkel ([89] and [93, Thm. 6.7.5], and Theorem 6.4.3 further below) who proved a conjecture of Ditters that $\mathrm{QSym}_{\mathbb{Z}}$ is a polynomial algebra; earlier Malvenuto and Reutenauer [146, Cor. 2.2] had shown that $\mathrm{QSym}_{\mathbb{Q}}$ is a polynomial algebra. In fact, one can find polynomial generators $\{P_\alpha\}$ for $\mathrm{QSym}_{\mathbb{Q}}$ as a subset of the dual basis to the $\mathbb{Q}$-basis $\{\xi_\alpha\}$ for $\mathrm{NSym}_{\mathbb{Q}}$ which comes from taking products $\xi_\alpha := \xi_{\alpha_1} \cdots \xi_{\alpha_\ell}$ of the elements $\{\xi_n\}$ defined in Remark 5.4.4 below. Specifically, one takes those P_α for which the composition α is a *Lyndon composition*; see the First proof of Proposition 6.4.4 for a mild variation on this construction.

Hazewinkel's proof [93, Thm. 6.7.5] of the polynomiality of $\mathrm{QSym}_{\mathbb{Z}}$ also shows that QSym is a polynomial ring over Λ (see Corollary 6.5.33); in particular, this yields that QSym is a free Λ-module.[265]

An affirmative answer to Question 5.2.25 is known at least in the special case where P is a connected column-strict labelling of a skew Ferrers diagram, that is, when $F_P(\mathbf{x}) = s_{\lambda/\mu}(\mathbf{x})$ for some connected skew diagram λ/μ; see [13].

5.3. **Standardization of n-tuples and the fundamental basis.** Another equivalent description of the fundamental quasisymmetric functions L_α (Lemma 5.3.6 below) relies on the concept of words and of their standardizations. We shall study words in detail in Chapter 6; at this point, we merely introduce the few notions that we will need:

Definition 5.3.1. We fix a totally ordered set $\mathfrak{A}$, which we call the *alphabet*.

We recall that a *word over* $\mathfrak{A}$ is just a (finite) tuple of elements of $\mathfrak{A}$. A word $(w_1, w_2, \ldots, w_n)$ can be written as $w_1 w_2 \cdots w_n$ when this incurs no ambiguity.

If $w \in \mathfrak{A}^n$ is a word and $i \in \{1, 2, \ldots, n\}$, then the *$i$-th letter* of w means the i-th entry of the n-tuple w. This i-th letter will be denoted by w_i.

Our next definition relies on a simple fact about permutations and words:[266]

Proposition 5.3.2. *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be any word. Then, there exists a unique permutation $\sigma \in \mathfrak{S}_n$ such that for every two elements a and b of $\{1, 2, \ldots, n\}$ satisfying $a < b$, we have ($\sigma(a) < \sigma(b)$ if and only if $w_a \leq w_b$).*

Definition 5.3.3. Let $w \in \mathfrak{A}^n$ be any word. The unique permutation $\sigma \in \mathfrak{S}_n$ defined in Proposition 5.3.2 is called the *standardization* of w, and is denoted by $\operatorname{std} w$.

Example 5.3.4. If $\mathfrak{A}$ is the alphabet $\{1 < 2 < 3 < \cdots\}$, then $\operatorname{std}(41211424)$ is the permutation which is written (in one-line notation) as 61423758.

A simple method to compute the standardization of a word $w \in \mathfrak{A}^n$ is the following: Replace all occurrences of the smallest letter appearing in w by the numbers $1, 2, \ldots, m_1$ (where m_1 is the number of these occurrences); then replace all occurrences of the second-smallest letter appearing in w by the numbers $m_1 + 1, m_1 + 2, \ldots, m_1 + m_2$ (where m_2 is the number of these occurrences), and so on, until all letters are replaced by numbers.[267] The result is the standardization of w, in one-line notation.

Another method to compute the standardization $\operatorname{std} w$ of a word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ is based on sorting. Namely, consider the total order on the set $\mathfrak{A} \times \mathbb{Z}$ given by

$$(a, i) \leq (b, j) \text{ if and only if } (\text{either } a < b \text{ or } (a = b \text{ and } i \leq j)).$$

(In other words, two pairs in $\mathfrak{A} \times \mathbb{Z}$ are compared by first comparing their first entries, and then, in the case of a tie, using the second entries as tiebreakers.) Now, in order to compute $\operatorname{std} w$, we sort the n-tuple $((w_1, 1), (w_2, 2), \ldots, (w_n, n)) \in (\mathfrak{A} \times \mathbb{Z})^n$ into increasing order (with respect to the total order just described), thus obtaining a new n-tuple of the form $\left(\left(w_{\tau(1)}, \tau(1)\right), \left(w_{\tau(2)}, \tau(2)\right), \ldots, \left(w_{\tau(n)}, \tau(n)\right)\right)$ for some $\tau \in \mathfrak{S}_n$; the standardization $\operatorname{std} w$ is then τ^{-1}.

Definition 5.3.5. Let $n \in \mathbb{N}$. Let $\sigma \in \mathfrak{S}_n$. Define a subset $\operatorname{Des}\sigma$ of $\{1, 2, \ldots, n-1\}$ by

$$\operatorname{Des}\sigma = \{i \in \{1, 2, \ldots, n-1\} \mid \sigma(i) > \sigma(i+1)\}.$$

(This is a particular case of the definition of $\operatorname{Des} w$ in Exercise 2.9.11, if we identify σ with the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. It is also a particular case of the definition of $\operatorname{Des} w$ in Proposition 5.2.10, if we identify σ with the total order $(\sigma(1) < \sigma(2) < \cdots < \sigma(n))$ on the set $\{1, 2, \ldots, n\}$.)

There is a unique composition α of n satisfying $D(\alpha) = \operatorname{Des}\sigma$ (where $D(\alpha)$ is defined as in Definition 5.1.10). This composition will be denoted by $\gamma(\sigma)$.

---

[265] The latter statement has an analogue in finitely many indeterminates, proven by Lauve and Mason in [125, Corollary 13]: The quasisymmetric functions $\mathrm{QSym}\left(\{x_i\}_{i \in I}\right)$ are free as a $\Lambda\left(\{x_i\}_{i \in I}\right)$-module for any totally ordered set I, infinite or not. In the case of finite I, this cannot be derived by Hazewinkel's arguments, as the ring $\mathrm{QSym}\left(\{x_i\}_{i \in I}\right)$ is not in general a polynomial ring (e.g., when $\mathbf{k} = \mathbb{Q}$ and $I = \{1, 2\}$, this ring is not even a UFD, as witnessed by $\left(x_1^2 x_2\right) \cdot \left(x_1 x_2^2\right) = (x_1 x_2)^3$).

[266] See Exercise 5.3.7 below for a proof of Proposition 5.3.2.

[267] Here, a number is not considered to be a letter; thus, a number that replaces a letter will always be left in peace afterwards.

The following lemma (equivalent to [182, Lemma 9.39]) yields another description of the fundamental quasisymmetric functions:

Lemma 5.3.6. *Let $\mathfrak{A}$ denote the totally ordered set $\{1 < 2 < 3 < \cdots\}$ of positive integers. For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$.*

Let $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Then,

$$L_{\gamma(\sigma)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w.$$

Exercise 5.3.7. Prove Proposition 5.3.2 and Lemma 5.3.6.

5.4. **The Hopf algebra** NSym **dual to** QSym**.** We introduce here the (graded) dual Hopf algebra to QSym. This is well-defined, as QSym is connected graded of finite type.

Definition 5.4.1. Let $\mathrm{NSym} := \mathrm{QSym}^o$, with dual pairing $\mathrm{NSym} \otimes \mathrm{QSym} \xrightarrow{(\cdot,\cdot)} \mathbf{k}$. Let $\{H_\alpha\}$ be the $\mathbf{k}$-basis of NSym dual to the $\mathbf{k}$-basis $\{M_\alpha\}$ of QSym, so that

$$(H_\alpha, M_\beta) = \delta_{\alpha,\beta}.$$

When the base ring $\mathbf{k}$ is not clear from the context, we write $\mathrm{NSym}_{\mathbf{k}}$ in lieu of NSym.

The Hopf algebra NSym is known as the *Hopf algebra of noncommutative symmetric functions*. Its study goes back to [77].

Theorem 5.4.2. *Letting $H_n := H_{(n)}$ for $n = 0, 1, 2, \ldots$, with $H_0 = 1$, one has that*

$$\mathrm{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots \rangle, \tag{5.4.1}$$

the free associative (but not commutative) algebra on generators $\{H_1, H_2, \ldots\}$ with coproduct determined by[268]

$$\Delta H_n = \sum_{i+j=n} H_i \otimes H_j. \tag{5.4.2}$$

Proof. Since Proposition 5.1.7 asserts that $\Delta M_\alpha = \sum_{(\beta,\gamma):\beta\cdot\gamma=\alpha} M_\beta \otimes M_\gamma$, and since $\{H_\alpha\}$ are dual to $\{M_\alpha\}$, one concludes that for any compositions β, γ, one has

$$H_\beta H_\gamma = H_{\beta\cdot\gamma}.$$

Iterating this gives

$$H_\alpha = H_{(\alpha_1,\ldots,\alpha_\ell)} = H_{\alpha_1} \cdots H_{\alpha_\ell}. \tag{5.4.3}$$

Since the H_α are a $\mathbf{k}$-basis for NSym, this shows $\mathrm{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots \rangle$.

Note that $H_n = H_{(n)}$ is dual to $M_{(n)}$, so to understand ΔH_n, one should understand how $M_{(n)}$ can appear as a term in the product $M_\alpha M_\beta$. By (5.1.1) this occurs only if $\alpha = (i), \beta = (j)$ where $i + j = n$, where

$$M_{(i)} M_{(j)} = M_{(i+j)} + M_{(i,j)} + M_{(j,i)}$$

(where the $M_{(i,j)}$ and $M_{(j,i)}$ addends have to be disregarded if one of i and j is 0). By duality, this implies the formula (5.4.2). □

Corollary 5.4.3. *The algebra homomorphism defined by*

$$\begin{array}{ccc} \mathrm{NSym} & \xrightarrow{\pi} & \Lambda, \\ H_n & \longmapsto & h_n \end{array}$$

is a Hopf algebra surjection, and adjoint to the inclusion $\Lambda \xhookrightarrow{i} \mathrm{QSym}$ (with respect to the dual pairing $\mathrm{NSym} \otimes \mathrm{QSym} \xrightarrow{(\cdot,\cdot)} \mathbf{k}$).

[268] The abbreviated summation indexing $\sum_{i+j=n} t_{i,j}$ used here is intended to mean

$$\sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j=n}} t_{i,j}.$$

Proof. As an algebra morphism, π may be identified with the surjection $T(V) \to \mathrm{Sym}(V)$ from the tensor algebra on a graded free $\mathbf{k}$-module V with basis $\{H_1, H_2, \ldots\}$ to the symmetric algebra on V, since

$$\begin{aligned} \mathrm{NSym} &\cong \mathbf{k}\langle H_1, H_2, \ldots\rangle, \\ \Lambda &\cong \mathbf{k}[h_1, h_2, \ldots]. \end{aligned}$$

As (5.4.2) and Proposition 2.3.6(iii) assert that

$$\begin{aligned} \Delta H_n &= \sum_{i+j=n} H_i \otimes H_j, \\ \Delta h_n &= \sum_{i+j=n} h_i \otimes h_j, \end{aligned}$$

this map π is also a bialgebra morphism, and hence a Hopf morphism by Corollary 1.4.27.

To check π is adjoint to i, let $\lambda(\alpha)$ denote the partition which is the weakly decreasing rearrangement of the composition α, and note that the bases $\{H_\alpha\}$ of NSym and $\{m_\lambda\}$ of Λ satisfy

$$(\pi(H_\alpha), m_\lambda) = (h_{\lambda(\alpha)}, m_\lambda) = \begin{Bmatrix} 1 & \text{if } \lambda(\alpha) = \lambda \\ 0 & \text{otherwise} \end{Bmatrix} = \left(H_\alpha, \sum_{\beta : \lambda(\beta) = \lambda} M_\beta \right) = (H_\alpha, i(m_\lambda)).$$

□

Remark 5.4.4. For those who prefer generating functions to sign-reversing involutions, we sketch here Malvenuto and Reutenauer's elegant proof [146, Cor. 2.3] of the antipode formula (Theorem 5.1.11). One needs to know that when $\mathbb{Q}$ is a subring of $\mathbf{k}$, and A is a $\mathbf{k}$-algebra (possibly noncommutative), in the ring of power series $A[[t]]$ where t commutes with all of A, one still has familiar facts, such as

$$a(t) = \log b(t) \quad \text{ if and only if } \quad b(t) = \exp a(t)$$

and whenever $a(t), b(t)$ commute in $A[[t]]$, one has

$$\exp\left(a(t) + b(t)\right) = \exp a(t) \exp b(t), \tag{5.4.4}$$

$$\log\left(a(t) b(t)\right) = \log a(t) + \log b(t). \tag{5.4.5}$$

Start by assuming WLOG that $\mathbf{k} = \mathbb{Z}$ (as $\mathrm{NSym}_{\mathbf{k}} = \mathrm{NSym}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbf{k}$ in the general case). Now, define in $\mathrm{NSym}_{\mathbb{Q}} = \mathrm{NSym} \otimes_{\mathbb{Z}} \mathbb{Q}$ the elements $\{\xi_1, \xi_2, \ldots\}$ via generating functions in $\mathrm{NSym}_{\mathbb{Q}}[[t]]$:

$$\begin{aligned} \widetilde{H}(t) &:= \sum_{n \geq 0} H_n t^n, \\ \xi(t) &:= \sum_{n \geq 1} \xi_n t^n = \log \widetilde{H}(t). \end{aligned} \tag{5.4.6}$$

One first checks that this makes each ξ_n primitive, via a computation in the ring $(\mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}})[[t]]$ (into which we "embed" the ring $(\mathrm{NSym}_{\mathbb{Q}}[[t]]) \otimes_{\mathbb{Q}[[t]]} (\mathrm{NSym}_{\mathbb{Q}}[[t]])$ via the canonical ring homomorphism from the latter into the former [269]):

$$\begin{aligned} \Delta\xi(t) = \Delta\left(\log \sum_{n \geq 0} H_n t^n \right) &= \log \sum_{n \geq 0} \Delta(H_n) t^n = \log \sum_{n \geq 0} \left(\sum_{i+j=n} H_i \otimes H_j \right) t^n \\ &= \log\left(\left(\sum_{i \geq 0} H_i t^i \right) \otimes \left(\sum_{j \geq 0} H_j t^j \right) \right) = \log\left(\left(\sum_{i \geq 0} H_i t^i \otimes 1 \right) \left(1 \otimes \sum_{j \geq 0} H_j t^j \right) \right) \\ &\overset{(5.4.5)}{=} \log \widetilde{H}(t) \otimes 1 + 1 \otimes \log \widetilde{H}(t) = \xi(t) \otimes 1 + 1 \otimes \xi(t). \end{aligned}$$

[269] This ring homomorphism might fail to be injective, whence the "embed" stands in quotation marks. This does not need to worry us, since we will not draw any conclusions in $(\mathrm{NSym}_{\mathbb{Q}}[[t]]) \otimes_{\mathbb{Q}[[t]]} (\mathrm{NSym}_{\mathbb{Q}}[[t]])$ from our computation.

We are also somewhat cavalier with the notation Δ: we use it both for the comultiplication $\Delta : \mathrm{NSym}_{\mathbb{Q}} \to \mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}}$ of the Hopf algebra $\mathrm{NSym}_{\mathbb{Q}}$ and for the continuous $\mathbf{k}$-algebra homomorphism $\mathrm{NSym}_{\mathbb{Q}}[[t]] \to \left(\mathrm{NSym}_{\mathbb{Q}} \otimes \mathrm{NSym}_{\mathbb{Q}}\right)[[t]]$ it induces.

Comparing coefficients in this equality yields $\Delta(\xi_n) = \xi_n \otimes 1 + 1 \otimes \xi_n$. Thus $S(\xi_n) = -\xi_n$, by Proposition 1.4.17. This allows one to determine $S(H_n)$ and $S(H_\alpha)$, after one first inverts the relation (5.4.6) to get that $\widetilde{H}(t) = \exp \xi(t)$, and hence

$$\begin{aligned} S(\widetilde{H}(t)) &= S(\exp \xi(t)) = \exp S(\xi(t)) = \exp(-\xi(t)) \overset{(5.4.4)}{=} (\exp \xi(t))^{-1} \\ &= \widetilde{H}(t)^{-1} = \left(1 + H_1 t + H_2 t^2 + \cdots\right)^{-1}. \end{aligned}$$

Upon expanding the right side, and comparing coefficients of t^n, this gives

$$S(H_n) = \sum_{\beta \in \mathrm{Comp}_n} (-1)^{\ell(\beta)} H_\beta$$

and hence

$$S(H_\alpha) = S(H_{\alpha_\ell}) \cdots S(H_{\alpha_2}) S(H_{\alpha_1}) = \sum_{\substack{\gamma: \\ \gamma \text{ refines } \mathrm{rev}(\alpha)}} (-1)^{\ell(\gamma)} H_\gamma = \sum_{\substack{\gamma: \\ \mathrm{rev}(\gamma) \text{ refines } \alpha}} (-1)^{\ell(\gamma)} H_\gamma$$

(because if μ and ν are two compositions, then μ refines ν if and only if $\mathrm{rev}(\mu)$ refines $\mathrm{rev}(\nu)$). As $S_{\mathrm{NSym}}, S_{\mathrm{QSym}}$ are adjoint, and $\{H_\alpha\}, \{M_\alpha\}$ are dual bases, this is equivalent to saying that

$$S(M_\alpha) = (-1)^{\ell(\alpha)} \sum_{\substack{\gamma: \\ \mathrm{rev}(\alpha) \text{ refines } \gamma}} M_\gamma \qquad \text{for all } \alpha \in \mathrm{Comp}.$$

But this is precisely the claim of Theorem 5.1.11. Thus, Theorem 5.1.11 is proven once again.

Let us say a bit more about the elements ξ_n defined in (5.4.6) above. The elements $n\xi_n$ are noncommutative analogues of the power sum symmetric functions p_n (and, indeed, are lifts of the latter to NSym, as Exercise 5.4.5 below shows). They are called the *noncommutative power sums of the second kind* in [77][270], and their products form a basis of NSym. They are furthermore useful in studying the so-called *Eulerian idempotent* of a cocommutative Hopf algebra, as shown in Exercise 5.4.6 below.

Exercise 5.4.5. Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Define a sequence of elements $\xi_1, \xi_2, \xi_3, \ldots$ of $\mathrm{NSym} = \mathrm{NSym}_{\mathbf{k}}$ by (5.4.6).

(a) For every $n \geq 1$, show that ξ_n is a primitive homogeneous element of NSym of degree n.

(b) For every $n \geq 1$, show that $\pi(n\xi_n)$ is the n-th power sum symmetric function $p_n \in \Lambda$.

(c) For every $n \geq 1$, show that

$$\xi_n = \sum_{\alpha \in \mathrm{Comp}_n} (-1)^{\ell(\alpha)-1} \frac{1}{\ell(\alpha)} H_\alpha. \tag{5.4.7}$$

(d) For every composition α, define an element ξ_α of NSym by $\xi_\alpha = \xi_{\alpha_1} \xi_{\alpha_2} \cdots \xi_{\alpha_\ell}$, where α is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$. Show that

$$H_n = \sum_{\alpha \in \mathrm{Comp}_n} \frac{1}{\ell(\alpha)!} \xi_\alpha \tag{5.4.8}$$

for every $n \in \mathbb{N}$.

Use this to prove that $(\xi_\alpha)_{\alpha \in \mathrm{Comp}_n}$ is a $\mathbf{k}$-basis of NSym_n for every $n \in \mathbb{N}$.

Exercise 5.4.6. Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let A be a cocommutative connected graded $\mathbf{k}$-bialgebra. Let $A = \bigoplus_{n \geq 0} A_n$ be the decomposition of A into homogeneous components. If f is any $\mathbf{k}$-linear map $A \to A$ annihilating A_0, then f is locally $\star$-nilpotent[271], and so the sum $\log^\star(f + u\epsilon) := \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}$ is a well-defined endomorphism of A [272]. Let $\mathfrak{e}$ denote the endomorphism $\log^\star(\mathrm{id}_A)$ of A (obtained by setting $f = \mathrm{id}_A - u\epsilon : A \to A$). Show that $\mathfrak{e}$ is a projection from A to the $\mathbf{k}$-submodule $\mathfrak{p}$ of all primitive elements of A (and thus, in particular, is idempotent).

[270] See Exercise 5.4.12 for the ones of the first kind.

[271] See the proof of Proposition 1.4.24 for what this means.

[272] This definition of $\log^\star(f + u\epsilon)$ is actually a particular case of Definition 1.7.17. This can be seen as follows:

We have $f(A_0) = 0$. Thus, Proposition 1.7.11(h) (applied to $C = A$) yields $f \in \mathfrak{n}(A, A)$ (where $\mathfrak{n}(A, A)$ is defined as in Section 1.7), so that $(f + u\epsilon) - u\epsilon = f \in \mathfrak{n}(A, A)$. Therefore, Definition 1.7.17 defines a map $\log^\star(f + u\epsilon) \in \mathfrak{n}(A, A)$. This map is identical to the map $\log^\star(f + u\epsilon) := \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}$ we have just defined, because Proposition 1.7.18(f) (applied

Hint: For every $n \geq 0$, let $\pi_n : A \to A$ be the projection onto the n-th homogeneous component A_n. Since NSym is the free $\mathbf{k}$-algebra with generators $H_1, H_2, H_3, \ldots$, we can define a $\mathbf{k}$-algebra homomorphism $\mathfrak{W} : \mathrm{NSym} \to (\mathrm{End}\, A, \star)$ by sending H_n to π_n. Show that:

(a) The map $\mathfrak{e} : A \to A$ is graded. For every $n \geq 0$, we will denote the map $\pi_n \circ \mathfrak{e} = \mathfrak{e} \circ \pi_n : A \to A$ by $\mathfrak{e}_n$.
(b) We have $\mathfrak{W}(\xi_n) = \mathfrak{e}_n$ for all $n \geq 1$, where ξ_n is defined as in Exercise 5.4.5.
(c) If w is an element of NSym, and if we write $\Delta(w) = \sum_{(w)} w_1 \otimes w_2$ using the Sweedler notation, then $\Delta \circ (\mathfrak{W}(w)) = \left(\sum_{(w)} \mathfrak{W}(w_1) \otimes \mathfrak{W}(w_2)\right) \circ \Delta$.
(d) We have $\mathfrak{e}_n(A) \subset \mathfrak{p}$ for every $n \geq 0$.
(e) We have $\mathfrak{e}(A) \subset \mathfrak{p}$.
(f) The map $\mathfrak{e}$ fixes any element of $\mathfrak{p}$.

Remark 5.4.7. The endomorphism $\mathfrak{e}$ of Exercise 5.4.6 is known as the *Eulerian idempotent* of A, and can be contrasted with the Dynkin idempotent of Remark 1.5.15. It has been studied in [166], [169], [31] and [60], and relates to the Hochschild cohomology of commutative algebras [134, §4.5.2].

Exercise 5.4.8. Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let A, A_n and $\mathfrak{e}$ be as in Exercise 5.4.6.

(a) Show that $\mathfrak{e}^{\star n} \circ \mathfrak{e}^{\star m} = n! \delta_{n,m} \mathfrak{e}^{\star n}$ for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$.
(b) Show that $\mathfrak{e}^{\star n} \circ \mathrm{id}_A^{\star m} = \mathrm{id}_A^{\star m} \circ \mathfrak{e}^{\star n} = m^n \mathfrak{e}^{\star n}$ for all $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

We next explore the basis for NSym dual to the $\{L_\alpha\}$ in QSym.

Definition 5.4.9. Define the *noncommutative ribbon functions* $\{R_\alpha\}_{\alpha \in \mathrm{Comp}}$ to be the $\mathbf{k}$-basis of NSym dual to the fundamental basis $\{L_\alpha\}_{\alpha \in \mathrm{Comp}}$ of QSym, so that

$$(R_\alpha, L_\beta) = \delta_{\alpha,\beta} \qquad \text{for all } \alpha, \beta \in \mathrm{Comp}.$$

Theorem 5.4.10. (a) *One has that*

$$H_\alpha = \sum_{\beta \text{ coarsens } \alpha} R_\beta; \tag{5.4.9}$$

$$R_\alpha = \sum_{\beta \text{ coarsens } \alpha} (-1)^{\ell(\beta)-\ell(\alpha)} H_\beta. \tag{5.4.10}$$

(b) *The surjection* $\mathrm{NSym} \xrightarrow{\pi} \Lambda$ *sends* $R_\alpha \longmapsto s_{\mathrm{Rib}(\alpha)}$, *the skew Schur function associated to the ribbon* $\mathrm{Rib}(\alpha)$.
(c) *Furthermore,*

$$R_\alpha R_\beta = R_{\alpha \cdot \beta} + R_{\alpha \odot \beta} \qquad \text{if } \alpha \text{ and } \beta \text{ are nonempty}; \tag{5.4.11}$$

$$S(R_\alpha) = (-1)^{|\alpha|} R_{\omega(\alpha)}. \tag{5.4.12}$$

Finally, $R_\varnothing$ *is the multiplicative identity of* NSym.

Proof. (a) For (5.4.9), note that

$$H_\alpha = \sum_\beta (H_\alpha, L_\beta) R_\beta = \sum_\beta \left(H_\alpha, \sum_{\substack{\gamma: \\ \gamma \text{ refines } \beta}} M_\gamma \right) R_\beta = \sum_{\substack{\beta: \\ \beta \text{ coarsens } \alpha}} R_\beta.$$

The equality (5.4.10) follows from (5.4.9) by Lemma 5.2.7(a).

(b) Write α as $(\alpha_1, \ldots, \alpha_\ell)$. To show that $\pi(R_\alpha) = s_{\mathrm{Rib}(\alpha)}$, we instead examine $\pi(H_\alpha)$:

$$\pi(H_\alpha) = \pi(H_{\alpha_1} \cdots H_{\alpha_\ell}) = h_{\alpha_1} \cdots h_{\alpha_\ell} = s_{(\alpha_1)} \cdots s_{(\alpha_\ell)} = s_{(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)}$$

---

to $C = A$) shows that the map $\log^\star(f + u\epsilon)$ defined using Definition 1.7.17 satisfies

$$\log^\star(f + u\epsilon) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} f^{\star n} = \sum_{n \geq 1} (-1)^{n-1} \frac{1}{n} f^{\star n}.$$

where $(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$ is some skew shape which is a horizontal strip having rows of lengths $\alpha_1, \ldots, \alpha_\ell$ from bottom to top. We claim

$$s_{(\alpha_1)\oplus\cdots\oplus(\alpha_\ell)} = \sum_{\substack{\beta: \\ \beta \text{ coarsens } \alpha}} s_{\mathrm{Rib}(\beta)},$$

because column-strict tableaux T of shape $(\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$ biject to column-strict tableaux T' of some ribbon $\mathrm{Rib}\,(\beta)$ with β coarsening α, as follows: Let a_i, b_i denote the leftmost, rightmost entries of the i-th row from the bottom in T, of length α_i, and

- if $b_i \leq a_{i+1}$, merge parts α_i, α_{i+1} in β, and concatenate the rows of length α_i, α_{i+1} in T', or
- if $b_i > a_{i+1}$, do not merge parts α_i, α_{i+1} in β, and let these two rows overlap in one column in T'.

E.g., if $\alpha = (3,3,2,3,2)$, then

$$\text{the tableau } T = \begin{array}{*{9}{c}} & & & & & & & 3 & 4 \\ & & & & & & 4 & 4 & 5 \\ & & & & 4 & 4 & & & \\ & & & 2 & 2 & 3 & & & \\ & & 1 & 1 & 3 & & & & \end{array} \quad \text{of shape } (\alpha_1) \oplus \cdots \oplus (\alpha_\ell)$$

$$\text{maps to the tableau } T' = \begin{array}{*{11}{c}} & & & & & & & & & 3 & 4 \\ & & 2 & 2 & 3 & 4 & 4 & 4 & 4 & 5 & \\ & 1 & 1 & 3 & & & & & & & \end{array} \quad \text{of shape } \mathrm{Rib}\,(\beta) \text{ for } \beta = (3,8,2).$$

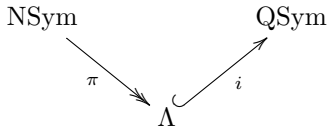
The reverse bijection breaks the rows of T' into the rows of T of lengths dictated by the parts of α. Having shown $\pi(H_\alpha) = \sum_{\beta:\beta \text{ coarsens } \alpha} s_{\mathrm{Rib}(\beta)}$, we can now apply Lemma 5.2.7(a) to obtain

$$s_{\mathrm{Rib}(\alpha)} = \sum_{\beta:\beta \text{ coarsens } \alpha} (-1)^{\ell(\alpha)-\ell(\beta)}\, \pi\left(H_\beta\right) = \pi\left(R_\alpha\right) \qquad (\text{by (5.4.10)});$$

thus, $\pi(R_\alpha) = s_{\mathrm{Rib}(\alpha)}$ is proven.

(c) Finally, (5.4.11) and (5.4.12) follow from (5.2.5) and (5.2.7) by duality. □

Remark 5.4.11. Since the maps



are Hopf morphisms, they must respect the antipodes $S_\Lambda, S_{\mathrm{QSym}}, S_{\mathrm{NSym}}$, but it is interesting to compare them explicitly using the fundamental basis for QSym and the ribbon basis for NSym.

On one hand (5.2.7) shows that $S_{\mathrm{QSym}}(L_\alpha) = (-1)^{|\alpha|} L_{\omega(\alpha)}$ extends the map S_Λ since $L_{(1^n)} = e_n$ and $L_{(n)} = h_n$, as observed in Example 5.2.5, and $\omega((n)) = (1^n)$.

On the other hand, (5.4.12) shows that $S_{\mathrm{NSym}}(R_\alpha) = (-1)^{|\alpha|} R_{\omega(\alpha)}$ lifts the map S_Λ to S_{NSym}: Theorem 5.4.10(b) showed that R_α lifts the skew Schur function $s_{\mathrm{Rib}(\alpha)}$, while (2.4.15) asserted that $S(s_{\lambda/\mu}) = (-1)^{|\lambda/\mu|} s_{\lambda^t/\mu^t}$, and a ribbon $\mathrm{Rib}\,(\alpha) = \lambda/\mu$ has $\mathrm{Rib}\,(\omega(\alpha)) = \lambda^t/\mu^t$.

Exercise 5.4.12. (a) Show that any integers n and i with $0 \leq i < n$ satisfy

$$R_{(1^i, n-i)} = \sum_{j=0}^{i} (-1)^{i-j} R_{(1^j)} H_{n-j}.$$

(Here, as usual, 1^i stands for the number 1 repeated i times.)

(b) Show that any integers n and i with $0 \leq i < n$ satisfy

$$(-1)^i R_{(1^i, n-i)} = \sum_{j=0}^{i} S\left(H_j\right) H_{n-j}.$$

(c) For every positive integer n, define an element Ψ_n of NSym by

$$\Psi_n = \sum_{i=0}^{n-1} (-1)^i R_{(1^i, n-i)}.$$

Show that $\Psi_n = (S \star E)(H_n)$, where the map $E : \mathrm{NSym} \to \mathrm{NSym}$ is defined as in Exercise 1.5.14 (for $A = \mathrm{NSym}$). Conclude that Ψ_n is primitive.

(d) Prove that

$$\sum_{k=0}^{n-1} H_k \Psi_{n-k} = n H_n$$

for every $n \in \mathbb{N}$.

(e) Define two power series $\psi(t)$ and $\widetilde{H}(t)$ in $\mathrm{NSym}[[t]]$ by

$$\psi(t) = \sum_{n \geq 1} \Psi_n t^{n-1};$$
$$\widetilde{H}(t) = \sum_{n \geq 0} H_n t^n.$$

Show that[273] $\dfrac{d}{dt}\widetilde{H}(t) = \widetilde{H}(t) \cdot \psi(t)$.

(The functions Ψ_n are called *noncommutative power sums of the first kind*; they are studied in [77]. The power sums of the second kind are the $n\xi_n$ in Remark 5.4.4.)

(f) Show that $\pi(\Psi_n)$ equals the power sum symmetric function p_n for every positive integer n.

(g) Show that every positive integer n satisfies

$$p_n = \sum_{i=0}^{n-1} (-1)^i s_{(n-i, 1^i)} \qquad \text{in } \Lambda.$$

(h) For every nonempty composition α, define a positive integer $\mathrm{lp}(\alpha)$ by $\mathrm{lp}(\alpha) = \alpha_\ell$, where α is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$. (Thus, $\mathrm{lp}(\alpha)$ is the last part of α.) Show that every positive integer n satisfies

$$\Psi_n = \sum_{\alpha \in \mathrm{Comp}_n} (-1)^{\ell(\alpha)-1} \mathrm{lp}(\alpha) H_\alpha. \tag{5.4.13}$$

(i) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. For every composition α, define an element Ψ_α of NSym by $\Psi_\alpha = \Psi_{\alpha_1} \Psi_{\alpha_2} \cdots \Psi_{\alpha_\ell}$, where α is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$. For every composition α, define $\pi_u(\alpha)$ to be the positive integer $\alpha_1 (\alpha_1 + \alpha_2) \cdots (\alpha_1 + \alpha_2 + \cdots + \alpha_\ell)$, where α is written in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$. Show that

$$H_n = \sum_{\alpha \in \mathrm{Comp}_n} \frac{1}{\pi_u(\alpha)} \Psi_\alpha \tag{5.4.14}$$

for every $n \in \mathbb{N}$.

Use this to prove that $(\Psi_\alpha)_{\alpha \in \mathrm{Comp}_n}$ is a $\mathbf{k}$-basis of NSym_n for every $n \in \mathbb{N}$.

(j) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let V be the free $\mathbf{k}$-module with basis $(\mathfrak{b}_n)_{n \in \{1,2,3,\ldots\}}$. Define a $\mathbf{k}$-module homomorphism $f : V \to \mathrm{NSym}$ by requiring that $f(\mathfrak{b}_n) = \Psi_n$ for every $n \in \{1, 2, 3, \ldots\}$. Let F be the $\mathbf{k}$-algebra homomorphism $T(V) \to \mathrm{NSym}$ induced by this f (using the universal property of the tensor algebra $T(V)$). Show that F is a Hopf algebra isomorphism (where the Hopf algebra structure on $T(V)$ is as in Example 1.4.18).

(k) Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let V be as in Exercise 5.4.12(j). Show that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ (defined as in Proposition 1.6.7) as Hopf algebras.

(l) Solve parts (a) and (b) of Exercise 2.9.14 again using the ribbon basis functions R_α.

[273] The derivative $\frac{d}{dt} Q(t)$ of a power series $Q(t) \in R[[t]]$ over a noncommutative ring R is defined just as in the case of R commutative: by setting $\frac{d}{dt} Q(t) = \sum_{i \geq 1} i q_i t^{i-1}$, where $Q(t)$ is written in the form $Q(t) = \sum_{i \geq 0} q_i t^i$.

One might wonder whether the Frobenius endomorphisms of Λ (defined in Exercise 2.9.9) and the Verschiebung endomorphisms of Λ (defined in Exercise 2.9.10) generalize to analogous operators on either QSym or NSym. The next two exercises (whose claims mostly come from [90, §13]) answer this question: The Frobenius endomorphisms extend to QSym, and the Verschiebung ones lift to NSym.

Exercise 5.4.13. For every $n \in \{1,2,3,\ldots\}$, define a map $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ by setting

$$\mathbf{F}_n(a) = a(x_1^n, x_2^n, x_3^n, \ldots) \qquad \text{for every } a \in \mathrm{QSym}.$$

(So what $\mathbf{F}_n$ does to a quasi-symmetric function is replacing all variables $x_1, x_2, x_3, \ldots$ by their n-th powers.)

(a) Show that $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ is a $\mathbf{k}$-algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.
(b) Show that $\mathbf{F}_n \circ \mathbf{F}_m = \mathbf{F}_{nm}$ for any two positive integers n and m.
(c) Show that $\mathbf{F}_1 = \mathrm{id}$.
(d) Prove that $\mathbf{F}_n\left(M_{(\beta_1,\beta_2,\ldots,\beta_s)}\right) = M_{(n\beta_1,n\beta_2,\ldots,n\beta_s)}$ for every $n \in \{1,2,3,\ldots\}$ and $(\beta_1,\beta_2,\ldots,\beta_s) \in \mathrm{Comp}$.
(e) Prove that $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ is a Hopf algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.
(f) Consider the maps $\mathbf{f}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.9. Show that $\mathbf{F}_n \mid_\Lambda = \mathbf{f}_n$ for every $n \in \{1,2,3,\ldots\}$.
(g) Assume that $\mathbf{k} = \mathbb{Z}$. Prove that $\mathbf{f}_p(a) \equiv a^p \bmod p\,\mathrm{QSym}$ for every $a \in \mathrm{QSym}$ and every prime number p.
(h) Give a new solution to Exercise 2.9.9(d).

Exercise 5.4.14. For every $n \in \{1,2,3,\ldots\}$, define a $\mathbf{k}$-algebra homomorphism $\mathbf{V}_n : \mathrm{NSym} \to \mathrm{NSym}$ by

$$\mathbf{V}_n(H_m) = \begin{cases} H_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases} \qquad \text{for every positive integer } m$$

[274].

(a) Show that any positive integers n and m satisfy

$$\mathbf{V}_n(\Psi_m) = \begin{cases} n\Psi_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases},$$

where the elements Ψ_m and $\Psi_{m/n}$ of NSym are as defined in Exercise 5.4.12(c).
(b) Show that if $\mathbb{Q}$ is a subring of $\mathbf{k}$, then any positive integers n and m satisfy

$$\mathbf{V}_n(\xi_m) = \begin{cases} \xi_{m/n}, & \text{if } n \mid m; \\ 0, & \text{if } n \nmid m \end{cases},$$

where the elements ξ_m and $\xi_{m/n}$ of NSym are as defined in Exercise 5.4.5.
(c) Prove that $\mathbf{V}_n \circ \mathbf{V}_m = \mathbf{V}_{nm}$ for any two positive integers n and m.
(d) Prove that $\mathbf{V}_1 = \mathrm{id}$.
(e) Prove that $\mathbf{V}_n : \mathrm{NSym} \to \mathrm{NSym}$ is a Hopf algebra homomorphism for every $n \in \{1,2,3,\ldots\}$.

Now, consider also the maps $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ defined in Exercise 2.9.9. Fix a positive integer n.

(f) Prove that the maps $\mathbf{F}_n : \mathrm{QSym} \to \mathrm{QSym}$ and $\mathbf{V}_n : \mathrm{NSym} \to \mathrm{NSym}$ are adjoint with respect to the dual pairing $\mathrm{NSym} \otimes \mathrm{QSym} \xrightarrow{(\cdot,\cdot)} \mathbf{k}$.
(g) Consider the maps $\mathbf{v}_n : \Lambda \to \Lambda$ defined in Exercise 2.9.10. Show that the surjection $\pi : \mathrm{NSym} \to \Lambda$ satisfies $\mathbf{v}_n \circ \pi = \pi \circ \mathbf{V}_n$ for every $n \in \{1,2,3,\ldots\}$.
(h) Give a new solution to Exercise 2.9.10(f).

[274] This is well-defined, since NSym is (isomorphic to) the free associative algebra with generators $H_1, H_2, H_3, \ldots$ (according to (5.4.1)).

6. Polynomial generators for QSym and Lyndon words

In this chapter, we shall construct an algebraically independent generating set for QSym as a $\mathbf{k}$-algebra, thus showing that QSym is a polynomial ring over $\mathbf{k}$. This has been done by Malvenuto [145, Cor. 4.19] when $\mathbf{k}$ is a field of characteristic 0, and by Hazewinkel [89] in the general case. We will begin by introducing the notion of *Lyndon words* (Section 6.1), on which both of these constructions rely; we will then (Section 6.2) elucidate the connection of Lyndon words with shuffles, and afterwards (Section 6.3) apply it to prove *Radford's theorem* stating that the shuffle algebra of a free $\mathbf{k}$-module over a commutative $\mathbb{Q}$-algebra is a polynomial algebra (Theorem 6.3.4). The shuffle algebra is not yet QSym, but Radford's theorem on the shuffle algebra serves as a natural stepping stone for the study of the more complicated algebra QSym. We will prove – in two ways – that QSym is a polynomial algebra when $\mathbb{Q}$ is a subring of $\mathbf{k}$ in Section 6.4, and then we will finally prove the general case in Section 6.5. In Section 6.6, we will explore a different aspect of the combinatorics of words: the notion of necklaces (which are in bijection with Lyndon words, as Exercise 6.1.34 will show) and the *Gessel-Reutenauer bijection*, which help us define and understand the *Gessel-Reutenauer symmetric functions*. This will rely on Section 6.1, but not on any of the other sections of Chapter 6.

Strictly speaking, this whole Chapter 6 is a digression, as it involves almost no coalgebraic or Hopf-algebraic structures, and its results will not be used in further chapters (which means it can be skipped if so desired). However, it sheds additional light on both quasisymmetric and symmetric functions, and serves as an excuse to study Lyndon words, which are a combinatorial object of independent interest (and are involved in the study of free algebras and Hopf algebras, apart from QSym – see [177] and [182][275]).

We will take a scenic route to the proof of Hazewinkel's theorem. A reader only interested in the proof proper can restrict themselves to reading only the following:

- from Section 6.1, everything up to Corollary 6.1.6, then from Definition 6.1.13 up to Proposition 6.1.18, then from Definition 6.1.25 up to Lemma 6.1.28, and finally Theorem 6.1.30. (Proposition 6.1.19 and Theorem 6.1.20 are also relevant if one wants to use a different definition of Lyndon words, as they prove the equivalence of most such definitions.)
- from Section 6.2, everything except for Exercise 6.2.25.
- from Section 6.3, Definition 6.3.1, Lemma 6.3.7, and Lemma 6.3.10.
- from Section 6.4, Definition 6.4.1, Theorem 6.4.3, then from Proposition 6.4.5 up to Definition 6.4.9, and Lemma 6.4.11.
- all of Section 6.5.

Likewise, Section 6.6 can be read immediately after Section 6.1.

6.1. Lyndon words.

Lyndon words have been independently defined by Shirshov [202], Lyndon [141], Radford [177, §2] and de Bruijn/Klarner [29] (though using different and sometimes incompatible notations). They have since been surfacing in various places in noncommutative algebra (particularly the study of free Lie algebras); expositions of their theory can be found in [139, §5], [182, §5.1] and [124, §1] (in German). We will follow our own approach to the properties of Lyndon words that we need.

Definition 6.1.1. We fix a totally ordered set $\mathfrak{A}$, which we call the *alphabet*. Throughout Section 6.1 and Section 6.2, we will understand "word" to mean a word over $\mathfrak{A}$.

We recall that a *word* is just a (finite) tuple of elements of $\mathfrak{A}$. In other words, a word is an element of the set $\bigsqcup_{n\geq 0}\mathfrak{A}^n$. We denote this set by $\mathfrak{A}^*$.

The *empty word* is the unique tuple with 0 elements. It is denoted by $\varnothing$. If $w\in\mathfrak{A}^n$ is a word and $i\in\{1,2,\ldots,n\}$, then the *i-th letter* of w means the i-th entry of the n-tuple w. This i-th letter will be denoted by w_i.

The *length* $\ell(w)$ of a word $w\in\bigsqcup_{n\geq 0}\mathfrak{A}^n$ is defined to be the $n\in\mathbb{N}$ satisfying $w\in\mathfrak{A}^n$. Thus, $w=\left(w_1,w_2,\ldots,w_{\ell(w)}\right)$ for every word w.

Given two words u and v, we say that u is *longer* than v (or, equivalently, v is *shorter* than u) if and only if $\ell(u)>\ell(v)$.

The *concatenation* of two words u and v is defined to be the word $\left(u_1,u_2,\ldots,u_{\ell(u)},v_1,v_2,\ldots,v_{\ell(v)}\right)$. This concatenation is denoted by uv or $u\cdot v$. The set $\mathfrak{A}^*$ of all words is a monoid with respect to concatenation,

[275] They also are involved in indexing basis elements of combinatorial Hopf algebras other than QSym. See Bergeron/Zabrocki [18].

with neutral element $\varnothing$. It is precisely the free monoid on generators $\mathfrak{A}$. If u is a word and $i \in \mathbb{N}$, we will understand u^i to mean the i-th power of u in this monoid (that is, the word $\underbrace{uu\cdots u}_{i \text{ times}}$).

The elements of $\mathfrak{A}$ are called *letters*, and will be identified with elements of $\mathfrak{A}^1 \subset \bigsqcup_{n\geq 0} \mathfrak{A}^n = \mathfrak{A}^*$. This identification equates every letter $u \in \mathfrak{A}$ with the one-letter word $(u) \in \mathfrak{A}^1$. Thus, every word $(u_1, u_2, \ldots, u_n) \in \mathfrak{A}^*$ equals the concatenation $u_1 u_2 \cdots u_n$ of letters, hence allowing us to use $u_1 u_2 \cdots u_n$ as a brief notation for the word $(u_1, u_2, \ldots, u_n)$.

If w is a word, then:

- a *prefix* of w means a word of the form $(w_1, w_2, \ldots, w_i)$ for some $i \in \{0, 1, \ldots, \ell(w)\}$;
- a *suffix* of w means a word of the form $(w_{i+1}, w_{i+2}, \ldots, w_{\ell(w)})$ for some $i \in \{0, 1, \ldots, \ell(w)\}$;
- a *proper suffix* of w means a word of the form $(w_{i+1}, w_{i+2}, \ldots, w_{\ell(w)})$ for some $i \in \{1, 2, \ldots, \ell(w)\}$.

In other words,

- a *prefix* of $w \in \mathfrak{A}^*$ is a word $u \in \mathfrak{A}^*$ such that there exists a $v \in \mathfrak{A}^*$ satisfying $w = uv$;
- a *suffix* of $w \in \mathfrak{A}^*$ is a word $v \in \mathfrak{A}^*$ such that there exists a $u \in \mathfrak{A}^*$ satisfying $w = uv$;
- a *proper suffix* of $w \in \mathfrak{A}^*$ is a word $v \in \mathfrak{A}^*$ such that there exists a nonempty $u \in \mathfrak{A}^*$ satisfying $w = uv$.

Clearly, any proper suffix of $w \in \mathfrak{A}^*$ is a suffix of w. Moreover, if $w \in \mathfrak{A}^*$ is any word, then a proper suffix of w is the same thing as a suffix of w distinct from w.

We define a relation $\leq$ on the set $\mathfrak{A}^*$ as follows: For two words $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$, we set $u \leq v$ to hold if and only if

> **either** there exists an $i \in \{1, 2, \ldots, \min\{\ell(u), \ell(v)\}\}$
> such that ($u_i < v_i$, and every $j \in \{1, 2, \ldots, i-1\}$ satisfies $u_j = v_j$),
> **or** the word u is a prefix of v.

This order relation (taken as the smaller-or-equal relation) makes $\mathfrak{A}^*$ into a poset (by Proposition 6.1.2(a) below), and we will always be regarding $\mathfrak{A}^*$ as endowed with this poset structure (thus, notations such as $<$, $\leq$, $>$ and $\geq$ will be referring to this poset structure). This poset is actually totally ordered (see Proposition 6.1.2(a)).

Here are some examples of words compared by the relation $\leq$:

$$113 \leq 114, \qquad 113 \leq 132, \qquad 19 \leq 195, \qquad 41 \leq 412,$$
$$41 \leq 421, \qquad 539 \leq 54, \qquad \varnothing \leq 21, \qquad \varnothing \leq \varnothing$$

(where $\mathfrak{A}$ is the alphabet $\{1 < 2 < 3 < \cdots\}$).

Notice that if u and v are two words of the same length (i.e., we have $u, v \in \mathfrak{A}^n$ for one and the same n), then $u \leq v$ holds if and only if u is lexicographically smaller-or-equal to v. In other words, the relation $\leq$ is an extension of the lexicographic order on every $\mathfrak{A}^n$ to $\mathfrak{A}^*$. This is the reason why this relation $\leq$ is usually called the *lexicographic order* on $\mathfrak{A}^*$. In particular, we will be using this name.[276] However, unlike the lexicographic order on $\mathfrak{A}^n$, it does not always respect concatenation from the right: It can happen that $u, v, w \in \mathfrak{A}^*$ satisfy $u \leq v$ but not $uw \leq vw$. (For example, $u = 1$, $v = 13$ and $w = 4$, again with $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$.) We will see in Proposition 6.1.2 that this is rather an exception than the rule and the relation $\leq$ still behaves mostly predictably with respect to concatenation.

Some basic properties of the order relation $\leq$ just defined are collected in the following proposition:

Proposition 6.1.2. (a) *The order relation $\leq$ is (the smaller-or-equal relation of) a total order on the set $\mathfrak{A}^*$.*

(b) *If $a, c, d \in \mathfrak{A}^*$ satisfy $c \leq d$, then $ac \leq ad$.*

(c) *If $a, c, d \in \mathfrak{A}^*$ satisfy $ac \leq ad$, then $c \leq d$.*

(d) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $a \leq c$, then either we have $ab \leq cd$ or the word a is a prefix of c.*

(e) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $ab \leq cd$, then either we have $a \leq c$ or the word c is a prefix of a.*

(f) *If $a, b, c, d \in \mathfrak{A}^*$ satisfy $ab \leq cd$ and $\ell(a) \leq \ell(c)$, then $a \leq c$.*

[276] The relation $\leq$ is also known as the *dictionary order*, due to the fact that it is the order in which words appear in a dictionary.

(g) *If $a, b, c \in \mathfrak{A}^*$ satisfy $a \leq b \leq ac$, then a is a prefix of b.*
(h) *If $a \in \mathfrak{A}^*$ is a prefix of $b \in \mathfrak{A}^*$, then $a \leq b$.*
(i) *If a and b are two prefixes of $c \in \mathfrak{A}^*$, then either a is a prefix of b, or b is a prefix of a.*
(j) *If $a, b, c \in \mathfrak{A}^*$ are such that $a \leq b$ and $\ell(a) \geq \ell(b)$, then $ac \leq bc$.*
(k) *If $a \in \mathfrak{A}^*$ and $b \in \mathfrak{A}^*$ are such that b is nonempty, then $a < ab$.*

Exercise 6.1.3. Prove Proposition 6.1.2.

[**Hint:** No part of Proposition 6.1.2 requires more than straightforward case analysis. However, the proof of (a) can be simplified by identifying the order relation $\leq$ on $\mathfrak{A}^*$ as a restriction of the lexicographic order on the set $\mathfrak{B}^\infty$, where $\mathfrak{B}$ is a suitable extension of the alphabet $\mathfrak{A}$. What is this extension, and how to embed $\mathfrak{A}^*$ into $\mathfrak{B}^\infty$?]

Proposition 6.1.2 provides a set of tools for working with the lexicographic order without having to refer to its definition; we shall use it extensively. Proposition 6.1.2(h) (and its equivalent form stating that $a \leq ac$ for every $a \in \mathfrak{A}^*$ and $c \in \mathfrak{A}^*$) and Proposition 6.1.2(k) will often be used without explicit mention.

Before we define Lyndon words, let us show two more facts about words which will be used later. First, when do words commute?

Proposition 6.1.4. *Let $u, v \in \mathfrak{A}^*$ satisfy $uv = vu$. Then, there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers n and m such that $u = t^n$ and $v = t^m$.*

Proof. We prove this by strong induction on $\ell(u) + \ell(v)$. We assume WLOG that $\ell(u)$ and $\ell(v)$ are positive (because otherwise, one of u and v is the empty word, and everything is trivial). It is easy to see that either u is a prefix of v, or v is a prefix of u [277]. We assume WLOG that u is a prefix of v (since our situation is symmetric). Thus, we can write v in the form $v = uw$ for some $w \in \mathfrak{A}^*$. Consider this w. Clearly, $\ell(u) + \ell(w) = \ell\left(\underbrace{uw}_{=v}\right) = \ell(v) < \ell(u) + \ell(v)$ (since $\ell(v)$ is positive). Since $v = uw$, the equality $uv = vu$ becomes $uuw = uwu$. Cancelling u from this equality, we obtain $uw = wu$. Now, we can apply Proposition 6.1.4 to w instead of v (by the induction assumption, since $\ell(u) + \ell(w) < \ell(u) + \ell(v)$), and obtain that there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers n and m such that $u = t^n$ and $w = t^m$. Consider this t and these n and m. Of course, $u = t^n$ and $v = \underbrace{u}_{=t^n}\underbrace{w}_{=t^m} = t^n t^m = t^{n+m}$. So the induction step is complete, and Proposition 6.1.4 is proven. ☐

Proposition 6.1.5. *Let $u, v, w \in \mathfrak{A}^*$ be nonempty words satisfying $uv \geq vu$, $vw \geq wv$ and $wu \geq uw$. Then, there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers n, m and p such that $u = t^n$, $v = t^m$ and $w = t^p$.*

Proof. We prove this by strong induction on $\ell(u) + \ell(v) + \ell(w)$. Clearly, $\ell(u)$, $\ell(v)$ and $\ell(w)$ are positive (since u, v and w are nonempty). We assume WLOG that $\ell(u) = \min\{\ell(u), \ell(v), \ell(w)\}$ (because there is a cyclic symmetry in our situation). Thus, $\ell(u) \leq \ell(v)$ and $\ell(u) \leq \ell(w)$. But $vu \leq uv$. Hence, Proposition 6.1.2(e) (applied to $a = v$, $b = u$, $c = u$ and $d = v$) yields that either we have $v \leq u$ or the word u is a prefix of v. But Proposition 6.1.2(f) (applied to $a = u$, $b = w$, $c = w$ and $d = u$) yields $u \leq w$ (since $uw \leq wu$ and $\ell(u) \leq \ell(w)$). Furthermore, $wv \leq vw$. Hence, Proposition 6.1.2(e) (applied to $a = w$, $b = v$, $c = v$ and $d = w$) yields that either we have $w \leq v$ or the word v is a prefix of w.

From what we have found so far, it is easy to see that u is a prefix of v [278]. In other words, there exists a $v' \in \mathfrak{A}^*$ such that $v = uv'$. Consider this v'.

If the word v' is empty, then the statement of Proposition 6.1.5 can be easily deduced from Proposition 6.1.4[279]. Thus, we assume WLOG that this is not the case. Hence, v' is nonempty.

---

[277] *Proof.* The word u is a prefix of uv. But the word v is also a prefix of uv (since $uv = vu$). Hence, Proposition 6.1.2(i) (applied to $a = u$, $b = v$ and $c = uv$) yields that either u is a prefix of v, or v is a prefix of u, qed.

[278] *Proof.* Assume the contrary. Then, u is not a prefix of v. Hence, we must have $v \leq u$ (since either we have $v \leq u$ or the word u is a prefix of v), and in fact $v < u$ (because $v = u$ would contradict to u not being a prefix of v). Thus, $v < u \leq w$. But recall that either we have $w \leq v$ or the word v is a prefix of w. Thus, v must be a prefix of w (because $v < w$ rules out $w \leq v$). In other words, there exists a $q \in \mathfrak{A}^*$ such that $w = vq$. Consider this q. We have $v < u \leq w = vq$. Thus, Proposition 6.1.2(g) (applied to $a = v$, $b = u$ and $c = q$) yields that v is a prefix of u. In light of $\ell(u) \leq \ell(v)$, this is only possible if $v = u$, but this contradicts $v < u$. This contradiction completes this proof.

[279] *Proof.* Assume that the word v' is empty. Then, $v = uv'$ becomes $v = u$. Therefore, $vw \geq wv$ becomes $uw \geq wu$. Combined with $wu \geq uw$, this yields $uw = wu$. Hence, Proposition 6.1.4 (applied to w instead of v) yields that there exist a

Using $v = uv'$, we can rewrite $uv \geq vu$ as $uuv' \geq uv'u$. That is, $uv'u \leq uuv'$, so that $v'u \leq uv'$ (by Proposition 6.1.2(c), applied to $a = u$, $c = v'u$ and $d = uv'$). That is, $uv' \geq v'u$. But $\ell(uw) = \ell(u) + \ell(w) = \ell(w) + \ell(u) = \ell(wu) \geq \ell(wu)$. Hence, Proposition 6.1.2(i) (applied to $a = uw$, $b = wu$ and $c = v'$) yields $uwv' \leq wuv'$ (since $uw \leq wu$). Now, $\underbrace{uv'}_{=v} w = vw \geq w \underbrace{v}_{=uv'} = wuv' \geq uwv'$ (since $uwv' \leq wuv'$), so that $uwv' \leq uv'w$. Hence, $wv' \leq v'w$ (by Proposition 6.1.2(c), applied to $a = u$, $c = wv'$ and $d = v'w$), so that $v'w \geq wv'$. Now, we can apply Proposition 6.1.5 to v' instead of v (by the induction hypothesis, because $\underbrace{\ell(u) + \ell(v')}_{\substack{=\ell(uv')=\ell(v) \\ (\text{since } uv'=v)}} + \ell(w) = \ell(v) + \ell(w) < \ell(u) + \ell(v) + \ell(w)$). As a result, we see that there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers n, m and p such that $u = t^n$, $v' = t^m$ and $w = t^p$. Clearly, this t and these n, m, p satisfy $v = \underbrace{u}_{=t^n} \underbrace{v'}_{=t^m} = t^n t^m = t^{n+m}$, and so the statement of Proposition 6.1.5 is satisfied. The induction step is thus complete. □

Corollary 6.1.6. *Let $u, v, w \in \mathfrak{A}^*$ be words satisfying $uv \geq vu$ and $vw \geq wv$. Assume that v is nonempty. Then, $uw \geq wu$.*

Proof. Assume the contrary. Thus, $uw < wu$, so that $wu \geq uw$.

If u or w is empty, then everything is obvious. We thus WLOG assume that u and w are nonempty. Thus, Proposition 6.1.5 shows that there exist a $t \in \mathfrak{A}^*$ and three nonnegative integers n, m and p such that $u = t^n$, $v = t^m$ and $w = t^p$. But this yields $wu = t^p t^n = t^{p+n} = t^{n+p} = \underbrace{t^n}_{=u} \underbrace{t^p}_{=w} = uw$, contradicting $uw < wu$. This contradiction finishes the proof. □

Exercise 6.1.7. Find an alternative proof of Corollary 6.1.6 which does not use Proposition 6.1.5.

The above results have a curious consequence, which we are not going to use:

Corollary 6.1.8. *We can define a preorder on the set $\mathfrak{A}^* \setminus \{\varnothing\}$ of all nonempty words by defining a nonempty word u to be greater-or-equal to a nonempty word v (with respect to this preorder) if and only if $uv \geq vu$. Two nonempty words u, v are equivalent with respect to the equivalence relation induced by this preorder if and only if there exist a $t \in \mathfrak{A}^*$ and two nonnegative integers n and m such that $u = t^n$ and $v = t^m$.*

Proof. The alleged preorder is transitive (by Corollary 6.1.6) and reflexive (obviously), and hence is really a preorder. The claim in the second sentence follows from Proposition 6.1.4. □

As another consequence of Proposition 6.1.5, we obtain a classical property of words [139, Proposition 1.3.1]:

Exercise 6.1.9. Let u and v be words and n and m be positive integers such that $u^n = v^m$. Prove that there exists a word t and positive integers i and j such that $u = t^i$ and $v = t^j$.

Here is another application of Corollary 6.1.6:

Exercise 6.1.10. Let n and m be positive integers. Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words. Prove that $uv \geq vu$ holds if and only if $u^n v^m \geq v^m u^n$ holds.

Exercise 6.1.11. Let n and m be positive integers. Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words satisfying $n\ell(u) = m\ell(v)$. Prove that $uv \geq vu$ holds if and only if $u^n \geq v^m$ holds.

We can also generalize Propositions 6.1.4 and 6.1.5:

Exercise 6.1.12. Let $u_1, u_2, \ldots, u_k$ be nonempty words such that every $i \in \{1, 2, \ldots, k\}$ satisfies $u_i u_{i+1} \geq u_{i+1} u_i$, where u_{k+1} means u_1. Show that there exist a word t and nonnegative integers $n_1, n_2, \ldots, n_k$ such that $u_1 = t^{n_1}$, $u_2 = t^{n_2}$, ..., $u_k = t^{n_k}$.

Now, we define the notion of a Lyndon word. There are several definitions in literature, some of which will be proven equivalent in Theorem 6.1.20.

$t \in \mathfrak{A}^*$ and two nonnegative integers n and m such that $u = t^n$ and $w = t^m$. Clearly, $v = u = t^n$ as well, and so the statement of Proposition 6.1.5 is true.

Definition 6.1.13. A word $w \in \mathfrak{A}^*$ is said to be *Lyndon* if it is nonempty and satisfies the following property: Every nonempty proper suffix v of w satisfies $v > w$.

For example, the word 113 is Lyndon (because its nonempty proper suffixes are 13 and 3, and these are both > 113), and the word 242427 is Lyndon (its nonempty proper suffixes are 42427, 2427, 427, 27 and 7, and again these are each > 242427). The words 2424 and 35346 are not Lyndon (the word 2424 has a nonempty proper suffix $24 \leq 2424$, and the word 35346 has a nonempty proper suffix $346 \leq 35346$). Every word of length 1 is Lyndon (since it has no nonempty proper suffixes). A word $w = (w_1, w_2)$ with two letters is Lyndon if and only if $w_1 < w_2$. A word $w = (w_1, w_2, w_3)$ of length 3 is Lyndon if and only if $w_1 < w_3$ and $w_1 \leq w_2$. A four-letter word $w = (w_1, w_2, w_3, w_4)$ is Lyndon if and only if $w_1 < w_4$, $w_1 \leq w_3$, $w_1 \leq w_2$ and (if $w_1 = w_3$ then $w_2 < w_4$). (These rules only get more complicated as the words grow longer.)

We will show several properties of Lyndon words now. We begin with trivialities which will make some arguments a bit shorter:

Proposition 6.1.14. *Let w be a Lyndon word. Let u and v be words such that $w = uv$.*

(a) *If v is nonempty, then $v \geq w$.*
(b) *If v is nonempty, then $v > u$.*
(c) *If u and v are nonempty, then $vu > uv$.*
(d) *We have $vu \geq uv$.*

Proof. (a) Assume that v is nonempty. Clearly, v is a suffix of w (since $w = uv$). If v is a proper suffix of w, then the definition of a Lyndon word yields that $v > w$ (since w is a Lyndon word); otherwise, v must be w itself. In either case, we have $v \geq w$. Hence, Proposition 6.1.14(a) is proven.

(b) Assume that v is nonempty. From Proposition 6.1.14(a), we obtain $v \geq w = uv > u$ (since v is nonempty). This proves Proposition 6.1.14(b).

(c) Assume that u and v are nonempty. Since u is nonempty, we have $vu > v \geq w$ (by Proposition 6.1.14(a)). Since $w = uv$, this becomes $vu > uv$. This proves Proposition 6.1.14(c).

(d) We need to prove that $vu \geq uv$. If either u or v is empty, vu and uv are obviously equal, and thus $vu \geq uv$ is true in this case. Hence, we can WLOG assume that u and v are nonempty. Assume this. Then, $vu \geq uv$ follows from Proposition 6.1.14(c). This proves Proposition 6.1.14(d). ☐

Corollary 6.1.15. *Let w be a Lyndon word. Let v be a nonempty suffix of w. Then, $v \geq w$.*

Proof. Since v is a nonempty suffix of w, there exists $u \in \mathfrak{A}^*$ such that $w = uv$. Thus, $v \geq w$ follows from Proposition 6.1.14(a). ☐

Our next proposition is [93, Lemma 6.5.4]; its part (a) is also [182, (5.1.2)]:

Proposition 6.1.16. *Let u and v be two Lyndon words such that $u < v$. Then:*

(a) *The word uv is Lyndon.*
(b) *We have $uv < v$.*

Proof. (b) The word u is Lyndon and thus nonempty. Hence, $uv \neq v$ [280]. If $uv \leq v\varnothing$, then Proposition 6.1.16(b) easily follows[281]. Hence, for the rest of this proof, we can WLOG assume that we don't have $uv \leq v\varnothing$. Assume this.

We have $u < v$. Hence, Proposition 6.1.2(d) (applied to $a = u$, $b = v$, $c = v$ and $d = \varnothing$) yields that either we have $uv \leq v\varnothing$ or the word u is a prefix of v. Since we don't have $uv \leq v\varnothing$, we thus see that the word u is a prefix of v. In other words, there exists a $t \in \mathfrak{A}^*$ satisfying $v = ut$. Consider this t. Then, t is nonempty (else we would have $v = u\underbrace{t}_{=\varnothing} = u$ in contradiction to $u < v$).

Now, $v = ut$. Hence, t is a proper suffix of v (proper because u is nonempty). Thus, t is a nonempty proper suffix of v. Since every nonempty proper suffix of v is $> v$ (because v is Lyndon), this shows that

[280] *Proof.* Assume the contrary. Then, $uv = v$. Thus, $uv = v = \varnothing v$. Cancelling v from this equation, we obtain $u = \varnothing$. That is, u is empty. This contradicts the fact that u is nonempty. This contradiction proves that our assumption was wrong, qed.

[281] *Proof.* Assume that $uv \leq v\varnothing$. Thus, $uv \leq v\varnothing = v$. Since $uv \neq v$, this becomes $uv < v$, so that Proposition 6.1.16(b) is proven.

$t > v$. Hence, $v \leq t$. Thus, Proposition 6.1.2(b) (applied to $a = u$, $c = v$ and $d = t$) yields $uv \leq ut = v$. Combined with $uv \neq v$, this yields $uv < v$. Hence, Proposition 6.1.16(b) is proven.

(a) The word v is nonempty (since it is Lyndon). Hence, uv is nonempty. It thus remains to check that every nonempty proper suffix p of uv satisfies $p > uv$.

So let p be a nonempty proper suffix of uv. We must show that $p > uv$. Since p is a nonempty proper suffix of uv, we must be in one of the following two cases (depending on whether this suffix begins before the suffix v of uv begins or afterwards):

Case 1: The word p is a nonempty suffix of v. (Note that $p = v$ is allowed.)

Case 2: The word p has the form qv where q is a nonempty proper suffix of u.

Let us first handle Case 1. In this case, p is a nonempty suffix of v. Since v is Lyndon, this yields that $p \geq v$ (by Corollary 6.1.15, applied to v and p instead of w and v). But Proposition 6.1.16(b) yields $uv < v$, thus $v > uv$. Hence, $p \geq v > uv$. We thus have proven $p > uv$ in Case 1.

Let us now consider Case 2. In this case, p has the form qv where q is a nonempty proper suffix of u. Consider this q. Clearly, $q > u$ (since u is Lyndon and since q is a nonempty proper suffix of u), so that $u \leq q$. Thus, Proposition 6.1.2(d) (applied to $a = u$, $b = v$, $c = q$ and $d = v$) yields that either we have $uv \leq qv$ or the word u is a prefix of q. Since u being a prefix of q is impossible (in fact, q is a proper suffix of u, thus shorter than u), we thus must have $uv \leq qv$. Since $uv \neq qv$ (because otherwise we would have $uv = qv$, thus $u = q$ (because we can cancel v from the equality $uv = qv$), contradicting $q > u$), this can be strengthened to $uv < qv = p$. Thus, $p > uv$ is proven in Case 2 as well.

Now that $p > uv$ is shown to hold in both cases, we conclude that $p > uv$ always holds.

Now, let us forget that we fixed p. We have thus shown that every nonempty proper suffix p of uv satisfies $p > uv$. Since uv is nonempty, this yields that uv is Lyndon (by the definition of a Lyndon word). Thus, the proof of Proposition 6.1.16(a) is complete. □

Proposition 6.1.16(b), combined with Corollary 6.1.6, leads to a technical result which we will find good use for later:

Corollary 6.1.17. *Let u and v be two Lyndon words such that $u < v$. Let z be a word such that $zv \geq vz$ and $uz \geq zu$. Then, z is the empty word.*

Proof. Assume the contrary. Then, z is nonempty. Thus, Corollary 6.1.6 (applied to z and v instead of v and w) yields $uv \geq vu$. But Proposition 6.1.16(b) yields $uv < v \leq vu$, contradicting $uv \geq vu$. This contradiction completes our proof. □

We notice that the preorder of Corollary 6.1.8 becomes particularly simple on Lyndon words:

Proposition 6.1.18. *Let u and v be two Lyndon words. Then, $u \geq v$ if and only if $uv \geq vu$.*

Proof. We distinguish between three cases:

Case 1: We have $u < v$.

Case 2: We have $u = v$.

Case 3: We have $u > v$.

Let us consider Case 1. In this case, we have $u < v$. Thus,

$$\begin{aligned} uv &< v && \text{(by Proposition 6.1.16(b))} \\ &\leq vu. \end{aligned}$$

Hence, we have neither $u \geq v$ nor $uv \geq vu$ (because we have $u < v$ and $uv < vu$). Thus, Proposition 6.1.18 is proven in Case 1.

In Case 2, we have $u = v$. Therefore, in Case 2, both inequalities $u \geq v$ and $uv \geq vu$ hold (and actually are equalities). Thus, Proposition 6.1.18 is proven in Case 2 as well.

Let us finally consider Case 3. In this case, we have $u > v$. In other words, $v < u$. Thus,

$$\begin{aligned} vu &< u && \text{(by Proposition 6.1.16(b), applied to } v \text{ and } u \text{ instead of } u \text{ and } v) \\ &\leq uv. \end{aligned}$$

Hence, we have both $u \geq v$ and $uv \geq vu$ (because we have $v < u$ and $vu < uv$). Thus, Proposition 6.1.18 is proven in Case 3.

Proposition 6.1.18 is now proven in all three possible cases. □

Proposition 6.1.19. *Let w be a nonempty word. Let v be the (lexicographically) smallest nonempty suffix of w. Then:*

(a) *The word v is a Lyndon word.*

(b) *Assume that w is not a Lyndon word. Then there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$, $u \geq v$ and $uv \geq vu$.*

Proof. (a) Every nonempty proper suffix of v is $\geq v$ (since every nonempty proper suffix of v is a nonempty suffix of w, but v is the smallest such suffix) and therefore $> v$ (since a proper suffix of v cannot be $= v$). Combined with the fact that v is nonempty, this yields that v is Lyndon. Proposition 6.1.19(a) is proven.

(b) Assume that w is not a Lyndon word. Then, $w \neq v$ (since v is Lyndon (by Proposition 6.1.19(a)) while w is not). Now, v is a suffix of w. Thus, there exists an $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this u. Clearly, u is nonempty (since $uv = w \neq v$). Assume (for the sake of contradiction) that $u < v$. Let v' be the (lexicographically) smallest nonempty suffix of u. Then, v' is a Lyndon word (by Proposition 6.1.19(a), applied to u and v' instead of w and v) and satisfies $v' \leq u$ (since u is a nonempty suffix of u, whereas v' is the smallest such suffix). Thus, v' and v are Lyndon words such that $v' \leq u < v$. Proposition 6.1.16(a) (applied to v' instead of u) now yields that the word $v'v$ is Lyndon. Hence, every nonempty proper suffix of $v'v$ is $> v'v$. Since v is a nonempty proper suffix of $v'v$, this yields that $v > v'v$.

But v' is a nonempty suffix of u, so that $v'v$ is a nonempty suffix of $uv = w$. Since v is the smallest such suffix, this yields that $v'v \geq v$. This contradicts $v > v'v$. Our assumption (that $u < v$) therefore falls. We conclude that $u \geq v$.

It remains to prove that $uv \geq vu$. Assume the contrary. Then, $uv < vu$. Thus, there exists at least one suffix t of u such that $tv < vt$ (namely, $t = u$). Let p be the **minimum-length** such suffix. Then, $pv < vp$. Thus, p is nonempty.

Since p is a suffix of u, it is clear that pv is a suffix of $uv = w$. So we know that pv is a nonempty suffix of w. Since v is the smallest such suffix, this yields that $v \leq pv < vp$. Thus, Proposition 6.1.2(g) (applied to $a = v$, $b = pv$ and $c = p$) yields that v is a prefix of pv. In other words, there exists a $q \in \mathfrak{A}^*$ such that $pv = vq$. Consider this q. This q is nonempty (because otherwise we would have $pv = v\underbrace{q}_{=\varnothing} = v$, contradicting the fact that p is nonempty). From $vq = pv < vp$, we obtain $q \leq p$ (by Proposition 6.1.2(c), applied to $a = v$, $c = q$ and $d = p$).

We know that q is a suffix of pv (since $vq = pv$), whereas pv is a suffix of w. Thus, q is a suffix of w. So q is a nonempty suffix of w. Since v is the smallest such suffix, this yields that $v \leq q$. We now have $v \leq q \leq p \leq pv < vp$. Hence, v is a prefix of p (by Proposition 6.1.2(g), applied to $a = v$, $b = p$ and $c = p$). In other words, there exists an $r \in \mathfrak{A}^*$ such that $p = vr$. Consider this r. Clearly, r is a suffix of p, while p is a suffix of u; therefore, r is a suffix of u. Also, $pv < vp$ rewrites as $vrv < vvr$ (because $p = vr$). Thus, Proposition 6.1.2(c) (applied to $a = v$, $c = rv$ and $d = vr$) yields $rv \leq vr$. Since $rv \neq vr$ (because otherwise, we would have $rv = vr$, thus $v\underbrace{rv}_{=vr} = vvr$, contradicting $vrv < vvr$), this becomes $rv < vr$.

Now, r is a suffix of u such that $rv < vr$. Since p is the minimum-length such suffix, this yields $\ell(r) \geq \ell(p)$. But this contradicts the fact that $\ell\left(\underbrace{p}_{=vr}\right) = \ell(vr) = \underbrace{\ell(v)}_{>0} + \ell(r) > \ell(r)$. This contradiction proves our assumption wrong; thus, we have shown that $uv \geq vu$. Proposition 6.1.19(b) is proven. ☐

Theorem 6.1.20. *Let w be a nonempty word. The following four assertions are equivalent:*

- *Assertion $\mathcal{A}$: The word w is Lyndon.*
- *Assertion $\mathcal{B}$: Any nonempty words u and v satisfying $w = uv$ satisfy $v > w$.*
- *Assertion $\mathcal{C}$: Any nonempty words u and v satisfying $w = uv$ satisfy $v > u$.*
- *Assertion $\mathcal{D}$: Any nonempty words u and v satisfying $w = uv$ satisfy $vu > uv$.*

Proof. Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{B}$: If Assertion $\mathcal{A}$ holds, then Assertion $\mathcal{B}$ clearly holds (in fact, whenever u and v are nonempty words satisfying $w = uv$, then v is a nonempty proper suffix of w, and therefore $> w$ by the definition of a Lyndon word).

Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{C}$: This implication follows from Proposition 6.1.14(b).

Proof of the implication $\mathcal{A} \Longrightarrow \mathcal{D}$: This implication follows from Proposition 6.1.14(c).

Proof of the implication $\mathcal{B} \Longrightarrow \mathcal{A}$: Assume that Assertion $\mathcal{B}$ holds. If v is a nonempty proper suffix of w, then there exists an $u \in \mathfrak{A}^*$ satisfying $w = uv$. This u is nonempty because v is a proper suffix, and thus Assertion $\mathcal{B}$ yields $v > w$. Hence, every nonempty proper suffix v of w satisfies $v > w$. By the definition of a Lyndon word, this yields that w is Lyndon, so that Assertion $\mathcal{A}$ holds.

Proof of the implication $\mathcal{C} \Longrightarrow \mathcal{A}$: Assume that Assertion $\mathcal{C}$ holds. If w was not Lyndon, then Proposition 6.1.19(b) would yield nonempty words u and v such that $w = uv$ and $u \geq v$; this would contradict Assertion $\mathcal{C}$. Thus, w is Lyndon, and Assertion $\mathcal{A}$ holds.

Proof of the implication $\mathcal{D} \Longrightarrow \mathcal{A}$: Assume that Assertion $\mathcal{D}$ holds. If w was not Lyndon, then Proposition 6.1.19(b) would yield nonempty words u and v such that $w = uv$ and $uv \geq vu$; this would contradict Assertion $\mathcal{D}$. Thus, w is Lyndon, and Assertion $\mathcal{A}$ holds.

Now we have proven enough implications to conclude the equivalence of all four assertions. □

Theorem 6.1.20 connects our definition of Lyndon words with some of the definitions appearing in literature. For example, Lothaire [139, §5.1], Shirshov [202] and de Bruijn/Klarner [29, §4] define Lyndon words using Assertion $\mathcal{D}$ (note, however, that Shirshov takes $<$ instead of $>$ and calls Lyndon words "regular words"; also, de Bruijn/Klarner call Lyndon words "normal words"). Chen-Fox-Lyndon [38, §1], Reutenauer [182] and Radford [177] use our definition (but Chen-Fox-Lyndon call the Lyndon words "standard sequences", and Radford calls them "primes" and uses $<$ instead of $>$).

Theorem 6.1.20 appears (with different notations) in Zhou-Lu [229, Proposition 1.4]. The equivalence $\mathcal{D} \Longleftrightarrow \mathcal{A}$ of our Theorem 6.1.20 is equivalent to [139, Proposition 5.12] and to [38, $\mathfrak{A}'' = \mathfrak{A}'''$].

The following exercise provides a different (laborious) approach to Theorem 6.1.20:

Exercise 6.1.21. (a) Prove that if $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ are two words satisfying $uv < vu$, then there exists a nonempty suffix s of u satisfying $sv < v$.

(b) Give a new proof of Theorem 6.1.20 (avoiding the use of Proposition 6.1.19).

[**Hint:** For (a), perform strong induction on $\ell(u) + \ell(v)$, assume the contrary, and distinguish between the case when $u \leq v$ and the case when v is a prefix of u. For (b), use part (a) in proving the implication $\mathcal{D} \Longrightarrow \mathcal{B}$, and factor v as $v = u^m v'$ with m maximal in the proof of the implication $\mathcal{C} \Longrightarrow \mathcal{B}$.]

The following two exercises are taken from [91][282].

Exercise 6.1.22. Let w be a nonempty word. Prove that w is Lyndon if and only if every nonempty word t and every positive integer n satisfy (if $w \leq t^n$, then $w \leq t$).

Exercise 6.1.23. Let w_1, w_2, …, w_n be n Lyndon words, where n is a positive integer. Assume that $w_1 \leq w_2 \leq \cdots \leq w_n$ and $w_1 < w_n$. Show that $w_1 w_2 \cdots w_n$ is a Lyndon word.

The following exercise is a generalization (albeit not in an obvious way) of Exercise 6.1.23:

Exercise 6.1.24. Let w_1, w_2, …, w_n be n Lyndon words, where n is a positive integer. Assume that $w_i w_{i+1} \cdots w_n \geq w_1 w_2 \cdots w_n$ for every $i \in \{1, 2, \ldots, n\}$. Show that $w_1 w_2 \cdots w_n$ is a Lyndon word.

We are now ready to meet one of the most important features of Lyndon words: a bijection between all words and multisets of Lyndon words[283]; it is clear that such a bijection is vital for constructing polynomial generating sets of commutative algebras with bases indexed by words, such as QSym or shuffle algebras. This bijection is given by the *Chen-Fox-Lyndon factorization*:

Definition 6.1.25. Let w be a word. A *Chen-Fox-Lyndon factorization* (in short, *CFL factorization*) of w means a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$ and $a_1 \geq a_2 \geq \cdots \geq a_k$.

Example 6.1.26. The tuple $(23, 2, 14, 13323, 13, 12, 12, 1)$ is a CFL factorization of the word 23214133231312121 over the alphabet $\{1, 2, 3, \ldots\}$ (ordered by $1 < 2 < 3 < \cdots$), since 23, 2, 14, 13323, 13, 12, 12 and 1 are Lyndon words satisfying $23214133231312121 = 23 \cdot 2 \cdot 14 \cdot 13323 \cdot 13 \cdot 12 \cdot 12 \cdot 1$ and $23 \geq 2 \geq 14 \geq 13323 \geq 13 \geq 12 \geq 12 \geq 1$.

The bijection is given by the following *Chen-Fox-Lyndon theorem* ([93, Theorem 6.5.5], [139, Thm. 5.1.5], [177, part of Thm. 2.1.4]):

[282] Exercise 6.1.22 is more or less [91, Lemma 4.3] with a converse added; Exercise 6.1.23 is [91, Lemma 4.2].

[283] And it is not even the only such bijection: we will see another in Subsection 6.6.1.

Theorem 6.1.27. *Let w be a word. Then, there exists a unique CFL factorization of w.*

Before we prove this, we need to state and prove a lemma (which is [139, Proposition 5.1.6]):

Lemma 6.1.28. *Let $(a_1, a_2, \ldots, a_k)$ be a CFL factorization of a nonempty word w. Let p be a nonempty suffix of w. Then, $p \geq a_k$.*

Proof. We will prove Lemma 6.1.28 by induction over the (obviously) positive integer k.

Induction base: Assume that $k = 1$. Thus, $(a_1, a_2, \ldots, a_k) = (a_1)$ is a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$. We have $w = a_1 a_2 \cdots a_k = a_1$ (since $k = 1$), so that w is a Lyndon word (since a_1 is a Lyndon word). Thus, Corollary 6.1.15 (applied to $v = p$) yields $p \geq w = a_1 = a_k$ (since $1 = k$). Thus, Lemma 6.1.28 is proven in the case $k = 1$. The induction base is complete.

Induction step: Let K be a positive integer. Assume (as the induction hypothesis) that Lemma 6.1.28 is proven for $k = K$. We now need to show that Lemma 6.1.28 holds for $k = K + 1$.

So let $(a_1, a_2, \ldots, a_{K+1})$ be a CFL factorization of a nonempty word w. Let p be a nonempty suffix of w. We need to prove that $p \geq a_{K+1}$.

By the definition of a CFL factorization, $(a_1, a_2, \ldots, a_{K+1})$ is a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_{K+1}$ and $a_1 \geq a_2 \geq \cdots \geq a_{K+1}$. Let $w' = a_2 a_3 \cdots a_{K+1}$; then, $w = a_1 a_2 \cdots a_{K+1} = a_1 \underbrace{(a_2 a_3 \cdots a_{K+1})}_{=w'} = a_1 w'$. Hence, every nonempty suffix of w is either a nonempty suffix of w', or has the form qw' for a nonempty suffix q of a_1. Since p is a nonempty suffix of w, we thus must be in one of the following two cases:

Case 1: The word p is a nonempty suffix of w'.

Case 2: The word p has the form qw' for a nonempty suffix q of a_1.

Let us first consider Case 1. In this case, p is a nonempty suffix of w'. The K-tuple $(a_2, a_3, \ldots, a_{K+1})$ of Lyndon words satisfies $w' = a_2 a_3 \cdots a_{K+1}$ and $a_2 \geq a_3 \geq \cdots \geq a_{K+1}$; therefore, $(a_2, a_3, \ldots, a_{K+1})$ is a CFL factorization of w'. We can thus apply Lemma 6.1.28 to K, w' and $(a_2, a_3, \ldots, a_{K+1})$ instead of k, w and $(a_1, a_2, \ldots, a_k)$ (because we assumed that Lemma 6.1.28 is proven for $k = K$). As a result, we obtain that $p \geq a_{K+1}$. Thus, $p \geq a_{K+1}$ is proven in Case 1.

Let us now consider Case 2. In this case, p has the form qw' for a nonempty suffix q of a_1. Consider this q. Since a_1 is a Lyndon word, we have $q \geq a_1$ (by Corollary 6.1.15, applied to a_1 and q instead of w and v). Thus, $q \geq a_1 \geq a_2 \geq \cdots \geq a_{K+1}$, so that $p = qw' \geq q \geq a_{K+1}$. Thus, $p \geq a_{K+1}$ is proven in Case 2.

We have now proven $p \geq a_{K+1}$ in all cases. This proves that Lemma 6.1.28 holds for $k = K + 1$. The induction step is thus finished, and with it the proof of Lemma 6.1.28. ☐

Proof of Theorem 6.1.27. Let us first prove that there exists a CFL factorization of w.

Indeed, there clearly exists a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words satisfying $w = a_1 a_2 \cdots a_k$ [284]. Fix such a tuple with **minimum** k. We claim that $a_1 \geq a_2 \geq \cdots \geq a_k$.

Indeed, if some $i \in \{1, 2, \ldots, k-1\}$ would satisfy $a_i < a_{i+1}$, then the word $a_i a_{i+1}$ would be Lyndon (by Proposition 6.1.16(a), applied to $u = a_i$ and $v = a_{i+1}$), whence $(a_1, a_2, \ldots, a_{i-1}, a_i a_{i+1}, a_{i+2}, a_{i+3}, \ldots, a_k)$ would also be a tuple of Lyndon words satisfying $w = a_1 a_2 \cdots a_{i-1} (a_i a_{i+1}) a_{i+2} a_{i+3} \cdots a_k$ but having length $k - 1 < k$, contradicting the fact that k is the minimum length of such a tuple. Hence, no $i \in \{1, 2, \ldots, k-1\}$ can satisfy $a_i < a_{i+1}$. In other words, every $i \in \{1, 2, \ldots, k-1\}$ satisfies $a_i \geq a_{i+1}$. In other words, $a_1 \geq a_2 \geq \cdots \geq a_k$. Thus, $(a_1, a_2, \ldots, a_k)$ is a CFL factorization of w, so we have shown that such a CFL factorization exists.

It remains to show that there exists at most one CFL factorization of w. We shall prove this by induction over $\ell(w)$. Thus, we fix a word w and assume that

(6.1.1) for every word v with $\ell(v) < \ell(w)$, there exists at most one CFL factorization of v.

We now have to prove that there exists at most one CFL factorization of w.

Indeed, let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_m)$ be two CFL factorizations of w. We need to prove that $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_m)$. If w is empty, then this is obvious, so we WLOG assume that it is not; thus, $k > 0$ and $m > 0$.

Since $(b_1, b_2, \ldots, b_m)$ is a CFL factorization of w, we have $w = b_1 b_2 \cdots b_m$, and thus b_m is a nonempty suffix of w. Thus, Lemma 6.1.28 (applied to $p = b_m$) yields $b_m \geq a_k$. The same argument (but with the

[284] For instance, the tuple $(w_1, w_2, \ldots, w_{\ell(w)})$ of one-letter words is a valid example (recall that one-letter words are always Lyndon).

roles of $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_m)$ switched) shows that $a_k \geq b_m$. Combined with $b_m \geq a_k$, this yields $a_k = b_m$. Now let $v = a_1 a_2 \cdots a_{k-1}$. Then, $(a_1, a_2, \ldots, a_{k-1})$ is a CFL factorization of v (since $a_1 \geq a_2 \geq \cdots \geq a_{k-1}$).

Since $(a_1, a_2, \ldots, a_k)$ is a CFL factorization of w, we have $w = a_1 a_2 \cdots a_k = \underbrace{a_1 a_2 \cdots a_{k-1}}_{=v} \underbrace{a_k}_{=b_m} = v b_m$, so that

$$v b_m = w = b_1 b_2 \cdots b_m = b_1 b_2 \cdots b_{m-1} b_m.$$

Cancelling b_m yields $v = b_1 b_2 \cdots b_{m-1}$. Thus, $(b_1, b_2, \ldots, b_{m-1})$ is a CFL factorization of v (since $b_1 \geq b_2 \geq \cdots \geq b_{m-1}$). Since $\ell(v) < \ell(w)$ (because $v = a_1 a_2 \cdots a_{k-1}$ is shorter than $w = a_1 a_2 \cdots a_k$), we can apply (6.1.1) to obtain that there exists at most one CFL factorization of v. But we already know two such CFL factorizations: $(a_1, a_2, \ldots, a_{k-1})$ and $(b_1, b_2, \ldots, b_{m-1})$. Thus, $(a_1, a_2, \ldots, a_{k-1}) = (b_1, b_2, \ldots, b_{m-1})$, which, combined with $a_k = b_m$, leads to $(a_1, a_2, \ldots, a_k) = (b_1, b_2, \ldots, b_m)$. This is exactly what we needed to prove. So we have shown (by induction) that there exists at most one CFL factorization of w. This completes the proof of Theorem 6.1.27. □

The CFL factorization allows us to count all Lyndon words of a given length if $\mathfrak{A}$ is finite:

Exercise 6.1.29. Assume that the alphabet $\mathfrak{A}$ is finite. Let $q = |\mathfrak{A}|$. Let μ be the number-theoretic Möbius function (defined as in Exercise 2.9.6). Show that the number of Lyndon words of length n equals $\frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$ for every positive integer n (where "$\sum_{d|n}$" means a sum over all positive divisors of n). [285]

Exercise 6.1.29 is a well-known result and appears, e.g., in [38, Theorem 1.5] or in [139, Section 5.1].

We will now study another kind of factorization: not of an arbitrary word into Lyndon words, but of a Lyndon word into two smaller Lyndon words. This factorization is called *standard factorization* ([139, §5.1]) or *canonical factorization* ([93, Lemma 6.5.33]); we only introduce it from the viewpoint we are interested in, namely its providing a way to do induction over Lyndon words[286]. Here is what we need to know:

Theorem 6.1.30. *Let w be a Lyndon word of length > 1. Let v be the (lexicographically) smallest nonempty* ***proper*** *suffix of w. Since v is a proper suffix of w, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this u. Then:*

(a) *The words u and v are Lyndon.*
(b) *We have $u < w < v$.*

Proof. Every nonempty proper suffix of v is $\geq v$ (since every nonempty proper suffix of v is a nonempty proper suffix of w, but v is the smallest such suffix) and therefore $> v$ (since a proper suffix of v cannot be $= v$). Combined with the fact that v is nonempty, this yields that v is Lyndon.

Since w is Lyndon, we know that every nonempty proper suffix of w is $> w$. Applied to the nonempty proper suffix v of w, this yields that $v > w$. Hence, $w < v$. Since v is nonempty, we have $u < uv = w < v$. This proves Theorem 6.1.30(b).

Let p be a nonempty proper suffix of u. Then, pv is a nonempty proper suffix of $uv = w$. Thus, $pv > w$ (since every nonempty proper suffix of w is $> w$). Thus, $pv > w = uv$, so that $uv < pv$. Thus, Proposition 6.1.2(e) (applied to $a = u$, $b = v$, $c = p$ and $d = v$) yields that either we have $u \leq p$ or the word p is a prefix of u.

Let us assume (for the sake of contradiction) that $p \leq u$. Then, $p < u$ (because p is a proper suffix of u, and therefore $p \neq u$). Hence, we cannot have $u \leq p$. Thus, the word p is a prefix of u (since either we have $u \leq p$ or the word p is a prefix of u). In other words, there exists a $q \in \mathfrak{A}^*$ such that $u = pq$. Consider this q. We have $w = \underbrace{u}_{=pq} v = pqv = p(qv)$, and thus qv is a proper suffix of w (proper because p is nonempty). Moreover, qv is nonempty (since v is nonempty). Hence, qv is a nonempty proper suffix of w. Since v is the smallest such suffix, this entails that $v \leq qv$. Proposition 6.1.2(b) (applied to $a = p$, $c = v$ and $d = qv$) thus yields $pv \leq pqv$. Hence, $pv \leq pqv = w$, which contradicts $pv > w$. This contradiction shows that our assumption (that $p \leq u$) was false. We thus have $p > u$.

[285] In particular, $\frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}$ is an integer.

[286] e.g., allowing to solve Exercise 6.1.24 in a simpler way

We now have shown that $p > u$ whenever p is a nonempty proper suffix of u. Combined with the fact that u is nonempty, this shows that u is a Lyndon word. This completes the proof of Theorem 6.1.30(a). $\square$

Another approach to the standard factorization is given in the following exercise:

Exercise 6.1.31. Let w be a Lyndon word of length > 1. Let v be the longest proper suffix of w such that v is Lyndon[287]. Since v is a proper suffix of w, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this u. Prove that:

(a) The words u and v are Lyndon.
(b) We have $u < w < v$.
(c) The words u and v are precisely the words u and v constructed in Theorem 6.1.30.

Notice that a well-known recursive characterization of Lyndon words [38, $\mathfrak{A}' = \mathfrak{A}''$] can be easily derived from Theorem 6.1.30 and Proposition 6.1.16(a). We will not dwell on it.

The following exercise surveys some variations on the characterizations of Lyndon words[288]:

Exercise 6.1.32. Let w be a nonempty word. Consider the following nine assertions:

- *Assertion $\mathcal{A}'$:* The word w is a power of a Lyndon word.
- *Assertion $\mathcal{B}'$:* If u and v are nonempty words satisfying $w = uv$, then either we have $v \geq w$ or the word v is a prefix of w.
- *Assertion $\mathcal{C}'$:* If u and v are nonempty words satisfying $w = uv$, then either we have $v \geq u$ or the word v is a prefix of u.
- *Assertion $\mathcal{D}'$:* If u and v are nonempty words satisfying $w = uv$, then we have $vu \geq uv$.
- *Assertion $\mathcal{E}'$:* If u and v are nonempty words satisfying $w = uv$, then either we have $v \geq u$ or the word v is a prefix of w.
- *Assertion $\mathcal{F}'$:* The word w is a prefix of a Lyndon word in $\mathfrak{A}^*$.
- *Assertion $\mathcal{F}''$:* Let m be an object not in the alphabet $\mathfrak{A}$. Let us equip the set $\mathfrak{A} \cup \{m\}$ with a total order which extends the total order on the alphabet $\mathfrak{A}$ and which satisfies ($a < m$ for every $a \in \mathfrak{A}$). Then, the word $wm \in (\mathfrak{A} \cup \{m\})^*$ (the concatenation of the word w with the one-letter word m) is a Lyndon word.
- *Assertion $\mathcal{G}'$:* There exists a Lyndon word $t \in \mathfrak{A}^*$, a positive integer ℓ and a prefix p of t (possibly empty) such that $w = t^\ell p$.
- *Assertion $\mathcal{H}'$:* There exists a Lyndon word $t \in \mathfrak{A}^*$, a nonnegative integer ℓ and a prefix p of t (possibly empty) such that $w = t^\ell p$.

(a) Prove the equivalence $\mathcal{A}' \iff \mathcal{D}'$.
(b) Prove the equivalence $\mathcal{B}' \iff \mathcal{C}' \iff \mathcal{E}' \iff \mathcal{F}'' \iff \mathcal{G}' \iff \mathcal{H}'$.
(c) Prove the implication $\mathcal{F}' \Longrightarrow \mathcal{B}'$.
(d) Prove the implication $\mathcal{D}' \Longrightarrow \mathcal{B}'$. (The implication $\mathcal{B}' \Longrightarrow \mathcal{D}'$ is false, as witnessed by the word 11211.)
(e) Prove that if there exists a letter $\mu \in \mathfrak{A}$ such that ($\mu > a$ for every letter a of w), then the equivalence $\mathcal{F}' \iff \mathcal{F}''$ holds.
(f) Prove that if there exists a letter $\mu \in \mathfrak{A}$ such that ($\mu > a$ for some letter a of w), then the equivalence $\mathcal{F}' \iff \mathcal{F}''$ holds.

The next exercise (based on work of Hazewinkel [92]) extends some of the above properties of Lyndon words (and words in general) to a more general setting, in which the alphabet $\mathfrak{A}$ is no longer required to be totally ordered, but only needs to be a poset:

Exercise 6.1.33. In this exercise, we shall loosen the requirement that the alphabet $\mathfrak{A}$ be a totally ordered set: Instead, we will only require $\mathfrak{A}$ to be a poset. The resulting more general setting will be called the *partial-order setting*, to distinguish it from the *total-order setting* in which $\mathfrak{A}$ is required to be a totally ordered set. All results in Chapter 6 so far address the total-order setting. In this exercise, we will generalize some of them to the partial-order setting.

[287] This is well-defined, because there exists at least one proper suffix v of w such that v is Lyndon. (Indeed, the last letter of w forms such a suffix, because it is a proper suffix of w (since w has length > 1) and is Lyndon (since it is a one-letter word, and since every one-letter word is Lyndon).)

[288] Compare this with [112, §7.2.11, Theorem Q].

All notions that we have defined in the total-order setting (the notion of a word, the relation $\leq$, the notion of a Lyndon word, etc.) are defined in precisely the same way in the partial-order setting. However, the poset $\mathfrak{A}^*$ is no longer totally ordered in the partial-order setting.

(a) Prove that Proposition 6.1.2 holds in the partial-order setting, as long as one replaces "a total order" by "a partial order" in part (a) of this Proposition.
(b) Prove (in the partial-order setting) that if $a, b, c, d \in \mathfrak{A}^*$ are four words such that the words ab and cd are comparable (with respect to the partial order $\leq$), then the words a and c are comparable.
(c) Prove that Proposition 6.1.4, Proposition 6.1.5, Corollary 6.1.6, Corollary 6.1.8, Exercise 6.1.9, Exercise 6.1.10, Exercise 6.1.11, Exercise 6.1.12, Proposition 6.1.14, Corollary 6.1.15, Proposition 6.1.16, Corollary 6.1.17, Proposition 6.1.18, Theorem 6.1.20, Exercise 6.1.21(a), Exercise 6.1.23, Exercise 6.1.24, Exercise 6.1.31(a) and Exercise 6.1.31(b) still hold in the partial-order setting.
(d) Find a counterexample to Exercise 6.1.22 in the partial-order setting.
(e) Salvage Exercise 6.1.22 in the partial-order setting (i.e., find a statement which is easily equivalent to this exercise in the total-order setting, yet true in the partial-order setting).
(f) In the partial-order setting, a *Hazewinkel-CFL factorization* of a word w will mean a tuple $(a_1, a_2, \ldots, a_k)$ of Lyndon words such that $w = a_1 a_2 \cdots a_k$ and such that no $i \in \{1, 2, \ldots, k-1\}$ satisfies $a_i < a_{i+1}$. Prove that every word w has a unique Hazewinkel-CFL factorization (in the partial-order setting).[289]
(g) Prove that Exercise 6.1.32 still holds in the partial-order setting.

The reader is invited to try extending other results to the partial-order setting (it seems that no research has been done on this except for Hazewinkel's [92]). We shall now, however, return to the total-order setting (which has the most known applications).

Another extension of the notion of Lyndon words has been introduced in 2018 by Dolce, Restivo and Reutenauer [53]; it is based on a generalized version of the lexicographic order, in which different letters are compared differently depending on their positions in the word (i.e., there is one total order for comparing first letters, another for comparing second letters, etc.).

Lyndon words are related to various other objects in mathematics, such as free Lie algebras (Subsection 6.1.1 below), shuffles and shuffle algebras (Sections 6.2 and 6.3 below), QSym (Sections 6.4 and 6.5), Markov chains on combinatorial Hopf algebras ([52]), de Bruijn sequences ([72], [159], [160], [112, §7.2.11, Algorithm F]), symmetric functions (specifically, the transition matrices between the bases $(h_\lambda)_{\lambda \in \mathrm{Par}}$, $(e_\lambda)_{\lambda \in \mathrm{Par}}$ and $(m_\lambda)_{\lambda \in \mathrm{Par}}$; see [117] for this), and the Burrows-Wheeler algorithm for data compression (see Remark 6.6.31 below for a quick idea, and [45], [81], [116] for more). They are also connected to *necklaces* (in the combinatorial sense) – a combinatorial object that also happens to be related to a lot of algebra ([185, Chapter 5], [48]). Let us survey the basics of this latter classical connection in an exercise:

Exercise 6.1.34. Let $\mathfrak{A}$ be any set (not necessarily totally ordered). Let C denote the infinite cyclic group, written multiplicatively. Fix a generator c of C. [290] Fix a positive integer n. The group C acts on $\mathfrak{A}^n$ from the left according to the rule

$$c \cdot (a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_n, a_1) \qquad \text{for all } (a_1, a_2, \ldots, a_n) \in \mathfrak{A}^n.$$

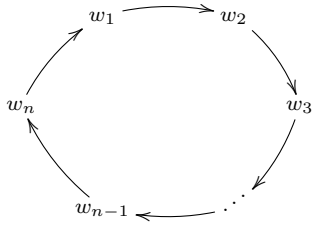
[291] The orbits of this C-action will be called *n-necklaces*[292]; they form a set partition of the set $\mathfrak{A}^n$.

[289] This result, as well as the validity of Proposition 6.1.16 in the partial-order setting, are due to Hazewinkel [92].

[290] So C is a group isomorphic to $(\mathbb{Z}, +)$, and the isomorphism $(\mathbb{Z}, +) \to C$ sends every $n \in \mathbb{Z}$ to c^n. (Recall that we write the binary operation of C as $\cdot$ instead of $+$.)

[291] In other words, c rotates any n-tuple of elements of $\mathfrak{A}$ cyclically to the left. Thus, $c^n \in C$ acts trivially on $\mathfrak{A}^n$, and so this action of C on $\mathfrak{A}^n$ factors through $C / \langle c^n \rangle$ (a cyclic group of order n).

[292] Classically, one visualizes them as necklaces of n beads of $|\mathfrak{A}|$ colors. (The colors are the elements of $\mathfrak{A}$.) For example, the necklace containing an n-tuple $(w_1, w_2, \ldots, w_n)$ is visualized as follows:



The n-necklace containing a given n-tuple $w \in \mathfrak{A}^n$ will be denoted by $[w]$.

(a) Prove that every n-necklace N is a finite nonempty set and satisfies $|N| \mid n$. (Recall that N is an orbit, thus a set; as usual, $|N|$ denotes the cardinality of this set.)

The *period* of an n-necklace N is defined as the positive integer $|N|$. (This $|N|$ is indeed a positive integer, since N is a finite nonempty set.)[293]

An n-necklace is said to be *aperiodic* if its period is n.

(b) Given any n-tuple $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, prove that the n-necklace $[w]$ is aperiodic if and only if every $k \in \{1, 2, \ldots, n-1\}$ satisfies $(w_{k+1}, w_{k+2}, \ldots, w_n, w_1, w_2, \ldots, w_k) \neq w$.

From now on, we assume that the set $\mathfrak{A}$ is totally ordered. We use $\mathfrak{A}$ as our alphabet to define the notions of words, the lexicographic order, and Lyndon words. All notations that we introduced for words will thus be used for elements of $\mathfrak{A}^n$.

(c) Prove that every aperiodic n-necklace contains exactly one Lyndon word.

(d) If N is an n-necklace which is not aperiodic, then prove that N contains no Lyndon word.

(e) Show that the aperiodic n-necklaces are in bijection with Lyndon words of length n.

From now on, we assume that the set $\mathfrak{A}$ is finite. Define the number-theoretic Möbius function μ and the Euler totient function ϕ as in Exercise 2.9.6.

(f) Prove that the number of all aperiodic n-necklaces is

$$\frac{1}{n} \sum_{d \mid n} \mu(d) \left|\mathfrak{A}\right|^{n/d}.$$

(g) Prove that the number of all n-necklaces is

$$\frac{1}{n} \sum_{d \mid n} \phi(d) \left|\mathfrak{A}\right|^{n/d}.$$

(h) Solve Exercise 6.1.29 again.

(i) Forget that we fixed $\mathfrak{A}$. Show that every $q \in \mathbb{Z}$ satisfies $n \mid \sum_{d \mid n} \mu(d)\, q^{n/d}$ and $n \mid \sum_{d \mid n} \phi(d)\, q^{n/d}$.

[**Hint:** For (c), use Theorem 6.1.20. For (i), either use parts (f) and (g) and a trick to extend to q negative; or recall Exercise 2.9.8.]

We will pick up the topic of necklaces again in Section 6.6, where we will connect it back to symmetric functions.

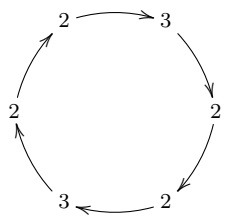
6.1.1. *Free Lie algebras.* In this brief subsection, we shall review the connection between Lyndon words and free Lie algebras (following [124, Kap. 4], but avoiding the generality of Hall sets in favor of just using Lyndon words). None of this material shall be used in the rest of these notes. We will only prove some basic results; for more thorough and comprehensive treatments of free Lie algebras, see [182], [27, Chapter 2] and [124, Kap. 4].

We begin with some properties of Lyndon words.

---

with $w_1, w_2, \ldots, w_n$ being the colors of the respective beads. The intuition behind this is that a necklace is an object that doesn't really change when we rotate it in its plane. However, to make this intuition match the definition, we need to think of a necklace as being stuck in its (fixed) plane, so that we cannot lift it up and turn it around, dropping it back to its plane in a reflected state.

[293] For example, the 6-necklace [232232] – or, visually,



– has period 3, as it is a set of size 3 (with elements 232232, 322322 and 223223). The word "period" hints at the geometric meaning: If an n-necklace N is represented by coloring the vertices of a regular n-gon, then its period is the smallest positive integer d such that the colors are preserved when the n-gon is rotated by $2\pi d/n$.

Exercise 6.1.35. Let $w \in \mathfrak{A}^*$ be a nonempty word. Let v be the longest Lyndon suffix of w [294]. Let t be a Lyndon word. Then, t is the longest Lyndon suffix of wt if and only if we do not have $v < t$.

(We have written "we do not have $v < t$" instead of "$v \geq t$" in Exercise 6.1.35 for reasons of generalizability: This way, Exercise 6.1.35 generalizes to the partial-order setting introduced in Exercise 6.1.33, whereas the version with "$v \geq t$" does not.)

Exercise 6.1.36. Let $w \in \mathfrak{A}^*$ be a word of length > 1. Let v be the longest Lyndon proper suffix of w [295]. Let t be a Lyndon word. Then, t is the longest Lyndon proper suffix of wt if and only if we do not have $v < t$.

(Exercise 6.1.36, while being a trivial consequence of Exercise 6.1.35, is rather useful in the study of free Lie algebras. It generalizes both [38, Lemma (1.6)] (which is obtained by taking $w = c$, $v = b$ and $t = d$) and [139, Proposition 5.1.4] (which is obtained by taking $v = m$ and $t = n$).)

Definition 6.1.37. For the rest of Subsection 6.1.1, we let $\mathfrak{L}$ be the set of all Lyndon words (over the alphabet $\mathfrak{A}$).

Definition 6.1.38. Let w be a Lyndon word of length > 1. Let v be the longest proper suffix of w such that v is Lyndon. (This is well-defined, as we know from Exercise 6.1.31.) Since v is a proper suffix of w, there exists a nonempty $u \in \mathfrak{A}^*$ such that $w = uv$. Consider this u. (Clearly, this u is unique.) Theorem 6.1.30(a) shows that the words u and v are Lyndon. In other words, $u \in \mathfrak{L}$ and $v \in \mathfrak{L}$. Hence, $(u, v) \in \mathfrak{L} \times \mathfrak{L}$. The pair $(u, v) \in \mathfrak{L} \times \mathfrak{L}$ is called the *standard factorization* of w, and is denoted by $\operatorname{stf} w$.

For the sake of easier reference, we gather a few basic properties of the standard factorization:

Exercise 6.1.39. Let w be a Lyndon word of length > 1. Let $(g, h) = \operatorname{stf} w$. Prove the following:

(a) The word h is the longest Lyndon proper suffix of w.
(b) We have $w = gh$.
(c) We have $g < gh < h$.
(d) The word g is Lyndon.
(e) We have $g \in \mathfrak{L}$, $h \in \mathfrak{L}$, $\ell(g) < \ell(w)$ and $\ell(h) < \ell(w)$.
(f) Let t be a Lyndon word. Then, t is the longest Lyndon proper suffix of wt if and only if we do not have $h < t$.

Exercise 6.1.40. Let $\mathfrak{g}$ be a Lie algebra. For every Lyndon word w, let b_w be an element of $\mathfrak{g}$. Assume that for every Lyndon word w of length > 1, we have

$$b_w = [b_u, b_v], \qquad \text{where } (u, v) = \operatorname{stf} w. \tag{6.1.2}$$

Let B be the $\mathbf{k}$-submodule of $\mathfrak{g}$ spanned by the family $(b_w)_{w \in \mathfrak{L}}$.

(a) Prove that B is a Lie subalgebra of $\mathfrak{g}$.
(b) Let $\mathfrak{h}$ be a $\mathbf{k}$-Lie algebra. Let $f : B \to \mathfrak{h}$ be a $\mathbf{k}$-module homomorphism. Assume that whenever w is a Lyndon word of length > 1, we have

$$f([b_u, b_v]) = [f(b_u), f(b_v)], \qquad \text{where } (u, v) = \operatorname{stf} w. \tag{6.1.3}$$

Prove that f is a Lie algebra homomorphism.

[**Hint:** Given two words w and w', write $w \sim w'$ if and only if w' is a permutation of w. Part (a) follows from the fact that for any $(p, q) \in \mathfrak{L} \times \mathfrak{L}$ satisfying $p < q$, we have $[b_p, b_q] \in B_{pq,q}$, where $B_{h,s}$ denotes the $\mathbf{k}$-linear span of $\{b_w \mid w \in \mathfrak{L},\ w \sim h \text{ and } w < s\}$ for any two words h and s. Prove this fact by a double induction, first inducting over $\ell(pq)$, and then (for fixed $\ell(pq)$) inducting over the rank of q in lexicographic order (i.e., assume that the fact is already proven for every $q' < q$ instead of q). In the induction step, assume that $(p, q) \neq \operatorname{stf}(pq)$ (since otherwise the claim is rather obvious) and conclude that p has length > 1; thus, set $(u, v) = \operatorname{stf} p$, so that $\left[\underbrace{b_p}_{=[b_u, b_v]}, b_q\right] = [[b_u, b_v], b_q] = [[b_u, b_q], b_v] - [[b_v, b_q], b_u]$, and use Exercise 6.1.36 to obtain $v < q$.

[294] Of course, a Lyndon suffix of w just means a suffix p of w such that p is Lyndon.

[295] Of course, a Lyndon proper suffix of w just means a proper suffix p of w such that p is Lyndon.

The proof of (b) proceeds by a similar induction, piggybacking on the $[b_p, b_q] \in B_{pq,q}$ claim.]

Exercise 6.1.41. Let V be the free $\mathbf{k}$-module with basis $(x_a)_{a \in \mathfrak{A}}$. For every word $w \in \mathfrak{A}^*$, let x_w be the tensor $x_{w_1} \otimes x_{w_2} \otimes \cdots \otimes x_{w_{\ell(w)}}$. As we know from Example 1.1.2, the tensor algebra $T(V)$ is a free $\mathbf{k}$-module with basis $(x_w)_{w \in \mathfrak{A}^*}$. We regard V as a $\mathbf{k}$-submodule of $T(V)$.

The tensor algebra $T(V)$ becomes a Lie algebra via the commutator (i.e., its Lie bracket is defined by $[\alpha, \beta] = \alpha\beta - \beta\alpha$ for all $\alpha \in T(V)$ and $\beta \in T(V)$).

We define a sequence $(\mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3, \ldots)$ of $\mathbf{k}$-submodules of $T(V)$ as follows: Recursively, we set $\mathfrak{g}_1 = V$, and for every $i \in \{2, 3, 4, \ldots\}$, we set $\mathfrak{g}_i = [V, \mathfrak{g}_{i-1}]$. Let $\mathfrak{g}$ be the $\mathbf{k}$-submodule $\mathfrak{g}_1 + \mathfrak{g}_2 + \mathfrak{g}_3 + \cdots$ of $T(V)$.

Prove the following:

(a) The $\mathbf{k}$-submodule $\mathfrak{g}$ is a Lie subalgebra of $T(V)$.

(b) If $\mathfrak{k}$ is any Lie subalgebra of $T(V)$ satisfying $V \subset \mathfrak{k}$, then $\mathfrak{g} \subset \mathfrak{k}$.

Now, for every $w \in \mathfrak{L}$, we define an element b_w of $T(V)$ as follows: We define b_w by recursion on the length of w. If the length of w is 1 [296], then we have $w = (a)$ for some letter $a \in \mathfrak{A}$, and we set $b_w = x_a$ for this letter a. If the length of w is > 1, then we set $b_w = [b_u, b_v]$, where $(u, v) = \operatorname{stf} w$ [297].

Prove the following:

(c) For every $w \in \mathfrak{L}$, we have

$$b_w \in x_w + \sum_{\substack{v \in \mathfrak{A}^{\ell(w)}; \\ v > w}} \mathbf{k} x_v.$$

(d) The family $(b_w)_{w \in \mathfrak{L}}$ is a basis of the $\mathbf{k}$-module $\mathfrak{g}$.

(e) Let $\mathfrak{h}$ be any $\mathbf{k}$-Lie algebra. Let $\xi : \mathfrak{A} \to \mathfrak{h}$ be any map. Then, there exists a unique Lie algebra homomorphism $\Xi : \mathfrak{g} \to \mathfrak{h}$ such that every $a \in \mathfrak{A}$ satisfies $\Xi(x_a) = \xi(a)$.

Remark 6.1.42. Let V and $\mathfrak{g}$ be as in Exercise 6.1.41. In the language of universal algebra, the statement of Exercise 6.1.41(e) says that $\mathfrak{g}$ (or, to be more precise, the pair $(\mathfrak{g}, f)$, where $f : \mathfrak{A} \to \mathfrak{g}$ is the map sending each $a \in \mathfrak{A}$ to $x_a \in \mathfrak{g}$) satisfies the universal property of the free Lie algebra on the set $\mathfrak{A}$. Thus, this exercise allows us to call $\mathfrak{g}$ the *free Lie algebra* on $\mathfrak{A}$. Most authors define the free Lie algebra differently, but all reasonable definitions of a free Lie algebra[298] lead to isomorphic Lie algebras (because the universal property determines the free Lie algebra uniquely up to canonical isomorphism).

Notice that the Lie algebra $\mathfrak{g}$ does not depend on the total order on the alphabet $\mathfrak{A}$, but the basis $(b_w)_{w \in \mathfrak{L}}$ constructed in Exercise 6.1.41(d) does. There is no known basis of $\mathfrak{g}$ defined without ordering $\mathfrak{A}$.

It is worth noticing that our construction of $\mathfrak{g}$ proves not only that the free Lie algebra on $\mathfrak{A}$ exists, but also that this free Lie algebra can be realized as a Lie subalgebra of the (associative) algebra $T(V)$. Therefore, if we want to prove that a certain identity holds in every Lie algebra, we only need to check that this identity holds in every associative algebra (if all Lie brackets are replaced by commutators); the universal property of the free Lie algebra (i.e., Exercise 6.1.41(e)) will then ensure that this identity also holds in every Lie algebra $\mathfrak{h}$.

There is much more to say about free Lie algebras than what we have said here; in particular, there are connections to symmetric functions, necklaces, representations of symmetric groups and NSym. See [139, §5.3], [182], [27, Chapter 2], [124, §4] and [24] for further developments[299].

6.2. **Shuffles and Lyndon words.** We will now connect the theory of Lyndon words with the notion of shuffle products. We have already introduced the latter notion in Definition 1.6.2, but we will now study it

[296] The length of any $w \in \mathfrak{L}$ must be at least 1. (Indeed, if $w \in \mathfrak{L}$, then the word w is Lyndon and thus nonempty, and hence its length must be at least 1.)

[297] This is well-defined, because b_u and b_v have already been defined. [*Proof.* Let $(u, v) = \operatorname{stf} w$. Then, Exercise 6.1.39(e) (applied to $(g, h) = (u, v)$) shows that $u \in \mathfrak{L}$, $v \in \mathfrak{L}$, $\ell(u) < \ell(w)$ and $\ell(v) < \ell(w)$. Recall that we are defining b_w by recursion on the length of w. Hence, b_p is already defined for every $p \in \mathfrak{L}$ satisfying $\ell(p) < \ell(w)$. Applying this to $p = u$, we see that b_u is already defined (since $u \in \mathfrak{L}$ and $\ell(u) < \ell(w)$). The same argument (but applied to v instead of u) shows that b_v is already defined. Hence, b_u and b_v have already been defined. Thus, b_w is well-defined by $b_w = [b_u, b_v]$, qed.]

[298] Here, we call a definition "reasonable" if the "free Lie algebra" it defines satisfies the universal property.

[299] The claim made in [24, page 2] that "$\{x_1, \ldots, x_n\}$ generates freely a Lie subalgebra of A_R" is essentially our Exercise 6.1.41(e).

more closely and introduce some more convenient notations (e.g., we will need a notation for single shuffles, not just the whole multiset).[300]

Definition 6.2.1. (a) Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Then, $\mathrm{Sh}_{n,m}$ denotes the subset

$$\left\{\sigma \in \mathfrak{S}_{n+m} \ : \ \sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n) \, ; \ \sigma^{-1}(n+1) < \sigma^{-1}(n+2) < \cdots < \sigma^{-1}(n+m)\right\}$$

of the symmetric group $\mathfrak{S}_{n+m}$.

(b) Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_m)$ be two words. If $\sigma \in \mathrm{Sh}_{n,m}$, then, $u \underset{\sigma}{\sqcup\!\sqcup} v$ will denote the word $\left(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n+m)}\right)$, where $(w_1, w_2, \ldots, w_{n+m})$ is the concatenation $u \cdot v = (u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_m)$. We notice that the multiset of all letters of $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the disjoint union of the multiset of all letters of u with the multiset of all letters of v. As a consequence, $\ell\left(u \underset{\sigma}{\sqcup\!\sqcup} v\right) = \ell(u) + \ell(v)$.

(c) Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_m)$ be two words. The *multiset of shuffles of u and v* is defined as the multiset $\left\{\left(w_{\sigma(1)}, w_{\sigma(2)}, \ldots, w_{\sigma(n+m)}\right) \ : \ \sigma \in \mathrm{Sh}_{n,m}\right\}_{\text{multiset}}$, where $(w_1, w_2, \ldots, w_{n+m})$ is the concatenation $u \cdot v = (u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_m)$. In other words, the multiset of shuffles of u and v is the multiset

$$\left\{u \underset{\sigma}{\sqcup\!\sqcup} v \ : \ \sigma \in \mathrm{Sh}_{n,m}\right\}_{\text{multiset}}.$$

It is denoted by $u \sqcup\!\sqcup v$.

The next fact provides the main connection between Lyndon words and shuffles:

Theorem 6.2.2. *Let u and v be two words.*

Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of u. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of v.

(a) *Let $(c_1, c_2, \ldots, c_{p+q})$ be the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order*[301]*. Then, the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $c_1 c_2 \cdots c_{p+q}$ (and $(c_1, c_2, \ldots, c_{p+q})$ is the CFL factorization of this element).*

(b) *Let $\mathfrak{L}$ denote the set of all Lyndon words. If w is a Lyndon word and z is any word, let $\mathrm{mult}_w z$ denote the number of terms in the CFL factorization of z which are equal to w. The multiplicity with which the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ appears in the multiset $u \sqcup\!\sqcup v$ is $\prod_{w \in \mathfrak{L}} \binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u}$. (This product is well-defined because almost all of its factors are 1.)*

(c) *If $a_i \geq b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$, then the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is uv.*

(d) *If $a_i > b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$, then the multiplicity with which the word uv appears in the multiset $u \sqcup\!\sqcup v$ is 1.*

(e) *Assume that u is a Lyndon word. Also, assume that $u \geq b_j$ for every $j \in \{1, 2, \ldots, q\}$. Then, the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is uv, and the multiplicity with which this word uv appears in the multiset $u \sqcup\!\sqcup v$ is $\mathrm{mult}_u v + 1$.*

Example 6.2.3. For this example, let u and v be the words $u = 23232$ and $v = 323221$ over the alphabet $\mathfrak{A} = \{1, 2, 3, \ldots\}$ with total order given by $1 < 2 < 3 < \cdots$. The CFL factorizations of u and v are $(23, 23, 2)$ and $(3, 23, 2, 2, 1)$, respectively. Thus, using the notations of Theorem 6.2.2, we have $p = 3$, $(a_1, a_2, \ldots, a_p) = (23, 23, 2)$, $q = 5$ and $(b_1, b_2, \ldots, b_q) = (3, 23, 2, 2, 1)$. Thus, Theorem 6.2.2(a) predicts that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8$, where $c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8$ are the words $23, 23, 2, 3, 23, 2, 2, 1$ listed in decreasing order (in other words, $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) = (3, 23, 23, 23, 2, 2, 2, 1)$). In other words, Theorem 6.2.2(a) predicts that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is 32323232221. We could verify this by brute force, but this would be laborious since the multiset $u \sqcup\!\sqcup v$ has $\binom{5+6}{5} = 462$ elements (with multiplicities). Theorem 6.2.2(b) predicts that this lexicographically highest element 32323232221 appears in the multiset $u \sqcup\!\sqcup v$ with a multiplicity of

[300] Parts (a) and (c) of the below Definition 6.2.1 define notions which have already been introduced in Definition 1.6.2. Of course, the definitions of these notions are equivalent; however, the variables are differently labelled in the two definitions (for example, the variables u, v, w and σ of Definition 6.2.1(c) correspond to the variables a, b, c and w of Definition 1.6.2). The labels in Definition 6.2.1 have been chosen to match with the rest of Section 6.2.

[301] with respect to the total order on $\mathfrak{A}^*$ whose greater-or-equal relation is $\geq$

$\prod_{w\in\mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$. This product $\prod_{w\in\mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$ is infinite, but all but finitely many of its factors are 1 and therefore can be omitted; the only factors which are not 1 are those corresponding to Lyndon words w which appear both in the CFL factorization of u and in the CFL factorization of v (since for any other factor, at least one of the numbers $\operatorname{mult}_w u$ or $\operatorname{mult}_w v$ equals 0, and therefore the binomial coefficient $\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$ equals 1). Thus, in order to compute the product $\prod_{w\in\mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}$, we only need to multiply these factors. In our example, these are the factors for $w = 23$ and for $w = 2$ (these are the only Lyndon words which appear both in the CFL factorization $(23, 23, 2)$ of u and in the CFL factorization $(3, 23, 2, 2, 1)$ of v). So we have

$$\prod_{w\in\mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} = \underbrace{\binom{\operatorname{mult}_{23} u + \operatorname{mult}_{23} v}{\operatorname{mult}_{23} u}}_{=\binom{2+1}{2}=3} \underbrace{\binom{\operatorname{mult}_2 u + \operatorname{mult}_2 v}{\operatorname{mult}_2 u}}_{=\binom{1+2}{1}=3} = 3 \cdot 3 = 9.$$

The word 32323232221 must thus appear in the multiset $u \sqcup\!\sqcup v$ with a multiplicity of 9. This, too, could be checked by brute force.

Theorem 6.2.2 (and Theorem 6.2.22 further below, which describes more precisely how the lexicographically highest element of $u \sqcup\!\sqcup v$ emerges by shuffling u and v) is fairly close to [177, Theorem 2.2.2] (and will be used for the same purposes), the main difference being that we are talking about the shuffle product of two (not necessarily Lyndon) words, while Radford (and most other authors) study the shuffle product of many Lyndon words.

In order to prove Theorem 6.2.2, we will need to make some stronger statements, for which we first have to introduce some more notation:

Definition 6.2.4. (a) If p and q are two integers, then $[p : q]^+$ denotes the interval $\{p+1, p+2, \ldots, q\}$ of $\mathbb{Z}$. Note that $\left|[p : q]^+\right| = q - p$ if $q \geq p$.

(b) If I and J are two nonempty intervals of $\mathbb{Z}$, then we say that $I < J$ if and only if every $i \in I$ and $j \in J$ satisfy $i < j$. This defines a partial order on the set of nonempty intervals of $\mathbb{Z}$. (Roughly speaking, $I < J$ if the interval I ends before J begins.)

(c) If w is a word with n letters (for some $n \in \mathbb{N}$), and I is an interval of $\mathbb{Z}$ such that $I \subset [0 : n]^+$, then $w[I]$ will denote the word $(w_{p+1}, w_{p+2}, \ldots, w_q)$, where I is written in the form $I = [p : q]^+$ with $q \geq p$. Obviously, $\ell(w[I]) = |I| = q - p$. A word of the form $w[I]$ for an interval $I \subset [0 : n]^+$ (equivalently, a word which is a prefix of a suffix of w) is called a *factor* of w.

(d) Let α be a composition. Then, we define a tuple $\operatorname{intsys}\alpha$ of intervals of $\mathbb{Z}$ as follows: Write α in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ (so that $\ell = \ell(\alpha)$). Then, set $\operatorname{intsys}\alpha = (I_1, I_2, \ldots, I_\ell)$, where

$$I_i = \left[\sum_{k=1}^{i-1} \alpha_k : \sum_{k=1}^{i} \alpha_k\right]^+ \qquad \text{for every } i \in \{1, 2, \ldots, \ell\}.$$

This ℓ-tuple $\operatorname{intsys}\alpha$ is a tuple of nonempty intervals of $\mathbb{Z}$. This tuple $\operatorname{intsys}\alpha$ is called the *interval system corresponding to* α. (This is precisely the ℓ-tuple $(I_1, I_2, \ldots, I_\ell)$ constructed in Definition 4.3.4.) The length of the tuple $\operatorname{intsys}\alpha$ is $\ell(\alpha)$.

Example 6.2.5. (a) We have $[2 : 4]^+ = \{3, 4\}$ and $[3 : 3]^+ = \varnothing$.

(b) We have $[2 : 4]^+ < [4 : 5]^+ < [6 : 8]^+$, but we have neither $[2 : 4]^+ < [3 : 5]^+$ nor $[3 : 5]^+ < [2 : 4]^+$.

(c) If w is the word 915352, then $w\left[[0 : 3]^+\right] = (w_1, w_2, w_3) = 915$ and $w\left[[2 : 4]^+\right] = (w_3, w_4) = 53$.

(d) If α is the composition $(4, 1, 4, 2, 3)$, then the interval system corresponding to α is

$$\begin{aligned}\operatorname{intsys}\alpha &= \left([0 : 4]^+, [4 : 5]^+, [5 : 9]^+, [9 : 11]^+, [11 : 14]^+\right) \\ &= (\{1, 2, 3, 4\}, \{5\}, \{6, 7, 8, 9\}, \{10, 11\}, \{12, 13, 14\}).\end{aligned}$$

The following properties of the notions introduced in the preceding definition are easy to check:

Remark 6.2.6. (a) If I and J are two nonempty intervals of $\mathbb{Z}$ satisfying $I < J$, then I and J are disjoint.

(b) If I and J are two disjoint nonempty intervals of $\mathbb{Z}$, then either $I < J$ or $J < I$.

(c) Let α be a composition. Write α in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ (so that $\ell = \ell(\alpha)$). The interval system $\operatorname{intsys}\alpha$ can be described as the unique ℓ-tuple $(I_1, I_2, \ldots, I_\ell)$ of nonempty intervals of $\mathbb{Z}$ satisfying the following three properties:
- The intervals I_1, I_2, ..., I_ℓ form a set partition of the set $[0:n]^+$, where $n = |\alpha|$.
- We have $I_1 < I_2 < \cdots < I_\ell$.
- We have $|I_i| = \alpha_i$ for every $i \in \{1, 2, \ldots, \ell\}$.

Exercise 6.2.7. Prove Remark 6.2.6.

The following two lemmas are collections of more or less trivial consequences of what it means to be an element of $\operatorname{Sh}_{n,m}$ and what it means to be a shuffle:

Lemma 6.2.8. *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\sigma \in \operatorname{Sh}_{n,m}$.*

(a) *If I is an interval of $\mathbb{Z}$ such that $I \subset [0:n+m]^+$, then $\sigma(I) \cap [0:n]^+$ and $\sigma(I) \cap [n:n+m]^+$ are intervals.*

(b) *Let K and L be nonempty intervals of $\mathbb{Z}$ such that $K \subset [0:n]^+$ and $L \subset [0:n]^+$ and $K < L$ and such that $K \cup L$ is an interval. Assume that $\sigma^{-1}(K)$ and $\sigma^{-1}(L)$ are intervals, but $\sigma^{-1}(K) \cup \sigma^{-1}(L)$ is not an interval. Then, there exists a nonempty interval $P \subset [n:n+m]^+$ such that $\sigma^{-1}(P)$, $\sigma^{-1}(K) \cup \sigma^{-1}(P)$ and $\sigma^{-1}(P) \cup \sigma^{-1}(L)$ are intervals and such that $\sigma^{-1}(K) < \sigma^{-1}(P) < \sigma^{-1}(L)$.*

(c) *Lemma 6.2.8(b) remains valid if "$K \subset [0:n]^+$ and $L \subset [0:n]^+$" and "$P \subset [n:n+m]^+$" are replaced by "$K \subset [n:n+m]^+$ and $L \subset [n:n+m]^+$" and "$P \subset [0:n]^+$", respectively.*

Exercise 6.2.9. Prove Lemma 6.2.8.

Lemma 6.2.10. *Let u and v be two words. Let $n = \ell(u)$ and $m = \ell(v)$. Let $\sigma \in \operatorname{Sh}_{n,m}$.*

(a) *If I is an interval of $\mathbb{Z}$ satisfying either $I \subset [0:n]^+$ or $I \subset [n:n+m]^+$, and if $\sigma^{-1}(I)$ is an interval, then*

$$\left(u \underset{\sigma}{\sqcup\!\sqcup} v\right)\left[\sigma^{-1}(I)\right] = (uv)[I]. \tag{6.2.1}$$

(b) *Assume that $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Let $I \subset [0:n]^+$ and $J \subset [n:n+m]^+$ be two nonempty intervals. Assume that $\sigma^{-1}(I)$ and $\sigma^{-1}(J)$ are also intervals, that $\sigma^{-1}(I) < \sigma^{-1}(J)$, and that $\sigma^{-1}(I) \cup \sigma^{-1}(J)$ is an interval as well. Then, $(uv)[I] \cdot (uv)[J] \geq (uv)[J] \cdot (uv)[I]$.*

(c) *Lemma 6.2.10(b) remains valid if "$I \subset [0:n]^+$ and $J \subset [n:n+m]^+$" is replaced by "$I \subset [n:n+m]^+$ and $J \subset [0:n]^+$".*

Exercise 6.2.11. Prove Lemma 6.2.10.

[**Hint:** For (b), show that there exists a $\tau \in \operatorname{Sh}_{n,m}$ such that $u \underset{\tau}{\sqcup\!\sqcup} v$ differs from $u \underset{\sigma}{\sqcup\!\sqcup} v$ only in the order of the subwords $(uv)[I]$ and $(uv)[J]$.]

We are still a few steps away from stating our results in a way that allows comfortably proving Theorem 6.2.2. For the latter aim, we introduce the notion of *α-clumping permutations*, and characterize them in two ways:

Definition 6.2.12. Let $n \in \mathbb{N}$. Let α be a composition of n. Let $\ell = \ell(\alpha)$.

(a) For every set S of positive integers, let $\overrightarrow{S}$ denote the list of all elements of S in increasing order (with each element appearing exactly once). Notice that this list $\overrightarrow{S}$ is a word over the set of positive integers.

(b) For every $\tau \in \mathfrak{S}_\ell$, we define a permutation $\operatorname{iper}(\alpha, \tau) \in \mathfrak{S}_n$ as follows:

The interval system corresponding to α is an ℓ-tuple of intervals (since $\ell(\alpha) = \ell$); denote this ℓ-tuple by $(I_1, I_2, \ldots, I_\ell)$. Now, define $\operatorname{iper}(\alpha, \tau)$ to be the permutation in $\mathfrak{S}_n$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\cdots\overrightarrow{I_{\tau(\ell)}}$ (a concatenation of ℓ words). This is well-defined[302]; hence, $\operatorname{iper}(\alpha, \tau) \in \mathfrak{S}_n$ is defined.

[302] In fact, from the properties of interval systems, we know that the intervals I_1, I_2, ..., I_ℓ form a set partition of the set $[0:n]^+$. Hence, the intervals $I_{\tau(1)}$, $I_{\tau(2)}$, ..., $I_{\tau(\ell)}$ form a set partition of the set $[0:n]^+$. As a consequence, the word

(c) The interval system corresponding to α is an ℓ-tuple of intervals (since $\ell(\alpha) = \ell$); denote this ℓ-tuple by $(I_1, I_2, \ldots, I_\ell)$.

A permutation $\sigma \in \mathfrak{S}_n$ is said to be *α-clumping* if every $i \in \{1, 2, \ldots, \ell\}$ has the two properties that:

- the set $\sigma^{-1}(I_i)$ is an interval;
- the restriction of the map σ^{-1} to the interval I_i is increasing.

Example 6.2.13. For this example, let $n = 7$ and $\alpha = (2, 1, 3, 1)$. Then, $\ell = \ell(\alpha) = 4$ and $(I_1, I_2, I_3, I_4) = (\{1, 2\}, \{3\}, \{4, 5, 6\}, \{7\})$ (where we are using the notations of Definition 6.2.12). Hence, $\overrightarrow{I_1} = 12$, $\overrightarrow{I_2} = 3$, $\overrightarrow{I_3} = 456$ and $\overrightarrow{I_4} = 7$.

(a) If $\tau \in \mathfrak{S}_\ell = \mathfrak{S}_4$ is the permutation $(2, 3, 1, 4)$, then $\operatorname{iper}(\alpha, \tau)$ is the permutation in $\mathfrak{S}_7$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\overrightarrow{I_{\tau(3)}}\overrightarrow{I_{\tau(4)}} = \overrightarrow{I_2}\overrightarrow{I_3}\overrightarrow{I_1}\overrightarrow{I_4} = 3456127$.

If $\tau \in \mathfrak{S}_\ell = \mathfrak{S}_4$ is the permutation $(3, 1, 4, 2)$, then $\operatorname{iper}(\alpha, \tau)$ is the permutation in $\mathfrak{S}_7$ which (in one-line notation) is the word $\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\overrightarrow{I_{\tau(3)}}\overrightarrow{I_{\tau(4)}} = \overrightarrow{I_3}\overrightarrow{I_1}\overrightarrow{I_4}\overrightarrow{I_2} = 4561273$.

(b) The permutation $\sigma = (3, 7, 4, 5, 6, 1, 2) \in \mathfrak{S}_7$ (given here in one-line notation) is α-clumping, because:

- every $i \in \{1, 2, \ldots, \ell\} = \{1, 2, 3, 4\}$ has the property that $\sigma^{-1}(I_i)$ is an interval (namely, $\sigma^{-1}(I_1) = \sigma^{-1}(\{1, 2\}) = \{6, 7\}$, $\sigma^{-1}(I_2) = \sigma^{-1}(\{3\}) = \{1\}$, $\sigma^{-1}(I_3) = \sigma^{-1}(\{4, 5, 6\}) = \{3, 4, 5\}$ and $\sigma^{-1}(I_4) = \sigma^{-1}(\{7\}) = \{2\}$), and
- the restrictions of the map σ^{-1} to the intervals I_i are increasing (this means that $\sigma^{-1}(1) < \sigma^{-1}(2)$ and $\sigma^{-1}(4) < \sigma^{-1}(5) < \sigma^{-1}(6)$, since the one-element intervals I_2 and I_4 do not contribute anything to this condition).

Here is a more or less trivial observation:

Proposition 6.2.14. *Let $n \in \mathbb{N}$. Let α be a composition of n. Let $\ell = \ell(\alpha)$. Write α in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$. The interval system corresponding to α is an ℓ-tuple of intervals (since $\ell(\alpha) = \ell$); denote this ℓ-tuple by $(I_1, I_2, \ldots, I_\ell)$. Let $\tau \in \mathfrak{S}_\ell$. Set $\sigma = \operatorname{iper}(\alpha, \tau)$.*

(a) *We have $\sigma^{-1}\left(I_{\tau(j)}\right) = \left[\sum_{k=1}^{j-1} \alpha_{\tau(k)} : \sum_{k=1}^{j} \alpha_{\tau(k)}\right]^+$ for every $j \in \{1, 2, \ldots, \ell\}$.*

(b) *For every $j \in \{1, 2, \ldots, \ell\}$, the restriction of the map σ^{-1} to the interval $I_{\tau(j)}$ is increasing.*

(c) *The permutation $\operatorname{iper}(\alpha, \tau)$ is α-clumping.*

(d) *Let $i \in \{1, 2, \ldots, \ell - 1\}$. Then, the sets $\sigma^{-1}\left(I_{\tau(i)}\right)$, $\sigma^{-1}\left(I_{\tau(i+1)}\right)$ and $\sigma^{-1}\left(I_{\tau(i)}\right) \cup \sigma^{-1}\left(I_{\tau(i+1)}\right)$ are nonempty intervals. Also, $\sigma^{-1}\left(I_{\tau(i)}\right) < \sigma^{-1}\left(I_{\tau(i+1)}\right)$.*

Exercise 6.2.15. Prove Proposition 6.2.14.

Proposition 6.2.16. *Let $n \in \mathbb{N}$. Let α be a composition of n. Let $\ell = \ell(\alpha)$.*

(a) *Define a map*

$$\operatorname{iper}_\alpha : \mathfrak{S}_\ell \longrightarrow \{\omega \in \mathfrak{S}_n \mid \omega \text{ is } \alpha\text{-clumping}\},$$
$$\tau \longmapsto \operatorname{iper}(\alpha, \tau)$$

[303]. *This map $\operatorname{iper}_\alpha$ is bijective.*

(b) *Let $\sigma \in \mathfrak{S}_n$ be an α-clumping permutation. Then, there exists a unique $\tau \in \mathfrak{S}_\ell$ satisfying $\sigma = \operatorname{iper}(\alpha, \tau)$.*

Exercise 6.2.17. Prove Proposition 6.2.16.

Next, we recall that the concatenation $\alpha \cdot \beta$ of two compositions α and β is defined in the same way as the concatenation of two words; if we regard compositions as words over the alphabet $\{1, 2, 3, \ldots\}$, then the concatenation $\alpha \cdot \beta$ of two compositions α and β **is** the concatenation $\alpha\beta$ of the words α and β. Thus, we are going to write $\alpha\beta$ for the concatenation $\alpha \cdot \beta$ of two compositions α and β from now on.

$\overrightarrow{I_{\tau(1)}}\overrightarrow{I_{\tau(2)}}\cdots\overrightarrow{I_{\tau(\ell)}}$ is a permutation of the word $12\ldots n$, and so there exists a permutation in $\mathfrak{S}_n$ which (in one-line notation) is this word, qed.

[303] This map is well-defined because for every $\tau \in \mathfrak{S}_\ell$, the permutation $\operatorname{iper}(\alpha, \tau)$ is α-clumping (according to Proposition 6.2.14(c)).

Proposition 6.2.18. *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let α be a composition of n, and β be a composition of m. Let $p = \ell(\alpha)$ and $q = \ell(\beta)$. Let $\tau \in \mathfrak{S}_{p+q}$. Notice that $\operatorname{iper}(\alpha\beta, \tau) \in \mathfrak{S}_{n+m}$ (since $\alpha\beta$ is a composition of $n+m$ having length $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta) = p+q$). Then, $\tau \in \operatorname{Sh}_{p,q}$ if and only if $\operatorname{iper}(\alpha\beta, \tau) \in \operatorname{Sh}_{n,m}$.*

Exercise 6.2.19. Prove Proposition 6.2.18.

Here is one more simple fact:

Lemma 6.2.20. *Let u and v be two words. Let $n = \ell(u)$ and $m = \ell(v)$. Let α be a composition of n, and let β be a composition of m. Let $p = \ell(\alpha)$ and $q = \ell(\beta)$. The concatenation $\alpha\beta$ is a composition of $n+m$ having length $\ell(\alpha\beta) = \ell(\alpha) + \ell(\beta) = p+q$. Thus, the interval system corresponding to $\alpha\beta$ is a $(p+q)$-tuple of intervals which covers $[0 : n+m]^+$. Denote this $(p+q)$-tuple by $(I_1, I_2, \ldots, I_{p+q})$.*

Let $\tau \in \operatorname{Sh}_{p,q}$. Set $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Then,

$$u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right].$$

Exercise 6.2.21. Prove Lemma 6.2.20.

Having these notations and trivialities in place, we can say a bit more about the lexicographically highest element of a shuffle product than what was said in Theorem 6.2.2:

Theorem 6.2.22. *Let u and v be two words. Let $n = \ell(u)$ and $m = \ell(v)$.*

Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of u. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of v.

Let α be the p-tuple $(\ell(a_1), \ell(a_2), \ldots, \ell(a_p))$. Then, α is a composition[304] of length p and size $\sum_{k=1}^{p} \ell(a_k) = \ell\left(\underbrace{a_1 a_2 \cdots a_p}_{=u}\right) = \ell(u) = n$.

Let β be the q-tuple $(\ell(b_1), \ell(b_2), \ldots, \ell(b_q))$. Then, β is a composition of length q and size $\sum_{k=1}^{q} \ell(b_k) = m$.[305]

Now, α is a composition of length p and size n, and β is a composition of length q and size m. Thus, the concatenation $\alpha\beta$ of these two tuples is a composition of length $p+q$ and size $n+m$. The interval system corresponding to this composition $\alpha\beta$ is a $(p+q)$-tuple (since said composition has length $p+q$); denote this $(p+q)$-tuple by $(I_1, I_2, \ldots, I_{p+q})$.

(a) *If $\tau \in \operatorname{Sh}_{p,q}$ satisfies $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$, and if we set $\sigma = \operatorname{iper}(\alpha\beta, \tau)$, then $\sigma \in \operatorname{Sh}_{n,m}$, and the word $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$.*

(b) *Let $\sigma \in \operatorname{Sh}_{n,m}$ be a permutation such that $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Then, there exists a unique permutation $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$.*

Proof. Before we step to the actual proof, we need to make some preparation. First of all, $(I_1, I_2, \ldots, I_{p+q})$ is the interval system corresponding to the composition $\alpha\beta$. In other words,

$$(I_1, I_2, \ldots, I_{p+q}) = \operatorname{intsys}(\alpha\beta). \tag{6.2.2}$$

But since $\alpha = (\ell(a_1), \ell(a_2), \ldots, \ell(a_p))$ and $\beta = (\ell(b_1), \ell(b_2), \ldots, \ell(b_q))$, we have

$$\alpha\beta = (\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q)).$$

Thus, (6.2.2) rewrites as

$$(I_1, I_2, \ldots, I_{p+q}) = \operatorname{intsys}(\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q)).$$

By the definition of $\operatorname{intsys}(\ell(a_1), \ell(a_2), \ldots, \ell(a_p), \ell(b_1), \ell(b_2), \ldots, \ell(b_q))$, we thus have

$$I_i = \left[\sum_{k=1}^{i-1} \ell(a_k) : \sum_{k=1}^{i} \ell(a_k)\right]^+ \qquad \text{for every } i \in \{1, 2, \ldots, p\},$$

[304] since Lyndon words are nonempty, and thus $\ell(a_i) > 0$ for every i

[305] The proof of this is the same as the proof of the fact that α is a composition of length p and size $\sum_{k=1}^{p} \ell(\alpha_k) = n$.

and besides

$$I_{p+j} = \left[n + \sum_{k=1}^{j-1} \ell(b_k) : n + \sum_{k=1}^{j} \ell(b_k) \right]^+ \qquad \text{for every } j \in \{1,2,\ldots,q\}$$

(since $\sum_{k=1}^{p} \ell(a_k) = n$). Moreover, Remark 6.2.6(c) shows that $(I_1, I_2, \ldots, I_{p+q})$ is a $(p+q)$-tuple of nonempty intervals of $\mathbb{Z}$ and satisfies the following three properties:

- The intervals I_1, I_2, ..., I_{p+q} form a set partition of the set $[0 : n+m]^+$.
- We have $I_1 < I_2 < \cdots < I_{p+q}$.
- We have $|I_i| = \ell(a_i)$ for every $i \in \{1,2,\ldots,p\}$ and $|I_{p+j}| = \ell(b_j)$ for every $j \in \{1,2,\ldots,q\}$.

Of course, every $i \in \{1,2,\ldots,p\}$ satisfies

$$I_i \subset [0:n]^+ \qquad \text{and} \qquad (uv)[I_i] = u[I_i] = a_i. \tag{6.2.3}$$

Meanwhile, every $i \in \{p+1, p+2, \ldots, p+q\}$ satisfies

$$I_i \subset [n : n+m]^+ \qquad \text{and} \qquad (uv)[I_i] = v[I_i - n] = b_{i-p} \tag{6.2.4}$$

(where $I_i - n$ denotes the interval $\{k - n \mid k \in I_i\}$). We thus see that

$$(uv)[I_i] \text{ is a Lyndon word} \qquad \text{for every } i \in \{1,2,\ldots,p+q\} \tag{6.2.5}$$

[306].

By the definition of a CFL factorization, we have $a_1 \geq a_2 \geq \cdots \geq a_p$ and $b_1 \geq b_2 \geq \cdots \geq b_q$.

We have $\sigma \in \mathrm{Sh}_{n,m}$, so that $\sigma^{-1}(1) < \sigma^{-1}(2) < \cdots < \sigma^{-1}(n)$ and $\sigma^{-1}(n+1) < \sigma^{-1}(n+2) < \cdots < \sigma^{-1}(n+m)$. In other words, the restriction of the map σ^{-1} to the interval $[0:n]^+$ is strictly increasing, and so is the restriction of the map σ^{-1} to the interval $[n : n+m]^+$.

(b) We will first show that

(6.2.6) if $J \subset [0:n]^+$ is an interval such that the word $(uv)[J]$ is Lyndon, then $\sigma^{-1}(J)$ is an interval.

Proof of (6.2.6): We will prove (6.2.6) by strong induction over $|J|$.

So, fix some $N \in \mathbb{N}$. Assume (as the induction hypothesis) that (6.2.6) has been proven whenever $|J| < N$. We now need to prove (6.2.6) when $|J| = N$.

Let $J \subset [0:n]^+$ be an interval such that the word $(uv)[J]$ is Lyndon and such that $|J| = N$. We have to prove that $\sigma^{-1}(J)$ is an interval. This is obvious if $|J| = 1$ (because in this case, $\sigma^{-1}(J)$ is a one-element set, thus trivially an interval). Hence, we WLOG assume that we don't have $|J| = 1$. We also don't have $|J| = 0$, because $(uv)[J]$ has to be Lyndon (and the empty word is not). So we have $|J| > 1$. Now, $\ell((uv)[J]) = |J| > 1$, and thus $(uv)[J]$ is a Lyndon word of length > 1. Let v' be the (lexicographically) smallest nonempty **proper** suffix of $(uv)[J]$. Since v' is a proper suffix of w, there exists a nonempty $u' \in \mathfrak{A}^*$ such that $(uv)[J] = u'v'$. Consider this u'.

Now, Theorem 6.1.30(a) (applied to $(uv)[J]$, u' and v' instead of w, u and v) yields that the words u' and v' are Lyndon. Also, Theorem 6.1.30(b) (applied to $(uv)[J]$, u' and v' instead of w, u and v) yields that $u' < (uv)[J] < v'$.

But from the fact that $(uv)[J] = u'v'$ with u' and v' both being nonempty, it becomes immediately clear that we can write J as a union of two disjoint nonempty intervals K and L such that $K < L$, $u' = (uv)[K]$ and $v' = (uv)[L]$. Consider these K and L. The intervals K and L are nonempty and have their sizes add up to $|J|$ (since they are disjoint and their union is J), and hence both must have size smaller than $|J| = N$. So $K \subset [0:n]^+$ is an interval of size $|K| < N$ having the property that $(uv)[K]$ is Lyndon (since $(uv)[K] = u'$ is Lyndon). Thus, we can apply (6.2.6) to K instead of J (because of the induction hypothesis). As a result, we conclude that $\sigma^{-1}(K)$ is an interval. Similarly, we can apply (6.2.6) to L instead of J (we know that $(uv)[L]$ is Lyndon since $(uv)[L] = v'$), and learn that $\sigma^{-1}(L)$ is an interval. The intervals $\sigma^{-1}(K)$ and $\sigma^{-1}(L)$ are both nonempty (since K and L are nonempty), and their union is $\sigma^{-1}(J)$ (because the union of K and L is J). The nonempty intervals K and L both are subsets of $[0:n]^+$ (since their union is $J \subset [0:n]^+$), and their union $K \cup L$ is an interval (since their union $K \cup L$ is J, and we know that J is an interval).

[306] Indeed, when $i \leq p$, this follows from (6.2.3) and the fact that a_i is Lyndon; whereas in the other case, this follows from (6.2.4) and the fact that b_{i-p} is Lyndon.

Now, assume (for the sake of contradiction) that $\sigma^{-1}(J)$ is not an interval. Since J is the union of K and L, we have $J = K \cup L$ and thus $\sigma^{-1}(J) = \sigma^{-1}(K \cup L) = \sigma^{-1}(K) \cup \sigma^{-1}(L)$ (since σ is a bijection). Therefore, $\sigma^{-1}(K) \cup \sigma^{-1}(L)$ is not an interval (since $\sigma^{-1}(J)$ is not an interval). Thus, Lemma 6.2.8(b) yields that there exists a nonempty interval $P \subset [n : n+m]^+$ such that $\sigma^{-1}(P)$, $\sigma^{-1}(K) \cup \sigma^{-1}(P)$ and $\sigma^{-1}(P) \cup \sigma^{-1}(L)$ are intervals and such that $\sigma^{-1}(K) < \sigma^{-1}(P) < \sigma^{-1}(L)$. Consider this P. Since P is nonempty, we have $|P| \neq 0$.

Lemma 6.2.10(b) (applied to K and P instead of I and J) yields

$$(uv)[K] \cdot (uv)[P] \geq (uv)[P] \cdot (uv)[K]. \tag{6.2.7}$$

Since $(uv)[K] = u'$, this rewrites as

$$u' \cdot (uv)[P] \geq (uv)[P] \cdot u'. \tag{6.2.8}$$

But Lemma 6.2.10(c) (applied to P and L instead of I and J) yields

$$(uv)[P] \cdot (uv)[L] \geq (uv)[L] \cdot (uv)[P]. \tag{6.2.9}$$

Since $(uv)[L] = v'$, this rewrites as

$$(uv)[P] \cdot v' \geq v' \cdot (uv)[P]. \tag{6.2.10}$$

Recall also that $u' < v'$, and that both words u' and v' are Lyndon. Now, Corollary 6.1.17 (applied to u', v' and $(uv)[P]$ instead of u, v and z) yields that $(uv)[P]$ is the empty word (because of (6.2.8) and (6.2.10)), so that $\ell((uv)[P]) = 0$. This contradicts $\ell((uv)[P]) = |P| \neq 0$. This contradiction shows that our assumption (that $\sigma^{-1}(J)$ is not an interval) was wrong. Hence, $\sigma^{-1}(J)$ is an interval. This completes the induction step, and thus (6.2.6) is proven.

Similarly to (6.2.6), we can show that

(6.2.11) if $J \subset [n : n+m]^+$ is an interval such that the word $(uv)[J]$ is Lyndon, then $\sigma^{-1}(J)$ is an interval.

Now, let $i \in \{1, 2, \ldots, p+q\}$ be arbitrary. We are going to prove that

$$\sigma^{-1}(I_i) \text{ is an interval.} \tag{6.2.12}$$

Proof of (6.2.12): We must be in one of the following two cases:

Case 1: We have $i \in \{1, 2, \ldots, p\}$.

Case 2: We have $i \in \{p+1, p+2, \ldots, p+q\}$.

Let us first consider Case 1. In this case, we have $i \in \{1, 2, \ldots, p\}$. Thus, $I_i \subset [0 : n]^+$ (by (6.2.3)). Also, (6.2.3) yields that $(uv)[I_i] = a_i$ is a Lyndon word. Hence, (6.2.6) (applied to $J = I_i$) yields that $\sigma^{-1}(I_i)$ is an interval. Thus, (6.2.12) is proven in Case 1.

Similarly, we can prove (6.2.12) in Case 2, using (6.2.4) and (6.2.11) instead of (6.2.3) and (6.2.6), respectively. Hence, (6.2.12) is proven.

So we know that $\sigma^{-1}(I_i)$ is an interval. But we also know that either $I_i \subset [0 : n]^+$ or $I_i \subset [n : n+m]^+$ (depending on whether $i \leq p$ or $i > p$). As a consequence, the restriction of the map σ^{-1} to the interval I_i is increasing (because the restriction of the map σ^{-1} to the interval $[0 : n]^+$ is strictly increasing, and so is the restriction of the map σ^{-1} to the interval $[n : n+m]^+$).

Now, let us forget that we fixed i. We thus have shown that every $i \in \{1, 2, \ldots, p+q\}$ has the two properties that:

- the set $\sigma^{-1}(I_i)$ is an interval;
- the restriction of the map σ^{-1} to the interval I_i is increasing.

In other words, the permutation σ is $(\alpha\beta)$-clumping (since $(I_1, I_2, \ldots, I_{p+q})$ is the interval system corresponding to the composition $\alpha\beta$). Hence, Proposition 6.2.16(b) (applied to $n+m$, $\alpha\beta$ and $p+q$ instead of n, α and ℓ) shows that there exists a unique $\tau \in \mathfrak{S}_{p+q}$ satisfying $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Thus, the uniqueness part of Theorem 6.2.22(b) (i.e., the claim that the τ in Theorem 6.2.22(b) is unique if it exists) is proven.

It now remains to prove the existence part of Theorem 6.2.22(b), i.e., to prove that there exists at least one permutation $\tau \in \operatorname{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. We already know that there exists a unique $\tau \in \mathfrak{S}_{p+q}$ satisfying $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Consider this τ. We will now prove that $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\tau \in \operatorname{Sh}_{p,q}$. Once this is done, the existence part of Theorem 6.2.22(b) will be proven, and thus the proof of Theorem 6.2.22(b) will be complete.

Proposition 6.2.18 yields that $\tau \in \mathrm{Sh}_{p,q}$ if and only if $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$. Since we know that $\operatorname{iper}(\alpha\beta, \tau) = \sigma \in \mathrm{Sh}_{n,m}$, we thus conclude that $\tau \in \mathrm{Sh}_{p,q}$. The only thing that remains to be proven now is that

$$(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.13}$$

Proof of (6.2.13): We have $\tau \in \mathrm{Sh}_{p,q}$. In other words, $\tau^{-1}(1) < \tau^{-1}(2) < \cdots < \tau^{-1}(p)$ and $\tau^{-1}(p+1) < \tau^{-1}(p+2) < \cdots < \tau^{-1}(p+q)$. In other words, the restriction of the map τ^{-1} to the interval $[0:p]^+$ is strictly increasing, and so is the restriction of the map τ^{-1} to the interval $[p:p+q]^+$.

Let $i \in \{1, 2, \ldots, p+q-1\}$. We will show that

$$(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]. \tag{6.2.14}$$

Clearly, both $\tau(i)$ and $\tau(i+1)$ belong to $\{1, 2, \ldots, p+q\} = \{1, 2, \ldots, p\} \cup \{p+1, p+2, \ldots, p+q\}$. Thus, we must be in one of the following four cases:

Case 1: We have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{1, 2, \ldots, p\}$.

Case 2: We have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$.

Case 3: We have $\tau(i) \in \{p+1, p+2, \ldots, p+q\}$ and $\tau(i+1) \in \{1, 2, \ldots, p\}$.

Case 4: We have $\tau(i) \in \{p+1, p+2, \ldots, p+q\}$ and $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$.

Let us consider Case 1 first. In this case, we have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{1, 2, \ldots, p\}$. From the fact that the restriction of the map τ^{-1} to the interval $[0:p]^+$ is strictly increasing, we can easily deduce $\tau(i) < \tau(i+1)$ [307]. Therefore, $a_{\tau(i)} \geq a_{\tau(i+1)}$ (since $a_1 \geq a_2 \geq \cdots \geq a_p$).

But $(uv)\left[I_{\tau(i)}\right] = a_{\tau(i)}$ (by (6.2.3), applied to $\tau(i)$ instead of i) and $(uv)\left[I_{\tau(i+1)}\right] = a_{\tau(i+1)}$ (similarly). In view of these equalities, the inequality $a_{\tau(i)} \geq a_{\tau(i+1)}$ rewrites as $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$. Thus, (6.2.14) is proven in Case 1.

Similarly, we can show (6.2.14) in Case 4 (observing that $(uv)\left[I_{\tau(i)}\right] = b_{\tau(i)-p}$ and $(uv)\left[I_{\tau(i+1)}\right] = b_{\tau(i+1)-p}$ in this case).

Let us now consider Case 2. In this case, we have $\tau(i) \in \{1, 2, \ldots, p\}$ and $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$. From $\tau(i) \in \{1, 2, \ldots, p\}$, we conclude that $I_{\tau(i)} \subset [0:n]^+$. From $\tau(i+1) \in \{p+1, p+2, \ldots, p+q\}$, we conclude that $I_{\tau(i+1)} \subset [n:n+m]^+$. The intervals $I_{\tau(i)}$ and $I_{\tau(i+1)}$ are clearly nonempty.

Proposition 6.2.14(d) (applied to $n+m$, $\alpha\beta$, $p+q$ and $(I_1, I_2, \ldots, I_{p+q})$ instead of n, α, ℓ and $(I_1, I_2, \ldots, I_\ell)$) yields that the sets $\sigma^{-1}\left(I_{\tau(i)}\right)$, $\sigma^{-1}\left(I_{\tau(i+1)}\right)$ and $\sigma^{-1}\left(I_{\tau(i)}\right) \cup \sigma^{-1}\left(I_{\tau(i+1)}\right)$ are nonempty intervals, and that we have $\sigma^{-1}\left(I_{\tau(i)}\right) < \sigma^{-1}\left(I_{\tau(i+1)}\right)$. Hence, Lemma 6.2.10(b) (applied to $I = I_{\tau(i)}$ and $J = I_{\tau(i+1)}$) yields

$$(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right].$$

But $(uv)\left[I_{\tau(i)}\right]$ and $(uv)\left[I_{\tau(i+1)}\right]$ are Lyndon words (as a consequence of (6.2.5)). Thus, Proposition 6.1.18 (applied to $(uv)\left[I_{\tau(i)}\right]$ and $(uv)\left[I_{\tau(i+1)}\right]$ instead of u and v) shows that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$ if and only if $(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right]$. Since we know that $(uv)\left[I_{\tau(i)}\right] \cdot (uv)\left[I_{\tau(i+1)}\right] \geq (uv)\left[I_{\tau(i+1)}\right] \cdot (uv)\left[I_{\tau(i)}\right]$ holds, we thus conclude that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$. Thus, (6.2.14) is proven in Case 2.

The proof of (6.2.14) in Case 3 is analogous to that in Case 2 (the main difference being that Lemma 6.2.10(c) is used in lieu of Lemma 6.2.10(b)).

Thus, (6.2.14) is proven in all possible cases. So we always have (6.2.14). In other words, $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$.

Now, forget that we fixed i. We hence have shown that $(uv)\left[I_{\tau(i)}\right] \geq (uv)\left[I_{\tau(i+1)}\right]$ for all $i \in \{1, 2, \ldots, p+q-1\}$. This proves (6.2.13), and thus completes our proof of Theorem 6.2.22(b).

(a) Let $\tau \in \mathrm{Sh}_{p,q}$ be such that

$$(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.15}$$

Set $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Then, Proposition 6.2.18 yields that $\tau \in \mathrm{Sh}_{p,q}$ if and only if $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$. Since we know that $\tau \in \mathrm{Sh}_{p,q}$, we can deduce from this that $\operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$, so that $\sigma = \operatorname{iper}(\alpha\beta, \tau) \in \mathrm{Sh}_{n,m}$.

It remains to prove that the word $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$.

[307] *Proof.* Assume the contrary. Then, $\tau(i) \geq \tau(i+1)$. Since both $\tau(i)$ and $\tau(i+1)$ belong to $\{1, 2, \ldots, p\} = [0:p]^+$, this yields $\tau^{-1}(\tau(i)) \geq \tau^{-1}(\tau(i+1))$ (since the restriction of the map τ^{-1} to the interval $[0:p]^+$ is strictly increasing), which contradicts $\tau^{-1}(\tau(i)) = i < i+1 = \tau^{-1}(\tau(i+1))$. This contradiction proves the assumption wrong, qed.

It is clear that the multiset $u \sqcup\!\sqcup v$ has **some** lexicographically highest element. This element has the form $u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v$ for some $\widetilde{\sigma} \in \mathrm{Sh}_{n,m}$ (because any element of this multiset has such a form). Consider this $\widetilde{\sigma}$. Theorem 6.2.22(b) (applied to $\widetilde{\sigma}$ instead of σ) yields that there exists a unique permutation $\widetilde{\tau} \in \mathrm{Sh}_{p,q}$ satisfying $(uv)\left[I_{\widetilde{\tau}(1)}\right] \geq (uv)\left[I_{\widetilde{\tau}(2)}\right] \geq \cdots \geq (uv)\left[I_{\widetilde{\tau}(p+q)}\right]$ and $\widetilde{\sigma} = \mathrm{iper}\left(\alpha\beta, \widetilde{\tau}\right)$. (What we call $\widetilde{\tau}$ here is what has been called τ in Theorem 6.2.22(b).)

Now, the chain of inequalities $(uv)\left[I_{\widetilde{\tau}(1)}\right] \geq (uv)\left[I_{\widetilde{\tau}(2)}\right] \geq \cdots \geq (uv)\left[I_{\widetilde{\tau}(p+q)}\right]$ shows that the list $\left((uv)\left[I_{\widetilde{\tau}(1)}\right], (uv)\left[I_{\widetilde{\tau}(2)}\right], \ldots, (uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right)$ is the result of sorting the list $\left((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}]\right)$ in decreasing order. But the chain of inequalities (6.2.15) shows that the list $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting the same list $\left((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}]\right)$ in decreasing order. So each of the two lists $\left((uv)\left[I_{\widetilde{\tau}(1)}\right], (uv)\left[I_{\widetilde{\tau}(2)}\right], \ldots, (uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right)$ and $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting one and the same list $\left((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}]\right)$ in decreasing order. Since the result of sorting a given list in decreasing order is unique, this yields

$$\left((uv)\left[I_{\widetilde{\tau}(1)}\right], (uv)\left[I_{\widetilde{\tau}(2)}\right], \ldots, (uv)\left[I_{\widetilde{\tau}(p+q)}\right]\right) = \left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right).$$

Hence,

$$(uv)\left[I_{\widetilde{\tau}(1)}\right] \cdot (uv)\left[I_{\widetilde{\tau}(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\widetilde{\tau}(p+q)}\right] = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.16}$$

But Lemma 6.2.20 yields

$$u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right]. \tag{6.2.17}$$

Meanwhile, Lemma 6.2.20 (applied to $\widetilde{\tau}$ and $\widetilde{\sigma}$ instead of τ and σ) yields

$$\begin{aligned} u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v &= (uv)\left[I_{\widetilde{\tau}(1)}\right] \cdot (uv)\left[I_{\widetilde{\tau}(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\widetilde{\tau}(p+q)}\right] \\ &= (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right] \qquad \text{(by (6.2.16))} \\ &= u \underset{\sigma}{\sqcup\!\sqcup} v \qquad \text{(by (6.2.17))}. \end{aligned}$$

Thus, $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ (since we know that $u \underset{\widetilde{\sigma}}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$). This proves Theorem 6.2.22(a). □

Now, in order to prove Theorem 6.2.2, we record a very simple fact about counting shuffles:

Proposition 6.2.23. *Let $p \in \mathbb{N}$ and $q \in \mathbb{N}$. Let $\mathfrak{W}$ be a totally ordered set, and let $h : \{1, 2, \ldots, p+q\} \to \mathfrak{W}$ be a map. Assume that $h(1) \geq h(2) \geq \cdots \geq h(p)$ and $h(p+1) \geq h(p+2) \geq \cdots \geq h(p+q)$.*

For every $w \in \mathfrak{W}$, let $\mathfrak{a}(w)$ denote the number of all $i \in \{1, 2, \ldots, p\}$ satisfying $h(i) = w$, and let $\mathfrak{b}(w)$ denote the number of all $i \in \{p+1, p+2, \ldots, p+q\}$ satisfying $h(i) = w$.

Then, the number of $\tau \in \mathrm{Sh}_{p,q}$ satisfying $h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))$ is $\prod_{w \in \mathfrak{W}} \dbinom{\mathfrak{a}(w) + \mathfrak{b}(w)}{\mathfrak{a}(w)}$.

(Of course, all but finitely many factors of this product are 1.)

Exercise 6.2.24. Prove Proposition 6.2.23.

Proof of Theorem 6.2.2. Let $n = \ell(u)$ and $m = \ell(v)$. Define α, β and $(I_1, I_2, \ldots, I_{p+q})$ as in Theorem 6.2.22.

Since $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of u, we have $a_1 \geq a_2 \geq \cdots \geq a_p$ and $a_1 a_2 \cdots a_p = u$. Similarly, $b_1 \geq b_2 \geq \cdots \geq b_q$ and $b_1 b_2 \cdots b_q = v$.

From (6.2.3), we see that $(uv)[I_i] = a_i$ for every $i \in \{1, 2, \ldots, p\}$. From (6.2.4), we see that $(uv)[I_i] = b_{i-p}$ for every $i \in \{p+1, p+2, \ldots, p+q\}$. Combining these two equalities, we obtain

$$(uv)[I_i] = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} \qquad \text{for every } i \in \{1, 2, \ldots, p+q\}. \tag{6.2.18}$$

In other words,

$$\left((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}]\right) = (a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q). \tag{6.2.19}$$

(a) Let z be the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. We must prove that $z = c_1 c_2 \cdots c_{p+q}$.

Since $z \in u \sqcup\!\sqcup v$, we can write z in the form $u \underset{\sigma}{\sqcup\!\sqcup} v$ for some $\sigma \in \mathrm{Sh}_{n,m}$ (since we can write any element of $u \sqcup\!\sqcup v$ in this form). Consider this σ. Then, $u \underset{\sigma}{\sqcup\!\sqcup} v = z$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Hence, Theorem 6.2.22(b) yields that there exists a unique permutation $\tau \in \mathrm{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$ and $\sigma = \operatorname{iper}(\alpha\beta, \tau)$. Consider this τ.

Now, $\tau \in \mathrm{Sh}_{p,q} \subset \mathfrak{S}_{p+q}$ is a permutation, and thus the list $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is a rearrangement of the list $((uv)[I_1], (uv)[I_2], \ldots, (uv)[I_{p+q}])$. Due to (6.2.19), this rewrites as follows: The list $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is a rearrangement of the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$. Hence, $\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right)$ is the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order (since $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$). But since the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order is $(c_1, c_2, \ldots, c_{p+q})$, this becomes

$$\left((uv)\left[I_{\tau(1)}\right], (uv)\left[I_{\tau(2)}\right], \ldots, (uv)\left[I_{\tau(p+q)}\right]\right) = (c_1, c_2, \ldots, c_{p+q}).$$

Hence,

$$(uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right] = c_1 \cdot c_2 \cdot \cdots \cdot c_{p+q}.$$

But Lemma 6.2.20 yields

$$u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right].$$

Altogether, we have

$$z = u \underset{\sigma}{\sqcup\!\sqcup} v = (uv)\left[I_{\tau(1)}\right] \cdot (uv)\left[I_{\tau(2)}\right] \cdot \cdots \cdot (uv)\left[I_{\tau(p+q)}\right] = c_1 \cdot c_2 \cdot \cdots \cdot c_{p+q} = c_1 c_2 \cdots c_{p+q}.$$

This proves Theorem 6.2.2(a).

(b) Recall that $u \sqcup\!\sqcup v = \left\{u \underset{\sigma}{\sqcup\!\sqcup} v \ : \ \sigma \in \mathrm{Sh}_{n,m}\right\}_{\text{multiset}}$. Hence,

$$\begin{aligned}
&(\text{the multiplicity with which the lexicographically highest element of the multiset} \\
&\qquad u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v) \\
&= \Big(\text{the number of all } \sigma \in \mathrm{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the} \\
&\qquad \text{lexicographically highest element of the multiset } u \sqcup\!\sqcup v\Big).
\end{aligned}$$

However, for a given $\sigma \in \mathrm{Sh}_{n,m}$, we know that $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ if and only if σ can be written in the form $\sigma = \operatorname{iper}(\alpha\beta, \tau)$ for some $\tau \in \mathrm{Sh}_{p,q}$ satisfying $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$. [308] Hence,

$$\begin{aligned}
&\Big(\text{the number of all } \sigma \in \mathrm{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the} \\
&\qquad \text{lexicographically highest element of the multiset } u \sqcup\!\sqcup v\Big) \\
&= (\text{the number of all } \sigma \in \mathrm{Sh}_{n,m} \text{ which can be written in the form } \sigma = \operatorname{iper}(\alpha\beta, \tau) \\
&\qquad \text{for some } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]) \\
&= \Big(\text{the number of all } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]\Big)
\end{aligned}$$

[308] In fact, the "if" part of this assertion follows from Theorem 6.2.22(a), whereas its "only if" part follows from Theorem 6.2.22(b).

(because if a $\sigma \in \mathrm{Sh}_{n,m}$ can be written in the form $\sigma = \mathrm{iper}\left(\alpha\beta, \tau\right)$ for some $\tau \in \mathrm{Sh}_{p,q}$ satisfying $\left(uv\right)\left[I_{\tau(1)}\right] \geq \left(uv\right)\left[I_{\tau(2)}\right] \geq \cdots \geq \left(uv\right)\left[I_{\tau(p+q)}\right]$, then σ can be written **uniquely** in this form[309]). Thus,

$$\begin{aligned}
&\left(\text{the multiplicity with which the lexicographically highest element of the multiset } u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v\right) \\
&= \Big(\text{the number of all } \sigma \in \mathrm{Sh}_{n,m} \text{ such that } u \underset{\sigma}{\sqcup\!\sqcup} v \text{ is the lexicographically highest element of the multiset } u \sqcup\!\sqcup v\Big) \\
&= \left(\text{the number of all } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } \left(uv\right)\left[I_{\tau(1)}\right] \geq \left(uv\right)\left[I_{\tau(2)}\right] \geq \cdots \geq \left(uv\right)\left[I_{\tau(p+q)}\right]\right). \qquad (6.2.20)
\end{aligned}$$

Now, define a map $h : \{1, 2, \ldots, p+q\} \to \mathfrak{L}$ by

$$h\left(i\right) = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} \qquad \text{for every } i \in \{1, 2, \ldots, p+q\}.$$

Then, $h\left(1\right) \geq h\left(2\right) \geq \cdots \geq h\left(p\right)$ (because this is just a rewriting of $a_1 \geq a_2 \geq \cdots \geq a_p$) and $h\left(p+1\right) \geq h\left(p+2\right) \geq \cdots \geq h\left(p+q\right)$ (since this is just a rewriting of $b_1 \geq b_2 \geq \cdots \geq b_q$). For every $w \in \mathfrak{L}$, the number of all $i \in \{1, 2, \ldots, p\}$ satisfying $h\left(i\right) = w$ is

$$\begin{aligned}
&\left|\left\{ i \in \{1, 2, \ldots, p\} \mid \underbrace{h\left(i\right)}_{=a_i} = w \right\}\right| \\
&= \left|\left\{ i \in \{1, 2, \ldots, p\} \mid a_i = w \right\}\right| \\
&= \left(\text{the number of terms in the list } \left(a_1, a_2, \ldots, a_p\right) \text{ which are equal to } w\right) \\
&= \left(\text{the number of terms in the CFL factorization of } u \text{ which are equal to } w\right) \\
&\qquad \left(\text{since the list } \left(a_1, a_2, \ldots, a_p\right) \text{ is the CFL factorization of } u\right) \\
&= \mathrm{mult}_w\, u
\end{aligned}$$

(because $\mathrm{mult}_w\, u$ is defined as the number of terms in the CFL factorization of u which are equal to w). Similarly, for every $w \in \mathfrak{L}$, the number of all $i \in \{p+1, p+2, \ldots, p+q\}$ satisfying $h\left(i\right) = w$ equals $\mathrm{mult}_w\, v$. Thus, we can apply Proposition 6.2.23 to $\mathfrak{W} = \mathfrak{L}$, $\mathfrak{a}\left(w\right) = \mathrm{mult}_w\, u$ and $\mathfrak{b}\left(w\right) = \mathrm{mult}_w\, v$. As a result, we see that the number of $\tau \in \mathrm{Sh}_{p,q}$ satisfying $h\left(\tau\left(1\right)\right) \geq h\left(\tau\left(2\right)\right) \geq \cdots \geq h\left(\tau\left(p+q\right)\right)$ is $\prod_{w \in \mathfrak{L}} \binom{\mathrm{mult}_w\, u + \mathrm{mult}_w\, v}{\mathrm{mult}_w\, u}$. In other words,

$$\begin{aligned}
&\left(\text{the number of all } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } h\left(\tau\left(1\right)\right) \geq h\left(\tau\left(2\right)\right) \geq \cdots \geq h\left(\tau\left(p+q\right)\right)\right) \\
&= \prod_{w \in \mathfrak{L}} \binom{\mathrm{mult}_w\, u + \mathrm{mult}_w\, v}{\mathrm{mult}_w\, u}. \qquad (6.2.21)
\end{aligned}$$

However, for every $i \in \{1, 2, \ldots, p+q\}$, we have

$$h\left(i\right) = \begin{cases} a_i, & \text{if } i \leq p; \\ b_{i-p}, & \text{if } i > p \end{cases} = \left(uv\right)\left[I_i\right] \qquad \left(\text{by (6.2.18)}\right).$$

[309] *Proof.* Let $\sigma \in \mathrm{Sh}_{n,m}$ be such that σ can be written in the form $\sigma = \mathrm{iper}\left(\alpha\beta, \tau\right)$ for some $\tau \in \mathrm{Sh}_{p,q}$ satisfying $\left(uv\right)\left[I_{\tau(1)}\right] \geq \left(uv\right)\left[I_{\tau(2)}\right] \geq \cdots \geq \left(uv\right)\left[I_{\tau(p+q)}\right]$. Then, the word $u \underset{\sigma}{\sqcup\!\sqcup} v$ is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ (according to Theorem 6.2.22(a)). Hence, there exists a unique permutation $\tau \in \mathrm{Sh}_{p,q}$ satisfying $\left(uv\right)\left[I_{\tau(1)}\right] \geq \left(uv\right)\left[I_{\tau(2)}\right] \geq \cdots \geq \left(uv\right)\left[I_{\tau(p+q)}\right]$ and $\sigma = \mathrm{iper}\left(\alpha\beta, \tau\right)$ (according to Theorem 6.2.22(b)). In other words, σ can be written **uniquely** in the form $\sigma = \mathrm{iper}\left(\alpha\beta, \tau\right)$ for some $\tau \in \mathrm{Sh}_{p,q}$ satisfying $\left(uv\right)\left[I_{\tau(1)}\right] \geq \left(uv\right)\left[I_{\tau(2)}\right] \geq \cdots \geq \left(uv\right)\left[I_{\tau(p+q)}\right]$, qed.

Hence, for any $\tau \in \mathrm{Sh}_{p,q}$, the condition $h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))$ is equivalent to $(uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]$. Thus,

$$\begin{aligned}
&\left(\text{the number of all } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } \underbrace{h(\tau(1)) \geq h(\tau(2)) \geq \cdots \geq h(\tau(p+q))}_{\substack{\text{this is equivalent to} \\ (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]}}\right) \\
&= \left(\text{the number of all } \tau \in \mathrm{Sh}_{p,q} \text{ satisfying } (uv)\left[I_{\tau(1)}\right] \geq (uv)\left[I_{\tau(2)}\right] \geq \cdots \geq (uv)\left[I_{\tau(p+q)}\right]\right) \\
&= (\text{the multiplicity with which the lexicographically highest element of the multiset} \\
&\qquad u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v)
\end{aligned}$$

(by (6.2.20)). Compared with (6.2.21), this yields

$$\begin{aligned}
&(\text{the multiplicity with which the lexicographically highest element of the multiset} \\
&\qquad u \sqcup\!\sqcup v \text{ appears in the multiset } u \sqcup\!\sqcup v) \\
&= \prod_{w \in \mathfrak{L}} \binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u}.
\end{aligned}$$

This proves Theorem 6.2.2(b).

(c) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Assume that $a_i \geq b_j$ for every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,q\}$. This, combined with $a_1 \geq a_2 \geq \cdots \geq a_p$ and $b_1 \geq b_2 \geq \cdots \geq b_q$, yields that $a_1 \geq a_2 \geq \cdots \geq a_p \geq b_1 \geq b_2 \geq \cdots \geq b_q$. Thus, the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ is weakly decreasing. Thus, the result of sorting the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ in decreasing order is the list $(a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$ itself. But since this result is $(c_1, c_2, \ldots, c_{p+q})$, this shows that $(c_1, c_2, \ldots, c_{p+q}) = (a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q)$. Hence, $c_1 c_2 \cdots c_{p+q} = \underbrace{a_1 a_2 \cdots a_p}_{=u} \underbrace{b_1 b_2 \cdots b_q}_{=v} = uv$. Now, Theorem 6.2.2(a) yields that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $c_1 c_2 \cdots c_{p+q} = uv$. This proves Theorem 6.2.2(c).

(d) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Assume that $a_i > b_j$ for every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,q\}$. Thus, $a_i \geq b_j$ for every $i \in \{1,2,\ldots,p\}$ and $j \in \{1,2,\ldots,q\}$. Hence, Theorem 6.2.2(c) yields that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is uv. Therefore, Theorem 6.2.2(b) shows that the multiplicity with which this word uv appears in the multiset $u \sqcup\!\sqcup v$ is $\prod_{w \in \mathfrak{L}} \binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u}$.

Now, every $w \in \mathfrak{L}$ satisfies $\binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u} = 1$ [310]. Thus, as we know, the multiplicity with which this word uv appears in the multiset $u \sqcup\!\sqcup v$ is $\prod_{w \in \mathfrak{L}} \underbrace{\binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u}}_{=1} = \prod_{w \in \mathfrak{L}} 1 = 1$. This proves Theorem 6.2.2(d).

(e) We shall use the notations of Theorem 6.2.2(a) and Theorem 6.2.2(b).

Since u is a Lyndon word, the 1-tuple (u) is the CFL factorization of u. Hence, we can apply Theorem 6.2.2(c) to 1 and (u) instead of p and $(a_1, a_2, \ldots, a_p)$. As a result, we conclude that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is uv. It remains to prove that the multiplicity with which this word uv appears in the multiset $u \sqcup\!\sqcup v$ is $\mathrm{mult}_u v + 1$.

---

[310] *Proof.* Assume the contrary. Then, there exists at least one $w \in \mathfrak{L}$ such that $\binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u} \neq 1$. Consider this w. Both $\mathrm{mult}_w u$ and $\mathrm{mult}_w v$ must be positive (since $\binom{\mathrm{mult}_w u + \mathrm{mult}_w v}{\mathrm{mult}_w u} \neq 1$). Since $\mathrm{mult}_w u$ is positive, there must be at least one term in the CFL factorization of u which is equal to w. In other words, there is at least one $i \in \{1,2,\ldots,p\}$ satisfying $a_i = w$ (since $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of u). Similarly, there is at least one $j \in \{1,2,\ldots,q\}$ satisfying $b_j = w$. These i and j satisfy $a_i = w = b_j$, which contradicts $a_i > b_j$. This contradiction shows that our assumption was false, qed.

For every $w \in \mathfrak{L}$ satisfying $w \neq u$, we have

$$\operatorname{mult}_w u = 0 \tag{6.2.22}$$

[311]. Also, $\operatorname{mult}_u u = 1$ (for a similar reason). But uv is the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$. Hence, the multiplicity with which the word uv appears in the multiset $u \sqcup\!\sqcup v$ is the multiplicity with which the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ appears in the multiset $u \sqcup\!\sqcup v$. According to Theorem 6.2.2(b), the latter multiplicity is

$$\begin{aligned}
&\prod_{w \in \mathfrak{L}} \binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u} \\
&= \underbrace{\binom{\operatorname{mult}_u u + \operatorname{mult}_u v}{\operatorname{mult}_u u}}_{\substack{= \binom{1 + \operatorname{mult}_u v}{1} \\ (\text{since } \operatorname{mult}_u u = 1)}} \cdot \prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} \underbrace{\binom{\operatorname{mult}_w u + \operatorname{mult}_w v}{\operatorname{mult}_w u}}_{\substack{= \binom{0 + \operatorname{mult}_w v}{0} \\ (\text{since } \operatorname{mult}_w u = 0 \text{ (by (6.2.22))})}} \qquad (\text{since } u \in \mathfrak{L}) \\
&= \underbrace{\binom{1 + \operatorname{mult}_u v}{1}}_{= 1 + \operatorname{mult}_u v = \operatorname{mult}_u v + 1} \cdot \prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} \underbrace{\binom{0 + \operatorname{mult}_w v}{0}}_{=1} = (\operatorname{mult}_u v + 1) \cdot \underbrace{\prod_{\substack{w \in \mathfrak{L}; \\ w \neq u}} 1}_{=1} = \operatorname{mult}_u v + 1.
\end{aligned}$$

This proves Theorem 6.2.2(e). □

As an application of our preceding results, we can prove a further necessary and sufficient criterion for a word to be Lyndon; this criterion is due to Chen/Fox/Lyndon [38, $\mathfrak{A}'' = \mathfrak{A}''''$]:

Exercise 6.2.25. Let $w \in \mathfrak{A}^*$ be a nonempty word. Prove that w is Lyndon if and only if for any two nonempty words $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ satisfying $w = uv$, there exists at least one $s \in u \sqcup\!\sqcup v$ satisfying $s > w$.

6.3. **Radford's theorem on the shuffle algebra.** We recall that our goal in Chapter 6 is to exhibit an algebraically independent generating set of the $\mathbf{k}$-algebra QSym. Having the notion of Lyndon words – which will, to some extent, but not literally, parametrize this generating set – in place, we could start the construction of this generating set immediately. However, it might come off as rather unmotivated this way, and so we begin with some warmups. First, we shall prove Radford's theorem on the shuffle algebra.

Definition 6.3.1. A *polynomial algebra* will mean a $\mathbf{k}$-algebra which is isomorphic to the polynomial ring $\mathbf{k}[x_i \mid i \in I]$ as a $\mathbf{k}$-algebra (for some indexing set I). Note that I need not be finite.

Equivalently, a polynomial algebra can be defined as a $\mathbf{k}$-algebra which has an algebraically independent (over $\mathbf{k}$) generating set. Yet equivalently, a polynomial algebra can be defined as a $\mathbf{k}$-algebra which is isomorphic to the symmetric algebra of a free $\mathbf{k}$-module.

Keep in mind that when we say that a certain bialgebra A is a polynomial algebra, we are making no statement about the coalgebra structure on A. The isomorphism from A to the symmetric algebra of a free $\mathbf{k}$-module need not be a coalgebra isomorphism, and the algebraically independent generating set of A need not consist of primitives. Thus, showing that a bialgebra A is a polynomial algebra does not trivialize the study of its bialgebraic structure.

Remark 6.3.2. Let V be a $\mathbf{k}$-module, and let $\mathfrak{A}$ be a totally ordered set. Let b_a be an element of V for every $a \in \mathfrak{A}$. Consider the shuffle algebra $\operatorname{Sh}(V)$ (defined in Definition 1.6.7).

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element b_w of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where ℓ is the length of w. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.)

Let $u \in \mathfrak{A}^*$ and $v \in \mathfrak{A}^*$ be two words over the alphabet $\mathfrak{A}$. Let $n = \ell(u)$ and $m = \ell(v)$. Then,

$$b_u \sqcup\!\sqcup b_v = \sum_{\sigma \in \operatorname{Sh}_{n,m}} b_{u \underset{\sigma}{\sqcup\!\sqcup} v}.$$

[311] *Proof of (6.2.22):* Let $w \in \mathfrak{L}$ be such that $w \neq u$. Then, the number of terms in the list (u) which are equal to w is 0. Since (u) is the CFL factorization of u, this rewrites as follows: The number of terms in the CFL factorization of u which are equal to w is 0. In other words, $\operatorname{mult}_w u = 0$. This proves (6.2.22).

Exercise 6.3.3. Prove Remark 6.3.2.

[**Hint:** This follows from the definition of $\sqcup\!\sqcup$.]

We can now state Radford's theorem [177, Theorem 3.1.1(e)]:

Theorem 6.3.4. *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let V be a free $\mathbf{k}$-module with a basis $(b_a)_{a\in\mathfrak{A}}$, where $\mathfrak{A}$ is a totally ordered set. Then, the shuffle algebra $\operatorname{Sh}(V)$ (defined in Definition 1.6.7) is a polynomial $\mathbf{k}$-algebra. An algebraically independent generating set of $\operatorname{Sh}(V)$ can be constructed as follows:*

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element b_w of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where ℓ is the length of w. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.) Let $\mathfrak{L}$ denote the set of all Lyndon words over the alphabet $\mathfrak{A}$. Then, $(b_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$.

Example 6.3.5. For this example, let $\mathfrak{A}$ be the alphabet $\{1,2,3,\ldots\}$ with total order given by $1<2<3<\cdots$, and assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let V be the free $\mathbf{k}$-module with basis $(b_a)_{a\in\mathfrak{A}}$. We use the notations of Theorem 6.3.4. Then, Theorem 6.3.4 yields that $(b_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$. Here are some examples of elements of $\operatorname{Sh}(V)$ written as polynomials in this generating set:

$$\begin{aligned}
b_{12} &= b_{12} \qquad \text{(the word 12 itself is Lyndon)};\\
b_{21} &= b_1 \sqcup\!\sqcup b_2 - b_{12};\\
b_{11} &= \frac{1}{2} b_1 \sqcup\!\sqcup b_1;\\
b_{123} &= b_{123} \qquad \text{(the word 123 itself is Lyndon)};\\
b_{132} &= b_{132} \qquad \text{(the word 132 itself is Lyndon)};\\
b_{213} &= b_2 \sqcup\!\sqcup b_{13} - b_{123} - b_{132};\\
b_{231} &= b_{23} \sqcup\!\sqcup b_1 - b_2 \sqcup\!\sqcup b_{13} + b_{132};\\
b_{312} &= b_3 \sqcup\!\sqcup b_{12} - b_{123} - b_{132};\\
b_{321} &= b_1 \sqcup\!\sqcup b_2 \sqcup\!\sqcup b_3 - b_{23} \sqcup\!\sqcup b_1 - b_3 \sqcup\!\sqcup b_{12} + b_{123};\\
b_{112} &= b_{112} \qquad \text{(the word 112 itself is Lyndon)};\\
b_{121} &= b_{12} \sqcup\!\sqcup b_1 - 2b_{112};\\
b_{1212} &= \frac{1}{2} b_{12} \sqcup\!\sqcup b_{12} - 2b_{1122};\\
b_{4321} &= b_1 \sqcup\!\sqcup b_2 \sqcup\!\sqcup b_3 \sqcup\!\sqcup b_4 - b_1 \sqcup\!\sqcup b_2 \sqcup\!\sqcup b_{34} - b_1 \sqcup\!\sqcup b_{23} \sqcup\!\sqcup b_4 - b_{12} \sqcup\!\sqcup b_3 \sqcup\!\sqcup b_4\\
&\qquad + b_1 \sqcup\!\sqcup b_{234} + b_{12} \sqcup\!\sqcup b_{34} + b_{123} \sqcup\!\sqcup b_4 - b_{1234}.
\end{aligned}$$

312

Note that Theorem 6.3.4 cannot survive without the condition that $\mathbb{Q}$ be a subring of $\mathbf{k}$. For instance, for any $v \in V$, we have $v \sqcup\!\sqcup v = 2vv$ in $\operatorname{Sh}(V)$, which vanishes if $2=0$ in $\mathbf{k}$; this stands in contrast to the fact that polynomial $\mathbf{k}$-algebras are integral domains when $\mathbf{k}$ itself is one. We will see that QSym is less sensitive towards the base ring in this regard (although proving that QSym is a polynomial algebra is much easier when $\mathbb{Q}$ is a subring of $\mathbf{k}$).

[312] A pattern emerges in the formulas for b_{21}, b_{321} and b_{4321}: for every $n\in\mathbb{N}$, we have

$$b_{(n,n-1,\ldots,1)} = \sum_{\alpha\in\operatorname{Comp}_n} (-1)^{n-\ell(\alpha)}\, b_{\mathbf{d}_1(\alpha)} \sqcup\!\sqcup b_{\mathbf{d}_2(\alpha)} \sqcup\!\sqcup \cdots \sqcup\!\sqcup b_{\mathbf{d}_{\ell(\alpha)}(\alpha)},$$

where $(\mathbf{d}_1(\alpha))\cdot(\mathbf{d}_2(\alpha))\cdot\cdots\cdot(\mathbf{d}_{\ell(\alpha)}(\alpha))$ is the factorization of the word $(1,2,\ldots,n)$ into factors of length α_1, α_2, …, α_ℓ (where $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$). This can be proved by an application of Lemma 5.2.7(a) (as it is easy to see that for any composition α of n, we have

$$\begin{aligned}
b_{\mathbf{d}_1(\alpha)} \sqcup\!\sqcup b_{\mathbf{d}_2(\alpha)} \sqcup\!\sqcup \cdots \sqcup\!\sqcup b_{\mathbf{d}_{\ell(\alpha)}(\alpha)} &= \left(\text{the sum of } b_\pi \text{ for all words } \pi\in\mathfrak{S}_n \text{ satisfying } \operatorname{Des}\left(\pi^{-1}\right)\subset D(\alpha)\right)\\
&= \sum_{\substack{\beta\in\operatorname{Comp}_n;\\ \beta \text{ coarsens } \alpha}} \; \sum_{\substack{\pi\in\mathfrak{S}_n;\\ \gamma\left(\pi^{-1}\right)=\beta}} b_\pi,
\end{aligned}$$

where $\gamma\left(\pi^{-1}\right)$ denotes the composition τ of n satisfying $D(\tau)=\operatorname{Des}\left(\pi^{-1}\right)$).

Remark 6.3.6. Theorem 6.3.4 can be contrasted with the following fact: If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the shuffle algebra $\operatorname{Sh}(V)$ of **any** $\mathbf{k}$-module V (not necessarily free!) is isomorphic (as a $\mathbf{k}$-algebra) to the symmetric algebra $\operatorname{Sym}\left(\left(\ker\epsilon\right)/\left(\ker\epsilon\right)^2\right)$ (by Theorem 1.7.29(e), applied to $A = \operatorname{Sh}(V)$). This fact is closely related to Theorem 6.3.4, but neither follows from it (since Theorem 6.3.4 only considers the case of free $\mathbf{k}$-modules V) nor yields it (since this fact does not provide explicit generators for the $\mathbf{k}$-module $\left(\ker\epsilon\right)/\left(\ker\epsilon\right)^2$ and thus for the $\mathbf{k}$-algebra $\operatorname{Sh}(V)$).

In our proof of Theorem 6.3.4 (but not only there), we will use part (a) of the following lemma[313], which makes proving that certain families indexed by Lyndon words generate certain $\mathbf{k}$-algebras more comfortable:

Lemma 6.3.7. *Let A be a commutative $\mathbf{k}$-algebra. Let $\mathfrak{A}$ be a totally ordered set. Let $\mathfrak{L}$ be the set of all Lyndon words over the alphabet $\mathfrak{A}$. Let b_w be an element of A for every $w \in \mathfrak{L}$. For every word $u \in \mathfrak{A}^*$, define an element $\mathbf{b}_u$ of A by $\mathbf{b}_u = b_{a_1} b_{a_2} \cdots b_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of u.*

(a) *The family $(b_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra A if and only if the family $(\mathbf{b}_u)_{u\in\mathfrak{A}^*}$ is a basis of the $\mathbf{k}$-module A.*

(b) *The family $(b_w)_{w\in\mathfrak{L}}$ generates the $\mathbf{k}$-algebra A if and only if the family $(\mathbf{b}_u)_{u\in\mathfrak{A}^*}$ spans the $\mathbf{k}$-module A.*

(c) *Assume that the $\mathbf{k}$-algebra A is graded. Let $\operatorname{wt} : \mathfrak{A} \to \{1, 2, 3, \ldots\}$ be any map such that for every $N \in \{1, 2, 3, \ldots\}$, the set $\operatorname{wt}^{-1}(N)$ is finite.*

For every word $w \in \mathfrak{A}^*$, define an element $\operatorname{Wt}(w) \in \mathbb{N}$ by $\operatorname{Wt}(w) = \operatorname{wt}(w_1) + \operatorname{wt}(w_2) + \cdots + \operatorname{wt}(w_k)$, where k is the length of w.

Assume that for every $w \in \mathfrak{L}$, the element b_w of A is homogeneous of degree $\operatorname{Wt}(w)$.

Assume further that the $\mathbf{k}$-module A has a basis $(g_u)_{u\in\mathfrak{A}^*}$ having the property that for every $u \in \mathfrak{A}^*$, the element g_u of A is homogeneous of degree $\operatorname{Wt}(u)$.

Assume also that the family $(b_w)_{w\in\mathfrak{L}}$ generates the $\mathbf{k}$-algebra A.

Then, this family $(b_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra A.

Exercise 6.3.8. Prove Lemma 6.3.7.

[**Hint:** For (a) and (b), notice that the $\mathbf{b}_u$ are the "monomials" in the b_w. For (c), use Exercise 2.5.18(b) in every homogeneous component of A.]

The main workhorse of our proof of Theorem 6.3.4 will be the following consequence of Theorem 6.2.2(c):

Proposition 6.3.9. *Let V be a free $\mathbf{k}$-module with a basis $(b_a)_{a\in\mathfrak{A}}$, where $\mathfrak{A}$ is a totally ordered set.*

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element b_w of $\operatorname{Sh}(V)$ by $b_w = b_{w_1} b_{w_2} \cdots b_{w_\ell}$, where ℓ is the length of w. (The multiplication used here is that of $T(V)$, not that of $\operatorname{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.)

For every word $u \in \mathfrak{A}^*$, define an element $\mathbf{b}_u$ by $\mathbf{b}_u = b_{a_1} \sqcup\!\sqcup b_{a_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup b_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of u.

If $\ell \in \mathbb{N}$ and if $x \in \mathfrak{A}^\ell$ is a word, then there is a family $(\eta_{x,y})_{y\in\mathfrak{A}^\ell} \in \mathbb{N}^{\mathfrak{A}^\ell}$ of elements of $\mathbb{N}$ satisfying

$$\mathbf{b}_x = \sum_{\substack{y\in\mathfrak{A}^\ell; \\ y\leq x}} \eta_{x,y} b_y$$

and $\eta_{x,x} \neq 0$ (in $\mathbb{N}$).

Before we prove this, let us show a very simple lemma:

Lemma 6.3.10. *Let $\mathfrak{A}$ be a totally ordered set. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\sigma \in \operatorname{Sh}_{n,m}$.*

(a) If u, v and v' are three words satisfying $\ell(u) = n$, $\ell(v) = m$, $\ell(v') = m$ and $v' < v$, then $u \underset{\sigma}{\sqcup\!\sqcup} v' < u \underset{\sigma}{\sqcup\!\sqcup} v$.

(b) If u, u' and v are three words satisfying $\ell(u) = n$, $\ell(u') = n$, $\ell(v) = m$ and $u' < u$, then $u' \underset{\sigma}{\sqcup\!\sqcup} v < u \underset{\sigma}{\sqcup\!\sqcup} v$.

(c) If u, v and v' are three words satisfying $\ell(u) = n$, $\ell(v) = m$, $\ell(v') = m$ and $v' \leq v$, then $u \underset{\sigma}{\sqcup\!\sqcup} v' \leq u \underset{\sigma}{\sqcup\!\sqcup} v$.

Exercise 6.3.11. Prove Lemma 6.3.10.

[313] And in a later proof, we will also use its part (c) (which is tailored for application to QSym).

Exercise 6.3.12. Prove Proposition 6.3.9.

[**Hint:** Proceed by induction over ℓ. In the induction step, apply Theorem 6.2.2(c)[314] to $u = a_1$ and $v = a_2 a_3 \cdots a_p$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of x. Use Lemma 6.3.10 to get rid of smaller terms.]

Exercise 6.3.13. Prove Theorem 6.3.4.

[**Hint:** According to Lemma 6.3.7(a), it suffices to show that the family $(\mathbf{b}_u)_{u \in \mathfrak{A}^*}$ defined in Proposition 6.3.9 is a basis of the $\mathbf{k}$-module $\mathrm{Sh}(V)$. When $\mathfrak{A}$ is finite, the latter can be proven by triangularity using Proposition 6.3.9. Reduce the general case to that of finite $\mathfrak{A}$.]

6.4. Polynomial freeness of QSym: statement and easy parts.

Definition 6.4.1. For the rest of Section 6.4 and for Section 6.5, we introduce the following notations: We let $\mathfrak{A}$ be the totally ordered set $\{1, 2, 3, \ldots\}$ with its natural order (that is, $1 < 2 < 3 < \cdots$.) Thus, the words over $\mathfrak{A}$ are precisely the compositions. That is, $\mathfrak{A}^* = \mathrm{Comp}$. We let $\mathfrak{L}$ denote the set of all Lyndon words over $\mathfrak{A}$. These Lyndon words are also called *Lyndon compositions*.

A natural question is how many Lyndon compositions of a given size exist. While we will not use the answer, we nevertheless record it:

Exercise 6.4.2. Show that the number of Lyndon compositions of size n equals

$$\frac{1}{n} \sum_{d \mid n} \mu(d) \left(2^{n/d} - 1\right) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, 2^{n/d} - \delta_{n,1}$$

for every positive integer n (where "$\sum_{d \mid n}$" means a sum over all positive divisors of n, and where μ is the number-theoretic Möbius function).

[**Hint:** One solution is similar to the solution of Exercise 6.1.29 using CFL factorization. Another proceeds by defining a bijection between Lyndon compositions and Lyndon words over a two-letter alphabet $\{\mathbf{0}, \mathbf{1}\}$ (with $\mathbf{0} < \mathbf{1}$) which are $\neq \mathbf{1}$. [315]]

Let us now state Hazewinkel's result ([89, Theorem 8.1], [93, §6.7]) which is the main goal of Chapter 6:

Theorem 6.4.3. *The* $\mathbf{k}$*-algebra* QSym *is a polynomial algebra. It is isomorphic, as a graded* $\mathbf{k}$*-algebra, to the* $\mathbf{k}$*-algebra* $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$*. Here, the grading on* $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$ *is defined by setting* $\deg(x_w) = \sum_{i=1}^{\ell(w)} w_i$ *for every* $w \in \mathfrak{L}$*.*

We shall prove Theorem 6.4.3 in the next section (Section 6.5). But the particular case of Theorem 6.4.3 when $\mathbb{Q}$ is a subring of $\mathbf{k}$ can be proven more easily; we state it as a proposition:

Proposition 6.4.4. *Assume that* $\mathbb{Q}$ *is a subring of* $\mathbf{k}$*. Then, Theorem 6.4.3 holds.*

We will give two proofs of Proposition 6.4.4 in this Section 6.4; a third proof of Proposition 6.4.4 will immediately result from the proof of Theorem 6.4.3 in Section 6.5. (There **is** virtue in giving three different proofs, as they all construct different isomorphisms $\mathbf{k}[x_w \mid w \in \mathfrak{L}] \to \mathrm{QSym}$.)

Our first proof – originating in Malvenuto's [145, Corollaire 4.20] – can be given right away; it relies on Exercise 5.4.12:

First proof of Proposition 6.4.4. Let V be the free $\mathbf{k}$-module with basis $(\mathfrak{b}_n)_{n \in \{1,2,3,\ldots\}}$. Endow the $\mathbf{k}$-module V with a grading by assigning to each basis vector $\mathfrak{b}_n$ the degree n. Exercise 5.4.12(k) shows that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ (defined as in Proposition 1.6.7) as Hopf algebras. By being a

[314] Or Theorem 6.2.2(e), if you prefer.

[315] This bijection is obtained by restricting the bijection

$$\mathrm{Comp} \to \{w \in \{\mathbf{0}, \mathbf{1}\}^* \mid w \text{ does not start with } \mathbf{1}\},$$
$$(\alpha_1, \alpha_2, \ldots, \alpha_\ell) \mapsto \mathbf{0}\mathbf{1}^{\alpha_1 - 1}\mathbf{0}\mathbf{1}^{\alpha_2 - 1} \cdots \mathbf{0}\mathbf{1}^{\alpha_\ell - 1}$$

(where $\mathbf{0}\mathbf{1}^k$ is to be read as $\mathbf{0}\left(\mathbf{1}^k\right)$, not as $(\mathbf{0}\mathbf{1})^k$) to the set of Lyndon compositions. The idea behind this bijection is well-known in the Grothendieck-Teichmüller community: see, e.g., [94, §3.1] (and see [77, Note 5.16] for a different appearance of this idea).

bit more careful, we can obtain the slightly stronger result that QSym is isomorphic to the shuffle algebra $\mathrm{Sh}(V)$ as **graded** Hopf algebras[316]. In particular, $\mathrm{QSym} \cong \mathrm{Sh}(V)$ as graded $\mathbf{k}$-algebras.

Theorem 6.3.4 (applied to $b_a = \mathfrak{b}_a$) yields that the shuffle algebra $\mathrm{Sh}(V)$ is a polynomial $\mathbf{k}$-algebra, and that an algebraically independent generating set of $\mathrm{Sh}(V)$ can be constructed as follows:

For every word $w \in \mathfrak{A}^*$ over the alphabet $\mathfrak{A}$, let us define an element $\mathfrak{b}_w$ of $\mathrm{Sh}(V)$ by $\mathfrak{b}_w = \mathfrak{b}_{w_1} \mathfrak{b}_{w_2} \cdots \mathfrak{b}_{w_\ell}$, where ℓ is the length of w. (The multiplication used here is that of $T(V)$, not that of $\mathrm{Sh}(V)$; the latter is denoted by $\sqcup\!\sqcup$.) Then, $(\mathfrak{b}_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\mathrm{Sh}(V)$.

For every $w \in \mathfrak{A}^*$, we have $\mathfrak{b}_w = \mathfrak{b}_{w_1} \mathfrak{b}_{w_2} \cdots \mathfrak{b}_{w_{\ell(w)}}$ (by the definition of $\mathfrak{b}_w$). For every $w \in \mathfrak{A}^*$, the element $\mathfrak{b}_w = \mathfrak{b}_{w_1} \mathfrak{b}_{w_2} \cdots \mathfrak{b}_{w_{\ell(w)}}$ of $\mathrm{Sh}(V)$ is homogeneous of degree $\sum_{i=1}^{\ell(w)} \underbrace{\deg(\mathfrak{b}_{w_i})}_{=w_i} = \sum_{i=1}^{\ell(w)} w_i$.

Now, define a grading on the $\mathbf{k}$-algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$ by setting $\deg(x_w) = \sum_{i=1}^{\ell(w)} w_i$ for every $w \in \mathfrak{L}$. By the universal property of the polynomial algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$, we can define a $\mathbf{k}$-algebra homomorphism $\Phi : \mathbf{k}[x_w \mid w \in \mathfrak{L}] \to \mathrm{Sh}(V)$ by setting

$$\Phi(x_w) = \mathfrak{b}_w \qquad \text{for every } w \in \mathfrak{L}.$$

This homomorphism Φ is a $\mathbf{k}$-algebra isomorphism (since $(\mathfrak{b}_w)_{w \in \mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra $\mathrm{Sh}(V)$) and is graded (because for every $w \in \mathfrak{L}$, the element $\mathfrak{b}_w$ of $\mathrm{Sh}(V)$ is homogeneous of degree $\sum_{i=1}^{\ell(w)} w_i = \deg(x_w)$). Thus, Φ is an isomorphism of graded $\mathbf{k}$-algebras. Hence, $\mathrm{Sh}(V) \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded $\mathbf{k}$-algebras. Altogether, $\mathrm{QSym} \cong \mathrm{Sh}(V) \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded $\mathbf{k}$-algebras. Thus, QSym is a polynomial algebra. This proves Theorem 6.4.3 under the assumption that $\mathbb{Q}$ be a subring of $\mathbf{k}$. In other words, this proves Proposition 6.4.4. □

Our second proof of Proposition 6.4.4 comes from Hazewinkel/Gubareni/Kirichenko [93] (where Proposition 6.4.4 appears as [93, Theorem 6.5.13]). This proof will construct an explicit algebraically independent family generating the $\mathbf{k}$-algebra QSym. [317] The generating set will be very unsophisticated: it will be $(M_\alpha)_{\alpha \in \mathfrak{L}}$, where $\mathfrak{A}$ and $\mathfrak{L}$ are as in Theorem 6.4.3. Here, we are using the fact that words over the alphabet $\{1, 2, 3, \ldots\}$ are the same thing as compositions, so, in particular, a monomial quasisymmetric function M_α is defined for every such word α.

It takes a bit of work to show that this family indeed fits the bill. We begin with a corollary of Proposition 5.1.3 that is essentially obtained by throwing away all non-bijective maps f:

Proposition 6.4.5. *Let $\alpha \in \mathfrak{A}^*$ and $\beta \in \mathfrak{A}^*$. Then,*

$$M_\alpha M_\beta = \sum_{\gamma \in \alpha \sqcup\!\sqcup \beta} M_\gamma + (\text{a sum of terms of the form } M_\delta \text{ with } \delta \in \mathfrak{A}^* \text{ satisfying } \ell(\delta) < \ell(\alpha) + \ell(\beta)).$$

[318]

Exercise 6.4.6. Prove Proposition 6.4.5.

[**Hint:** Recall what was said about the $p = \ell + m$ case in Example 5.1.4.]

Corollary 6.4.7. *Let $\alpha \in \mathfrak{A}^*$ and $\beta \in \mathfrak{A}^*$. Then, $M_\alpha M_\beta$ is a sum of terms of the form M_δ with $\delta \in \mathfrak{A}^*$ satisfying $\ell(\delta) \leq \ell(\alpha) + \ell(\beta)$.*

Exercise 6.4.8. Prove Corollary 6.4.7.

We now define a partial order on the compositions of a given nonnegative integer:

[316] *Proof.* In the solution of Exercise 5.4.12(k), we have shown that $\mathrm{QSym} \cong T(V)^o$ as graded Hopf algebras. But Remark 1.6.9(b) shows that the Hopf algebra $T(V)^o$ is naturally isomorphic to the shuffle algebra $\mathrm{Sh}(V^o)$ as Hopf algebras; it is easy to see that the natural isomorphism $T(V)^o \to \mathrm{Sh}(V^o)$ is graded (because it is the direct sum of the isomorphisms $(V^{\otimes n})^o \to (V^o)^{\otimes n}$ over all $n \in \mathbb{N}$, and each of these isomorphisms is graded). Hence, $T(V)^o \cong \mathrm{Sh}(V^o)$ as graded Hopf algebras. But $V^o \cong V$ as graded $\mathbf{k}$-modules (since V is of finite type), and thus $\mathrm{Sh}(V^o) \cong \mathrm{Sh}(V)$ as graded Hopf algebras. Altogether, we obtain $\mathrm{QSym} \cong T(V)^o \cong \mathrm{Sh}(V^o) \cong \mathrm{Sh}(V)$ as graded Hopf algebras, qed.

[317] We could, of course, obtain such a family from our above proof as well (this is done by Malvenuto in [145, Corollaire 4.20]), but it won't be a very simple one.

[318] The sum $\sum_{\gamma \in \alpha \sqcup\!\sqcup \beta} M_\gamma$ ranges over the **multiset** $\alpha \sqcup\!\sqcup \beta$; if an element appears several times in $\alpha \sqcup\!\sqcup \beta$, then it has accordingly many addends corresponding to it.

Definition 6.4.9. Let $n \in \mathbb{N}$. We define a binary relation $\underset{\text{wll}}{\leq}$ on the set Comp_n as follows: For two compositions α and β in Comp_n, we set $\alpha \underset{\text{wll}}{\leq} \beta$ if and only if

$$\text{either } \ell(\alpha) < \ell(\beta) \text{ or } (\ell(\alpha) = \ell(\beta) \text{ and } \alpha \leq \beta \text{ in lexicographic order}).$$

This binary relation $\underset{\text{wll}}{\leq}$ is the smaller-or-equal relation of a total order on Comp_n; we refer to said total order as the *wll-order* on Comp_n, and we denote by $\underset{\text{wll}}{<}$ the smaller relation of this total order.

Notice that if α and β are two compositions satisfying $\ell(\alpha) = \ell(\beta)$, then $\alpha \leq \beta$ in lexicographic order if and only if $\alpha \leq \beta$ with respect to the relation $\leq$ defined in Definition 6.1.1.

A remark about the name "wll-order" is in order. We have taken this notation from [89, Definition 6.7.14], where it is used for an extension of this order to the whole set Comp. We will never use this extension, as we will only ever compare two compositions of the same integer.[319]

We now state a fact which is similar (and plays a similar role) to Proposition 6.3.9:

Proposition 6.4.10. *For every composition $u \in \operatorname{Comp} = \mathfrak{A}^*$, define an element $\mathbf{M}_u \in \operatorname{QSym}$ by $\mathbf{M}_u = M_{a_1} M_{a_2} \cdots M_{a_p}$, where $(a_1, a_2, \ldots, a_p)$ is the CFL factorization of the word u.*

If $n \in \mathbb{N}$ and if $x \in \operatorname{Comp}_n$, then there is a family $(\eta_{x,y})_{y \in \operatorname{Comp}_n} \in \mathbb{N}^{\operatorname{Comp}_n}$ of elements of $\mathbb{N}$ satisfying

$$\mathbf{M}_x = \sum_{\substack{y \in \operatorname{Comp}_n; \\ y \underset{\text{wll}}{\leq} x}} \eta_{x,y} M_y$$

and $\eta_{x,x} \neq 0$ (in $\mathbb{N}$).

Before we prove it, let us show the following lemma:

Lemma 6.4.11. *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \operatorname{Comp}_n$ and $v \in \operatorname{Comp}_m$. Let z be the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$.*

(a) We have $z \in \operatorname{Comp}_{n+m}$.

(b) There exists a positive integer h such that

$$M_u M_v = h M_z + \left(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} z \right).$$

(c) Let $v' \in \operatorname{Comp}_m$ be such that $v' \underset{\text{wll}}{<} v$. Then,

$$M_u M_{v'} = \left(\text{a sum of terms of the form } M_w \text{ with } w \in \operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} z \right).$$

Exercise 6.4.12. Prove Lemma 6.4.11.

[**Hint:** For (b), set h to be the multiplicity with which the word z appears in the multiset $u \sqcup\!\sqcup v$, then use Proposition 6.4.5 and notice that $M_u M_v$ is homogeneous of degree $n+m$. For (c), use (b) for v' instead of v and notice that Lemma 6.3.10(a) shows that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v'$ is $\underset{\text{wll}}{<} z$.]

Exercise 6.4.13. Prove Proposition 6.4.10.

[**Hint:** Proceed by strong induction over n. In the induction step, let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of x, and set $u = a_1$ and $v = a_2 a_3 \cdots a_p$; then apply Proposition 6.4.10 to v instead of x, and multiply the resulting equality $\mathbf{M}_v = \sum_{\substack{y \in \operatorname{Comp}_{|v|}; \\ y \underset{\text{wll}}{\leq} v}} \eta_{v,y} M_y$ with M_u to obtain an expression for $M_u \mathbf{M}_v = \mathbf{M}_x$. Use Lemma 6.4.11 to show that this expression has the form $\sum_{\substack{y \in \operatorname{Comp}_n; \\ y \underset{\text{wll}}{\leq} x}} \eta_{x,y} M_y$ with $\eta_{x,x} \neq 0$; here it helps to remember that the lexicographically highest element of the multiset $u \sqcup\!\sqcup v$ is $uv = x$ (by Theorem 6.2.2(c)).]

[319] In [89, Definition 6.7.14], the name "wll-order" is introduced as an abbreviation for "**w**eight first, then **l**ength, then **l**exicographic" (in the sense that two compositions are first compared by their weights, then, if the weights are equal, by their lengths, and finally, if the lengths are also equal, by the lexicographic order). For us, the alternative explanation "**w**ord **l**ength, then **l**exicographic" serves just as well.

We are almost ready to give our second proof of Proposition 6.4.4; our last step is the following proposition:

Proposition 6.4.14. *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Then, $(M_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra* QSym.

Exercise 6.4.15. Prove Proposition 6.4.14.

[**Hint:** Define $\mathbf{M}_u$ for every $u \in \mathrm{Comp}$ as in Proposition 6.4.10. Conclude from Proposition 6.4.10 that, for every $n \in \mathbb{N}$, the family $(\mathbf{M}_u)_{u\in\mathrm{Comp}_n}$ expands invertibly triangularly[320] (with respect to the total order $\underset{\text{wll}}{\leq}$ on Comp_n) with respect to the basis $(M_u)_{u\in\mathrm{Comp}_n}$ of QSym_n. Conclude that this family $(\mathbf{M}_u)_{u\in\mathrm{Comp}_n}$ is a basis of QSym_n itself, and so the whole family $(\mathbf{M}_u)_{u\in\mathrm{Comp}}$ is a basis of QSym. Conclude using Lemma 6.3.7(a).]

Second proof of Proposition 6.4.4. Proposition 6.4.14 yields that $(M_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym.

Define a grading on the $\mathbf{k}$-algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$ by setting $\deg(x_w) = \sum_{i=1}^{\ell(w)} w_i$ for every $w \in \mathfrak{L}$. By the universal property of the polynomial algebra $\mathbf{k}[x_w \mid w \in \mathfrak{L}]$, we can define a $\mathbf{k}$-algebra homomorphism $\Phi : \mathbf{k}[x_w \mid w \in \mathfrak{L}] \to \mathrm{QSym}$ by setting

$$\Phi(x_w) = M_w \qquad \text{for every } w \in \mathfrak{L}.$$

This homomorphism Φ is a $\mathbf{k}$-algebra isomorphism (since $(M_w)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym) and is graded (because for every $w \in \mathfrak{L}$, the element M_w of QSym is homogeneous of degree $|w| = \sum_{i=1}^{\ell(w)} w_i = \deg(x_w)$). Thus, Φ is an isomorphism of graded $\mathbf{k}$-algebras. Hence, $\mathrm{QSym} \cong \mathbf{k}[x_w \mid w \in \mathfrak{L}]$ as graded $\mathbf{k}$-algebras. In particular, this shows that QSym is a polynomial algebra. This proves Theorem 6.4.3 under the assumption that $\mathbb{Q}$ be a subring of $\mathbf{k}$. Proposition 6.4.4 is thus proven again. □

6.5. **Polynomial freeness of** QSym**: the general case.** We now will prepare for proving Theorem 6.4.3 without any assumptions on $\mathbf{k}$. In our proof, we follow [89] and [93, §6.7], but without using the language of plethysm and Frobenius maps. We start with the following definition:

Definition 6.5.1. Let α be a composition. Write α in the form $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ with $\ell = \ell(\alpha)$.

(a) Let $\mathrm{SIS}(\ell)$ denote the set of all strictly increasing ℓ-tuples $(i_1, i_2, \ldots, i_\ell)$ of positive integers.[321] For every ℓ-tuple $\mathbf{i} = (i_1, i_2, \ldots, i_\ell) \in \mathrm{SIS}(\ell)$, we denote the monomial $x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell}$ by $\mathbf{x}_{\mathbf{i}}^{\alpha}$. This $\mathbf{x}_{\mathbf{i}}^{\alpha}$ is a monomial of degree $\alpha_1 + \alpha_2 + \cdots + \alpha_\ell = |\alpha|$. Then,

$$M_\alpha = \sum_{\mathbf{i}\in\mathrm{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha}. \tag{6.5.1}$$

322

[320] See Definition 11.1.16(b) for the meaning of this.

[321] "Strictly increasing" means that $i_1 < i_2 < \cdots < i_\ell$ here. Of course, the elements of $\mathrm{SIS}(\ell)$ are in 1-to-1 correspondence with ℓ-element subsets of $\{1, 2, 3, \ldots\}$.

[322] *Proof of (6.5.1):* By the definition of M_α, we have

$$M_\alpha = \underbrace{\sum_{i_1<i_2<\cdots<i_\ell \text{ in } \{1,2,3,\ldots\}}}_{=\sum_{(i_1,i_2,\ldots,i_\ell)\in\mathrm{SIS}(\ell)}} x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell} = \sum_{(i_1,i_2,\ldots,i_\ell)\in\mathrm{SIS}(\ell)} x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell} = \sum_{\mathbf{i}=(i_1,i_2,\ldots,i_\ell)\in\mathrm{SIS}(\ell)} \underbrace{x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_\ell}^{\alpha_\ell}}_{=\mathbf{x}_{\mathbf{i}}^{\alpha}}$$
$$\text{(by the definition of } \mathbf{x}_{\mathbf{i}}^{\alpha})$$
$$= \sum_{\mathbf{i}=(i_1,i_2,\ldots,i_\ell)\in\mathrm{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha} = \sum_{\mathbf{i}\in\mathrm{SIS}(\ell)} \mathbf{x}_{\mathbf{i}}^{\alpha},$$

qed.

(b) Consider the ring $\mathbf{k}[[\mathbf{x}]]$ endowed with the coefficientwise topology[323]. The family $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$ of elements of $\mathbf{k}[[\mathbf{x}]]$ is power-summable[324]. Hence, for every $f\in\Lambda$, there is a well-defined power series $f\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}\right)\in\mathbf{k}[[\mathbf{x}]]$ obtained by "evaluating" f at $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$ [325]. In particular, for every $s\in\mathbb{Z}$, we can evaluate the symmetric function $e_s\in\Lambda$ [326] at $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$. The resulting power series $e_s\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}\right)\in\mathbf{k}[[\mathbf{x}]]$ will be denoted $M_{\alpha}^{\langle s\rangle}$. Thus,

$$M_{\alpha}^{\langle s\rangle}=e_s\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}\right).$$

The power series $M_{\alpha}^{\langle s\rangle}$ are the power series $e_s(\alpha)$ in [93]. We will shortly (in Corollary 6.5.8(a)) see that $M_{\alpha}^{\langle s\rangle}\in\mathrm{QSym}$ (although this is also easy to prove by inspection). Here are some examples of $M_{\alpha}^{\langle s\rangle}$:

---

[323]This topology is defined as follows:

We endow the ring $\mathbf{k}$ with the discrete topology. Then, we can regard the $\mathbf{k}$-module $\mathbf{k}[[\mathbf{x}]]$ as a direct product of infinitely many copies of $\mathbf{k}$ (by identifying every power series in $\mathbf{k}[[\mathbf{x}]]$ with the family of its coefficients). Hence, the product topology is a well-defined topology on $\mathbf{k}[[\mathbf{x}]]$; this topology is denoted as the *coefficientwise topology*. A sequence $(a_n)_{n\in\mathbb{N}}$ of power series converges to a power series a with respect to this topology if and only if for every monomial $\mathfrak{m}$, all sufficiently high $n\in\mathbb{N}$ satisfy

$$(\text{the coefficient of }\mathfrak{m}\text{ in }a_n)=(\text{the coefficient of }\mathfrak{m}\text{ in }a).$$

Note that this is **not** the topology obtained by taking the completion of $\mathbf{k}[x_1,x_2,x_3,\ldots]$ with respect to the standard grading (in which all x_i have degree 1). (The latter completion is actually a smaller ring than $\mathbf{k}[[\mathbf{x}]]$.)

[324]Let us define what "power-summable" means for us:

A family $(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}}$ (where $\mathbf{I}$ is some set) is said to be *finitely supported* if all but finitely many $\mathbf{i}\in\mathbf{I}$ satisfy $n_{\mathbf{i}}=0$.

If $(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}}$ is a finitely supported family, then $\sum_{\mathbf{i}\in\mathbf{I}}n_{\mathbf{i}}$ is a well-defined element of $\mathbb{N}$. If $N\in\mathbb{N}$, then a family $(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}}$ will be called $(\leq N)$-*supported* if it is finitely supported and satisfies $\sum_{\mathbf{i}\in\mathbf{I}}n_{\mathbf{i}}\leq N$.

We say that a family $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in R^{\mathbf{I}}$ of elements of a topological commutative $\mathbf{k}$-algebra R is *power-summable* if it satisfies the following property: For every $N\in\mathbb{N}$, the sum

$$\sum_{\substack{(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}};\\ (n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\text{ is }(\leq N)\text{-supported}}}\alpha_{(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}}\prod_{\mathbf{i}\in\mathbf{I}}s_{\mathbf{i}}^{n_{\mathbf{i}}}$$

converges in the topology on R for every choice of scalars $\alpha_{(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}}\in\mathbf{k}$ corresponding to all $(\leq N)$-supported $(n_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in\mathbb{N}^{\mathbf{I}}$. In our specific case, we consider $\mathbf{k}[[\mathbf{x}]]$ as a topological commutative $\mathbf{k}$-algebra, where the topology is the coefficientwise topology. The fact that the family $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$ is power-summable then can be proven as follows:

- If $\alpha\neq\varnothing$, then this fact follows from the (easily-verified) observation that every given monomial in the variables $x_1,x_2,x_3,\ldots$ can be written as a product of monomials of the form $\mathbf{x}_{\mathbf{i}}^{\alpha}$ (with $\mathbf{i}\in\mathrm{SIS}(\ell)$) in only finitely many ways.
- If $\alpha=\varnothing$, then this fact follows by noticing that $\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$ is a finite family (indeed, $\mathrm{SIS}(\ell)=\mathrm{SIS}(0)=\{()\}$), and every finite family is power-summable.

[325]Here is how this power series $f\left(\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}\right)$ is formally defined:

Let R be any topological commutative $\mathbf{k}$-algebra, and let $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in R^{\mathbf{I}}$ be any power-summable family of elements of R. Assume that the indexing set $\mathbf{I}$ is countably infinite, and fix a bijection $\mathfrak{j}:\{1,2,3,\ldots\}\to\mathbf{I}$. Let $g\in R(\mathbf{x})$ be arbitrary. Then, we can substitute $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, $s_{\mathfrak{j}(3)}$, ... for the variables x_1, x_2, x_3, ... in g, thus obtaining an infinite sum which converges in R (in fact, its convergence follows from the fact that the family $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in R^{\mathbf{I}}$ is power-summable). The value of this sum will be denoted by $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$. In general, this value depends on the choice of the bijection $\mathfrak{j}$, so the notation $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$ is unambiguous only if this bijection $\mathfrak{j}$ is chosen once and for all. However, when $g\in\Lambda$, one can easily see that the choice of $\mathfrak{j}$ has no effect on $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$.

We can still define $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$ when the set $\mathbf{I}$ is finite instead of being countably infinite. In this case, we only need to modify our above definition as follows: Instead of fixing a bijection $\mathfrak{j}:\{1,2,3,\ldots\}\to\mathbf{I}$, we now fix a bijection $\mathfrak{j}:\{1,2,\ldots,|\mathbf{I}|\}\to\mathbf{I}$, and instead of substituting $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, $s_{\mathfrak{j}(3)}$, ... for the variables x_1, x_2, x_3, ... in g, we now substitute $s_{\mathfrak{j}(1)}$, $s_{\mathfrak{j}(2)}$, ..., $s_{\mathfrak{j}(|\mathbf{I}|)}$, 0, 0, 0, ... for the variables x_1, x_2, x_3, ... in g. Again, the same observations hold as before: $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$ is independent on $\mathfrak{j}$ if $g\in\Lambda$.

Hence, $g\left((s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\right)$ is well-defined for every $g\in R(\mathbf{x})$, every countable (i.e., finite or countably infinite) set $\mathbf{I}$, every topological commutative $\mathbf{k}$-algebra R and every power-summable family $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}\in R^{\mathbf{I}}$ of elements of R, as long as a bijection $\mathfrak{j}$ is chosen. In particular, we can apply this to $g=f$, $\mathbf{I}=\mathrm{SIS}(\ell)$, $R=\mathbf{k}[[\mathbf{x}]]$ and $(s_{\mathbf{i}})_{\mathbf{i}\in\mathbf{I}}=\left(\mathbf{x}_{\mathbf{i}}^{\alpha}\right)_{\mathbf{i}\in\mathrm{SIS}(\ell)}$, choosing $\mathfrak{j}$ to be the bijection which sends every positive integer k to the k-th smallest element of $\mathrm{SIS}(\ell)$ in the lexicographic order. (Of course, since $f\in\Lambda$, the choice of $\mathfrak{j}$ is irrelevant.)

[326]Recall that $e_0=1$, and that $e_s=0$ for $s<0$.

Example 6.5.2. If α is a composition and ℓ denotes its length $\ell(\alpha)$, then

$$M_\alpha^{\langle 0\rangle} = \underbrace{e_0}_{=1}\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = 1\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = 1$$

and

$$M_\alpha^{\langle 1\rangle} = e_1\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = \sum_{\mathbf{i}\in \mathrm{SIS}(\ell)} \mathbf{x}_\mathbf{i}^\alpha = M_\alpha \qquad \text{(by (6.5.1))}$$

and[327]

$$M_\alpha^{\langle 2\rangle} = e_2\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = \sum_{\substack{\mathbf{i}\in \mathrm{SIS}(\ell),\ \mathbf{j}\in \mathrm{SIS}(\ell);\\ \mathbf{i}<\mathbf{j}}} \mathbf{x}_\mathbf{i}^\alpha \mathbf{x}_\mathbf{j}^\alpha$$

(where the notation "$\mathbf{i}<\mathbf{j}$" should be interpreted with respect to an arbitrary but fixed total order on the set $\mathrm{SIS}(\ell)$ – for example, the lexicographic order). Applying the last of these three equalities to $\alpha=(2,1)$, we obtain

$$\begin{aligned}
M_{(2,1)}^{\langle 2\rangle} &= \sum_{\substack{\mathbf{i}\in \mathrm{SIS}(2),\ \mathbf{j}\in \mathrm{SIS}(2),\\ \mathbf{i}<\mathbf{j}}} \mathbf{x}_\mathbf{i}^{(2,1)}\mathbf{x}_\mathbf{j}^{(2,1)} = \sum_{\substack{(i_1,i_2)\in \mathrm{SIS}(2),\ (j_1,j_2)\in \mathrm{SIS}(2);\\ (i_1,i_2)<(j_1,j_2)}} \underbrace{\mathbf{x}_{(i_1,i_2)}^{(2,1)}}_{=x_{i_1}^2x_{i_2}^1}\underbrace{\mathbf{x}_{(j_1,j_2)}^{(2,1)}}_{=x_{j_1}^2x_{j_2}^1} \\
&= \sum_{\substack{(i_1,i_2)\in \mathrm{SIS}(2),\ (j_1,j_2)\in \mathrm{SIS}(2);\\ (i_1,i_2)<(j_1,j_2)}} x_{i_1}^2x_{i_2}^1x_{j_1}^2x_{j_2}^1 \\
&= \underbrace{\sum_{\substack{i_1<i_2;\ j_1<j_2;\\ i_1<j_1}} x_{i_1}^2x_{i_2}^1x_{j_1}^2x_{j_2}^1}_{=M_{(2,1,2,1)}+M_{(2,3,1)}+2M_{(2,2,1,1)}+M_{(2,2,2)}} + \underbrace{\sum_{\substack{i_1<i_2;\ j_1<j_2;\\ i_1=j_1;\ i_2<j_2}} x_{i_1}^2x_{i_2}^1x_{j_1}^2x_{j_2}^1}_{=M_{(4,1,1)}} \\
&\qquad \text{(here, we have WLOG assumed that the order on } \mathrm{SIS}(2) \text{ is lexicographic)} \\
&= M_{(2,1,2,1)}+M_{(2,3,1)}+2M_{(2,2,1,1)}+M_{(2,2,2)}+M_{(4,1,1)}.
\end{aligned}$$

Of course, every negative integer s satisfies $M_\alpha^{\langle s\rangle} = \underbrace{e_s}_{=0}\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = 0$.

There is a determinantal formula for the $s!M_\alpha^{\langle s\rangle}$ (and thus also for $M_\alpha^{\langle s\rangle}$ when $s!$ is invertible in $\mathbf{k}$), but in order to state it, we need to introduce one more notation:

Definition 6.5.3. Let $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$ be a composition, and let k be a positive integer. Then, $\alpha\{k\}$ will denote the composition $(k\alpha_1,k\alpha_2,\ldots,k\alpha_\ell)$. Clearly, $\ell(\alpha\{k\})=\ell(\alpha)$ and $|\alpha\{k\}|=k|\alpha|$.

Exercise 6.5.4. Let α be a composition. Write the composition α in the form $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_\ell)$ with $\ell=\ell(\alpha)$.

(a) Show that the s-th power-sum symmetric function $p_s\in\Lambda$ satisfies

$$p_s\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = M_{\alpha\{s\}}$$

for every positive integer s.

(b) Let us fix a total order on the set $\mathrm{SIS}(\ell)$ (for example, the lexicographic order). Show that the s-th elementary symmetric function $e_s\in\Lambda$ satisfies

$$M_\alpha^{\langle s\rangle} = e_s\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right) = \sum_{\substack{(\mathbf{i}_1,\mathbf{i}_2,\ldots,\mathbf{i}_s)\in(\mathrm{SIS}(\ell))^s;\\ \mathbf{i}_1<\mathbf{i}_2<\cdots<\mathbf{i}_s}} \mathbf{x}_{\mathbf{i}_1}^\alpha\mathbf{x}_{\mathbf{i}_2}^\alpha\cdots\mathbf{x}_{\mathbf{i}_s}^\alpha$$

for every $s\in\mathbb{N}$.

(c) Let $s\in\mathbb{N}$, and let n be a positive integer. Let $e_s^{\langle n\rangle}$ be the symmetric function $\sum_{i_1<i_2<\cdots<i_s} x_{i_1}^n x_{i_2}^n\cdots x_{i_s}^n\in\Lambda$. Then, show that

$$M_{\alpha\{n\}}^{\langle s\rangle} = e_s^{\langle n\rangle}\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i}\in \mathrm{SIS}(\ell)}\right).$$

[327] This is not completely obvious, but easy to check (see Exercise 6.5.4(b)).

(d) Let $s \in \mathbb{N}$, and let n be a positive integer. Prove that there exists a polynomial $P \in \mathbf{k}[z_1, z_2, z_3, \ldots]$ such that $M_{\alpha\{n\}}^{\langle s \rangle} = P\left(M_\alpha^{\langle 1 \rangle}, M_\alpha^{\langle 2 \rangle}, M_\alpha^{\langle 3 \rangle}, \ldots\right)$.

[**Hint:** For (a), (b) and (c), apply the definition of $f\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i} \in \mathrm{SIS}(\ell)}\right)$ with f a symmetric function[328]. For (d), recall that Λ is generated by $e_1, e_2, e_3, \ldots$.]

Exercise 6.5.5. Let $s \in \mathbb{N}$. Show that the composition (1) satisfies $M_{(1)}^{\langle s \rangle} = e_s$.

Proposition 6.5.6. *Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ be a composition.*

(a) Let $n \in \mathbb{N}$. Define a matrix $A_n^{\langle \alpha \rangle} = \left(a_{i,j}^{\langle \alpha \rangle}\right)_{i,j=1,2,\ldots,n}$ by

$$a_{i,j}^{\langle \alpha \rangle} = \begin{cases} M_{\alpha\{i-j+1\}}, & \text{if } i \geq j; \\ i, & \text{if } i = j-1; \\ 0, & \text{if } i < j-1 \end{cases} \qquad \text{for all } (i,j) \in \{1,2,\ldots,n\}^2.$$

This matrix $A_n^{\langle \alpha \rangle}$ looks as follows:

$$A_n^{\langle \alpha \rangle} = \begin{pmatrix} M_{\alpha\{1\}} & 1 & 0 & \cdots & 0 & 0 \\ M_{\alpha\{2\}} & M_{\alpha\{1\}} & 2 & \cdots & 0 & 0 \\ M_{\alpha\{3\}} & M_{\alpha\{2\}} & M_{\alpha\{1\}} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ M_{\alpha\{n-1\}} & M_{\alpha\{n-2\}} & M_{\alpha\{n-3\}} & \cdots & M_{\alpha\{1\}} & n-1 \\ M_{\alpha\{n\}} & M_{\alpha\{n-1\}} & M_{\alpha\{n-2\}} & \cdots & M_{\alpha\{2\}} & M_{\alpha\{1\}} \end{pmatrix}.$$

Then, $\det\left(A_n^{\langle \alpha \rangle}\right) = n! M_\alpha^{\langle n \rangle}$.

(b) Let n be a positive integer. Define a matrix $B_n^{\langle \alpha \rangle} = \left(b_{i,j}^{\langle \alpha \rangle}\right)_{i,j=1,2,\ldots,n}$ by

$$b_{i,j}^{\langle \alpha \rangle} = \begin{cases} i M_\alpha^{\langle i \rangle}, & \text{if } j = 1; \\ M_\alpha^{\langle i-j+1 \rangle}, & \text{if } j > 1 \end{cases} \qquad \text{for all } (i,j) \in \{1,2,\ldots,n\}^2.$$

[328] There are two subtleties that need to be addressed:

- the fact that the definition of $f\left(\left(\mathbf{x}_\mathbf{i}^\alpha\right)_{\mathbf{i} \in \mathrm{SIS}(\ell)}\right)$ distinguishes between two cases depending on whether or not $\mathrm{SIS}(\ell)$ is finite;
- the fact that the total order on the set $\{1,2,3,\ldots\}$ (which appears in the summation subscript in the equality $e_s = \sum_{\substack{(i_1,i_2,\ldots,i_s) \in \{1,2,3,\ldots\}^s; \\ i_1 < i_2 < \cdots < i_s}} x_{i_1} x_{i_2} \cdots x_{i_s}$) has nothing to do with the total order on the set $\mathrm{SIS}(\ell)$ (which appears in the summation subscript in $\sum_{\substack{(\mathbf{i}_1,\mathbf{i}_2,\ldots,\mathbf{i}_s) \in (\mathrm{SIS}(\ell))^s; \\ \mathbf{i}_1 < \mathbf{i}_2 < \cdots < \mathbf{i}_s}} \mathbf{x}_{\mathbf{i}_1}^\alpha \mathbf{x}_{\mathbf{i}_2}^\alpha \cdots \mathbf{x}_{\mathbf{i}_s}^\alpha$). For instance, the former total order is well-founded, whereas the latter may and may not be. So there is (generally) no bijection between $\{1,2,3,\ldots\}$ and $\mathrm{SIS}(\ell)$ preserving these orders (even if $\mathrm{SIS}(\ell)$ is infinite). Fortunately, this does not matter much, because the total order is only being used to ensure that every product of s distinct elements appears exactly once in the sum.

The matrix $B_n^{\langle\alpha\rangle}$ *looks as follows:*

$$B_n^{\langle\alpha\rangle} = \begin{pmatrix} M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} & M_\alpha^{\langle -1\rangle} & \cdots & M_\alpha^{\langle -n+3\rangle} & M_\alpha^{\langle -n+2\rangle} \\ 2M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} & \cdots & M_\alpha^{\langle -n+4\rangle} & M_\alpha^{\langle -n+3\rangle} \\ 3M_\alpha^{\langle 3\rangle} & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & \cdots & M_\alpha^{\langle -n+5\rangle} & M_\alpha^{\langle -n+4\rangle} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\, M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & M_\alpha^{\langle n-3\rangle} & \cdots & M_\alpha^{\langle 1\rangle} & M_\alpha^{\langle 0\rangle} \\ nM_\alpha^{\langle n\rangle} & M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & \cdots & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} \end{pmatrix}$$

$$= \begin{pmatrix} M_\alpha^{\langle 1\rangle} & 1 & 0 & \cdots & 0 & 0 \\ 2M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & 1 & \cdots & 0 & 0 \\ 3M_\alpha^{\langle 3\rangle} & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\, M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & M_\alpha^{\langle n-3\rangle} & \cdots & M_\alpha^{\langle 1\rangle} & 1 \\ nM_\alpha^{\langle n\rangle} & M_\alpha^{\langle n-1\rangle} & M_\alpha^{\langle n-2\rangle} & \cdots & M_\alpha^{\langle 2\rangle} & M_\alpha^{\langle 1\rangle} \end{pmatrix}.$$

Then, $\det\left(B_n^{\langle\alpha\rangle}\right) = M_{\alpha\{n\}}$.

Exercise 6.5.7. Prove Proposition 6.5.6.

[**Hint:** Substitute $(\mathbf{x}_{\mathbf{i}}^{\alpha})_{\mathbf{i}\in \mathrm{SIS}(\ell)}$ for the variable set in Exercise 2.9.13, and recall Exercise 6.5.4(a).]

Corollary 6.5.8. *Let* α *be a composition. Let* $s \in \mathbb{Z}$.

(a) *We have* $M_\alpha^{\langle s\rangle} \in \mathrm{QSym}$.

(b) *We have* $M_\alpha^{\langle s\rangle} \in \mathrm{QSym}_{s|\alpha|}$.

Exercise 6.5.9. Prove Corollary 6.5.8.

We make one further definition:

Definition 6.5.10. Let α be a nonempty composition. Then, we denote by $\gcd\alpha$ the greatest common divisor of the parts of α. (For instance, $\gcd(8,6,4) = 2$.) We also define $\operatorname{red}\alpha$ to be the composition $\left(\frac{\alpha_1}{\gcd\alpha}, \frac{\alpha_2}{\gcd\alpha}, \ldots, \frac{\alpha_\ell}{\gcd\alpha}\right)$, where α is written in the form $(\alpha_1, \alpha_2, \ldots, \alpha_\ell)$.

We say that a nonempty composition α is *reduced* if $\gcd\alpha = 1$.

We define $\mathfrak{RL}$ to be the set of all reduced Lyndon compositions. In other words, $\mathfrak{RL} = \{w \in \mathfrak{L} \mid w \text{ is reduced}\}$ (since $\mathfrak{L}$ is the set of all Lyndon compositions).

Hazewinkel, in [93, proof of Thm. 6.7.5], denotes $\mathfrak{RL}$ by $eLYN$, calling reduced Lyndon compositions "elementary Lyndon words".

Remark 6.5.11. Let α be a nonempty composition.

(a) We have $\alpha = (\operatorname{red}\alpha)\{\gcd\alpha\}$.

(b) The composition α is Lyndon if and only if the composition $\operatorname{red}\alpha$ is Lyndon.

(c) The composition $\operatorname{red}\alpha$ is reduced.

(d) If α is reduced, then $\operatorname{red}\alpha = \alpha$.

(e) If $s \in \{1,2,3,\ldots\}$, then the composition $\alpha\{s\}$ is nonempty and satisfies $\operatorname{red}(\alpha\{s\}) = \operatorname{red}\alpha$ and $\gcd(\alpha\{s\}) = s\gcd\alpha$.

(f) We have $(\gcd\alpha)\,|\operatorname{red}\alpha| = |\alpha|$.

Exercise 6.5.12. Prove Remark 6.5.11.

Our goal in this section is now to prove the following result of Hazewinkel:

Theorem 6.5.13. *The family* $\left(M_w^{\langle s\rangle}\right)_{(w,s)\in\mathfrak{RL}\times\{1,2,3,\ldots\}}$ *is an algebraically independent generating set of the* $\mathbf{k}$*-algebra* QSym.

This will (almost) immediately yield Theorem 6.4.3.

Our first step towards proving Theorem 6.5.13 is the following observation:

Lemma 6.5.14. *The family* $\left(M_w^{\langle s\rangle}\right)_{(w,s)\in\mathfrak{RL}\times\{1,2,3,\ldots\}}$ *is a reindexing of the family* $\left(M_{\operatorname{red}\alpha}^{\langle \gcd\alpha\rangle}\right)_{\alpha\in\mathfrak{L}}$.

Exercise 6.5.15. Prove Lemma 6.5.14.

Next, we show a lemma:

Lemma 6.5.16. *Let* α *be a nonempty composition. Let* $s\in\mathbb{N}$. *Then,*

$$s!M_\alpha^{\langle s\rangle} - M_\alpha^s \in \sum_{\substack{\beta\in\operatorname{Comp}_{s|\alpha|};\\ \ell(\beta)\le(s-1)\ell(\alpha)}} \mathbf{k}M_\beta. \tag{6.5.2}$$

(That is, $s!M_\alpha^{\langle s\rangle}-M_\alpha^s$ *is a* $\mathbf{k}$*-linear combination of terms of the form* M_β *with* β *ranging over the compositions of* $s\,|\alpha|$ *satisfying* $\ell(\beta)\le(s-1)\,\ell(\alpha)$*.)*

Exercise 6.5.17. Prove Lemma 6.5.16.

[**Hint:** There are two approaches: One is to apply Proposition 6.5.6(a) and expand the determinant; the other is to argue which monomials can appear in $s!M_\alpha^{\langle s\rangle} - M_\alpha^s$.]

We now return to studying products of monomial quasisymmetric functions:

Lemma 6.5.18. *Let* $n\in\mathbb{N}$ *and* $m\in\mathbb{N}$. *Let* $u\in\operatorname{Comp}_n$ *and* $v\in\operatorname{Comp}_m$. *Let* z *be the lexicographically highest element of the multiset* $u\sqcup\!\sqcup v$. *Let* h *be the multiplicity with which the word* z *appears in the multiset* $u\sqcup\!\sqcup v$. *Then,*[329]

$$M_uM_v = hM_z + \left(\text{a sum of terms of the form } M_w \text{ with } w\in\operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} z\right).$$

Proof of Lemma 6.5.18. Lemma 6.5.18 was shown during the proof of Lemma 6.4.11(b). □

Corollary 6.5.19. *Let* $n\in\mathbb{N}$ *and* $m\in\mathbb{N}$. *Let* $u\in\operatorname{Comp}_n$ *and* $v\in\operatorname{Comp}_m$. *Regard* u *and* v *as words in* $\mathfrak{A}^*$. *Assume that* u *is a Lyndon word. Let* $(b_1,b_2,\ldots,b_q)$ *be the CFL factorization of the word* v.

Assume that $u\ge b_j$ *for every* $j\in\{1,2,\ldots,q\}$. *Let*

$$h = 1+\left|\{j\in\{1,2,\ldots,q\} \mid b_j=u\}\right|.$$

Then,

$$M_uM_v = hM_{uv} + \left(\text{a sum of terms of the form } M_w \text{ with } w\in\operatorname{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} uv\right).$$

Exercise 6.5.20. Prove Corollary 6.5.19.

[**Hint:** Apply Lemma 6.5.18, and notice that uv is the lexicographically highest element of the multiset $u\sqcup\!\sqcup v$ (by Theorem 6.2.2(e)), and that h is the multiplicity with which this word uv appears in the multiset $u\sqcup\!\sqcup v$ (this is a rewriting of Theorem 6.2.2(e)).]

Corollary 6.5.21. *Let* $k\in\mathbb{N}$ *and* $s\in\mathbb{N}$. *Let* $x\in\operatorname{Comp}_k$ *be such that* x *is a Lyndon word. Then:*

(a) *The lexicographically highest element of the multiset* $x\sqcup\!\sqcup x^s$ *is* x^{s+1}.

(b) *We have*

$$M_xM_{x^s} = (s+1)\,M_{x^{s+1}} + \left(\text{a sum of terms of the form } M_w \text{ with } w\in\operatorname{Comp}_{(s+1)k} \text{ satisfying } w \underset{\text{wll}}{<} x^{s+1}\right).$$

(c) *Let* $t\in\operatorname{Comp}_{sk}$ *be such that* $t \underset{\text{wll}}{<} x^s$. *Then,*

$$M_xM_t = \left(\text{a sum of terms of the form } M_w \text{ with } w\in\operatorname{Comp}_{(s+1)k} \text{ satisfying } w \underset{\text{wll}}{<} x^{s+1}\right).$$

[329] The following equality makes sense because we have $z\in\operatorname{Comp}_{n+m}$ (by Lemma 6.4.11(a)).

Exercise 6.5.22. Prove Corollary 6.5.21.

[**Hint:** Notice that $\left(\underbrace{x, x, \ldots, x}_{s \text{ times}}\right)$ is the CFL factorization of the word x^s. Now, part (a) of Corollary 6.5.21 follows from Theorem 6.2.2(c), part (b) follows from Corollary 6.5.19, and part (c) from Lemma 6.4.11(c) (using part (a)).]

Corollary 6.5.23. *Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $u \in \mathrm{Comp}_n$ and $v \in \mathrm{Comp}_m$. Regard u and v as words in $\mathfrak{A}^*$. Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of u. Let $(b_1, b_2, \ldots, b_q)$ be the CFL factorization of the word v. Assume that $a_i > b_j$ for every $i \in \{1, 2, \ldots, p\}$ and $j \in \{1, 2, \ldots, q\}$. Then,*

$$M_u M_v = M_{uv} + \left(\text{a sum of terms of the form } M_w \text{ with } w \in \mathrm{Comp}_{n+m} \text{ satisfying } w \underset{\text{wll}}{<} uv\right).$$

Exercise 6.5.24. Prove Corollary 6.5.23.

[**Hint:** Combine Lemma 6.5.18 with the parts (c) and (d) of Theorem 6.2.2.]

Corollary 6.5.25. *Let $n \in \mathbb{N}$. Let $u \in \mathrm{Comp}_n$ be a nonempty composition. Regard u as a word in $\mathfrak{A}^*$. Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of u. Let $k \in \{1, 2, \ldots, p-1\}$ be such that $a_k > a_{k+1}$. Let x be the word $a_1 a_2 \cdots a_k$, and let y be the word $a_{k+1} a_{k+2} \cdots a_p$. Then,*

$$M_u = M_x M_y - \left(\text{a sum of terms of the form } M_w \text{ with } w \in \mathrm{Comp}_n \text{ satisfying } w \underset{\text{wll}}{<} u\right).$$

Exercise 6.5.26. Prove Corollary 6.5.25.

[**Hint:** Apply Corollary 6.5.23 to x, y, $|x|$, $|y|$, k, $p-k$, $(a_1, a_2, \ldots, a_k)$ and $(a_{k+1}, a_{k+2}, \ldots, a_p)$ instead of u, v, n, m, p, q, $(a_1, a_2, \ldots, a_p)$ and $(b_1, b_2, \ldots, b_q)$; then, notice that $xy = u$ and $|x| + |y| = n$.]

Corollary 6.5.27. *Let $k \in \mathbb{N}$. Let $x \in \mathrm{Comp}_k$ be a composition. Assume that x is a Lyndon word. Let $s \in \mathbb{N}$. Then,*

$$M_x^s - s! M_{x^s} \in \sum_{\substack{w \in \mathrm{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w.$$

(Recall that x^s is defined to be the word $\underbrace{xx\cdots x}_{s \text{ times}}$.)

Exercise 6.5.28. Prove Corollary 6.5.27.

[**Hint:** Rewrite the claim of Corollary 6.5.27 in the form $M_x^s \in s! M_{x^s} + \sum_{\substack{w \in \mathrm{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w$. This can be proven by induction over s, where in the induction step we need the following two observations:

(1) We have $M_x M_{x^s} \in (s+1)\, M_{x^{s+1}} + \sum_{\substack{w \in \mathrm{Comp}_{(s+1)k}; \\ w \underset{\text{wll}}{<} x^{s+1}}} \mathbf{k} M_w$.

(2) For every $t \in \mathrm{Comp}_{sk}$ satisfying $t \underset{\text{wll}}{<} x^s$, we have $M_x M_t \in \sum_{\substack{w \in \mathrm{Comp}_{(s+1)k}; \\ w \underset{\text{wll}}{<} x^{s+1}}} \mathbf{k} M_w$.

These two observations follow from parts (b) and (c) of Corollary 6.5.21.]

Corollary 6.5.29. *Let $k \in \mathbb{N}$. Let $x \in \mathrm{Comp}_k$ be a composition. Assume that x is a Lyndon word. Let $s \in \mathbb{N}$. Then,*

$$M_x^{\langle s \rangle} - M_{x^s} \in \sum_{\substack{w \in \mathrm{Comp}_{sk}; \\ w \underset{\text{wll}}{<} x^s}} \mathbf{k} M_w.$$

(Recall that x^s is defined to be the word $\underbrace{xx\cdots x}_{s \text{ times}}$.)

Exercise 6.5.30. Prove Corollary 6.5.29.

[**Hint:** Lemma 6.5.16 (applied to $\alpha = x$) yields

$$s!M_x^{\langle s\rangle} - M_x^s \in \sum_{\substack{\beta\in\mathrm{Comp}_{sk};\\ \ell(\beta)\leq(s-1)\ell(x)}} M_\beta = \sum_{\substack{w\in\mathrm{Comp}_{sk};\\ \ell(w)\leq(s-1)\ell(x)}} \mathbf{k}M_w \subset \sum_{\substack{w\in\mathrm{Comp}_{sk};\\ w<_{\mathrm{wll}}x^s}} \mathbf{k}M_w$$

[330]. Adding this to the claim of Corollary 6.5.27, obtain $s!M_x^{\langle s\rangle} - s!M_{x^s} \in \sum_{\substack{w\in\mathrm{Comp}_{sk};\\ w<_{\mathrm{wll}}x^s}} \mathbf{k}M_w$, that is, $s!\left(M_x^{\langle s\rangle} - M_{x^s}\right) \in \sum_{\substack{w\in\mathrm{Comp}_{sk};\\ w<_{\mathrm{wll}}x^s}} \mathbf{k}M_w$. It remains to get rid of the $s!$ on the left hand side. Assume WLOG that $\mathbf{k} = \mathbb{Z}$, and argue that every $f \in \mathrm{QSym}$ satisfying $s!\cdot f \in \sum_{\substack{w\in\mathrm{Comp}_{sk};\\ w<_{\mathrm{wll}}x^s}} \mathbf{k}M_w$ must itself lie in $\sum_{\substack{w\in\mathrm{Comp}_{sk};\\ w<_{\mathrm{wll}}x^s}} \mathbf{k}M_w$.]

We are now ready to prove Theorem 6.5.13:

Exercise 6.5.31. Prove Theorem 6.5.13.

[**Hint:** Lemma 6.5.14 yields that the family $\left(M_w^{\langle s\rangle}\right)_{(w,s)\in\mathfrak{RL}\times\{1,2,3,\ldots\}}$ is a reindexing of the family $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$. Hence, it is enough to prove that the family $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$ is an algebraically independent generating set of the $\mathbf{k}$-algebra QSym. The latter claim, in turn, will follow from Lemma 6.3.7(c)[331] once it is proven that the family $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$ generates the $\mathbf{k}$-algebra QSym. So it remains to show that the family $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$ generates the $\mathbf{k}$-algebra QSym.

Let U denote the $\mathbf{k}$-subalgebra of QSym generated by $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$. It then suffices to prove that $U = \mathrm{QSym}$. To this purpose, it is enough to prove that

$$M_\beta \in U \qquad \text{for every composition } \beta. \tag{6.5.3}$$

For every reduced Lyndon composition α and every $j \in \{1,2,3,\ldots\}$, the quasisymmetric function $M_\alpha^{\langle j\rangle}$ is an element of the family $\left(M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}\right)_{w\in\mathfrak{L}}$ and thus belongs to U. Combine this with Exercise 6.5.4(d) to see that

$$M_\beta^{\langle s\rangle} \in U \qquad \text{for every Lyndon composition } \beta \text{ and every } s \in \{1,2,3,\ldots\} \tag{6.5.4}$$

(because every Lyndon composition β can be written as $\alpha\{n\}$ for a reduced Lyndon composition α and an $n \in \{1,2,3,\ldots\}$). Now, prove (6.5.3) by strong induction: first, induct on $|\beta|$, and then, for fixed $|\beta|$, induct on β in the wll-order. The induction step looks as follows: Fix some composition α, and assume (as induction hypothesis) that:

- (6.5.3) holds for every composition β satisfying $|\beta| < |\alpha|$;
- (6.5.3) holds for every composition β satisfying $|\beta| = |\alpha|$ and $\beta <_{\mathrm{wll}} \alpha$.

It remains to prove that (6.5.3) holds for $\beta = \alpha$. In other words, it remains to prove that $M_\alpha \in U$.

Let $(a_1, a_2, \ldots, a_p)$ be the CFL factorization of the word α. Assume WLOG that $p \neq 0$ (else, all is trivial). We are in one of the following two cases:

Case 1: All of the words a_1, a_2, …, a_p are equal.

Case 2: Not all of the words a_1, a_2, …, a_p are equal.

---

[330] since every $w \in \mathrm{Comp}_{sk}$ with the property that $\ell(w) \leq (s-1)\,\ell(x)$ must satisfy $w <_{\mathrm{wll}} x^s$

[331] applied to $A = \mathrm{QSym}$, $b_w = M_{\mathrm{red}\,w}^{\langle \gcd w\rangle}$, $\mathrm{wt}\,(N) = N$ and $g_u = M_u$

In Case 2, there exists a $k \in \{1,2,\ldots,p-1\}$ satisfying $a_k > a_{k+1}$ (since $a_1 \geq a_2 \geq \cdots \geq a_p$), and thus Corollary 6.5.25 (applied to $u=\alpha$, $n=|\alpha|$, $x = a_1 a_2 \cdots a_k$ and $y = a_{k+1} a_{k+2} \cdots a_p$) shows that

$$M_\alpha = \underbrace{M_{a_1 a_2 \cdots a_k}}_{\substack{\in U \\ \text{(by the induction hypothesis)}}} \underbrace{M_{a_{k+1} a_{k+2} \cdots a_p}}_{\substack{\in U \\ \text{(by the induction hypothesis)}}} - \left(\text{a sum of terms of the form } \underbrace{M_w}_{\substack{\in U \\ \text{(by the induction hypothesis)}}} \text{ with } w \in \mathrm{Comp}_{|\alpha|} \text{ satisfying } w \underset{\text{wll}}{<} \alpha \right)$$
$$\in UU - (\text{a sum of terms in } U) \subset U.$$

Hence, it only remains to deal with Case 1. In this case, set $x = a_1 = a_2 = \cdots = a_p$. Thus, $\alpha = a_1 a_2 \cdots a_p = x^p$, whence $|\alpha| = p\,|x|$. But Corollary 6.5.29 (applied to $s=p$ and $k=|x|$) yields

$$M_x^{\langle p \rangle} - M_{x^p} \in \sum_{\substack{w \in \mathrm{Comp}_{p|x|}; \\ w \underset{\text{wll}}{<} x^p}} \mathbf{k} M_w = \sum_{\substack{w \in \mathrm{Comp}_{|\alpha|}; \\ w \underset{\text{wll}}{<} \alpha}} \mathbf{k} \underbrace{M_w}_{\substack{\in U \\ \text{(by the induction hypothesis)}}} \qquad \text{(since } p\,|x| = |\alpha| \text{ and } x^p = \alpha\text{)}$$
$$\subset \sum_{\substack{w \in \mathrm{Comp}_N; \\ w \underset{\text{wll}}{<} \alpha}} \mathbf{k} U \subset U,$$

so that $M_{x^p} \in \underbrace{M_x^{\langle p \rangle}}_{\substack{\in U \\ \text{(by (6.5.4))}}} - U \subset U - U \subset U$. This rewrites as $M_\alpha \in U$ (since $\alpha = x^p$). So $M_\alpha \in U$ is proven in both Cases 1 and 2, and thus the induction proof of (6.5.3) is finished.]

Exercise 6.5.32. Prove Theorem 6.4.3.

Of course, this proof of Theorem 6.4.3 yields a new (third) proof for Proposition 6.4.4.

We notice the following corollary of our approach to Theorem 6.4.3:

Corollary 6.5.33. *The Λ-algebra* QSym *is a polynomial algebra (over Λ).*

Exercise 6.5.34. Prove Corollary 6.5.33.

[**Hint:** The algebraically independent generating set $\left(M_w^{\langle s \rangle}\right)_{(w,s) \in \mathfrak{RL} \times \{1,2,3,\ldots\}}$ of QSym contains the elements $M_{(1)}^{\langle s \rangle} = e_s \in \Lambda$ for all $s \in \{1,2,3,\ldots\}$.]

6.6. **The Gessel-Reutenauer bijection and symmetric functions.** In this section, we shall discuss the Gessel-Reutenauer bijection between words and multisets of aperiodic necklaces, and use it to study another family of symmetric functions.

The Gessel-Reutenauer bijection was studied in [82], where it was applied to various enumeration problems (e.g., counting permutations in $\mathfrak{S}_n$ with given descent set and given cycle type); it is also closely related to the Burrows-Wheeler bijection used in data compression ([45]), and to the structure of free Lie algebras ([81], [182]). We shall first introduce the Gessel-Reutenauer bijection and study it combinatorially in Subsection 6.6.1; then, in the following Subsection 6.6.2, we shall apply it to symmetric functions.

6.6.1. *Necklaces and the Gessel-Reutenauer bijection.* We begin with definitions, some of which have already been made in Exercise 6.1.34:

Definition 6.6.1. Throughout Section 6.6, we shall freely use Definition 6.1.1 and Definition 6.1.13. We fix a totally ordered alphabet $\mathfrak{A}$. (This alphabet can be arbitrary, although most examples will use $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$.)

Let C denote the infinite cyclic group, written multiplicatively. Fix a generator c of C. [332]

[332] So C is a group isomorphic to $(\mathbb{Z},+)$, and the isomorphism $(\mathbb{Z},+) \to C$ sends every $n \in \mathbb{Z}$ to c^n. (Recall that we write the binary operation of C as $\cdot$ instead of $+$.)

For any positive integer n, the group C acts on $\mathfrak{A}^n$ from the left according to the rule

$$c \cdot (a_1, a_2, \ldots, a_n) = (a_2, a_3, \ldots, a_n, a_1) \qquad \text{for all } (a_1, a_2, \ldots, a_n) \in \mathfrak{A}^n.$$

[333] The orbits of this C-action will be called *n-necklaces*[334]; they form a set partition of the set $\mathfrak{A}^n$.

The n-necklace containing a given n-tuple $w \in \mathfrak{A}^n$ will be denoted by $[w]$.

A *necklace* shall mean an n-necklace for some positive integer n. Thus, for each nonempty word w, there is a well-defined necklace $[w]$ (namely, $[w]$ is an n-necklace, where $n = \ell(w)$).

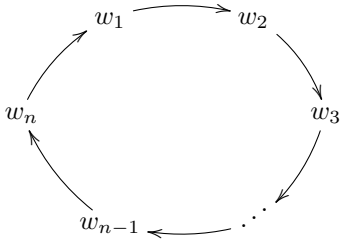
The *period* of a necklace N is defined as the positive integer $|N|$. (This $|N|$ is indeed a positive integer, since N is a finite nonempty set[335].)

An n-necklace is said to be *aperiodic* if its period is n.

Example 6.6.2. Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$. The orbit of the word 223 under the C-action is the 3-necklace $\{223, 232, 322\}$; it is an aperiodic 3-necklace. The orbit of the word 223223 under the C-action is the 6-necklace $\{223223, 232232, 322322\}$; it is not aperiodic (since it has period 3). The orbit of any nonempty word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ is the n-necklace

$$\{(w_i, w_{i+1}, \ldots, w_n, w_1, w_2, \ldots, w_{i-1}) \mid i \in \{1, 2, \ldots, n\}\}.$$

We can draw this n-necklace on the plane as follows:



It is easy to see that the notion of an "aperiodic necklace" we just defined is equivalent to the notion of a "primitive necklace" used in Exercise 4.6.4(b).

Exercise 6.1.34(a) shows that any n-necklace for any positive integer n is a finite nonempty set. In other words, any necklace is a finite nonempty set.

Let us next introduce some notations regarding words and permutations. We recall that a cycle of a permutation $\tau \in \mathfrak{S}_n$ is an orbit under the action of τ on $\{1, 2, \ldots, n\}$. (This orbit can be a 1-element set, when τ has fixed points.) We begin with a basic definition:

Definition 6.6.3. Let $\tau \in \mathfrak{S}_n$ be a permutation. Let $h \in \{1, 2, \ldots, n\}$.

(a) We let $\operatorname{ord}_\tau(h)$ denote the smallest positive integer i such that $\tau^i(h) = h$. (Basic properties of permutations show that this i exists.)

(b) Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Then, $w_{\tau,h}$ shall denote the word $w_{\tau^1(h)} w_{\tau^2(h)} \cdots w_{\tau^k(h)}$, where $k = \operatorname{ord}_\tau(h)$.

Example 6.6.4. Let τ be the permutation $3142765 \in \mathfrak{S}_7$ (in one-line notation). Then, $\operatorname{ord}_\tau(1) = 4$ (since $\tau^4(1) = 1$, but $\tau^i(1) \neq 1$ for every positive integer $i < 4$). Likewise, $\operatorname{ord}_\tau(2) = 4$ and $\operatorname{ord}_\tau(3) = 4$ and $\operatorname{ord}_\tau(4) = 4$ and $\operatorname{ord}_\tau(5) = 2$ and $\operatorname{ord}_\tau(6) = 1$ and $\operatorname{ord}_\tau(7) = 2$.

Now, let w be the word $4112524 \in \mathfrak{A}^7$. Then,

$$\begin{aligned} w_{\tau,3} &= w_{\tau^1(3)} w_{\tau^2(3)} w_{\tau^3(3)} w_{\tau^4(3)} \qquad (\text{since } \operatorname{ord}_\tau(3) = 4) \\ &= w_4 w_2 w_1 w_3 \\ &\qquad \left(\text{since } \tau^1(3) = 4 \text{ and } \tau^2(3) = \tau(4) = 2 \text{ and } \tau^3(3) = \tau(2) = 1 \text{ and } \tau^4(3) = \tau(1) = 3\right) \\ &= 2141. \end{aligned}$$

Likewise, we can check that $w_{\tau,1} = w_3 w_4 w_2 w_1 = 1214$ and $w_{\tau,5} = w_7 w_5 = 45$ and $w_{\tau,6} = w_6 = 2$.

---

[333] In other words, c rotates any n-tuple of elements of $\mathfrak{A}$ cyclically to the left. Thus, $c^n \in C$ acts trivially on $\mathfrak{A}^n$, and so this action of C on $\mathfrak{A}^n$ factors through $C/\langle c^n \rangle$ (a cyclic group of order n).

[334] See Exercise 6.1.34 for the motivation behind this word.

Notice that there are no 0-necklaces, because we required n to be positive in the definition of a necklace. This is intentional.

[335] by Exercise 6.1.34(a), because N is an n-necklace for some positive integer n

We begin the study of the words $w_{\tau,h}$ by stating some of their simplest properties:[336]

Proposition 6.6.5. *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Let $\tau \in \mathfrak{S}_n$. Let $h \in \{1, 2, \ldots, n\}$. Then:*

(a) *The word $w_{\tau,h}$ is nonempty and has length $\operatorname{ord}_\tau(h)$.*
(b) *The first letter of the word $w_{\tau,h}$ is $w_{\tau(h)}$.*
(c) *The last letter of the word $w_{\tau,h}$ is w_h.*
(d) *We have $w_{\tau,\tau(h)} = c \cdot w_{\tau,h}$.*
(e) *We have $w_{\tau,\tau^i(h)} = c^i \cdot w_{\tau,h}$ for each $i \in \mathbb{Z}$.*

Recall that if $n \in \mathbb{N}$ and if $w \in \mathfrak{A}^n$ is a word, then a permutation $\operatorname{std} w \in \mathfrak{S}_n$ was defined in Definition 5.3.3. The words $w_{\tau,h}$ have particularly nice properties when $\tau = (\operatorname{std} w)^{-1}$:

Lemma 6.6.6. *Let $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$ be a word. Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let α and β be two elements of $\{1, 2, \ldots, n\}$ such that $\alpha < \beta$. Then:*

(a) *If $\tau^{-1}(\alpha) < \tau^{-1}(\beta)$, then $w_\alpha \leq w_\beta$.*
(b) *If $\tau^{-1}(\alpha) \geq \tau^{-1}(\beta)$, then $w_\alpha > w_\beta$.*
(c) *We have $w_{\tau(\alpha)} \leq w_{\tau(\beta)}$.*
(d) *If $\tau(\alpha) \geq \tau(\beta)$, then $w_{\tau(\alpha)} < w_{\tau(\beta)}$.*
(e) *If $w_{\tau(\alpha)} = w_{\tau(\beta)}$, then $\tau(\alpha) < \tau(\beta)$.*
(f) *If $w_{\tau,\alpha} = w_{\tau,\beta}$, then $\tau(\alpha) < \tau(\beta)$ and $w_{\tau,\tau(\alpha)} = w_{\tau,\tau(\beta)}$.*
(g) *If $w_{\tau,\alpha} = w_{\tau,\beta}$, then $\tau^i(\alpha) < \tau^i(\beta)$ for each $i \in \mathbb{N}$.*
(h) *Let $j \in \mathbb{N}$ be such that every $i \in \{0, 1, \ldots, j-1\}$ satisfies $w_{\tau^{i+1}(\alpha)} = w_{\tau^{i+1}(\beta)}$. Then, $w_{\tau^{j+1}(\alpha)} \leq w_{\tau^{j+1}(\beta)}$.*

Proposition 6.6.7. *Let $w \in \mathfrak{A}^n$ be a word. Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let z be a cycle of τ. Then:*

(a) *For each $h \in z$, we have $[w_{\tau,h}] = \{w_{\tau,i} \mid i \in z\}$.*
(b) *If α and β are two distinct elements of z, then $w_{\tau,\alpha} \neq w_{\tau,\beta}$.*
(c) *We have $|\{w_{\tau,i} \mid i \in z\}| = |z|$.*
(d) *The set $\{w_{\tau,i} \mid i \in z\}$ is an aperiodic necklace.*

Exercise 6.6.8. Prove Proposition 6.6.5, Lemma 6.6.6 and Proposition 6.6.7.

Definition 6.6.9. Let $w \in \mathfrak{A}^n$ be a word. Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Let z be a cycle of τ. Then, we define an aperiodic necklace $[w]_z$ by $[w]_z = \{w_{\tau,i} \mid i \in z\}$. (This is indeed an aperiodic necklace, according to Proposition 6.6.7(d).)

Example 6.6.10. Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let w be the word $2511321 \in \mathfrak{A}^7$. Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_7$; this is the permutation 3471652 (in one-line notation). One cycle of τ is $z = \{1, 3, 7, 2, 4\}$. The corresponding aperiodic necklace $[w]_z$ is

$$\begin{aligned}[w]_z &= \{w_{\tau,i} \mid i \in z\} = \{w_{\tau,1}, w_{\tau,3}, w_{\tau,7}, w_{\tau,2}, w_{\tau,4}\} \qquad (\text{since } z = \{1,3,7,2,4\}) \\ &= \{11512, 15121, 51211, 12115, 21151\} = [11512]\,.\end{aligned}$$

Definition 6.6.11. We let $\mathfrak{N}$ be the set of all necklaces. We let $\mathfrak{N}^{\mathfrak{a}}$ be the set of all aperiodic necklaces. We let $\mathfrak{MN}^{\mathfrak{a}}$ be the set of all finite multisets of aperiodic necklaces.

Definition 6.6.12. We define a map $\operatorname{GR} : \mathfrak{A}^* \to \mathfrak{MN}^{\mathfrak{a}}$ as follows:

Let $w \in \mathfrak{A}^*$. Let $n = \ell(w)$ (so that $w \in \mathfrak{A}^n$). Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Then, we define the multiset $\operatorname{GR} w \in \mathfrak{MN}^{\mathfrak{a}}$ by setting

$$\operatorname{GR} w = \{[w]_z \mid z \text{ is a cycle of } \tau\}_{\text{multiset}}\,.$$

(This multiset $\operatorname{GR} w$ is indeed a finite multiset of aperiodic necklaces[337], and thus belongs to $\mathfrak{MN}^{\mathfrak{a}}$.)

[336] See Exercise 6.6.8 below for the proof of Proposition 6.6.5, as well as for the proofs of all other propositions stated before Exercise 6.6.8.

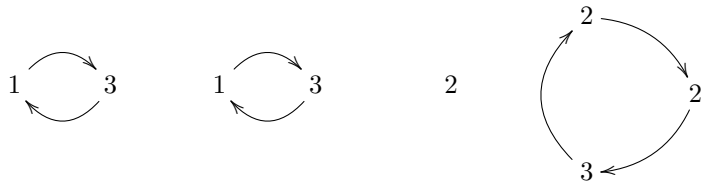
[337] Indeed, this multiset $\operatorname{GR} w$ is finite (since τ has only finitely many cycles), and its elements $[w]_z$ are aperiodic necklaces (as we have seen in the definition of $[w]_z$).

Example 6.6.13. Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let $w = 33232112 \in \mathfrak{A}^8$.

To compute $\operatorname{GR} w$, we first notice that $\operatorname{std} w = 67384125$ (in one-line notation). Hence, the permutation τ from Definition 6.6.12 satisfies $\tau = (\operatorname{std} w)^{-1} = 67358124$. The cycles of τ are $\{1,6\}$, $\{2,7\}$, $\{3\}$ and $\{4,5,8\}$. Thus,

$$\begin{aligned}\operatorname{GR} w &= \{[w]_z \mid z \text{ is a cycle of } \tau\}_{\text{multiset}} = \left\{[w]_{\{1,6\}}, [w]_{\{2,7\}}, [w]_{\{3\}}, [w]_{\{4,5,8\}}\right\}_{\text{multiset}} \\ &= \{[31], [31], [2], [322]\}_{\text{multiset}} = \{[13], [13], [2], [223]\}_{\text{multiset}}\end{aligned}$$

(since $[31] = [13]$ and $[322] = [223]$ as necklaces). Drawn on the plane, the necklaces in $\operatorname{GR} w$ look as follows:



The map GR is called the *Gessel-Reutenauer bijection*. In order to show that it indeed is a bijection, we shall construct its inverse. First, we introduce some further objects.

Definition 6.6.14. A nonempty word w is said to be *aperiodic* if there exist no $m \geq 2$ and $u \in \mathfrak{A}^*$ satisfying $w = u^m$.

Let $\mathfrak{A}^{\mathfrak{a}}$ be the set of all aperiodic words in $\mathfrak{A}^*$.

For example, the word 132231 is aperiodic, but the word 132132 is not (since $132132 = u^m$ for $u = 132$ and $m = 2$).

Aperiodic words are directly connected to aperiodic necklaces, as the following facts show:[338]

Proposition 6.6.15. *Let $w \in \mathfrak{A}^*$ be a nonempty word. Then, the word w is aperiodic if and only if the necklace $[w]$ is aperiodic.*

Corollary 6.6.16. *Let $w \in \mathfrak{A}^*$ be an aperiodic word. Then, the word $c \cdot w$ is aperiodic.*[339]

Corollary 6.6.17. *Each aperiodic necklace is a set of aperiodic words.*

Let us now introduce a new total order on the set $\mathfrak{A}^{\mathfrak{a}}$ of all aperiodic words:

Definition 6.6.18. Let u and v be two aperiodic words. Then, we write $u \leq_\omega v$ if and only if $uv \leq vu$. Thus, we have defined a binary relation $\leq_\omega$ on the set $\mathfrak{A}^{\mathfrak{a}}$ of all aperiodic words.

Proposition 6.6.19. *The relation $\leq_\omega$ on the set $\mathfrak{A}^{\mathfrak{a}}$ is the smaller-or-equal relation of a total order.*

For the next proposition, we should recall Definition 6.6.1 (and, in particular, the meaning of c and its action on words).

Proposition 6.6.20. *Let u and v be two aperiodic words.*

(a) *We have $u \leq_\omega v$ if and only if either $u_1 < v_1$ or ($u_1 = v_1$ and $c \cdot u \leq_\omega c \cdot v$).* [340]

(b) *If $u \neq v$, then there exists some $i \in \mathbb{N}$ satisfying $\left(c^i \cdot u\right)_1 \neq \left(c^i \cdot v\right)_1$.*

(c) *We have $u \leq_\omega v$ if and only if the smallest $i \in \mathbb{N}$ satisfying $\left(c^i \cdot u\right)_1 \neq \left(c^i \cdot v\right)_1$ **either** does not exist **or** satisfies $\left(c^i \cdot u\right)_1 < \left(c^i \cdot v\right)_1$.*

(d) *Let n and m be positive integers such that $n\ell(u) = m\ell(v)$. We have $u \leq_\omega v$ if and only if $u^n \leq v^m$.*

Remark 6.6.21. We are avoiding the use of infinite words here; if we didn't, we could restate the relation $\leq_\omega$ in a simpler way (which is easily seen to be equivalent to Proposition 6.6.20(c)): Two aperiodic words u and v satisfy $u \leq_\omega v$ if and only if $u^\infty \leq v^\infty$. Here, for any nonempty word w, we are letting w^∞ denote the infinite word

$$\left(w_1, w_2, \ldots, w_{\ell(w)}, w_1, w_2, \ldots, w_{\ell(w)}, w_1, w_2, \ldots, w_{\ell(w)}, \ldots\right)$$

[338] See Exercise 6.6.23 for the proofs of all unproved statements made until Exercise 6.6.23.

[339] See Definition 6.6.1 for the definition of c and its action on words.

[340] The relation "$c \cdot u \leq_\omega c \cdot v$" here makes sense because the words $c \cdot u$ and $c \cdot v$ are aperiodic (by Corollary 6.6.16).

(that is, the word w repeated endlessly), and the symbol "$\leq$" in "$u^\infty \leq v^\infty$" refers to the lexicographic order on $\mathfrak{A}^\infty$.

Other equivalent descriptions of the relation $\leq_\omega$ (or, more precisely, of the "strictly less" relation corresponding to it) can be found in [54, Corollary 11].

Proposition 6.6.22. *Let $w \in \mathfrak{A}^n$ be a word. Let τ be the permutation $(\operatorname{std} w)^{-1} \in \mathfrak{S}_n$. Then:*

(a) *The words $w_{\tau,1}, w_{\tau,2}, \ldots, w_{\tau,n}$ are aperiodic.*
(b) *We have $w_{\tau,1} \leq_\omega w_{\tau,2} \leq_\omega \cdots \leq_\omega w_{\tau,n}$.*

Exercise 6.6.23. Prove Proposition 6.6.15, Corollary 6.6.16, Corollary 6.6.17, Proposition 6.6.19, Proposition 6.6.20 and Proposition 6.6.22.

We need two more notations about multisets:

Definition 6.6.24. Let T be a totally ordered set, and let $\leq_T$ be the smaller-or-equal relation of T. Let M be a finite multiset of elements of T. Then, there is a unique list $(m_1, m_2, \ldots, m_n)$ such that

$$\{m_1, m_2, \ldots, m_n\}_{\text{multiset}} = M \qquad \text{and} \qquad m_1 \leq_T m_2 \leq_T \cdots \leq_T m_n.$$

This list $(m_1, m_2, \ldots, m_n)$ is obtained by listing all elements of M (with their multiplicities) in increasing order (increasing with respect to $\leq_T$). We shall refer to this list $(m_1, m_2, \ldots, m_n)$ as the *$\leq_T$-increasing list* of M.

(For example, the $\leq_{\mathbb{Z}}$-increasing list of $\{1,2,3,2,1\}_{\text{multiset}}$ is $(1,1,2,2,3)$.)

Definition 6.6.25. Let S be a finite multiset.

(a) The *support* $\operatorname{Supp} S$ is defined to be the set of all elements of S. Thus, if $S = \{m_1, m_2, \ldots, m_n\}_{\text{multiset}}$, then $\operatorname{Supp} S = \{m_1, m_2, \ldots, m_n\}$.
(b) For each $s \in S$, let M_s be a finite multiset. Then, we define the *multiset union* $\biguplus_{s \in S} M_s$ to be the finite multiset M with the following property: For any object x, we have

$$(\text{multiplicity of } x \text{ in } M) = \sum_{s \in \operatorname{Supp} S} (\text{multiplicity of } s \text{ in } S) \cdot (\text{multiplicity of } x \text{ in } M_s).$$

For example:
- If $S = \{1,2,3\}_{\text{multiset}}$ and $M_s = \{s, s+1\}_{\text{multiset}}$ for each $s \in \operatorname{Supp} S$, then $\biguplus_{s \in S} M_s = \{1,2,2,3,3,4\}_{\text{multiset}}$.
- If $S = \{1,1,2\}_{\text{multiset}}$ and $M_s = \{s, s+1\}_{\text{multiset}}$ for each $s \in \operatorname{Supp} S$, then $\biguplus_{s \in S} M_s = \{1,1,2,2,2,3\}_{\text{multiset}}$.

We regard each set as a multiset; thus, the multiset union $\biguplus_{s \in S} M_s$ is also defined when the M_s are sets.

Now, we can construct the inverse of the Gessel-Reutenauer bijection:

Definition 6.6.26. We define a map $\operatorname{RG} : \mathfrak{MM}^{\mathfrak{a}} \to \mathfrak{A}^*$ as follows:

Let $M \in \mathfrak{MM}^{\mathfrak{a}}$ be a finite multiset of aperiodic necklaces. Let $M' = \biguplus_{N \in M} N$. (We are here using the fact that each necklace $N \in M$ is a finite set, thus a finite multiset.) Notice that M' is a finite multiset of aperiodic words[341]. Let $(m_1, m_2, \ldots, m_n)$ be the $\leq_\omega$-increasing list of M'. For each $i \in \{1,2,\ldots,n\}$, let ℓ_i be the last letter of the nonempty word m_i. Then, $\operatorname{RG}(M)$ is defined to be the word $(\ell_1, \ell_2, \ldots, \ell_n) \in \mathfrak{A}^*$.

Example 6.6.27. Let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$, and let $M = \{[13], [13], [2], [223]\}_{\text{multiset}}$. Clearly, $M \in \mathfrak{MM}^{\mathfrak{a}}$ (since M is a finite multiset of aperiodic necklaces). (Actually, M is the multiset of

[341] Indeed:
- Each $N \in M$ is an aperiodic necklace (since M is a multiset of aperiodic necklaces), and thus (by Corollary 6.6.17) a set of aperiodic words. Therefore, $\biguplus_{N \in M} N$ is a multiset of aperiodic words.
- Each $N \in M$ is a necklace, and thus is a finite set (since any necklace is a finite set). Since the multiset M is also finite, this shows that $\biguplus_{N \in M} N$ is finite.

Thus, $\biguplus_{N \in M} N$ is a finite multiset of aperiodic words. In other words, M' is a finite multiset of aperiodic words (since $M' = \biguplus_{N \in M} N$).

aperiodic necklaces drawn in Example 6.6.13.) In order to compute the word $\operatorname{RG}(M)$, let us first compute the multiset M' from Definition 6.6.26. Indeed, the definition of M' yields

$$M' = \biguplus_{N \in M} N = \underbrace{[13]}_{=\{13,31\}} \uplus \underbrace{[13]}_{=\{13,31\}} \uplus \underbrace{[2]}_{=\{2\}} \uplus \underbrace{[223]}_{=\{223,232,322\}}$$

$$\left(\text{where we are using the notation } M_1 \uplus M_2 \uplus \cdots \uplus M_k \text{ for a multiset union } \biguplus_{s \in \{1,2,\ldots,k\}} M_s \right)$$

$$= \{13,31\} \uplus \{13,31\} \uplus \{2\} \uplus \{223,232,322\}$$

$$= \{13,31,13,31,2,223,232,322\}_{\text{multiset}}.$$

Hence, the $\leq_\omega$-increasing list of M' is $(13,13,2,223,232,31,31,322)$ (since $13 \leq_\omega 13 \leq_\omega 2 \leq_\omega 223 \leq_\omega 232 \leq_\omega 31 \leq_\omega 31 \leq_\omega 322$). The last letters of the words in this list are $3,3,2,3,2,1,1,2$ (in this order). Hence, Definition 6.6.26 shows that

$$\operatorname{RG}(M) = (3,3,2,3,2,1,1,2) = 33232112.$$

Remark 6.6.28. The $\leq_\omega$-increasing list of a multiset M' of aperiodic words is not always the same as its $\leq$-increasing list. For example, the $\leq_\omega$-increasing list of $\{2,21\}$ is $(21,2)$ (since $21 \leq_\omega 2$), whereas its $\leq$-increasing list is $(2,21)$ (since $2 \leq 21$).

A comparison of Examples 6.6.13 and 6.6.27 suggests that the maps GR and RG undo one another. This is indeed true, as the following theorem (due to Gessel and Reutenauer [82, Lemma 3.4 and Example 3.5]; also proved in [182, Theorem 7.20], [51, Theorem 3.1 and Proposition 3.1] and [81, §2]) shows:

Theorem 6.6.29. *The maps* $\operatorname{GR}: \mathfrak{A}^* \to \mathfrak{MM}^{\mathfrak{a}}$ *and* $\operatorname{RG}: \mathfrak{MM}^{\mathfrak{a}} \to \mathfrak{A}^*$ *are mutually inverse bijections.*

Exercise 6.6.30. Prove Theorem 6.6.29.

[**Hint:** First, use Proposition 6.6.22 to show that $\operatorname{RG} \circ \operatorname{GR} = \operatorname{id}$. Then recall the fact that any injective map between two finite sets of the same sizes is a bijection. This does not directly apply here, since the sets $\mathfrak{A}^*$ and $\mathfrak{MM}^{\mathfrak{a}}$ are usually not finite. However, GR can be restricted to a map between two appropriate finite subsets, obtained by focussing on a finite sub-alphabet of $\mathfrak{A}$ and fixing the length of the words; these subsets can be shown to have equal size using the Chen-Fox-Lyndon factorization (see the following paragraph for the connection).[342]]

Theorem 6.6.29 shows that the sets $\mathfrak{A}^*$ and $\mathfrak{MM}^{\mathfrak{a}}$ are in bijection. This bijection is in some sense similar to the Chen-Fox-Lyndon factorization[343], and preserves various quantities (for example, the number of times a given letter a appears in a word $w \in \mathfrak{A}^*$ equals the number of times this letter a appears in the words in the corresponding multiset $\operatorname{GR} w \in \mathfrak{MM}^{\mathfrak{a}}$, provided that we pick one representative of each necklace in $\operatorname{GR} w$), and predictably affects other quantities (for example, the cycles of the standardization $\operatorname{std} w$ of a word $w \in \mathfrak{A}^*$ have the same lengths as the aperiodic necklaces in the corresponding multiset $\operatorname{GR} w \in \mathfrak{MM}^{\mathfrak{a}}$); these properties have ample applications to enumerative questions (discussed in [82]).

Remark 6.6.31. The Gessel-Reutenauer bijection relates to the *Burrows-Wheeler transformation* (e.g., [45, §2]). Indeed, the latter sends an aperiodic word $w \in \mathfrak{A}^{\mathfrak{a}}$ to the word $\operatorname{RG}(\{[w]\}_{\text{multiset}})$ obtained by applying RG to the multiset consisting of the single aperiodic necklace $[w]$. This transformation is occasionally applied in (lossless) data compression, as the word $\operatorname{RG}(\{[w]\}_{\text{multiset}})$ tends to have many strings of consecutive equal letters when w has substrings occurring multiple times (for example, if $\mathfrak{A} = \{a < b < c < d < \cdots\}$ and $w = bananaban$, then $\operatorname{RG}(\{[w]\}_{\text{multiset}}) = nnbbnaaaa$), and strings of consecutive equal letters can easily be compressed. (In order to guarantee that w can be recovered from the result, one can add a new letter ζ – called a "sentinel symbol" – to the alphabet $\mathfrak{A}$, and apply the Burrows-Wheeler transformation to the word

[342] This argument roughly follows [81].

[343] The Chen-Fox-Lyndon factorization (Theorem 6.1.27) provides a bijection between words in $\mathfrak{A}^*$ and multisets of Lyndon words (because the factors in the CFL factorization of a word $w \in \mathfrak{A}^*$ can be stored in a multiset), whereas the Gessel-Reutenauer bijection $\operatorname{GR}: \mathfrak{A}^* \to \mathfrak{MM}^{\mathfrak{a}}$ is a bijection between words in $\mathfrak{A}^*$ and multisets of aperiodic necklaces. Since the Lyndon words are in bijection with the aperiodic necklaces (by Exercise 6.1.34(e)), we can thus view the two bijections as having the same targets (and the same domains). That said, they are not the same bijection.

$w\zeta$ instead of w. This also ensures that $w\zeta$ is an aperiodic word, so the Burrows-Wheeler transformation can be applied to $w\zeta$ even if it cannot be applied to w.)

Kufleitner, in [116, §4], suggests a bijective variant of the Burrows-Wheeler transformation. In our notations, it sends a word $w \in \mathfrak{A}^*$ to the word $\operatorname{RG}\left(\{[a_1], [a_2], \ldots, [a_k]\}_{\text{multiset}}\right)$, where $(a_1, a_2, \ldots, a_k)$ is the CFL factorization of w.

For variants and generalizations of the Gessel-Reutenauer bijection, see [116], [209], [200], [56] and [179].

6.6.2. *The Gessel-Reutenauer symmetric functions.* In this subsection, we shall study a certain family of symmetric functions. First, we recall that every word $w \in \mathfrak{A}^*$ has a unique CFL factorization (see Theorem 6.1.27). Based on this fact, we can make the following definition:

Definition 6.6.32. For the rest of Subsection 6.6.2, we let $\mathfrak{A}$ be the alphabet $\{1 < 2 < 3 < \cdots\}$.

Let $w \in \mathfrak{A}^*$ be a word. The *CFL type* of w is defined to be the partition whose parts are the positive integers $\ell(a_1), \ell(a_2), \ldots, \ell(a_k)$ (listed in decreasing order), where $(a_1, a_2, \ldots, a_k)$ is the CFL factorization of w. This CFL type is denoted by $\operatorname{CFLtype} w$.

Example 6.6.33. Let w be the word 213212412112. Then, the tuple $(2, 132, 124, 12, 112)$ is the CFL factorization of w. Hence, the CFL type of w is the partition whose parts are the positive integers $\ell(2), \ell(132), \ell(124), \ell(12), \ell(112)$ (listed in decreasing order). In other words, the CFL type of w is the partition $(3, 3, 3, 2, 1)$ (since the positive integers $\ell(2), \ell(132), \ell(124), \ell(12), \ell(112)$ are $1, 3, 3, 2, 3$).

Definition 6.6.34. For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^*$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$. (For example, $\mathbf{x}_{(1,3,2,1)} = x_1 x_3 x_2 x_1 = x_1^2 x_2 x_3$.)

For any partition λ, we define a power series $\mathbf{GR}_\lambda \in \mathbf{k}[[\mathbf{x}]]$ by

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{CFLtype} w = \lambda}} \mathbf{x}_w.$$

Example 6.6.35. Let us compute $\mathbf{GR}_{(2,1)}$. Indeed, the words $w \in \mathfrak{A}^*$ satisfying $\operatorname{CFLtype} w = (2,1)$ are the words whose CFL factorization consists of two words, one of which has length 1 and the other has length 2. In other words, these words $w \in \mathfrak{A}^*$ must have the form $w = a_1 a_2$ for two Lyndon words a_1 and a_2 satisfying $a_1 \geq a_2$ and $(\ell(a_1), \ell(a_2)) \in \{(1,2), (2,1)\}$. A straightforward analysis of possibilities reveals that these are precisely the 3-letter words $w = (w_1, w_2, w_3)$ satisfying either ($w_1 < w_2$ and $w_1 \geq w_3$) or ($w_1 > w_2$ and $w_2 < w_3$). Hence,

$$\begin{aligned}
\mathbf{GR}_{(2,1)} &= \sum_{\substack{w \in \mathfrak{A}^*; \\ \operatorname{CFLtype} w = (2,1)}} \mathbf{x}_w = \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 < w_2 \text{ and } w_1 \geq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3}} \mathbf{x}_w \\
&= \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 < w_2 \text{ and } w_1 \geq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3 \text{ and } w_1 \leq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_1 > w_2 \text{ and } w_2 < w_3 \text{ and } w_1 > w_3}} \mathbf{x}_w \\
&\qquad \text{(here, we have split the second sum according to the relation between } w_1 \text{ and } w_3) \\
&= \sum_{\substack{w \in \mathfrak{A}^*; \\ w_3 \leq w_1 < w_2}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_2 < w_1 \leq w_3}} \mathbf{x}_w + \sum_{\substack{w \in \mathfrak{A}^*; \\ w_2 < w_3 < w_1}} \mathbf{x}_w
\end{aligned}$$

(here, we rewrote the conditions under the summation signs). The three sums on the right hand side are clearly quasisymmetric functions. Using (5.2.3), we can rewrite them as $L_{(2,1)}$, $L_{(1,2)}$ and $L_{(1,1,1)}$, respectively. Thus, we obtain

$$\begin{aligned}
\mathbf{GR}_{(2,1)} &= L_{(2,1)} + L_{(1,2)} + L_{(1,1,1)} = 3M_{(1,1,1)} + M_{(1,2)} + M_{(2,1)} \\
&= 3m_{(1,1,1)} + m_{(2,1)}.
\end{aligned}$$

Thus, $\mathbf{GR}_{(2,1)}$ is actually a symmetric function! We shall soon (in Proposition 6.6.37) see that this is not a coincidence.

We shall now state various properties of the power series $\mathbf{GR}_\lambda$; their proofs are all part of Exercise 6.6.51.

Proposition 6.6.36. *Let n be a positive integer. Then:*

(a) *The partition* (n) *satisfies*

$$\mathbf{GR}_{(n)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ w \text{ is Lyndon}}} \mathbf{x}_w.$$

(b) *Assume that* $\mathbf{k}$ *is a* $\mathbb{Q}$*-algebra. Then,*

$$\mathbf{GR}_{(n)} = \frac{1}{n} \sum_{d \mid n} \mu(d)\, p_d^{n/d}.$$

Here, μ *denotes the number-theoretical Möbius function (defined as in Exercise 2.9.6), and the summation sign "*$\sum_{d|n}$*" is understood to range over all* ***positive*** *divisors* d *of* n*.*

Proposition 6.6.37. *Let* λ *be a partition. Then, the power series* $\mathbf{GR}_\lambda$ *belongs to* Λ*.*

Thus, $(\mathbf{GR}_\lambda)_{\lambda \in \mathrm{Par}}$ is a family of symmetric functions.[344] Unlike many other such families we have studied, it is not a basis of Λ; it is not linearly independent (e.g., it satisfies $\mathbf{GR}_{(2,1,1)} = \mathbf{GR}_{(4)}$). Nevertheless, it satisfies a Cauchy-kernel-like identity[345]:

Proposition 6.6.38. *Consider two countable sets of indeterminates* $\mathbf{x} = (x_1, x_2, x_3, \ldots)$ *and* $\mathbf{y} = (y_1, y_2, y_3, \ldots)$*.*

(a) *In the power series ring* $\mathbf{k}[[\mathbf{x}, \mathbf{y}]] = \mathbf{k}[[x_1, x_2, x_3, \ldots, y_1, y_2, y_3, \ldots]]$*, we have*

$$\sum_{\lambda \in \mathrm{Par}} \mathbf{GR}_\lambda(\mathbf{x})\, p_\lambda(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} p_\lambda(\mathbf{x})\, \mathbf{GR}_\lambda(\mathbf{y}).$$

(b) *For each word* $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^*$*, we define a monomial* $\mathbf{y}_w$ *in* $\mathbf{k}[[\mathbf{y}]]$ *by setting* $\mathbf{y}_w = y_{w_1} y_{w_2} \cdots y_{w_n}$*. Then,*

$$\begin{aligned} \sum_{\lambda \in \mathrm{Par}} \mathbf{GR}_\lambda(\mathbf{x})\, p_\lambda(\mathbf{y}) &= \sum_{w \in \mathfrak{A}^*} \mathbf{x}_w p_{\mathrm{CFLtype}\, w}(\mathbf{y}) = \prod_{w \in \mathfrak{L}} \prod_{u \in \mathfrak{L}} \frac{1}{1 - \mathbf{x}_w^{\ell(u)} \mathbf{y}_u^{\ell(w)}} \\ &= \sum_{\lambda \in \mathrm{Par}} p_\lambda(\mathbf{x})\, \mathbf{GR}_\lambda(\mathbf{y}). \end{aligned}$$

The proof of this proposition rests upon the following simple equality[346]:

Proposition 6.6.39. *In the power series ring* $(\mathbf{k}[[\mathbf{x}]])[[t]]$*, we have*

$$\frac{1}{1 - p_1 t} = \prod_{w \in \mathfrak{L}} \frac{1}{1 - \mathbf{x}_w t^{\ell(w)}}.$$

We can furthermore represent the symmetric functions $\mathbf{GR}_\lambda$ in terms of the fundamental basis $(L_\alpha)_{\alpha \in \mathrm{Comp}}$ of QSym; here, the Gessel-Reutenauer bijection from Theorem 6.6.29 reveals its usefulness. We will use Definition 5.3.5.

Proposition 6.6.40. *Let* λ *be a partition. Let* $n = |\lambda|$*. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{\sigma \in \mathfrak{S}_n; \\ \sigma \text{ has cycle type } \lambda}} L_{\gamma(\sigma)}.$$

The proof of this relies on Lemma 5.3.6 (see Exercise 6.6.51 below for the details).

Definition 6.6.41. Let $\mathfrak{S} = \bigsqcup_{n \in \mathbb{N}} \mathfrak{S}_n$ (an external disjoint union). For each $\sigma \in \mathfrak{S}$, we let $\mathrm{type}\, \sigma$ denote the cycle type of σ.

[344] Several sources, including [82], [206, Exercise 7.89] and [66], write L_λ for what we call $\mathbf{GR}_\lambda$. (So would we if L_α didn't already have another meaning here.)

[345] Recall that $\mathfrak{L}$ denotes the set of Lyndon words in $\mathfrak{A}^*$.

[346] Recall that $\mathfrak{L}$ denotes the set of Lyndon words in $\mathfrak{A}^*$. Also, recall that $\mathfrak{A} = \{1 < 2 < 3 < \cdots\}$. Thus, $p_1 = \sum_{i \geq 1} x_i = \sum_{a \in \mathfrak{A}} x_a$.

Proposition 6.6.42. *Consider two countable sets of indeterminates* $\mathbf{x} = (x_1, x_2, x_3, \ldots)$ *and* $\mathbf{y} = (y_1, y_2, y_3, \ldots)$. *In the power series ring* $\mathbf{k}[[\mathbf{x}, \mathbf{y}]]$, *we have*

$$\sum_{\lambda \in \mathrm{Par}} \mathbf{GR}_\lambda(\mathbf{x})\, p_\lambda(\mathbf{y}) = \sum_{\lambda \in \mathrm{Par}} p_\lambda(\mathbf{x})\, \mathbf{GR}_\lambda(\mathbf{y}) = \sum_{\sigma \in \mathfrak{S}} L_{\gamma(\sigma)}(\mathbf{x})\, p_{\mathrm{type}\,\sigma}(\mathbf{y}).$$

Let us finally give two alternative descriptions of the $\mathbf{GR}_\lambda$ that do not rely on the notion of CFL factorization. First, we state a fact that is essentially trivial:

Proposition 6.6.43. *Let* N *be a necklace. Let* w *and* w' *be two elements of* N. *Then:*

(a) *There exist words* u *and* v *such that* $w = uv$ *and* $w' = vu$.
(b) *We have* $\mathbf{x}_w = \mathbf{x}_{w'}$.

Definition 6.6.44. Let $N \in \mathfrak{N}$ be a necklace. Then, we define a monomial $\mathbf{x}_N$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_N = \mathbf{x}_w$, where w is any element of N. (This is well-defined, because Proposition 6.6.43(b) shows that $\mathbf{x}_w$ does not depend on the choice of w.)

Definition 6.6.45. Let M be a finite multiset of necklaces. Then, we define a monomial $\mathbf{x}_M$ in $\mathbf{k}[[\mathbf{x}]]$ by setting $\mathbf{x}_M = \mathbf{x}_{N_1}\mathbf{x}_{N_2}\cdots\mathbf{x}_{N_k}$, where M is written in the form $M = \{N_1, N_2, \ldots, N_k\}_{\mathrm{multiset}}$.

Definition 6.6.46. Let M be a finite multiset of necklaces. Then, we can obtain a partition by listing the sizes of the necklaces in M in decreasing order. This partition will be called the *type* of M, and will be denoted by $\mathrm{type}\, M$.

Example 6.6.47. If $M = \{[13], [13], [2], [223]\}_{\mathrm{multiset}}$, then the type of M is $(3, 2, 2, 1)$ (because the sizes of the necklaces in M are $2, 2, 1, 3$).

Proposition 6.6.48. *Let* λ *be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{M \in \mathfrak{M}\mathfrak{N}^{\mathfrak{a}}; \\ \mathrm{type}\, M = \lambda}} \mathbf{x}_M.$$

This was our first alternative description of $\mathbf{GR}_\lambda$. Note that it is used as a definition of $\mathbf{GR}_\lambda$ in [82, (2.1)] (where $\mathbf{GR}_\lambda$ is denoted by L_λ). Using the Gessel-Reutenauer bijection, we can restate it as follows:

Proposition 6.6.49. *Let* λ *be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \mathrm{type}(\mathrm{GR}\, w) = \lambda}} \mathbf{x}_w.$$

Let us finally give a second alternative description of $\mathbf{GR}_\lambda$:

Proposition 6.6.50. *Let* λ *be a partition. Then,*

$$\mathbf{GR}_\lambda = \sum_{\substack{w \in \mathfrak{A}^*; \\ \mathrm{type}(\mathrm{std}\, w) = \lambda}} \mathbf{x}_w.$$

Exercise 6.6.51. Prove all statements made in Subsection 6.6.2.

[**Hint:** Here is one way to proceed:

- First prove Proposition 6.6.39, by using the CFL factorization to argue that both sides equal $\sum_{w \in \mathfrak{A}^*} \mathbf{x}_w t^{\ell(w)}$.
- Use a similar argument to derive Proposition 6.6.38 (starting with part (b)).
- Proposition 6.6.43 is almost trivial.
- Derive Proposition 6.6.48 from the definition of $\mathbf{GR}_\lambda$ using the uniqueness of the CFL factorization.
- Derive Proposition 6.6.49 from Proposition 6.6.48 using the bijectivity of GR.
- Derive Proposition 6.6.50 from Proposition 6.6.49.
- Obtain Proposition 6.6.40 by combining Proposition 6.6.50 with Lemma 5.3.6.
- Derive Proposition 6.6.42 from Propositions 6.6.40 and 6.6.38.

- Derive Proposition 6.6.37 either from Proposition 6.6.48 or from Proposition 6.6.38. (In the latter case, make sure to work with $\mathbf{k} = \mathbb{Q}$ first, and then extend to all other $\mathbf{k}$, as the proof will rely on the $\mathbf{k}$-linear independence of $(p_\lambda)_{\lambda \in \mathrm{Par}}$, which doesn't hold for all $\mathbf{k}$.)
- Prove Proposition 6.6.36(a) directly using the definition of $\mathbf{GR}_{(n)}$.
- Show that each positive integer n satisfies $p_1^n = \sum_{d|n} d \cdot \mathbf{GR}_{(d)} \left(x_1^{n/d}, x_2^{n/d}, x_3^{n/d}, \ldots\right)$ by taking logarithms in Proposition 6.6.39. Use this and (2.9.7) to prove Proposition 6.6.36(b) recursively.

Other approaches are, of course, possible.]

Remark 6.6.52. Let n be a positive integer. The symmetric function $\mathbf{GR}_{(n)}$ has a few more properties:

(a) It is an $\mathbb{N}$-linear combination of Schur functions. To state the precise rule, we need a few more notations: A *standard tableau* can be defined as a column-strict tableau T with $\mathrm{cont}(T) = (1^m)$, where m is the number of boxes of T. (That is, each of the numbers $1, 2, \ldots, m$ appears exactly once in T, and no other numbers appear.) If T is a standard tableau with m boxes, then a *descent* of T means an $i \in \{1, 2, \ldots, m-1\}$ such that the entry $i+1$ appears in T in a row further down than i does. The *major index* $\mathrm{maj}\, T$ of a standard tableau T is defined to be the sum of its descents.[347] Now,

$$\mathbf{GR}_{(n)} = \sum_{\lambda \in \mathrm{Par}_n} a_{\lambda,1} s_\lambda,$$

where $a_{\lambda,1}$ is the number of standard tableaux T of shape λ satisfying $\mathrm{maj}\, T \equiv 1 \bmod n$. (See [206, Exercise 7.89 (c)].)

(b) Assume that $\mathbf{k} = \mathbb{C}$. Recall the map $\mathrm{ch} : A(\mathfrak{S}) \to \Lambda$ from Theorem 4.4.1. Embed the cyclic group $C_n = \mathbb{Z}/n\mathbb{Z}$ as a subgroup in the symmetric group $\mathfrak{S}_n$ by identifying some generator g of C_n with some n-cycle in $\mathfrak{S}_n$. Let ω be a primitive n-th root of unity in $\mathbb{C}$ (for instance, $\exp(2\pi i/n)$). Let $\gamma : C_n \to \mathbb{C}$ be the character of C_n that sends each $g^i \in C_n$ to ω^i. Then,

$$\mathbf{GR}_{(n)} = \mathrm{ch}\left(\mathrm{Ind}_{C_n}^{\mathfrak{S}_n} \gamma\right).$$

(See [206, Exercise 7.89 (b)].)

(c) The character $\mathrm{Ind}_{C_n}^{\mathfrak{S}_n} \gamma$ of $\mathfrak{S}_n$ is actually the character of a representation. To construct it, set $\mathbf{k} = \mathbb{C}$, and recall the notations from Exercise 6.1.41 (while keeping $\mathfrak{A} = \{1, 2, 3, \ldots\}$). Let $\mathfrak{m}_n$ be the $\mathbb{C}$-vector subspace of $T(V)$ spanned by the products $x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ with $\sigma \in \mathfrak{S}_n$. The symmetric group $\mathfrak{S}_n$ acts on $T(V)$ by algebra homomorphisms, with $\sigma \in \mathfrak{S}_n$ sending each x_i to $x_{\sigma(i)}$ when $i \leq n$ and to x_i otherwise. Both $\mathfrak{g}_n$ and $\mathfrak{m}_n$ are $\mathbb{C}\mathfrak{S}_n$-submodules of $T(V)$. Thus, so is the intersection $\mathfrak{g}_n \cap \mathfrak{m}_n$. It is not hard to see that this intersection is spanned by all "nested commutators" $\left[x_{\sigma(1)}, \left[x_{\sigma(2)}, \left[x_{\sigma(3)}, \ldots\right]\right]\right]$ (in $T(V)$) with $\sigma \in \mathfrak{S}_n$. The character of this $\mathbb{C}\mathfrak{S}_n$-module $\mathfrak{g}_n \cap \mathfrak{m}_n$ is precisely the $\mathrm{Ind}_{C_n}^{\mathfrak{S}_n} \gamma$ from Remark 6.6.52(b), so applying the Frobenius characteristic map ch to it yields the symmetric function $\mathbf{GR}_{(n)}$. (See [182, Theorem 9.41(i)]. There are similar ways to obtain $\mathbf{GR}_\lambda$ for all $\lambda \in \mathrm{Par}$.)

Exercise 6.6.53. Prove the claim of Remark 6.6.52(b).

[**Hint:** It helps to recall (or prove) that for any positive integer m, the sum of all primitive m-th roots of unity in $\mathbb{C}$ is $\mu(m)$.]

The symmetric functions $\mathbf{GR}_\lambda$ for more general partitions λ can be expressed in terms of the symmetric functions $\mathbf{GR}_{(n)}$ (which, as we recall from Proposition 6.6.36(b), have a simple expression in terms of the p_m) using the concept of *plethysm*; see [82, Theorem 3.6].

In [82], Gessel and Reutenauer apply the symmetric functions $\mathbf{GR}_\lambda$ to questions of permutation enumeration via the following result[348]:

[347] For example, the tableau

$$\begin{array}{cccc} 1 & 3 & 4 & 8 \\ 2 & 5 & 6 & 9 \\ 7 & & & \end{array}$$

is standard and has descents $1, 4, 6, 8$ and major index $1 + 4 + 6 + 8 = 19$.

[348] Proposition 6.6.54(a) is [82, Corollary 2.2]; Proposition 6.6.54(b) is [82, Theorem 2.1].

Proposition 6.6.54. *Let $n \in \mathbb{N}$. Let $\lambda \in \operatorname{Par}_n$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in \operatorname{Comp}_n$. We shall use the notations introduced in Definition 5.1.10. Definition 5.3.5 and Definition 6.6.41.*

(a) *Let $\mu \in \operatorname{Par}_n$ be the partition obtained by sorting the entries of β into decreasing order. Then,*

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \text{ such that } \beta \text{ refines } \gamma(\sigma)) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \text{ and } \operatorname{Des}\sigma \subset D(\beta)) \\
&= \left(\text{the coefficient of } x_1^{\beta_1} x_2^{\beta_2} \cdots x_k^{\beta_k} \text{ in } \mathbf{GR}_\lambda\right) = (\text{the coefficient of } \mathbf{x}^\mu \text{ in } \mathbf{GR}_\lambda) \\
&= (\mathbf{GR}_\lambda, h_\mu) \qquad (\text{this is the Hall inner product of } \mathbf{GR}_\lambda \in \Lambda \text{ and } h_\mu \in \Lambda).
\end{aligned}$$

(b) *Recall the ribbon diagram $\operatorname{Rib}(\beta)$ corresponding to the composition β (defined as in Definition 5.1.10). Then,*

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \text{ and } \beta = \gamma(\sigma)) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{type}\sigma = \lambda \text{ and } \operatorname{Des}\sigma = D(\beta)) \\
&= \left(\mathbf{GR}_\lambda, s_{\operatorname{Rib}(\beta)}\right) \qquad \left(\text{this is the Hall inner product of } \mathbf{GR}_\lambda \in \Lambda \text{ and } s_{\operatorname{Rib}(\beta)} \in \Lambda\right).
\end{aligned}$$

Exercise 6.6.55. Prove Proposition 6.6.54.

[**Hint:** Use Proposition 6.6.40, Theorem 5.4.10, the equality (5.4.3) and the adjointness between π and i in Corollary 5.4.3.]

By strategic application of Proposition 6.6.54, Gessel and Reutenauer arrive at several enumerative consequences, such as the following:

- ([82, Theorem 8.3]) If A is a proper subset of $\{1, 2, \ldots, n-1\}$, then

$$\begin{aligned}
&(\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } |\operatorname{Fix}\sigma| = 0 \text{ and } \operatorname{Des}\sigma = A) \\
&= (\text{the number of permutations } \sigma \in \mathfrak{S}_n \text{ satisfying } |\operatorname{Fix}\sigma| = 1 \text{ and } \operatorname{Des}\sigma = A),
\end{aligned}$$

  where $\operatorname{Fix}\sigma$ denotes the set of all fixed points of a permutation σ. This can also be proved bijectively; such a bijective proof can be obtained by combining [50, Theorems 5.1 and 6.1].
- ([82, Theorem 9.4]) If $i \in \{1, 2, \ldots, n-1\}$, then

$$(\text{the number of } n\text{-cycles } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}\sigma = \{i\}) = \sum_{d \mid \gcd(n,i)} \mu(d) \binom{n/d}{i/d}.$$

  Note that this also equals the number of necklaces $[(w_1, w_2, \ldots, w_n)]$ (or, equivalently, Lyndon words $(w_1, w_2, \ldots, w_n)$) with $w_1, w_2, \ldots, w_n \in \{0, 1\}$ and $w_1 + w_2 + \cdots + w_n = i$. This suggests that there should be a bijection between $\{n\text{-cycles } \sigma \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}\sigma = \{i\}\}$ and the set of such necklaces; and indeed, such a bijection can be found in [45, Theorem 1].

See [82] and [66] for more such applications.

7. Aguiar-Bergeron-Sottile character theory Part I: QSym as a terminal object

It turns out that the universal mapping property of NSym as a free associative algebra leads via duality to a universal property for its dual QSym, elegantly explaining several combinatorial invariants that take the form of quasisymmetric or symmetric functions:

- Ehrenborg's quasisymmetric function of a *ranked poset* [64],
- Stanley's *chromatic* symmetric function of a *graph* [205],
- the quasisymmetric function of a *matroid* considered in [21].

7.1. Characters and the universal property.

Definition 7.1.1. Given a Hopf algebra A over $\mathbf{k}$, a *character* is an algebra morphism $A \xrightarrow{\zeta} \mathbf{k}$, that is,

- $\zeta(1_A) = 1_{\mathbf{k}}$,
- ζ is $\mathbf{k}$-linear, and
- $\zeta(ab) = \zeta(a)\zeta(b)$ for a, b in A.

Example 7.1.2. A particularly important character for $A = \mathrm{QSym}$ is defined as follows:[349]

$$\begin{array}{rcl} \mathrm{QSym} & \xrightarrow{\zeta_Q} & \mathbf{k}, \\ f(\mathbf{x}) & \longmapsto & f(1,0,0,\ldots) = [f(\mathbf{x})]_{x_1=1, x_2=x_3=\cdots=0}. \end{array}$$

Hence,

$$\zeta_Q(M_\alpha) = \zeta_Q(L_\alpha) = \begin{cases} 1, & \text{if } \alpha = (n) \text{ for some } n; \\ 0, & \text{otherwise.} \end{cases}$$

In other words, the restriction $\zeta_Q|_{\mathrm{QSym}_n}$ coincides with the functional H_n in $\mathrm{NSym}_n = \mathrm{Hom}_{\mathbf{k}}(\mathrm{QSym}_n, \mathbf{k})$: one has for f in QSym_n that

$$\zeta_Q(f) = (H_n, f). \tag{7.1.1}$$

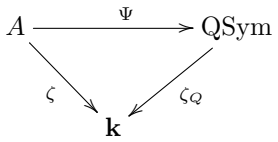
It is worth remarking that there is nothing special about setting $x_1 = 1$ and $x_2 = x_3 = \cdots = 0$: for quasisymmetric f, we could have defined the same character ζ_Q by picking any variable, say x_n, and sending

$$f(\mathbf{x}) \longmapsto [f(\mathbf{x})]_{\substack{x_n=1, \text{ and} \\ x_m=0 \text{ for } m \neq n}}.$$

This character $\mathrm{QSym} \xrightarrow{\zeta_Q} \mathbf{k}$ has a certain universal property, known as the *Aguiar-Bergeron-Sottile universality theorem* (part of [4, Theorem 4.1]):

Theorem 7.1.3. *Let A be a connected graded Hopf algebra, and let $A \xrightarrow{\zeta} \mathbf{k}$ be a character. Then, there is a unique graded Hopf morphism $A \xrightarrow{\Psi} \mathrm{QSym}$ making the following diagram commute:*

(7.1.2)



Furthermore, Ψ is given by the following formula on homogeneous elements:

$$\Psi(a) = \sum_{\alpha \in \mathrm{Comp}_n} \zeta_\alpha(a) M_\alpha \qquad \text{for all } n \in \mathbb{N} \text{ and } a \in A_n, \tag{7.1.3}$$

where for $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, the map ζ_α is the composite

$$A_n \xrightarrow{\Delta^{(\ell-1)}} A^{\otimes \ell} \xrightarrow{\pi_\alpha} A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_\ell} \xrightarrow{\zeta^{\otimes \ell}} \mathbf{k}$$

in which $A^{\otimes \ell} \xrightarrow{\pi_\alpha} A_{\alpha_1} \otimes \cdots \otimes A_{\alpha_\ell}$ is the canonical projection.

[349] We are using the notation of Proposition 5.1.9 here, and we are still identifying QSym with $\mathrm{QSym}(\mathbf{x})$, where $\mathbf{x}$ denotes the infinite chain $(x_1 < x_2 < \cdots)$.

Proof. One argues that Ψ is unique, and has formula (7.1.3), using only that ζ is $\mathbf{k}$-linear and sends 1 to 1 and that Ψ is a graded $\mathbf{k}$-*coalgebra* map making (7.1.2) commute. Equivalently, consider the adjoint $\mathbf{k}$-*algebra* map[350]

$$\mathrm{NSym} = \mathrm{QSym}^o \xrightarrow{\Psi^*} A^o.$$

Commutativity of (7.1.2) implies that for a in A_n,

$$(\Psi^*(H_n), a) = (H_n, \Psi(a)) \overset{(7.1.1)}{=} \zeta_Q(\Psi(a)) = \zeta(a),$$

whereas gradedness of Ψ^* yields that $(\Psi^*(H_m), a) = 0$ whenever $a \in A_n$ and $m \neq n$. In other words, $\Psi^*(H_n)$ is the element of A^o defined as the following functional on A:

$$\Psi^*(H_n)(a) = \begin{cases} \zeta(a), & \text{if } a \in A_n; \\ 0, & \text{if } a \in A_m \text{ for some } m \neq n. \end{cases} \tag{7.1.4}$$

By the universal property for $\mathrm{NSym} \cong \mathbf{k}\langle H_1, H_2, \ldots \rangle$ as free associative $\mathbf{k}$-algebra, we see that any choice of a $\mathbf{k}$-linear map $A \xrightarrow{\zeta} \mathbf{k}$ uniquely produces a $\mathbf{k}$-algebra morphism $\Psi^* : \mathrm{QSym}^o \to A^o$ which satisfies (7.1.4) for all $n \geq 1$. It is easy to see that this Ψ^* then automatically satisfies (7.1.4) for $n = 0$ as well if ζ sends 1 to 1 (it is here that we use $\zeta(1) = 1$ and the connectedness of A). Hence, any given $\mathbf{k}$-linear map $A \xrightarrow{\zeta} \mathbf{k}$ sending 1 to 1 uniquely produces a $\mathbf{k}$-algebra morphism $\Psi^* : \mathrm{QSym}^o \to A^o$ which satisfies (7.1.4) for all $n \geq 0$. Formula (7.1.3) follows as

$$\Psi(a) = \sum_{\alpha \in \mathrm{Comp}} (H_\alpha, \Psi(a))\ M_\alpha$$

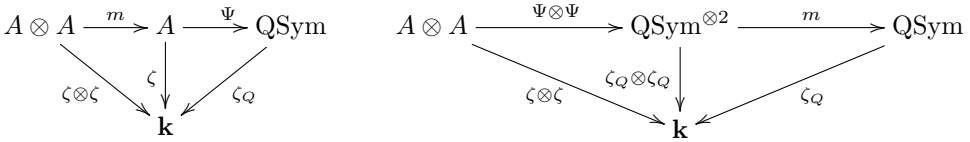
and for a composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, one has

$$\begin{aligned} (H_\alpha, \Psi(a)) = (\Psi^*(H_\alpha), a) &= (\Psi^*(H_{\alpha_1}) \cdots \Psi^*(H_{\alpha_\ell}), a) \\ &= \left(\Psi^*(H_{\alpha_1}) \otimes \cdots \otimes \Psi^*(H_{\alpha_\ell}), \Delta^{(\ell-1)}(a)\right) \\ &\overset{(7.1.4)}{=} \left(\zeta^{\otimes \ell} \circ \pi_\alpha\right)\left(\Delta^{(\ell-1)}(a)\right) = \zeta_\alpha(a), \end{aligned}$$

where the definition of ζ_α was used in the last equality.

We wish to show that if, in addition, A is a Hopf algebra and $A \xrightarrow{\zeta} \mathbf{k}$ is a character (i.e., an algebra morphism), then $A \xrightarrow{\Psi} \mathrm{QSym}$ will be an algebra morphism, that is, the two maps $A \otimes A \longrightarrow \mathrm{QSym}$ given by $\Psi \circ m$ and $m \circ (\Psi \otimes \Psi)$ coincide. To see this, consider these two diagrams having the two maps in question as the composites of their top rows:

(7.1.5)



The fact that ζ, ζ_Q are algebra morphisms makes the above diagrams commute, so that applying the uniqueness in the first part of the proof to the character $A \otimes A \xrightarrow{\zeta \otimes \zeta} \mathbf{k}$ proves the desired equality $\Psi \circ m = m \circ (\Psi \otimes \Psi)$. □

Remark 7.1.4. When one assumes in addition that A is cocommutative, it follows that the image of Ψ will lie in the subalgebra $\Lambda \subset \mathrm{QSym}$, e.g. from the explicit formula (7.1.3) and the fact that one will have $\zeta_\alpha = \zeta_\beta$ whenever β is a rearrangement of α. In other words, the character $\Lambda \xrightarrow{\zeta_\Lambda} \mathbf{k}$ defined by restricting ζ_Q to Λ, or by

$$\zeta_\Lambda(m_\lambda) = \begin{cases} 1, & \text{if } \lambda = (n) \text{ for some } n; \\ 0, & \text{otherwise,} \end{cases}$$

has a universal property as terminal object with respect to characters on cocommutative Hopf algebras.

[350]Here we are using the fact that there is a 1-to-1 correspondence between graded $\mathbf{k}$-linear maps $A \to \mathrm{QSym}$ and graded $\mathbf{k}$-linear maps $\mathrm{QSym}^o \to A^o$ given by $f \mapsto f^*$, and this correspondence has the property that a given graded map $f : A \to \mathrm{QSym}$ is a $\mathbf{k}$-coalgebra morphism if and only if f^* is a $\mathbf{k}$-algebra morphism. This is a particular case of Exercise 1.6.1(f).

The graded Hopf morphism Ψ in Theorem 7.1.3 will be called the *map* $A \to \mathrm{QSym}$ *induced by the character* ζ.

We close this section by discussing a well-known polynomiality and reciprocity phenomenon; see, e.g., Humpert and Martin [103, Prop. 2.2], Stanley [205, §4].

Definition 7.1.5. The *binomial Hopf algebra* (over the commutative ring $\mathbf{k}$) is the polynomial algebra $\mathbf{k}[m]$ in a single variable m, with a Hopf algebra structure transported from the symmetric algebra $\mathrm{Sym}\left(\mathbf{k}^1\right)$ (which is a Hopf algebra by virtue of Example 1.3.14, applied to $V = \mathbf{k}^1$) along the isomorphism $\mathrm{Sym}\left(\mathbf{k}^1\right) \to \mathbf{k}[m]$ which sends the standard basis element of $\mathbf{k}^1$ to m. Thus the element m is primitive; that is, $\Delta m = 1 \otimes m + m \otimes 1$ and $S(m) = -m$. As S is an algebra anti-endomorphism by Proposition 1.4.10 and $\mathbf{k}[m]$ is commutative, one has $S(g)(m) = g(-m)$ for all polynomials $g(m)$ in $\mathbf{k}[m]$.

Definition 7.1.6. For an element $f(\mathbf{x})$ in QSym and a nonnegative integer m, let $\mathrm{ps}^1(f)(m)$ denote the element of $\mathbf{k}$ obtained by *principal specialization at* $q = 1$

$$\begin{aligned}\mathrm{ps}^1(f)(m) &= [f(\mathbf{x})]_{\substack{x_1=x_2=\cdots=x_m=1,\\ x_{m+1}=x_{m+2}=\cdots=0}} \\ &= f(\underbrace{1,1,\ldots,1}_{m \text{ ones}},0,0,\ldots).\end{aligned}$$

Proposition 7.1.7. *Assume that* $\mathbb{Q}$ *is a subring of* $\mathbf{k}$. *The map* ps^1 *has the following properties.*

(i) *Let* $f \in \mathrm{QSym}$. *There is a unique polynomial in* $\mathbf{k}[m]$ *which agrees for each nonnegative integer* m *with* $\mathrm{ps}^1(f)(m)$, *and which, by abuse of notation, we will also denote* $\mathrm{ps}^1(f)(m)$. *If* f *lies in* QSym_n, *then* $\mathrm{ps}^1(f)(m)$ *is a polynomial of degree at most* n, *taking these values on* M_α, L_α *for* $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ *in* Comp_n:

$$\begin{aligned}\mathrm{ps}^1(M_\alpha)(m) &= \binom{m}{\ell}, \\ \mathrm{ps}^1(L_\alpha)(m) &= \binom{m-\ell+n}{n}.\end{aligned}$$

(ii) *The map* $\mathrm{QSym} \xrightarrow{\mathrm{ps}^1} \mathbf{k}[m]$ *is a Hopf morphism into the binomial Hopf algebra.*

(iii) *For all* m *in* $\mathbb{Z}$ *and* f *in* QSym *one has*

$$\zeta_Q^{\star m}(f) = \mathrm{ps}^1(f)(m).$$

In particular, one also has

$$\zeta_Q^{\star(-m)}(f) = \mathrm{ps}^1(S(f))(m) = \mathrm{ps}^1(f)(-m).$$

(iv) *For a graded Hopf algebra* A *with a character* $A \xrightarrow{\zeta} \mathbf{k}$, *and any element* a *in* A_n, *the polynomial* $\mathrm{ps}^1(\Psi(a))(m)$ *in* $\mathbf{k}[m]$ *has degree at most* n, *and when specialized to* m *in* $\mathbb{Z}$ *satisfies*

$$\zeta^{\star m}(a) = \mathrm{ps}^1(\Psi(a))(m).$$

Proof. To prove assertion (i), note that one has

$$\begin{aligned}\mathrm{ps}^1(M_\alpha)(m) = M_\alpha(1,1,\ldots,1,0,0,\ldots) &= \sum_{1 \le i_1 < \cdots < i_\ell \le m} \left[x_{i_1}^{\alpha_1} \cdots x_{i_\ell}^{\alpha_\ell}\right]_{x_j=1} = \binom{m}{\ell}, \\ \mathrm{ps}^1(L_\alpha)(m) = L_\alpha(1,1,\ldots,1,0,0,\ldots) &= \sum_{\substack{1 \le i_1 \le \cdots \le i_n \le m: \\ i_k < i_{k+1} \text{ if } k \in D(\alpha)}} [x_{i_1} \cdots x_{i_n}]_{x_j=1} \\ &= |\{1 \le j_1 \le j_2 \le \cdots \le j_n \le m-\ell+1\}| = \binom{m-\ell+n}{n}.\end{aligned}$$

As $\{M_\alpha\}_{\alpha \in \mathrm{Comp}_n}$ form a basis for QSym_n, and $\binom{m}{\ell}$ is a polynomial function in m of degree $\ell(\le n)$, one concludes that for f in QSym_n one has that $\mathrm{ps}^1(f)(m)$ is a polynomial function in m of degree at most n. The polynomial giving rise to this function is unique, since infinitely many of its values are fixed.

To prove assertion (ii), note that ps^1 is an algebra morphism because it is an evaluation homomorphism. To check that it is a coalgebra morphism, it suffices to check $\Delta \circ \mathrm{ps}^1 = (\mathrm{ps}^1 \otimes \mathrm{ps}^1) \circ \Delta$ on each M_α for $\alpha = (\alpha_1, \ldots, \alpha_\ell)$ in Comp_n. Using the Vandermonde summation $\binom{A+B}{\ell} = \sum_k \binom{A}{k}\binom{B}{\ell-k}$, one has

$$(\Delta \circ \mathrm{ps}^1)(M_\alpha) = \Delta \binom{m}{\ell} = \binom{m \otimes 1 + 1 \otimes m}{\ell} = \sum_{k=0}^{\ell} \binom{m \otimes 1}{k}\binom{1 \otimes m}{\ell - k} = \sum_{k=0}^{\ell} \binom{m}{k} \otimes \binom{m}{\ell - k}$$

while at the same time

$$\left((\mathrm{ps}^1 \otimes \mathrm{ps}^1) \circ \Delta\right)(M_\alpha) = \sum_{k=0}^{\ell} \mathrm{ps}^1(M_{(\alpha_1,\ldots,\alpha_k)}) \otimes \mathrm{ps}^1(M_{(\alpha_{k+1},\ldots,\alpha_\ell)}) = \sum_{k=0}^{\ell} \binom{m}{k} \otimes \binom{m}{\ell - k}.$$

Thus ps^1 is a bialgebra morphism, and hence also a Hopf morphism, by Corollary 1.4.27.

For assertion (iii), first assume m lies in $\{0, 1, 2, \ldots\}$. Since $\zeta_Q(f) = f(1, 0, 0, \ldots)$, one has

$$\begin{aligned}
\zeta_Q^{\star m}(f) &= \zeta_Q^{\otimes m} \circ \Delta^{(m-1)} f(\mathbf{x}) = \zeta_Q^{\otimes m}\left(f(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)})\right) \\
&= \left[f(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)})\right]_{\substack{x_1^{(1)}=x_1^{(2)}=\cdots=x_1^{(m)}=1, \\ x_2^{(j)}=x_3^{(j)}=\cdots=0 \text{ for all } j}} \\
&= f(1,0,0,\ldots,1,0,0,\ldots,\cdots,1,0,0,\ldots) = f(\underbrace{1,1,\ldots,1}_{m \text{ ones}},0,0,\ldots) = \mathrm{ps}^1(f)(m).
\end{aligned}$$

[351] But then Proposition 1.4.26(a) also implies

$$\begin{aligned}
\zeta_Q^{\star(-m)}(f) &= \left(\zeta_Q^{\star(-1)}\right)^{\star m}(f) = (\zeta_Q \circ S)^{\star m}(f) = \zeta_Q^{\star m}(S(f)) \\
&= \mathrm{ps}^1(S(f))(m) = S(\mathrm{ps}^1(f))(m) = \mathrm{ps}^1(f)(-m).
\end{aligned}$$

For assertion (iv), note that

$$\zeta^{\star m}(a) = (\zeta_Q \circ \Psi)^{\star m}(a) = (\zeta_Q^{\star m})(\Psi(a)) = \mathrm{ps}^1(\Psi(a))(m),$$

where the three equalities come from (7.1.2), Proposition 1.4.26(a), and assertion (iii) above, respectively. □

Remark 7.1.8. Aguiar, Bergeron and Sottile give a very cute (third) proof of the QSym antipode formula Theorem 5.1.11, via Theorem 7.1.3, in [4, Example 4.8]. They apply Theorem 7.1.3 to the *coopposite coalgebra* QSym^{cop} and its character $\zeta_Q^{\star(-1)}$. One can show that the map $\mathrm{QSym}^{cop} \xrightarrow{\Psi} \mathrm{QSym}$ induced by $\zeta_Q^{\star(-1)}$ is $\Psi = S$, the antipode of QSym, because $S : \mathrm{QSym} \to \mathrm{QSym}$ is a coalgebra anti-endomorphism (by Exercise 1.4.28) satisfying $\zeta_Q^{\star(-1)} = \zeta_Q \circ S$. They then use the formula (7.1.3) for $\Psi = S$ (together with the polynomiality Proposition 7.1.7) to derive Theorem 5.1.11.

Exercise 7.1.9. Show that $\zeta_Q^{\star m}(f) = \mathrm{ps}^1(f)(m)$ for all $f \in \mathrm{QSym}$ and $m \in \{0, 1, 2, \ldots\}$. (This was already proven in Proposition 7.1.7(iii); give an alternative proof using Proposition 5.1.7.)

7.2. **Example: Ehrenborg's quasisymmetric function of a ranked poset.** Here we consider incidence algebras, coalgebras and Hopf algebras generally, and then particularize to the case of graded posets, to recover Ehrenborg's interesting quasisymmetric function invariant via Theorem 7.1.3.

7.2.1. *Incidence algebras, coalgebras, Hopf algebras.*

Definition 7.2.1. Given a family $\mathcal{P}$ of finite partially ordered sets P, let $\mathbf{k}[\mathcal{P}]$ denote the free $\mathbf{k}$-module whose basis consists of symbols $[P]$ corresponding to isomorphism classes of posets P in $\mathcal{P}$.

We will assume throughout that each P in $\mathcal{P}$ is *bounded*, that is, it has a unique minimal element $\hat{0} := \hat{0}_P$ and a unique maximal element $\hat{1} := \hat{1}_P$. In particular, $P \neq \varnothing$, although it is allowed that $|P| = 1$, so that $\hat{0} = \hat{1}$; denote this isomorphism class of posets with one element by $[o]$.

If $\mathcal{P}$ is closed under taking intervals

$$[x, y] := [x, y]_P := \{z \in P : x \leq_P z \leq_P y\},$$

[351] See Exercise 7.1.9 for an alternative way to prove this, requiring less thought to verify its soundness.

then one can easily see that the following coproduct and counit endow $\mathbf{k}[\mathcal{P}]$ with the structure of a coalgebra, called the *(reduced) incidence coalgebra*:

$$\Delta[P] := \sum_{x \in P} [\hat{0}, x] \otimes [x, \hat{1}],$$

$$\epsilon[P] := \begin{cases} 1, & \text{if } |P| = 1; \\ 0, & \text{otherwise.} \end{cases}$$

The dual algebra $\mathbf{k}[\mathcal{P}]^*$ is generally called the *reduced incidence algebra (modulo isomorphism)* for the family $\mathcal{P}$ (see, e.g., [192]). It contains the important element $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$, called the *$\zeta$-function* that takes the value $\zeta[P] = 1$ for all P.

If $\mathcal{P}$ (is not empty and) satisfies the further property of being *hereditary* in the sense that for every P_1, P_2 in $\mathcal{P}$, the *Cartesian product poset* $P_1 \times P_2$ with componentwise partial order is also in $\mathcal{P}$, then one can check that the following product and unit endow $\mathbf{k}[\mathcal{P}]$ with the structure of a (commutative) algebra:

$$[P_1] \cdot [P_2] := m([P_1] \otimes [P_2]) := [P_1 \times P_2],$$
$$1_{\mathbf{k}[\mathcal{P}]} := [o].$$

Proposition 7.2.2. *For any hereditary family $\mathcal{P}$ of finite posets, $\mathbf{k}[\mathcal{P}]$ is a bialgebra, and even a Hopf algebra with antipode S given as in (1.4.7) (Takeuchi's formula):*

$$S[P] = \sum_{k \geq 0} (-1)^k \sum_{\hat{0} = x_0 < \cdots < x_k = \hat{1}} [x_0, x_1] \cdots [x_{k-1}, x_k].$$

Proof. Checking the commutativity of the pentagonal diagram in (1.3.4) amounts to the fact that, for any $(x_1, x_2) <_{P_1 \times P_2} (y_1, y_2)$, one has a poset isomorphism

$$[(x_1, x_2)\ ,\ (y_1, y_2)]_{P_1 \times P_2} \cong [x_1, y_1]_{P_1} \times [x_2, y_2]_{P_2}.$$

Commutativity of the remaining diagrams in (1.3.4) is straightforward, and so $\mathbf{k}[\mathcal{P}]$ is a bialgebra. But then Remark 1.4.25 implies that it is a Hopf algebra, with antipode S as in (1.4.7), because the map $f := \mathrm{id}_{\mathbf{k}[\mathcal{P}]} - u\epsilon$ (sending the class $[o]$ to 0, and fixing all other $[P]$) is locally $\star$-nilpotent:

$$f^{\star k}[P] = \sum_{\hat{0} = x_0 < \cdots < x_k = \hat{1}} [x_0, x_1] \cdots [x_{k-1}, x_k]$$

will vanish due to an empty sum whenever k exceeds the maximum length of a chain in the finite poset P. □

It is perhaps worth remarking how this generalizes the Möbius function formula of P. Hall. Note that the zeta function $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$ is a *character*, that is, an algebra morphism. Proposition 1.4.26(a) then tells us that ζ should have a convolutional inverse $\mathbf{k}[\mathcal{P}] \xrightarrow{\mu = \zeta^{\star -1}} \mathbf{k}$, traditionally called the *Möbius function*, with the formula $\mu = \zeta^{\star -1} = \zeta \circ S$. Rewriting this via the antipode formula for S given in Proposition 7.2.2 yields P. Hall's formula.

Corollary 7.2.3. *For a finite bounded poset P, one has*

$$\mu[P] = \sum_{k \geq 0} (-1)^k |\{\textit{chains } \hat{0} = x_0 < \cdots < x_k = \hat{1} \textit{ in } P\}|.$$

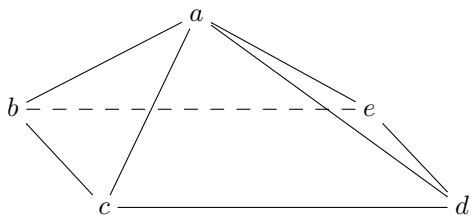
We can also notice that S is an algebra anti-endomorphism (by Proposition 1.4.10), thus an algebra endomorphism (since $\mathbf{k}[\mathcal{P}]$ is commutative, so Exercise 1.5.8(a) shows that the algebra anti-endomorphisms of $\mathbf{k}[\mathcal{P}]$ are the same as the algebra endomorphisms of $\mathbf{k}[\mathcal{P}]$). Hence, $\mu = \zeta \circ S$ is a composition of two algebra homomorphisms, thus an algebra homomorphism itself. We therefore obtain the following classical fact:

Corollary 7.2.4. *For two finite bounded posets P and Q, we have $\mu[P \times Q] = \mu[P] \cdot \mu[Q]$.*

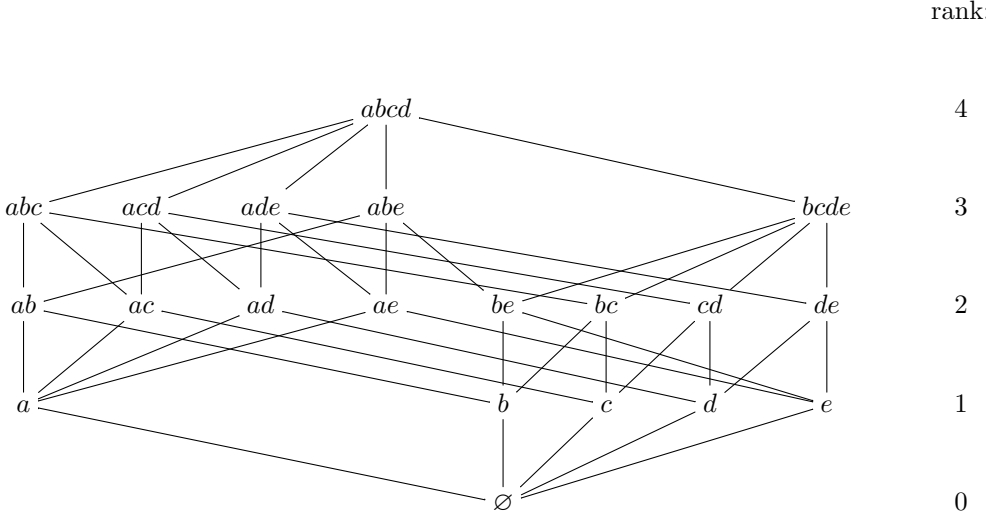
7.2.2. *The incidence Hopf algebras for ranked posets and Ehrenborg's function.*

Definition 7.2.5. Take $\mathcal{P}$ to be the class of bounded *ranked* finite posets P, that is, those for which all maximal chains from $\hat{0}$ to $\hat{1}$ have the same length $r(P)$. This is a hereditary class, as it implies that any interval is $[x, y]_P$ is also ranked, and the product of two bounded ranked posets is also bounded and ranked. It also uniquely defines a *rank function* $P \xrightarrow{r} \mathbb{N}$ in which $r(\hat{0}) = 0$ and $r(x)$ is the length of any maximal chain from $\hat{0}$ to x.

Example 7.2.6. Consider a pyramid with apex vertex a over a square base with vertices b, c, d, e:



Ordering its faces by inclusion gives a bounded ranked poset P, where the rank of an element is one more than the dimension of the face it represents:



Definition 7.2.7. *Ehrenborg's quasisymmetric function* $\Psi[P]$ for a bounded ranked poset P is the image of $[P]$ under the map $\mathbf{k}[\mathcal{P}] \xrightarrow{\Psi} \mathrm{QSym}$ induced by the zeta function $\mathbf{k}[\mathcal{P}] \xrightarrow{\zeta} \mathbf{k}$ as a character, via Theorem 7.1.3.

The quasisymmetric function $\Psi[P]$ captures several interesting combinatorial invariants of P; see Stanley [206, Chap. 3] for more background on these notions.

Definition 7.2.8. Let P be a bounded ranked poset P of rank $r(P) := r(\hat{1})$. Define its *rank-generating function*

$$RGF(P, q) := \sum_{p \in P} q^{r(p)} \in \mathbb{Z}[q],$$

its *characteristic polynomial*

$$\chi(P, q) := \sum_{p \in P} \mu(\hat{0}, p) q^{r(p)} \in \mathbb{Z}[q]$$

(where $\mu(u, v)$ is shorthand for $\mu([u, v])$), and its *zeta polynomial*

$$Z(P, m) = |\{\text{multichains } \hat{0} \leq_P p_1 \leq_P \cdots \leq_P p_{m-1} \leq_P \hat{1}\}| \tag{7.2.1}$$

$$= \sum_{s=0}^{r(P)-1} \binom{m}{s+1} |\{\text{chains } \hat{0} < p_1 < \cdots < p_s < \hat{1}\}| \in \mathbb{Q}[m] \tag{7.2.2}$$

[352]. Also, for each subset $S \subset \{1, 2, \ldots, r(P)-1\}$, define the *flag number* f_S of P by

$$f_S = |\{\text{chains } \hat{0} <_P p_1 <_P \cdots <_P p_s <_P \hat{1} \text{ with } \{r(p_1), \ldots, r(p_s)\} = S\}|.$$

These flag numbers are the components of the *flag f-vector* $(f_S)_{S\subset[r-1]}$ of P. Further define the *flag h-vector* $(h_T)_{T\subset[r-1]}$ of P, whose entries h_T are given by $f_S = \sum_{T\subset S} h_T$, or, equivalently[353], by $h_S = \sum_{T\subset S}(-1)^{|S\setminus T|} f_T$.

Example 7.2.9. For the poset P in Example 7.2.6, one has $RGF(P,q) = 1 + 5q + 8q^2 + 5q^3 + q^4$. Since P is the poset of faces of a polytope, the Möbius function values for its intervals are easily predicted: $\mu(x,y) = (-1)^{r[x,y]}$, that is, P is an *Eulerian ranked poset*; see Stanley [206, §3.16]. Hence its characteristic polynomial is trivially related to the rank generating function, sending $q \mapsto -q$, that is,

$$\chi(P,q) = RGF(P,-q) = 1 - 5q + 8q^2 - 5q^3 + q^4.$$

Its flag f-vector and h-vector entries are given in the following table.

S	f_S		h_S
$\varnothing$	1		1
$\{1\}$	5	$5-1=$	4
$\{2\}$	8	$8-1=$	7
$\{3\}$	5	$5-1=$	4
$\{1,2\}$	16	$16-(5+8)+1=$	4
$\{1,3\}$	16	$16-(5+5)+1=$	7
$\{2,3\}$	16	$16-(5+8)+1=$	4
$\{1,2,3\}$	32	$32-(16+16+16)+(5+8+5)-1=$	1

and using (7.2.2), its zeta polynomial is

$$Z(P,m) = 1\binom{m}{1} + (5+8+5)\binom{m}{2} + (16+16+16)\binom{m}{3} + 32\binom{m}{4} = \frac{m^2(2m-1)(2m+1)}{3}.$$

Theorem 7.2.10. *Assume that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Ehrenborg's quasisymmetric function $\Psi[P]$ for a bounded ranked poset P encodes*

(i) *the flag f-vector entries f_S and flag h-vector entries h_S as its M_α and L_α expansion coefficients*[354] *:*

$$\Psi[P] = \sum_\alpha f_{D(\alpha)}(P)\ M_\alpha = \sum_\alpha h_{D(\alpha)}(P)\ L_\alpha,$$

(ii) *the zeta polynomial as the specialization from Definition 7.1.6*

$$Z(P,m) = \mathrm{ps}^1(\Psi[P])(m) = [\Psi[P]]_{\substack{x_1=x_2=\cdots=x_m=1,\\ x_{m+1}=x_{m+2}=\cdots=0}},$$

(iii) *the rank-generating function as the specialization*

$$RGF(P,q) = [\Psi[P]]_{\substack{x_1=q, x_2=1,\\ x_3=x_4=\cdots=0}},$$

(iv) *the characteristic polynomial as the convolution*

$$\chi(P,q) = ((\psi_q \circ S) \star \zeta_Q) \circ \Psi[P],$$

where $\mathrm{QSym} \xrightarrow{\psi_q} \mathbf{k}[q]$ *maps* $f(\mathbf{x}) \longmapsto f(q,0,0,\ldots)$.

Proof. In assertion (i), the expansion $\Psi[P] = \sum_\alpha f_{D(\alpha)}(P)\, M_\alpha$ is (7.1.3), since $\zeta_\alpha[P] = f_{D(\alpha)}(P)$. The L_α expansion follows from this, as $L_\alpha = \sum_{\beta: D(\beta)\supset D(\alpha)} M_\beta$ and $f_S(P) = \sum_{T\subset S} h_T$.

Assertion (ii) is immediate from Proposition 7.1.7(iv), since $Z(P,m) = \zeta^{\star m}[P]$.

[352] Actually, (7.2.2) is false if $|P| = 1$ (but only then). We use (7.2.1) to define $Z(P,m)$ in this case.

[353] The equivalence follows from inclusion-exclusion (more specifically, from the converse of Lemma 5.2.6(a)).

[354] In fact, Ehrenborg *defined* $\Psi[P]$ in [64, Defn. 4.1] via this M_α expansion, and then showed that it gave a Hopf morphism.

Assertion (iii) can be deduced from assertion (i), but it is perhaps more fun and in the spirit of things to proceed as follows. Note that $\psi_q(M_\alpha) = q^n$ for $\alpha = (n)$, and $\psi_q(M_\alpha)$ vanishes for all other $\alpha \neq (n)$ in Comp_n. Hence for a bounded ranked poset P one has

$$(\psi_q \circ \Psi)[P] = q^{r(P)}. \tag{7.2.3}$$

But if we treat $\zeta_Q : \mathrm{QSym} \to \mathbf{k}$ as a map $\mathrm{QSym} \to \mathbf{k}[q]$, then (1.4.2) (applied to $\mathbf{k}[\mathcal{P}]$, QSym, $\mathbf{k}[q]$, $\mathbf{k}[q]$, Ψ, $\mathrm{id}_{\mathbf{k}[q]}$, ψ_q and ζ_Q instead of C, C', A, A', γ, α, f and g) shows that

$$(\psi_q \star \zeta_Q) \circ \Psi = (\psi_q \circ \Psi) \star (\zeta_Q \circ \Psi), \tag{7.2.4}$$

since $\Psi : \mathbf{k}[\mathcal{P}] \to \mathrm{QSym}$ is a $\mathbf{k}$-coalgebra homomorphism. Consequently, one can compute

$$\begin{aligned} RGF(P,q) &= \sum_{p \in P} q^{r(p)} \cdot 1 = \sum_{p \in P} q^{r([\hat{0},p])} \cdot \zeta[p,\hat{1}] \overset{\substack{(7.2.3),\\(7.1.2)}}{=} \sum_{p \in P} (\psi_q \circ \Psi)[\hat{0},p] \cdot (\zeta_Q \circ \Psi)[p,\hat{1}] \\ &= ((\psi_q \circ \Psi) \star (\zeta_Q \circ \Psi))[P] \overset{(7.2.4)}{=} (\psi_q \star \zeta_Q)(\Psi[P]) = (\psi_q \otimes \zeta_Q)(\Delta\Psi[P]) \\ &= [\Psi[P](\mathbf{x},\mathbf{y})]_{\substack{x_1=q, x_2=x_3=\cdots=0 \\ y_1=1, y_2=y_3=\cdots=0}} = [\Psi[P](\mathbf{x})]_{\substack{x_1=q, x_2=1, \\ x_3=x_4=\cdots=0}}. \end{aligned}$$

Similarly, for assertion (iv) first note that

$$((\psi_q \circ S) \star \zeta_Q) \circ \Psi = (\psi_q \circ S \circ \Psi) \star (\zeta_Q \circ \Psi), \tag{7.2.5}$$

(this is proven similarly to (7.2.4), but now using the map $\psi_q \circ S$ instead of ψ_q). Now, Proposition 7.2.2 and Corollary 7.2.3 let one calculate that

$$\begin{aligned} (\psi_q \circ \Psi \circ S)[P] &= \sum_k (-1)^k \sum_{\hat{0}=x_0<\cdots<x_k=\hat{1}} (\psi_q \circ \Psi)([x_0,x_1]) \cdots (\psi_q \circ \Psi)([x_{k-1},x_k]) \\ &\overset{(7.2.3)}{=} \sum_k (-1)^k \sum_{\hat{0}=x_0<\cdots<x_k=\hat{1}} q^{r(P)} = \mu(\hat{0},\hat{1}) q^{r(P)}. \end{aligned}$$

This is used in the penultimate equality here:

$$\begin{aligned} ((\psi_q \circ S) \star \zeta_Q) \circ \Psi[P] &\overset{(7.2.5)}{=} ((\psi_q \circ S \circ \Psi) \star (\zeta_Q \circ \Psi))[P] = ((\psi_q \circ \Psi \circ S) \star \zeta)[P] \\ &= \sum_{p \in P} (\psi_q \circ \Psi \circ S)[\hat{0},p] \cdot \zeta[p,\hat{1}] = \sum_{p \in P} \mu[\hat{0},p] q^{r(p)} = \chi(P,q). \end{aligned}$$

□

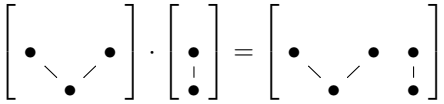
7.3. **Example: Stanley's chromatic symmetric function of a graph.** We introduce the *chromatic Hopf algebra of graphs* and an associated character ζ so that the map Ψ from Theorem 7.1.3 sends a graph G to Stanley's *chromatic symmetric function* of G. Then principal specialization ps^1 sends this to the *chromatic polynomial* of the graph.

7.3.1. *The chromatic Hopf algebra of graphs.*

Definition 7.3.1. The *chromatic Hopf algebra* (see Schmitt [194, §3.2]) $\mathcal{G}$ is a free $\mathbf{k}$-module whose $\mathbf{k}$-basis elements $[G]$ are indexed by isomorphism classes of (finite) simple graphs $G = (V,E)$. Define for $G_1 = (V_1,E_1), G_2 = (V_2,E_2)$ the multiplication

$$[G_1] \cdot [G_2] := [G_1 \sqcup G_2]$$

where $[G_1 \sqcup G_2]$ denote the isomorphism class of the disjoint union, on vertex set $V = V_1 \sqcup V_2$ which is a disjoint union of copies of their vertex sets V_1, V_2, with edge set $E = E_1 \sqcup E_2$. For example,



Thus the class $[\varnothing]$ of the empty graph $\varnothing$ having $V = \varnothing, E = \varnothing$ is a unit element.

Given a graph $G = (V, E)$ and a subset $V' \subset V$, the *subgraph induced on vertex set* V' is defined as the graph $G|_{V'} := (V', E')$ with edge set $E' = \{e \in E : e = \{v_1, v_2\} \subset V'\}$. This lets one define a comultiplication $\Delta : \mathcal{G} \to \mathcal{G} \otimes \mathcal{G}$ by setting

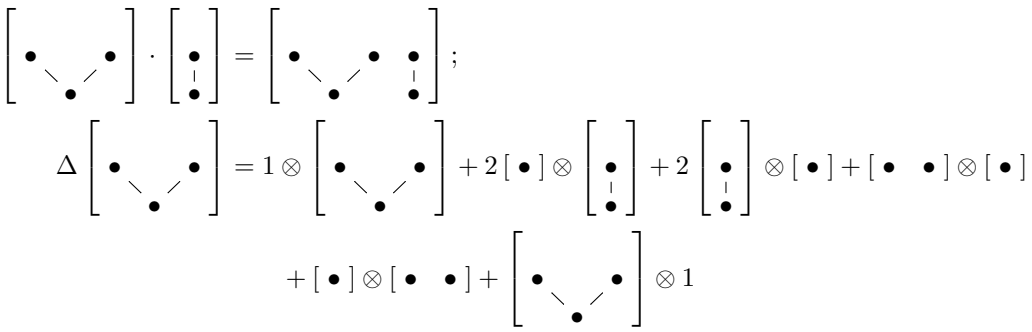
$$\Delta[G] := \sum_{(V_1,V_2):V_1 \sqcup V_2 = V} [G|_{V_1}] \otimes [G|_{V_2}].$$

Define a counit $\epsilon : \mathcal{G} \to \mathbf{k}$ by

$$\epsilon[G] := \begin{cases} 1, & \text{if } G = \varnothing; \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 7.3.2. *The above maps endow $\mathcal{G}$ with the structure of a connected graded finite type Hopf algebra over $\mathbf{k}$, which is both commutative and cocommutative.*

Example 7.3.3. Here are some examples of these structure maps:



Proof of Proposition 7.3.2. The associativity of the multiplication and comultiplication should be clear as

$$m^{(2)}([G_1] \otimes [G_2] \otimes [G_3]) = [G_1 \sqcup G_2 \sqcup G_3],$$
$$\Delta^{(2)}[G] = \sum_{\substack{(V_1,V_2,V_3): \\ V = V_1 \sqcup V_2 \sqcup V_3}} [G|_{V_1}] \otimes [G|_{V_2}] \otimes [G|_{V_3}].$$

Checking the unit and counit conditions are straightforward. Commutativity of the pentagonal bialgebra diagram in (1.3.4) comes down to check that, given graphs G_1, G_2 on disjoint vertex sets V_1, V_2 , when one applies to $[G_1] \otimes [G_2]$ either the composite $\Delta \circ m$ or the composite $(m \otimes m) \circ (\mathrm{id} \otimes T \otimes \mathrm{id}) \circ (\Delta \otimes \Delta)$, the result is the same:

$$\sum_{\substack{(V_{11},V_{12},V_{21},V_{22}): \\ V_1 = V_{11} \sqcup V_{12} \\ V_2 = V_{21} \sqcup V_{22}}} [G_1|_{V_{11}} \sqcup G_2|_{V_{21}}] \otimes [G_1|_{V_{12}} \sqcup G_2|_{V_{22}}].$$

Letting $\mathcal{G}_n$ be the $\mathbf{k}$-span of $[G]$ having n vertices makes $\mathcal{G}$ a bialgebra which is graded and connected, and hence also a Hopf algebra by Proposition 1.4.16. Cocommutativity should be clear, and commutativity follows from the graph isomorphism $G_1 \sqcup G_2 \cong G_2 \sqcup G_1$. Finally, $\mathcal{G}$ is of finite type since there are only finitely many isomorphism classes of simple graphs on n vertices for every given n. □

Remark 7.3.4. Humpert and Martin [103, Theorem 3.1] gave the following expansion for the antipode in the chromatic Hopf algebra, containing fewer terms than Takeuchi's general formula (1.4.7): given a graph $G = (V, E)$, one has

$$S[G] = \sum_F (-1)^{|V| - \mathrm{rank}(F)} \, \mathrm{acyc}(G/F)[G_{V,F}]. \tag{7.3.1}$$

Here F runs over all subsets of edges that form *flats* in the graphic matroid for G, meaning that if $e = \{v, v'\}$ is an edge in E for which one has a path of edges in F connecting v to v', then e also lies in F. Here G/F denotes the quotient graph in which all of the edges of F have been *contracted*, while $\mathrm{acyc}(G/F)$ denotes its number of *acyclic orientations*, and $G_{V,F} := (V, F)$ as a simple graph.[355]

[355]The notation $\mathrm{rank}(F)$ denotes the *rank* of F in the graphic matroid of G. We can define it without reference to matroid theory as the maximum cardinality of a subset F' of F such that the graph $G_{V,F'}$ is acyclic. Equivalently, $\mathrm{rank}(F)$ is $|V| - c(F)$,

Remark 7.3.5. In [14], Benedetti, Hallam and Machacek define a Hopf algebra of simplicial complexes, which contains $\mathcal{G}$ as a Hopf subalgebra (and also has $\mathcal{G}$ as a quotient Hopf algebra). They compute a formula for its antipode similar to (and generalizing) (7.3.1).

Remark 7.3.6. The chromatic Hopf algebra $\mathcal{G}$ is used in [122] and [39, §14.4] to study *Vassiliev invariants of knots*. In fact, a certain quotient of $\mathcal{G}$ (named $\mathcal{F}$ in [122] and $\mathcal{L}$ in [39, §14.4]) is shown to naturally host invariants of *chord diagrams* and therefore Vassiliev invariants of knots.

Remark 7.3.7. The $\mathbf{k}$-algebra $\mathcal{G}$ is isomorphic to a polynomial algebra (in infinitely many indeterminates) over $\mathbf{k}$. Indeed, every finite graph can be uniquely written as a disjoint union of finitely many connected finite graphs (up to order). Therefore, the basis elements $[G]$ of $\mathcal{G}$ corresponding to connected finite graphs G are algebraically independent in $\mathcal{G}$ and generate the whole $\mathbf{k}$-algebra $\mathcal{G}$ (indeed, the disjoint unions of connected finite graphs are precisely the monomials in these elements). Thus, $\mathcal{G}$ is isomorphic to a polynomial $\mathbf{k}$-algebra with countably many generators (one for each isomorphism class of connected finite graphs). As a consequence, for example, we see that $\mathcal{G}$ is an integral domain if $\mathbf{k}$ is an integral domain.

7.3.2. *A "ribbon basis" for $\mathcal{G}$ and self-duality.* In this subsection, we shall explore a second basis of $\mathcal{G}$ and a bilinear form on $\mathcal{G}$. This material will not be used in the rest of these notes (except in Exercise 7.3.25), but it is of some interest and provides an example of how a commutative cocommutative Hopf algebra can be studied.

First, let us define a second basis of $\mathcal{G}$, which is obtained by Möbius inversion (in an appropriate sense) from the standard basis $([G])_{[G] \text{ is an isomorphism class of finite graphs}}$:

Definition 7.3.8. For every finite graph $G = (V, E)$, set

$$[G]^\sharp = \sum_{\substack{H=(V,E');\\ E' \supset E^c}} (-1)^{\left|E' \setminus E^c\right|} [H] \in \mathcal{G},$$

where E^c denotes the complement of the subset E in the set of all two-element subsets of V. Clearly, $[G]^\sharp$ depends only on the isomorphism class $[G]$ of G, not on G itself.

Proposition 7.3.9. (a) *Every finite graph $G = (V, E)$ satisfies*

$$[G] = \sum_{\substack{H=(V,E');\\ E' \cap E = \varnothing}} [H]^\sharp .$$

(b) *The elements $[G]^\sharp$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$.*

(c) *For any graph $H = (V, E)$, we have*

$$\Delta\left([H]^\sharp\right) = \sum_{\substack{(V_1,V_2);\\ V = V_1 \sqcup V_2;\\ H = H|_{V_1} \sqcup H|_{V_2}}} [H|_{V_1}]^\sharp \otimes [H|_{V_2}]^\sharp . \tag{7.3.2}$$

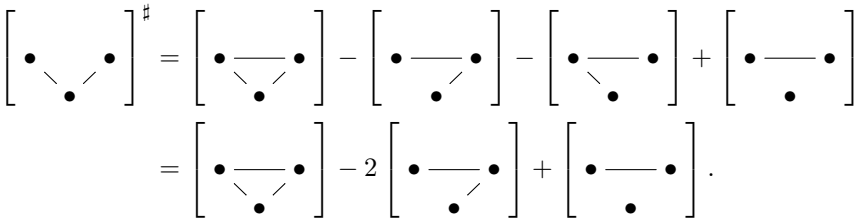
(d) *For any two graphs $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$, we have*

$$[H_1]^\sharp [H_2]^\sharp = \sum_{\substack{H=(V_1 \sqcup V_2, E);\\ H|_{V_1} = H_1;\\ H|_{V_2} = H_2}} [H]^\sharp . \tag{7.3.3}$$

---

where $c(F)$ denotes the number of connected components of the graph $G_{V,F}$. Thus, the equality (7.3.1) can be rewritten as $S[G] = \sum_F (-1)^{c(F)} \operatorname{acyc}(G/F)[G_{V,F}]$. In this form, this equality is also proven in [15, Thm. 7.1].

For example,



Proving Proposition 7.3.9 is part of Exercise 7.3.14 further below.

The equalities that express the elements $[G]^\sharp$ in terms of the elements $[H]$ (as in Definition 7.3.8), and vice versa (Proposition 7.3.9(a)), are reminiscent of the relations (5.4.10) and (5.4.9) between the bases (R_α) and (H_α) of NSym. In this sense, we can call the basis of $\mathcal{G}$ formed by the $[G]^\sharp$ a "ribbon basis" of $\mathcal{G}$.

We now define a $\mathbf{k}$-bilinear form on $\mathcal{G}$:

Definition 7.3.10. For any two graphs G and H, let $\operatorname{Iso}(G,H)$ denote the set of all isomorphisms from G to H [356]. Let us now define a $\mathbf{k}$-bilinear form $(\cdot,\cdot):\mathcal{G}\times\mathcal{G}\to\mathbf{k}$ on $\mathcal{G}$ by setting

$$\left(\left[G\right]^\sharp,\left[H\right]\right)=\left|\operatorname{Iso}(G,H)\right|.$$

[357]

Proposition 7.3.11. *The form $(\cdot,\cdot):\mathcal{G}\times\mathcal{G}\to\mathbf{k}$ is symmetric.*

Again, we refer to Exercise 7.3.14 for a proof of Proposition 7.3.11.

The basis of $\mathcal{G}$ constructed in Proposition 7.3.9(b) and the bilinear form $(\cdot,\cdot)$ defined in Definition 7.3.10 can be used to construct a Hopf algebra homomorphism from $\mathcal{G}$ to its graded dual $\mathcal{G}^o$:

Definition 7.3.12. For any finite graph G, let $\operatorname{aut}(G)$ denote the number $|\operatorname{Iso}(G,G)|$. Notice that this is a positive integer, since the set $\operatorname{Iso}(G,G)$ is nonempty (it contains id_G).

Now, recall that the Hopf algebra $\mathcal{G}$ is a connected graded Hopf algebra of finite type. The n-th homogeneous component is spanned by the $[G]$ where G ranges over the graphs with n vertices. Since $\mathcal{G}$ is of finite type, its graded dual $\mathcal{G}^o$ is defined. Let $\left(\left[G\right]^*\right)_{[G]\text{ is an isomorphism class of finite graphs}}$ be the basis of $\mathcal{G}^o$ dual to the basis $\left(\left[G\right]\right)_{[G]\text{ is an isomorphism class of finite graphs}}$ of $\mathcal{G}$. Define a $\mathbf{k}$-linear map $\psi:\mathcal{G}\to\mathcal{G}^o$ by

$$\psi\left(\left[G\right]^\sharp\right)=\operatorname{aut}(G)\cdot\left[G\right]^* \qquad \text{for every finite graph } G.$$

[358]

Proposition 7.3.13. *Consider the map $\psi:\mathcal{G}\to\mathcal{G}^o$ defined in Definition 7.3.12.*

(a) *This map ψ satisfies $(\psi(a))(b)=(a,b)$ for all $a\in\mathcal{G}$ and $b\in\mathcal{G}$.*
(b) *The map $\psi:\mathcal{G}\to\mathcal{G}^o$ is a Hopf algebra homomorphism.*
(c) *If $\mathbb{Q}$ is a subring of $\mathbf{k}$, then the map ψ is a Hopf algebra isomorphism $\mathcal{G}\to\mathcal{G}^o$.*

Exercise 7.3.14. Prove Proposition 7.3.9, Proposition 7.3.11 and Proposition 7.3.13.

---

[356] We recall that if $G=(V,E)$ and $H=(W,F)$ are two graphs, then an *isomorphism* from G to H means a bijection $\varphi:V\to W$ such that $\varphi_*(E)=F$. Here, φ_* denotes the map from the powerset of V to the powerset of W which sends every $T\subset V$ to $\varphi(T)\subset W$.

[357] This is well-defined, because:

- the number $|\operatorname{Iso}(G,H)|$ depends only on the isomorphism classes $[G]$ and $[H]$ of G and H, but not on G and H themselves;
- the elements $[G]^\sharp$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$ (because of Proposition 7.3.9(b));
- the elements $[G]$, where $[G]$ ranges over all isomorphism classes of finite graphs, form a basis of the $\mathbf{k}$-module $\mathcal{G}$.

[358] This is well-defined, since $\left(\left[G\right]^\sharp\right)_{[G]\text{ is an isomorphism class of finite graphs}}$ is a basis of the $\mathbf{k}$-module $\mathcal{G}$ (because of Proposition 7.3.9(b)).

Remark 7.3.15. Proposition 7.3.13(c) shows that the Hopf algebra $\mathcal{G}$ is self-dual when $\mathbb{Q}$ is a subring of $\mathbf{k}$. On the other hand, if $\mathbf{k}$ is a field of positive characteristic, then $\mathcal{G}$ is never self-dual. Here is a quick way to see this: The elements $[G]^*$ of $\mathcal{G}^o$ defined in Definition 7.3.12 have the property that

$$\left([\circ]^*\right)^n = n! \cdot \sum_{\substack{[G] \text{ is an isomorphism} \\ \text{class of finite graphs on} \\ n \text{ vertices}}} [G]^*$$

for every $n \in \mathbb{N}$, where $\circ$ denotes the graph with one vertex.[359] Thus, if p is a prime and $\mathbf{k}$ is a field of characteristic p, then $\left([\circ]^*\right)^p = 0$. Hence, the $\mathbf{k}$-algebra $\mathcal{G}^o$ has nilpotents in this situation. However, the $\mathbf{k}$-algebra $\mathcal{G}$ does not (indeed, Remark 7.3.7 shows that it is an integral domain whenever $\mathbf{k}$ is an integral domain). Thus, when $\mathbf{k}$ is a field of characteristic p, then $\mathcal{G}$ and $\mathcal{G}^o$ are not isomorphic as $\mathbf{k}$-algebras (let alone as Hopf algebras).

7.3.3. *Stanley's chromatic symmetric function of a graph.*

Definition 7.3.16. *Stanley's chromatic symmetric function* $\Psi[G]$ for a simple graph $G = (V, E)$ is the image of $[G]$ under the map $\mathcal{G} \xrightarrow{\Psi} \mathrm{QSym}$ induced via Theorem 7.1.3 from the *edge-free character* $\mathcal{G} \xrightarrow{\zeta} \mathbf{k}$ defined by

$$\zeta[G] = \begin{cases} 1, & \text{if } G \text{ has no edges, that is, } G \text{ is an independent/stable set of vertices;} \\ 0, & \text{otherwise.} \end{cases} \tag{7.3.4}$$

Note that, because $\mathcal{G}$ is cocommutative, $\Psi[G]$ is symmetric and not just quasisymmetric; see Remark 7.1.4.

Recall that for a graph $G = (V, E)$, a (vertex-)coloring $f : V \to \{1, 2, \ldots\}$ is called *proper* if no edge $e = \{v, v'\}$ in E has $f(v) = f(v')$.

Proposition 7.3.17. *For a graph $G = (V, E)$, the symmetric function $\Psi[G]$ has the expansion* [360]

$$\Psi[G] = \sum_{\substack{\text{proper colorings} \\ f: V \to \{1,2,\ldots\}}} \mathbf{x}_f$$

where $\mathbf{x}_f := \prod_{v \in V} x_{f(v)}$. In particular, its specialization from Proposition 7.1.6 gives the chromatic polynomial of G:

$$\mathrm{ps}^1 \Psi[G](m) = \chi_G(m) = \left|\{\text{proper colorings } f : V \to \{1, 2, \ldots, m\}\}\right|.$$

Proof. The iterated coproduct $\mathcal{G} \xrightarrow{\Delta^{(\ell-1)}} \mathcal{G}^{\otimes \ell}$ sends

$$[G] \longmapsto \sum_{\substack{(V_1, \ldots, V_\ell): \\ V = V_1 \sqcup \cdots \sqcup V_\ell}} [G|_{V_1}] \otimes \cdots \otimes [G|_{V_\ell}]$$

and the map $\zeta^{\otimes \ell}$ sends each addend on the right to 1 or 0, depending upon whether each $V_i \subset V$ is a stable set or not, that is, whether the assignment of color i to the vertices in V_i gives a proper coloring of G. Thus formula (7.1.3) shows that the coefficient ζ_α of $x_1^{\alpha_1} \cdots x_\ell^{\alpha_\ell}$ in $\Psi[G]$ counts the proper colorings f in which $|f^{-1}(i)| = \alpha_i$ for each i. □

Example 7.3.18. For the complete graph K_n on n vertices, one has

$$\Psi[K_n] = n! e_n, \qquad \text{thus}$$

$$\begin{aligned} \mathrm{ps}^1(\Psi[K_n])(m) &= n! e_n(\underbrace{1, 1, \ldots, 1}_{m \text{ ones}}) = n! \binom{m}{n} \\ &= m(m-1)\cdots(m-(n-1)) = \chi_{K_n}(m). \end{aligned}$$

In particular, the single vertex graph K_1 has $\Psi[K_1] = e_1$, and since the Hopf morphism Ψ is in particular an algebra morphism, a graph $K_1^{\sqcup n}$ having n isolated vertices and no edges will have $\Psi[K_1^{\sqcup n}] = e_1^n$.

[359] To see this, observe that the tensor $[\circ]^{\otimes n}$ appears in the iterated coproduct $\Delta^{(n-1)}([G])$ exactly $n!$ times whenever G is a graph on n vertices.

[360] In fact, Stanley *defined* $\Psi[G]$ in [205, Defn. 2.1] via this expansion.

As a slightly more interesting example, the graph P_3 which is a path having three vertices and two edges will have

$$\Psi[P_3] = m_{(2,1)} + 6m_{(1,1,1)} = e_2e_1 + 3e_3.$$

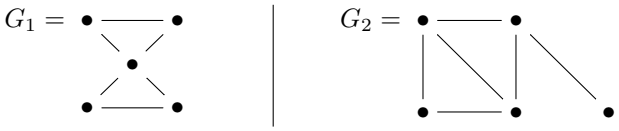
One might wonder, based on the previous examples, when $\Psi[G]$ is *e-positive*, that is, when does its unique expansion in the $\{e_\lambda\}$ basis for Λ have nonnegative coefficients? This is an even stronger assertion than *s-positivity*, that is, having nonnegative coefficients for the expansion in terms of Schur functions $\{s_\lambda\}$, since each e_λ is s-positive. This weaker property fails, starting with the *claw graph* $K_{3,1}$, which has

$$\Psi[K_{3,1}] = s_{(3,1)} - s_{(2,2)} + 5s_{(2,1,1)} + 8s_{(1,1,1,1)}.$$

On the other hand, a result of Gasharov [75, Theorem 2] shows that one at least has s-positivity for $\Psi[\mathrm{inc}(P)]$ where $\mathrm{inc}(P)$ is the *incomparability graph* of a poset which is $(\mathbf{3}+\mathbf{1})$-free; we refer the reader to Stanley [205, §5] for a discussion of the following conjecture, which remains open[361]:

Conjecture 7.3.19. *For any $(\mathbf{3}+\mathbf{1})$-free poset P, the incomparability graph $\mathrm{inc}(P)$ has $\Psi[\mathrm{inc}(P)]$ an e-positive symmetric function.*

Here is another question about $\Psi[G]$: how well does it distinguish nonisomorphic graphs? Stanley gave this example of two graphs G_1, G_2 having $\Psi[G_1] = \Psi[G_2]$:



At least $\Psi[G]$ appears to do better at distinguishing *trees*, much better than its specialization, the chromatic polynomial $\chi_G(m)$, which takes the same value $m(m-1)^{n-1}$ on all trees with n vertices.

Question 7.3.20. Does the chromatic symmetric function (for $\mathbf{k} = \mathbb{Z}$) distinguish trees?

It has been checked that the answer is affirmative for trees on 23 vertices or less. There are also interesting partial results on this question by Martin, Morin and Wagner [161].

We close this section with a few other properties of $\Psi[G]$ proven by Stanley which follow easily from the theory we have developed. For example, his work makes no explicit mention of the chromatic Hopf algebra $\mathcal{G}$, and the fact that Ψ is a Hopf morphism (although he certainly notes the trivial algebra morphism property $\Psi[G_1 \sqcup G_2] = \Psi[G_1]\Psi[G_2]$). One property he proves is implicitly related to Ψ as a coalgebra morphism: he considers (in the case when $\mathbb{Q}$ is a subring of $\mathbf{k}$) the effect on Ψ of the operator $\frac{\partial}{\partial p_1} : \Lambda_{\mathbb{Q}} \longrightarrow \Lambda_{\mathbb{Q}}$ which acts by first expressing a symmetric function $f \in \Lambda_{\mathbb{Q}}$ as a polynomial in the power sums $\{p_n\}$, and then applies the partial derivative operator $\frac{\partial}{\partial p_1}$ of the polynomial ring $\mathbb{Q}[p_1, p_2, p_3, \ldots]$. It is not hard to see that $\frac{\partial}{\partial p_1}$ is the same as the skewing operator $s^\perp_{(1)} = p^\perp_1$: both act as derivations on $\Lambda_{\mathbb{Q}} = \mathbb{Q}[p_1, p_2, \ldots]$ (since $p_1 \in \Lambda_{\mathbb{Q}}$ is primitive), and agree in their effect on each p_n, in that both send $p_1 \mapsto 1$, and both annihilate $p_2, p_3, \ldots$.

Proposition 7.3.21. *(Stanley [205, Cor. 2.12(a)]) For any graph $G = (V, E)$, one has*

$$\frac{\partial}{\partial p_1}\Psi[G] = \sum_{v \in V} \Psi[G|_{V \setminus v}].$$

Proof. Since Ψ is a coalgebra homomorphism, we have

$$\Delta\Psi[G] = (\Psi \otimes \Psi)\Delta[G] = \sum_{\substack{(V_1,V_2):\\ V = V_1 \sqcup V_2}} \Psi[G|_{V_1}] \otimes \Psi[G|_{V_2}].$$

Using this expansion (and the equality $\frac{\partial}{\partial p_1} = s^\perp_{(1)}$), we now compute

$$\frac{\partial}{\partial p_1}\Psi[G] = s^\perp_{(1)}\Psi[G] = \sum_{\substack{(V_1,V_2):\\ V = V_1 \sqcup V_2}} (s_{(1)}, \Psi[G|_{V_1}]) \cdot \Psi[G|_{V_2}] = \sum_{v \in V} \Psi[G|_{V \setminus v}]$$

(since degree considerations force $(s_{(1)}, \Psi[G|_{V_1}]) = 0$ unless $|V_1| = 1$, in which case $\Psi[G|_{V_1}] = s_{(1)}$). □

[361] A recent refinement for incomparability graphs of posets which are both $(\mathbf{3}+\mathbf{1})$- and $(\mathbf{2}+\mathbf{2})$-free, also known as *unit interval orders* is discussed by Shareshian and Wachs [198].

Definition 7.3.22. Given a graph $G = (V, E)$, an acyclic orientation Ω of the edges E (that is, an orientation of each edge such that the resulting directed graph has no cycles), and a vertex-coloring $f : V \to \{1, 2, \ldots\}$, say that the pair (Ω, f) are *weakly compatible* if whenever Ω orients an edge $\{v, v'\}$ in E as $v \to v'$, one has $f(v) \leq f(v')$. Note that a *proper* vertex-coloring f of a graph $G = (V, E)$ is weakly compatible with a unique acyclic orientation Ω.

Proposition 7.3.23. *(Stanley* [205, Prop. 4.1, Thm. 4.2]*) The involution ω of Λ sends $\Psi[G]$ to $\omega(\Psi[G]) = \sum_{(\Omega,f)} \mathbf{x}_f$ in which the sum runs over weakly compatible pairs (Ω, f) of an acyclic orientation Ω and vertex-coloring f.*

Furthermore, the chromatic polynomial $\chi_G(m)$ has the property that $(-1)^{|V|}\chi_G(-m)$ counts all such weakly compatible pairs (Ω, f) in which $f : V \to \{1, 2, \ldots, m\}$ is a vertex-m-coloring.

Proof. As observed above, a proper coloring f is weakly compatible with a unique acyclic orientation Ω of G. Denote by P_Ω the poset on V which is the transitive closure of Ω, endowed with a *strict labelling* by integers, that is, every $i \in P_\Omega$ and $j \in P_\Omega$ satisfying $i <_{P_\Omega} j$ must satisfy $i >_{\mathbb{Z}} j$. Then proper colorings f that induce Ω are the same as P_Ω-partitions, so that

$$\Psi[G] = \sum_{\Omega} F_{P_\Omega}(\mathbf{x}). \tag{7.3.5}$$

Applying the antipode S and using Corollary 5.2.20 gives

$$\omega(\Psi[G]) = (-1)^{|V|} S(\Psi[G]) = \sum_{\Omega} F_{P_\Omega^{\mathrm{opp}}}(\mathbf{x}) = \sum_{(\Omega,f)} \mathbf{x}_f$$

where in the last line one sums over weakly compatible pairs as in the proposition. The last equality comes from the fact that since each P_Ω has been given a strict labelling, P_Ω^{opp} acquires a *weak (or natural) labelling*, that is, every $i \in P_\Omega$ and $j \in P_\omega$ satisfying $i <_{P_\Omega^{\mathrm{opp}}} j$ must satisfy $i <_{\mathbb{Z}} j$.

The last assertion follows from Proposition 7.1.7(iii). □

Remark 7.3.24. The interpretation of $\chi_G(-m)$ in Proposition 7.3.23 is a much older result of Stanley [204]. The special case interpreting $\chi_G(-1)$ as $(-1)^{|V|}$ times the number of acyclic orientations of G has sometimes been called Stanley's *(-1)-color theorem*. It also follows (via Proposition 7.1.7) from Humpert and Martin's antipode formula for $\mathcal{G}$ discussed in Remark 7.3.4: taking ζ to be the character of $\mathcal{G}$ given in (7.3.4),

$$\chi_G(-1) = \zeta^{\star(-1)}[G] = \zeta(S[G]) = \sum_F (-1)^{|V|-\mathrm{rank}(F)} \operatorname{acyc}(G/F)\zeta[G_{V,F}] = (-1)^{|V|} \operatorname{acyc}(G)$$

where the last equality uses the vanishing of ζ on graphs that have edges, so only the $F = \varnothing$ term survives.

Exercise 7.3.25. If V and X are two sets, and if $f : V \to X$ is any map, then $\operatorname{eqs} f$ will denote the set

$$\{\{u, u'\} \mid u \in V,\ u' \in V,\ u \neq u' \text{ and } f(u) = f(u')\}.$$

This is a subset of the set of all two-element subsets of V.

If $G = (V, E)$ is a finite graph, then show that the map Ψ introduced in Definition 7.3.16 satisfies

$$\Psi\left([G]^\sharp\right) = \sum_{\substack{f : V \to \{1,2,3,\ldots\}; \\ \operatorname{eqs} f = E}} \mathbf{x}_f,$$

where $\mathbf{x}_f := \prod_{v \in V} x_{f(v)}$. Here, $[G]^\sharp$ is defined as in Definition 7.3.8.

7.4. **Example: The quasisymmetric function of a matroid.** We introduce the *matroid-minor Hopf algebra* of Schmitt [191], and studied extensively by Crapo and Schmitt [41, 42, 43]. A very simple character ζ on this Hopf algebra will then give rise, via the map Ψ from Theorem 7.1.3, to the quasisymmetric function invariant of matroids from the work of Billera, Jia and the second author [21].

7.4.1. *The matroid-minor Hopf algebra.* We begin by reviewing some notions from matroid theory; see Oxley [164] for background, undefined terms and unproven facts.

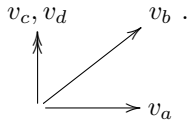
Definition 7.4.1. A *matroid* M of rank r on a (finite) ground set E is specified by a nonempty collection $\mathcal{B}(M)$ of r-element subsets of E with the following *exchange property*:

For any B, B' in $\mathcal{B}(M)$ and b in B, there exists b' in B' with $(B \setminus \{b\}) \cup \{b'\}$ in $\mathcal{B}(M)$.

The elements of $\mathcal{B}(M)$ are called the *bases* of the matroid M.

Example 7.4.2. A matroid M with ground set E is *represented* by a family of vectors $S = (v_e)_{e \in E}$ in a vector space if $\mathcal{B}(M)$ is the collection of subsets $B \subset E$ having the property that the subfamily $(v_e)_{e \in B}$ is a basis for the span of all of the vectors in S.

For example, if M is the matroid with $\mathcal{B}(M) = \{\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\}\}$ on the ground set $E = \{a,b,c,d\}$, then M is represented by the family $S = (v_a, v_b, v_c, v_d)$ of the four vectors $v_a = (1,0), v_b = (1,1), v_c = (0,1) = v_d$ in $\mathbb{R}^2$ depicted here



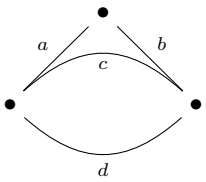
Conversely, whenever E is a finite set and $S = (v_e)_{e \in E}$ is a family of vectors in a vector space, then the set

$$\left\{B \subset E : \text{the subfamily } (v_e)_{e \in B} \text{ is a basis for the span of all of the vectors in } S\right\}$$

is a matroid on the ground set E.

A matroid is said to be *linear* if there exists a family of vectors in a vector space representing it. Not all matroids are linear, but many important ones are.

Example 7.4.3. A special case of matroids M represented by vectors are *graphic matroids*, coming from a graph $G = (V, E)$, with parallel edges and self-loops allowed. One represents these by vectors in $\mathbb{R}^V$ with standard basis $\{\epsilon_v\}_{v \in V}$ by associating the vector $\epsilon_v - \epsilon_{v'}$ to any edge connecting a vertex v with a vertex v'. One can check (or see [164, §1.2]) that the bases B in $\mathcal{B}(M)$ correspond to the edge sets of *spanning forests* for G, that is, edge sets which are acyclic and contain one spanning tree for each connected component of G. For example, the matroid $\mathcal{B}(M)$ corresponding to the graph $G = (V, E)$ shown below:



is exactly the matroid represented by the vectors in Example 7.4.2; indeed, the spanning forests of this graph G are the edge sets $\{a,b\},\{a,c\},\{a,d\},\{b,c\},\{b,d\}$. (In this example, spanning forests are the same as spanning trees, since G is connected.)

To define the matroid-minor Hopf algebra one needs the basic matroid operations of *deletion* and *contraction*. These model the operations of deleting or contracting an edge in a graph. For configurations of vectors they model the deletion of a vector, or the passage to images in the quotient space modulo the span of a vector.

Definition 7.4.4. Given a matroid M of rank r and an element e of its ground set E, say that e is *loop* (resp. *coloop*) of M if e lies in no basis (resp. every basis) B in $\mathcal{B}(M)$. If e is not a coloop, the *deletion* $M \setminus e$ is a matroid of rank r on ground set $E \setminus \{e\}$ having bases

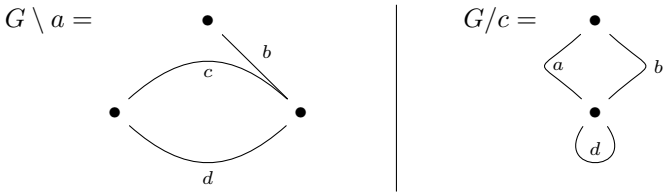
$$\mathcal{B}(M \setminus e) := \{B \in \mathcal{B}(M) : e \notin B\}. \tag{7.4.1}$$

If e is not a loop, the *contraction* M/e is a matroid of rank $r-1$ on ground set $E \setminus \{e\}$ having bases

$$\mathcal{B}(M/e) := \{B \setminus \{e\} : e \in B \in \mathcal{B}(M)\}. \tag{7.4.2}$$

When e is a loop of M, then M/e has rank r instead of $r-1$ and one defines its bases as in (7.4.1) rather than (7.4.2); similarly, if e is a coloop of M then $M \setminus e$ has rank $r-1$ instead of r and one defines its bases as in (7.4.2) rather than (7.4.1).

Example 7.4.5. Starting with the graph G and its graphic matroid M from Example 7.4.3, the deletion $M \setminus a$ and contraction M/c correspond to the graphs $G \setminus a$ and G/c shown here:



One has

- $\mathcal{B}(M \setminus a) = \{\{b,c\},\{b,d\}\}$, so that b has become a coloop in $M \setminus a$, and
- $\mathcal{B}(M/c) = \{\{a\},\{b\}\}$, so that d has become a loop in M/c.

Definition 7.4.6. Deletions and contractions commute with each other. Thus, given a matroid M with ground set E, and a subset $A \subset E$, two well-defined matroids can be constructed:

- the *restriction* $M|_A$, which is a matroid on ground set A, obtained from M by deleting all $e \in E \setminus A$ in any order, and
- the *quotient/contraction* M/A, which is a matroid on ground set $E \setminus A$, obtained from M by contracting all $e \in A$ in any order.

We will also need the *direct sum* $M_1 \oplus M_2$ of two matroids M_1 and M_2. This is the matroid whose ground set $E = E_1 \sqcup E_2$ is the disjoint union of a copy of the ground sets E_1, E_2 for M_1, M_2, and whose bases are

$$\mathcal{B}(M_1 \oplus M_2) := \{B_1 \sqcup B_2 : B_i \in \mathcal{B}(M_i) \text{ for } i = 1,2\}.$$

Lastly, say that two matroids M_1, M_2 are *isomorphic* if there is a bijection of their ground sets $E_1 \xrightarrow{\varphi} E_2$ having the property that $\varphi\mathcal{B}(M_1) = \mathcal{B}(M_2)$.

Now one can define the matroid-minor Hopf algebra, originally introduced by Schmitt [191, §15], and studied further by Crapo and Schmitt [41, 42, 43].

Definition 7.4.7. Let $\mathcal{M}$ have $\mathbf{k}$-basis elements $[M]$ indexed by isomorphism classes of matroids. Define the multiplication via

$$[M_1] \cdot [M_2] := [M_1 \oplus M_2],$$

so that the class $[\varnothing]$ of the *empty matroid* $\varnothing$ having empty ground set gives a unit. Define the comultiplication for M a matroid on ground set E via

$$\Delta[M] := \sum_{A \subset E} [M|_A] \otimes [M/A],$$

and a counit

$$\epsilon[M] := \begin{cases} 1, & \text{if } M = \varnothing; \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 7.4.8. *The above maps endow $\mathcal{M}$ with the structure of a connected graded finite type Hopf algebra over $\mathbf{k}$, which is commutative.*

Proof. Checking the unit and counit conditions are straightforward. Associativity and commutativity of the multiplication follow because the direct sum operation $\oplus$ for matroids is associative and commutative up to isomorphism. Coassociativity follows because for a matroid M on ground set E, one has the following equality between the two candidates for $\Delta^{(2)}[M]$:

$$\begin{aligned} &\sum_{\varnothing \subset A_1 \subset A_2 \subset E} [M|_{A_1}] \otimes [(M|_{A_2})/A_1] \otimes [M/A_2] \\ &= \sum_{\varnothing \subset A_1 \subset A_2 \subset E} [M|_{A_1}] \otimes [(M/A_1)|_{A_2 \setminus A_1}] \otimes [M/A_2] \end{aligned}$$

due to the matroid isomorphism $(M|_{A_2})/A_1 \cong (M/A_1)|_{A_2 \setminus A_1}$. Commutativity of the bialgebra diagram in (1.3.4) amounts to the fact that for a pair of matroids M_1, M_2 and subsets A_1, A_2 of their (disjoint) ground sets E_1, E_2, one has isomorphisms

$$M_1|_{A_1} \oplus M_2|_{A_2} \cong (M_1 \oplus M_2)\,|_{A_1 \sqcup A_2},$$
$$M_1/A_1 \oplus M_2/A_2 \cong (M_1 \oplus M_2)\,/(A_1 \sqcup A_2).$$

Letting $\mathcal{M}_n$ be the $\mathbf{k}$-span of $[M]$ for matroids whose ground set E has cardinality $|E| = n$, one can then easily check that $\mathcal{M}$ becomes a bialgebra which is graded, connected, and of finite type, hence also a Hopf algebra by Proposition 1.4.16. □

See [59] for an application of $\mathcal{M}$ (and the operator $\exp^\star$ from Section 1.7) to proving the *Tutte recipe theorem*, a "universal" property of the Tutte polynomial of a matroid.

7.4.2. *A quasisymmetric function for matroids.*

Definition 7.4.9. Define a character $\mathcal{M} \xrightarrow{\zeta} \mathbf{k}$ by

$$\zeta[M] = \begin{cases} 1, & \text{if } M \text{ has only one basis;} \\ 0, & \text{otherwise.} \end{cases}$$

It is easily checked that this is a character, that is, an algebra morphism $\mathcal{M} \xrightarrow{\zeta} \mathbf{k}$. Note that if M has only one basis, say $\mathcal{B}(M) = \{B\}$, then $B := \text{coloops}(M)$ is the set of coloops of M, and $E \setminus B = \text{loops}(M)$ is the set of loops of M. Equivalently, $M = \bigoplus_{e \in E} M|_{\{e\}}$ is the direct sum of matroids each having one element, each a coloop or loop.

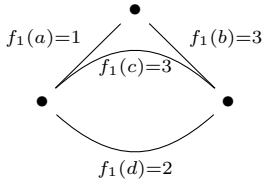
Define $\Psi[M]$ for a matroid M to be the image of $[M]$ under the map $\mathcal{M} \xrightarrow{\Psi}$ QSym induced via Theorem 7.1.3 from the above character ζ.

It turns out that $\Psi[M]$ is intimately related with greedy algorithms and finding minimum cost bases. A fundamental property of matroids (and one that characterizes them, in fact; see [164, §1.8]) is that no matter how one assigns costs $f : E \to \mathbb{R}$ to the elements of E, the following *greedy algorithm* (generalizing *Kruskal's algorithm* for finding minimum cost spanning trees) always succeeds in finding one basis B in $\mathcal{B}(M)$ achieving the minimum *total cost* $f(B) := \sum_{b \in B} f(b)$:

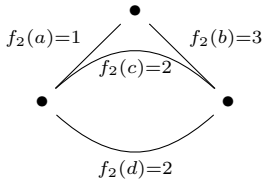
Algorithm 7.4.10. Start with the empty subset $I_0 = \varnothing$ of E. For $j = 1, 2, \ldots, r$, having already defined the set I_{j-1}, let e be the element of $E \setminus I_{j-1}$ having the lowest cost $f(e)$ among all those for which $I_{j-1} \cup \{e\}$ is *independent*, that is, still a subset of at least one basis B in $\mathcal{B}(M)$. Then define $I_j := I_{j-1} \cup \{e\}$. Repeat this until $j = r$, and $B = I_r$ will be among the bases that achieve the minimum cost.

Definition 7.4.11. Say that a cost function $f : E \to \{1, 2, \ldots\}$ is *M-generic* if there is a *unique* basis B in $\mathcal{B}(M)$ achieving the minimum cost $f(B)$.

Example 7.4.12. For the graphic matroid M of Example 7.4.3, this cost function $f_1 : E \to \{1, 2, \ldots\}$



is M-generic, as it minimizes uniquely on the basis $\{a, d\}$, whereas this cost function $f_2 : E \to \{1, 2, \ldots\}$



is *not* M-generic, as it achieves its minimum value on the two bases $\{a,c\},\{a,d\}$.

Proposition 7.4.13. *For a matroid M on ground set E, one has this expansion*[362]

$$\Psi[M] = \sum_{\substack{M\text{-generic} \\ f:E\to\{1,2,\ldots\}}} \mathbf{x}_f$$

where $\mathbf{x}_f := \prod_{e\in E} x_{f(e)}$. In particular, for $m \geq 0$, its specialization ps^1 from Definition 7.1.6 has this interpretation:

$$\mathrm{ps}^1\Psi[M](m) = |\{M\text{-generic } f : E \to \{1,2,\ldots,m\}\}|.$$

Proof. The iterated coproduct $\mathcal{M} \xrightarrow{\Delta^{(\ell-1)}} \mathcal{M}^{\otimes\ell}$ sends

$$[M] \longmapsto \sum [M|_{A_1}] \otimes [(M|_{A_2})/A_1] \otimes \cdots \otimes [(M|_{A_\ell})/A_{\ell-1}]$$

where the sum is over flags of nested subsets

$$\varnothing = A_0 \subset A_1 \subset \cdots \subset A_{\ell-1} \subset A_\ell = E. \tag{7.4.3}$$

The map $\zeta^{\otimes\ell}$ sends each summand to 1 or 0, depending upon whether each $(M|_{A_j})/A_{j-1}$ has a unique basis or not. Thus formula (7.1.3) shows that the coefficient ζ_α of $x_{i_1}^{\alpha_1}\cdots x_{i_\ell}^{\alpha_\ell}$ in $\Psi[M]$ counts the flags of subsets in (7.4.3) for which $|A_j \setminus A_{j-1}| = \alpha_j$ and $(M|_{A_j})/A_{j-1}$ has a unique basis, for each j.

Given a flag as in (7.4.3), associate the cost function $f : E \to \{1,2,\ldots\}$ whose value on each element of $A_j \setminus A_{j-1}$ is i_j; conversely, given any cost function f, say whose distinct values are $i_1 < \cdots < i_\ell$, one associates the flag having $A_j \setminus A_{j-1} = f^{-1}(i_j)$ for each j.

Now, apply the greedy algorithm (Algorithm 7.4.10) to find a minimum-cost basis of M for such a cost function f. At each step of the greedy algorithm, one new element is added to the independent set; these elements weakly increase in cost as the algorithm progresses[363]. Thus, the algorithm first adds some elements of cost i_1, then adds some elements of cost i_2, then adds some elements of cost i_3, and so on. We can therefore subdivide the execution of the algorithm into phases $1,2,\ldots,\ell$, where each phase consists of some finite number of steps, such that all elements added in phase k have cost i_k. (A phase may be empty.) For each $k \in \{1,2,\ldots,\ell\}$, we let β_k be the number of steps in phase k; in other words, β_k is the number of elements of elements of cost i_k added during the algorithm.

We will prove below, using induction on $s = 0,1,2,\ldots,\ell$ the following **claim**: After having completed phases $1,2,\ldots,s$ in the greedy algorithm (Algorithm 7.4.10), there is *a unique choice* for the independent set produced thus far, namely

$$I_{\beta_1+\beta_2+\cdots+\beta_s} = \bigsqcup_{j=1}^{s} \mathrm{coloops}((M|_{A_j})/A_{j-1}), \tag{7.4.4}$$

if and only if each of the matroids $(M|_{A_j})/A_{j-1}$ for $j = 1,2,\ldots,s$ *has a unique basis.*

The case $s = \ell$ in this claim would show what we want, namely that f is M-generic, minimizing uniquely on the basis shown in (7.4.4) with $s = \ell$, if and only if each $(M|_{A_j})/A_{j-1}$ has a unique basis.

The assertion of the claim is trivially true for $s = 0$. In the inductive step, one may assume that

- the independent set $I_{\beta_1+\beta_2+\cdots+\beta_{s-1}}$ takes the form in (7.4.4), replacing s by $s-1$,
- it is the unique f-minimizing basis for $M|_{A_{s-1}}$, and
- $(M|_{A_j})/A_{j-1}$ has a unique basis for $j = 1,2,\ldots,s-1$.

Since A_{s-1} exactly consists of all of the elements e of E whose costs $f(e)$ lie in the range $\{i_1,i_2,\ldots,i_{s-1}\}$, in phase s the algorithm will work in the quotient matroid M/A_{s-1} and attempt to augment $I_{\beta_1+\beta_2+\cdots+\beta_{s-1}}$ using the next-cheapest elements, namely the elements of $A_s \setminus A_{s-1}$, which all have cost f equal to i_s. Thus the algorithm will have no choices about how to do this augmentation if and only if $(M|_{A_s})/A_{s-1}$ has a unique basis, namely its set of coloops, in which case the algorithm will choose to add all of these coloops, giving $I_{\beta_1+\beta_2+\cdots+\beta_s}$ as described in (7.4.4). This completes the induction.

The last assertion follows from Proposition 7.1.7. □

[362] In fact, this expansion was the original definition of $\Psi[M]$ in [21, Defn. 1.1].

[363] *Proof.* Let e be the element added at step i, and let e' be the element added at step $i+1$. We want to show that $f(e) \leq f(e')$. But the element e' could already have been added at step i. Since it wasn't, we thus conclude that the element e that was added instead must have been cheaper or equally expensive. In other words, $f(e) \leq f(e')$, qed.

Example 7.4.14. If M has one basis then every function $f : E \to \{1, 2, \ldots\}$ is M-generic, and

$$\Psi[M] = \sum_{f:E\to\{1,2,\ldots\}} \mathbf{x}_f = (x_1 + x_2 + \cdots)^{|E|} = M_{(1)}^{|E|}.$$

Example 7.4.15. Let $U_{r,n}$ denote the *uniform matroid* of rank r on n elements E, having $\mathcal{B}(U_{r,n})$ equal to all of the r-element subsets of E.

As $U_{1,2}$ has $E = \{1, 2\}$ and $\mathcal{B} = \{\{1\}, \{2\}\}$, genericity means $f(1) \neq f(2)$, so

$$\Psi[U_{1,2}] = \sum_{\substack{(f(1),f(2)):\\ f(1)\neq f(2)}} x_{f(1)}x_{f(2)} = x_1x_2 + x_2x_1 + x_1x_3 + x_3x_1 + \cdots = 2M_{(1,1)}.$$

Similarly $U_{1,3}$ has $E = \{1, 2, 3\}$ with $\mathcal{B} = \{\{1\}, \{2\}, \{3\}\}$, and genericity means either that $f(1), f(2), f(3)$ are all distinct, or that two of them are the same and the third is smaller. This shows

$$\begin{aligned}\Psi[U_{1,3}] &= 3\sum_{i<j} x_i x_j^2 + 6\sum_{i<j<k} x_i x_j x_k \\ &= 3M_{(1,2)} + 6M_{(1,1,1)}; \\ \mathrm{ps}^1\Psi[U_{1,3}](m) &= 3\binom{m}{2} + 6\binom{m}{3} = \frac{m(m-1)(2m-1)}{2}.\end{aligned}$$

One can similarly analyze $U_{2,3}$ and check that

$$\begin{aligned}\Psi[U_{2,3}] &= 3M_{(2,1)} + 6M_{(1,1,1)}; \\ \mathrm{ps}^1\Psi[U_{2,3}](m) &= 3\binom{m}{2} + 6\binom{m}{3} = \frac{m(m-1)(2m-1)}{2}.\end{aligned}$$

These last examples illustrate the behavior of Ψ under the duality operation on matroids.

Definition 7.4.16. Given a matroid M of rank r on ground set E, its *dual* or *orthogonal matroid* $M^\perp$ is a matroid of rank $|E| - r$ on the same ground set E, having

$$\mathcal{B}(M^\perp) := \{E \setminus B\}_{B\in\mathcal{B}(M)}.$$

See [164, Theorem 2.1.1] or [34, Section 4] for a proof of the fact that this is well-defined (i.e., that the collection $\{E \setminus B\}_{B\in\mathcal{B}(M)}$ really satisfies the exchange property). Here are a few examples of dual matroids.

Example 7.4.17. The dual of a uniform matroid is another uniform matroid:

$$U_{r,n}^\perp = U_{n-r,n}.$$

Example 7.4.18. If M is matroid of rank r represented by family of vectors $\{e_1, \ldots, e_n\}$ in a vector space over some field $\mathbf{k}$, one can find a family of vectors $\{e_1^\perp, \ldots, e_n^\perp\}$ that represent $M^\perp$ in the following way. Pick a basis for the span of the vectors $\{e_i\}_{i=1}^n$, and create a matrix A in $\mathbf{k}^{r\times n}$ whose columns express the e_i in terms of this basis. Then pick any matrix $A^\perp$ whose row space is the null space of A, and one finds that the columns $\{e_i^\perp\}_{i=1}^n$ of $A^\perp$ represent $M^\perp$. See Oxley [164, §2.2].

Example 7.4.19. Let $G = (V, E)$ be a graph embedded in the plane with edge set E, giving rise to a graphic matroid M on ground set E. Let $G^\perp$ be a planar dual of G, so that, in particular, for each edge e in E, the graph $G^\perp$ has one edge $e^\perp$, crossing e transversely. Then the graphic matroid of $G^\perp$ is $M^\perp$. See Oxley [164, §2.3].

Proposition 7.4.20. *If $\Psi[M] = \sum_\alpha c_\alpha M_\alpha$ then $\Psi[M^\perp] = \sum_\alpha c_\alpha M_{\mathrm{rev}(\alpha)}$.*

Consequently, $\mathrm{ps}^1\Psi[M](m) = \mathrm{ps}^1\Psi[M^\perp](m)$.

Proof. First, let us prove that if $\Psi[M] = \sum_\alpha c_\alpha M_\alpha$ then $\Psi[M^\perp] = \sum_\alpha c_\alpha M_{\mathrm{rev}(\alpha)}$. In other words, let us show that for any given composition α, the coefficient of M_α in $\Psi[M]$ (when $\Psi[M]$ is expanded in the basis $(M_\beta)_{\beta\in\mathrm{Comp}}$ of QSym) equals the coefficient of $M_{\mathrm{rev}(\alpha)}$ in $\Psi[M^\perp]$. This amounts to showing that for any composition $\alpha = (\alpha_1, \ldots, \alpha_\ell)$, the cardinality of the set of M-generic f having $\mathbf{x}_f = \mathbf{x}^\alpha$ is the same as the

cardinality of the set of $M^\perp$-generic $f^\perp$ having $\mathbf{x}_{f^\perp} = \mathbf{x}^{\mathrm{rev}(\alpha)}$. We claim that the map $f \longmapsto f^\perp$ in which $f^\perp(e) = \ell + 1 - f(e)$ gives a bijection between these sets. To see this, note that any basis B of M satisfies

$$f(B) + f(E \setminus B) = \sum_{e \in E} f(e), \tag{7.4.5}$$

$$f(E \setminus B) + f^\perp(E \setminus B) = (\ell + 1)(|E| - r), \tag{7.4.6}$$

where r denotes the rank of M. Thus B is f-minimizing if and only if $E \setminus B$ is f-maximizing (by (7.4.5)) if and only if $E \setminus B$ is $f^\perp$-minimizing (by (7.4.6)). Consequently f is M-generic if and only if $f^\perp$ is $M^\perp$-generic.

The last assertion follows, for example, from the calculation in Proposition 7.1.7(i) that $\mathrm{ps}^1(M_\alpha)(m) = \binom{m}{\ell(\alpha)}$ together with the fact that $\ell(\mathrm{rev}(\alpha)) = \ell(\alpha)$. □

Just as (7.3.5) showed that Stanley's chromatic symmetric function of a graph has an expansion as a sum of P-partition enumerators for certain strictly labelled posets[364] P, the same holds for $\Psi[M]$.

Definition 7.4.21. Given a matroid M on ground set E, and a basis B in $\mathcal{B}(M)$, define the *base-cobase poset* P_B to have $b < b'$ whenever b lies in B and b' lies in $E \setminus B$ and $(B \setminus \{b\}) \cup \{b'\}$ is in $\mathcal{B}(M)$.

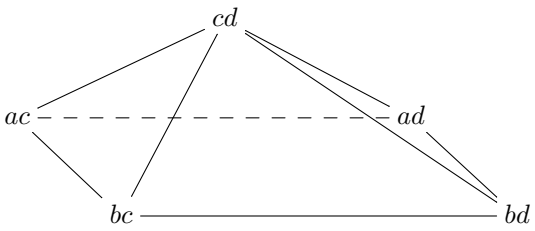
Proposition 7.4.22. *For any matroid M, one has $\Psi[M] = \sum_{B \in \mathcal{B}(M)} F_{(P_B, \mathrm{strict})}(\mathbf{x})$ where $F_{(P,\,\mathrm{strict})}(\mathbf{x})$ for a poset P means the P-partition enumerator for any strict labelling of P, i.e. a labelling such that the P-partitions satisfy $f(i) < f(j)$ whenever $i <_P j$.*

In particular, $\Psi[M]$ expands nonnegatively in the $\{L_\alpha\}$ basis.

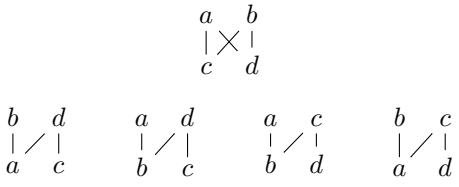
Proof. A basic result about matroids, due to Edmonds [62], describes the *edges* in the *matroid base polytope* which is the convex hull of all vectors $\{\sum_{b \in B} \epsilon_b\}_{B \in \mathcal{B}(M)}$ inside $\mathbb{R}^E$ with standard basis $\{\epsilon_e\}_{e \in E}$. He shows that all such edges connect two bases B, B' that differ by a single *basis exchange*, that is, $B' = (B \setminus \{b\}) \cup \{b'\}$ for some b in B and b' in $E \setminus B$.

Polyhedral theory then says that a cost function f on E will minimize uniquely at B if and only if one has a strict increase $f(B) < f(B')$ along each such edge $B \to B'$ emanating from B, that is, if and only if $f(b) < f(b')$ whenever $b <_{P_B} b'$ in the base-cobase poset P_B, that is, f lies in $\mathcal{A}(P_B, \mathrm{strict})$. □

Example 7.4.23. The graphic matroid from Example 7.4.3 has this matroid base polytope, with the bases B in $\mathcal{B}(M)$ labelling the vertices:



The base-cobase posets P_B for its five vertices B are as follows:



One can label the first of these five strictly as

and compute its strict P-partition enumerator from the linear extensions $\{3412, 3421, 4312, 4321\}$ as

$$L_{(2,2)} + L_{(2,1,1)} + L_{(1,1,2)} + L_{(1,1,1,1)},$$

[364] A labelled poset P is said to be *strictly labelled* if every two elements i and j of P satisfying $i <_P j$ satisfy $i >_{\mathbb{Z}} j$.

while any of the last four can be labelled strictly as

$$\begin{array}{cc} 1 & 2 \\ | & | \\ 3 & 4 \end{array}$$

and they each have an extra linear extension 3142 giving their strict P-partition enumerators as

$$L_{(2,2)} + L_{(2,1,1)} + L_{(1,1,2)} + L_{(1,1,1,1)} + L_{(1,2,1)}.$$

Hence one has

$$\Psi[M] = 5L_{(2,2)} + 5L_{(1,1,2)} + 4L_{(1,2,1)} + 5L_{(2,1,1)} + 5L_{(1,1,1,1)}.$$

As M is a graphic matroid for a self-dual planar graph, one has a matroid isomorphism $M \cong M^{\perp}$ (see Example 7.4.19), reflected in the fact that $\Psi[M]$ is invariant under the symmetry swapping $M_\alpha \leftrightarrow M_{\mathrm{rev}(\alpha)}$ (and simultaneously swapping $L_\alpha \leftrightarrow L_{\mathrm{rev}(\alpha)}$).

This P-partition expansion for $\Psi[M]$ also allows us to identify its image under the antipode of QSym.

Proposition 7.4.24. *For a matroid M on ground set E, one has*

$$S(\Psi[M]) = (-1)^{|E|} \sum_{f: E \to \{1,2,\ldots\}} |\{f\text{-maximizing bases } B\}| \cdot \mathbf{x}_f$$

and

$$\mathrm{ps}^1\Psi[M](-m) = (-1)^{|E|} \sum_{f: E \to \{1,2,\ldots,m\}} |\{f\text{-maximizing bases } B\}|.$$

In particular, the expected number of f-maximizing bases among all cost functions $f : E \to \{1, 2, \ldots, m\}$ is $(-m)^{-|E|}\mathrm{ps}^1\Psi[M](-m)$.

Proof. Corollary 5.2.20 implies

$$S(\Psi[M]) = \sum_{B \in \mathcal{B}(M)} S(F_{(P_B,\mathrm{strict})}(\mathbf{x})) = (-1)^{|E|} \sum_{B \in \mathcal{B}(M)} F_{(P_B^{\mathrm{opp}},\mathrm{natural})}(\mathbf{x}),$$

where $F_{(P,\mathrm{natural})}(\mathbf{x})$ is the enumerator for P-partitions in which P has been *naturally* labelled, so that they satisfy $f(i) \leq f(j)$ whenever $i <_P j$. When $P = P_B^{\mathrm{opp}}$, this is exactly the condition for f to achieve its maximum value at $f(B)$ (possibly not uniquely), that is, for f to lie in the *closed* normal cone to the vertex indexed by B in the matroid base polytope; compare this with the discussion in the proof of Proposition 7.4.22. Thus one has

$$S(\Psi[M]) = (-1)^{|E|} \sum_{\substack{(B,f): \\ B \in \mathcal{B}(M) \\ f \text{ maximizing at } B}} \mathbf{x}_f,$$

which agrees with the statement of the proposition, after reversing the order of the summation.

The rest follows from Proposition 7.1.7. □

Example 7.4.25. We saw in Example 7.4.23 that the matroid M from Example 7.4.3 has

$$\Psi[M] = 5L_{(2,2)} + 5L_{(1,1,2)} + 4L_{(1,2,1)} + 5L_{(2,1,1)} + 5L_{(1,1,1,1)},$$

and therefore will have

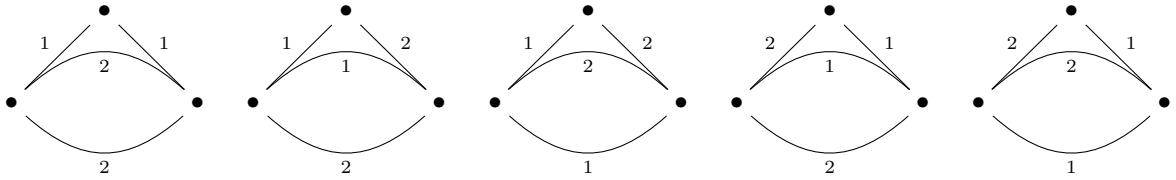
$$\mathrm{ps}^1\Psi[M](m) = 5\binom{m-2+4}{4} + (5+4+5)\binom{m-3+4}{4} + 5\binom{m-4+4}{4} = \frac{m(m-1)(2m^2-2m+1)}{2}$$

using $\mathrm{ps}^1(L_\alpha)(m) = \binom{m-\ell+|\alpha|}{|\alpha|}$ from Proposition 7.1.7 (i). Let us first do a reality-check on a few of its values with $m \geq 0$ using Proposition 7.4.13, and for negative m using Proposition 7.4.24:

m	-1	0	1	2
$\mathrm{ps}^1\Psi[M](m)$	5	0	0	5

When $m = 0$, interpreting the set of cost functions $f : E \to \{1, 2, \ldots, m\}$ as being empty explains why the value shown is 0. When $m = 1$, there is only one function $f : E \to \{1\}$, and it is not M-generic; any of

the 5 bases in $\mathcal{B}(M)$ will minimize $f(B)$, explaining both why the value for $m = 1$ is 0, but also explaining the value of 5 for $m = -1$. The value of 5 for $m = 2$ counts these M-generic cost functions $f : E \to \{1, 2\}$:



Lastly, Proposition 7.4.24 predicts the expected number of f-minimizing bases for $f : E \to \{1, 2, \ldots, m\}$ as

$$(-m)^{-|E|}\mathrm{ps}^1\Psi[M](-m) = (-m)^{-4}\frac{m(m+1)(2m^2+2m+1)}{2} = \frac{(m+1)(2m^2+2m+1)}{2m^3},$$

whose limit as $m \to \infty$ is 1, consistent with the notion that "most" cost functions should be generic with respect to the bases of M, and maximize/minimize on a unique basis.

Remark 7.4.26. It is not coincidental that there is a similarity of results for Stanley's chromatic symmetric function of a graph $\Psi[G]$ and for the matroid quasisymmetric function $\Psi[M]$, such as the P-partition expansions (7.3.5) versus Proposition 7.4.22, and the reciprocity results Proposition 7.3.23 versus Proposition 7.4.24. It was noted in [21, §9] that one can associate a similar quasisymmetric function invariant to any *generalized permutohedra* in the sense of Postnikov [173]. Furthermore, recent work of Ardila and Aguiar [3] has shown that there is a Hopf algebra of such generalized permutohedra, arising from a *Hopf monoid* in the sense of Aguiar and Mahajan [6]. This Hopf algebra generalizes the chromatic Hopf algebra of graphs[365] and the matroid-minor Hopf algebra, and its quasisymmetric function invariant derives as usual from Theorem 7.1.3. Their work [3] also provides a generalization of the chromatic Hopf algebra antipode formula of Humpert and Martin [103] discussed in Remark 7.3.4 above.

[365] Aguiar and Ardila actually work with a larger Hopf algebra of graphs. Namely, their concept of graphs allows parallel edges, and it also allows "half-edges", which have only one endpoint. If $G = (V, E)$ is such a graph (where E is the set of its edges and its half-edges), and if V' is a subset of V, then they define $G/_{V'}$ to be the graph on vertex set V' obtained from G by

- removing all vertices that are not in V',
- removing all edges that have no endpoint in V', and all half-edges that have no endpoint in V', and
- replacing all edges that have only one endpoint in V' by half-edges.

(This is to be contrasted with the induced subgraph $G\,|_{V'}$, which is constructed in the same way but with the edges that have only one endpoint in V' getting removed as well.) The comultiplication they define on the Hopf algebra of such graphs sends the isomorphism class $[G]$ of a graph $G = (V, E)$ to $\sum_{(V_1,V_2):V_1 \sqcup V_2 = V} [G\,|_{V_1}] \otimes [G/_{V_2}]$. This is no longer a cocommutative Hopf algebra; our Hopf algebra $\mathcal{G}$ is a quotient of it. In [3, Corollary 13.10], Ardila and Aguiar compute the antipode of the Hopf monoid of such graphs; this immediately leads to a formula for the antipode of the corresponding Hopf algebra, because what they call the Fock functor $\overline{\mathcal{K}}$ preserves antipodes [3, Theorem 2.18].

8. The Malvenuto-Reutenauer Hopf algebra of permutations

Like so many Hopf algebras we have seen, the *Malvenuto-Reutenauer Hopf algebra* FQSym can be thought of fruitfully in more than one way. One is that it gives a natural noncommutative lift of the quasisymmetric P-partition enumerators and the fundamental basis $\{L_\alpha\}$ of QSym, rendering their product and coproduct formulas even more natural.

8.1. Definition and Hopf structure.

Definition 8.1.1. We shall regard permutations as words (over the alphabet $\{1, 2, 3, \ldots\}$) by identifying every permutation $\pi \in \mathfrak{S}_n$ with the word $(\pi(1), \pi(2), \ldots, \pi(n))$.

Define $\mathrm{FQSym} = \bigoplus_{n \geq 0} \mathrm{FQSym}_n$ to be a graded $\mathbf{k}$-module in which FQSym_n has $\mathbf{k}$-basis $\{F_w\}_{w \in \mathfrak{S}_n}$ indexed by the permutations $w = (w_1, \ldots, w_n)$ in $\mathfrak{S}_n$.

We first attempt to lift the product and coproduct formulas (5.2.6), (5.2.5) in the $\{L_\alpha\}$ basis of QSym. We attempt to define a product for $u \in \mathfrak{S}_k$ and $v \in \mathfrak{S}_\ell$ as follows[366]:

$$F_u F_v := \sum_{w \in u \sqcup\!\sqcup v[k]} F_w, \tag{8.1.1}$$

where for any word $v = (v_1, \ldots, v_\ell)$ we set $v[k] := (k + v_1, \ldots, k + v_\ell)$. Note that the multiset $u \sqcup\!\sqcup v[k]$ is an actual set in this situation (i.e., has each element appear only once) and is a subset of $\mathfrak{S}_{k+\ell}$.

The coproduct will be defined using the notation of standardization of $\mathrm{std}(w)$ a word w in some linearly ordered alphabet (see Definition 5.3.3).

Example 8.1.2. Considering words in the Roman alphabet $a < b < c < \cdots$, we have

$$\begin{array}{l} \mathrm{std}(b\ \ a\ \ c\ \ c\ \ b\ \ a\ \ a\ \ b\ \ a\ \ c\ \ b) \\ = (5\ \ 1\ \ 9\ \ 10\ \ 6\ \ 2\ \ 3\ \ 7\ \ 4\ \ 11\ \ 8). \end{array}$$

Using this, define for $w = (w_1, \ldots, w_n)$ in $\mathfrak{S}_n$ the element $\Delta F_w \in \mathrm{FQSym} \otimes \mathrm{FQSym}$ by

$$\Delta F_w := \sum_{k=0}^{n} F_{\mathrm{std}(w_1, w_2, \ldots, w_k)} \otimes F_{\mathrm{std}(w_{k+1}, w_{k+2}, \ldots, w_n)}. \tag{8.1.2}$$

It is possible to check directly that the maps defined in (8.1.1) and (8.1.2) endow FQSym with the structure of a connected graded finite type Hopf algebra; see Hazewinkel, Gubareni, Kirichenko [93, Thm. 7.1.8]. However in justifying this here, we will follow the approach of Duchamp, Hivert and Thibon [58, §3], which exhibits FQSym as a subalgebra of a larger ring of (noncommutative) power series of bounded degree in a totally ordered alphabet.

Definition 8.1.3. Given a totally ordered set I, create a totally ordered variable set $\{X_i\}_{i \in I}$, and the ring $R\langle\{X_i\}_{i \in I}\rangle$ of *noncommutative power series of bounded degree* in this alphabet[367]. Many times, we will use a variable set $\mathbf{X} := (X_1 < X_2 < \cdots)$, and call the ring $R\langle\mathbf{X}\rangle$.

---

[366] Recall that we regard permutations as words.

[367] Let us recall the definition of $R\langle\{X_i\}_{i \in I}\rangle$.

Let N denote the free monoid on the alphabet $\{X_i\}_{i \in I}$; it consists of words $X_{i_1} X_{i_2} \cdots X_{i_k}$. We define a topological $\mathbf{k}$-module $\mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ to be the Cartesian product $\mathbf{k}^N$ (equipped with the product topology), but we identify its element $(\delta_{w,u})_{u \in N}$ with the word w for every $w \in N$. Thus, every element $(\lambda_w)_{w \in N} \in \mathbf{k}^N = \mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ can be rewritten as the convergent sum $\sum_{w \in N} \lambda_w w$. We call λ_w the *coefficient of* w in this element (or the *coefficient of this element before* w). The elements of $\mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ will be referred to as *noncommutative power series*. We define a multiplication on $\mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ by the formula

$$\left(\sum_{w \in N} \lambda_w w\right)\left(\sum_{w \in N} \mu_w w\right) = \sum_{w \in N} \left(\sum_{(u,v) \in N^2;\ w = uv} \lambda_u \mu_v\right) w.$$

(This is well-defined thanks to the fact that, for each $w \in N$, there are only finitely many $(u, v) \in N^2$ satisfying $w = uv$.) Thus, $\mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ becomes a $\mathbf{k}$-algebra with unity 1 (the empty word). (It is similar to the monoid algebra $\mathbf{k}N$ of N over $\mathbf{k}$, with the only difference that infinite sums are allowed.)

Now, we define $R\langle\{X_i\}_{i \in I}\rangle$ to be the $\mathbf{k}$-subalgebra of $\mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ consisting of all noncommutative power series $\sum_{w \in N} \lambda_w w \in \mathbf{k}\langle\langle\{X_i\}_{i \in I}\rangle\rangle$ *of bounded degree* (i.e., such that all words $w \in N$ of sufficiently high length satisfy $\lambda_w = 0$).

We first identify the algebra structure for FQSym as the subalgebra of finite type within $R\langle\{X_i\}_{i\in I}\rangle$ spanned by the elements

$$F_w = F_w(\{X_i\}_{i\in I}) := \sum_{\substack{\mathbf{i}=(i_1,\ldots,i_n):\\ \mathrm{std}(\mathbf{i})=w^{-1}}} \mathbf{X_i}, \tag{8.1.3}$$

where $\mathbf{X_i} := X_{i_1}\cdots X_{i_n}$, as w ranges over $\bigcup_{n\geq 0}\mathfrak{S}_n$.

Example 8.1.4. For the alphabet $\mathbf{X} = (X_1 < X_2 < \cdots)$, in $R\langle\mathbf{X}\rangle$ one has

$$\begin{aligned}
F_1 &= \sum_{1\leq i} X_i = X_1 + X_2 + \cdots, \\
F_{12} &= \sum_{1\leq i\leq j} X_iX_j = X_1^2 + X_2^2 + \cdots + X_1X_2 + X_1X_3 + X_2X_3 + X_1X_4 + \cdots, \\
F_{21} &= \sum_{1\leq i<j} X_jX_i = X_2X_1 + X_3X_1 + X_3X_2 + X_4X_1 + \cdots, \\
F_{312} &= \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=231} \mathbf{X_i} = \sum_{1\leq i<j\leq k} X_jX_kX_i \\
&= X_2^2X_1 + X_3^2X_1 + X_3^2X_2 + \cdots + X_2X_3X_1 + X_2X_4X_1 + \cdots.
\end{aligned}$$

Proposition 8.1.5. *For any totally ordered infinite set I, the elements $\{F_w\}$ as w ranges over $\bigcup_{n\geq 0}\mathfrak{S}_n$ form a* $\mathbf{k}$*-basis for a subalgebra* $\mathrm{FQSym}(\{X_i\}_{i\in I})$ *of $R\langle\mathbf{X}\rangle$, which is connected graded and of finite type, having multiplication defined* $\mathbf{k}$*-linearly by (8.1.1).*

Consequently all such algebras are isomorphic to a single algebra FQSym*, having basis $\{F_w\}$ and multiplication given by the rule (8.1.1), with the isomorphism mapping $F_w \longmapsto F_w(\{X_i\}_{i\in I})$.*

For example,

$$\begin{aligned}
F_1F_{21} &= (X_1 + X_2 + X_3 + \cdots)(X_2X_1 + X_3X_1 + X_3X_2 + X_4X_1 + \cdots) \\
&= X_1\cdot X_3X_2 + X_1\cdot X_4X_2 + \cdots + X_1\cdot X_2X_1 + X_2\cdot X_3X_2 + X_2\cdot X_4X_2 + \cdots \\
&\quad + X_2\cdot X_3X_1 + X_2\cdot X_4X_1 + \cdots + X_2\cdot X_2X_1 + X_3\cdot X_3X_1 + X_3\cdot X_3X_2 + \cdots \\
&\quad + X_3\cdot X_2X_1 + X_4\cdot X_2X_1 + \cdots \\
&= \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=132} \mathbf{X_i} + \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=231} \mathbf{X_i} + \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=321} \mathbf{X_i} = F_{132} + F_{312} + F_{321} = \sum_{w\in 1\sqcup\sqcup 32} F_w.
\end{aligned}$$

Proof of Proposition 8.1.5. The elements $\{F_w(\{X_i\}_{i\in I})\}$ are linearly independent as they are supported on disjoint monomials, and so form a $\mathbf{k}$-basis for their span. The fact that they multiply via rule (8.1.1) is the equivalence of conditions (i) and (iii) in the following Lemma 8.1.6, from which all the remaining assertions follow. □

Lemma 8.1.6. *For a triple of permutations*

$$\begin{aligned}
u &= (u_1,\ldots,u_k) \text{ in } \mathfrak{S}_k, \\
v &= (v_1,\ldots,v_{n-k}) \text{ in } \mathfrak{S}_{n-k}, \\
w &= (w_1,\ldots,w_n) \text{ in } \mathfrak{S}_n,
\end{aligned}$$

the following conditions are equivalent:

(i) w^{-1} *lies in the set* $u^{-1} \sqcup\sqcup v^{-1}[k]$.
(ii) $u = \mathrm{std}(w_1,\ldots,w_k)$ *and* $v = \mathrm{std}(w_{k+1},\ldots,w_n)$,
(iii) *for some word* $\mathbf{i} = (i_1,\ldots,i_n)$ *with* $\mathrm{std}(\mathbf{i}) = w$ *one has* $u = \mathrm{std}(i_1,\ldots,i_k)$ *and* $v = \mathrm{std}(i_{k+1},\ldots,i_n)$.

Proof. The implication (ii) $\Rightarrow$ (iii) is clear since $\mathrm{std}(w) = w$. The reverse implication (iii) $\Rightarrow$ (ii) is best illustrated by example, e.g. considering Example 8.1.2 as concatenated, with $n = 11$ and $k = 6$ and $n-k = 5$:

$$\begin{array}{rcccccc|cccccc} w = \mathrm{std} & (b & a & c & c & b & a & | & a & b & a & c & b) \\ = & (5 & 1 & 9 & 10 & 6 & 2 & | & 3 & 7 & 4 & 11 & 8) \end{array}$$

$$\begin{array}{rcccccc||rcccccc} u = \mathrm{std} & (5 & 1 & 9 & 10 & 6 & 2) & v = \mathrm{std} & (3 & 7 & 4 & 11 & 8) \\ = & (3 & 1 & 5 & 6 & 4 & 2) & = & (1 & 3 & 2 & 5 & 4) \\ = \mathrm{std} & (b & a & c & c & b & a) & = \mathrm{std} & (a & b & a & c & b) \end{array}$$

The equivalence of (i) and (ii) is a fairly standard consequence of unique parabolic factorization $W = W^J W_J$ where $W = \mathfrak{S}_n$ and $W_J = \mathfrak{S}_k \times \mathfrak{S}_{n-k}$, so that W^J are the minimum-length coset representatives for cosets xW_J (that is, the permutations $x \in \mathfrak{S}_n$ satisfying $x_1 < \cdots < x_k$ and $x_{k+1} < \cdots < x_n$). One can uniquely express any w in W as $w = xy$ with x in W^J and y in W_J, which here means that $y = u \cdot v[k] = v[k] \cdot u$ for some u in $\mathfrak{S}_k$ and v in $\mathfrak{S}_{n-k}$. Therefore $w = xuv[k]$, if and only if $w^{-1} = u^{-1}v^{-1}[k]x^{-1}$, which means that w^{-1} is the shuffle of the sequences u^{-1} in positions $\{x_1, \ldots, x_k\}$ and $v^{-1}[k]$ in positions $\{x_{k+1}, \ldots, x_n\}$. $\square$

Example 8.1.7. To illustrate the equivalence of (i) and (ii) and the parabolic factorization in the preceding proof, let $n = 9$ and $k = 5$ with

$$\begin{aligned} w &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & | & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 1 & 5 & | & 8 & 2 & 3 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & | & 6 & 7 & 8 & 9 \\ 1 & 4 & 5 & 6 & 9 & | & 2 & 3 & 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \\ 9 & 6 & 7 & 8 \end{pmatrix} \\ &= x \cdot u \cdot v[k]; \end{aligned}$$

then

$$\begin{aligned} w^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 6 & 1 & 5 & 8 & 2 & 3 & 7 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 3 & 2 \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \\ 7 & 8 & 9 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \underline{1} & \underline{\underline{6}} & \underline{\underline{7}} & \underline{2} & \underline{3} & \underline{4} & \underline{\underline{8}} & \underline{\underline{9}} & \underline{5} \end{pmatrix} \\ &= u^{-1} \cdot v^{-1}[k] \cdot x^{-1}. \end{aligned}$$

Proposition 8.1.5 yields that FQSym is isomorphic to the $\mathbf{k}$-subalgebra $\mathrm{FQSym}(\mathbf{X})$ of the $\mathbf{k}$-algebra $R\langle\mathbf{X}\rangle$ when $\mathbf{X}$ is the variable set $(X_1 < X_2 < \cdots)$. We identify FQSym with $\mathrm{FQSym}(\mathbf{X})$ along this isomorphism. For any infinite alphabet $\{X_i\}_{i \in I}$ and any $f \in \mathrm{FQSym}$, we denote by $f\left(\{X_i\}_{i \in I}\right)$ the image of f under the algebra isomorphism $\mathrm{FQSym} \to \mathrm{FQSym}\left(\{X_i\}_{i \in I}\right)$ defined in Proposition 8.1.5.

One can now use this to define a coalgebra structure on FQSym. Roughly speaking, one wants to first evaluate an element f in $\mathrm{FQSym} \cong \mathrm{FQSym}(\mathbf{X}) \cong \mathrm{FQSym}(\mathbf{X}, \mathbf{Y})$ as $f(\mathbf{X}, \mathbf{Y})$, using the linearly ordered variable set $(\mathbf{X}, \mathbf{Y}) := (X_1 < X_2 < \cdots < Y_1 < Y_2 < \cdots)$. Then one should take the image of $f(\mathbf{X}, \mathbf{Y})$ after imposing the partial commutativity relations

$$X_i Y_j = Y_j X_i \text{ for every pair } (X_i, Y_j) \in \mathbf{X} \times \mathbf{Y}, \tag{8.1.4}$$

and hope that this image lies in a subalgebra isomorphic to

$$\mathrm{FQSym}(\mathbf{X}) \otimes \mathrm{FQSym}(\mathbf{Y}) \cong \mathrm{FQSym} \otimes \mathrm{FQSym}.$$

We argue this somewhat carefully. Start by considering the canonical monoid epimorphism

$$F\langle\mathbf{X}, \mathbf{Y}\rangle \overset{\rho}{\twoheadrightarrow} M, \tag{8.1.5}$$

where $F\langle\mathbf{X}, \mathbf{Y}\rangle$ denotes the *free monoid* on the alphabet $(\mathbf{X}, \mathbf{Y})$ and M denotes its quotient monoid imposing the partial commutativity relations (8.1.4). Let $\mathbf{k}^M$ denote the $\mathbf{k}$-module of all functions $f : M \to \mathbf{k}$, with pointwise addition and scalar multiplication; similarly define $\mathbf{k}^{F\langle\mathbf{X},\mathbf{Y}\rangle}$. As both monoids $F\langle\mathbf{X}, \mathbf{Y}\rangle$ and M enjoy the property that an element m has only finitely many factorizations as $m = m_1 m_2$, one can define a convolution algebra structure on both $\mathbf{k}^{F\langle\mathbf{X},\mathbf{Y}\rangle}$ and $\mathbf{k}^M$ via

$$(f_1 \star f_2)(m) = \sum_{\substack{(m_1, m_2) \in N \times N: \\ m = m_1 m_2}} f_1(m_1) f_2(m_2),$$

where N is respectively $F\langle \mathbf{X}, \mathbf{Y}\rangle$ or M. As fibers of the map ρ in (8.1.5) are finite, it induces a map of convolution algebras, which we also call ρ:

$$\mathbf{k}^{F\langle \mathbf{X},\mathbf{Y}\rangle} \overset{\rho}{\twoheadrightarrow} \mathbf{k}^{M}. \tag{8.1.6}$$

Now recall that $R\langle \mathbf{X}\rangle$ denotes the algebra of noncommutative formal power series in the variable set $\mathbf{X}$, of bounded degree, with coefficients in $\mathbf{k}$. One similarly has the ring $R\langle \mathbf{X}, \mathbf{Y}\rangle$, which can be identified with the subalgebra of $\mathbf{k}^{F\langle \mathbf{X},\mathbf{Y}\rangle}$ consisting of the functions $f : F\langle \mathbf{X}, \mathbf{Y}\rangle \to \mathbf{k}$ having a bound on the length of the words in their support (the value of f on a word in $(\mathbf{X}, \mathbf{Y})$ gives its power series coefficient corresponding to said word). We let $R\langle M\rangle$ denote the analogous subalgebra of $\mathbf{k}^M$; this can be thought of as the algebra of bounded degree "partially commutative power series" in the variable sets $\mathbf{X}$ and $\mathbf{Y}$. Note that ρ restricts to a map

$$R\langle \mathbf{X}, \mathbf{Y}\rangle \overset{\rho}{\to} R\langle M\rangle. \tag{8.1.7}$$

Finally, we claim (and see Proposition 8.1.9 below for a proof) that this further restricts to a map

$$\mathrm{FQSym}\,(\mathbf{X}, \mathbf{Y}) \overset{\rho}{\to} \mathrm{FQSym}\,(\mathbf{X}) \otimes \mathrm{FQSym}\,(\mathbf{Y}) \tag{8.1.8}$$

in which the target is identified with its image under the (injective[368]) multiplication map

$$\begin{array}{rcl} \mathrm{FQSym}\,(\mathbf{X}) \otimes \mathrm{FQSym}\,(\mathbf{Y}) & \hookrightarrow & R\langle M\rangle, \\ f(\mathbf{X}) \otimes g(\mathbf{Y}) & \mapsto & f(\mathbf{X})g(\mathbf{Y}). \end{array}$$

Using the identification of FQSym with all three of $\mathrm{FQSym}\,(\mathbf{X}), \mathrm{FQSym}\,(\mathbf{Y}), \mathrm{FQSym}\,(\mathbf{X}, \mathbf{Y})$, the map ρ in (8.1.8) will then define a coproduct structure on FQSym. Abusing notation, for f in FQSym, we will simply write $\Delta(f) = f(\mathbf{X}, \mathbf{Y})$ instead of $\rho(f(\mathbf{X}, \mathbf{Y}))$.

Example 8.1.8. Recall from Example 8.1.4 that one has

$$F_{312} = \sum_{\mathbf{i}:\mathrm{std}(\mathbf{i})=231} \mathbf{X}_{\mathbf{i}} = \sum_{1\le i<j\le k} X_j X_k X_i,$$

and therefore its coproduct is

$$\begin{aligned} \Delta F_{312} &= F_{312}(X_1, X_2, \ldots, Y_1, Y_2, \ldots) \qquad \text{(by our abuse of notation)} \\ &= \sum_{i<j\le k} X_j X_k X_i + \sum_{\substack{i<j,\\ k}} X_j Y_k X_i + \sum_{\substack{i,\\ j\le k}} Y_j Y_k X_i + \sum_{i<j\le k} Y_j Y_k Y_i \\ &= \sum_{i<j\le k} X_j X_k X_i \cdot 1 + \sum_{\substack{i<j,\\ k}} X_j X_i \cdot Y_k + \sum_{\substack{i,\\ j\le k}} X_i \cdot Y_j Y_k + \sum_{i<j\le k} 1 \cdot Y_j Y_k Y_i \\ &= F_{312}(\mathbf{X}) \cdot 1 + F_{21}(\mathbf{X}) \cdot F_1(\mathbf{Y}) + F_1(\mathbf{X}) \cdot F_{12}(\mathbf{Y}) + 1 \cdot F_{312}(\mathbf{Y}) \\ &= F_{312} \otimes 1 + F_{21} \otimes F_1 + F_1 \otimes F_{12} + 1 \otimes F_{312}. \end{aligned}$$

Proposition 8.1.9. *The map ρ in (8.1.7) does restrict as claimed to a map as in (8.1.8), and hence defines a coproduct on* FQSym, *acting on the $\{F_w\}$ basis by the rule (8.1.2). This endows* FQSym *with the structure of a connected graded finite type Hopf algebra.*

Proof. Let I be the totally ordered set $\{1 < 2 < 3 < \cdots\}$. Let J be the totally ordered set $\left\{1 < 2 < 3 < \cdots < \widetilde{1} < \widetilde{2} < \widetilde{3} < \cdots\right\}$. We set $X_{\widetilde{i}} = Y_i$ for every positive integer i. Then, the alphabet $(\mathbf{X}, \mathbf{Y})$ can be written as $\{X_i\}_{i\in J}$.

If $\mathbf{i}$ is a word over the alphabet $I = \{1 < 2 < 3 < \cdots\}$, then we denote by $\widetilde{\mathbf{i}}$ the word over J obtained from $\mathbf{i}$ by replacing every letter i by $\widetilde{i}$.

[368] as images of the basis $F_u(\mathbf{X}) \otimes F_v(\mathbf{Y})$ of $\mathrm{FQSym}(\mathbf{X}) \otimes \mathrm{FQSym}(\mathbf{Y})$ are supported on disjoint monomials in $R\langle M\rangle$, so linearly independent.

For the first assertion of Proposition 8.1.9, it suffices to check that F_w indeed has the image under Δ claimed in (8.1.2). Let $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$. Then,

$$\begin{aligned}
\Delta F_w &= F_w\left(\mathbf{X}, \mathbf{Y}\right) \qquad \text{(by our abuse of notation)} \\
&= \sum_{\mathbf{i} \in J^n : \operatorname{std}(\mathbf{i}) = w^{-1}} (\mathbf{X}, \mathbf{Y})_{\mathbf{i}} = \sum_{\mathbf{t} \in J^n : \operatorname{std}(\mathbf{t}) = w^{-1}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}} \\
&= \sum_{k=0}^{n} \sum_{(\mathbf{i}, \mathbf{j}) \in I^k \times I^{n-k}} \sum_{\substack{\mathbf{t} \in J^n : \\ \operatorname{std}(\mathbf{t}) = w^{-1}; \\ \mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}} \qquad (8.1.9)
\end{aligned}$$

(since for every $\mathbf{t} \in J^n$, there exists exactly one choice of $k \in \{0, 1, \ldots, n\}$ and $(\mathbf{i}, \mathbf{j}) \in I^k \times I^{n-k}$ satisfying $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$; namely, $\mathbf{i}$ is the restriction of $\mathbf{t}$ to the subalphabet I of J, whereas $\mathbf{j}$ is the restriction of $\mathbf{t}$ to $J \setminus I$, and k is the length of $\mathbf{i}$).

We now fix k and $(\mathbf{i}, \mathbf{j})$, and try to simplify the inner sum $\sum_{\substack{\mathbf{t} \in J^n : \\ \operatorname{std}(\mathbf{t}) = w^{-1}; \\ \mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}}} (\mathbf{X}, \mathbf{Y})_{\mathbf{t}}$ on the right hand side of (8.1.9). First we notice that this sum is nonempty if and only if there exists some $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ satisfying $\operatorname{std}(\mathbf{t}) = w^{-1}$. This existence is easily seen to be equivalent to $w^{-1} \in \operatorname{std}(\mathbf{i}) \sqcup\!\sqcup \operatorname{std}(\mathbf{j})[k]$ (since the standardization of any shuffle in $\mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ is the corresponding shuffle in $\operatorname{std}(\mathbf{i}) \sqcup\!\sqcup \operatorname{std}(\mathbf{j})[k]$). This, in turn, is equivalent to $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$ (according to the equivalence (i) $\Longleftrightarrow$ (ii) in Lemma 8.1.6). Hence, the inner sum on the right hand side of (8.1.9) is nonempty if and only if $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$. When it is nonempty, it has only one addend[369], and this addend is $(\mathbf{X}, \mathbf{Y})_{\mathbf{t}} = \mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}}$ (since $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$). Summarizing, we see that the inner sum on the right hand side of (8.1.9) equals $\mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}}$ when $\operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1}$ and $\operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}$, and is empty otherwise. Thus, (8.1.9) simplifies to

$$\begin{aligned}
\Delta F_w &= \sum_{k=0}^{n} \sum_{\substack{(\mathbf{i}, \mathbf{j}) \in I^k \times I^{n-k} : \\ \operatorname{std}(\mathbf{i}) = (\operatorname{std}(w_1, \ldots, w_k))^{-1} \\ \operatorname{std}(\mathbf{j}) = (\operatorname{std}(w_{k+1}, \ldots, w_n))^{-1}}} \mathbf{X}_{\mathbf{i}} \mathbf{Y}_{\mathbf{j}} \\
&= \sum_{k=0}^{n} F_{\operatorname{std}(w_1, \ldots, w_k)}(\mathbf{X}) F_{\operatorname{std}(w_{k+1}, \ldots, w_n)}(\mathbf{Y}) \\
&= \sum_{k=0}^{n} F_{\operatorname{std}(w_1, \ldots, w_k)} \otimes F_{\operatorname{std}(w_{k+1}, \ldots, w_n)} \in \mathrm{FQSym} \otimes \mathrm{FQSym}\,.
\end{aligned}$$

This proves (8.1.2), and thus the first assertion of Proposition 8.1.9.

From this, it is easy to derive that Δ satisfies coassociativity (i.e., the diagram (1.2.1) holds for $C = \mathrm{FQSym}$). (Alternatively, one can obtain this from the associativity of multiplication using Corollary 8.1.11.) We have already verified the rule (8.1.2). The connected graded structure on FQSym gives a counit and an antipode for free. □

Exercise 8.1.10. We say that a permutation $w \in \mathfrak{S}_n$ is *connected* if n is a positive integer and if there exists no $i \in \{1, 2, \ldots, n-1\}$ satisfying $f(\{1, 2, \ldots, i\}) = \{1, 2, \ldots, i\}$. Let $\mathfrak{CS}$ denote the set of all connected permutations of all $n \in \mathbb{N}$. Show that FQSym is a free (noncommutative) $\mathbf{k}$-algebra with generators $(F_w)_{w \in \mathfrak{CS}}$. (This statement means that $(F_{w_1} F_{w_2} \cdots F_{w_k})_{k \in \mathbb{N};\ (w_1, w_2, \ldots, w_k) \in \mathfrak{CS}^k}$ is a basis of the $\mathbf{k}$-module FQSym.)

[**Hint:** This is a result of Poirier and Reutenauer [172, Theorem 2.1]; it is much easier than the similar Theorem 6.4.3.]

[369] In fact, the elements $\operatorname{std}(\mathbf{t})$ for $\mathbf{t} \in \mathbf{i} \sqcup\!\sqcup \widetilde{\mathbf{j}}$ are distinct, and thus only one of them can equal w^{-1}.

Corollary 8.1.11. *The Hopf algebra* FQSym *is self-dual: Let* $\{G_w\}$ *be the dual* $\mathbf{k}$*-basis to the* $\mathbf{k}$*-basis* $\{F_w\}$ *for* FQSym*. Then, the* $\mathbf{k}$*-linear map sending* $G_w \longmapsto F_{w^{-1}}$ *is a Hopf algebra isomorphism* $\mathrm{FQSym}^o \longrightarrow \mathrm{FQSym}$*.*

Proof. For any $0 \leq k \leq n$, any $u \in \mathfrak{S}_k$ and any $v \in \mathfrak{S}_{n-k}$, one has

$$F_{u^{-1}} F_{v^{-1}} = \sum_{w^{-1} \in u^{-1} \sqcup\!\sqcup v^{-1}[k]} F_{w^{-1}} = \sum_{\substack{w \in \mathfrak{S}_n: \\ \mathrm{std}(w_1,\ldots,w_k)=u \\ \mathrm{std}(w_{k+1},\ldots,w_n)=v}} F_{w^{-1}}$$

via the equivalence of (i) and (ii) in Lemma 8.1.6. On the other hand, in FQSym^o, the dual $\mathbf{k}$-basis $\{G_w\}$ to the $\mathbf{k}$-basis $\{F_w\}$ for FQSym should have product formula

$$G_u G_v = \sum_{\substack{w \in \mathfrak{S}_n: \\ \mathrm{std}(w_1,\ldots,w_k)=u \\ \mathrm{std}(w_{k+1},\ldots,w_n)=v}} G_w$$

coming from the coproduct formula (8.1.2) for FQSym in the $\{F_w\}$-basis. Comparing these equalities, we see that the $\mathbf{k}$-linear map τ sending $G_w \longmapsto F_{w^{-1}}$ is an isomorphism $\mathrm{FQSym}^o \longrightarrow \mathrm{FQSym}$ of $\mathbf{k}$-algebras. Hence, the adjoint $\tau^* : \mathrm{FQSym}^o \to (\mathrm{FQSym}^o)^o$ of this map is an isomorphism of $\mathbf{k}$-coalgebras. But identifying $(\mathrm{FQSym}^o)^o$ with FQSym in the natural way (since FQSym is of finite type), we easily see that $\tau^* = \tau$, whence τ itself is an isomorphism of both $\mathbf{k}$-algebras and $\mathbf{k}$-coalgebras, hence of $\mathbf{k}$-bialgebras, hence of Hopf algebras. □

We can now be a bit more precise about the relations between the various algebras

$$\Lambda, \mathrm{QSym}, \mathrm{NSym}, \mathrm{FQSym}, R\langle \mathbf{X} \rangle, R(\mathbf{x}).$$

Not only does FQSym allow one to *lift* the Hopf structure of QSym, it dually allows one to *extend* the Hopf structure of NSym. To set up this duality, note that Corollary 8.1.11 motivates the choice of an inner product on FQSym in which

$$(F_u, F_v) := \delta_{u^{-1},v}.$$

We wish to identify the images of the ribbon basis $\{R_\alpha\}$ of NSym when included in FQSym.

Definition 8.1.12. For any composition α, define an element $\mathbf{R}_\alpha$ of FQSym by

$$\mathbf{R}_\alpha := \sum_{\substack{w \in \mathfrak{S}_{|\alpha|}: \\ \mathrm{Des}(w)=D(\alpha)}} F_{w^{-1}} = \sum_{\substack{(w,\mathbf{i}): \\ w \in \mathfrak{S}_{|\alpha|}; \\ \mathrm{Des}(w)=D(\alpha); \\ \mathrm{std}(\mathbf{i})=w}} \mathbf{X}_{\mathbf{i}} = \sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha)} \mathbf{X}_{\mathbf{i}},$$

where the *descent set* of a sequence $\mathbf{i} = (i_1, \ldots, i_n)$ is defined by

$$\mathrm{Des}(\mathbf{i}) := \{j \in \{1, 2, \ldots, n-1\} : i_j > i_{j+1}\} = \mathrm{Des}(\mathrm{std}(\mathbf{i})).$$

Alternatively,

$$\mathbf{R}_\alpha = \sum_T \mathbf{X}_T \tag{8.1.10}$$

in which the sum is over column-strict tableaux of the ribbon skew shape $\mathrm{Rib}\,(\alpha)$, and $\mathbf{X}_T = \mathbf{X}_{\mathbf{i}}$ in which $\mathbf{i}$ is the sequence of entries of T read in order from the southwest toward the northeast.

Example 8.1.13. Taking $\alpha = (1, 3, 2)$, with ribbon shape and column-strict fillings T as shown:

$$\mathrm{Rib}\,(\alpha) = \begin{array}{ccc} & \square & \square \\ \square & \square & \square \\ \square & & \end{array} \qquad \text{and} \qquad T = \begin{array}{ccccccc} & & & & & & i_5 \\ & & & & & & \wedge \\ i_2 & \leq & i_3 & \leq & i_4 & \leq & i_6 \\ \wedge & & & & & & \\ i_1 & & & & & & \end{array}$$

one has that

$$\mathbf{R}_{(1,3,2)} = \sum_{\substack{\mathbf{i}=(i_1,i_2,i_3,i_4,i_5,i_6): \\ \mathrm{Des}(\mathbf{i})=D(\alpha)=\{1,4\}}} \mathbf{X}_{\mathbf{i}} = \sum_{i_1 > i_2 \leq i_3 \leq i_4 > i_5 \leq i_6} X_{i_1} X_{i_2} X_{i_3} X_{i_4} X_{i_5} X_{i_6} = \sum_T \mathbf{X}_T.$$

Corollary 8.1.14. *For every $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$, we let $\gamma(w)$ denote the unique composition α of n satisfying $D(\alpha) = \operatorname{Des}(w)$.*

(a) *The* $\mathbf{k}$*-linear map*

$$\begin{array}{ccc} \mathrm{FQSym} & \overset{\pi}{\twoheadrightarrow} & \mathrm{QSym}, \\ F_w & \longmapsto & L_{\gamma(w)} \end{array}$$

is a surjective Hopf algebra homomorphism.

(b) *The* $\mathbf{k}$*-linear map*

$$\begin{array}{ccc} \mathrm{NSym} & \overset{\iota}{\hookrightarrow} & \mathrm{FQSym}, \\ R_\alpha & \longmapsto & \mathbf{R}_\alpha \end{array}$$

is an injective Hopf algebra homomorphism.

(c) *The linear maps π and ι are adjoint maps with respect to the above choice of inner product on* FQSym *and the usual dual pairing between* NSym *and* QSym.

Now, consider the abelianization map $\mathrm{ab} : R\langle \mathbf{X} \rangle \twoheadrightarrow R(\mathbf{x})$ *defined as the continuous* $\mathbf{k}$*-algebra homomorphism sending the noncommutative variable X_i to the commutative x_i.*

(d) *The map π is a restriction of* ab.

(e) *The map ι lets one factor the surjection* $\mathrm{NSym} \twoheadrightarrow \Lambda$ *as follows:*

$$\begin{array}{ccccccc} \mathrm{NSym} & \to & \mathrm{FQSym} \hookrightarrow R\langle \mathbf{X} \rangle & \overset{\mathrm{ab}}{\to} & R(\mathbf{x}), \\ R_\alpha & \longmapsto & \mathbf{R}_\alpha & \longmapsto & s_{\mathrm{Rib}(\alpha)}(\mathbf{x}). \end{array}$$

Proof. Given $n \in \mathbb{N}$, each composition α of n can be written in the form $\gamma(w)$ for some $w \in \mathfrak{S}_n$.[370] Hence, each fundamental quasisymmetric function L_α lies in the image of π. Thus, π is surjective.

Also, for each $n \in \mathbb{N}$ and $\alpha \in \mathrm{Comp}_n$, the element $\mathbf{R}_\alpha$ is a nonempty sum of noncommutative monomials (nonempty because α can be written in the form $\gamma(w)$ for some $w \in \mathfrak{S}_n$). Moreover, the elements $\mathbf{R}_\alpha$ for varying n and α are supported on disjoint monomials. Thus, these elements are linearly independent. Hence, the map ι is injective.

(d) Let $\mathfrak{A}$ denote the totally ordered set $\{1 < 2 < 3 < \cdots\}$ of positive integers. For each word $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{A}^n$, we define a monomial $\mathbf{x}_w$ in $\mathbf{k}[[\mathbf{x}]]$ by $\mathbf{x}_w = x_{w_1} x_{w_2} \cdots x_{w_n}$.

Let $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Then,

$$L_{\gamma(\sigma)} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w$$

(by Lemma 5.3.6). But (8.1.3) (applied to $w = \sigma$) yields

$$F_\sigma = \sum_{\substack{\mathbf{i} = (i_1, \ldots, i_n): \\ \operatorname{std}(\mathbf{i}) = \sigma^{-1}}} \mathbf{X}_{\mathbf{i}} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{X}_w$$

and thus

$$\mathrm{ab}(F_\sigma) = \mathrm{ab}\left(\sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{X}_w \right) = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \underbrace{\mathrm{ab}(\mathbf{X}_w)}_{= \mathbf{x}_w} = \sum_{\substack{w \in \mathfrak{A}^n; \\ \operatorname{std} w = \sigma^{-1}}} \mathbf{x}_w = L_{\gamma(\sigma)} = \pi(F_\sigma).$$

We have shown this for all $n \in \mathbb{N}$ and $\sigma \in \mathfrak{S}_n$. Thus, π is a restriction of ab. This proves Corollary 8.1.14(d).

[370] Indeed, write our composition α as $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Then, we can pick w to be the permutation whose first α_1 entries are the largest α_1 elements of $\{1, 2, \ldots, n\}$ in increasing order; whose next α_2 entries are the next-largest α_2 elements of $\{1, 2, \ldots, n\}$ in increasing order; and so on. This permutation w will satisfy $\operatorname{Des}(w) = \{\alpha_1, \alpha_1 + \alpha_2, \ldots, \alpha_1 + \alpha_2 + \cdots + \alpha_{k-1}\} = D(\alpha)$ and thus $\gamma(w) = \alpha$.

(a) Let $n \in \mathbb{N}$ and $w = (w_1, w_2, \ldots, w_n) \in \mathfrak{S}_n$. Let α be the composition $\gamma(w)$ of n. Thus, the definition of π yields $\pi(F_w) = L_\alpha$. But applying the map $\pi \otimes \pi$ to the equality (8.1.2), we obtain

$$\begin{aligned}(\pi \otimes \pi)(\Delta F_w) &= (\pi \otimes \pi)\left(\sum_{k=0}^{n} F_{\mathrm{std}(w_1,w_2,\ldots,w_k)} \otimes F_{\mathrm{std}(w_{k+1},w_{k+2},\ldots,w_n)}\right) \\ &= \sum_{k=0}^{n} \pi\left(F_{\mathrm{std}(w_1,w_2,\ldots,w_k)}\right) \otimes \pi\left(F_{\mathrm{std}(w_{k+1},w_{k+2},\ldots,w_n)}\right) \\ &= \sum_{k=0}^{n} L_{\gamma(\mathrm{std}(w_1,w_2,\ldots,w_k))} \otimes L_{\gamma(\mathrm{std}(w_{k+1},w_{k+2},\ldots,w_n))} \qquad (8.1.11)\end{aligned}$$

(by the definition of π). Now, for each $k \in \{0, 1, \ldots, n\}$, the two compositions $\gamma(\mathrm{std}(w_1, w_2, \ldots, w_k))$ $\gamma(\mathrm{std}(w_{k+1}, w_{k+2}, \ldots, w_n))$ form a pair (β, γ) of compositions satisfying[371] either $\beta \cdot \gamma = \alpha$ or $\beta \odot \gamma = \alpha$, and in fact they form the only such pair satisfying $|\beta| = k$ and $|\gamma| = n - k$. Thus, the right hand side of (8.1.11) can be rewritten as

$$\sum_{\substack{(\beta,\gamma):\\ \beta\cdot\gamma=\alpha \text{ or } \beta\odot\gamma=\alpha}} L_\beta \otimes L_\gamma.$$

But this sum is ΔL_α, as we know from (5.2.5). Hence, (8.1.11) becomes

$$(\pi \otimes \pi)(\Delta F_w) = \Delta L_\alpha = \Delta(\pi(F_w)) \qquad (\text{since } L_\alpha = \pi(F_w)).$$

We have proven this for each $n \in \mathbb{N}$ and $w \in \mathfrak{S}_n$. Thus, we have proven that $(\pi \otimes \pi) \circ \Delta_{\mathrm{FQSym}} = \Delta_{\mathrm{QSym}} \circ \pi$. Combined with $\epsilon_{\mathrm{FQSym}} = \epsilon_{\mathrm{QSym}} \circ \pi$ (which is easy to check), this shows that π is a coalgebra homomorphism.

We can similarly see that π is an algebra homomorphism by checking that it respects the product (compare (5.2.6) and (8.1.1)). However, this also follows trivially from Corollary 8.1.14(d).

Thus, π is a bialgebra morphism, and therefore a Hopf algebra morphism (by Corollary 1.4.27). This proves Corollary 8.1.14(a).

(c) For any composition α and any $w \in \mathfrak{S}$, we have

$$\begin{aligned}(\iota(R_\alpha), F_w) = (\mathbf{R}_\alpha, F_w) &= \sum_{u:\mathrm{Des}(u)=D(\alpha)} (F_{u^{-1}}, F_w) = \begin{cases} 1, & \text{if } \mathrm{Des}(w) = D(\alpha); \\ 0, & \text{otherwise} \end{cases} = \begin{cases} 1, & \text{if } \gamma(w) = \alpha; \\ 0, & \text{otherwise} \end{cases} \\ &= (R_\alpha, L_{\gamma(w)}) = (R_\alpha, \pi(F_w)).\end{aligned}$$

Thus, the maps π and ι are adjoint. This proves Corollary 8.1.14(c).

(b) Again, there are several ways to prove this. Here is one:

First, note that $\iota(1) = 1$ (because $R_\varnothing = 1$ and $\mathbf{R}_\varnothing = 1$). Next, let α and β be two nonempty compositions. Let $m = |\alpha|$ and $n = |\beta|$. Then, $R_\alpha R_\beta = R_{\alpha\cdot\beta} + R_{\alpha\odot\beta}$ (by (5.4.11)) and thus

$$\begin{aligned}\iota(R_\alpha R_\beta) = \iota(R_{\alpha\cdot\beta} + R_{\alpha\odot\beta}) &= \underbrace{\iota(R_{\alpha\cdot\beta})}_{=\mathbf{R}_{\alpha\cdot\beta}=\sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha\cdot\beta)}\mathbf{X}_\mathbf{i}} + \underbrace{\iota(R_{\alpha\odot\beta})}_{=\mathbf{R}_{\alpha\odot\beta}=\sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha\odot\beta)}\mathbf{X}_\mathbf{i}} \\ &= \sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha\cdot\beta)} \mathbf{X}_\mathbf{i} + \sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha\odot\beta)} \mathbf{X}_\mathbf{i} = \sum_{\mathbf{i}:\mathrm{Des}(\mathbf{i})=D(\alpha\cdot\beta) \text{ or } \mathrm{Des}(\mathbf{i})=D(\alpha\odot\beta)} \mathbf{X}_\mathbf{i} \\ &= \sum_{\substack{\mathbf{i}=(i_1,i_2,\ldots,i_{m+n}):\\ \mathrm{Des}(i_1,i_2,\ldots,i_m)=D(\alpha) \text{ and} \\ \mathrm{Des}(i_{m+1},i_{m+2},\ldots,i_{m+n})=D(\beta)}} \mathbf{X}_\mathbf{i} \qquad (8.1.12)\end{aligned}$$

(since the words $\mathbf{i}$ of length $m+n$ satisfying $\mathrm{Des}(\mathbf{i}) = D(\alpha \cdot \beta)$ or $\mathrm{Des}(\mathbf{i}) = D(\alpha \odot \beta)$ are precisely the words $\mathbf{i} = (i_1, i_2, \ldots, i_{m+n})$ satisfying $\mathrm{Des}(i_1, i_2, \ldots, i_m) = D(\alpha)$ and $\mathrm{Des}(i_{m+1}, i_{m+2}, \ldots, i_{m+n}) = D(\beta)$). But choosing a word $\mathbf{i} = (i_1, i_2, \ldots, i_{m+n})$ satisfying $\mathrm{Des}(i_1, i_2, \ldots, i_m) = D(\alpha)$ and $\mathrm{Des}(i_{m+1}, i_{m+2}, \ldots, i_{m+n}) =$

[371] See Definition 5.2.14 for the notation we are using.

$D(\beta)$ is tantamount to choosing a pair $(\mathbf{u}, \mathbf{v})$ of a word $\mathbf{u} = (i_1, i_2, \ldots, i_m)$ satisfying $\operatorname{Des}\mathbf{u} = D(\alpha)$ and a word $\mathbf{v} = (i_{m+1}, i_{m+2}, \ldots, i_{m+n})$ satisfying $\operatorname{Des}\mathbf{v} = D(\beta)$. Thus, (8.1.12) becomes

$$\begin{aligned}\iota(R_\alpha R_\beta) &= \sum_{\substack{\mathbf{i}=(i_1,i_2,\ldots,i_{m+n}):\\ \operatorname{Des}(i_1,i_2,\ldots,i_m)=D(\alpha) \text{ and}\\ \operatorname{Des}(i_{m+1},i_{m+2},\ldots,i_{m+n})=D(\beta)}} \mathbf{X}_\mathbf{i} = \sum_{\mathbf{u}:\operatorname{Des}\mathbf{u}=D(\alpha)} \sum_{\mathbf{v}:\operatorname{Des}\mathbf{v}=D(\beta)} \mathbf{X}_\mathbf{u}\mathbf{X}_\mathbf{v} \\ &= \underbrace{\left(\sum_{\mathbf{u}:\operatorname{Des}\mathbf{u}=D(\alpha)} \mathbf{X}_\mathbf{u}\right)}_{=\mathbf{R}_\alpha=\iota(R_\alpha)} \underbrace{\left(\sum_{\mathbf{v}:\operatorname{Des}\mathbf{v}=D(\beta)} \mathbf{X}_\mathbf{v}\right)}_{=\mathbf{R}_\beta=\iota(R_\beta)} = \iota(R_\alpha)\,\iota(R_\beta).\end{aligned}$$

Thus, we have proven the equality $\iota(R_\alpha R_\beta) = \iota(R_\alpha)\,\iota(R_\beta)$ whenever α and β are two nonempty compositions. It also holds if we drop the "nonempty" requirement (since $R_\varnothing = 1$ and $\iota(1) = 1$). Thus, the $\mathbf{k}$-linear map ι respects the multiplication. Since $\iota(1) = 1$, this shows that ι is a $\mathbf{k}$-algebra homomorphism.

For each $n \in \mathbb{N}$, we let id_n be the identity permutation in $\mathfrak{S}_n$. Next, we observe that each $n \in \mathbb{N}$ satisfies $H_n = R_{(n)}$ (this follows, e.g., from (5.4.9), because the composition (n) is coarsened only by itself). Hence, each $n \in \mathbb{N}$ satisfies

$$\begin{aligned}\iota(H_n) = \iota\left(R_{(n)}\right) = \mathbf{R}_{(n)} &= \sum_{\substack{w\in\mathfrak{S}_n:\\ \operatorname{Des}(w)=D((n))}} F_{w^{-1}} \\ &= F_{\mathrm{id}_n^{-1}} \qquad \text{(since the only } w \in \mathfrak{S}_n \text{ satisfying } \operatorname{Des}(w) = D((n)) \text{ is } \mathrm{id}_n) \\ &= F_{\mathrm{id}_n}. \qquad (8.1.13)\end{aligned}$$

In order to show that ι is a $\mathbf{k}$-coalgebra homomorphism, it suffices to check the equalities $(\iota\otimes\iota)\circ\Delta_{\mathrm{NSym}} = \Delta_{\mathrm{FQSym}}\circ\iota$ and $\epsilon_{\mathrm{NSym}} = \epsilon_{\mathrm{FQSym}}\circ\iota$. We shall only prove the first one, since the second is easy. Since ι, Δ_{NSym} and Δ_{FQSym} are $\mathbf{k}$-algebra homomorphisms, it suffices to check it on the generators $H_1, H_2, H_3, \ldots$ of NSym. But on these generators, it follows from comparing

$$\begin{aligned}((\iota\otimes\iota)\circ\Delta_{\mathrm{NSym}})(H_n) &= (\iota\otimes\iota)(\Delta_{\mathrm{NSym}}H_n) = (\iota\otimes\iota)\left(\sum_{i+j=n} H_i\otimes H_j\right) \qquad \text{(by (5.4.2))} \\ &= \sum_{i+j=n} \underbrace{\iota(H_i)}_{\substack{=F_{\mathrm{id}_i}\\ \text{(by (8.1.13))}}} \otimes \underbrace{\iota(H_j)}_{\substack{=F_{\mathrm{id}_j}\\ \text{(by (8.1.13))}}} = \sum_{i+j=n} F_{\mathrm{id}_i}\otimes F_{\mathrm{id}_j} = \sum_{k=0}^{n} F_{\mathrm{id}_k}\otimes F_{\mathrm{id}_{n-k}}\end{aligned}$$

with

$$\begin{aligned}(\Delta_{\mathrm{FQSym}}\circ\iota)(H_n) &= \Delta_{\mathrm{FQSym}}(\iota(H_n)) = \Delta_{\mathrm{FQSym}}(F_{\mathrm{id}_n}) \qquad \text{(by (8.1.13))} \\ &= \sum_{k=0}^{n} F_{\mathrm{id}_k}\otimes F_{\mathrm{id}_{n-k}} \qquad \text{(by (8.1.2))}.\end{aligned}$$

Thus, we know that ι is a $\mathbf{k}$-algebra homomorphism and a $\mathbf{k}$-coalgebra homomorphism. Hence, ι is a bialgebra morphism, and therefore a Hopf algebra morphism (by Corollary 1.4.27). This proves Corollary 8.1.14(b).

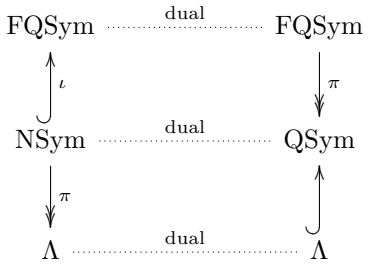
An alternative proof of Corollary 8.1.14(b) can be obtained by adjointness from Corollary 8.1.14(a). Both the inner product on FQSym and the dual pairing $(\cdot,\cdot) : \mathrm{NSym}\otimes\mathrm{QSym}\to\mathbf{k}$ respect the Hopf structures (i.e., the maps Δ_{NSym} and m_{QSym} are mutually adjoint with respect to these forms, and so are the maps m_{NSym} and Δ_{QSym}, and the maps Δ_{FQSym} and m_{FQSym}, and so on). Corollary 8.1.14(c) shows that the map ι is adjoint to the map π with respect to these two bilinear forms. Hence, we have a commutative diagram

$$\begin{array}{ccc} \mathrm{NSym} & \xhookrightarrow{\ \iota\ } & \mathrm{FQSym} \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{QSym}^o & \xrightarrow[\pi^*]{} & \mathrm{FQSym}^o \end{array}$$

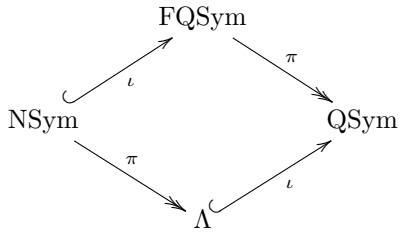
of Hopf algebras (where the two vertical arrows are the isomorphisms induced by the two bilinear forms). Thus, Corollary 8.1.14(b) follows from Corollary 8.1.14(a) by duality.

(e) For each composition α, the abelianization map ab sends the noncommutative tableau monomial $\mathbf{X}_T$ to the commutative tableau monomial $\mathbf{x}_T$ whenever T is a tableau of ribbon shape $\mathrm{Rib}\,(\alpha)$. Thus, ab sends $\mathbf{R}_\alpha$ to $s_{\mathrm{Rib}(\alpha)}(\mathbf{x})$ (because of the formula (8.1.10)). Hence, the composition $\mathrm{NSym} \to \mathrm{FQSym} \hookrightarrow R\langle\mathbf{X}\rangle \overset{\mathrm{ab}}{\to} R(\mathbf{x})$ does indeed send R_α to $s_{\mathrm{Rib}(\alpha)}(\mathbf{x})$. But so does the projection $\pi : \mathrm{NSym} \to \Lambda$, according to Theorem 5.4.10(b). Hence, the composition factors the projection. This proves Corollary 8.1.14(e). □

We summarize some of this picture as follows:



Furthermore, if we denote by ι the canonical inclusion $\Lambda \to \mathrm{QSym}$ as well, then the diagram



is commutative (according to Corollary 8.1.14(e)).

Remark 8.1.15. Different notations for FQSym appear in the literature. In the book [24] (which presents an unusual approach to the character theory of the symmetric group using FQSym), the Hopf algebra FQSym is called $\mathcal{P}$, and its basis that we call $\{G_w\}_{w\in\mathfrak{S}_n}$ is denoted $\{w\}_{w\in\mathfrak{S}_n}$. In [93, Chapter 7], the Hopf algebra FQSym and its basis $\{F_w\}_{w\in\mathfrak{S}_n}$ are denoted MPR and $\{w\}_{w\in\mathfrak{S}_n}$, respectively.

9. Further topics

The following is a list of topics that were, at one point, planned to be touched in class, but did not make the cut. They might get elaborated upon in a future version of these notes.

9.0.1. 0-*Hecke algebras.*

- **Review of representation theory of finite-dimensional algebras.**
  Review the notions of indecomposables, simples, projectives, along with the theorems of Krull-Remak-Schmidt, of Jordan-Hölder, and the two kinds of Grothendieck groups dual to each other.
- **0-Hecke algebra representation theory.**
  Describe the simples and projectives, following Denton, Hivert, Schilling, Thiery [49] on $\mathcal{J}$-trivial monoids.
- **Nsym and Qsym as Grothendieck groups.**
  Give Krob and Thibon's interpretation (see [216, §5] for a brief summary) of
  - QSym and the Grothendieck group of composition series, and
  - NSym and the Grothendieck group of projectives.

  Remark 9.0.1. Mention P. McNamara's interpretation, in the case of *supersolvable lattices*, of the Ehrenborg quasisymmetric function as the composition series enumerator for an $H_n(0)$-action on the maximal chains

9.0.2. *Aguiar-Bergeron-Sottile character theory Part II: Odd and even characters, subalgebras.*

9.0.3. *Face enumeration, Eulerian posets, and cd-indices.* Borrowing from Billera's ICM notes [19].

- f-vectors, h-vectors
- flag f-vectors, flag h-vectors
- ab-indices and cd-indices

9.0.4. *Other topics.*

- Loday-Ronco Hopf algebra of planar binary trees [137]
- Poirier-Reutenauer Hopf algebra of tableaux
- Reading Hopf algebra of Baxter permutations
- Hopf monoids, e.g. of Hopf algebra of generalized permutohedra, of matroids, of graphs, Stanley chromatic symmetric functions and Tutte polynomials
- Lam-Pylyavskyy Hopf algebra of set-valued tableaux
- Connes-Kreimer Hopf algebra and renormalization
- Noncommutative symmetric functions and $\Omega\Sigma\mathbb{C}P^\infty$
- Maschke's theorem and "integrals" for Hopf algebras
- Nichols-Zoeller structure theorem and group-like elements
- Cartier-Milnor-Moore structure theorem and primitive elements
- Quasi-triangular Hopf algebras and quantum groups
- The Steenrod algebra, its dual, and tree Hopf algebras
- Ringel-Hall algebras of quivers
- Ellis-Khovanov odd symmetric function Hopf algebras [67] (see also Lauda-Russell [123])

Student talks given in class were:

(1) Al Garver, on Maschke's theorem for finite-dimensional Hopf algebras
(2) Jonathan Hahn, on the paper by Humpert and Martin.
(3) Emily Gunawan, on the paper by Lam, Lauve and Sottile.
(4) Jonas Karlsson, on the paper by Connes and Kreimer
(5) Thomas McConville, on Butcher's group and generalized Runge-Kutta methods.
(6) Cihan Bahran, on universal enveloping algebras and the Poincaré-Birkhoff-Witt theorem.
(7) Theodosios Douvropolos, on the Cartier-Milnor-Moore theorem.
(8) Alex Csar, on the Loday-Ronco Hopf algebra of binary trees
(9) Kevin Dilks, on Reading's Hopf algebra of (twisted) Baxter permutations
(10) Becky Patrias, on the paper by Lam and Pylyavskyy
(11) Meng Wu, on multiple zeta values and Hoffman's homomorphism from QSym

10. Some open problems and conjectures

- Is there a proof of the Assaf-McNamara skew Pieri rule that gives a resolution of Specht or Schur/Weyl modules whose character corresponds to $s_{\lambda/\mu}h_n$, whose terms model their alternating sum?
- Explicit antipodes in the Lam-Pylyavskyy Hopf algebras? (Answered by Patrias in [170].)
- P. McNamara's question [152, Question 7.1]: are P-partition enumerators irreducible for connected posets P?
- Stanley's question: are the only P-partition enumerators which are symmetric (not just quasisymmetric) those for which P is a skew shape with a column-strict labelling?
- Does Stanley's chromatic symmetric function distinguish trees?
- Hoffman's stuffle conjecture
- Billera-Brenti's nonnegativity conjecture for the total *cd*-index of Bruhat intervals ([20, Conjecture 6.1])

11. Appendix: Some basics

In this appendix, we briefly discuss some basic notions from linear algebra and elementary combinatorics that are used in these notes.

11.1. **Linear expansions and triangularity.** In this Section, we shall recall some fundamental results from linear algebra (most importantly, the notions of a change-of-basis matrix and of a unitriangular matrix), but in greater generality than how it is usually done in textbooks. We shall use these results later when studying bases of combinatorial Hopf algebras; but per se, this section has nothing to do with Hopf algebras.

11.1.1. *Matrices.* Let us first define the notion of a matrix whose rows and columns are indexed by arbitrary objects (as opposed to numbers):[372]

Definition 11.1.1. Let S and T be two sets. An $S \times T$-*matrix over* $\mathbf{k}$ shall mean a family $(a_{s,t})_{(s,t)\in S\times T} \in \mathbf{k}^{S\times T}$ of elements of $\mathbf{k}$ indexed by elements of $S \times T$. Thus, the set of all $S \times T$-matrices over $\mathbf{k}$ is $\mathbf{k}^{S\times T}$.

We shall abbreviate "$S \times T$-matrix over $\mathbf{k}$" by "$S \times T$-matrix" when the value of $\mathbf{k}$ is clear from the context.

This definition of $S \times T$-matrices generalizes the usual notion of matrices (i.e., the notion of $n \times m$-matrices): Namely, if $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then the $\{1, 2, \ldots, n\} \times \{1, 2, \ldots, m\}$-matrices are precisely the $n \times m$-matrices (in the usual meaning of this word). We shall often use the word "*matrix*" for both the usual notion of matrices and for the more general notion of $S \times T$-matrices.

Various concepts defined for $n \times m$-matrices (such as addition and multiplication of matrices, or the notion of a row) can be generalized to $S \times T$-matrices in a straightforward way. The following four definitions are examples of such generalizations:

Definition 11.1.2. Let S and T be two sets.

(a) The sum of two $S \times T$-matrices is defined by $(a_{s,t})_{(s,t)\in S\times T} + (b_{s,t})_{(s,t)\in S\times T} = (a_{s,t} + b_{s,t})_{(s,t)\in S\times T}$.

(b) If $u \in \mathbf{k}$ and if $(a_{s,t})_{(s,t)\in S\times T} \in \mathbf{k}^{S\times T}$, then we define $u\,(a_{s,t})_{(s,t)\in S\times T}$ to be the $S \times T$-matrix $(ua_{s,t})_{(s,t)\in S\times T}$.

(c) Let $A = (a_{s,t})_{(s,t)\in S\times T}$ be an $S \times T$-matrix. For every $s \in S$, we define the *s-th row of A* to be the $\{1\} \times T$-matrix $(a_{s,t})_{(i,t)\in\{1\}\times T}$. (Notice that $\{1\} \times T$-matrices are a generalization of row vectors.) Similarly, for every $t \in T$, we define the *t-th column of A* to be the $S \times \{1\}$-matrix $(a_{s,t})_{(s,i)\in S\times\{1\}}$.

Definition 11.1.3. Let S be a set.

(a) The $S \times S$ *identity matrix* is defined to be the $S \times S$-matrix $(\delta_{s,t})_{(s,t)\in S\times S}$. This $S \times S$-matrix is denoted by I_S. (Notice that the $n \times n$ identity matrix I_n is $I_{\{1,2,\ldots,n\}}$ for each $n \in \mathbb{N}$.)

(b) An $S \times S$-matrix $(a_{s,t})_{(s,t)\in S\times S}$ is said to be *diagonal* if every $(s, t) \in S \times T$ satisfying $s \neq t$ satisfies $a_{s,t} = 0$.

(c) Let $A = (a_{s,t})_{(s,t)\in S\times S}$ be an $S \times S$-matrix. The *diagonal* of A means the family $(a_{s,s})_{s\in S}$. The *diagonal entries* of A are the entries of this diagonal $(a_{s,s})_{s\in S}$.

Definition 11.1.4. Let S, T and U be three sets. Let $A = (a_{s,t})_{(s,t)\in S\times T}$ be an $S \times T$-matrix, and let $B = (b_{t,u})_{(t,u)\in T\times U}$ be a $T \times U$-matrix. Assume that the sum $\sum_{t\in T} a_{s,t}b_{t,u}$ is well-defined for every $(s, u) \in S \times U$. (For example, this is guaranteed to hold if the set T is finite. For infinite T, it may and may not hold.) Then, the $S \times U$-matrix AB is defined by

$$AB = \left(\sum_{t\in T} a_{s,t}b_{t,u}\right)_{(s,u)\in S\times U}.$$

Definition 11.1.5. Let S and T be two finite sets. We say that an $S \times T$-matrix A is *invertible* if and only if there exists a $T \times S$-matrix B satisfying $AB = I_S$ and $BA = I_T$. In this case, this matrix B is unique; it is denoted by A^{-1} and is called the *inverse* of A.

[372] As before, $\mathbf{k}$ denotes a commutative ring.

The definitions that we have just given are straightforward generalizations of the analogous definitions for $n \times m$-matrices; thus, unsurprisingly, many properties of $n \times m$-matrices still hold for $S \times T$-matrices. For example:

Proposition 11.1.6. (a) *Let S and T be two sets. Let A be an $S \times T$-matrix. Then, $I_S A = A$ and $A I_T = A$.*

(b) *Let S, T and U be three sets such that T is finite. Let A and B be two $S \times T$-matrices. Let C be a $T \times U$-matrix. Then, $(A + B) C = AC + BC$.*

(c) *Let S, T, U and V be four sets such that T and U are finite. Let A be an $S \times T$-matrix. Let B be a $T \times U$-matrix. Let C be a $U \times V$-matrix. Then, $(AB) C = A (BC)$.*

The proof of Proposition 11.1.6 (and of similar properties that will be left unstated) is analogous to the proofs of the corresponding properties of $n \times m$-matrices.[373] As a consequence of these properties, it is easy to see that if S is any finite set, then $\mathbf{k}^{S \times S}$ is a $\mathbf{k}$-algebra.

In general, $S \times T$-matrices (unlike $n \times m$-matrices) do not have a predefined order on their rows and their columns. Thus, the classical notion of a triangular $n \times n$-matrix cannot be generalized to a notion of a "triangular $S \times S$-matrix" when S is just a set with no additional structure. However, when S is a poset, such a generalization can be made:

Definition 11.1.7. Let S be a poset. Let $A = (a_{s,t})_{(s,t) \in S \times S}$ be an $S \times S$-matrix.

(a) The matrix A is said to be *triangular* if and only if every $(s,t) \in S \times S$ which does not satisfy $t \leq s$ must satisfy $a_{s,t} = 0$. (Here, $\leq$ denotes the smaller-or-equal relation of the poset S.)

(b) The matrix A is said to be *unitriangular* if and only if A is triangular and has the further property that, for every $s \in S$, we have $a_{s,s} = 1$.

(c) The matrix A is said to be *invertibly triangular* if and only if A is triangular and has the further property that, for every $s \in S$, the element $a_{s,s}$ of $\mathbf{k}$ is invertible.

Of course, all three notions of "triangular", "unitriangular" and "invertibly triangular" depend on the partial order on S.

Clearly, every invertibly triangular $S \times S$-matrix is triangular. Also, every unitriangular $S \times S$-matrix is invertibly triangular (because the element 1 of $\mathbf{k}$ is invertible).

We can restate the definition of "invertibly triangular" as follows: The matrix A is said to be *invertibly triangular* if and only if it is triangular and its diagonal entries are invertible. Similarly, we can restate the definition of "unitriangular" as follows: The matrix A is said to be *unitriangular* if and only if it is triangular and all its diagonal entries equal 1.

Definition 11.1.7(a) generalizes both the notion of upper-triangular matrices and the notion of lower-triangular matrices. To wit:

Example 11.1.8. Let $n \in \mathbb{N}$. Let N_1 be the poset whose ground set is $\{1, 2, \ldots, n\}$ and whose smaller-or-equal relation $\leq_1$ is given by

$$s \leq_1 t \iff s \leq t \text{ (as integers)}.$$

(This is the usual order relation on this set.) Let N_2 be the poset whose ground set is $\{1, 2, \ldots, n\}$ and whose order relation $\leq_2$ is given by

$$s \leq_2 t \iff s \geq t \text{ (as integers)}.$$

Let $A \in \mathbf{k}^{n \times n}$.

(a) The matrix A is upper-triangular if and only if A is triangular when regarded as an $N_1 \times N_1$-matrix.

---

[373] A little **warning**: In Proposition 11.1.6(c), the condition that T and U be finite can be loosened (we leave this to the interested reader), but cannot be completely disposed of. It can happen that both $(AB) C$ and $A (BC)$ are defined, but $(AB) C = A (BC)$ does not hold (if we remove this condition). For example, this happens if $S = \mathbb{Z}$, $T = \mathbb{Z}$, $U = \mathbb{Z}$, $V = \mathbb{Z}$, $A = \left(\begin{cases} 1, & \text{if } i \geq j; \\ 0, & \text{if } i < j \end{cases} \right)_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$, $B = (\delta_{i,j} - \delta_{i,j+1})_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$ and $C = \left(\begin{cases} 0, & \text{if } i \geq j; \\ 1, & \text{if } i < j \end{cases} \right)_{(i,j) \in \mathbb{Z} \times \mathbb{Z}}$. (Indeed, in this example, it is easy to check that $AB = I_{\mathbb{Z}}$ and $BC = -I_{\mathbb{Z}}$ and thus $\underbrace{(AB)}_{= I_{\mathbb{Z}}} C = I_{\mathbb{Z}} C = C \neq -A = A \underbrace{(-I_{\mathbb{Z}})}_{= BC} = A (BC)$.)

This seeming paradox is due to the subtleties of rearranging infinite sums (similarly to how a conditionally convergent series of real numbers can change its value when its entries are rearranged).

(b) The matrix A is lower-triangular if and only if A is triangular when regarded as an $N_2 \times N_2$-matrix.

More interesting examples of triangular matrices are obtained when the order on S is not a total order:

Example 11.1.9. Let S be the poset whose ground set is $\{1,2,3\}$ and whose smaller relation $<_S$ is given by $1 <_S 2$ and $3 <_S 2$. Then, the triangular $S \times S$-matrices are precisely the 3×3-matrices of the form $\begin{pmatrix} a_{1,1} & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} \\ 0 & 0 & a_{3,3} \end{pmatrix}$ with $a_{1,1}, a_{2,1}, a_{2,2}, a_{2,3}, a_{3,3} \in \mathbf{k}$.

We shall now state some basic properties of triangular matrices:

Proposition 11.1.10. *Let S be a finite poset.*

(a) *The triangular $S \times S$-matrices form a subalgebra of the $\mathbf{k}$-algebra $\mathbf{k}^{S \times S}$.*
(b) *The invertibly triangular $S \times S$-matrices form a group with respect to multiplication.*
(c) *The unitriangular $S \times S$-matrices form a group with respect to multiplication.*
(d) *Any invertibly triangular $S \times S$-matrix is invertible, and its inverse is again invertibly triangular.*
(e) *Any unitriangular $S \times S$-matrix is invertible, and its inverse is again unitriangular.*

Exercise 11.1.11. Prove Proposition 11.1.10.

11.1.2. *Expansion of a family in another.* We will often study situations where two families $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ of vectors in a $\mathbf{k}$-module M are given, and the vectors e_s can be written as linear combinations of the vectors f_t. In such situations, we can form an $S \times T$-matrix out of the coefficients of these linear combinations; this is one of the ways how matrices arise in the theory of modules. Let us define the notations we are going to use in such situations:

Definition 11.1.12. Let M be a $\mathbf{k}$-module. Let $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ be two families of elements of M. (The sets S and T may and may not be finite.)

Let $A = (a_{s,t})_{(s,t) \in S \times T}$ be an $S \times T$-matrix. Assume that, for every $s \in S$, all but finitely many $t \in T$ satisfy $a_{s,t} = 0$. (This assumption is automatically satisfied if T is finite.)

We say that the family $(e_s)_{s \in S}$ *expands in the family* $(f_t)_{t \in T}$ *through the matrix* A if

$$\text{every } s \in S \text{ satisfies } e_s = \sum_{t \in T} a_{s,t} f_t. \tag{11.1.1}$$

In this case, we furthermore say that the matrix A is a *change-of-basis matrix* (or *transition matrix*) from the family $(e_s)_{s \in S}$ to the family $(f_t)_{t \in T}$.

Remark 11.1.13. The notation in Definition 11.1.12 is not really standard; even we ourselves will occasionally deviate in its use. In the formulation "the family $(e_s)_{s \in S}$ expands in the family $(f_t)_{t \in T}$ through the matrix A", the word "in" can be replaced by "with respect to", and the word "through" can be replaced by "using".

The notion of a "change-of-basis matrix" is slightly misleading, because neither of the families $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ has to be a basis. Our use of the words "transition matrix" should not be confused with the different meaning that these words have in the theory of Markov chains. The indefinite article in "a change-of-basis matrix" is due to the fact that, for given families $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$, there might be more than one change-of-basis matrix from $(e_s)_{s \in S}$ to $(f_t)_{t \in T}$. (There also might be no such matrix.) When $(e_s)_{s \in S}$ and $(f_t)_{t \in T}$ are bases of the $\mathbf{k}$-module M, there exists precisely one change-of-basis matrix from $(e_s)_{s \in S}$ to $(f_t)_{t \in T}$.

So a change-of-basis matrix $A = (a_{s,t})_{(s,t) \in S \times T}$ from one family $(e_s)_{s \in S}$ to another family $(f_t)_{t \in T}$ allows us to write the elements of the former family as linear combinations of the elements of the latter (using (11.1.1)). When such a matrix A is invertible (and the sets S and T are finite[374]), it also (indirectly) allows us to do the opposite: i.e., to write the elements of the latter family as linear combinations of the elements of the former. This is because if A is an invertible change-of-basis matrix from $(e_s)_{s \in S}$ to $(f_t)_{t \in T}$, then A^{-1} is a change-of-basis matrix from $(f_t)_{t \in T}$ to $(e_s)_{s \in S}$. This is part (a) of the following theorem:

[374]We are requiring the finiteness of S and T mainly for the sake of simplicity. We could allow S and T to be infinite, but then we would have to make some finiteness requirements on A and A^{-1}.

Theorem 11.1.14. *Let M be a $\mathbf{k}$-module. Let S and T be two finite sets. Let $(e_s)_{s\in S}$ and $(f_t)_{t\in T}$ be two families of elements of M.*

Let A be an invertible $S\times T$-matrix. Thus, A^{-1} is a $T\times S$-matrix.

Assume that the family $(e_s)_{s\in S}$ expands in the family $(f_t)_{t\in T}$ through the matrix A. Then:

(a) *The family $(f_t)_{t\in T}$ expands in the family $(e_s)_{s\in S}$ through the matrix A^{-1}.*

(b) *The $\mathbf{k}$-submodule of M spanned by the family $(e_s)_{s\in S}$ is the $\mathbf{k}$-submodule of M spanned by the family $(f_t)_{t\in T}$.*

(c) *The family $(e_s)_{s\in S}$ spans the $\mathbf{k}$-module M if and only if the family $(f_t)_{t\in T}$ spans the $\mathbf{k}$-module M.*

(d) *The family $(e_s)_{s\in S}$ is $\mathbf{k}$-linearly independent if and only if the family $(f_t)_{t\in T}$ is $\mathbf{k}$-linearly independent.*

(e) *The family $(e_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module M if and only if the family $(f_t)_{t\in T}$ is a basis of the $\mathbf{k}$-module M.*

Exercise 11.1.15. Prove Theorem 11.1.14.

Definition 11.1.16. Let M be a $\mathbf{k}$-module. Let S be a finite poset. Let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of M.

(a) We say that the family $(e_s)_{s\in S}$ *expands triangularly in the family* $(f_s)_{s\in S}$ if and only if there exists a triangular $S\times S$-matrix A such that the family $(e_s)_{s\in S}$ expands in the family $(f_s)_{s\in S}$ through the matrix A.

(b) We say that the family $(e_s)_{s\in S}$ *expands invertibly triangularly in the family* $(f_s)_{s\in S}$ if and only if there exists an invertibly triangular $S\times S$-matrix A such that the family $(e_s)_{s\in S}$ expands in the family $(f_s)_{s\in S}$ through the matrix A.

(c) We say that the family $(e_s)_{s\in S}$ *expands unitriangularly in the family* $(f_s)_{s\in S}$ if and only if there exists a unitriangular $S\times S$-matrix A such that the family $(e_s)_{s\in S}$ expands in the family $(f_s)_{s\in S}$ through the matrix A.

Clearly, if the family $(e_s)_{s\in S}$ expands unitriangularly in the family $(f_s)_{s\in S}$, then it also expands invertibly triangularly in the family $(f_s)_{s\in S}$ (because any unitriangular matrix is an invertibly triangular matrix).

We notice that in Definition 11.1.16, the two families $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ must be indexed by one and the same set S.

The concepts of "expanding triangularly", "expanding invertibly triangularly" and "expanding unitriangularly" can also be characterized without referring to matrices, as follows:

Remark 11.1.17. Let M be a $\mathbf{k}$-module. Let S be a finite poset. Let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of M. Let $<$ denote the smaller relation of the poset S, and let $\leq$ denote the smaller-or-equal relation of the poset S. Then:

(a) The family $(e_s)_{s\in S}$ expands triangularly in the family $(f_s)_{s\in S}$ if and only if every $s\in S$ satisfies

$$e_s = (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \text{ for } t\in S \text{ satisfying } t\leq s)\,.$$

(b) The family $(e_s)_{s\in S}$ expands invertibly triangularly in the family $(f_s)_{s\in S}$ if and only if every $s\in S$ satisfies

$$e_s = \alpha_s f_s + (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \text{ for } t\in S \text{ satisfying } t<s)$$

for some invertible $\alpha_s\in\mathbf{k}$.

(c) The family $(e_s)_{s\in S}$ expands unitriangularly in the family $(f_s)_{s\in S}$ if and only if every $s\in S$ satisfies

$$e_s = f_s + (\text{a } \mathbf{k}\text{-linear combination of the elements } f_t \text{ for } t\in S \text{ satisfying } t<s)\,.$$

All three parts of Remark 11.1.17 follow easily from the definitions.

Example 11.1.18. Let $n\in\mathbb{N}$. For this example, let S be the poset $\{1,2,\ldots,n\}$ (with its usual order). Let M be a $\mathbf{k}$-module, and let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of M. We shall identify these families $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ with the n-tuples $(e_1,e_2,\ldots,e_n)$ and $(f_1,f_2,\ldots,f_n)$. Then, the family $(e_s)_{s\in S}=(e_1,e_2,\ldots,e_n)$ expands triangularly in the family $(f_s)_{s\in S}=(f_1,f_2,\ldots,f_n)$ if and only if, for every $s\in\{1,2,\ldots,n\}$, the vector e_s is a $\mathbf{k}$-linear combination of $f_1,f_2,\ldots,f_s$. Moreover, the family $(e_s)_{s\in S}=(e_1,e_2,\ldots,e_n)$ expands unitriangularly in the family $(f_s)_{s\in S}=(f_1,f_2,\ldots,f_n)$ if and only if, for every $s\in\{1,2,\ldots,n\}$, the vector e_s is a sum of f_s with a $\mathbf{k}$-linear combination of $f_1,f_2,\ldots,f_{s-1}$.

Corollary 11.1.19. *Let M be a $\mathbf{k}$-module. Let S be a finite poset. Let $(e_s)_{s\in S}$ and $(f_s)_{s\in S}$ be two families of elements of M. Assume that the family $(e_s)_{s\in S}$ expands invertibly triangularly in the family $(f_s)_{s\in S}$. Then:*

(a) *The family $(f_s)_{s\in S}$ expands invertibly triangularly in the family $(e_s)_{s\in S}$.*
(b) *The $\mathbf{k}$-submodule of M spanned by the family $(e_s)_{s\in S}$ is the $\mathbf{k}$-submodule of M spanned by the family $(f_s)_{s\in S}$.*
(c) *The family $(e_s)_{s\in S}$ spans the $\mathbf{k}$-module M if and only if the family $(f_s)_{s\in S}$ spans the $\mathbf{k}$-module M.*
(d) *The family $(e_s)_{s\in S}$ is $\mathbf{k}$-linearly independent if and only if the family $(f_s)_{s\in S}$ is $\mathbf{k}$-linearly independent.*
(e) *The family $(e_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module M if and only if the family $(f_s)_{s\in S}$ is a basis of the $\mathbf{k}$-module M.*

Exercise 11.1.20. Prove Remark 11.1.17 and Corollary 11.1.19.

An analogue of Corollary 11.1.19 can be stated for unitriangular expansions, but we leave this to the reader.

12. Further hints to the exercises (work in progress)

The following pages contain hints to (some of[375]) the exercises in the text (beyond the hints occasionally included in the exercises themselves). Some of the hints rise to the level of outlined solutions.

Note that there is also a version of this text that contains detailed solutions for all the exercises; this version can be downloaded from http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf (or compiled from the sourcecode of the text).

Warning: The hints below are new and have never been proofread. Typos (or worse) are likely. In case of doubt, consult the detailed solutions.

12.1. **Hints for Chapter 1.** *Hint to Exercise 1.2.3.* The claim of the exercise is dual to the classical fact that if A is a $\mathbf{k}$-module and $m : A \otimes A \to A$ is a $\mathbf{k}$-linear map, then there exists *at most one* $\mathbf{k}$-linear map $u : \mathbf{k} \to A$ such that the diagram (1.1.2) commutes[376]. Take any proof of this latter fact, rewrite it in an "element-free" fashion[377], and "reverse all arrows". This will yield a solution to Exercise 1.2.3.

For an alternative solution, use Sweedler notation (as in (1.2.3)) as follows: The commutativity of the diagram (1.2.2) says that

$$c = \sum_{(c)} \epsilon\left(c_1\right) c_2 = \sum_{(c)} \epsilon\left(c_2\right) c_1 \qquad \text{for each } c \in C.$$

Thus, if ϵ_1 and ϵ_2 are two $\mathbf{k}$-linear maps $\epsilon : C \to \mathbf{k}$ such that the diagram (1.2.2) commutes, then each $c \in C$ satisfies

$$c = \sum_{(c)} \epsilon_1\left(c_1\right) c_2 = \sum_{(c)} \epsilon_1\left(c_2\right) c_1$$

and

$$c = \sum_{(c)} \epsilon_2\left(c_1\right) c_2 = \sum_{(c)} \epsilon_2\left(c_2\right) c_1.$$

Apply ϵ_2 to both sides of the equality $c = \sum_{(c)} \epsilon_1\left(c_2\right) c_1$, and apply ϵ_1 to both sides of the equality $c = \sum_{(c)} \epsilon_2\left(c_1\right) c_2$. Compare the results, and conclude that $\epsilon_1 = \epsilon_2$.

Hint to Exercise 1.3.4. Part (a) is well-known, and part (b) is dual to part (a). So the trick is (again) to rewrite the classical proof of part (a) in an "element-free" way, and then "reversing all arrows". Alternatively, part (b) can be solved using Sweedler notation.

Hint to Exercise 1.3.6. Same method as for Exercise 1.3.4 above.

Hint to Exercise 1.3.13. (a) Use the following fact from linear algebra: If U, V, U' and V' are four $\mathbf{k}$-modules, and $\phi : U \to U'$ and $\psi : V \to V'$ are two surjective $\mathbf{k}$-linear maps, then the kernel of $\phi \otimes \psi : U \otimes V \to U' \otimes V'$ is

$$\ker\left(\phi \otimes \psi\right) = \left(\ker \phi\right) \otimes V + U \otimes \left(\ker \psi\right).$$

(b) The fact just mentioned also holds if we no longer require ϕ and ψ to be surjective, but instead require $\mathbf{k}$ to be a field.

Hint to Exercise 1.3.18. Let $f : V \to W$ be an invertible graded $\mathbf{k}$-linear map. Let $n \in \mathbb{N}$ and $w \in W_n$. Show that the n-th homogeneous component of $f^{-1}\left(w\right)$ is also a preimage of w under f, and thus must equal $f^{-1}\left(w\right)$. Therefore, $f^{-1}\left(w\right) \in W_n$.

Hint to Exercise 1.3.19. (a) Define the $\mathbf{k}$-linear map $\widetilde{\Delta} : A \to A \otimes A$ by $\widetilde{\Delta}\left(x\right) = \Delta\left(x\right) - \left(x \otimes 1 + 1 \otimes x\right)$. Argue that $\widetilde{\Delta}$ is graded, so its kernel $\ker \widetilde{\Delta}$ is a graded $\mathbf{k}$-submodule of A. But this kernel is precisely $\mathfrak{p}$.

---

[375] Currently only the ones from Chapter 1.

[376] This fact is just the linearization of the known fact that any binary operation has at most one neutral element.

[377] This means rewriting it completely in terms of linear maps rather than elements. For example, instead of talking about $m\left(m\left(a \otimes b\right) \otimes c\right)$ for three elements $a, b, c \in A$, you should talk about the map $m \circ \left(m \otimes \mathrm{id}_A\right) : A \otimes A \otimes A \to A$ (which is, of course, the map that sends each $a \otimes b \otimes c$ to $m\left(m\left(a \otimes b\right) \otimes c\right)$). Instead of computing with elements, you should compute with maps (and commutative diagrams).

(b) The hard part is to show that $\epsilon(\mathfrak{p}) = 0$. To do so, consider any $x \in \mathfrak{p}$, and apply the map $\epsilon \otimes \mathrm{id}$ to both sides of the equality $\Delta(x) = x \otimes 1 + 1 \otimes x$. The result simplifies to $x = \epsilon(x) \cdot 1_A + x$. Thus, $\epsilon(x) \cdot 1_A = 0$. Now apply ϵ to this, thus obtaining $\epsilon(x) = 0$.

Hint to Exercise 1.3.20. (a) This follows from $1_A \in A_0$, which is part of what it means for A to be a graded $\mathbf{k}$-algebra.

(b) Let $\epsilon' : A_0 \to \mathbf{k}$ be the restriction of the map ϵ to A_0. We know that ϵ' is surjective (since $\epsilon'(1_A) = 1_\mathbf{k}$), and that both A_0 and $\mathbf{k}$ are free $\mathbf{k}$-modules of rank 1 (since connectedness of A means $A_0 \cong \mathbf{k}$ as $\mathbf{k}$-modules). It is an an easy exercise in linear algebra to conclude from these facts that ϵ' is an isomorphism. Since $\epsilon' \circ u = \mathrm{id}_\mathbf{k}$, we thus conclude that $u : \mathbf{k} \to A_0$ is an isomorphism as well (from $\mathbf{k}$ to A_0).

(c) This follows from part (b).

(e) This follows from how we solved part (b).

(d) Since the bialgebra A is graded, the map ϵ must be graded. Thus, for each positive integer n, we have $\epsilon(A_n) \subset \mathbf{k}_n = 0$. This quickly yields $\epsilon(I) = 0$ (where $I = \bigoplus_{n>0} A_n$), hence $I \subset \ker\epsilon$. On the other hand, $\ker\epsilon \subset I$ can be shown as follows: Let $a \in \ker\epsilon$; write a in the form $a = a' + a''$ for some $a' \in A_0$ and some $a'' \in I$, and then argue that $0 = \epsilon(a) = \epsilon(a' + a'') = \epsilon(a') + \underbrace{\epsilon(a'')}_{\substack{=0 \\ (\text{since } a'' \in I \subset \ker\epsilon)}} = \epsilon(a')$, so that $a' = 0$ by part (e) and therefore $a \in I$.

(f) This is most intuitive with Sweedler notation: Let $x \in A$. Then, $\Delta(x) = \sum_{(x)} x_1 \otimes x_2$. Applying $\mathrm{id} \otimes \epsilon$ and recalling the commutativity of (1.2.2), we thus get $x = \sum_{(x)} \epsilon(x_2)\, x_1$. Thus,

$$\underbrace{\Delta(x)}_{=\sum_{(x)} x_1 \otimes x_2} - \underbrace{x}_{=\sum_{(x)} \epsilon(x_2) x_1} \otimes 1 = \sum_{(x)} x_1 \otimes x_2 - \sum_{(x)} \epsilon(x_2)\, x_1 \otimes 1$$
$$= \sum_{(x)} \underbrace{x_1}_{\in A} \otimes \underbrace{(x_2 - \epsilon(x_2) \cdot 1)}_{\substack{\in \ker\epsilon = I \\ (\text{by part (d)})}} \in A \otimes I.$$

(g) Let $x \in I$. Proceeding similarly to part (f), show that

$$\Delta(x) - 1 \otimes x - x \otimes 1 + \epsilon(x)\, 1 \otimes 1 = \sum_{(x)} \underbrace{(x_1 - \epsilon(x_1) \cdot 1)}_{\substack{\in \ker\epsilon = I \\ (\text{by part (d)})}} \otimes \underbrace{(x_2 - \epsilon(x_2) \cdot 1)}_{\substack{\in \ker\epsilon = I \\ (\text{by part (d)})}} \in I \otimes I.$$

Since $x \in I = \ker\epsilon$, the $\epsilon(x)\, 1 \otimes 1$ term on the left hand side vanishes.

(h) This follows from part (g), since a simple homogeneity argument shows that $(I \otimes I)_n = \sum_{k=1}^{n-1} A_k \otimes A_{n-k}$.

Hint to Exercise 1.3.24. We need to check the four equalities $D_q \circ m = m \circ (D_q \otimes D_q)$ and $D_q \circ u = u$ and $(D_q \otimes D_q) \circ \Delta = \Delta \circ D_q$ and $\epsilon \circ D_q = \epsilon$. This can easily be done by hand (just check everything on homogeneous elements); a more erudite proof proceeds as follows: Generalize the map D_q to a map $D_{q,V} : V \to V$ defined (in the same way as D_q) for every graded $\mathbf{k}$-module V, and show that these maps $D_{q,V}$ are functorial (i.e., if $f : V \to W$ is a graded $\mathbf{k}$-linear map between two graded $\mathbf{k}$-modules V and W, then $D_{q,W} \circ f = f \circ D_{q,V}$) and "respect tensor products" (i.e., we have $D_{q,V \otimes W} = D_{q,V} \otimes D_{q,W}$ for any two graded $\mathbf{k}$-modules V and W). The four equalities are then easily obtained from these two facts, without having to introduce elements.

Hint to Exercise 1.3.26. (a) Our definition of the $\mathbf{k}$-coalgebra $A \otimes B$ yields

$$\Delta_{A \otimes B} = (\mathrm{id}_A \otimes T_{A,B} \otimes \mathrm{id}_B) \circ (\Delta_A \otimes \Delta_B) \qquad \text{and} \qquad \epsilon_{A \otimes B} = \theta \circ (\epsilon_A \otimes \epsilon_B),$$

where θ is the canonical $\mathbf{k}$-module isomorphism $\mathbf{k} \otimes \mathbf{k} \to \mathbf{k}$. All maps on the right hand sides are $\mathbf{k}$-algebra homomorphisms (see Exercise 1.3.6(a)); thus, so are $\Delta_{A \otimes B}$ and $\epsilon_{A \otimes B}$.

(b) Straightforward.

Hint to Exercise 1.4.2. Simple computation (either element-free or with Sweedler notation).

Hint to Exercise 1.4.4. Simple computation (either element-free or with Sweedler notation).

Hint to Exercise 1.4.5. Straightforward computation, best done using Sweedler notation.

Hint to Exercise 1.4.15. Use Exercise 1.4.2.

Hint to Exercise 1.4.19. The following is more context than hint (see the last paragraph for an actual hint).

It is easiest to prove this by calculating with elements. To wit, in order to prove that two $\mathbf{k}$-linear maps from $A^{\otimes(k+1)}$ are identical, it suffices to show that they agree on all pure tensors $a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1} \in A^{\otimes(k+1)}$. But the recursive definition of $m^{(k)}$ shows that

$$m^{(k)}\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right) = a_1\left(a_2\left(a_3\left(\cdots\left(a_k a_{k+1}\right)\cdots\right)\right)\right) \tag{12.1.1}$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$. Now, the "general associativity" law (a fundamental result in abstract algebra, commonly used without mention) says that, because the multiplication of A is associative, the parentheses in the product $a_1\left(a_2\left(a_3\left(\cdots\left(a_k a_{k+1}\right)\cdots\right)\right)\right)$ can be omitted without making it ambiguous – i.e., any two ways of parenthesizing the product $a_1 a_2 \cdots a_{k+1}$ evaluate to the same result. (For example, for $k = 4$, this says that

$$a_1\left(a_2\left(a_3 a_4\right)\right) = a_1\left(\left(a_2 a_3\right) a_4\right) = \left(a_1 a_2\right)\left(a_3 a_4\right) = \left(a_1\left(a_2 a_3\right)\right) a_4 = \left(\left(a_1 a_2\right) a_3\right) a_4$$

for all $a_1, a_2, a_3, a_4 \in A$.) Thus, we can rewrite (12.1.1) as

$$m^{(k)}\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right) = a_1 a_2 \cdots a_{k+1}.$$

Using this formula, all four parts of the exercise become trivial: For example, part (a) simply says that

$$a_1 a_2 \cdots a_{k+1} = \left(a_1 a_2 \cdots a_{i+1}\right)\left(a_{i+2} a_{i+3} \cdots a_{k+1}\right)$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$, because we have

$$\left(m \circ \left(m^{(i)} \otimes m^{(k-1-i)}\right)\right)\left(a_1 \otimes a_2 \otimes \cdots \otimes a_{k+1}\right) = \left(a_1 a_2 \cdots a_{i+1}\right)\left(a_{i+2} a_{i+3} \cdots a_{k+1}\right).$$

Likewise, part (c) simply says that

$$a_1 a_2 \cdots a_{k+1} = a_1 a_2 \cdots a_i\left(a_{i+1} a_{i+2}\right) a_{i+3} a_{i+4} \cdots a_{k+1}$$

for all $a_1, a_2, \ldots, a_{k+1} \in A$. Parts (b) and (d) are particular cases of parts (a) and (c), respectively.

Of course, in order for this to be a complete solution, you have to prove the "general associativity" law used above. It turns out that doing so is not much easier than solving the exercise from scratch (in fact, part (a) of the exercise is an equivalent form of the "general associativity" law). So we can just as well start from scratch and solve part (a) directly by induction on k, then derive part (b) as its particular case, then solve part (c) by induction on k using the result of part (b), then derive part (d) as a particular case of (c).

Hint to Exercise 1.4.20. If you have solved Exercise 1.4.19 in an "element-free" way, then you can reverse all arrows in said solution and thus obtain a solution to Exercise 1.4.20.

Hint to Exercise 1.4.22. (a) Induction on k, using Exercise 1.3.6(b).

(b) This is dual to (a).

(d) For every $\mathbf{k}$-coalgebra C, consider the map $\Delta_C^{(k)} : C \to C^{\otimes(k+1)}$ (this is the map $\Delta^{(k)}$ defined in Exercise 1.4.20). This map $\Delta_C^{(k)}$ is clearly functorial in C. By this we mean that if C and D are any two $\mathbf{k}$-coalgebras, and $f : C \to D$ is any $\mathbf{k}$-coalgebra homomorphism, then the diagram

$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ \downarrow{\scriptstyle \Delta_C^{(k)}} & & \downarrow{\scriptstyle \Delta_D^{(k)}} \\ C^{\otimes(k+1)} & \xrightarrow[f^{\otimes(k+1)}]{} & D^{\otimes(k+1)} \end{array}$$

commutes. Now, apply this to $C = H^{\otimes(\ell+1)}$, $D = H$ and $f = m_H^{(\ell)}$ (using part (a)).

(c) This is dual to (d).

Hint to Exercise 1.4.23. Induction on k.

Hint to Exercise 1.4.28. This is dual to Proposition 1.4.10, so the usual strategy (viz., rewriting element-free and reversing all arrows) applies.

Hint to Exercise 1.4.29. (a) A straightforward generalization of the proof of Proposition 1.4.10 (which corresponds to the particular case when $C = A$ and $r = \mathrm{id}$) does the trick.

(b) This is dual to (a).

(c) Easy.

(d) Apply Exercise 1.4.29(a) to $C = A$ and $r = \mathrm{id}_A$; then, apply Proposition 1.4.26(a) to $H = A$ and $\alpha = S$.

(e) Let $s : C \to A$ be the $\mathbf{k}$-linear map that sends every homogeneous element $c \in C_n$ (for every $n \in \mathbb{N}$) to the n-th homogeneous component of $r^{\star(-1)}(c)$. Then, s is graded, and (this takes some work) is also a $\star$-inverse to r. But r has only one $\star$-inverse.

Hint to Exercise 1.4.30. (a) Rewrite the assumption as $m \circ (P \otimes \mathrm{id}) \circ T \circ \Delta = u \circ \epsilon$, where T is the twist map $T_{A,A}$. Proposition 1.4.10 leads to $m \circ (S \otimes S) = S \circ m \circ T$ and $u = S \circ u$. Exercise 1.4.28 leads to $(S \otimes S) \circ \Delta = T \circ \Delta \circ S$ and $\epsilon \circ S = \epsilon$. Use these to show that $(P \circ S) \star S = u \circ \epsilon$, so that $P \circ S = \mathrm{id}$. Also, show that $S \star (S \circ P) = u \circ \epsilon$, so that $S \circ P = \mathrm{id}$.

(b) Similar to (a).

(c) Let A be a connected graded Hopf algebra. Just as a left $\star$-inverse S to id_A has been constructed in the proof of Proposition 1.4.16, we could construct a $\mathbf{k}$-linear map $P : A \to A$ such that every $a \in A$ satisfies $\sum_{(a)} P(a_2) \cdot a_1 = u(\epsilon(a))$. Now apply part (a).

Hint to Exercise 1.4.32. Since D is a direct summand of C, we can identify the tensor products $D \otimes C$, $C \otimes D$ and $D \otimes D$ with their canonical images inside $C \otimes C$. Now, we can show that $\Delta(D) \subset D \otimes D$ as follows: Let $p : C \to D$ be the canonical projection from C onto its direct summand D; then, $\Delta(D) \subset D \otimes C$ shows that $(p \otimes \mathrm{id}) \circ \Delta = \Delta$, and $\Delta(D) \subset C \otimes D$ shows that $(\mathrm{id} \otimes p) \circ \Delta = \Delta$. Hence,

$$\underbrace{(p \otimes p)}_{=(p \otimes \mathrm{id}) \circ (\mathrm{id} \otimes p)} \circ \Delta = (p \otimes \mathrm{id}) \circ \underbrace{(\mathrm{id} \otimes p) \circ \Delta}_{=\Delta} = (p \otimes \mathrm{id}) \circ \Delta = \Delta.$$

This yields $\Delta(D) \subset D \otimes D$. Hence, we get a map $\Delta_D : D \to D \otimes D$ by restricting Δ. Obviously, the map $\epsilon : C \to \mathbf{k}$ restricts to a map $\epsilon_D : D \to \mathbf{k}$ as well. It remains to check the commutativity of the diagrams (1.2.1) and (1.2.2) for D instead of C; but this is inherited from C.

Hint to Exercise 1.4.33. (a) Let $\widetilde{f} = (\mathrm{id}_C \otimes f \otimes \mathrm{id}_C) \circ \Delta^{(2)} : C \to C \otimes U \otimes C$; then, $K = \ker \widetilde{f}$. Show (by manipulation of maps, using Exercise 1.4.20(b)) that $(\mathrm{id}_C \otimes \mathrm{id}_U \otimes \Delta) \circ \widetilde{f} = \left(\widetilde{f} \otimes \mathrm{id}_C\right) \circ \Delta$. Now,

$$K = \ker \widetilde{f} \subset \ker \left(\underbrace{(\mathrm{id}_C \otimes \mathrm{id}_U \otimes \Delta) \circ \widetilde{f}}_{=\left(\widetilde{f} \otimes \mathrm{id}_C\right) \circ \Delta} \right) = \ker \left(\left(\widetilde{f} \otimes \mathrm{id}_C\right) \circ \Delta \right) = \Delta^{-1} \left(\ker \left(\widetilde{f} \otimes \mathrm{id}_C\right) \right)$$

and therefore

$$\Delta(K) \subset \ker \left(\widetilde{f} \otimes \mathrm{id}_C\right) = \underbrace{\left(\ker \widetilde{f}\right)}_{=K} \otimes C \qquad \text{(since tensoring over a field is left-exact)}$$
$$= K \otimes C.$$

Similarly, $\Delta(K) \subset C \otimes K$. Now, apply Exercise 1.4.32 to $D = K$.

(b) Let E be a $\mathbf{k}$-subcoalgebra of C which is a subset of $\ker f$. Then, $\Delta^{(2)}(E) \subset E \otimes E \otimes E$ (since E is a subcoalgebra) and $f(E) = 0$ (since $E \subset \ker f$). Now,

$$\begin{aligned}\left(\left(\mathrm{id}_C \otimes f \otimes \mathrm{id}_C\right) \circ \Delta^{(2)}\right)(E) &= \left(\mathrm{id}_C \otimes f \otimes \mathrm{id}_C\right)\left(\underbrace{\Delta^{(2)}(E)}_{\subset E\otimes E\otimes E}\right) \\ &\subset \left(\mathrm{id}_C \otimes f \otimes \mathrm{id}_C\right)(E \otimes E \otimes E) \\ &= \mathrm{id}_C(E) \otimes \underbrace{f(E)}_{=0} \otimes \mathrm{id}_C(E) = 0.\end{aligned}$$

Hence, $E \subset \ker\left(\left(\mathrm{id}_C \otimes f \otimes \mathrm{id}_C\right) \circ \Delta^{(2)}\right) = K$.

[*Remark:* Exercise 1.4.33(a) would not hold if we allowed $\mathbf{k}$ to be an arbitrary commutative ring rather than a field.]

Hint to Exercise 1.4.34. (a) Here is Takeuchi's argument: We know that the map $h|_{C_0} \in \mathrm{Hom}(C_0, A)$ is $\star$-invertible; let $\widetilde{g}$ be its $\star$-inverse. Extend $\widetilde{g}$ to a $\mathbf{k}$-linear map $g : C \to A$ by defining it as 0 on every C_n for $n > 0$. It is then easy to see that $(h \star g)|_{C_0} = (g \star h)|_{C_0} = (u\epsilon)|_{C_0}$. This allows us to assume WLOG that $h|_{C_0} = (u\epsilon)|_{C_0}$ (because once we know that $h \star g$ and $g \star h$ are $\star$-invertible, it follows that so is h). Assuming this, we conclude that $h - u\epsilon$ annihilates C_0. Define f as $h - u\epsilon$. Now, we can proceed as in the proof of Proposition 1.4.24 to show that $\sum_{k\geq 0}(-1)^k f^{\star k}$ is a well-defined linear map $C \to A$ and a two-sided $\star$-inverse for h. Thus, h is $\star$-invertible, and part (a) of the exercise is proven. (An alternative proof proceeds by mimicking the proof of Proposition 1.4.16, again by first assuming WLOG that $h|_{C_0} = (u\epsilon)|_{C_0}$.)

(b) Apply part (a) to $C = A$ and the map $\mathrm{id}_A : A \to A$.

(c) Applying part (b), we see that A is a Hopf algebra (since $A_0 = \mathbf{k}$ is a Hopf algebra) in the setting of Proposition 1.4.16. This yields the existence of the antipode. Its uniqueness is trivial, and its gradedness follows from Exercise 1.4.29(e).

Hint to Exercise 1.4.35. (a) Let I be a two-sided coideal of A such that $I \cap \mathfrak{p} = 0$ and such that $I = \bigoplus_{n\geq 0}(I \cap A_n)$. Let $I_n = I \cap A_n$ for every $n \in \mathbb{N}$. Then, $I = \bigoplus_{n\geq 0} I_n$. Since I is a two-sided coideal, we have $\epsilon(I) = 0$.

We want to prove that $I = 0$. It clearly suffices to show that every $n \in \mathbb{N}$ satisfies $I_n = 0$ (since $I = \bigoplus_{n\geq 0} I_n$). We shall show this by strong induction: We fix an $N \in \mathbb{N}$, and we assume (as induction hypothesis) that $I_n = 0$ for all $n < N$. We must prove that $I_N = 0$.

Fix $i \in I_N$; we aim to show that $i = 0$. We have $i \in I_N \subset A_N$ and thus $\Delta(i) \in (A \otimes A)_N$ (since Δ is a graded map). On the other hand, from $i \in I_N \subset I$, we obtain

$$\begin{aligned}\Delta(i) \in \Delta(I) &\subset \underbrace{I}_{=\bigoplus_{n\geq 0} I_n} \otimes \underbrace{A}_{=\bigoplus_{m\geq 0} A_m} + \underbrace{A}_{=\bigoplus_{m\geq 0} A_m} \otimes \underbrace{I}_{=\bigoplus_{n\geq 0} I_n} \qquad \text{(since } I \text{ is a two-sided coideal)} \\ &= \sum_{(m,n)\in\mathbb{N}^2} I_n \otimes A_m + \sum_{(m,n)\in\mathbb{N}^2} A_m \otimes I_n.\end{aligned}$$

Combining this with $\Delta(i) \in (A \otimes A)_N$, we obtain

$$\begin{aligned}\Delta(i) &\in \sum_{\substack{(m,n)\in\mathbb{N}^2;\\ m+n=N}} I_n \otimes A_m + \sum_{\substack{(m,n)\in\mathbb{N}^2;\\ m+n=N}} A_m \otimes I_n \qquad \left(\text{since } I_n \otimes A_m \text{ and } A_m \otimes I_n \text{ are subsets of } (A \otimes A)_{n+m}\right) \\ &= \sum_{n=0}^{N} I_n \otimes A_{N-n} + \sum_{n=0}^{N} A_{N-n} \otimes I_n \\ &= I_N \otimes \underbrace{A_0}_{=\mathbf{k}\cdot 1_A} + \sum_{n=0}^{N-1} \underbrace{I_n}_{\substack{=0\\ \text{(by the induction}\\ \text{hypothesis)}}} \otimes A_{N-n} + \underbrace{A_0}_{=\mathbf{k}\cdot 1_A} \otimes I_N + \sum_{n=0}^{N-1} A_{N-n} \otimes \underbrace{I_n}_{\substack{=0\\ \text{(by the induction}\\ \text{hypothesis)}}} \\ &= I_N \otimes (\mathbf{k} \cdot 1_A) + (\mathbf{k} \cdot 1_A) \otimes I_N.\end{aligned}$$

In other words,

$$\Delta(i) = j \otimes 1_A + 1_A \otimes k \tag{12.1.2}$$

for some $j, k \in I_N$. By applying $\epsilon \otimes \mathrm{id}$ to both sides of this equality, and recalling the commutativity of (1.2.2), we obtain $i = \epsilon(j)\, 1_A + k$. But $\epsilon(j) = 0$ (since $j \in I_N \subset I$, so $\epsilon(j) \in \epsilon(I) = 0$), so this simplifies to $i = k$. Similarly, $i = j$. Hence, (12.1.2) rewrites as $\Delta(i) = i \otimes 1_A + 1_A \otimes i$, which shows that $i \in \mathfrak{p}$, hence $i \in I \cap \mathfrak{p} = 0$ and thus $i = 0$. This was for proved for each $i \in I_N$, so we obtain $I_N = 0$. This completes the induction step, and so part (a) is solved.

(b) Exercise 1.3.13(a) shows that $\ker f$ is a two-sided coideal of C. If $f|_{\mathfrak{p}}$ is injective, then $(\ker f) \cap \mathfrak{p} = 0$. Now, apply part (a) of the current exercise to $I = \ker f$.

(c) Proceed as in part (b), but use Exercise 1.3.13(b) instead of Exercise 1.3.13(a).

Hint to Exercise 1.5.4. (a) Straightforward (if slightly laborious) computations.

(b) Direct verification (the hard part of which has been done in (1.3.7) already).

(c) For every subset S of a $\mathbf{k}$-module U, we let $\langle S \rangle$ denote the $\mathbf{k}$-submodule of U spanned by S. Our definition of J thus becomes

$$J = T(\mathfrak{p}) \cdot C \cdot T(\mathfrak{p}), \tag{12.1.3}$$

where $C = \langle xy - yx - [x, y] \mid x, y \in \mathfrak{p} \rangle$. A simple computation shows that each element of C is primitive. Hence,

$$\Delta(C) \subset C \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes C.$$

Applying Δ to both sides of (12.1.3), and recalling that Δ is a $\mathbf{k}$-algebra homomorphism, we find

$$\begin{aligned}
\Delta(J) &= \underbrace{\Delta(T(\mathfrak{p}))}_{\subset T(\mathfrak{p}) \otimes T(\mathfrak{p})} \cdot \underbrace{\Delta(C)}_{\subset C \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes C} \cdot \underbrace{\Delta(T(\mathfrak{p}))}_{\subset T(\mathfrak{p}) \otimes T(\mathfrak{p})} \\
&\subset (T(\mathfrak{p}) \otimes T(\mathfrak{p})) \cdot (C \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes C) \cdot (T(\mathfrak{p}) \otimes T(\mathfrak{p})) \\
&= J \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes J.
\end{aligned}$$

A similar (but simpler) argument shows $\epsilon(J) = 0$. Thus, J is a two-sided coideal of $T(\mathfrak{p})$. This yields that $T(\mathfrak{p})/J$ is a $\mathbf{k}$-bialgebra.

(d) We need to show that $S(J) \subset J$. This can be done in a similar way as we proved $\Delta(J) \subset J \otimes T(\mathfrak{p}) + T(\mathfrak{p}) \otimes J$ in part (c), once you know (from Proposition 1.4.10) that the antipode S of $T(\mathfrak{p})$ is a $\mathbf{k}$-algebra anti-homomorphism.

Hint to Exercise 1.5.5. Straightforward and easy verification.

Hint to Exercise 1.5.6. Straightforward and easy verification. Parts (a) and (b) are dual, of course.

Hint to Exercise 1.5.8. (a) Straightforward and easy verification.

(b) The dual says the following: Let A and B be two $\mathbf{k}$-coalgebras, at least one of which is cocommutative. Prove that the $\mathbf{k}$-coalgebra anti-homomorphisms from A to B are the same as the $\mathbf{k}$-coalgebra homomorphisms from A to B.

Hint to Exercise 1.5.9. For every $1 \leq i < j \leq k$, let $t_{i,j}$ be the transposition in $\mathfrak{S}_k$ which transposes i with j. It is well-known that the symmetric group $\mathfrak{S}_k$ is generated by the transpositions $t_{i,i+1}$ with i ranging over $\{1, 2, \ldots, k-1\}$. However, we have $(\rho(\pi)) \circ (\rho(\psi)) = \rho(\pi\psi)$ for any two elements π and ψ of $\mathfrak{S}_k$. Thus, it suffices to check that

$$m^{(k-1)} \circ (\rho(t_{i,i+1})) = m^{(k-1)} \qquad \text{for all } i \in \{1, 2, \ldots, k-1\}.$$

But this is not hard to check using $m^{(k-1)} = m^{(k-2)} \circ (\mathrm{id}_{A^{\otimes(i-1)}} \otimes m \otimes \mathrm{id}_{A^{\otimes(k-1-i)}})$ (a consequence of Exercise 1.4.19(c)) and $m \circ T = m$.

Hint to Exercise 1.5.10. Here is the dual statement: Let C be a cocommutative $\mathbf{k}$-coalgebra, and let $k \in \mathbb{N}$. The symmetric group $\mathfrak{S}_k$ acts on the k-fold tensor power $C^{\otimes k}$ by permuting the tensor factors: $\sigma(v_1 \otimes v_2 \otimes \cdots \otimes v_k) = v_{\sigma^{-1}(1)} \otimes v_{\sigma^{-1}(2)} \otimes \cdots \otimes v_{\sigma^{-1}(k)}$ for all $v_1, v_2, \ldots, v_k \in C$ and $\sigma \in \mathfrak{S}_k$. For every $\pi \in \mathfrak{S}_k$, denote by $\rho(\pi)$ the action of π on $C^{\otimes k}$ (this is an endomorphism of $C^{\otimes k}$). Show that every $\pi \in \mathfrak{S}_k$

satisfies $(\rho(\pi)) \circ \Delta^{(k-1)} = \Delta^{(k-1)}$. (Recall that $\Delta^{(k-1)} : C \to C^{\otimes k}$ is defined as in Exercise 1.4.20 for $k \geq 1$, and by $\Delta^{(-1)} = \epsilon : C \to \mathbf{k}$ for $k = 0$.)

Hint to Exercise 1.5.11. (a) Use Exercise 1.5.6(b) and Exercise 1.3.6(a) to represent $f \star g$ as a composition of three $\mathbf{k}$-algebra homomorphisms.

(b) Induction on k, using part (a).

(c) Use Proposition 1.4.10, Proposition 1.4.26(a) and the easy fact that a composition of a $\mathbf{k}$-algebra homomorphism with a $\mathbf{k}$-algebra anti-homomorphism (in either order) always is a $\mathbf{k}$-algebra anti-homomorphism.

(d) Use Exercise 1.5.6(b). Then, proceed by induction on k as in the solution of Exercise 1.4.22(a).

(e) Use Proposition 1.4.3.

(f) Let H be a commutative $\mathbf{k}$-bialgebra. Let k and ℓ be two nonnegative integers. Then, Exercise 1.5.11(b) (applied to $A = H$ and $f_i = \mathrm{id}_H$) yields that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism $H \to H$. Now, apply Exercise 1.5.11(e) to H, H, H, H, ℓ, id_H, $\mathrm{id}_H^{\star k}$ and id_H instead of C, C', A, A', k, f_i, α and γ.

(g) This is an exercise in bootstrapping. First, let $k \in \mathbb{N}$. Then, part (b) of this exercise shows that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism. Use this together with part (c) to conclude that $\mathrm{id}_H^{\star k} \circ S$ is again a $\mathbf{k}$-algebra homomorphism and a $\star$-inverse to $\mathrm{id}_H^{\star k}$; thus, $\mathrm{id}_H^{\star k} \circ S = \left(\mathrm{id}_H^{\star k}\right)^{\star(-1)} = \mathrm{id}_H^{\star(-k)}$, and this map $\mathrm{id}_H^{\star(-k)}$ is a $\mathbf{k}$-algebra homomorphism.

Now forget that we fixed k. We thus have shown that $\mathrm{id}_H^{\star k}$ and $\mathrm{id}_H^{\star(-k)}$ are $\mathbf{k}$-algebra homomorphisms for each $k \in \mathbb{N}$. In other words,

$$\mathrm{id}_H^{\star k} \text{ is a } \mathbf{k}\text{-algebra homomorphism} \qquad \text{for every } k \in \mathbb{Z}. \tag{12.1.4}$$

Furthermore, we have proved the equality $\mathrm{id}_H^{\star k} \circ S = \mathrm{id}_H^{\star(-k)}$ for each $k \in \mathbb{N}$. Repeating the proof of this, but now taking $k \in \mathbb{Z}$ instead of $k \in \mathbb{N}$, we conclude that it also holds for each $k \in \mathbb{Z}$ (since we already have proved (12.1.4)). In other words,

$$\mathrm{id}_H^{\star(-k)} = \mathrm{id}_H^{\star k} \circ S \qquad \text{for every } k \in \mathbb{Z}. \tag{12.1.5}$$

Now, fix two integers k and ℓ. From (12.1.4), we know that $\mathrm{id}_H^{\star k}$ is a $\mathbf{k}$-algebra homomorphism. Hence, if ℓ is nonnegative, then we can prove $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star(k\ell)}$ just as we did in the solution to Exercise 1.5.11(f). But the case when ℓ is negative can be reduced to the previous case by applying (12.1.5) (once to $-\ell$ instead of k, and once again to $-k\ell$ instead of k). Thus, in each case, we obtain $\mathrm{id}_H^{\star k} \circ \mathrm{id}_H^{\star \ell} = \mathrm{id}_H^{\star(k\ell)}$.

(h) The dual of Exercise 1.5.11(a) is the following exercise:

> If H is a $\mathbf{k}$-bialgebra and C is a cocommutative $\mathbf{k}$-coalgebra, and if f and g are two $\mathbf{k}$-coalgebra homomorphisms $C \to H$, then prove that $f \star g$ also is a $\mathbf{k}$-coalgebra homomorphism $C \to H$.

The dual of Exercise 1.5.11(b) is the following exercise:

> If H is a $\mathbf{k}$-bialgebra and C is a cocommutative $\mathbf{k}$-coalgebra, and if $f_1, f_2, \ldots, f_k$ are several $\mathbf{k}$-coalgebra homomorphisms $C \to H$, then prove that $f_1 \star f_2 \star \cdots \star f_k$ also is a $\mathbf{k}$-coalgebra homomorphism $C \to H$.

The dual of Exercise 1.5.11(c) is the following exercise:

> If H is a Hopf algebra and C is a cocommutative $\mathbf{k}$-coalgebra, and if $f : C \to H$ is a $\mathbf{k}$-coalgebra homomorphism, then prove that $S \circ f : C \to H$ (where S is the antipode of H) is again a $\mathbf{k}$-coalgebra homomorphism, and is a $\star$-inverse to f.

The dual of Exercise 1.5.11(d) is the following exercise:

> If C is a cocommutative $\mathbf{k}$-coalgebra, then show that $\Delta^{(k)}$ is a $\mathbf{k}$-coalgebra homomorphism for every $k \in \mathbb{N}$. (The map $\Delta^{(k)} : C \to C^{\otimes(k+1)}$ is defined as in Exercise 1.4.20.)

The dual of Exercise 1.5.11(e) is Exercise 1.5.11(e) itself (up to renaming objects and maps).

The dual of Exercise 1.5.11(f) is the following exercise:

> If H is a cocommutative $\mathbf{k}$-bialgebra, and k and ℓ are two nonnegative integers, then prove that $\mathrm{id}_H^{\star \ell} \circ \mathrm{id}_H^{\star k} = \mathrm{id}_H^{\star(\ell k)}$.

The dual of Exercise 1.5.11(g) is the following exercise:

If H is a cocommutative $\mathbf{k}$-Hopf algebra, and k and ℓ are two integers, then prove that $\mathrm{id}_H^{\star\ell} \circ \mathrm{id}_H^{\star k} = \mathrm{id}_H^{\star(\ell k)}$.

Hint to Exercise 1.5.13. This is dual to Corollary 1.4.12 (but can also easily be shown using Exercise 1.4.29(b), Exercise 1.5.8(b) and Proposition 1.4.26(b)).

Hint to Exercise 1.5.14. (a) This can be proved computationally (using Sweedler notation), but there is a nicer argument as well:

A *coderivation* of a $\mathbf{k}$-coalgebra (C, Δ, ϵ) is defined as a $\mathbf{k}$-linear map $F : C \to C$ such that $\Delta \circ F = (F \otimes \mathrm{id} + \mathrm{id} \otimes F) \circ \Delta$. (The reader can check that this axiom is the result of writing the axiom for a derivation in element-free terms and reversing all arrows. Nothing less should be expected.) It is easy to see that E is a coderivation. Hence, it will be enough to check that $(S \star f)(a)$ and $(f \star S)(a)$ are primitive whenever $f : A \to A$ is a coderivation and $a \in A$. So fix a coderivation $f : A \to A$. Notice that the antipode S of A is a coalgebra anti-endomorphism (by Exercise 1.4.28), thus a coalgebra endomorphism (by Exercise 1.5.8(b)). Thus, $\Delta \circ S = (S \otimes S) \circ \Delta$. Moreover, $\Delta : A \to A \otimes A$ is a coalgebra homomorphism (by Exercise 1.5.6(a)) and an algebra homomorphism (since A is a bialgebra). Applying (1.4.2) to $A \otimes A$, A, A, Δ, id_A, S and f instead of A', C, C', α, γ, f and g, we obtain

$$\begin{aligned}
\Delta \circ (S \star f) &= \underbrace{(\Delta \circ S)}_{=(S\otimes S)\circ\Delta} \star \underbrace{(\Delta \circ f)}_{\substack{=(f\otimes\mathrm{id}+\mathrm{id}\otimes f)\circ\Delta \\ \text{(since } f \text{ is a coderivation)}}} \\
&= ((S \otimes S) \circ \Delta) \star ((f \otimes \mathrm{id} + \mathrm{id} \otimes f) \circ \Delta) = ((S \otimes S) \star (f \otimes \mathrm{id} + \mathrm{id} \otimes f)) \circ \Delta \\
&= \underbrace{((S \otimes S) \star (f \otimes \mathrm{id}))}_{\substack{=(S\star f)\otimes(S\star\mathrm{id}) \\ \text{(by Exercise 1.4.4(a))}}} \circ \Delta + \underbrace{((S \otimes S) \star (\mathrm{id} \otimes f))}_{\substack{=(S\star\mathrm{id})\otimes(S\star f) \\ \text{(by Exercise 1.4.4(a))}}} \circ \Delta \\
&= \left((S \star f) \otimes \underbrace{(S \star \mathrm{id})}_{=u\epsilon} \right) \circ \Delta + \left(\underbrace{(S \star \mathrm{id})}_{=u\epsilon} \otimes (S \star f) \right) \circ \Delta \\
&= ((S \star f) \otimes u\epsilon) \circ \Delta + (u\epsilon \otimes (S \star f)) \circ \Delta.
\end{aligned}$$

Hence, every $a \in A$ satisfies

$$\begin{aligned}
(\Delta \circ (S \star f))(a) &= (((S \star f) \otimes u\epsilon) \circ \Delta + (u\epsilon \otimes (S \star f)) \circ \Delta)(a) \\
&= (S \star f)(a) \otimes 1 + 1 \otimes (S \star f)(a)
\end{aligned}$$

(after some brief computations using (1.2.2)). In other words, for every $a \in A$, the element $(S \star f)(a)$ is primitive. Similarly the same can be shown for $(f \star S)(a)$, and so we are done.

(b) is a very simple computation. (Alternatively, the $(S \star E)(p) = E(p)$ part follows from applying part (c) to $a = 1$, and similarly one can show $(E \star S)(p) = E(p)$.)

(c) This is another computation, using Proposition 1.4.17 and the (easy) observation that E is a derivation of the algebra A.

(d) Assume that the graded algebra $A = \bigoplus_{n \geq 0} A_n$ is connected and that $\mathbb{Q}$ is a subring of $\mathbf{k}$. Let B be the $\mathbf{k}$-subalgebra of A generated by $\mathfrak{p}$. In order to prove part (d), we need to show that $A \subset B$. Clearly, it suffices to show that $A_n \subset B$ for every $n \in \mathbb{N}$. We prove this by strong induction on n; thus, we fix some $n \in \mathbb{N}$, and assume as induction hypothesis that $A_m \subset B$ for every $m < n$. Our goal is then to show that $A_n \subset B$. This being trivial for $n = 0$ (since A is connected), we WLOG assume that $n > 0$. Let $a \in A_n$. Part (a) of this exercise yields $(S \star E)(a) \in \mathfrak{p} \subset B$. On the other hand, Exercise 1.3.20(h) (applied to $x = a$) yields

$$\Delta(a) \in 1 \otimes a + a \otimes 1 + \sum_{k=1}^{n-1} A_k \otimes A_{n-k}.$$

Hence, from the definition of convolution, we obtain

$$(S \star E)(a) \in \underbrace{S(1)}_{=1} E(a) + S(a) \underbrace{E(1)}_{=0} + \underbrace{(m \circ (S \otimes E)) \left(\sum_{k=1}^{n-1} A_k \otimes A_{n-k} \right)}_{= \sum_{k=1}^{n-1} S(A_k) E(A_{n-k})}$$

$$= E(a) + \sum_{k=1}^{n-1} \underbrace{S(A_k)}_{\subset A_k} \underbrace{E(A_{n-k})}_{\subset A_{n-k} \subset B} \subset E(a) + \sum_{k=1}^{n-1} \underbrace{A_k}_{\subset B} \qquad B \subset E(a) + B$$

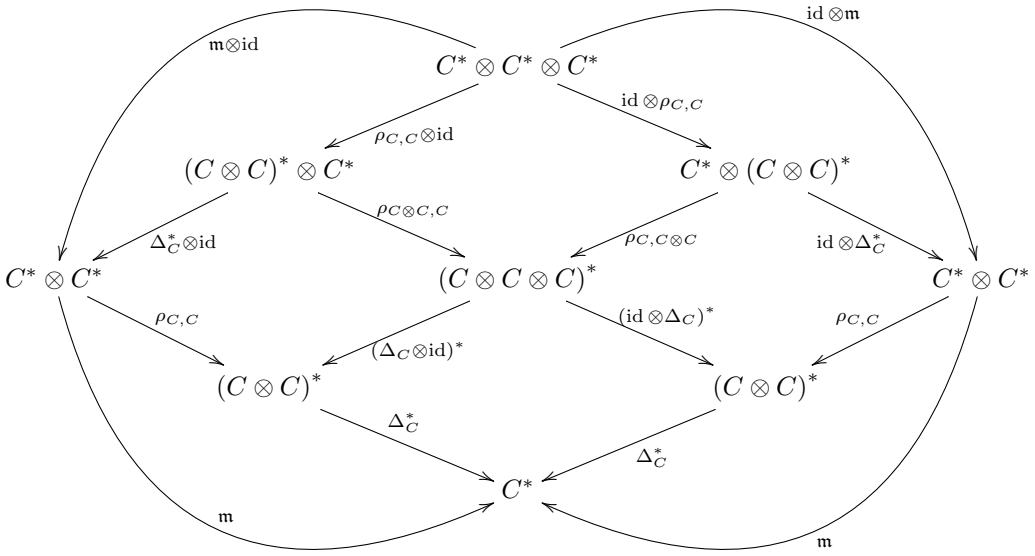
(since S is graded) (by the induction hypothesis) (by the induction hypothesis)

(since B is a subalgebra). Hence, $E(a) \in (S \star E)(a) + B = B$ (since $(S \star E)(a) \in B$). Since $E(a) = na$, this becomes $na \in B$, thus $a \in B$ (since $\mathbb{Q}$ is a subring of $\mathbf{k}$). Since we have shown this for each $a \in A_n$, we thus obtain $A_n \subset B$, and our induction is complete.

This solution of part (d) is not the most generalizable one – for instance, (d) also holds if A is connected filtered instead of connected graded, and then a different argument is necessary. This is a part of the Cartier-Milnor-Moore theorem, and appears e.g. in [60, §3.2].

(e) If $a \in T(V)$ is homogeneous of positive degree and $p \in V$, then part (c) quickly yields $(S \star E)(ap) = [(S \star E)(a), p]$. This allows proving (e) by induction over n, with the induction base $n = 1$ being a consequence of part (b).

Hint to Exercise 1.6.1. (a) This can be done by diagram chasing. For example, if $\mathfrak{m}$ denotes the map $\Delta_C^* \circ \rho_{C,C} : C^* \otimes C^* \to C^*$, then the diagram



is commutative (since each of its little triangles and squares is); thus, $\mathfrak{m} \circ (\mathfrak{m} \otimes \mathrm{id}) = \mathfrak{m} \circ (\mathrm{id} \otimes \mathfrak{m})$ for $\mathfrak{m}$. This proves that the diagram (1.1.1) commutes for our algebra C^*. The commutativity of (1.1.2) is obtained similarly.

Alternatively, we could also solve part (a) trivially by first solving part (b) and then recalling Exercise 1.4.2.

(b) Straightforward verification on pure tensors.

(c) Let $C = \bigoplus_{n \geq 0} C_n$ be a graded $\mathbf{k}$-coalgebra. For every $n \in \mathbb{N}$, we identify $(C_n)^*$ with a $\mathbf{k}$-submodule of C^*, namely with the $\mathbf{k}$-submodule $\{f \in C^* \mid f(C_p) = 0 \text{ for all } p \in \mathbb{N} \text{ satisfying } p \neq n\}$. By the definition of C^o, we have $C^o = \bigoplus_{n \geq 0} (C_n)^*$. Hence, it remains to show that $(C_a)^* (C_b)^* \subset (C_{a+b})^*$ for all $a, b \in \mathbb{N}$, and that $1_{C^*} \in (C_0)^*$. But this is straightforward using the gradedness of Δ and ϵ.

(d) Diagram chasing or simple element-wise verification.

(e) Simple linear algebra (no Hopf algebras involved here).

(f) The "only if" direction is proved in the same way as part (d) (or as a corollary of part (d), since D° and C° are subalgebras of D^* and C^*). It remains to prove the "if" direction.

Assume that $f^* : D^o \to C^o$ is a $\mathbf{k}$-algebra morphism. We want to show that $f : C \to D$ is a $\mathbf{k}$-coalgebra morphism. In other words, we want to show that the two diagrams

(12.1.6)
$$\begin{array}{ccc} C & \xrightarrow{f} & D \\ {\scriptstyle \Delta_C}\downarrow & & \downarrow{\scriptstyle \Delta_D} \\ C \otimes C & \xrightarrow{f \otimes f} & D \otimes D \end{array} \qquad \text{and} \qquad \begin{array}{ccc} C & \xrightarrow{f} & D \\ & {\scriptstyle \epsilon_C}\searrow \quad \swarrow{\scriptstyle \epsilon_D} & \\ & \mathbf{k} & \end{array}$$

commute. Let us start with the left one of these diagrams. The graded $\mathbf{k}$-module D is of finite type, and therefore the map $\rho_{D,D} : D^o \otimes D^o \to (D \otimes D)^o$ (a restriction of the map $\rho_{D,D} : D^* \otimes D^* \to (D \otimes D)^*$) is an isomorphism. Its inverse $\rho_{D,D}^{-1} : (D \otimes D)^o \to D^o \otimes D^o$ is therefore well-defined[378]. We can thus form the (asymmetric!) diagram

(12.1.7)
$$\begin{array}{ccccc} D^o & & \xrightarrow{\quad f^* \quad} & & C^o \\ {\scriptstyle \Delta_D^*}\uparrow & {\scriptstyle m_{D^*}}\nwarrow & & {\scriptstyle m_{C^*}}\nearrow & \uparrow{\scriptstyle \Delta_C^*} \\ & & D^o \otimes D^o \xrightarrow{f^* \otimes f^*} C^o \otimes C^o & & \\ & {\scriptstyle \rho_{D,D}^{-1}}\nearrow & & \searrow{\scriptstyle \rho_{C,C}} & \\ (D \otimes D)^o & & \xrightarrow[(f \otimes f)^*]{} & & (C \otimes C)^o \end{array} .$$

(The arrows labelled m_{C^*} and m_{D^*} could just as well have been labelled m_{C^o} and m_{D^o}, since the multiplication maps m_{C^o} and m_{D^o} are restrictions of m_{C^*} and m_{D^*}.) Argue that the diagram (12.1.7) commutes. Thus, $f^* \circ \Delta_D^* = \Delta_C^* \circ (f \otimes f)^*$ as maps from $(D \otimes D)^o$ to C^o. In other words, $(\Delta_D \circ f)^* = ((f \otimes f) \circ \Delta_C)^*$ as maps from $(D \otimes D)^o$ to C^o. But a general linear-algebraic fact states that if U and V are two graded $\mathbf{k}$-modules such that V is of finite type, and if α and β are two graded $\mathbf{k}$-linear maps $U \to V$ such that $\alpha^* = \beta^*$ as maps from V^o to U^o, then $\alpha = \beta$ [379]. Hence, $(\Delta_D \circ f)^* = ((f \otimes f) \circ \Delta_C)^*$ leads to $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$. In other words, the first diagram in (12.1.6) commutes. The second is similar but easier. Thus, f is a $\mathbf{k}$-coalgebra morphism, and the "if" direction is proved.

Hint to Exercise 1.6.4. Straightforward computations. For part (d), first show (independently of whether $\mathbf{k}$ is a field and its characteristic) that $\left(f^{(1)}\right)^m = m! f^{(m)}$ for every $m \in \mathbb{N}$.

Hint to Exercise 1.6.5. It is best to solve parts (c) and (d) before approaching (b).

(a) Both maps $\Delta_{\operatorname{Sym} V}$ and

$$\begin{array}{ccc} \mathbf{k}[\mathbf{x}] & \xrightarrow{\Delta} & \mathbf{k}[\mathbf{x}, \mathbf{y}], \\ f(x_1, \ldots, x_n) & \longmapsto & f(x_1 + y_1, \ldots, x_n + y_n) \end{array}$$

are $\mathbf{k}$-algebra homomorphisms. Thus, in order to check that they are equal, it suffices to verify that they agree on V (since V generates $\operatorname{Sym} V$).

(c) This is a straightforward computation unless you get confused with the topologist's sign convention. The latter convention affects the twist map $T = T_{T(V),T(V)} : T(V) \otimes T(V) \to T(V) \otimes T(V)$ (in particular, we now have $T(x \otimes x) = -x \otimes x$ instead of $T(x \otimes x) = x \otimes x$), and thus also affects the multiplication in the $\mathbf{k}$-algebra $T(V) \otimes T(V)$, because this multiplication is given by

$$m_{T(V) \otimes T(V)} = \left(m_{T(V)} \otimes m_{T(V)}\right) \circ (\mathrm{id} \otimes T \otimes \mathrm{id}) .$$

Make sure you understand why this leads to $(1 \otimes x) \cdot (x \otimes 1) = -x \otimes x$ (whereas $(x \otimes 1) \cdot (1 \otimes x) = x \otimes x$).

(d) The trickiest part is showing that J is a graded $\mathbf{k}$-submodule of $T(V)$. It suffices to check that J is generated (as a two-sided ideal) by homogeneous elements[380]; however, this is not completely trivial, as the

[378] Beware: we don't have an inverse of the non-restricted map $\rho_{D,D} : D^* \otimes D^* \to (D \otimes D)^*$.

[379] This follows immediately from Exercise 1.6.1 (e).

[380] Make sure you understand why.

designated generators x^2 for $x \in V$ need not be homogeneous. However, it helps to observe that J is also the two-sided ideal generated by the set

$$\{x \otimes x\}_{x \in V \text{ is homogeneous}} \cup \{x \otimes y + y \otimes x\}_{x,y \in V \text{ are homogeneous}}$$

(why?), which set does consist of homogeneous elements. Thus, J is a graded $\mathbf{k}$-submodule of $T(V)$. From part (c), it is easy to observe that J is a two-sided coideal of $T(V)$ as well. Hence, $T(V)/J$ inherits a graded $\mathbf{k}$-bialgebra structure from $T(V)$. The rest is easy.

(b) is now a consequence of what has been done in (d).

Hint to Exercise 1.6.6. Easy and straightforward.

Hint to Exercise 1.6.8. The hint after the exercise shows the way; here are a few more pointers. The solution proceeds in two steps:

- *Step 1:* Show that Proposition 1.6.7 holds when V is a finite free $\mathbf{k}$-module.
- *Step 2:* Use this to conclude that Proposition 1.6.7 always holds.

The trick to Step 1 is to reduce the proof to Example 1.6.3. In a bit more detail: If V is a finite free $\mathbf{k}$-module with basis $(v_1, v_2, \ldots, v_n)$, then we know from Example 1.6.3 that the graded dual A^o of its tensor algebra $A := T(V)$ is a Hopf algebra whose basis $\left\{y_{(i_1,i_2,\ldots,i_\ell)}\right\}$ is indexed by words in the alphabet $I := \{1, 2, \ldots, n\}$. This allows us to define a $\mathbf{k}$-linear map $\phi : A^o \to T(V)$ by setting

$$\phi\left(y_{(i_1,i_2,\ldots,i_\ell)}\right) = v_{i_1} v_{i_2} \cdots v_{i_\ell} \qquad \text{for every } \ell \in \mathbb{N} \text{ and } (i_1, i_2, \ldots, i_\ell) \in I^\ell.$$

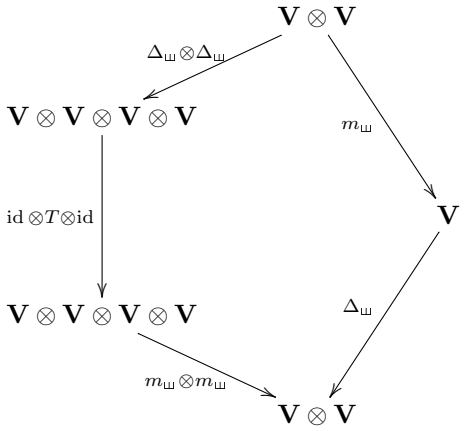
This $\mathbf{k}$-linear map ϕ then is an isomorphism from the Hopf algebra A^o to the putative Hopf algebra $\left(\mathrm{Sh}(V), \sqcup\!\sqcup, 1_{T(V)}, \Delta_{\sqcup\!\sqcup}, \epsilon, S\right)$, in the sense that it is invertible (since it sends a basis to a basis) and satisfies the five equalities

$$\begin{aligned}
\phi \circ m_{A^o} &= m_{\sqcup\!\sqcup} \circ (\phi \otimes \phi), \\
\phi \circ u_{A^o} &= u, \\
(\phi \otimes \phi) \circ \Delta_{A^o} &= \Delta_{\sqcup\!\sqcup} \circ \phi, \\
\epsilon_{A^o} &= \epsilon \circ \phi, \\
\phi \circ S_{A^o} &= S \circ \phi
\end{aligned}$$

(check all these – for instance, the first of these equalities follows by comparing (1.6.4) with the definition of $\sqcup\!\sqcup$). Thus, the latter putative Hopf algebra is an actual Hopf algebra (since the former is). This proves Proposition 1.6.7 for our finite free V, and thus completes Step 1.

Step 2 demonstrates the power of functoriality. We want to prove Proposition 1.6.7 in the general case, knowing that it holds when V is finite free. So let V be an arbitrary $\mathbf{k}$-module. For the sake of brevity, we shall write $\mathbf{V}$ for $T(V)$. Let $m_{\sqcup\!\sqcup}$ denote the $\mathbf{k}$-linear map $\mathbf{V} \otimes \mathbf{V} \to \mathbf{V}$ which sends every $a \otimes b$ to $a \sqcup\!\sqcup b$. One of the things that need to be shown is the commutativity of the diagram

(12.1.8)

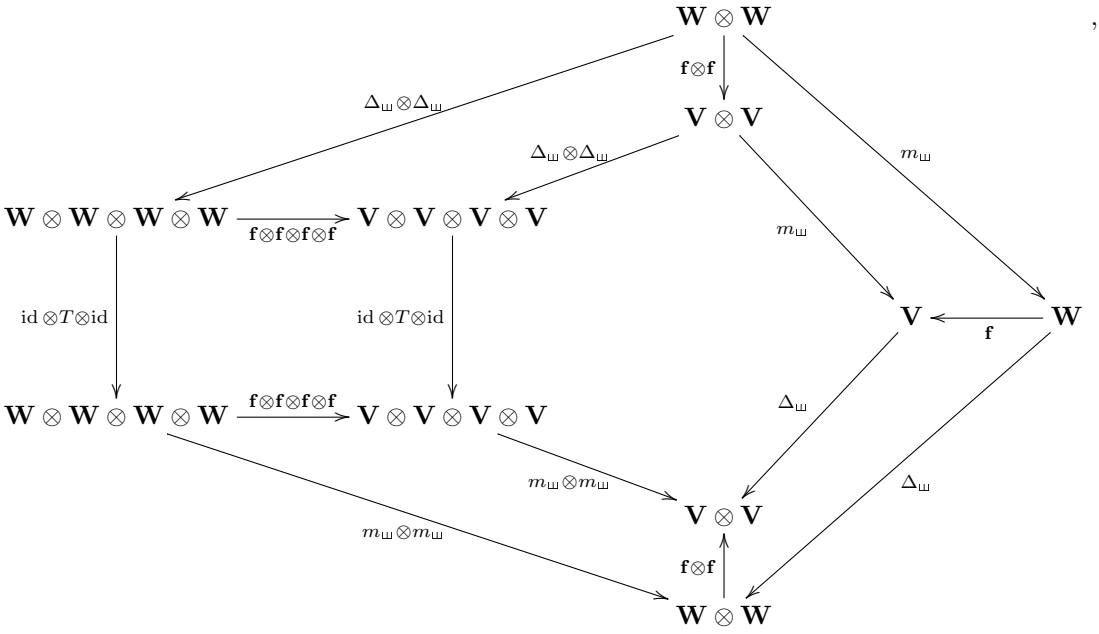


,

where T is the twist map $T_{\mathbf{V},\mathbf{V}}$. By linearity, it is clearly enough to verify this only on the pure tensors; that is, it is enough to check that every $a \in \mathbf{V}$ and $b \in \mathbf{V}$ satisfy

$$((m_{\sqcup\!\sqcup} \otimes m_{\sqcup\!\sqcup}) \circ (\mathrm{id} \otimes T \otimes \mathrm{id}) \circ (\Delta_{\sqcup\!\sqcup} \otimes \Delta_{\sqcup\!\sqcup}))(a \otimes b) = (\Delta_{\sqcup\!\sqcup} \circ m_{\sqcup\!\sqcup})(a \otimes b). \tag{12.1.9}$$

So let $a, b \in \mathbf{V}$ be arbitrary. WLOG assume that $a = v_1 v_2 \cdots v_p$ and $b = v_{p+1} v_{p+2} \cdots v_{p+q}$ for some $p, q \in \mathbb{N}$ and $v_1, v_2, \ldots, v_{p+q} \in V$. Define W to be the free $\mathbf{k}$-module with basis $(x_1, x_2, \ldots, x_{p+q})$, and let $\mathbf{W}$ be its tensor algebra $T(W)$. Then, W is a finite free $\mathbf{k}$-module, and so we know from Step 1 that Proposition 1.6.7 holds for W instead of V. But we can define a $\mathbf{k}$-linear map $f : W \to V$ that sends $x_1, x_2, \ldots, x_{p+q}$ to $v_1, v_2, \ldots, v_{p+q}$, respectively. This map $f : W \to V$ clearly induces a $\mathbf{k}$-algebra homomorphism $\mathbf{f} := T(f) : \mathbf{W} \to \mathbf{V}$ that respects all relevant shuffle-algebraic structure (i.e., it satisfies $\mathbf{f} \circ m_{\sqcup\!\sqcup} = m_{\sqcup\!\sqcup} \circ (\mathbf{f} \otimes \mathbf{f})$ and $(\mathbf{f} \otimes \mathbf{f}) \circ \Delta_{\sqcup\!\sqcup} = \Delta_{\sqcup\!\sqcup} \circ \mathbf{f}$ and so on), simply because this structure has been defined canonically in terms of each of V and W. Thus, in the diagram



all the little quadrilaterals commute. The outer pentagon also commutes, since Proposition 1.6.7 holds for W instead of V. If $\mathbf{f}$ was surjective, then we would be able to conclude that the inner pentagon also commutes, so we would immediately get the commutativity of (12.1.8). But even if $\mathbf{f}$ is not surjective, we are almost there: The inner pentagon commutes on the image of the map $\mathbf{f} \otimes \mathbf{f} : \mathbf{W} \otimes \mathbf{W} \to \mathbf{V} \otimes \mathbf{V}$ (because when we start at $\mathbf{W} \otimes \mathbf{W}$, we can walk around the outer pentagon instead, which is known to commute), but this image contains $a \otimes b$ (since $a = v_1 v_2 \cdots v_p = \mathbf{f}(x_1 x_2 \cdots x_p)$ and similarly $b = \mathbf{f}(x_{p+1} x_{p+2} \cdots x_{p+q})$), so we conclude that (12.1.9) holds, as we wanted to show.

This is only one of the diagrams we need to prove in order to prove Proposition 1.6.7, but the other diagrams are done in the exact same way.

Hint to Exercise 1.7.9. Straightforward reasoning using facts like "a union of finitely many finite sets is finite" and "a tensor is a sum of finitely many pure tensors".

Hint to Exercise 1.7.13. Parts (a), (b), (d) and (e) of Proposition 1.7.11 are easy. (In proving (1.7.3) and later, it helps to first establish an extension of (1.7.2) to infinite sums[381].) For part (c), recall that the binomial formula $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ holds for any two commuting elements a and b of any ring (such as f and g in the convolution algebra $\mathrm{Hom}(C, A)$). Part (f) follows from (e) using (1.7.3). Part (g)

[381] Namely: Let $(r_q)_{q \in Q} \in (\mathbf{k}[[T]])^Q$ be a family of power series such that the (possibly infinite) sum $\sum_{q \in Q} r_q$ converges in $\mathbf{k}[[T]]$. Let $f \in \mathfrak{n}(C, A)$. Then, the family $((r_q)^\star(f))_{q \in Q} \in (\mathrm{Hom}(C, A))^Q$ is pointwise finitely supported and satisfies $\left(\sum_{q \in Q} r_q\right)^\star (f) = \sum_{q \in Q} (r_q)^\star (f)$.

is best proved in two steps: First, use induction to prove part (g) in the case when $u = T^k$ for some $k \in \mathbb{N}$ (this relies on (1.7.3)); then, notice that both sides of (1.7.7) depend $\mathbf{k}$-linearly on u, whence the general case follows (up to some mudfighting with infinite sums). Part (h) is an instance of the "local $\star$-nilpotence" already observed in the proof of Proposition 1.4.7. Part (j) follows from (h). Part (i) follows from Proposition 1.4.3 (applied to $C' = C$, $A' = B$, $\gamma = \mathrm{id}_C$ and $\alpha = s$) in a similar way as part (g) followed from (1.7.3).

Hint to Exercise 1.7.20. Proposition 1.7.15 is a classical result, often proved by a lazy reference to the mythical complex analysis class the reader has surely seen it in. Here is a do-it-yourself purely algebraic proof:

- *Step 1:* If $u, v \in \mathbf{k}[[T]]$ are two power series having the same constant term and satisfying $\frac{d}{dT}u = \frac{d}{dT}v$, then $u = v$. This simple lemma (whose analogue for differentiable functions is a fundamental fact of real analysis) is easily proved by comparing coefficients in $\frac{d}{dT}u = \frac{d}{dT}v$ and recalling that $\mathbf{k}$ is a $\mathbb{Q}$-algebra (so $1, 2, 3, \ldots$ are invertible in $\mathbf{k}$).
- *Step 2:* If $u, v \in \mathbf{k}[[T]]$ are two power series having constant term 1 and satisfying $\left(\frac{d}{dT}u\right) \cdot v = \left(\frac{d}{dT}v\right) \cdot u$, then $u = v$. This can be proved by applying Step 1 to uv^{-1} and 1 instead of u and v.
- *Step 3:* The power series $\overline{\log}[\overline{\exp}]$ and $\overline{\exp}[\overline{\log}]$ are well-defined and have constant term 0. (Easy.)
- *Step 4:* If $w \in \mathbf{k}[[T]]$ is a power series having constant term 0, then
$$\frac{d}{dT}\left(\overline{\exp}[w]\right) = \left(\frac{d}{dT}w\right) \cdot \exp[w] \qquad \text{and}$$
$$\frac{d}{dT}\left(\overline{\log}[w]\right) = \left(\frac{d}{dT}w\right) \cdot \frac{1}{1+w}.$$
These formulas can be derived from the chain rule, or more directly from $\overline{\exp}[w] = \sum_{n\geq 1}\frac{1}{n!}w^n$ and $\overline{\log}[w] = \sum_{n\geq 1}\frac{(-1)^{n-1}}{n}w^n$.
- *Step 5:* Show $\overline{\exp}[\overline{\log}] = T$ by applying Step 2 to $u = \exp[\overline{\log}]$ and $v = 1 + T$.
- *Step 6:* Show $\overline{\log}[\overline{\exp}] = T$ by applying Step 1 to $u = \overline{\log}[\overline{\exp}]$ and $v = T$.

Lemma 1.7.16 easily follows from Proposition 1.7.11(f).

Remains to prove Proposition 1.7.18. It is easy to see that $\log^\star(\exp^\star f) = \overline{\log}^\star(\overline{\exp}^\star f)$ for each $f \in \mathfrak{n}(C, A)$; thus, Proposition 1.7.18(a) follows from (1.7.7) using Proposition 1.7.15 and Proposition 1.7.11(f) (since $T^\star(f) = f$). A similar argument yields Proposition 1.7.18(b) (this time, we need to observe that $\exp^\star(\log^\star g) = \overline{\exp}^\star\left(\overline{\log}^\star(g - u_A\epsilon_C)\right) + u_A\epsilon_C$ first). To prove Proposition 1.7.18(c), first use Proposition 1.7.11(c) to show that $\exp^\star(f+g)$ is well-defined; then, apply the well-known fact that $\exp(x+y) = \exp x \cdot \exp y$ for any two commuting elements x and y of a ring (provided the exponentials are well-defined; some yak-shaving is required here to convince oneself that the infinite sums behave well)[382]. Part (d) is trivial. Part (e) is an induction on n. Part (f) is a rehash of the definition of $\log^\star(f + u_A\epsilon_C) = \overline{\log}^\star f$.

Hint to Exercise 1.7.28. Proposition 1.7.21(a) is easily proved by unpacking the definition of convolution (just like Proposition 1.4.3). Part (b) follows from (a) by induction.

The trick to Proposition 1.7.22 is to realize that if $f \in \mathrm{Hom}(C, A)$ is as in Proposition 1.7.22, then every $x, y \in C$ satisfy

$$f(xy) = \epsilon(y) f(x) + \epsilon(x) f(y), \tag{12.1.10}$$

because $xy - \epsilon(x)y - \epsilon(y)x = \epsilon(x)\epsilon(y)\cdot 1 + \underbrace{(x - \epsilon(x))}_{\in \ker\epsilon}\underbrace{(y - \epsilon(y))}_{\in\ker\epsilon}$ is annihilated by f. Once this equality is known, it is not hard to prove Proposition 1.7.22 "by hand" by induction on n (using Sweedler notation).

[382] If you have not seen this well-known fact, prove it by a quick computation using the binomial formula.

Alternatively, for a cleaner proof, the equality (12.1.10) can be restated in an element-free way as

$$f \circ m_C = m_A \circ (f \otimes \mathfrak{i} + \mathfrak{i} \otimes f),$$

where $\mathfrak{i} = u_A \circ \epsilon_C$ is the unity of the $\mathbf{k}$-algebra $(\operatorname{Hom}(C, A), \star)$; then, an application of Proposition 1.7.21(b) shows that every $n \in \mathbb{N}$ satisfies

$$f^{\star n} \circ m_C = m_A \circ \underbrace{(f \otimes \mathfrak{i} + \mathfrak{i} \otimes f)^{\star n}}_{= \sum_{i=0}^{n} \binom{n}{i} (f \otimes \mathfrak{i})^{\star i} \star (\mathfrak{i} \otimes f)^{\star (n-i)}} = m_A \circ \left(\sum_{i=0}^{n} \binom{n}{i} \underbrace{(f \otimes \mathfrak{i})^{\star i} \star (\mathfrak{i} \otimes f)^{\star (n-i)}}_{= f^{\star i} \otimes f^{\star (n-i)}} \right)$$

(by the binomial formula, since $f \otimes \mathfrak{i}$ and $\mathfrak{i} \otimes f$ commute in the convolution algebra $\operatorname{Hom}(C \otimes C, A \otimes A)$)

(by repeated application of Exercise 1.4.4(a))

$$= m_A \circ \left(\sum_{i=0}^{n} \binom{n}{i} f^{\star i} \otimes f^{\star (n-i)} \right),$$

which is precisely Proposition 1.7.22 (restated in an element-free way).

Proposition 1.7.23 is an easy consequence of Proposition 1.7.22, since $(\exp^\star f)(xy) = \sum_{n \in \mathbb{N}} \frac{1}{n!} f^{\star n}(xy)$. (Again, fighting infinite sums is probably the most laborious part of the proof.)

Lemma 1.7.24 can be reduced to the fact that the matrix $\left(i^{N+1-j}\right)_{i,j=1,2,\ldots,N+1} \in \mathbb{Q}^{(N+1)\times(N+1)}$ is invertible (since its determinant is the Vandermonde determinant $\prod_{1 \le i < j \le N+1} \underbrace{(i-j)}_{\neq 0} \neq 0$) and thus has trivial kernel (not just over $\mathbb{Q}$, but on any torsionfree abelian group).

Lemma 1.7.25 follows from Lemma 1.7.24, because a finitely supported family indexed by nonnegative integers must become all zeroes from some point on.

The proof of Proposition 1.7.26 is rather surprising: It suffices to show that $f(xy) = 0$ for all $x, y \in \ker \epsilon$. So let us fix $x, y \in \ker \epsilon$. Proposition 1.7.11(h) yields $f \in \mathfrak{n}(C, A)$. Let $t \in \mathbb{N}$ be arbitrary. Then, Proposition 1.7.18(e) (applied to $n = t$) shows that $tf \in \mathfrak{n}(C, A)$ and $\exp^\star(tf) = (\exp^\star f)^{\star t}$. But Exercise 1.5.11(b) shows that $(\exp^\star f)^{\star t}$ is a $\mathbf{k}$-algebra homomorphism $C \to A$. Hence, $(\exp^\star f)^{\star t}(xy) = (\exp^\star f)^{\star t}(x) \cdot (\exp^\star f)^{\star t}(y)$. Rewriting $(\exp^\star f)^{\star t}$ as $\exp^\star(tf) = \sum_{n \in \mathbb{N}} \frac{1}{n!} f^{\star n} t^n$ on both sides, and multiplying out the right hand side, we can rewrite this as

$$\sum_{k \in \mathbb{N}} \frac{1}{k!} f^{\star k}(xy)\, t^k = \sum_{k \in \mathbb{N}} \left(\sum_{i=0}^{k} \frac{f^{\star i}(x)}{i!} \cdot \frac{f^{\star (k-i)}(y)}{(k-i)!} \right) t^k.$$

In other words,

$$\sum_{k \in \mathbb{N}} w_k t^k = 0, \qquad \text{where we set } w_k = \frac{1}{k!} f^{\star k}(xy) - \sum_{i=0}^{k} \frac{f^{\star i}(x)}{i!} \cdot \frac{f^{\star (k-i)}(y)}{(k-i)!}.$$

But we have proved this for all $t \in \mathbb{N}$. Thus, Lemma 1.7.25 shows that

$$w_k = 0 \qquad \text{for every } k \in \mathbb{N}.$$

Applying this to $k = 1$ and simplifying, we obtain $f(xy) - \epsilon(x) f(y) - f(x) \epsilon(y) = 0$. Since $x, y \in \ker \epsilon$, this simplifies even further to $f(xy) = 0$, which proves Proposition 1.7.26.

Finally, we need to prove Proposition 1.7.27. Set $F = \exp^\star f$ and $\widetilde{F} = F - u_A \epsilon_C$, so that $\widetilde{F} \in \mathfrak{n}(C, A)$. Then, Proposition 1.7.23 shows that $F : C \to A$ is a $\mathbf{k}$-algebra homomorphism, so it remains to show that F is surjective. But it is easy to see using Proposition 1.7.18(a) that $f = \overline{\log}^\star \widetilde{F}$.

Define $\widetilde{\mathrm{id}} \in \mathfrak{n}(C, C)$ by $\widetilde{\mathrm{id}} = \mathrm{id}_C - u_C \epsilon_C$. Then, it is not hard to see that $F \circ \widetilde{\mathrm{id}} = \widetilde{F}$. Hence, $f = \overline{\log}^\star \underbrace{\widetilde{F}}_{= F \circ \widetilde{\mathrm{id}}} = \overline{\log}^\star \left(F \circ \widetilde{\mathrm{id}} \right) = F \circ \left(\overline{\log}^\star \left(\widetilde{\mathrm{id}} \right) \right)$ (by Proposition 1.7.11(i), since F is a $\mathbf{k}$-algebra homomorphism). Therefore, $f(C) \subset F(C)$. Since F is a $\mathbf{k}$-algebra homomorphism, this entails that $F(C)$ is a $\mathbf{k}$-subalgebra

of A that contains $f(C)$ as a subset. But this causes $F(C)$ to be the whole A (since $f(C)$ generates A). Thus, F is surjective, so Proposition 1.7.27 is proven.

Hint to Exercise 1.7.33. We must prove Theorem 1.7.29. Part (a) is easy. For the remainder of the proof, we set $\widetilde{\mathrm{id}} = \mathrm{id}_A - u_A \epsilon_A \in \operatorname{End} A$, and equip ourselves with some simple lemmas:

- The kernel $\ker \epsilon$ is an ideal of A.
- We have $\widetilde{\mathrm{id}} \in \mathfrak{n}(A, A)$ and $\ker \widetilde{\mathrm{id}} = \mathbf{k} \cdot 1_A$ and $\widetilde{\mathrm{id}}(A) = \ker \epsilon$.
- We have $A / \left(\mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \right) \cong (\ker \epsilon) / (\ker \epsilon)^2$ as $\mathbf{k}$-modules.

Now, to the proof of Theorem 1.7.29(b). Using $\mathfrak{e} = \log^\star(\mathrm{id}_A) = \overline{\log}^\star \widetilde{\mathrm{id}}$ and $\widetilde{\mathrm{id}}(1_A) = 0$, it is easy to see that $\mathfrak{e}(1_A) = 0$. Hence, $\mathfrak{e}(A_0) = 0$ since A is connected. Thus, Proposition 1.7.26 shows that $\mathfrak{e}\left((\ker \epsilon)^2 \right) = 0$ (since $\exp^\star \mathfrak{e} = \mathrm{id}_A$ is a $\mathbf{k}$-algebra homomorphism). Combined with $\mathfrak{e}(1_A) = 0$, this yields $\mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \subset \ker \mathfrak{e}$. But this inclusion is actually an equality, as we can show by the following computation: We have $\mathfrak{e} = \overline{\log}^\star \widetilde{\mathrm{id}} = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}$, and therefore each $x \in A$ satisfies

$$\mathfrak{e}(x) = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} \widetilde{\mathrm{id}}^{\star n}(x) = \underbrace{\widetilde{\mathrm{id}}(x)}_{\substack{= x - \epsilon(x) 1_A \\ \text{(by the definition of } \widetilde{\mathrm{id}}\text{)}}} + \sum_{n \geq 2} \frac{(-1)^{n-1}}{n} \underbrace{\widetilde{\mathrm{id}}^{\star n}(x)}_{\substack{\in \left(\widetilde{\mathrm{id}}(A)\right)^n \\ \text{(by induction on } n\text{,} \\ \text{using the definition} \\ \text{of convolution)}}}$$

$$\in x - \epsilon(x) 1_A + \sum_{n \geq 2} \frac{(-1)^{n-1}}{n} \left(\underbrace{\widetilde{\mathrm{id}}(A)}_{= \ker \epsilon} \right)^n = x - \underbrace{\epsilon(x)}_{\in \mathbf{k}} 1_A + \underbrace{\sum_{n \geq 2} \frac{(-1)^{n-1}}{n} (\ker \epsilon)^n}_{\subset (\ker \epsilon)^2} \subset x - \mathbf{k} \cdot 1_A + (\ker \epsilon)^2,$$

so that

$$x - \mathfrak{e}(x) \in \mathbf{k} \cdot 1_A + (\ker \epsilon)^2. \tag{12.1.11}$$

If $x \in \ker \mathfrak{e}$, then this simplifies to $x \in \mathbf{k} \cdot 1_A + (\ker \epsilon)^2$. Thus, $\ker \mathfrak{e} \subset \mathbf{k} \cdot 1_A + (\ker \epsilon)^2$. Combining this with $\mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \subset \ker \mathfrak{e}$, we obtain $\ker \mathfrak{e} = \mathbf{k} \cdot 1_A + (\ker \epsilon)^2$. But the homomorphism theorem yields

$$\mathfrak{e}(A) \cong A / \underbrace{\ker \mathfrak{e}}_{= \mathbf{k} \cdot 1_A + (\ker \epsilon)^2} = A / \left(\mathbf{k} \cdot 1_A + (\ker \epsilon)^2 \right) \cong (\ker \epsilon) / (\ker \epsilon)^2 \qquad \text{(as seen above)}$$

as $\mathbf{k}$-modules. This completes the proof of Theorem 1.7.29(b).

Theorem 1.7.29(c) just requires showing that $\mathfrak{q}(A_0) = 0$, which is a consequence of $\mathfrak{e}(A_0) = 0$.

Next, we shall prove Theorem 1.7.29(d). We have $\mathfrak{q} \in \mathfrak{n}(A, \operatorname{Sym}(\mathfrak{e}(A)))$. Furthermore, $\mathfrak{q}(A)$ generates the $\mathbf{k}$-algebra $\operatorname{Sym}(\mathfrak{e}(A))$ (since $\mathfrak{q}(A) = \operatorname{Sym}^1(\mathfrak{e}(A))$). From Theorem 1.7.29(b), we get $\ker \mathfrak{e} = \mathbf{k} \cdot 1_A + (\ker \epsilon)^2$, from which we easily obtain $\mathfrak{q}(1_A) = 0$ and $\mathfrak{q}\left((\ker \epsilon)^2 \right) = 0$. Thus, Proposition 1.7.27 (applied to A, $\operatorname{Sym}(\mathfrak{e}(A))$ and $\mathfrak{q}$ instead of C, A and f) shows that $\exp^\star \mathfrak{q} : A \to \operatorname{Sym}(\mathfrak{e}(A))$ is a surjective $\mathbf{k}$-algebra homomorphism. But $\mathfrak{s}$ is a $\mathbf{k}$-algebra homomorphism $\operatorname{Sym}(\mathfrak{e}(A)) \to A$ and satisfies $\mathbf{i} = \mathfrak{s} \circ \iota_{\mathfrak{e}(A)}$ (by its definition). Thus, Proposition 1.7.11(i) (applied to A, $\operatorname{Sym}(\mathfrak{e}(A))$, A, $\mathfrak{s}$, exp and $\mathfrak{q}$ instead of C, A, B, s, u and f) shows that $\mathfrak{s} \circ \mathfrak{q} \in \mathfrak{n}(A, A)$ and $\exp^\star(\mathfrak{s} \circ \mathfrak{q}) = \mathfrak{s} \circ (\exp^\star \mathfrak{q})$. However, it is easy to see that $\mathfrak{s} \circ \mathfrak{q} = \mathfrak{e}$ (since $\mathbf{i} = \mathfrak{s} \circ \iota_{\mathfrak{e}(A)}$); this lets us rewrite the equality $\exp^\star(\mathfrak{s} \circ \mathfrak{q}) = \mathfrak{s} \circ (\exp^\star \mathfrak{q})$ as $\exp^\star \mathfrak{e} = \mathfrak{s} \circ (\exp^\star \mathfrak{q})$. Comparing this with $\exp^\star \mathfrak{e} = \mathrm{id}_A$, we obtain $\mathfrak{s} \circ (\exp^\star \mathfrak{q}) = \mathrm{id}_A$. Since $\exp^\star \mathfrak{q}$ is surjective, this entails that the maps $\exp^\star \mathfrak{q}$ and $\mathfrak{s}$ are mutually inverse. This proves Theorem 1.7.29(d).

Theorem 1.7.29(d) shows that $A \cong \operatorname{Sym}(\mathfrak{e}(A))$ as $\mathbf{k}$-algebras, but Theorem 1.7.29(b) shows that $\mathfrak{e}(A) \cong (\ker \epsilon) / (\ker \epsilon)^2$ as $\mathbf{k}$-modules. Combining these, we obtain Theorem 1.7.29(e).

Finally, to prove Theorem 1.7.29(f), we notice that each $x \in A$ satisfies

$$\begin{aligned} x - \mathfrak{e}(x) &\in \mathbf{k} \cdot 1_A + (\ker \epsilon)^2 && \text{(by (12.1.11))} \\ &= \ker \mathfrak{e} && \text{(by Theorem 1.7.29(b))} \end{aligned}$$

and thus $0 = \mathfrak{e}(x - \mathfrak{e}(x)) = \mathfrak{e}(x) - (\mathfrak{e} \circ \mathfrak{e})(x)$.

Acknowledgements

The authors thank the following for helpful comments and/or teaching them about Hopf algebras: Marcelo Aguiar, Federico Ardila, Lou Billera, Richard Ehrenborg, Mark Haiman, Florent Hivert, Christophe Hohlweg, Jia Huang, Jang Soo Kim, Aaron Lauve, Dominique Manchon, John Palmieri, Alexander Postnikov, Margie Readdy, Nathan Reading, Christophe Reutenauer, Hans-Jürgen Schneider, Richard Stanley, Josh Swanson, Muge Taskin, Jean-Yves Thibon.

Parts of this text have been written during stays at the Mathematisches Forschungsinstitut Oberwolfach (2019 and 2020)[383] and at the Institut Mittag–Leffler Djursholm (Spring 2020, supported by the Swedish Research Council under grant no. 2016-06596); DG thanks both for their hospitality.

References

[1] Eiichi Abe. Hopf algebras. *Cambridge Tracts in Mathematics* **74**. Cambridge University Press, Cambridge-New York, 1980.

[2] Marcelo Aguiar, et al. (28 authors). Supercharacters, symmetric functions in noncommuting variables, and related Hopf algebras. *Adv. Math.* **229** (2012), 2310–2337. https://doi.org/10.1016/j.aim.2011.12.024 . Also available as arXiv:1009.4134v2.

[3] Marcelo Aguiar and Federico Ardila. Hopf monoids and generalized permutahedra. arXiv:1709.07504v1.

[4] Marcelo Aguiar, Nantel Bergeron, and Frank Sottile. Combinatorial Hopf algebras and generalized Dehn-Sommerville relations. *Compos. Math.* **142** (2006), pp. 1–30. A newer version of this paper appears at http://pi.math.cornell.edu/~maguiar/CHalgebra.pdf.

[5] Marcelo Aguiar, Aaron Lauve. The characteristic polynomial of the Adams operators on graded connected Hopf algebras. *Algebra & Number Theory* **9-3** (2015), 547–583. Also available at http://pi.math.cornell.edu/~maguiar/adams.pdf and as arXiv:1403.7584v2.

[6] Marcelo Aguiar and Swapneel Mahajan. Monoidal functors, species and Hopf algebras. *CRM Monograph Series* **29**. American Mathematical Society, Providence, RI, 2010. Available at http://pi.math.cornell.edu/~maguiar/a.pdf

[7] Marcelo Aguiar and Frank Sottile. Structure of the Malvenuto-Reutenauer Hopf algebra of permutations. *Adv. Math.* **191** (2005), 225–275. https://doi.org/10.1016/j.aim.2004.03.007.
A preprint is available at http://pi.math.cornell.edu/~maguiar/MR.pdf

[8] Nicolas Andruskiewitsch, Walter Ferrer Santos. The beginnings of the theory of Hopf algebras. *Acta Appl Math* **108** (2009), 3–17. See also a corrected postprint published on arXiv as arXiv:0901.2460v3.

[9] Sami H. Assaf and Peter R.W. McNamara. A Pieri rule for skew shapes. *J. Combin. Theory, Ser. A* **118** (2011), 277–290. https://doi.org/10.1016/j.jcta.2010.03.010

[10] Olga Azenhas. Littlewood-Richardson fillings and their symmetries. *Matrices and group representations* (Coimbra, 1998), 81–92, Textos Mat. Ser. B, 19, Univ. Coimbra, Coimbra, 1999. http://www.mat.uc.pt/~oazenhas/graciano+.pdf.

[11] Olga Azenhas, Ronald C. King, Itaru Terada. The involutive nature of the Littlewood-Richardson commutativity bijection. arXiv:1603.05037v1.

[12] Andrew Baker, and Birgit Richter. Quasisymmetric functions from a topological point of view. *Math. Scand.* **103** (2008), 208–242. http://dx.doi.org/10.7146/math.scand.a-15078

[13] Farzin Barekat, Victor Reiner, Stephanie van Willigenburg. Corrigendum to "Coincidences among skew Schur functions" [*Adv. Math.* **216** (2007), 118–152]. *Adv. Math.* **220** (2009), 1655–1656. See also a corrected version of this paper on arXiv:math/0602634v4.

[14] Carolina Benedetti, Joshua Hallam, John Machacek. Combinatorial Hopf Algebras of Simplicial Complexes. arXiv:1505.04458v2. (Published in: *SIAM J. Discrete Math.* **30** (3), 1737–1757.)

[15] Carolina Benedetti, Bruce Sagan. Antipodes and involutions. arXiv:1410.5023v4. (Published in: *Journal of Combinatorial Theory, Series A* **148** (2017), 275–315.)

[16] Georgia Benkart, Frank Sottile, Jeffrey Stroomer. Tableau Switching: Algorithms and Applications. *Journal of Combinatorial Theory, Series A* **76**, 1, October 1996, 11–43. https://doi.org/10.1006/jcta.1996.0086
Preprint available at http://www.math.tamu.edu/~sottile/research/pdf/switching.pdf

[17] Chris Berg, Nantel Bergeron, Franco Saliola, Luis Serrano, Mike Zabrocki. A lift of the Schur and Hall-Littlewood bases to non-commutative symmetric functions. *Canad. J. Math.* **66** (2014), 525–565. http://dx.doi.org/10.4153/CJM-2013-013-0.
A preprint is arXiv:1208.5191v3.

[18] Nantel Bergeron, Mike Zabrocki. The Hopf algebras of symmetric functions and quasi-symmetric functions in non-commutative variables are free and co-free. *Journal of Algebra and Its Applications* **08**, Issue 04, August 2009, 581–600. A preprint also appears at arXiv:math/0509265v3.

[19] Louis J. Billera. Flag enumeration in polytopes, Eulerian partially ordered sets and Coxeter groups. *Proceedings of the International Congress of Mathematicians* **IV**, 2389–2415, Hindustan Book Agency, New Delhi, 2010. http://pi.math.cornell.edu/~billera/papers/eulericm.pdf

[20] Louis J. Billera, Francesco Brenti. Quasisymmetric functions and Kazhdan-Lusztig polynomials. arXiv:0710.3965v2. Published in: Israel Journal of Mathematics, August 2011, 184, pp. 317–348. https://doi.org/10.1007/s11856-011-0070-0

[383] This research was supported through the programme "Oberwolfach Leibniz Fellows" by the Mathematisches Forschungsinstitut Oberwolfach in 2019 and 2020.

[21] Louis J. Billera, Ning Jia, and Victor Reiner. A quasisymmetric function for matroids. *European J. Combin.* **30** (2009), pp. 1727–1757. https://doi.org/10.1016/j.ejc.2008.12.007 . A preprint also appears at arXiv:math/0606646v3.
[22] Anders Björner. Some combinatorial and algebraic properties of Coxeter complexes and Tits buildings. *Adv. in Math.* **52** (1984), 173–212. https://doi.org/10.1016/0001-8708(84)90021-5
[23] Jonah Blasiak. Kronecker coefficients for one hook shape. *Seminaire Lotharingien de Combinatoire* **77** (2017), B77c. https://www.emis.de/journals/SLC/wpapers/s77blasiak.html
[24] D. Blessenohl, H. Laue. Algebraic combinatorics related to the free Lie algebra. *Seminaire Lotharingien de Combinatoire* **29** (1992), B29e. https://www.emis.de/journals/SLC/opapers/s29laue.html
[25] Dieter Blessenohl, Manfred Schocker. Noncommutative character theory of the symmetric group. Imperial College Press 2005. https://www.worldscientific.com/worldscibooks/10.1142/p369
[26] Ben Blum-Smith, Samuel Coskey. The Fundamental Theorem on Symmetric Polynomials: History's First Whiff of Galois Theory. arXiv:1301.7116v4. An updated version was published in: The College Mathematics Journal Vol. 48, No. 1 (January 2017), pp. 18–29. https://doi.org/10.4169/college.math.j.48.1.18
[27] N. Bourbaki. Éléments de Mathématique: Groupes et algèbres de Lie, Chapitres 2 et 3. Springer, Heidelberg 2006.
[28] Thomas Britz, Sergey Fomin. Finite posets and Ferrers shapes. *Adv. in Math.* **158**, Issue 1, 1 March 2001, 86–127. Better version to be found on arXiv as arXiv:math/9912126v1.
[29] N.G. de Bruijn, D.A. Klarner. Multisets of aperiodic cycles. *SIAM J. Alg. Disc. Math.* **3** (1982), no. 3, 359–368. https://pure.tue.nl/ws/files/1674487/597568.pdf
[30] Daniel Bump. Notes on representations of $GL(r)$ over a finite field. Available at http://math.stanford.edu/~bump/.
[31] Emily Burgunder. Eulerian idempotent and Kashiwara-Vergne conjecture. *Annales de l'institut Fourier* **58** (2008), Issue 4, 1153–1184. https://eudml.org/doc/10345.
[32] Lynne M. Butler, Alfred W. Hales. Nonnegative Hall polynomials. *Journal of Algebraic Combinatorics* **2** (1993), Issue 2, 125–135. https://www.emis.de/journals/JACO/Volume2_2/l42886q158156k2u.html
[33] Stefaan Caenepeel, J. Vercruysse. Hopf algebras. *Lecture notes, Vrije Universiteit Brussel* **2013**. http://homepages.ulb.ac.be/~scaenepe/Hopfalgebra.pdf
[34] Peter J. Cameron. Notes on matroids and codes. *Lecture notes*, 2000. http://www.maths.qmul.ac.uk/~pjc/comb/matroid.pdf
[35] Pierre F. Cartier. A primer of Hopf algebras. Frontiers in number theory, physics, and geometry. II, 537–615, Springer, Berlin, 2007.
A preprint is available at http://preprints.ihes.fr/2006/M/M-06-40.pdf
[36] Vyjayanthi Chari, and Andrew N. Pressley. A guide to quantum groups. Cambridge University Press, Cambridge, 1994.
[37] Sunil K. Chebolu, Jan Minac. Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. *Math. Mag.* **84** (2011), 369–371. A preprint is arXiv:1001.0409v6.
[38] K.T. Chen, R.H. Fox, R.C. Lyndon. Free Differential Calculus, IV: The Quotient Groups of the Lower Central Series. *Annals of Mathematics* **68** (1), 81–95. https://doi.org/10.2307/1970044
[39] Sergei Chmutov, Sergei V. Duzhin, Jacob Mostovoy. Introduction to Vassiliev Knot Invariants. CUP 2012.
Various preprint versions can be found at https://people.math.osu.edu/chmutov.1/preprints/ , at http://www.pdmi.ras.ru/~duzhin/papers/cdbook/ and at arXiv:1103.5628v3.
[40] Keith Conrad. Expository papers ("Blurbs"), specifically *Tensor Products I*, *Tensor Products II*, *Exterior Powers*. http://www.math.uconn.edu/~kconrad/blurbs
[41] Henry Crapo and William Schmitt. Primitive elements in the matroid-minor Hopf algebra. *J. Algebraic Combin.* **28** (2008), 43–64. https://doi.org/10.1007/s10801-007-0066-3.
A preprint is arXiv:math/0511033v1.
[42] ———. A unique factorization theorem for matroids. *J. Combin. Theory Ser. A* **112** (2005), 222–249. https://doi.org/10.1016/j.jcta.2005.02.004
[43] ———. A free subalgebra of the algebra of matroids. *European J. Combin.* **26** (2005), 1066–1085. https://doi.org/10.1016/j.ejc.2004.05.006
[44] William Crawley-Boevey. *Lectures on representation theory and invariant theory*, Bielefeld 1989/90. Available from https://www.math.uni-bielefeld.de/~wcrawley/.
[45] Maxime Crochemore, Jacques Désarménien, Dominique Perrin. A note on the Burrows–Wheeler transformation. *Theoretical Computer Science* **332** (2005), pp. 567–572. https://doi.org/10.1016/j.tcs.2004.11.014
A preprint is arXiv:cs/0502073.
[46] Geir Dahl. Network flows and combinatorial matrix theory. Lecture notes, 4 September 2013. http://www.uio.no/studier/emner/matnat/math/MAT-INF4110/h13/lecturenotes/combmatrix.pdf
[47] Sorin Dascalescu, Constantin Nastasescu, Serban Raianu. Hopf algebras. An introduction. *Monographs and Textbooks in Pure and Applied Mathematics* **235**. Marcel Dekker, Inc., New York, 2001.
[48] Barry Dayton. Witt vectors, the Grothendieck Burnside ring, and Necklaces. http://orion.neiu.edu/~bhdayton/necksum.htm
[49] Tom Denton, Florent Hivert, Anne Schilling, and Nicolas M. Thiéry. On the representation theory of finite J-trivial monoids. *Sém. Lothar. Combin.* **64** (2010/11), Art. B64d, 44 pp. https://www.emis.de/journals/SLC/wpapers/s64dehiscth.html
[50] Jacques Désarménien, Michelle L. Wachs. Descent classes of permutations with a given number of fixed points. *Journal of Combinatorial Theory, Series A* **64**, Issue 2, pp. 311–328. https://doi.org/10.1016/0097-3165(93)90100-M
[51] Persi Diaconis, Michael Mc Grath, Jim Pitman. Riffle shuffles, cycles, and descents. *Combinatorica* **15**(1), 1995, pp. 11–29. https://doi.org/10.1007/bf01294457

[52] Persi Diaconis, C.Y. Amy Pang and Arun Ram. Hopf algebras and Markov chains: Two examples and a theory. *J. Algebraic Combin.* **39**, Issue 3, May 2014, 527–585. A newer version is available at https://amypang.github.io/papers/hpmc.pdf

[53] Francesco Dolce, Antonio Restivo, Christophe Reutenauer. On generalized Lyndon words. Theoretical Computer Science **777** (2019), 232–242. Also available at arXiv:1812.04515v1.

[54] Francesco Dolce, Antonio Restivo, Christophe Reutenauer. Some variations on Lyndon words. arXiv:1904.00954v1.

[55] William F. Doran IV. A Proof of Reutenauer's $-q_{(n)}$ Conjecture. *J. Combin. Theory, Ser. A* **74** (1996), 342–344. https://doi.org/10.1006/jcta.1996.0056

[56] Andreas W. M. Dress, and Christian Siebeneicher. On the number of solutions of certain linear diophantine equations. *Hokkaido Math. J.* **19** (1990), pp. 385–401. http://www.math.sci.hokudai.ac.jp/hmj/page/19-3/pdf/HMJ_19_3_1990_385-401.pdf

[57] Andreas W. M. Dress, and Christian Siebeneicher. The Burnside Ring of the Infinite Cyclic Group and Its Relations to the Necklace Algebra, λ-Rings, and the Universal Ring of Witt Vectors. *Advances in Mathematics* **78** (1989), 1–41. https://doi.org/10.1016/0001-8708(89)90027-3

[58] Gérard Duchamp, Florent Hivert, and Jean-Yves Thibon. Noncommutative symmetric functions VI. Free quasi-symmetric functions and related algebras. *Internat. J. Algebra Comput.* **12** (2002), 671–717. A preprint is available at http://monge.univ-mlv.fr/~hivert/PAPER/NCSF6.ps.

[59] Gérard H. E. Duchamp, Nguyen Hoang-Nghia, Thomas Krajewski, Adrian Tanasa. Recipe theorem for the Tutte polynomial for matroids, renormalization group-like approach. *Advances in Applied Mathematics* **51**(3), 345—358. https://doi.org/10.1016/j.aam.2013.04.006

[60] Gérard Henry Edmond Duchamp, Vincel Hoang Ngoc Minh, Christophe Tollu, Bùi Chiên, Nguyen Hoang Nghia. Combinatorics of φ-deformed stuffle Hopf algebras. arXiv:1302.5391v7.

[61] Tobias Dyckerhoff. Hall Algebras - Bonn, Wintersemester 14/15. Lecture notes, version February 5, 2015. https://web.archive.org/web/20150601115158/http://www.math.uni-bonn.de/people/dyckerho/notes.pdf

[62] Jack Edmonds. Submodular functions, matroids, and certain polyhedra. In: Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969), Gordon and Breach, New York, 1970, pp. 66–87; reprinted in Combinatorial optimization: Eureka, you shrink!, pp. 11–26, *Lecture Notes in Comput. Sci.* **2570**, Springer, Berlin, 2003. https://doi.org/10.1007/3-540-36478-1_2

[63] Eric S. Egge. *An Introduction to Symmetric Functions and Their Combinatorics*. Student Mathematical Library **91**, American Mathematical Society, 2019. https://bookstore.ams.org/stml-91

[64] Richard Ehrenborg. On posets and Hopf algebras. *Adv. Math.* **119** (1996), 1–25. https://doi.org/10.1006/aima.1996.0026

[65] David Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry. *Graduate Texts in Mathematics* **150**, Springer 1995. https://doi.org/10.1007/978-1-4612-5350-1

[66] Sergi Elizalde, Justin M. Troyka. Exact and asymptotic enumeration of cyclic permutations according to descent set. *J. Combin. Theory, Ser. A* **165** (2019), 360–391. Also available at arXiv:1710.05103v3.

[67] Alexander P. Ellis, and Mikhail Khovanov. The Hopf algebra of odd symmetric functions. *Adv. Math.* **231** (2012), 965–999. A newer version is available as arXiv:1107.5610v2.

[68] Brittney Ellzey. On Chromatic Quasisymmetric Functions of Directed Graphs. PhD thesis, University of Miami, 2018. https://scholarlyrepository.miami.edu/oa_dissertations/2091

[69] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. Introduction to representation theory. *Student Mathematical Library* **59**, Amer. Math. Soc., Providence, RI, 2011. http://www-math.mit.edu/~etingof/repb.pdf . (Parts of this book appear in arXiv:0901.0827v5.) A newer version is available at http://www-math.mit.edu/~etingof/reprbook.pdf .

[70] Loic Foissy. Algèbres de Hopf combinatoires. http://loic.foissy.free.fr/pageperso/Hopf.pdf

[71] Loic Foissy. Free and cofree Hopf algebras. *Journal of Pure and Applied Algebra* **216**, Issue 2, February 2012, 480–494. https://doi.org/10.1016/j.jpaa.2011.07.010 . A preprint is arXiv:1010.5402v3.

[72] Harold Fredricksen, James Maiorana. Necklaces of beads in k colors and k-ary de Bruijn sequences. *Discrete Mathematics* **23** (1978), 207–210. https://doi.org/10.1016/0012-365X(78)90002-X

[73] William Fulton. Young Tableaux. *London Mathematical Society Student Texts* **35**, Cambridge University Press, Cambridge-New York, 1997. https://doi.org/10.1017/CBO9780511626241

[74] Adriano M. Garsia. Permutation q-enumeration with the Schur row adder. *PU. M. A. (Pure Mathematics and Applications)* **21** (2010), No. 2, 233–248. http://puma.dimai.unifi.it/21_2/7_Garsia.pdf (also mirrored at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.432.8196&rep=rep1&type=pdf).

[75] Vesselin Gasharov. Incomparability graphs of (3+1)-free posets are s-positive. Proceedings of the 6th Conference on Formal Power Series and Algebraic Combinatorics (New Brunswick, NJ, 1994). *Discrete Math.* **157** (1996), 193–197. https://doi.org/10.1016/S0012-365X(96)83014-7

[76] Vesselin Gasharov. A Short Proof of the Littlewood-Richardson Rule. *European Journal of Combinatorics*, Volume 19, Issue 4, May 1998, Pages 451–453. https://doi.org/10.1006/eujc.1998.0212

[77] Israel M. Gelfand, Daniel Krob, Alain Lascoux, Bernard Leclerc, Vladimir S. Retakh, Jean-Yves Thibon. Noncommutative symmetric functions. *Adv. Math.* **112** (1995), 218–348. https://doi.org/10.1006/aima.1995.1032
A preprint is available as arXiv:hep-th/9407124v1.

[78] M. Gerstenhaber, S.D. Schack. The shuffle bialgebra and the cohomology of commutative algebras. *Journal of Pure and Applied Algebra* **70** (1991), 263–272. https://doi.org/10.1016/0022-4049(91)90073-B

[79] Ira M. Gessel. Multipartite P-partitions and inner products of skew Schur functions. Combinatorics and algebra (Boulder, Colo., 1983), 289–317, *Contemp. Math.* **34**, Amer. Math. Soc., Providence, RI, 1984. http://people.brandeis.edu/~gessel/homepage/papers/multipartite.pdf

[80] Ira M. Gessel. A Historical Survey of P-Partitions. 2015, arXiv:1506.03508v1. Published in: Patricia Hersh, Thomas Lam, Pavlo Pylyavskyy and Victor Reiner (eds.), *The Mathematical Legacy of Richard P. Stanley*, Amer. Math. Soc., Providence, RI, 2016, pp. 169–188.

[81] Ira M. Gessel, Antonio Restivo, Christophe Reutenauer. A Bijection between Words and Multisets of Necklaces. *European Journal of Combinatorics* **33** (2012), pp. 1537–1546. https://doi.org/10.1016/j.ejc.2012.03.016

[82] Ira M. Gessel, Christophe Reutenauer. Counting Permutations with Given Cycle Structure and Descent Set. *Journal of Combinatorial Theory, Series A* **64** (1993), 189–215. https://doi.org/10.1016/0097-3165(93)90095-P

[83] Ira M. Gessel, X.G. Viennot. Determinants, Paths, and Plane Partitions. preprint, 1989, http://people.brandeis.edu/~gessel/homepage/papers/pp.pdf

[84] Andrew Granville. Number Theory Revealed: A Masterclass. *Number Theory Revealed: The Series* **#1B**, American Mathematical Society 2019.

[85] Darij Grinberg. Double posets and the antipode of QSym. arXiv:1509.08355v3.

[86] Darij Grinberg. A constructive proof of Orzech's theorem. Preprint, 20 November 2016. https://www.cip.ifi.lmu.de/~grinberg/algebra/orzech.pdf

[87] Frank D. Grosshans, Gian-Carlo Rota, Joel A. Stein. Invariant Theory and Superalgebras. *CBMS Regional Conference Series in Mathematics* **69**, American Mathematical Society, 1987. https://bookstore.ams.org/cbms-69

[88] A.M. Hamel, I.P. Goulden. Planar Decompositions of Tableaux and Schur Function Determinants. *Europ. J. Combinatorics* **16** (1995), 461–477. https://doi.org/10.1016/0195-6698(95)90002-0

[89] Michiel Hazewinkel. The algebra of quasi-symmetric functions is free over the integers. *Adv. Math.* **164** (2001), 283–300. https://doi.org/10.1006/aima.2001.2017

[90] Michiel Hazewinkel. Witt vectors. Part 1. In: M. Hazewinkel (ed.), *Handbook of Algebra* **6**, Elsevier 2009. Also available at arXiv:0804.3888v1.

[91] Michiel Hazewinkel. The Leibniz-Hopf Algebra and Lyndon Words. *Preprint AM CWI* **9612** (1996). http://oai.cwi.nl/oai/asset/4828/04828D.pdf

[92] Michiel Hazewinkel. Chen-Fox-Lyndon Factorization for Words over Partially Ordered Sets. *Journal of Mathematical Sciences* **131** (12-2005), Issue 6, 6027–6031. https://doi.org/10.1007/s10958-005-0458-7

[93] Michiel Hazewinkel, Nadiya Gubareni, and Vladimir V. Kirichenko. Algebras, rings and modules. Lie algebras and Hopf algebras. *Mathematical Surveys and Monographs* **168**. American Mathematical Society, Providence, RI, 2010.

[94] Robert Henderson. The Algebra Of Multiple Zeta Values. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.227.5432

[95] Lars Hesselholt. Lecture notes on Witt vectors. http://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.ps

[96] Lars Hesselholt. The big de Rham–Witt complex. *Acta Math.* **214** (2015), 135–207. https://doi.org/10.1007/s11511-015-0124-y

[97] Florent Hivert. An introduction to combinatorial Hopf algebras: examples and realizations. *Nato Advanced Study Institute School on Physics and Computer Science, 2005, october, 17–29, Cargese, France*. http://www-igm.univ-mlv.fr/~hivert/PAPER/Cargese.pdf

[98] Florent Hivert, Jean-Christophe Novelli and Jean-Yves Thibon. Commutative combinatorial Hopf algebras. *J. Algebraic Combin.* **28** (2008), no. 1, 65–95. https://doi.org/10.1007/s10801-007-0077-0
Also available as arXiv:math/0605262v1.

[99] ———. The algebra of binary search trees. *Theoret. Comput. Sci.* **339** (2005), no. 1, 129–165. https://doi.org/10.1016/j.tcs.2005.01.012
A preprint appears as arXiv:math/0401089v2.

[100] ———. Trees, functional equations, and combinatorial Hopf algebras. *European J. Combin.* **29** (2008), no. 7, 1682–1695. https://doi.org/10.1016/j.ejc.2007.09.005
A preprint appears as arXiv:math/0701539v1.

[101] Michael E. Hoffman. Combinatorics of rooted trees and Hopf algebras. *Trans. AMS* **355** (2003), 3795–3811. https://doi.org/10.1090/S0002-9947-03-03317-8

[102] ———. A character on the quasi-symmetric functions coming from multiple zeta values. *The Electronic Journal of Combinatorics* **15** (2008), R97. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v15i1r97

[103] Brandon Humpert, and Jeremy L. Martin. The incidence Hopf algebra of graphs. *SIAM Journal on Discrete Mathematics* **26**, no. 2 (2012), 555–570. Also available as arXiv:1012.4786v3.

[104] Gordon James and Martin Liebeck. Representations and characters of groups. 2nd edition, Cambridge University Press, Cambridge-New York, 2001.

[105] Emma Yu Jin. Outside nested decompositions of skew diagrams and Schur function determinants. *European Journal of Combinatorics* **67** (2018), 239–267. https://doi.org/10.1016/j.ejc.2017.08.007 . A preprint is available at http://www.emmayujin.at/Pubs/Jin18.pdf.

[106] S.A. Joni and Gian-Carlo Rota. Coalgebras and bialgebras in combinatorics. *Studies in Applied Mathematics* **61** (1979), 93–139. https://doi.org/10.1002/sapm197961293

[107] Christian Kassel. Quantum groups. *Graduate Texts in Mathematics* **155**. Springer, Berlin, 1995.

[108] Sergei V. Kerov. Asymptotic representation theory of the symmetric group and its applications in analysis. *Translations of Mathematical Monographs* **219**. American Mathematical Society, Providence, RI, 2003.

[109] Anatol N. Kirillov, Arkadiy D. Berenstein. Groups generated by involutions, Gelfand-Tsetlin patterns and the combinatorics of Young tableaux. *Algebra i Analiz* **7** (1995), issue 1, 92–152. A preprint is available at http://pages.uoregon.edu/arkadiy/bk1.pdf

[110] T. Klein. The multiplication of Schur-functions and extensions of p-modules. *J. London Math. Soc.* **43** (1968), 280–284. https://doi.org/10.1112/jlms/s1-43.1.280

[111] Donald E. Knuth. Permutations, matrices, and generalized Young tableaux. *Pacific J. Math.* **34**, Number 3 (1970), 709–727. https://projecteuclid.org/euclid.pjm/1102971948

[112] Donald E. Knuth. The Art of Computer Programming, Volume 4A: Combinatorial Algorithms, Part 1. Pearson 2011. See https://www-cs-faculty.stanford.edu/~knuth/taocp.html for errata.

[113] Donald Knutson. λ-Rings and the Representation Theory of the Symmetric Group. *Lecture Notes in Mathematics* **308**, Springer, Berlin-Heidelberg-New York 1973. https://doi.org/10.1007/BFb0069217

[114] Manfred Krause. A Simple Proof of the Gale-Ryser Theorem. *The American Mathematical Monthly* **103** (1996), 335–337. https://doi.org/10.2307/2975191

[115] Daniel Krob. Eléments de combinatoire. Magistère 1-ère année, Ecole Normale Supérieure, version 1.0, Novembre 1995. http://krob.cesames.net/IMG/ps/combi.ps

[116] Manfred Kufleitner. On Bijective Variants of the Burrows-Wheeler Transform. Presented at the Prague Stringology Conference 2009 (PSC 2009). arXiv:0908.0239v1.

[117] Andrius Kulikauskas, Jeffrey Remmel. Lyndon words and transition matrices between elementary, homogeneous and monomial symmetric functions. *Electronic Journal of Combinatorics* **13** (2006), Research Paper ♯R18. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v13i1r18

[118] Kalle Kytölä. Introduction to Hopf algebras and representations. Lecture notes, Spring 2011. https://math.aalto.fi/~kkytola/files_KK/lectures_files_KK/Hopf-lecture_notes.pdf

[119] Dan Laksov, Alain Lascoux, Piotr Pragacz, and Anders Thorup. The LLPT Notes. Edited by A. Thorup, 1995–2018. http://web.math.ku.dk/noter/filer/sympol.pdf

[120] Thomas Lam, Aaron Lauve, and Frank Sottile. Skew Littlewood-Richardson rules from Hopf Algebras. *DMTCS Proceedings, 22nd International Conference on Formal Power Series and Algebraic Combinatorics (FPSAC 2010)* **2010**, 355–366. A preprint can also be found at arXiv:0908.3714v3.

[121] Thomas Lam, and Pavlo Pylyavskyy. Combinatorial Hopf algebras and K-homology of Grassmanians. *International Mathematics Research Notices*, **2007** (2007), rnm 125, 48 pages. A preprint is arXiv:0705.2189v1.

[122] Sergei K. Lando. On a Hopf Algebra in Graph Theory. *Journal of Combinatorial Theory, Series B* **80** (2000), 104–121. https://doi.org/10.1006/jctb.2000.1973

[123] Aaron D. Lauda, Heather M. Russell. Oddification of the cohomology of type A Springer varieties. *International Math Research Notices* **2014**, No. 17, 4822–4854. A preprint is arXiv:1203.0797v1.

[124] Hartmut Laue. Freie algebraische Strukturen. Lecture notes, Mathematisches Seminar der Universität Kiel 2013, version 16 Sep 2013. http://www.uni-kiel.de/math/algebra/laue/vorlesungen/frei/freiealgstr.pdf

[125] Aaron Lauve and Sarah K. Mason. QSym over Sym has a stable basis. FPSAC 2010, San Francisco, USA. *DMTCS proc. AN* **2010**, 367–378. Also available as arXiv:1003.2124v1.

[126] Marc van Leeuwen. Schur functions and alternating sums. *Electronic Journal of Combinatorics* **11(2)** A5 (2006). Also available at http://www-math.univ-poitiers.fr/~maavl/pdf/alt-Schur.pdf.

[127] Marc van Leeuwen. Flag varieties, and interpretations of Young tableau algorithms. *Journal of Algebra* **224** (2000). Also available at http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/geometry.pdf

[128] Marc van Leeuwen. An application of Hopf-Algebra techniques to representations of finite Classical Groups. *Journal of Algebra* **140**, Issue 1, 15 June 1991, pp. 210–246. Also available at http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/Hopf.pdf

[129] Marc van Leeuwen. The Littlewood-Richardson rule, and related combinatorics. *Math. Soc. of Japan Memoirs* **11**, Interaction of Combinatorics and Representation Theory. Also available at http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/lrr.pdf

[130] Marc van Leeuwen. The Robinson-Schensted and Schützenberger algorithms, an elementary approach. *Electronic Journal of Combinatorics*, Foata Festschrift, **3** (no. 2), R15 (1996). Also available at http://wwwmathlabo.univ-poitiers.fr/~maavl/pdf/foata-fest.pdf

[131] Ji Li. Prime Graphs and Exponential Composition of Species. *Journal of Combinatorial Theory, Series A* **115**, Issue 8, November 2008, 1374–1401. See arXiv:0705.0038v4 for a preprint.

[132] Ricky Ini Liu. A simplified Kronecker rule for one hook shape. *Proc. Amer. Math. Soc.* **145** (2017), pp. 3657–3664. https://doi.org/10.1090/proc/13692 See arXiv:1412.2180v1 for a preprint.

[133] Arunas Liulevicius. Arrows, symmetries and representation rings. *Journal of Pure and Applied Algebra* **19** (1980), 259–273. https://doi.org/10.1016/0022-4049(80)90103-6

[134] Jean-Louis Loday. Cyclic Homology. *Grundlehren der mathematischen Wissenschaften* **301**, 2nd edition, Springer, Berlin-Heidelberg 1998.

[135] Jean-Louis Loday. Série de Hausdorff, idempotents Eulériens et algèbres de Hopf. *Expo. Math.* **12** (1994), 165–178. http://www-irma.u-strasbg.fr/~loday/PAPERS/94Loday%28Eulerien%29.pdf

[136] Jean-Louis Loday and María O. Ronco. Combinatorial Hopf algebras. Quanta of maths, *Clay Math. Proc.* **11**, 347–383, Amer. Math. Soc., Providence, RI, 2010. http://www-irma.u-strasbg.fr/~loday/PAPERS/2011LodayRonco(CHA).pdf

[137] ———. Hopf algebra of the planar binary trees. *Adv. Math.* **139** (1998), no. 2, 293–309. https://doi.org/10.1006/aima.1998.1759

[138] Nicholas A. Loehr. Bijective Combinatorics. CRC Press, 2011. See http://www.math.vt.edu/people/nloehr/bijbook.html for errata.
[139] M. Lothaire. *Combinatorics on words*. Corrected printing, Cambridge University Press, 1997.
[140] Kurt Luoto, Stefan Mykytiuk, Stephanie van Willigenburg. An introduction to quasisymmetric Schur functions – Hopf algebras, quasisymmetric functions, and Young composition tableaux. Springer, May 23, 2013. http://www.math.ubc.ca/~steph/papers/QuasiSchurBook.pdf
[141] R.C. Lyndon. On Burnside's Problem. *Transactions of the AMS* **77**, 202–215. https://doi.org/10.1090/S0002-9947-1954-0064049-X
[142] Ian Grant Macdonald. Symmetric functions and Hall polynomials. 2nd edition, Oxford University Press, Oxford-New York, 1995.
[143] I.G. Macdonald. Schur functions : theme and variations. *Publ. I.R.M.A. Strasbourg*, **1992**, 498/S-27, Actes 28 e Seminaire Lotharingien, 5–39. https://www.emis.de/journals/SLC/opapers/s28macdonald.html
[144] Manuel Maia, Miguel Méndez. On the arithmetic product of combinatorial species. *Discrete Mathematics* **308**, Issue 23, 6 December 2008, 5407–5427. https://doi.org/10.1016/j.disc.2007.09.062 .
See arXiv:math/0503436v2 for a preprint.
[145] Claudia Malvenuto. Produits et coproduits des fonctions quasi-symétriques et de l'algèbre des descents. PhD dissertation, Univ. du Québéc à Montreal, 1993. http://lacim.uqam.ca/wp-content/uploads/Publications/16.pdf
[146] Clauda [sic] Malvenuto and Christophe Reutenauer. Duality between quasi-symmetric functions and the Solomon descent algebra. *J. Algebra* **177** (1995), 967–982. https://doi.org/10.1006/jabr.1995.1336
[147] Claudia Malvenuto and Christophe Reutenauer. Plethysm and conjugation of quasi-symmetric functions. *Discrete Mathematics* **193**, Issues 1–3, 28 November 1998, 225–233. https://doi.org/10.1016/S0012-365X(98)00142-3
[148] Claudia Malvenuto and Christophe Reutenauer. A self paired Hopf algebra on double posets and a Littlewood-Richardson rule. *Journal of Combinatorial Theory, Series A* **118** (2011), 1322–1333. https://doi.org/10.1016/j.jcta.2010.10.010
[149] Dominique Manchon. Hopf algebras, from basics to applications to renormalization. *Comptes Rendus des Rencontres Mathematiques de Glanon* 2001 (published in 2003). arXiv:math/0408405v2.
[150] Marco Manetti. A voyage round coalgebras. 27 June 2016. https://www1.mat.uniroma1.it/people/manetti/dispense/voyage.pdf
[151] Laurent Manivel. Chern classes of tensor products. arXiv:1012.0014v1.
[152] Peter R.W. McNamara, Ryan E. Ward. Equality of P-partition generating functions. arXiv:1210.2412v2.
[153] Pierre-Loïc Méliot. Representation Theory of Symmetric Groups. *Discrete Mathematics and its Applications*, CRC Press 2017.
[154] Anthony Mendes, Jeffrey Remmel. Counting with Symmetric Functions. *Developments in Mathematics* **43**, Springer 2015.
[155] Miguel Mendez. *MathOverflow answer #139482*. http://mathoverflow.net/a/139482/.
[156] John W. Milnor and John C. Moore. On the structure of Hopf algebras. *The Annals of Mathematics, Second Series* **81**, No. 2 (Mar., 1965), 211–264. https://doi.org/10.2307/1970615
[157] Susan Montgomery. Hopf algebras and their actions on rings. *Regional Conference Series in Mathematics* **82**, Amer. Math. Soc., Providence, RI, 2010. https://bookstore.ams.org/cbms-82
[158] Jack Morava. Homotopy-theoretically enriched categories of noncommutative motives. *Research in the Mathematical Sciences* **2** (2015), no. 8. https://doi.org/10.1186/s40687-015-0028-7
[159] Eduardo Moreno. On the theorem of Fredricksen and Maiorana about de Bruijn sequences. *Advances in Applied Mathematics* **33**, Issue 2, August 2004, 413–415. https://doi.org/10.1016/j.aam.2003.10.002
[160] Eduardo Moreno, Dominique Perrin. Corrigendum to "On the theorem of Fredricksen and Maiorana about de Bruijn sequences" [Adv. in Appl. Math. 33 (2) (2004) 413–415]. *Advances in Applied Mathematics* **62**, January 2015, Pages 184–187. http://www.sciencedirect.com/science/article/pii/S0196885814000918
[161] Jeremy L. Martin, Matthew Morin, Jennifer D. Wagner. On distinguishing trees by their chromatic symmetric functions. *Journal of Combinatorial Theory, Series A* **115**, Issue 2, February 2008, 237–253. https://doi.org/10.1016/j.jcta.2007.05.008
[162] Robert Morris. Umbral Calculus and Hopf Algebras. *Contemporary Mathematics* **6**, AMS, Providence 1982. https://bookstore.ams.org/conm-6
[163] Jakob Oesinghaus. Quasisymmetric functions and the Chow ring of the stack of expanded pairs. *Res. Math. Sci.* **6** (2019), no. 5. https://doi.org/10.1007/s40687-018-0168-7 . A preprint is arXiv:1806.10700v1.
[164] James Oxley. Matroid theory. Oxford University Press, Oxford-New York, 1992.
[165] Igor Pak, Alexander Postnikov. Oscillating Tableaux, $S_p \times S_q$-modules, and Robinson-Schensted-Knuth Correspondence. Updated (yet unfinished) version of FPSAC 1996 abstract, January 15, 1994. http://math.mit.edu/~apost/papers/osc.pdf
[166] Frédéric Patras. La décomposition en poids des algèbres de Hopf. *Annales de l'institut Fourier* **43**, no 4 (1993), 1067–1087. https://eudml.org/doc/75026
[167] F. Patras. L'algèbre des descentes d'une bigèbre graduée. *Journal of Algebra* **170** (1994), 547–566. https://doi.org/10.1006/jabr.1994.1352
[168] Frédéric Patras, Christophe Reutenauer. On Dynkin and Klyachko idempotents in graded bialgebras. *Advanced in Applied Mathematics* **28**, Issues 3–4, April 2002, 560–579. https://doi.org/10.1006/aama.2001.0795
[169] Frédéric Patras, Christophe Reutenauer. Higher Lie idempotents. *J. Algebra* **222** (1999), no. 1, 51–64. https://doi.org/10.1006/jabr.1999.7887

[170] Rebecca Patrias. Antipode formulas for combinatorial Hopf algebras. arXiv:1501.00710v2. Published in: *The Electronic Journal of Combinatorics* **23**, Issue 4 (2016), P4.30. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v23i4p30/

[171] Victor Prasolov. Problems and theorems in linear algebra. *Translations of mathematical monographs* **134**, 1st edition 1994, AMS. http://www2.math.su.se/~mleites/books/prasolov-1994-problems.pdf

[172] Stéphane Poirier, Christophe Reutenauer. Algèbres de Hopf de tableaux. *Ann. Sci. Math. Québec* **19** (1995), no. 1, 79–90. http://www.lacim.uqam.ca/~christo/Publi%C3%A9s/1995/Alg%C3%A8bres%20de%20Hopf%20de%20tableaux.pdf

[173] Alexander Postnikov. Permutohedra, associahedra, and beyond. *Int. Math. Res. Notices* **2009**, No. 6, pp. 1026–1106. A preprint appears at https://math.mit.edu/~apost/papers/permutohedron.pdf and as arXiv:math/0507163v1.

[174] Amritanshu Prasad. An Introduction to Schur Polynomials. *Graduate J. Math.* **4** (2019), 62–84. https://www.gradmath.org/wp-content/uploads/2020/01/Prasad-GJM2019.pdf . A preprint appears at arXiv:1802.06073v2.

[175] Pavlo Pylyavskyy. Comparing products of Schur functions and quasisymmetric functions. PhD dissertation, MIT, 2007. https://dspace.mit.edu/handle/1721.1/38957

[176] David E. Radford. Hopf algebras. *Series on Knots and Everything* **49**. World Scientific, 2012. https://doi.org/10.1142/8055

[177] David E. Radford. A Natural Ring Basis for the Shuffle Algebra and an Application to Group Schemes. *Journal of Algebra* **58** (1979), 432–454. https://doi.org/10.1016/0021-8693(79)90171-6

[178] Nathan Reading. Lattice congruences, fans and Hopf algebras. *Journal of Combinatorial Theory, Series A* **110**, Issue 2, May 2005, pp. 237–273. https://doi.org/10.1016/j.jcta.2004.11.001 . A preprint is arXiv:math/0402063v1.

[179] Victor Reiner. Signed permutation statistics and cycle type. *European J. Combin.* **14** (1993), no. 6, 569–579. https://doi.org/10.1006/eujc.1993.1059

[180] Victor Reiner, Kristin M. Shaw, and Stephanie van Willigenburg. Coincidences among skew Schur functions. arXiv:math/0602634v4. (Update of a paper published in *Advances in Mathematics*, **216(1)**:118–152, 2007.)

[181] Jeffrey B. Remmel. The combinatorics of (k,ℓ)-hook Schur functions. In: C. Greene (ed.), *Combinatorics and algebra*, Proceedings of the AMS-IMS-SIAM joint summer research conference in the mathematical sciences on combinatorics and algebra, Colorado, Boulder, 1983, *Contemporary Mathematics* **34**, 1984, 253–287.

[182] Christophe Reutenauer. Free Lie Algebras. *London Mathematical Society Monographs, New Series* **7**. Clarendon Press, Oxford 1993.

[183] Mercedes H. Rosas. The Kronecker Product of Schur Functions Indexed by Two-Row Shapes or Hook Shapes. *Journal of Algebraic Combinatorics* **14** (2001), 153–173. https://doi.org/10.1023/A:1011942029902
A preprint is arXiv:math/0001084v1.

[184] Mercedes H. Rosas, Bruce E. Sagan. Symmetric functions in noncommuting variables. *Transactions of the American Mathematical Society* **358**, 183–214. https://doi.org/10.1090/S0002-9947-04-03623-2

[185] Joseph P.S. Kung, Gian-Carlo Rota. Gian-Carlo Rota on Combinatorics: Introductory Papers and Commentaries. Birkhäuser 1995.

[186] Bruce E. Sagan. The symmetric group: representations, combinatorial algorithms, and symmetric functions. 2nd edition, Springer, New York-Berlin-Heidelberg 2001. See https://users.math.msu.edu/users/bsagan/Books/Sym/errata.pdf for errata.

[187] Bruce E. Sagan. Combinatorics: The Art of Counting. Draft of a textbook, 2020. https://users.math.msu.edu/users/bsagan/Books/Aoc/aocAMS.pdf

[188] Bruce E. Sagan, Richard P. Stanley. Robinson-Schensted Algorithms for Skew Tableaux. *Journal of Combinatorial Theory, Series A* **55** (1990), 161–193. https://doi.org/10.1016/0097-3165(90)90066-6

[189] Steven V. Sam. Notes for Math 740 (Symmetric Functions), 27 April 2017. https://www.math.wisc.edu/~svs/740/notes.pdf

[190] Olivier Schiffmann. Lectures on Hall algebras. arXiv:math/0611617v2.

[191] William R. Schmitt. Incidence Hopf algebras. *Journal of Pure and Applied Algebra* **96** (1994), 299–330. https://doi.org/10.1016/0022-4049(94)90105-8 . A preprint appears at http://home.gwu.edu/~wschmitt/papers/iha.pdf

[192] William R. Schmitt. Antipodes and Incidence Coalgebras. *Journal of Combinatorial Theory, Series A* **46** (1987), 264–290. https://doi.org/10.1016/0097-3165(87)90006-9

[193] William R. Schmitt. Expository notes, specifically "A concrete introduction to category theory" and "Notes on modules and algebras". http://home.gwu.edu/~wschmitt/

[194] ———. Hopf algebras of combinatorial structures. *Canadian Journal of Mathematics* **45** (1993), 412–428. https://doi.org/10.4153/CJM-1993-021-5 . A preprint appears at http://home.gwu.edu/~wschmitt/papers/hacs.pdf

[195] I. Schur. Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung. *Compositio Mathematica* **4** (1937), 432–444. http://www.numdam.org/item?id=CM_1937__4__432_0

[196] Christoph Schweigert. Hopf algebras, quantum groups and topological field theory. Lecture notes, Winter term 2014/15, Hamburg. Version of 16 May 2015. http://www.math.uni-hamburg.de/home/schweigert/ws12/hskript.pdf

[197] Jean-Pierre Serre. Linear representations of finite groups. Springer, Berlin-Heidelberg-New York, 1977. https://doi.org/10.1007/978-1-4684-9458-7

[198] John Shareshian and Michelle L. Wachs. Chromatic quasisymmetric functions and Hessenberg varieties. In: A. Björner, F. Cohen, C. De Concini, C. Procesi, M. Salvetti (Eds.), Configuration Spaces, *Publications of the Scuola Normale Superiore* **14**, Springer, Berlin-Heidelberg-New York 2013. A preprint is arXiv:1106.4287v3.

[199] John Shareshian and Michelle L. Wachs. Chromatic quasisymmetric functions. *Advances in Mathematics* **295** (2016), pp. 497–551. A preprint is arXiv:1405.4629v2.

[200] John Shareshian and Michelle L. Wachs. Eulerian quasisymmetric functions. *Advances in Mathematics* **225** (2010), pp. 2921–2966. https://doi.org/10.1016/j.aim.2010.05.009 . A preprint is arXiv:0812.0764v2

[201] Seth Shelley-Abrahamson. Hopf Modules and Representations of Finite Groups of Lie Type. Honors thesis, Stanford, May 2013. http://mathematics.stanford.edu/wp-content/uploads/2013/08/Shelley-Abrahamson-Honors-Thesis-2013.pdf

[202] Anatolii I. Shirshov. On Free Lie Rings. *Mat. Sbornik N.S.* **45** (87), (1958), no. 2, 113–122. Original at: http://mi.mathnet.ru/msb4963. Translation in: L.A. Bokut, V. Latyshev, I. Shestakov, E. Zelmanov (eds.), *Selected works of A.I. Shirshov*, Birkhäuser 2009.

[203] Richard P. Stanley. Ordered structures and partitions. *Memoirs of the Amer. Math. Soc.* **119**, American Mathematical Society, Providence, R.I., 1972. http://www-math.mit.edu/~rstan/pubs/pubfiles/9.pdf

[204] ———. Acyclic orientations of graphs. *Discrete Math.* **5** (1973), 171–178. Reprinted in: *Discrete Math.* **306** (2006), 905–909. https://doi.org/10.1016/j.disc.2006.03.010

[205] ———. A symmetric function generalization of the chromatic polynomial of a graph. *Adv. Math.* **111** (1995), 166–194. https://doi.org/10.1006/aima.1995.1020

[206] ———. Enumerative Combinatorics, Volumes 1 and 2. *Cambridge Studies in Advanced Mathematics*, **49** and **62**. Cambridge University Press, Cambridge, 2nd edition 2011 (volume 1) and 1st edition 1999 (volume 2).

[207] Shishuo Fu, Victor Reiner, Dennis Stanton, Nathaniel Thiem. The negative q-binomial. *The Electronic Journal of Combinatorics* **19**, Issue 1 (2012), P36. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v19i1p36

[208] R. Steinberg. A geometric approach to the representations of the full linear group over a Galois field. *Trans. Amer. Math. Soc.* **71**, (1951), 274–282. https://doi.org/10.1090/S0002-9947-1951-0043784-0

[209] Jacob Steinhardt. Permutations with Ascending and Descending Blocks. *The Electronic Journal of Combinatorics* **17** (2010), #R14. https://www.combinatorics.org/ojs/index.php/eljc/article/view/v17i1r14

[210] John R. Stembridge. A concise proof of the Littlewood-Richardson rule. *The Electronic Journal of Combinatorics* **9**, 2002, N5. http://www.combinatorics.org/ojs/index.php/eljc/article/view/v9i1n5

[211] John Stembridge. Multiplicity-Free Products of Schur Functions. *Annals of Combinatorics* **5** (2001), 113–121. http://www.math.lsa.umich.edu/~jrs/papers/mfree.ps.gz

[212] Gilbert Strang. The algebra of Elimination. http://www-math.mit.edu/~gs/papers/Paper7_ver8.pdf.

[213] Moss E. Sweedler. Hopf algebras. W.A. Benjamin, New York, 1969.

[214] Mitsuhiro Takeuchi. Free Hopf algebras generated by coalgebras. *J. Math. Soc. Japan* **23** (1971), 561–582. http://projecteuclid.org/euclid.jmsj/1259849779

[215] Harry Tamvakis. The theory of Schur polynomials revisited. *Enseign. Math.* **58** (2012), 147–163. A preprint appears at http://www2.math.umd.edu/~harryt/papers/schurrev.pdf

[216] Jean-Yves Thibon. An Introduction to Noncommutative Symmetric Functions. Cargese lecture, October 2005. J.-P. Gazeau, J. Nesetril, B. Rovan (eds.): From Numbers and Languages to (Quantum) Cryptography, *NATO Security through Science Series: Information and Communication Security* **7**, IOS Press, 2007. Available at http://igm.univ-mlv.fr/~jyt/ARTICLES/cargese_thibon.ps.

[217] Nathaniel Thiem and C. Ryan Vinroot. On the characteristic map of finite unitary groups. *Advances in Mathematics* **210**, Issue 2, 1 April 2007, pp. 707–732. https://doi.org/10.1016/j.aim.2006.07.018 . A preprint is http://www.math.wm.edu/~vinroot/charunitary.pdf

[218] Hugh Thomas, Alexander Yong. An S_3-symmetric Littlewood-Richardson rule. *Math. Res. Lett.* **15** (2008), no. 5, 1027–1037. arXiv:0704.0817v1.

[219] Stijn Vermeeren. Sequences and nets in topology. Version of 11 September 2013. http://stijnvermeeren.be/download/mathematics/nets.pdf

[220] Michelle L. Wachs. Flagged Schur Functions, Schubert Polynomials, and Symmetrizing Operators. *Journal of Combinatorial Theory, Series A* **40** (1985), 276–289. https://doi.org/10.1016/0097-3165(85)90091-3

[221] Bartel Leendert van der Waerden. Algebra, Volume I. Translation of the 7th (German) edition. Springer 2003.

[222] Peter Webb. A Course in Finite Group Representation Theory. 23 February 2016. http://www-users.math.umn.edu/~webb/RepBook/

[223] Mark Wildon. Representation theory of the symmetric group. 5 April 2018. http://www.ma.rhul.ac.uk/~uvah099/teaching.html

[224] Mark Wildon. An involutive introduction to symmetric functions. 8 May 2020. http://www.ma.rhul.ac.uk/~uvah099/teaching.html

[225] Robert Wisbauer. Coalgebras and Bialgebras. *The Egyptian Mathematical Society, The Mathematical Sciences Research Centre (MSRC) Technical Reports* **No. 1**, 2004. http://www.math.uni-duesseldorf.de/~wisbauer/

[226] Qimh Richey Xantcha. Binomial Rings: Axiomatisation, Transfer, and Classification. arXiv:1104.1931v4.

[227] Andrey V. Zelevinsky. Representations of finite classical groups: a Hopf algebra approach. *Lecture Notes in Mathematics* **869**. Springer-Verlag, Berlin-New York, 1981.

[228] Andrey V. Zelevinsky. A Generalization of the Littlewood-Richardson Rule and the Robinson-Schensted-Knuth Correspondence. *Journal of Algebra* **69** (1981), 82–94. https://doi.org/10.1016/0021-8693(81)90128-9

[229] G.-S. Zhou, D.-M. Lu. Lyndon words for Artin-Schelter regular algebras. arXiv:1403.0385v1.

An index goes here!

Email address: darijgrinberg@gmail.com

Drexel University, Korman Center, Room 263, 15 S 33rd Street, Philadelphia PA, 19104, USA // (temporary) Mathematisches Forschungsinstitut Oberwolfach, Schwarzwaldstrasse 9–11, 77709 Oberwolfach, Germany

Email address: reiner@math.umn.edu

School of Mathematics, University of Minnesota, Minneapolis, MN 55455, USA