An Introduction to Algebraic Combinatorics

[Math 701, Spring 2021 lecture notes]

Darij Grinberg

September 11, 2022 (unfinished!)

Contents

1. What is this?

These are the notes for an introductory course on algebraic combinatorics held in the Spring Quarter 2021 at Drexel University[1]. The topics covered are

- formal power series and their use as generating functions (Chapter 3);
- integer partitions and q-binomial coefficients (Chapter 4);
- permutations and their lengths, inversions and cycles (Chapter 5);
- alternating sums, the use of sign-reversing involutions and the combinatorial view on determinants (Chapter 6);
- the basics of symmetric polynomials, particularly Schur polynomials (Chapter 7).

Most (but not all) of these chapters are in a finished state (the final few sections of Chapter 3 need details). However, as these notes have been written within a 3-months window, they are improvable both in detail and in coverage. Some plans for improvement exist, but will likely have to wait for a second iteration of the course. Various topics, such as the matrix-tree theorem or the basis theorems for symmetric polynomials, are slated for eventual inclusion. Errors and confusions will be fixed whenever I become aware of them (any assistance is greatly appreciated![2]).

Exercises of varying difficulty appear at the end of the text (Chapter A).

[1] The website of this course is `https://www.cip.ifi.lmu.de/~grinberg/t/21s/`

[2] Please send comments to `darijgrinberg@gmail.com`

Acknowledgments

Thanks to the students in my Math 701 course for what was in essence an alpha-test of these notes. Some exercises have been adapted from collections by Richard Stanley, Martin Aigner, Donald Knuth, Miklós Bóna, Mark Wildon and Igor Pak. A math.stackexchange user named Mindlack has contributed the proof of Proposition 3.11.26.

2. Before we start...

This is a course on algebraic combinatorics. This subject can be viewed either as a continuation of enumerative combinatorics by other means (specifically, algebraic ones), or as the part of algebra where one studies concrete polynomials (more precisely, families of polynomials). For example, the Schur polynomials (which I think are one of the main stars in this course, but it will take us a while to get to them) can be viewed on the one hand as a tool for enumerating certain kinds of tableaux (essentially, tabular arrangements of numbers that increase along rows and columns), while on the other hand they form a family of polynomials with a myriad surprising properties, generalizing (e.g.) the Vandermonde determinant. I hope to cover both aspects of the subject to a reasonable amount in this course.

To understand this course, you are assumed to speak the language of rings and fields (we will mostly need the basic properties of polynomials and linear maps; we will define what we need about power series), and to have some basic knowledge of enumerative combinatorics (see below). My Math 533 course from Winter 2021 (`http://www.cip.ifi.lmu.de/~grinberg/t/21w/`), and the references I gave therein, can help refresh your knowledge of the former. As for the latter, there are dozens of sources available (I made a list at `https://math.stackexchange.com/a/1454420/` , focussing mostly on texts available online).

We let $\mathbb{N}$ denote the set $\{0, 1, 2, 3, \ldots\}$ of nonnegative integers.

We will need some basics from enumerative combinatorics (see, e.g., [Newste19, §8.1] for details, and [19fco, Chapters 1 and 2] for more details):

- **(addition principle = sum rule)** If A and B are two disjoint sets, then $|A \cup B| = |A| + |B|$.

- **(multiplication principle = product rule)** If A and B are any two sets, then $|A \times B| = |A| \cdot |B|$.

- **(bijection principle)** There is a bijection (= bijective map = invertible map = one-to-one correspondence) between two sets X and Y if and only if $|X| = |Y|$.

- A set with n elements has 2^n subsets, and has $\dbinom{n}{k}$ size-k subsets for any $k \in \mathbb{R}$.
- A set with n elements has $n!$ permutations (= bijective maps from this set to itself).
- **(dependent product rule)** Consider a situation in which you have to make n choices (sequentially). Assume that you have a_1 options available in choice 1, and then (after making choice 1) you have a_2 options available in choice 2 (no matter which option you chose in choice 1), and then (after both choices 1 and 2) you have a_3 options available in choice 3 (no matter which options you chose in choices 1 and 2), and so on. Then, the total # of ways to make all n choices is $a_1 a_2 \cdots a_n$. (This is formalized in [Newste19, Theorem 8.1.19].)

A few words about binomial coefficients are in order:

Definition 2.0.1. For any numbers n and k, we set

$$\binom{n}{k} = \begin{cases} \dfrac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}, & \text{if } k \in \mathbb{N}; \\ 0, & \text{else.} \end{cases} \qquad (1)$$

Note that "numbers" is to be understood fairly liberally here. In particular, n can be any integer, rational, real or complex number (or, more generally, any element in a $\mathbb{Q}$-algebra), whereas k can be anything (although the only nonzero values of $\dbinom{n}{k}$ will be achieved for $k \in \mathbb{N}$, by the above definition).

Example 2.0.2. For any $k \in \mathbb{N}$, we have

$$\begin{aligned} \binom{-1}{k} &= \frac{\left(-1\right)\left(-1-1\right)\left(-1-2\right)\cdots\left(-1-k+1\right)}{k!} \\ &= \frac{\left(-1\right)\left(-2\right)\left(-3\right)\cdots\left(-k\right)}{k!} = \frac{\left(-1\right)^k k!}{k!} = \left(-1\right)^k. \end{aligned}$$

If $n, k \in \mathbb{N}$ and $n \geq k$, then

$$\binom{n}{k} = \frac{n!}{k!\left(n-k\right)!}. \qquad (2)$$

But this formula only applies to the case when $n, k \in \mathbb{N}$ and $n \geq k$. Our above definition is more general than it.

Example 2.0.3. Let $n \in \mathbb{N}$. Then, $\dbinom{2n}{n} = \dfrac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2^n$.

Proof of Example 2.0.3. We have

$$\begin{aligned}(2n)! &= 1 \cdot 2 \cdot \cdots \cdot (2n) \\ &= (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot \underbrace{(2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n))}_{\substack{=(2\cdot 1)\cdot(2\cdot 2)\cdot\cdots\cdot(2\cdot n) \\ =2^n(1\cdot 2\cdot\cdots\cdot n)}} \\ &= (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot 2^n \underbrace{(1 \cdot 2 \cdot \cdots \cdot n)}_{=n!} \\ &= (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot 2^n n!.\end{aligned}$$

Now, (2) yields

$$\begin{aligned}\binom{2n}{n} &= \frac{(2n)!}{n!\,(2n-n)!} = \frac{(2n)!}{n!n!} = \frac{(1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot 2^n n!}{n! \cdot n!} \\ &\qquad \left(\text{since } (2n)! = (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot 2^n n!\right) \\ &= \frac{(1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \cdot 2^n}{n!} = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2^n.\end{aligned}$$

This proves Example 2.0.3. □

Entire books have been written about binomial coefficients and their properties. See [Spivey19] for a recent text (and [GrKnPa94, Chapter 5] and [Grinbe15, Chapter 3] and [Knuth1, §1.2.6] and [Wildon19, Chapter 2] for elementary introductions). Here are two more basic facts that we will need ([19fco, Theorem 1.3.8] and [19fco, Proposition 1.3.6], respectively):

Proposition 2.0.4 (*Pascal's identity*, aka *recurrence of the binomial coefficients*). We have

$$\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n} \tag{3}$$

for any numbers m and n.

Proposition 2.0.5. Let $m, n \in \mathbb{N}$ satisfy $m < n$. Then, $\dbinom{m}{n} = 0$.

Note that Proposition 2.0.5 really requires $m \in \mathbb{N}$. For example, $1.5 < 2$ but $\dbinom{1.5}{2} = 0.375 \neq 0$.

Yet another useful property of the binomial coefficients is the following ([19fco, Theorem 1.3.11]):

Theorem 2.0.6 (*Symmetry of the binomial coefficients*)**.** Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. Then,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Note the $n \in \mathbb{N}$ requirement. Convince yourself that Theorem 2.0.6 would fail for $n = -1$ and $k = 0$.

3. Generating functions

In this first chapter, we will discuss generating functions: first informally, then on a rigorous footing. You may have seen generating functions already, as their usefulness extends far beyond combinatorics; but they are so important to this course that they are worth covering twice in case of doubt.

Rigorous introductions to generating functions (and formal power series in general) can also be found in [Loehr11, Chapter 7 (in the 1st edition)], in [Henric74, Chapter 1], in [Sambal22], and (to some extent) in [19s, Chapter 7].[3] A quick overview is given in [Niven69], and many applications are found in [Wilf09]. There are furthermore numerous books that explore enumerative combinatorics through the lens of generating functions ([GouJac83], [Wagner08], [Lando03] and others).

3.1. Examples

Let me first show what generating functions are good for. Then, starting in the next section, I will explain how to rigorously define them. For now, I will work informally; please suspend your disbelief until the next section.

The **idea** behind generating functions is easy: Any sequence $(a_0, a_1, a_2, \ldots)$ of numbers gives rise to a "power series" $a_0 + a_1 x + a_2 x^2 + \cdots$, which is called the *generating function* of this sequence. This "power series" is an infinite sum (an "infinite polynomial" in an indeterminate x), so it is not immediately clear what it means and what we are allowed to do with it; but before we answer such questions, let us first play around with these power series and hope for the best. The following four examples show how they can be useful.

3.1.1. Example 1: The Fibonacci sequence

Example 1. The *Fibonacci sequence* is the sequence $(f_0, f_1, f_2, \ldots)$ of integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad f_n = f_{n-1} + f_{n-2} \text{ for each } n \geq 2.$$

[3] Bourbaki's [Bourba03, §IV.4] contains what might be the most rigorous and honest treatment of formal power series available in the literature; however, it is not the most readable source, as the notation is dense and heavily relies on other volumes by the same author.

Its entries are known as the *Fibonacci numbers*. Here are the first few of them:

n	0	1	2	3	4	5	6	7	8	9	10	11
f_n	0	1	1	2	3	5	8	13	21	34	55	89

Let us see what we can learn about this sequence by considering its generating function

$$\begin{aligned} F(x) &:= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots \\ &= 0 + 1x + 1x^2 + 2x^3 + 3x^4 + 5x^5 + \cdots . \end{aligned}$$

We have

$$\begin{aligned} F(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \cdots \\ &= \underbrace{0 + 1x}_{=x} + (f_1 + f_0)\, x^2 + (f_2 + f_1)\, x^3 + (f_3 + f_2)\, x^4 + \cdots \\ &\qquad\qquad \left(\text{since } f_0 = 0 \text{ and } f_1 = 1 \text{ and } f_n = f_{n-1} + f_{n-2} \text{ for each } n \geq 2\right) \\ &= x + \underbrace{(f_1 + f_0)\, x^2 + (f_2 + f_1)\, x^3 + (f_3 + f_2)\, x^4 + \cdots}_{\substack{=\left(f_1x^2+f_2x^3+f_3x^4+\cdots\right)+\left(f_0x^2+f_1x^3+f_2x^4+\cdots\right) \\ \text{(here we are hoping that this manipulation of} \\ \text{infinite sums is indeed legitimate)}}} \\ &= x + \underbrace{\left(f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{\substack{=x\left(f_1x+f_2x^2+f_3x^3+\cdots\right) \\ =x(F(x)-f_0)=xF(x) \\ \text{(since } f_0=0\text{)}}} + \underbrace{\left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right)}_{\substack{=x^2\left(f_0+f_1x+f_2x^2+f_3x^3+\cdots\right) \\ =x^2F(x)}} \\ &= x + xF(x) + x^2 F(x) = x + \left(x + x^2\right) F(x) . \end{aligned}$$

Solving this equation for $F(x)$ (assuming that we are allowed to divide by $1 - x - x^2$), we get

$$F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \phi_+ x)(1 - \phi_- x)},$$

where $\phi_+ = \dfrac{1+\sqrt{5}}{2}$ and $\phi_- = \dfrac{1-\sqrt{5}}{2}$ are the two roots of the quadratic polynomial $1 - x - x^2$ (note that ϕ_+ and ϕ_- are sometimes known as the "golden ratios"; we have $\phi_+ \approx 1.618$ and $\phi_- \approx -0.618$). Hence,

$$\begin{aligned} F(x) &= \frac{x}{(1 - \phi_+ x)(1 - \phi_- x)} \\ &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \phi_+ x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \phi_- x} \end{aligned} \tag{4}$$

(by partial fraction decomposition).

Now, what are the coefficients of the power series $\dfrac{1}{1-\alpha x}$ for an $\alpha \in \mathbb{C}$? Let me first answer this question for $\alpha = 1$. Namely, I claim that

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots . \tag{5}$$

Indeed, this follows by observing that

$$\begin{aligned}
&(1-x)\left(1 + x + x^2 + x^3 + \cdots\right) \\
&= \left(1 + x + x^2 + x^3 + \cdots\right) - x\left(1 + x + x^2 + x^3 + \cdots\right) \\
&= \left(1 + x + x^2 + x^3 + \cdots\right) - \left(x + x^2 + x^3 + x^4 + \cdots\right) \\
&= 1
\end{aligned}$$

(again, we are hoping that these manipulations of infinite sums are allowed). Note that the equality (5) is a version of the *geometric series formula* familiar from real analysis. Now, for any $\alpha \in \mathbb{C}$, we can substitute αx for x in the equality (5), and thus obtain

$$\begin{aligned}
\frac{1}{1-\alpha x} &= 1 + \alpha x + (\alpha x)^2 + (\alpha x)^3 + \cdots \\
&= 1 + \alpha x + \alpha^2 x^2 + \alpha^3 x^3 + \cdots .
\end{aligned} \tag{6}$$

Hence, our above formula (4) becomes

$$\begin{aligned}
F(x) &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi_+ x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi_- x} \\
&= \frac{1}{\sqrt{5}} \cdot \left(1 + \phi_+ x + \phi_+^2 x^2 + \phi_+^3 x^3 + \cdots\right) - \frac{1}{\sqrt{5}} \cdot \left(1 + \phi_- x + \phi_-^2 x^2 + \phi_-^3 x^3 + \cdots\right) \\
&\qquad \left(\text{by (6), applied to } \alpha = \phi_+ \text{ and again to } \alpha = \phi_-\right) \\
&= \frac{1}{\sqrt{5}} \sum_{k\geq 0} \phi_+^k x^k - \frac{1}{\sqrt{5}} \sum_{k\geq 0} \phi_-^k x^k \\
&= \sum_{k\geq 0} \left(\frac{1}{\sqrt{5}} \cdot \phi_+^k - \frac{1}{\sqrt{5}} \cdot \phi_-^k\right) x^k .
\end{aligned}$$

Now, for any given $n \in \mathbb{N}$, the coefficient of x^n in the power series on the left hand side of this equality is f_n (since $F(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$), whereas the coefficient of x^n on the right hand side is clearly $\dfrac{1}{\sqrt{5}} \cdot \phi_+^n - \dfrac{1}{\sqrt{5}} \cdot \phi_-^n$.

Thus, comparing coefficients before x^n, we obtain

$$\begin{aligned} f_n &= \frac{1}{\sqrt{5}} \cdot \phi_+^n - \frac{1}{\sqrt{5}} \cdot \phi_-^n \\ &\qquad \left(\begin{array}{c} \text{assuming that "comparing coefficients" is allowed, i.e.,} \\ \text{that equal power series really have equal coefficients} \end{array} \right) \\ &= \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2} \right)^n \end{aligned}$$

for any $n \in \mathbb{N}$. This formula is known as *Binet's formula*. It has many consequences; for example, it implies easily that $\lim\limits_{n\to\infty} \frac{f_{n+1}}{f_n} = \phi_+ = \frac{1+\sqrt{5}}{2} \approx 1.618\ldots$. Thus, $f_n \sim \phi_+^n$ in the asymptotical sense.

3.1.2. Example 2: Dyck words and Catalan numbers

Before the next example, let us address a warmup question: What is the number of $2n$-tuples that contain n entries equal to 0 and n entries equal to 1 ?

(For example, for $n = 2$, these $2n$-tuples are $(1,1,0,0)$, $(1,0,1,0)$, $(1,0,0,1)$, $(0,1,1,0)$, $(0,1,0,1)$, $(0,0,1,1)$, so there are 6 of them.)

Answer: The number is $\binom{2n}{n}$, since choosing a $2n$-tuple that contains n entries equal to 0 and n entries equal to 1 is tantamount to choosing an n-element subset of $\{1,2,\ldots,2n\}$ (and we know that there are $\binom{2n}{n}$ ways to choose the latter).

Example 2. A *Dyck word* of length $2n$ (where $n \in \mathbb{N}$) is a $2n$-tuple that contains n entries equal to 0 and n entries equal to 1, and has the additional property that for each k, we have

$$\begin{aligned} &(\text{\# of 0's among its first } k \text{ entries}) \\ &\leq (\text{\# of 1's among its first } k \text{ entries}). \end{aligned} \tag{7}$$

(The symbol "#" means "number".)

Some examples: The tuples

$$(1,0,1,0), \quad (1,1,0,0), \quad (1,1,0,1,0,0), \quad (), \quad (1,0)$$

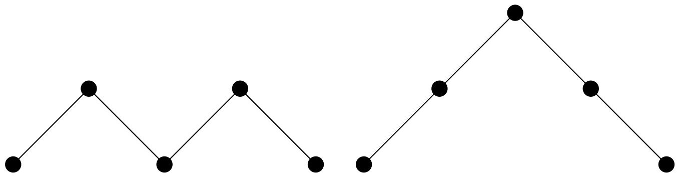
are Dyck words. The tuples

$$(0,1,1,0), \quad (1,0,0,1), \quad (1,1,0), \quad (1), \quad (1,1,1,0)$$

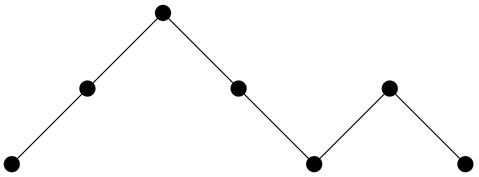
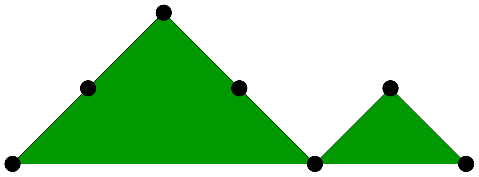
are not Dyck words.

A *Dyck path* is a path from the point $(0,0)$ to the point $(2n,0)$ in the Cartesian plane that moves only using "NE-steps" (i.e., steps of the form $(x,y) \to (x+1,y+1)$) and "SE-steps" (i.e., steps of the form $(x,y) \to (x+1,y-1)$) and never falls below the x-axis (i.e., does not contain any point (x,y) with $y < 0$).

Examples: For $n = 2$, the Dyck paths from $(0,0)$ to $(2n,0)$ are



A Dyck path can be viewed as the "skyline" of a "mountain range". For example:

Dyck path	"mountain range"
	

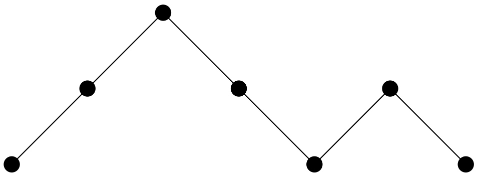
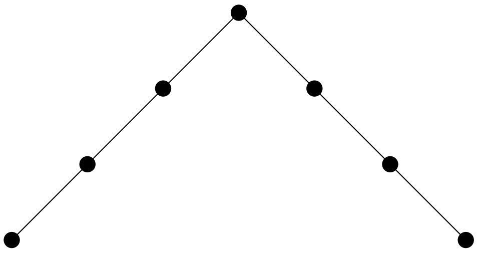
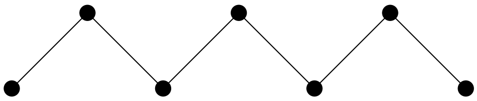
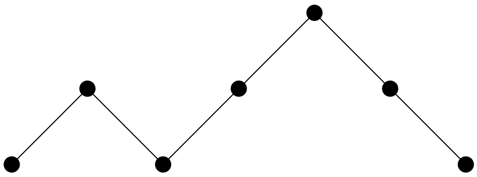
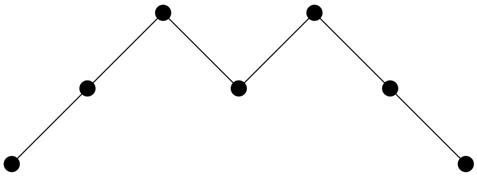
The names "NE-steps" and "SE-steps" in the definition of a Dyck path refer to compass directions: If we treat the Cartesian plane as a map with the x-axis directed eastwards and the y-axis directed northwards, then an NE-step moves to the northeast, and an SE-step moves to the southeast.

Note that any NE-step and any SE-step increases the x-coordinate by 1 (that is, the step goes from a point with x-coordinate k to a point with x-coordinate $k+1$). Thus, any Dyck path from $(0,0)$ to $(2n,0)$ has precisely $2n$ steps. Of these $2n$ steps, exactly n are NE-steps while the remaining n are SE-steps (because any NE-step increases the y-coordinate by 1, while any SE-step decreases the y-coordinate by 1). Since a Dyck path must never fall below the x-axis, we see that the number of SE-steps up to any given point can never be larger than the number of NE-steps up to this point. But this is exactly the condition (7) from the definition of a Dyck word, except that we are talking about NE-steps and SE-steps instead of 1's and 0's. Thus, there is a simple bijection between Dyck words of length $2n$ and Dyck paths $(0,0) \to (2n,0)$:

- send each 1 in the Dyck word to a NE-step in the Dyck path;
- send each 0 in the Dyck word to a SE-step in the Dyck path.

So the # of Dyck words (of length $2n$) equals the # of Dyck paths (from $(0,0)$ to $(2n,0)$). But what is this number?

Example: For $n = 3$, this number is 5. Indeed, here are all Dyck paths from $(0,0)$ to $(6,0)$, and their corresponding Dyck words:

Dyck path	Dyck word
	$(1,1,0,0,1,0)$
	$(1,1,1,0,0,0)$
	$(1,0,1,0,1,0)$
	$(1,0,1,1,0,0)$
	$(1,1,0,1,0,0)$

(We will soon stop writing the commas and parentheses when writing down words. For example, the word $(1,1,0,0,1,0)$ will just become 110010.)

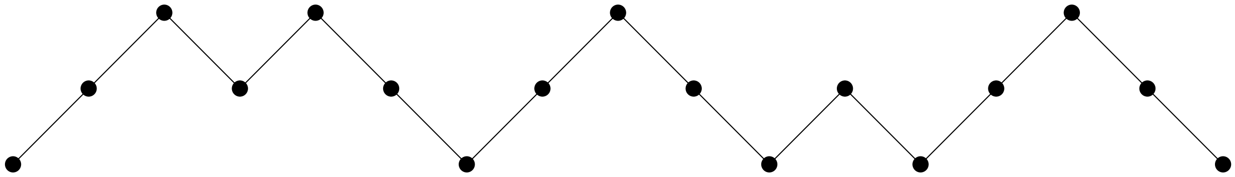
Back to the general question.

For each $n \in \mathbb{N}$, let

$$\begin{aligned} c_n &= (\text{\# of Dyck paths } (0,0) \to (2n,0)) \\ &= (\text{\# of Dyck words of length } 2n) \qquad (\text{as we have seen above}). \end{aligned}$$

Then, $c_0 = 1$ (since the only Dyck path from $(0,0)$ to $(0,0)$ is the trivial path) and $c_1 = 1$ and $c_2 = 2$ and $c_3 = 5$ and $c_4 = 14$ and so on. These numbers c_n are known as the *Catalan numbers*. Entire books have been written about them, such as [Stanle15].

Let us first find a recurrence relation for c_n. The argument below is best understood by following an example; namely, consider the following Dyck path from $(0,0)$ to $(16,0)$ (so the corresponding n is 8):



Fix a positive integer n. If D is a Dyck path from $(0,0)$ to $(2n,0)$, then the *first return* of D (this is short for "first return of D to the x-axis") shall mean the first point on D that lies on the x-axis but is not the origin (i.e., that has the form $(i,0)$ for some integer $i > 0$). For instance, in the example that we just gave, the first return is the point $(6,0)$. If D is a Dyck path from $(0,0)$ to $(2n,0)$, and if $(i,0)$ is its first return, then i is even[4], and therefore we have $i = 2k$ for some $k \in \{1,2,\ldots,n\}$. Hence, for any Dyck path from $(0,0)$ to $(2n,0)$, the first return is a point of the form $(2k,0)$ for some $k \in \{1,2,\ldots,n\}$. Thus,

$$\begin{aligned}&(\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0))\\ &= \sum_{k=1}^{n} (\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0) \text{ whose first return is } (2k,0)).\end{aligned}$$

Now, let us fix some $k \in \{1,2,\ldots,n\}$. We shall compute the # of Dyck paths from $(0,0)$ to $(2n,0)$ whose first return is $(2k,0)$. Any such Dyck path has a natural "two-part" structure: Its first $2k$ steps form a path from $(0,0)$ to $(2k,0)$, while its last (i.e., remaining) $2(n-k)$ steps form a path from $(2k,0)$ to $(2n,0)$. Thus, in order to construct such a path, we

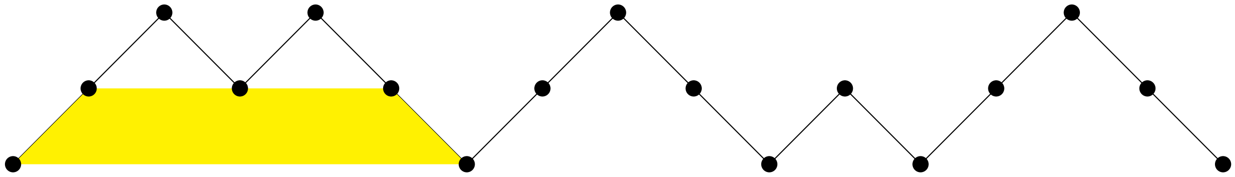
- first choose its first $2k$ steps: They have to form a Dyck path from $(0,0)$ to $(2k,0)$ that never returns to the x-axis until $(2k,0)$. Hence, they begin with a NE-step and end with a SE-step (since any other steps here would cause the path to fall below the x-axis). Between these two steps, the remaining $2k-2 = 2(k-1)$ steps form a path that not only never falls below the x-axis, but also never touches it (since $(2k,0)$ is the first return of our Dyck path, so that our Dyck path does not touch the x-axis between $(0,0)$ and $(2k,0)$). In other words, these $2(k-1)$ steps form a path from $(1,1)$ to $(2k-1,1)$ that never falls below the $y=1$ line (i.e., below the x-axis shifted by 1 upwards). This means that it is a Dyck path from $(0,0)$ to $(2(k-1),0)$ (shifted by $(1,1)$). Thus, there are c_{k-1} possibilities for this path. Hence, there are c_{k-1} choices for the first $2k$ steps of our Dyck path.

[4] *Proof.* The number of NE-steps before the first return must equal the number of SE-steps before the first return (because these steps have altogether taken us from the origin to a point on the x-axis, and thus must have increased and decreased the y-coordinate an equal number of times). This shows that the total number of steps before the first return is even. In other words, i is even (because the total number of steps before the first return is i).

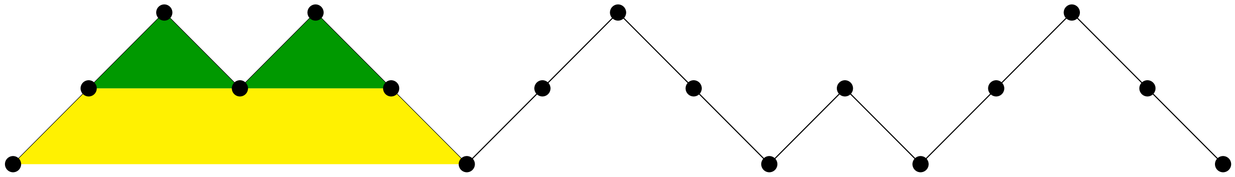
- then choose its last $2(n-k)$ steps: They have to form a path from $(2k,0)$ to $(2(n-k),0)$ that never falls below the x-axis (but is allowed to touch it any number of times). Thus, they form a Dyck path from $(0,0)$ to $(2(n-k),0)$ (shifted by $(2k,0)$). So there are c_{n-k} choices for these last $2(n-k)$ steps.

Thus, there are $c_{k-1}c_{n-k}$ many options for such a Dyck path from $(0,0)$ to $(2n,0)$ (since choosing the first $2k$ steps and choosing the last $2(n-k)$ steps are independent).

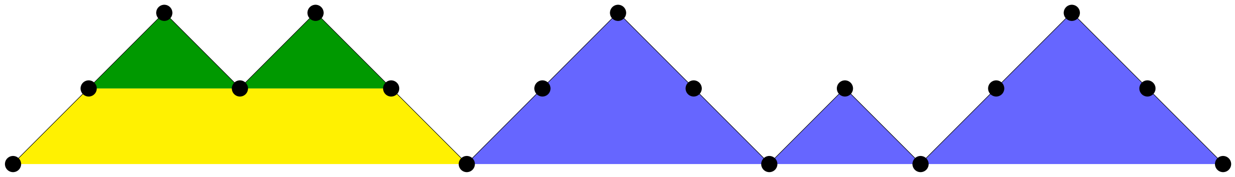
Let me illustrate this reasoning on the Dyck path from $(0,0)$ to $(16,0)$ shown above. This Dyck path has first return $(6,0)$; thus, the corresponding k is 3. Since this Dyck path does not return to the x-axis before $(2k,0)=(6,0)$, its first $2k$ steps stay above the yellow trapezoid shown here:



In particular, the first and the last of these $2k$ steps are uniquely determined, while the steps between them form a diagonally shifted Dyck path that is filled in green here:



Finally, the last $2(n-k)$ steps form a horizontally shifted Dyck path that is filled in purple here:



Our above argument shows that there are c_{k-1} choices for the green Dyck path and c_{n-k} choices for the purple Dyck path, therefore $c_{k-1}c_{n-k}$ options in total.

Forget that we fixed k. Our counting argument above shows that

$$\begin{aligned}&(\#\text{ of Dyck paths from } (0,0) \text{ to } (2n,0) \text{ whose first return is } (2k,0))\\&=c_{k-1}c_{n-k}.\end{aligned} \tag{8}$$

Now,

$$\begin{aligned} c_n &= (\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0)) \\ &= \sum_{k=1}^{n} \underbrace{(\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0) \text{ whose first return is } (2k,0))}_{\substack{=c_{k-1}c_{n-k} \\ \text{(by (8))}}} \\ &= \sum_{k=1}^{n} c_{k-1}c_{n-k} = c_0 c_{n-1} + c_1 c_{n-2} + c_2 c_{n-3} + \cdots + c_{n-1} c_0 . \end{aligned}$$

This is a recurrence equation for c_n. Combining it with $c_0 = 1$, we can use it to compute any value of c_n recursively. Let us, however, try to digest it using generating functions!

Let

$$C(x) := \sum_{n \geq 0} c_n x^n = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots .$$

Thus,

$$\begin{aligned} C(x) &= c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots \\ &= 1 + (c_0 c_0)\, x + (c_0 c_1 + c_1 c_0)\, x^2 + (c_0 c_2 + c_1 c_1 + c_2 c_0)\, x^3 + \cdots \\ &\qquad \left(\begin{array}{c} \text{since } c_0 = 1 \\ \text{and } c_n = c_0 c_{n-1} + c_1 c_{n-2} + c_2 c_{n-3} + \cdots + c_{n-1} c_0 \text{ for each } n > 0 \end{array} \right) \\ &= 1 + x \underbrace{\left((c_0 c_0) + (c_0 c_1 + c_1 c_0)\, x + (c_0 c_2 + c_1 c_1 + c_2 c_0)\, x^2 + \cdots \right)}_{\substack{= \left(c_0 + c_1 x + c_2 x^2 + \cdots\right)^2 \\ \text{(because if we multiply out } \left(c_0 + c_1 x + c_2 x^2 + \cdots\right)^2 \\ \text{and collect like powers of } x \text{, we obtain} \\ \text{exactly } (c_0c_0) + (c_0c_1 + c_1c_0)x + (c_0c_2 + c_1c_1 + c_2c_0)x^2 + \cdots)}} \\ &= 1 + x \Bigg(\underbrace{c_0 + c_1 x + c_2 x^2 + \cdots}_{=C(x)} \Bigg)^2 = 1 + x\,(C(x))^2 . \end{aligned}$$

This is a quadratic equation in $C(x)$. Let us solve it by the quadratic formula (assuming for now that this is allowed – i.e., that the quadratic formula really does apply to our "power series", whatever they are). Thus, we get

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}. \tag{9}$$

The ± sign here cannot be a + sign, because if it was a +, then the power series on top of the fraction would not be divisible by $2x$ (as its constant term would be 2 and thus nonzero[5]). Thus, (9) becomes

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x} = \frac{1}{2x} \left(1 - (1-4x)^{1/2} \right). \tag{10}$$

[5] If you find this unconvincing, here is a cleaner way to argue this: Multiplying the equality

How do we find the coefficients of the power series $\left(1-4x\right)^{1/2}$?
For each $n \in \mathbb{N}$, the binomial formula yields

$$\left(1+x\right)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k\geq 0} \binom{n}{k} x^k. \tag{11}$$

(Here, we have replaced the $\sum\limits_{k=0}^{n}$ sign by a $\sum\limits_{k\geq 0}$ sign, thus extending the summation from all $k \in \{0,1,\ldots,n\}$ to all $k \in \mathbb{N}$. This does not change the value of the sum, since all the newly appearing addends are 0, as you can easily check.)

Let us pretend that the formula (11) holds not only for $n \in \mathbb{N}$, but also for $n = 1/2$. That is, we have

$$\left(1+x\right)^{1/2} = \sum_{k\geq 0} \binom{1/2}{k} x^k. \tag{12}$$

Now, substitute $-4x$ for x in this equality (here we are making the rather plausible assumption that we can substitute $-4x$ for x in a power series); then, we get

$$\begin{aligned}\left(1-4x\right)^{1/2} &= \sum_{k\geq 0} \binom{1/2}{k} \left(-4x\right)^k = \sum_{k\geq 0} \binom{1/2}{k} \left(-4\right)^k x^k \\ &= \underbrace{\binom{1/2}{0}}_{=1} \underbrace{\left(-4\right)^0}_{=1} \underbrace{x^0}_{=1} + \sum_{k\geq 1} \binom{1/2}{k} \left(-4\right)^k x^k \\ &= 1 + \sum_{k\geq 1} \binom{1/2}{k} \left(-4\right)^k x^k.\end{aligned}$$

Hence,

$$1 - \left(1-4x\right)^{1/2} = 1 - \left(1 + \sum_{k\geq 1} \binom{1/2}{k} \left(-4\right)^k x^k\right) = -\sum_{k\geq 1} \binom{1/2}{k} \left(-4\right)^k x^k.$$

(9) by $2x$, we obtain $2xC\left(x\right) = 1 \pm \sqrt{1-4x}$. The left hand side of this equality has constant term 0, but the right hand side has constant term 1 ± 1 (here, we are making the assumption that $\sqrt{1-4x}$ is a power series with constant term 1; this is plausible because $\sqrt{1-4\cdot 0} = 1$ and will also be justified further below). Thus, $0 = 1 \pm 1$; this shows that the ± sign is a $-$ sign.

Thus, (10) becomes

$$\begin{aligned}
C\left(x\right) &= \frac{1}{2x} \underbrace{\left(1-\left(1-4x\right)^{1/2}\right)}_{=-\sum\limits_{k\geq 1}\binom{1/2}{k}\left(-4\right)^k x^k} = \frac{1}{2x}\left(-\sum_{k\geq 1}\binom{1/2}{k}\left(-4\right)^k x^k\right) \\
&= \sum_{k\geq 1}\binom{1/2}{k}\underbrace{\frac{-\left(-4\right)^k x^k}{2x}}_{=2\left(-4\right)^{k-1}x^{k-1}} = \sum_{k\geq 1}\binom{1/2}{k} 2\left(-4\right)^{k-1}x^{k-1} \\
&= \sum_{k\geq 0}\binom{1/2}{k+1} 2\left(-4\right)^{k}x^{k} \\
&\qquad\qquad \left(\text{here, we have substituted } k+1 \text{ for } k \text{ in the sum}\right).
\end{aligned}$$

Comparing coefficients before x^n in this equality gives

$$c_n = \binom{1/2}{n+1} 2\left(-4\right)^n. \tag{13}$$

This is an explicit formula for c_n (and makes computation of c_n pretty easy!), but it turns out that it can be simplified further. Indeed, the definition of $\binom{1/2}{n+1}$ yields

$$\begin{aligned}
\binom{1/2}{n+1} &= \frac{\left(1/2\right)\left(1/2-1\right)\left(1/2-2\right)\cdots\left(1/2-n\right)}{\left(n+1\right)!} \\
&= \frac{\frac{1}{2}\cdot\frac{-1}{2}\cdot\frac{-3}{2}\cdot\frac{-5}{2}\cdot\cdots\cdot\frac{-\left(2n-1\right)}{2}}{\left(n+1\right)!} \\
&= \frac{\left(1\cdot\left(-1\right)\cdot\left(-3\right)\cdot\left(-5\right)\cdot\cdots\cdot\left(-\left(2n-1\right)\right)\right)/2^{n+1}}{\left(n+1\right)!} \\
&= \frac{\left(\left(-1\right)\cdot\left(-3\right)\cdot\left(-5\right)\cdot\cdots\cdot\left(-\left(2n-1\right)\right)\right)/2^{n+1}}{\left(n+1\right)!} \\
&= \frac{\left(-1\right)^n\left(1\cdot 3\cdot 5\cdot\cdots\cdot\left(2n-1\right)\right)/2^{n+1}}{\left(n+1\right)!}.
\end{aligned}$$

Thus, (13) rewrites as

$$\begin{aligned} c_n &= \frac{(-1)^n \left(1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)\right) / 2^{n+1}}{(n+1)!} \cdot 2 \left(-4\right)^n \\ &= \underbrace{\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{(n+1)!}}_{\substack{= \frac{1}{n+1} \cdot \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \\ \text{(since } (n+1)! = (n+1) \cdot n!\text{)}}} \cdot \underbrace{\frac{(-1)^n \cdot 2 \left(-4\right)^n}{2^{n+1}}}_{=2^n} \\ &= \frac{1}{n+1} \cdot \underbrace{\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2^n}_{\substack{= \binom{2n}{n} \\ \text{(by Example 2.0.3)}}} = \frac{1}{n+1} \binom{2n}{n}. \end{aligned}$$

Hence, we have shown that

$$c_n = \frac{1}{n+1} \binom{2n}{n}.$$

Moreover, we can rewrite this further as

$$c_n = \binom{2n}{n} - \binom{2n}{n-1}$$

(since another binomial coefficient manipulation[6] yields $\frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}$).

Here is the upshot: The # of Dyck words of length $2n$ is $c_n = \frac{1}{n+1} \binom{2n}{n}$. In other words, a $2n$-tuple that consists of n entries equal to 0 and n entries equal to 1 (chosen uniformly at random) is a Dyck word with probability $\frac{1}{n+1}$.

(There are also combinatorial ways to prove this; see, e.g., [GrKnPa94, §7.5, discussion at the end of Example 4] or [Stanle15, §1.6] or [Martin13] or [Loehr11, Theorem 1.56][7] or [Spivey19, §8.5, proofs of Identity 244][8].)

[6] See Exercise A.2.1.2 **(a)** for this.

[7] Note that the "Dyck paths" in [Loehr11] differ from ours in that they use N-steps (i.e., steps $(i,j) \mapsto (i, j+1)$) and E-steps (i.e., steps $(i,j) \mapsto (i+1, j)$) instead of NE-steps and SE-steps, and stay above the $x = y$ line instead of above the x-axis. But this notion of Dyck paths is equivalent to ours, since a clockwise rotation by 45° followed by a $\sqrt{2}$-homothety transforms it into ours.

[8] Again, [Spivey19] works not directly with Dyck paths, but rather with paths that use E-steps (i.e., steps $(i,j) \mapsto (i+1, j)$) and N-steps (i.e., steps $(i,j) \mapsto (i, j+1)$) instead of NE-steps and SE-steps, and stay below the $x = y$ line instead of above the x-axis. But this kind of Dyck paths is equivalent to our Dyck paths, since a reflection across the $x = y$ line, followed by a clockwise rotation by 45° followed by a $\sqrt{2}$-homothety transforms it into ours.

Here is a list of the first 12 Catalan numbers c_n:

n	0	1	2	3	4	5	6	7	8	9	10	11
c_n	1	1	2	5	14	42	132	429	1430	4862	16 796	58 786

.

3.1.3. Example 3: The Vandermonde convolution

Example 3: The *Vandermonde convolution identity* (also known as the *Chu–Vandermonde identity*) says that

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k} \qquad \text{for any numbers } a, b \text{ and any } n \in \mathbb{N}$$

(where "numbers" can mean, e.g., "complex numbers").

Let us prove this using generating functions. For now, we shall only prove this for $a, b \in \mathbb{N}$; later I will explain why it also holds for arbitrary (rational, real or complex) numbers a, b as well.

Indeed, fix $a, b \in \mathbb{N}$. Recall (from (11)) that

$$(1+x)^n = \sum_{k \geq 0} \binom{n}{k} x^k$$

for each $n \in \mathbb{N}$. Hence,

$$\begin{aligned}
(1+x)^a &= \sum_{k \geq 0} \binom{a}{k} x^k \qquad \text{and} \\
(1+x)^b &= \sum_{k \geq 0} \binom{b}{k} x^k \qquad \text{and} \\
(1+x)^{a+b} &= \sum_{k \geq 0} \binom{a+b}{k} x^k.
\end{aligned}$$

Thus,

$$\begin{aligned}\underbrace{(1+x)^a}_{=\sum\limits_{k\geq 0}\binom{a}{k}x^k}\quad\underbrace{(1+x)^b}_{=\sum\limits_{k\geq 0}\binom{b}{k}x^k} &= \left(\sum_{k\geq 0}\binom{a}{k}x^k\right)\left(\sum_{k\geq 0}\binom{b}{k}x^k\right)\\ &= \left(\sum_{k\geq 0}\binom{a}{k}x^k\right)\left(\sum_{\ell\geq 0}\binom{b}{\ell}x^\ell\right)\\ &= \sum_{k\geq 0}\ \sum_{\ell\geq 0}\binom{a}{k}x^k\binom{b}{\ell}x^\ell\\ &= \sum_{k\geq 0}\ \sum_{\ell\geq 0}\binom{a}{k}\binom{b}{\ell}x^{k+\ell}\\ &= \sum_{n\geq 0}\left(\sum_{k=0}^{n}\binom{a}{k}\binom{b}{n-k}\right)x^n\end{aligned}$$

(here, we have merged addends in which x appears in the same power). Hence,

$$\begin{aligned}\sum_{n\geq 0}\left(\sum_{k=0}^{n}\binom{a}{k}\binom{b}{n-k}\right)x^n = (1+x)^a(1+x)^b = (1+x)^{a+b} &= \sum_{k\geq 0}\binom{a+b}{k}x^k\\ &= \sum_{n\geq 0}\binom{a+b}{n}x^n.\end{aligned}$$

Comparing coefficients in this equality, we obtain

$$\sum_{k=0}^{n}\binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n} \qquad \text{for each } n\in\mathbb{N}.$$

This completes the proof of the Vandermonde convolution identity for $a,b\in\mathbb{N}$.

3.1.4. Example 4: Solving a recurrence

Example 4. The following example is from [Wilf04, §1.2]. Define a sequence $(a_0, a_1, a_2, \ldots)$ of numbers recursively by

$$a_0 = 1, \qquad a_{n+1} = 2a_n + n \text{ for all } n\geq 0.$$

Thus, the first entries of this sequence are $1, 2, 5, 12, 27, 58, 121, \ldots$. This sequence appears in the OEIS (= Online Encyclopedia of Integer Sequences) as A000325, with index shifted.

Can we find an explicit formula for a_n (without looking it up in the OEIS)?

Again, generating functions are helpful. Set

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots.$$

Then,

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \\ &= 1 + (2a_0 + 0)\,x + (2a_1 + 1)\,x^2 + (2a_2 + 2)\,x^3 + \cdots \\ &\qquad\qquad (\text{since } a_0 = 1 \text{ and } a_{n+1} = 2a_n + n \text{ for all } n \geq 0) \\ &= 1 + 2\underbrace{\left(a_0 x + a_1 x^2 + a_2 x^3 + \cdots\right)}_{=xA(x)} + \underbrace{\left(0x + 1x^2 + 2x^3 + \cdots\right)}_{=x(0+1x+2x^2+3x^3+\cdots)} \\ &= 1 + 2xA(x) + x\left(0 + 1x + 2x^2 + 3x^3 + \cdots\right). \end{aligned} \tag{14}$$

Thus, it would clearly be helpful to find a simple expression for $0 + 1x + 2x^2 + 3x^3 + \cdots$. Here are two ways to do so:

First way: We assume that our power series (whatever they actually are) can be differentiated (as if they were functions). We furthermore assume that these derivatives satisfy the same basic rules (sum rule, product rule, quotient rule, chain rule) as the derivatives in real analysis. (Again, these assumptions shall be justified later on.)

Denoting the derivative of a power series f by f', we then have

$$\left(1 + x + x^2 + x^3 + \cdots\right)' = 1 + 2x + 3x^2 + 4x^3 + \cdots.$$

Hence,

$$1 + 2x + 3x^2 + 4x^3 + \cdots = \left(1 + x + x^2 + x^3 + \cdots\right)' = \left(\frac{1}{1-x}\right)'$$

(since (5) yields $1 + x + x^2 + x^3 + \cdots = \dfrac{1}{1-x}$). Using the quotient rule, we can easily find that $\left(\dfrac{1}{1-x}\right)' = \dfrac{1}{(1-x)^2}$, so that

$$1 + 2x + 3x^2 + 4x^3 + \cdots = \left(\frac{1}{1-x}\right)' = \frac{1}{(1-x)^2}. \tag{15}$$

The left hand side of this looks very similar to the power series $0 + 1x + 2x^2 + 3x^3 + \cdots$ that we want to simplify. And indeed, we have the following:

$$\begin{aligned} 0 + 1x + 2x^2 + 3x^3 + \cdots &= x\underbrace{\left(1 + 2x + 3x^2 + 4x^3 + \cdots\right)}_{=\frac{1}{(1-x)^2}} = x \cdot \frac{1}{(1-x)^2} \\ &= \frac{x}{(1-x)^2}. \end{aligned} \tag{16}$$

Second way: We rewrite $0 + 1x + 2x^2 + 3x^3 + \cdots$ as an infinite sum of infinite sums:

$$\begin{aligned}
&0 + 1x + 2x^2 + 3x^3 + \cdots \\
&= \begin{array}{ccccccccc} x^1 & + & x^2 & + & x^3 & + & x^4 & + & \cdots \\ & + & x^2 & + & x^3 & + & x^4 & + & \cdots \\ & & & + & x^3 & + & x^4 & + & \cdots \\ & & & & & + & x^4 & + & \cdots \\ & & & & & & & \ddots & \ddots \end{array} \\
&= \sum_{k\geq 1} \underbrace{\left(x^k + x^{k+1} + x^{k+2} + \cdots\right)}_{\substack{=x^k \cdot \left(1+x+x^2+x^3+\cdots\right) \\ =x^k \cdot \dfrac{1}{1-x} \\ \text{(by (5))}}} = \sum_{k\geq 1} x^k \cdot \frac{1}{1-x} = \frac{1}{1-x} \cdot \underbrace{\sum_{k\geq 1} x^k}_{\substack{=x^1+x^2+x^3+\cdots \\ =x\cdot\left(1+x+x^2+x^3+\cdots\right) \\ =x\cdot\dfrac{1}{1-x} \\ \text{(by (5))}}} \\
&= \frac{1}{1-x} \cdot x \cdot \frac{1}{1-x} = \frac{x}{(1-x)^2}. \qquad (17)
\end{aligned}$$

(We used some unstated assumptions here about infinite sums – specifically, we assumed that we can rearrange them without worrying about absolute convergence or similar issues – but we will later see that these assumptions are well justified. Besides, we obtained the same result as by our first way, which is reassuring.)

Having computed $0 + 1x + 2x^2 + 3x^3 + \cdots$, we can now simplify (14), obtaining

$$\begin{aligned}
A(x) &= 1 + 2xA(x) + x \underbrace{\left(0 + 1x + 2x^2 + 3x^3 + \cdots\right)}_{=\dfrac{x}{(1-x)^2}} \\
&= 1 + 2xA(x) + x \cdot \frac{x}{(1-x)^2}.
\end{aligned}$$

This is a linear equation in $A(x)$. Solving it yields

$$\begin{aligned}A(x) &= \frac{1-2x+2x^2}{(1-x)^2(1-2x)} \\ &= \underbrace{\frac{2}{1-2x}}_{\substack{=2\sum\limits_{k\geq 0}2^k x^k \\ \text{(by (6))}}} - \underbrace{\frac{1}{(1-x)^2}}_{\substack{=1+2x+3x^2+4x^3+\cdots \\ \text{(by (15), or alternatively} \\ \text{by dividing the} \\ \text{equality (17) by } x)}} \qquad \text{(by partial fraction decomposition)} \\ &= \underbrace{2\sum_{k\geq 0}2^k x^k}_{=\sum\limits_{k\geq 0}2^{k+1}x^k} - \underbrace{\left(1+2x+3x^2+4x^3+\cdots\right)}_{=\sum\limits_{k\geq 0}(k+1)x^k} \\ &= \sum_{k\geq 0}2^{k+1}x^k - \sum_{k\geq 0}(k+1)x^k = \sum_{k\geq 0}\left(2^{k+1}-(k+1)\right)x^k.\end{aligned}$$

Comparing coefficients, we obtain

$$a_n = 2^{n+1} - (n+1) \qquad \text{for each } n \in \mathbb{N}.$$

This is also easy to prove directly (by induction on n).

3.2. Definitions

The four examples above should have convinced you that generating functions can be useful. Thus, it is worthwhile to put them on a rigorous footing by first **defining** generating functions and then **justifying** the manipulations we have been doing to them in the previous section (e.g., dividing them, solving quadratic equations, taking infinite sums, taking derivatives, ...). We are next going to sketch how this can be done (see [Loehr11, Chapter 7 (in the 1st edition)] and [19s, Chapter 7] for some details).

First things first: Generating functions are not actually functions. They are so-called *formal power series* (short *FPSs*). Roughly speaking, a formal power series is a "formal" infinite sum of the form $a_0 + a_1x + a_2x^2 + \cdots$, where x is an "indeterminate" (we shall soon see what this all means). You cannot substitute $x = 2$ into such a power series. (For example, substituting $x = 2$ into $\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$ would lead to the absurd equality $\frac{1}{-1} = 1 + 2 + 4 + 8 + 16 + \cdots$.) The word "function" in "generating function" is somewhat of a historical artifact.

3.2.1. Reminder: Commutative rings

In order to obtain a precise understanding of what FPSs are, we go back to abstract algebra. We begin by recalling the concept of a commutative ring. This is defined in any textbook on abstract algebra for more details, but we recall the definition for the sake of completeness.

Informally, a *commutative ring* is a set K equipped with binary operations $\oplus$, $\ominus$ and $\odot$ and elements $\mathbf{0}$ and $\mathbf{1}$ that "behave" like addition, subtraction and multiplication (of numbers) and the numbers 0 and 1, respectively. For example, they should satisfy rules like $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$.

Formally, commutative rings are defined as follows:

Definition 3.2.1. A *commutative ring* means a set K equipped with three maps

$$\begin{aligned} \oplus &: K \times K \to K, \\ \ominus &: K \times K \to K, \\ \odot &: K \times K \to K \end{aligned}$$

and two elements $\mathbf{0} \in K$ and $\mathbf{1} \in K$ satisfying the following axioms:

1. *Commutativity of addition:* We have $a \oplus b = b \oplus a$ for all $a, b \in K$.

   (Here and in the following, we write the three maps $\oplus$, $\ominus$ and $\odot$ infix – i.e., we denote the image of a pair $(a, b) \in K \times K$ under the map $\oplus$ by $a \oplus b$ rather than by $\oplus (a, b)$.)

2. *Associativity of addition:* We have $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ for all $a, b, c \in K$.

3. *Neutrality of zero:* We have $a \oplus \mathbf{0} = \mathbf{0} \oplus a = a$ for all $a \in K$.

4. *Subtraction undoes addition:* Let $a, b, c \in K$. We have $a \oplus b = c$ if and only if $a = c \ominus b$.

5. *Commutativity of multiplication:* We have $a \odot b = b \odot a$ for all $a, b \in K$.

6. *Associativity of multiplication:* We have $a \odot (b \odot c) = (a \odot b) \odot c$ for all $a, b, c \in K$.

7. *Distributivity:* We have

   $$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c) \qquad \text{and} \qquad (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

   for all $a, b, c \in K$.

8. *Neutrality of one:* We have $a \odot \mathbf{1} = \mathbf{1} \odot a = a$ for all $a \in K$.

9. *Annihilation:* We have $a \odot \mathbf{0} = \mathbf{0} \odot a = \mathbf{0}$ for all $a \in K$.

[**Note:** Most authors do not include $\ominus$ in the definition of a commutative ring, but instead require the existence of additive inverses for all $a \in K$. This is equivalent to our definition, because if additive inverses exist, then we can define $a \ominus b$ to be $a \oplus \overline{b}$ where $\overline{b}$ is the additive inverse of b.]

The operations $\oplus$, $\ominus$ and $\odot$ are called the *addition*, the *subtraction* and the *multiplication* of the ring K. This does not imply that they have any connection with the usual addition, subtraction and multiplication of numbers; it merely means that they play similar roles to the latter and behave similarly. When confusion is unlikely, we will denote these three operations $\oplus$, $\ominus$ and $\odot$ by $+$, $-$ and $\cdot$, respectively, and we will abbreviate $a \odot b = a \cdot b$ by ab.

The elements $\mathbf{0}$ and $\mathbf{1}$ are called the *zero* and the *unity* (or the *one*) of the ring K. Again, this does not imply that they equal the numbers 0 and 1, but merely that they play analogous roles. We will simply call these elements 0 and 1 when confusion with the corresponding numbers is unlikely.

We will use *PEMDAS conventions* for the three operations $\oplus$, $\ominus$ and $\odot$. These imply that the operation $\odot$ has higher precedence than $\oplus$ and $\ominus$, while the operations $\oplus$ and $\ominus$ are left-associative. Thus, for example, "$ab + ac$" means $(ab) + (ac)$ (that is, $(a \odot b) \oplus (a \odot c)$). Likewise, "$a - b + c$" means $(a - b) + c = (a \ominus b) \oplus c$.

Here are some examples of commutative rings:

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are commutative rings. (Of course, the operations $\oplus$, $\ominus$ and $\odot$ of these rings are just the usual operations $+$, $-$ and $\cdot$ known from high school.)

- The set $\mathbb{N}$ is not a commutative ring, since it has no subtraction. (It is, however, something called a *commutative semiring*.)

- The matrix ring $\mathbb{Q}^{m \times m}$ (this is the ring of all $m \times m$-matrices with rational entries) is not a commutative ring for $m > 1$ (because it fails the "commutativity of multiplication" axiom). However, it satisfies all axioms other than "commutativity of multiplication". This makes it a *noncommutative ring*.

- The set
$$\mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$$
is a commutative ring with operations $+$, $-$ and $\cdot$ inherited from $\mathbb{R}$. This is because any $a, b, c, d \in \mathbb{Z}$ satisfy
$$\begin{aligned}\left(a + b\sqrt{5}\right) + \left(c + d\sqrt{5}\right) &= (a + c) + (b + d)\sqrt{5} \in \mathbb{Z}\left[\sqrt{5}\right];\\ \left(a + b\sqrt{5}\right) - \left(c + d\sqrt{5}\right) &= (a - c) + (b - d)\sqrt{5} \in \mathbb{Z}\left[\sqrt{5}\right];\\ \left(a + b\sqrt{5}\right)\left(c + d\sqrt{5}\right) &= (ac + 5bd) + (ad + bc)\sqrt{5} \in \mathbb{Z}\left[\sqrt{5}\right].\end{aligned}$$
This is called a *subring* of $\mathbb{R}$ (i.e., a subset of $\mathbb{R}$ that is closed under the operations $+$, $-$ and $\cdot$ and therefore constitutes a commutative ring with these operations inherited from $\mathbb{R}$).

- For each $m \in \mathbb{Z}$, the set

  $$\begin{aligned} \mathbb{Z}/m &= \{\text{all residue classes modulo } m\} \\ &= \left\{ \begin{array}{c} \text{equivalence classes of integers with respect to} \\ \text{the equivalence ``congruent modulo } m\text{''} \\ \text{(that is, ``differ by a multiple of } m\text{'')} \end{array} \right\} \end{aligned}$$

  is a commutative ring, with its operations defined by

  $$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} - \overline{b} = \overline{a-b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}.$$

  If $m > 0$, then this ring $\mathbb{Z}/m$ is finite and has size m. It is also known as $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}_m$ (careful with the latter notation; it can mean different things to different people). When m is prime, the ring $\mathbb{Z}/m$ is actually a finite field and is called $\mathbb{F}_m$. (But, e.g., the ring $\mathbb{Z}/4$ is not a field, and not the same as $\mathbb{F}_4$.)

- In the examples we have seen so far, the elements of the commutative ring either are numbers or (as in the case of matrices or residue classes) consist of numbers. For a contrast, here is an example where they are sets:

  For any two sets X and Y, we define the *symmetric difference* $X \triangle Y$ of X and Y to be the set

  $$\begin{aligned} &(X \cup Y) \setminus (X \cap Y) = (X \setminus Y) \cup (Y \setminus X) \\ &\qquad\qquad = \{\text{all elements that belong to exactly one of } X \text{ and } Y\}. \end{aligned}$$

  Fix a set S. Consider the power set $\mathcal{P}(S)$ of S (that is, the set of all subsets of S). This power set $\mathcal{P}(S)$ is a commutative ring if we equip it with the operation $\triangle$ as addition (that is, $X \oplus Y = X \triangle Y$ for any subsets X and Y of S), with the same operation $\triangle$ as subtraction (that is, $X \ominus Y = X \triangle Y$), and with the operation $\cap$ as multiplication (that is, $X \odot Y = X \cap Y$), and with the elements $\varnothing$ and S as zero and unity (that is, with $\mathbf{0} = \varnothing$ and $\mathbf{1} = S$). Indeed, it is straightforward to see that all the axioms in Definition 3.2.1 hold for this ring. (For example, distributivity holds because any three sets A, B, C satisfy $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ and $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$.) This is an example of a *Boolean ring* (i.e., a ring in which $aa = a$ for each element a of the ring).

- Here is another example of a semiring, which is rather useful in combinatorics. Let $\mathbb{T}$ be the set $\mathbb{Z} \cup \{-\infty\}$, where $-\infty$ is just some extra symbol. Define two operations $\oplus$ and $\odot$ on this set $\mathbb{T}$ by setting

  $$a \oplus b = \max\{a, b\} \qquad (\text{where } \max\{n, -\infty\} := n \text{ for each } n \in \mathbb{T})$$

and

$$a \odot b = a + b \qquad \text{(where } n + (-\infty) := (-\infty) + n := -\infty \text{ for each } n \in \mathbb{T}\text{)} .$$

Then, $\mathbb{T}$ is a commutative semiring (i.e., it would satisfy Definition 3.2.1 if not for the lack of subtraction). It is called the *tropical semiring* of $\mathbb{Z}$.

More examples can be found in algebra textbooks (or in [Grinbe15, §6.1] or [19s, §5.2] or [21w, Lectures 1 and 2]).

Good news: In any commutative ring K, the standard rules of computation apply:

- You can compute finite sums (of elements of K) without specifying the order of summation or the placement of parentheses. For example, for any $a, b, c, d, e \in K$, we have

  $$((a+b)+(c+d))+e = (a+(b+c))+(d+e),$$

  so you can write the sum $a+b+c+d+e$ without putting parentheses around anything. (This is called "general associativity".)

  Also, finite sums do not depend on the order of addends. For example, for any $a, b, c, d, e \in K$, we have

  $$a+b+c+d+e = d+b+a+e+c.$$

  (This is called "general commutativity".)

  More formally: If $(a_s)_{s \in S}$ is any finite family of elements of a commutative ring K (this means that S is a finite set, and a_s is an element of K for each $s \in S$), then the finite sum

  $$\sum_{s \in S} a_s$$

  is a well-defined element of K. Furthermore, such sums satisfy the usual rules of sums (see [Grinbe15, §1.4.2]); for instance:

  - If $S = X \cup Y$ and $X \cap Y = \varnothing$, then $\sum\limits_{s \in S} a_s = \sum\limits_{s \in X} a_s + \sum\limits_{s \in Y} a_s$.
  - We have $\sum\limits_{s \in S} (a_s + b_s) = \sum\limits_{s \in S} a_s + \sum\limits_{s \in S} b_s$.
  - If S and W are two finite sets, and if $f : S \to W$ is a map, then $\sum\limits_{s \in S} a_s = \sum\limits_{w \in W} \sum\limits_{\substack{s \in S; \\ f(s) = w}} a_s$. (That is, you can subdivide a finite sum into a finite sum of finite sums by bunching its addends arbitrarily.)

  (See [Grinbe15, §2.14] for very detailed proofs[9]. Alternatively, you can treat them as exercises on induction.)

[9] These proofs are stated for numbers rather than elements of an arbitrary commutative ring K, but the exact same reasoning works in an arbitrary ring K.

If $S = \varnothing$, then $\sum\limits_{s \in S} a_s = 0$ by definition. Such a sum $\sum\limits_{s \in S} a_s$ with $S = \varnothing$ is called an empty sum.

- The same holds for finite products. If $S = \varnothing$, then $\prod\limits_{s \in S} a_s = 1$ by definition.
- If $a \in K$, then $-a$ denotes $0 - a = \mathbf{0} - a \in K$.
- If $n \in \mathbb{Z}$ and $a \in K$, then we can define an element $na \in K$ by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ times}} \right), & \text{if } n < 0. \end{cases}$$

  This generalizes the classical definition of multiplication (for integers) as repeated addition.

- If $n \in \mathbb{N}$ and $a \in K$, then we can define an element

$$a^n = \underbrace{aa \cdots a}_{n \text{ times}} \in K.$$

  In particular, $a^0 = \underbrace{aa \cdots a}_{0 \text{ times}} = 1$ (since an empty product is always 1).

- Standard rules hold:

$$\begin{aligned} -(a+b) &= (-a) + (-b) && \text{for any } a, b \in K; \\ -(-a) &= a && \text{for any } a \in K; \\ (n+m)\,a &= na + ma && \text{for any } a \in K \text{ and } n, m \in \mathbb{Z}; \\ (nm)\,a &= n\,(ma) && \text{for any } a \in K \text{ and } n, m \in \mathbb{Z}; \\ a\,(b-c) &= (ab) - (ac) && \text{for any } a, b, c \in K; \\ (ab)^n &= a^n b^n && \text{for any } a, b \in K \text{ and } n \in \mathbb{N}; \\ a^{n+m} &= a^n a^m && \text{for any } a \in K \text{ and } n, m \in \mathbb{N}; \\ a^{nm} &= (a^n)^m && \text{for any } a \in K \text{ and } n, m \in \mathbb{N}; \\ &\ldots; \\ (a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} && \text{for any } a, b \in K \text{ and } n \in \mathbb{N}. \end{aligned}$$

  (The latter equality is known as the *binomial theorem* or *binomial formula*.)

A further concept will be useful. Namely, if K is a commutative ring, then the notion of a K*-module* is the straightforward generalization of the concept of a K-vector space to cases where K is not a field (but just a commutative ring). Here is the definition of a K-module in detail:

Definition 3.2.2. Let K be a commutative ring.

A *K-module* means a set M equipped with three maps

$$\begin{aligned} \oplus &: M \times M \to M, \\ \ominus &: M \times M \to M, \\ \rightharpoonup &: K \times M \to M \end{aligned}$$

(notice that the third map has domain $K \times M$, not $M \times M$) and an element $\overrightarrow{0} \in M$ satisfying the following axioms:

1. *Commutativity of addition:* We have $a \oplus b = b \oplus a$ for all $a, b \in M$.

   (Here and in the following, we write the three maps $\oplus$, $\ominus$ and $\rightharpoonup$ infix, just as for a commutative ring.)

2. *Associativity of addition:* We have $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ for all $a, b, c \in M$.

3. *Neutrality of zero:* We have $a \oplus \overrightarrow{0} = \overrightarrow{0} \oplus a = a$ for all $a \in M$.

4. *Subtraction undoes addition:* Let $a, b, c \in M$. We have $a \oplus b = c$ if and only if $a = c \ominus b$.

5. *Associativity of scaling:* We have $u \rightharpoonup (v \rightharpoonup a) = (uv) \rightharpoonup a$ for all $u, v \in K$ and $a \in M$.

6. *Left distributivity:* We have $u \rightharpoonup (a \oplus b) = (u \rightharpoonup a) \oplus (u \rightharpoonup b)$ for all $u \in K$ and $a, b \in M$.

7. *Right distributivity:* We have $(u + v) \rightharpoonup a = (u \rightharpoonup a) \oplus (v \rightharpoonup a)$ for all $u, v \in K$ and $a \in M$.

8. *Neutrality of one:* We have $1 \rightharpoonup a = a$ for all $a \in M$.

9. *Left annihilation:* We have $0 \rightharpoonup a = \overrightarrow{0}$ for all $a \in M$.

10. *Right annihilation:* We have $u \rightharpoonup \overrightarrow{0} = \overrightarrow{0}$ for all $u \in K$.

[**Note:** Most authors do not include $\ominus$ in the definition of a K-module, but instead require the existence of additive inverses for all $a \in M$. Just as for commutative rings, this is equivalent.]

The operations $\oplus$, $\ominus$ and $\rightharpoonup$ are called the *addition*, the *subtraction* and the *scaling* (or the *K-action*) of the K-module M. When confusion is unlikely, we will denote these three operations $\oplus$, $\ominus$ and $\rightharpoonup$ by $+$, $-$ and $\cdot$, respectively, and we will abbreviate $a \rightharpoonup b = a \cdot b$ by ab.

The element $\overrightarrow{0}$ is called the *zero* (or the *zero vector*) of the K-module M. We will usually just call it 0.

When M is a K-module, the elements of M are called *vectors*, while the elements of K are called *scalars*.

We will use *PEMDAS conventions* for the three operations $\oplus$, $\ominus$ and $\rightharpoonup$, with the operation $\rightharpoonup$ having higher precedence than $\oplus$ and $\ominus$.

This all having been said, we can now define formal power series.

3.2.2. The definition of formal power series

Until the end of Chapter 3, the following convention will be in place:

Convention 3.2.3. Fix a commutative ring K. (For example, K can be $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{C}$.)

Definition 3.2.4. A *formal power series* (or, short, *FPS*) in 1 indeterminate over K means a sequence $(a_0, a_1, a_2, \ldots) = (a_n)_{n \in \mathbb{N}} \in K^{\mathbb{N}}$ of elements of K.

Examples of FPSs over $\mathbb{Z}$ are $(0, 0, 0, \ldots)$ and $(1, 0, 0, 0, \ldots)$ and $(1, 1, 1, 1, \ldots)$ and $(1, 2, 3, 4, \ldots)$.

Definition 3.2.4 technically answers the question "what is an FPS"; however, the questions "what can we do with an FPS" and "why do the examples in Section 3.1 work" or "what is x" remain open. These questions will take us a while.

First, let us define some operations on FPSs.

Definition 3.2.5. (a) The *sum* of two FPSs $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$ is defined to be the FPS

$$(a_0 + b_0,\ \ a_1 + b_1,\ \ a_2 + b_2,\ \ \ldots).$$

It is denoted by $\mathbf{a} + \mathbf{b}$.

(b) The *difference* of two FPSs $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$ is defined to be the FPS

$$(a_0 - b_0,\ \ a_1 - b_1,\ \ a_2 - b_2,\ \ \ldots).$$

It is denoted by $\mathbf{a} - \mathbf{b}$.

(c) If $\lambda \in K$ and if $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ is an FPS, then we define an FPS

$$\lambda \mathbf{a} := (\lambda a_0, \lambda a_1, \lambda a_2, \ldots).$$

(d) The *product* of two FPSs $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ and $\mathbf{b} = (b_0, b_1, b_2, \ldots)$ is defined to be the FPS $(c_0, c_1, c_2, \ldots)$, where

$$\begin{aligned} c_n &= \sum_{i=0}^{n} a_i b_{n-i} = \sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}} a_i b_j \\ &= a_0 b_n + a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0 \qquad \text{for each } n \in \mathbb{N}. \end{aligned}$$

This product is denoted by $\mathbf{a} \cdot \mathbf{b}$ or just by $\mathbf{ab}$.

(e) For each $a \in K$, we define $\underline{a}$ to be the FPS $(a, 0, 0, 0, \ldots)$. An FPS of the form $\underline{a}$ for some $a \in K$ (that is, an FPS $(a_0, a_1, a_2, \ldots)$ satisfying $a_1 = a_2 = a_3 = \cdots = 0$) is said to be *constant*.

(f) The set of all FPSs (in 1 indeterminate over K) is denoted $K[[x]]$.

The following theorem is crucial: essentially it says that the operations on FPSs that we have just defined behave as such operations should:

Theorem 3.2.6. **(a)** The set $K[[x]]$ is a commutative ring (with its operations $+$, $-$ and $\cdot$ defined in Definition 3.2.5). Its zero and its unity are the FPSs $\underline{0} = (0, 0, 0, \ldots)$ and $\underline{1} = (1, 0, 0, 0, \ldots)$. This means, concretely, that the following facts hold:

1. *Commutativity of addition:* We have $\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}$ for all $\mathbf{a}, \mathbf{b} \in K[[x]]$.

2. *Associativity of addition:* We have $\mathbf{a} + (\mathbf{b} + \mathbf{c}) = (\mathbf{a} + \mathbf{b}) + \mathbf{c}$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K[[x]]$.

3. *Neutrality of zero:* We have $\mathbf{a} + \underline{0} = \underline{0} + \mathbf{a} = \mathbf{a}$ for all $\mathbf{a} \in K[[x]]$.

4. *Subtraction undoes addition:* Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K[[x]]$. We have $\mathbf{a} + \mathbf{b} = \mathbf{c}$ if and only if $\mathbf{a} = \mathbf{c} - \mathbf{b}$.

5. *Commutativity of multiplication:* We have $\mathbf{ab} = \mathbf{ba}$ for all $\mathbf{a}, \mathbf{b} \in K[[x]]$.

6. *Associativity of multiplication:* We have $\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c}$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K[[x]]$.

7. *Distributivity:* We have
$$\mathbf{a}(\mathbf{b} + \mathbf{c}) = \mathbf{ab} + \mathbf{ac} \qquad \text{and} \qquad (\mathbf{a} + \mathbf{b})\mathbf{c} = \mathbf{ac} + \mathbf{bc}$$
for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K[[x]]$.

8. *Neutrality of one:* We have $\mathbf{a} \cdot \underline{1} = \underline{1} \cdot \mathbf{a} = \mathbf{a}$ for all $\mathbf{a} \in K[[x]]$.

9. *Annihilation:* We have $\mathbf{a} \cdot \underline{0} = \underline{0} \cdot \mathbf{a} = \underline{0}$ for all $\mathbf{a} \in K[[x]]$.

(b) Furthermore, $K[[x]]$ is a K-module (with its scaling being the map that sends each $(\lambda, \mathbf{a}) \in K \times K[[x]]$ to the FPS $\lambda\mathbf{a}$ defined in Definition 3.2.5 **(c)**). Its zero vector is $\underline{0}$. Concretely, this means that:

10. *Associativity of scaling:* We have $\lambda(\mu\mathbf{a}) = (\lambda\mu)\mathbf{a}$ for all $\lambda, \mu \in K$ and $\mathbf{a} \in K[[x]]$.

11. *Left distributivity:* We have $\lambda(\mathbf{a} + \mathbf{b}) = \lambda\mathbf{a} + \lambda\mathbf{b}$ for all $\lambda \in K$ and $\mathbf{a}, \mathbf{b} \in K[[x]]$.

12. *Right distributivity:* We have $(\lambda + \mu)\,\mathbf{a} = \lambda\mathbf{a} + \mu\mathbf{a}$ for all $\lambda, \mu \in K$ and $\mathbf{a} \in K[[x]]$.

13. *Neutrality of one:* We have $1\mathbf{a} = \mathbf{a}$ for all $\mathbf{a} \in K[[x]]$.

14. *Left annihilation:* We have $0\mathbf{a} = \underline{0}$ for all $\mathbf{a} \in K[[x]]$.

15. *Right annihilation:* We have $\lambda\underline{0} = \underline{0}$ for all $\lambda \in K$.

(Also, some of the facts from part **(a)** are included in this statement.)
(c) We have $\lambda(\mathbf{a} \cdot \mathbf{b}) = (\lambda\mathbf{a}) \cdot \mathbf{b} = \mathbf{a} \cdot (\lambda\mathbf{b})$ for all $\lambda \in K$ and $\mathbf{a}, \mathbf{b} \in K[[x]]$.
(d) Finally, we have $\lambda\mathbf{a} = \underline{\lambda} \cdot \mathbf{a}$ for all $\lambda \in K$ and $\mathbf{a} \in K[[x]]$.

Theorem 3.2.6 allows us to calculate with FPSs as we do with numbers, at least as far as the operations $+$, $-$ and $\cdot$ are concerned. Hence, e.g., we know that:

- Sums and products in $K[[x]]$ need no parentheses and do not depend on the order of addends/factors. For example, for any $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in K[[x]]$, we have $((\mathbf{ab})\,\mathbf{c})\,\mathbf{d} = \mathbf{a}((\mathbf{bc})\,\mathbf{d}) = (\mathbf{ab})(\mathbf{cd})$, so that we can write $\mathbf{abcd}$ for each of these products; and moreover, we have $\mathbf{abcd} = \mathbf{bdac} = \mathbf{dacb}$.

- Finite sums and products (such as $\sum\limits_{i=1}^{k} \mathbf{a}_i$ or $\sum\limits_{i \in I} \mathbf{a}_i$ or $\prod\limits_{i=1}^{k} \mathbf{a}_i$ or $\prod\limits_{i \in I} \mathbf{a}_i$, where I is a finite set) make sense and behave as one would expect.

- Powers exist: that is, you can take $\mathbf{a}^n$ for each FPS $\mathbf{a}$ and each $n \in \mathbb{N}$.

- Standard rules hold: e.g., we have $\mathbf{a}^{n+m} = \mathbf{a}^n\mathbf{a}^m$ and $(\mathbf{ab})^n = \mathbf{a}^n\mathbf{b}^n$ for any $\mathbf{a}, \mathbf{b} \in K[[x]]$ and any $n, m \in \mathbb{N}$.

- The binomial theorem holds: For any $\mathbf{a}, \mathbf{b} \in K[[x]]$ and any $n \in \mathbb{N}$, we have
$$(\mathbf{a} + \mathbf{b})^n = \sum_{k=0}^{n} \binom{n}{k} \mathbf{a}^k \mathbf{b}^{n-k}.$$

Before we prove Theorem 3.2.6, we introduce one more notation:

Definition 3.2.7. If $n \in \mathbb{N}$, and if $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in K[[x]]$ is an FPS, then we define an element $[x^n]\,\mathbf{a} \in K$ by
$$[x^n]\,\mathbf{a} := a_n.$$

This is called the *coefficient of x^n in* $\mathbf{a}$, or the *n-th coefficient* of $\mathbf{a}$, or the *x^n-coefficient* of $\mathbf{a}$.

Thus, the definition of the sum of two FPSs (Definition 3.2.5 **(a)**) rewrites as follows: For any $\mathbf{a}, \mathbf{b} \in K[[x]]$ and any $n \in \mathbb{N}$, we have

$$[x^n](\mathbf{a}+\mathbf{b}) = [x^n]\mathbf{a} + [x^n]\mathbf{b}. \tag{18}$$

Similarly, for any $\mathbf{a}, \mathbf{b} \in K[[x]]$ and any $n \in \mathbb{N}$, we have

$$[x^n](\mathbf{a}-\mathbf{b}) = [x^n]\mathbf{a} - [x^n]\mathbf{b}. \tag{19}$$

Meanwhile, the definition of the product of two FPSs (Definition 3.2.5 **(d)**) rewrites as follows: For any $\mathbf{a}, \mathbf{b} \in K[[x]]$ and any $n \in \mathbb{N}$, we have

$$\begin{aligned}
&[x^n](\mathbf{ab}) \\
&= \left[x^0\right]\mathbf{a}\cdot[x^n]\mathbf{b} + \left[x^1\right]\mathbf{a}\cdot\left[x^{n-1}\right]\mathbf{b} + \left[x^2\right]\mathbf{a}\cdot\left[x^{n-2}\right]\mathbf{b} + \cdots + [x^n]\mathbf{a}\cdot\left[x^0\right]\mathbf{b} \\
&= \sum_{i=0}^{n}\left[x^i\right]\mathbf{a}\cdot\left[x^{n-i}\right]\mathbf{b} && (20) \\
&= \sum_{j=0}^{n}\left[x^{n-j}\right]\mathbf{a}\cdot\left[x^j\right]\mathbf{b} && (21)
\end{aligned}$$

(here, we have substituted $n-j$ for i in the sum). For $n=0$, this equality simplifies to

$$\left[x^0\right](\mathbf{ab}) = \left[x^0\right]\mathbf{a}\cdot\left[x^0\right]\mathbf{b}. \tag{22}$$

In other words, when we multiply two FPSs, their constant terms get multiplied. Here and in the following, the *constant term* of an FPS $\mathbf{a} \in K[[x]]$ is defined to be its 0-th coefficient $\left[x^0\right]\mathbf{a}$.

Finally, Definition 3.2.5 **(c)** rewrites as follows: For any $\lambda \in K$ and $\mathbf{a} \in K[[x]]$ and any $n \in \mathbb{N}$, we have

$$[x^n](\lambda\mathbf{a}) = \lambda\cdot[x^n]\mathbf{a}. \tag{23}$$

Proof of Theorem 3.2.6. Most parts of Theorem 3.2.6 are straightforward to verify. Let us check the associativity of multiplication.

Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K[[x]]$. We must prove that $\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c}$. Let $n \in \mathbb{N}$. Consider the two equalities

$$\begin{aligned}
[x^n]((\mathbf{ab})\mathbf{c}) &= \sum_{j=0}^{n} \underbrace{\left[x^{n-j}\right](\mathbf{ab})}_{\substack{=\sum_{i=0}^{n-j}\left[x^i\right]\mathbf{a}\cdot\left[x^{n-j-i}\right]\mathbf{b} \\ \text{(by (20),} \\ \text{applied to } n-j \text{ instead of } n)}} \cdot \left[x^j\right]\mathbf{c} \\
&\qquad \left(\begin{array}{c}\text{by (21), applied to } \mathbf{ab} \text{ and } \mathbf{c} \\ \text{instead of } \mathbf{a} \text{ and } \mathbf{b}\end{array}\right) \\
&= \sum_{j=0}^{n}\left(\sum_{i=0}^{n-j}\left[x^i\right]\mathbf{a}\cdot\left[x^{n-j-i}\right]\mathbf{b}\right)\cdot\left[x^j\right]\mathbf{c} = \sum_{j=0}^{n}\sum_{i=0}^{n-j}\left[x^i\right]\mathbf{a}\cdot\left[x^{n-j-i}\right]\mathbf{b}\cdot\left[x^j\right]\mathbf{c}
\end{aligned}$$

and

$$\left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right) = \sum_{i=0}^{n} \left[x^i\right] \mathbf{a} \cdot \underbrace{\left[x^{n-i}\right]\left(\mathbf{bc}\right)}_{\substack{=\sum_{j=0}^{n-i}\left[x^{n-i-j}\right]\mathbf{b}\cdot\left[x^j\right]\mathbf{c} \\ \text{(by (21), applied to } n-i-j,\ \mathbf{b} \text{ and } \mathbf{c} \\ \text{instead of } n,\ \mathbf{a} \text{ and } \mathbf{b})}}$$

$$\text{(by (20), applied to } \mathbf{bc} \text{ instead of } \mathbf{b})$$

$$= \sum_{i=0}^{n} \left[x^i\right] \mathbf{a} \cdot \left(\sum_{j=0}^{n-i} \left[x^{n-i-j}\right] \mathbf{b} \cdot \left[x^j\right] \mathbf{c}\right) = \sum_{i=0}^{n}\sum_{j=0}^{n-i} \left[x^i\right] \mathbf{a} \cdot \left[x^{n-i-j}\right] \mathbf{b} \cdot \left[x^j\right] \mathbf{c}.$$

The right hand sides of these two equalities are equal, since[10]

$$\sum_{j=0}^{n}\sum_{i=0}^{n-j} = \sum_{\substack{(i,j)\in\mathbb{N}^2; \\ i+j\leq n}} = \sum_{i=0}^{n}\sum_{j=0}^{n-i}$$

and $n-j-i = n-i-j$. Thus, their left hand sides are equal as well. In other words,

$$\left[x^n\right]\left(\left(\mathbf{ab}\right)\mathbf{c}\right) = \left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right).$$

Now, forget that we fixed n. We thus have shown that $\left[x^n\right]\left(\left(\mathbf{ab}\right)\mathbf{c}\right) = \left[x^n\right]\left(\mathbf{a}\left(\mathbf{bc}\right)\right)$ for each $n \in \mathbb{N}$. In other words, each entry of $\left(\mathbf{ab}\right)\mathbf{c}$ equals the corresponding entry of $\mathbf{a}\left(\mathbf{bc}\right)$. This entails $\left(\mathbf{ab}\right)\mathbf{c} = \mathbf{a}\left(\mathbf{bc}\right)$ (since a FPS is just the sequence of its entries). In other words, $\mathbf{a}\left(\mathbf{bc}\right) = \left(\mathbf{ab}\right)\mathbf{c}$. This concludes the proof of associativity of multiplication.

The remaining claims of Theorem 3.2.6 are LTTR[11] (their proofs follow the same pattern, but are easier to execute). □

Since $K\left[\left[x\right]\right]$ is a commutative ring, any finite sum of FPSs is well-defined. Sometimes, however, infinite sums of FPSs make sense as well: for example, it stands to reason that

$$\begin{aligned} &\left(1,1,1,1,\ldots\right) \\ &+\left(0,1,1,1,\ldots\right) \\ &+\left(0,0,1,1,\ldots\right) \\ &+\left(0,0,0,1,\ldots\right) \\ &+\cdots \\ &=\left(1,2,3,4,\ldots\right), \end{aligned} \tag{24}$$

[10] The first equality we are about to state is an equality of summation signs. Such an equality means that whatever you put inside the summation signs, they produce equal results. For example, $\sum\limits_{i\in\{1,2,3\}} = \sum\limits_{i=1}^{3}$ and $\sum\limits_{i\in\mathbb{N}} = \sum\limits_{i\geq 0}$.

[11] "LTTR" means "left to the reader".

because FPSs are added entrywise. Let us rigorously define such sums. First, we define "essentially finite" sums of elements of K:

> **Definition 3.2.8.** **(a)** A family $(a_i)_{i \in I} \in K^I$ of elements of K is said to be *essentially finite* if all but finitely many $i \in I$ satisfy $a_i = 0$ (in other words, if the set $\{i \in I \mid a_i \neq 0\}$ is finite).
>
> **(b)** Let $(a_i)_{i \in I} \in K^I$ be an essentially finite family of elements of K. Then, the infinite sum $\sum\limits_{i \in I} a_i$ is defined to equal the finite sum $\sum\limits_{\substack{i \in I; \\ a_i \neq 0}} a_i$. Such an infinite sum is said to be *essentially finite*.

For example, the family $\left(\left\lfloor \dfrac{5}{2^n} \right\rfloor \right)_{n \in \mathbb{N}}$ of integers is essentially finite[12], and its sum is

$$\sum_{n \in \mathbb{N}} \left\lfloor \frac{5}{2^n} \right\rfloor = \left\lfloor \frac{5}{2^0} \right\rfloor + \left\lfloor \frac{5}{2^1} \right\rfloor + \left\lfloor \frac{5}{2^2} \right\rfloor + \left\lfloor \frac{5}{2^3} \right\rfloor + \left\lfloor \frac{5}{2^4} \right\rfloor + \cdots$$
$$= 5 + 2 + 1 + \underbrace{0 + 0 + 0 + \cdots}_{\text{throw these away}} = 5 + 2 + 1 = 8.$$

Note the following:

- A family $(a_i)_{i \in I} \in K^I$ is always essentially finite if I is finite; thus, essentially finite families are a wider class than finite families.
- Any essentially finite sum of real or complex numbers is convergent in the sense of analysis, but the converse is not true; for instance, the infinite sum $\sum\limits_{n \in \mathbb{N}} \dfrac{1}{2^n} = \dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \cdots$ is convergent in the sense of analysis, but not essentially finite. Essential finiteness is a crude algebraic imitation of convergence. One of its advantage is that it works for sums of elements of any commutative ring, not just of $\mathbb{R}$ or $\mathbb{C}$.

So the idea behind Definition 3.2.8 **(b)** is that addends that equal 0 can be discarded in a sum, even when there are infinitely many of them.

Sums of essentially finite families satisfy the usual rules for sums (such as the breaking-apart rule $\sum\limits_{i \in S} a_s = \sum\limits_{i \in X} a_s + \sum\limits_{i \in Y} a_s$ when a set S is the union of two disjoint sets X and Y). See [Grinbe15, §2.14.15] for details[13]. There is only one **caveat**: Interchange of summation signs (e.g., replacing $\sum\limits_{i \in I} \sum\limits_{j \in J} a_{i,j}$ by

[12] Here and in the following, the notation $\lfloor x \rfloor$ (where x is a real number) stands for the largest integer that is $\leq x$. For instance, $\lfloor \pi \rfloor = 3$ and $\lfloor 3 \rfloor = 3$.

[13] Note that [Grinbe15, §2.14.15] uses the words "*finitely supported*" instead of "essentially finite".

$\sum\limits_{j\in J}\ \sum\limits_{i\in I} a_{i,j}$) works only if the family $\left(a_{i,j}\right)_{(i,j)\in I\times J}$ is essentially finite (i.e., all but finitely many **pairs** $(i,j) \in I \times J$ satisfy $a_{i,j} = 0$); it does not suffice that the sums $\sum\limits_{i\in I}\ \sum\limits_{j\in J} a_{i,j}$ and $\sum\limits_{j\in J}\ \sum\limits_{i\in I} a_{i,j}$ themselves are essentially finite (i.e., that the families $\left(a_{i,j}\right)_{j\in J}$ for all $i \in I$, the families $\left(a_{i,j}\right)_{i\in I}$ for all $j \in J$, and the families $\left(\sum\limits_{j\in J} a_{i,j}\right)_{i\in I}$ and $\left(\sum\limits_{i\in I} a_{i,j}\right)_{j\in J}$ are essentially finite).

For a counterexample, consider the family $\left(a_{i,j}\right)_{(i,j)\in I\times J}$ of integers with $I = \{1,2,3,\ldots\}$ and $J = \{1,2,3,\ldots\}$, where $a_{i,j}$ is given by the following table:

$a_{i,j}$	1	2	3	4	5	$\cdots$
1	1	-1				$\cdots$
2		1	-1			$\cdots$
3			1	-1		$\cdots$
4				1	-1	$\cdots$
5					1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(where all the entries in the empty cells are 0). For this family $\left(a_{i,j}\right)_{(i,j)\in I\times J}$, both sums $\sum\limits_{i\in I}\ \sum\limits_{j\in J} a_{i,j}$ and $\sum\limits_{j\in J}\ \sum\limits_{i\in I} a_{i,j}$ are essentially finite, but they are not equal (indeed, the former sum is $\sum\limits_{i\in I}\ \underbrace{\sum\limits_{j\in J} a_{i,j}}_{=0} = \sum\limits_{i\in I} 0 = 0$, whereas the latter sum is $\sum\limits_{j\in J}\ \sum\limits_{i\in I} a_{i,j} = \underbrace{\sum\limits_{i\in I} a_{i,1}}_{=1} + \sum\limits_{j>1}\ \underbrace{\sum\limits_{i\in I} a_{i,j}}_{=0} = 1 + \sum\limits_{j>1} 0 = 1$). And indeed, this family $\left(a_{i,j}\right)_{(i,j)\in I\times J}$ is not essentially finite.

We have now made sense of infinite sums of elements of K when all but finitely many addends are 0. Of course, we can do the same for $K[[x]]$ instead of K (since $K[[x]]$, too, is a commutative ring). However, this does not help make sense of the sum on the left hand side of (24), because this sum is not essentially finite (it is a sum of infinitely many nonzero FPSs). Thus, for sums of FPSs, we need a weaker version of essential finiteness. Here is its definition:

Definition 3.2.9. A (possibly infinite) family $(\mathbf{a}_i)_{i \in I}$ of FPSs is said to be *summable* (or *entrywise essentially finite*) if

$$\text{for each } n \in \mathbb{N}, \text{ all but finitely many } i \in I \text{ satisfy } [x^n]\,\mathbf{a}_i = 0.$$

In this case, the sum $\sum\limits_{i \in I} \mathbf{a}_i$ is defined to be the FPS with

$$[x^n]\left(\sum_{i \in I} \mathbf{a}_i\right) = \underbrace{\sum_{i \in I} [x^n]\,\mathbf{a}_i}_{\substack{\text{an essentially} \\ \text{finite sum}}} \qquad \text{for all } n \in \mathbb{N}. \tag{25}$$

Remark 3.2.10. The condition "all but finitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$" in Definition 3.2.9 is **not** equivalent to "infinitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$".

Any essentially finite family of FPSs is summable, but the converse is not generally the case.

Example 3.2.11. Let us see how Definition 3.2.9 justifies (24). Consider the family $(\mathbf{a}_i)_{i \in \mathbb{N}} \in K[[x]]^{\mathbb{N}}$ of FPSs, where

$$\mathbf{a}_i := \left(\underbrace{0, 0, \ldots, 0}_{i \text{ zeroes}}, 1, 1, 1, \ldots\right) \qquad \text{for each } i \in \mathbb{N}.$$

The left hand side of (24) is precisely $\mathbf{a}_0 + \mathbf{a}_1 + \mathbf{a}_2 + \cdots = \sum\limits_{i \in \mathbb{N}} \mathbf{a}_i$, so let us check that the family $(\mathbf{a}_i)_{i \in \mathbb{N}}$ is summable and that its sum $\sum\limits_{i \in \mathbb{N}} \mathbf{a}_i$ really equals the right hand side of (24).

For each $n \in \mathbb{N}$, all but finitely many $i \in \mathbb{N}$ satisfy $[x^n]\,\mathbf{a}_i = 0$ (indeed, all $i > n$ satisfy this equality). Thus, the family $(\mathbf{a}_i)_{i \in \mathbb{N}}$ is summable. For each $n \in \mathbb{N}$, we have

$$\begin{aligned}
[x^n]\left(\sum_{i \in \mathbb{N}} \mathbf{a}_i\right) &= \sum_{i \in \mathbb{N}} [x^n]\,\mathbf{a}_i \qquad \text{(by (25))} \\
&= \sum_{i=0}^{n} \underbrace{[x^n]\,\mathbf{a}_i}_{\substack{=1 \\ (\text{since } i \leq n)}} + \sum_{i>n} \underbrace{[x^n]\,\mathbf{a}_i}_{\substack{=0 \\ (\text{since } i > n)}} = \sum_{i=0}^{n} 1 + \underbrace{\sum_{i>n} 0}_{=0} \\
&= \sum_{i=0}^{n} 1 = n + 1.
\end{aligned}$$

Thus, $\sum\limits_{i\in\mathbb{N}} \mathbf{a}_i = (1,2,3,4,\ldots)$. This is precisely the right hand side of (24). Thus, (24) has been justified rigorously.

You can think of summable infinite sums of FPSs as a crude algebraic imitate of uniformly convergent infinite sums of holomorphic functions in complex analysis. (However, the former are a much simpler concept than the latter. In particular, complex analysis is completely unnecessary in their study.)

Just as with essentially finite families, we can work with summable sums of FPSs "as if they were finite" most of the time:

Proposition 3.2.12. Sums of summable families of FPSs satisfy the usual rules for sums (such as the breaking-apart rule $\sum\limits_{i\in S} a_s = \sum\limits_{i\in X} a_s + \sum\limits_{i\in Y} a_s$ when a set S is the union of two disjoint sets X and Y). See [19s, Proposition 7.2.11] for details. Again, the only **caveat** is about interchange of summation signs: The equality

$$\sum_{i\in I}\ \sum_{j\in J} \mathbf{a}_{i,j} = \sum_{j\in J}\ \sum_{i\in I} \mathbf{a}_{i,j}$$

holds when the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable (i.e., when for each $n \in \mathbb{N}$, all but finitely many **pairs** $(i,j) \in I \times J$ satisfy $[x^n]\,\mathbf{a}_{i,j} = 0$); it does not generally hold if we merely assume that the sums $\sum\limits_{i\in I}\ \sum\limits_{j\in J} \mathbf{a}_{i,j}$ and $\sum\limits_{j\in J}\ \sum\limits_{i\in I} \mathbf{a}_{i,j}$ are summable.

Proof of Proposition 3.2.12. The proof is tedious (as there are many rules to check), but fairly straightforward (the idea is always to focus on a single coefficient, and then to reduce the infinite sums to finite sums). For example, consider the "discrete Fubini rule", which says that

$$\sum_{i\in I}\ \sum_{j\in J} \mathbf{a}_{i,j} = \sum_{(i,j)\in I\times J} \mathbf{a}_{i,j} = \sum_{j\in J}\ \sum_{i\in I} \mathbf{a}_{i,j} \tag{26}$$

whenever $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is a summable family of FPSs. In order to prove this rule, we fix a summable family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ of FPSs. It is easy to see that the families $\left(\mathbf{a}_{i,j}\right)_{j\in J}$ for all $i \in I$ are summable as well, as are the families $\left(\mathbf{a}_{i,j}\right)_{i\in I}$ for all $j \in J$, and the families $\left(\sum\limits_{j\in J} \mathbf{a}_{i,j}\right)_{i\in I}$ and $\left(\sum\limits_{i\in I} \mathbf{a}_{i,j}\right)_{j\in J}$. Hence, all sums in (26) are well-defined. Now, in order to prove (26), it suffices to check that

$$[x^n]\left(\sum_{i\in I}\ \sum_{j\in J} \mathbf{a}_{i,j}\right) = [x^n]\left(\sum_{(i,j)\in I\times J} \mathbf{a}_{i,j}\right) = [x^n]\left(\sum_{j\in J}\ \sum_{i\in I} \mathbf{a}_{i,j}\right)$$

for each $n \in \mathbb{N}$. Fix $n \in \mathbb{N}$; then, we have $[x^n]\left(\mathbf{a}_{i,j}\right) = 0$ for all but finitely many $(i,j) \in I \times J$ (since the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable). That is, the set of all pairs $(i, j) \in I \times J$ satisfying $[x^n] \left(\mathbf{a}_{i,j}\right) \neq 0$ is finite. Hence, the set $I' := \left\{i \mid (i, j) \in I \times J \text{ with } [x^n] \left(\mathbf{a}_{i,j}\right) \neq 0\right\}$ of the first entries of all these pairs is also finite, and so is the set $J' := \left\{i \mid (i, j) \in I \times J \text{ with } [x^n] \left(\mathbf{a}_{i,j}\right) \neq 0\right\}$ of the second entries of all these pairs. Now, the definitions of I' and J' ensure that any pair $(i, j) \in I \times J$ satisfies $[x^n] \mathbf{a}_{i,j} = 0$ unless $i \in I'$ and $j \in J'$. Hence, we easily obtain the three equalities

$$[x^n] \left(\sum_{i \in I} \sum_{j \in J} \mathbf{a}_{i,j} \right) = \sum_{i \in I} \sum_{j \in J} [x^n] \mathbf{a}_{i,j} = \sum_{i \in I'} \sum_{j \in J'} [x^n] \mathbf{a}_{i,j}$$

and

$$[x^n] \left(\sum_{(i,j) \in I \times J} \mathbf{a}_{i,j} \right) = \sum_{(i,j) \in I \times J} [x^n] \mathbf{a}_{i,j} = \sum_{(i,j) \in I' \times J'} [x^n] \mathbf{a}_{i,j}$$

and

$$[x^n] \left(\sum_{j \in J} \sum_{i \in I} \mathbf{a}_{i,j} \right) = \sum_{j \in J} \sum_{i \in I} [x^n] \mathbf{a}_{i,j} = \sum_{j \in J'} \sum_{i \in I'} [x^n] \mathbf{a}_{i,j}.$$

However, the right hand sides of these three equalities are equal (since the sums appearing in them are finite sums, and thus satisfy the usual rules for sums). Thus, the left hand sides are equal, exactly as we needed to show. See [19s, proof of Proposition 7.2.11] for more details of this proof. Proving the other properties of sums is easier. □

A few conventions about infinite sums will be used rather often:

Convention 3.2.13. **(a)** For any given integer $m \in \mathbb{Z}$, the summation sign $\sum\limits_{k \geq m}$ is to be understood as $\sum\limits_{k \in \{m, m+1, m+2, \ldots\}}$. We also write $\sum\limits_{k=m}^{\infty}$ for this summation sign.

(b) For any given integer $m \in \mathbb{Z}$, the summation sign $\sum\limits_{k > m}$ is to be understood as $\sum\limits_{k \in \{m+1, m+2, m+3, \ldots\}}$.

(c) Let I be a set, and let $\mathcal{A}(i)$ be a logical statement for each $i \in I$. (For example, I can be $\mathbb{N}$, and $\mathcal{A}(i)$ can be the statement "i is odd".) Then, the summation sign $\sum\limits_{\substack{i \in I; \\ \mathcal{A}(i)}}$ is to be understood as $\sum\limits_{i \in \{j \in I \mid \mathcal{A}(j)\}}$. (For example, the summation sign $\sum\limits_{\substack{i \in \mathbb{N}; \\ i \text{ is odd}}}$ means $\sum\limits_{i \in \{j \in \mathbb{N} \mid j \text{ is odd}\}}$, that is, a sum over all odd elements of $\mathbb{N}$.)

We can now define the x that figured so prominently in our informal exploration of formal power series back in Section 3.1:

Definition 3.2.14. Let x denote the FPS $(0, 1, 0, 0, 0, \ldots)$. In other words, let x denote the FPS with $\left[x^1\right] x = 1$ and $\left[x^i\right] x = 0$ for all $i \neq 1$.

The following simple lemma follows almost immediately from the definition of multiplication of FPSs:

Lemma 3.2.15. Let $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ be an FPS. Then, $x \cdot \mathbf{a} = (0, a_0, a_1, a_2, \ldots)$.

In other words, multiplying an FPS $\mathbf{a}$ by x is tantamount to inserting a 0 at the front of $\mathbf{a}$ (and shifting all the previously existing entries of $\mathbf{a}$ to the right by one position).

Proof of Lemma 3.2.15. If n is a positive integer, then

$$\begin{aligned}
\left[x^n\right](x \cdot \mathbf{a}) &= \sum_{i=0}^{n} \left[x^i\right] x \cdot \underbrace{\left[x^{n-i}\right] \mathbf{a}}_{\substack{=a_{n-i} \\ \text{(since } \mathbf{a}=(a_0,a_1,a_2,\ldots))}} \\
&\qquad \left(\text{by (20), applied to } x \text{ and } \mathbf{a} \text{ instead of } \mathbf{a} \text{ and } \mathbf{b}\right) \\
&= \sum_{i=0}^{n} \left[x^i\right] x \cdot a_{n-i} = \underbrace{\left[x^0\right] x}_{=0} \cdot a_{n-0} + \underbrace{\left[x^1\right] x}_{=1} \cdot a_{n-1} + \sum_{i=2}^{n} \underbrace{\left[x^i\right] x}_{\substack{=0 \\ \text{(since } i \geq 2 > 1)}} \cdot a_{n-i} \\
&\qquad \left(\begin{array}{c}\text{here, we have split off the addends} \\ \text{for } i=0 \text{ and } i=1 \text{ from the sum}\end{array}\right) \\
&= \underbrace{0 \cdot a_{n-0}}_{=0} + 1 \cdot a_{n-1} + \underbrace{\sum_{i=2}^{n} 0 \cdot a_{n-i}}_{=0} = 1 \cdot a_{n-1} = a_{n-1}.
\end{aligned}$$

A similar argument can be used for $n = 0$ (except that now, the sum $\sum_{i=0}^{n} \left[x^i\right] x \cdot a_{n-i}$ has no $\left[x^1\right] x \cdot a_{n-1}$ addend), and results in the conclusion that $\left[x^n\right](x \cdot \mathbf{a}) = 0$ in this case. Thus, for each $n \in \mathbb{N}$, we have

$$\left[x^n\right](x \cdot \mathbf{a}) = \begin{cases} a_{n-1}, & \text{if } n > 0; \\ 0, & \text{if } n = 0. \end{cases}$$

In other words, $x \cdot \mathbf{a} = (0, a_0, a_1, a_2, \ldots)$. This proves Lemma 3.2.15. □

Recall that $x^k = \underbrace{xx \cdots x}_{k \text{ times}}$ for each $k \in \mathbb{N}$ (by the definition of powers in any commutative ring). In particular, $x^0 = \underline{1}$ (since $\underline{1}$ is the unity of the ring $K[[x]]$). The following proposition describes x^k explicitly for each $k \in \mathbb{N}$:

Proposition 3.2.16. We have

$$x^k = \left(\underbrace{0,0,\ldots,0}_{k \text{ times}},1,0,0,0,\ldots\right) \qquad \text{for each } k \in \mathbb{N}.$$

Proof of Proposition 3.2.16. We induct on k.

Induction base: We have $x^0 = \underline{1} = (1,0,0,0,0,\ldots) = \left(\underbrace{0,0,\ldots,0}_{0 \text{ times}},1,0,0,0,\ldots\right)$. In other words, Proposition 3.2.16 holds for $k = 0$.

Induction step: Let $m \in \mathbb{N}$. Assume that Proposition 3.2.16 holds for $k = m$. We must prove that Proposition 3.2.16 holds for $k = m+1$.

We have $x^m = \left(\underbrace{0,0,\ldots,0}_{m \text{ times}},1,0,0,0,\ldots\right)$ (since Proposition 3.2.16 holds for $k = m$). Thus, Lemma 3.2.15 (applied to $\mathbf{a} = x^m$ and $(a_0,a_1,a_2,\ldots) = \left(\underbrace{0,0,\ldots,0}_{m \text{ times}},1,0,0,0,\ldots\right)$) yields

$$x \cdot x^m = \left(0,\underbrace{0,0,\ldots,0}_{m \text{ times}},1,0,0,0,\ldots\right) = \left(\underbrace{0,0,\ldots,0}_{m+1 \text{ times}},1,0,0,0,\ldots\right).$$

In other words, $x^{m+1} = \left(\underbrace{0,0,\ldots,0}_{m+1 \text{ times}},1,0,0,0,\ldots\right)$ (since $x \cdot x^m = x^{m+1}$). In other words, Proposition 3.2.16 holds for $k = m+1$. This completes the induction step, thus proving Proposition 3.2.16. □

Finally, the following corollary allows us to rewrite any FPS $(a_0,a_1,a_2,\ldots)$ in the familiar form $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$:

Corollary 3.2.17. Any FPS $(a_0,a_1,a_2,\ldots) \in K[[x]]$ satisfies

$$(a_0,a_1,a_2,\ldots) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots = \sum_{n\in\mathbb{N}} a_nx^n.$$

In particular, the right hand side here is well-defined, i.e., the family $(a_nx^n)_{n\in\mathbb{N}}$ is summable.

Proof of Corollary 3.2.17 (sketched). (See [19s, Corollary 7.2.16] for details.) By

Proposition 3.2.16, we have

$$\begin{aligned}
& a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \\
&= \quad a_0 (1, 0, 0, 0, \ldots) \\
&\quad + a_1 (0, 1, 0, 0, \ldots) \\
&\quad + a_2 (0, 0, 1, 0, \ldots) \\
&\quad + a_3 (0, 0, 0, 1, \ldots) \\
&\quad + \cdots \\
&= \quad (a_0, 0, 0, 0, \ldots) \\
&\quad + (0, a_1, 0, 0, \ldots) \\
&\quad + (0, 0, a_2, 0, \ldots) \\
&\quad + (0, 0, 0, a_3, \ldots) \\
&\quad + \cdots \\
&= (a_0, a_1, a_2, a_3, \ldots).
\end{aligned}$$

This proves Corollary 3.2.17 (since $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots = \sum\limits_{n \in \mathbb{N}} a_n x^n$ holds for obvious reasons). □

So we have "found" our x and given a rigorous justification for writing $(a_0, a_1, a_2, \ldots)$ as $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. Note that we did not use any analysis (real or complex) in the process; in particular, we did not have to worry about convergence (we did have to worry about summability, but this is much simpler than convergence). It is easy to come up with FPSs that don't converge when any nonzero real number is substituted for x (for example, $\sum\limits_{n \in \mathbb{N}} n! x^n = 1 + x + 2x^2 + 6x^3 + 24x^4 + \cdots$ is such an FPS); they are nevertheless completely legitimate FPSs.

We can now also answer the question "what is a generating function", albeit the answer is somewhat anticlimactic:

Definition 3.2.18. Let $(a_0, a_1, a_2, \ldots)$ be a sequence of elements of K. Then, the *(ordinary) generating function* of $(a_0, a_1, a_2, \ldots)$ will mean the FPS $(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$.

3.2.3. The Chu–Vandermonde identity

What we have done so far is sufficient to justify Example 3 from Section 3.1. Thus, let us record the result of Example 3 as a proposition:

Proposition 3.2.19. Let $a, b \in \mathbb{N}$, and let $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}. \tag{27}$$

We have yet to justify Examples 1, 2 and 4; we shall do so later. First, however, let us generalize Proposition 3.2.19 to arbitrary numbers a, b (as opposed to merely $a, b \in \mathbb{N}$). That is, we shall prove the following:

> **Theorem 3.2.20** (*Vandermonde convolution identity*, aka *Chu–Vandermonde identity*)**.** Let $a, b \in \mathbb{C}$, and let $n \in \mathbb{N}$. Then,
>
> $$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}. \tag{28}$$

(Actually, the "Let $a, b \in \mathbb{C}$" in Theorem 3.2.20 can be replaced by "Let a, b be any numbers", where "numbers" is understood appropriately[14]. We just wrote "Let $a, b \in \mathbb{C}$" for simplicity.)

To recall, back in Example 3, we proved Proposition 3.2.19 by multiplying out the identity $(1+x)^{a+b} = (1+x)^{a} (1+x)^{b}$ using the binomial formula. If we wanted to extend this argument to arbitrary $a, b \in \mathbb{C}$, then we would need to make sense of powers like $(1+x)^{-3}$ or $(1+x)^{1/2}$ or $(1+x)^{\pi}$. This is indeed possible (in fact, we will briefly outline this later on), but there is a much shorter way.

In fact, there is a slick trick to automatically extend a claim like (27) from nonnegative integers to complex numbers. It is sometimes known as the *polynomial identity trick*, and is used a lot in algebra. The proof of Theorem 3.2.20 that we shall sketch below should illustrate this trick; you can find more details and further examples in [20f, §7.5.3].

Proof of Theorem 3.2.20 (sketched). Fix $n \in \mathbb{N}$ and $b \in \mathbb{N}$, but forget that a was fixed. Then, Lemma 3.2.19 (which we have already proved) says that the equality

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k} \tag{29}$$

holds for each $a \in \mathbb{N}$. However, both sides of this equality are polynomials (more precisely, polynomial functions) in a: indeed,

$$\binom{a+b}{n} = \frac{(a+b)(a+b-1)(a+b-2)\cdots(a+b-n+1)}{n!} \qquad \text{and}$$

$$\sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k} = \sum_{k=0}^{n} \frac{a(a-1)\cdots(a-k+1)}{k!} \binom{b}{n-k}.$$

If two univariate polynomials p and q (with rational, real or complex coefficients) are equal for each $a \in \mathbb{N}$ (that is: if we have $p(a) = q(a)$ for each

[14] Namely, a "number" should here be viewed as an element of a commutative $\mathbb{Q}$-algebra. This includes complex numbers, polynomials over complex numbers, power series over complex numbers and even commuting matrices with complex entries.

$a \in \mathbb{N}$), then they must be identical (because two univariate polynomials that are equal at infinitely many points must necessarily be identical[15]). Hence, the two sides of (29) must be identical as polynomials in a. Thus, the equality (29) holds not only for each $a \in \mathbb{N}$, but also for each $a \in \mathbb{C}$.

Now, forget that b was fixed. Instead, let us fix $a \in \mathbb{C}$. As we just have proved, the equality (29) holds for each $b \in \mathbb{N}$. We want to show that it holds for each $b \in \mathbb{C}$. But this can be achieved by the same argument that we just used to extend it from $a \in \mathbb{N}$ to $a \in \mathbb{C}$: We view both sides of the equality as polynomials (but this time in b, not in a), and argue that these polynomials must be identical because they are equal at infinitely many points. The upshot is that the equality (29) holds for all $a, b \in \mathbb{C}$; thus, Theorem 3.2.20 is proven. (See [20f, proofs of Lemma 7.5.8 and Theorem 7.5.3] or [19s, §2.17.3] for this proof in more detail. Alternatively, see [Grinbe15, §3.3.2 and §3.3.3] for two other proofs.) □

3.2.4. What next?

Let us now return to our quest of justifying Examples 1, 2 and 4 from Section 3.1. In order to do so, we need to know

- what we can substitute into a FPS;
- when and why can we divide FPSs by FPSs;
- when and why can we take the square root of an FPS and solve a quadratic equation using the quadratic formula.

So we need to do more. The following sections are devoted to this.

3.3. Dividing FPSs

3.3.1. Conventions

We shall make ourselves at home in the ring $K[[x]]$ a bit more. (Recall that K is a fixed commutative ring.)

Convention 3.3.1. From now on, we identify each $a \in K$ with the constant FPS $\underline{a} = (a, 0, 0, 0, 0, \ldots) \in K[[x]]$.

[15] Quick reminder on why this is true: If p and q are two univariate polynomials (with rational, real or complex coefficients) that are equal at infinitely many points (i.e., if there exist infinitely many numbers z satisfying $p(z) = q(z)$), then $p = q$ (because the assumption entails that the difference $p - q$ has infinitely many roots, but this entails $p - q = 0$ and thus $p = q$). See [20f, Corollary 7.5.7] for this argument in more detail.

This is motivated by the fact that $\underline{a} = a + 0x + 0x^2 + 0x^3 + \cdots$ for any $a \in K$. Convention 3.3.1 does not cause any dangerous ambiguities, because we have

$$\begin{aligned} \underline{a+b} &= \underline{a} + \underline{b} && \text{and} \\ \underline{a-b} &= \underline{a} - \underline{b} && \text{and} \\ \underline{a \cdot b} &= \underline{a} \cdot \underline{b} && \text{for any } a, b \in K \end{aligned}$$

(check this!), and because the zero and the unity of the ring $K[[x]]$ are $\underline{0}$ and $\underline{1}$, respectively.

Furthermore, I will stop using boldfaced letters (like $\mathbf{a}, \mathbf{b}, \mathbf{c}$) for FPSs. (I did this above for the sake of convenience, but this is rarely done in the literature.)

3.3.2. Inverses in commutative rings

We recall the notion of an *inverse* in a commutative ring:

Definition 3.3.2. Let L be a commutative ring. Let $a \in L$. Then:

(a) An *inverse* (or *multiplicative inverse*) of a means an element $b \in L$ such that $ab = ba = 1$ (where the "1" means the unity of L).

(b) We say that a is *invertible* in L (or a *unit* of L) if a has an inverse.

Note that the condition "$ab = ba = 1$" in Definition 3.3.2 **(a)** can be restated as "$ab = 1$", because we automatically have $ab = ba$ (since L is a commutative ring). I have chosen to write "$ab = ba = 1$" in order to state the definition in a form that applies verbatim to noncommutative rings as well.

Example 3.3.3. **(a)** In the ring $\mathbb{Z}$, the only two invertible elements are 1 and -1. Each of these two elements is its own inverse.

(b) In the ring $\mathbb{Q}$, every nonzero element is invertible. The same holds for the rings $\mathbb{R}$ and $\mathbb{C}$ (and, more generally, for any field).

Our next goal is to study inverses of FPSs in $K[[x]]$, answering in particular the natural question "which elements of $K[[x]]$ have inverses". But let us first prove their uniqueness in the generality of an arbitrary commutative ring:

Theorem 3.3.4. Let L be a commutative ring. Let $a \in L$. Then, there is **at most one** inverse of a.

Proof. Let b and c be two inverses of a. We must prove that $b = c$.

Since b is an inverse of a, we have $ab = ba = 1$. Since c is an inverse of a, we have $ac = ca = 1$. Now, we have $b\underbrace{(ac)}_{=1} = b \cdot 1 = b$ and $\underbrace{(ba)}_{=1}c = 1 \cdot c = c$. However, because of the "associativity of multiplication" axiom in Definition 3.2.1, we have $b(ac) = (ba)c$. Hence, $b = b(ac) = (ba)c = c$. This proves Theorem 3.3.4. □

Theorem 3.3.4 allows us to make the following definition:

Definition 3.3.5. Let L be a commutative ring. Let $a \in L$. Assume that a is invertible. Then:

(a) The inverse of a is called a^{-1}. (This notation is unambiguous, since Theorem 3.3.4 shows that the inverse of a is unique.)

(b) For any $b \in L$, the product $b \cdot a^{-1}$ is called $\frac{b}{a}$ (or b/a).

(c) For any negative integer n, we define a^n to be $\left(a^{-1}\right)^{-n}$. Thus, the n-th power a^n is defined for each $n \in \mathbb{Z}$.

The following facts are easy to check:

Proposition 3.3.6. Let L be a commutative ring. Then:

(a) Any invertible element $a \in L$ satisfies $a^{-1} = 1/a$.

(b) For any invertible elements $a, b \in L$, the element ab is invertible as well, and satisfies $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$.

(c) If $a \in L$ is invertible, and if $n \in \mathbb{Z}$ is arbitrary, then $a^{-n} = \left(a^{-1}\right)^n = (a^n)^{-1}$.

(d) Laws of exponents hold for negative exponents as well: If a and b are invertible elements of L, then

$$\begin{aligned} a^{n+m} &= a^n a^m && \text{for all } n, m \in \mathbb{Z}; \\ (ab)^n &= a^n b^n && \text{for all } n \in \mathbb{Z}; \\ (a^n)^m &= a^{nm} && \text{for all } n, m \in \mathbb{Z}. \end{aligned}$$

(e) Laws of fractions hold: If a and c are two invertible elements of L, and if b and d are any two elements of L, then $\frac{b}{a} + \frac{d}{c} = \frac{bc + ad}{ac}$ and $\frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}$.

(f) Division undoes multiplication: If a, b, c are three elements of L with a being invertible, then the equality $\frac{c}{a} = b$ is equivalent to $c = ab$.

Proof. Exercise. (See, e.g., [19s, solution to Exercise 4.1.1] for a proof of parts **(c)** and **(d)** in the special case where $L = \mathbb{C}$; essentially the same argument works in the general case. The remaining parts of Proposition 3.3.6 are even easier to check. Note that parts **(a)** and **(c)** as well as the $(ab)^{-1} = b^{-1}a^{-1}$ part of part **(b)** would hold even if L was a noncommutative ring.) □

3.3.3. Inverses in $K[[x]]$

Now, which FPSs are invertible in the ring $K[[x]]$? For example, we know from (5) that the FPS $1 - x$ is invertible, with inverse $1 + x + x^2 + x^3 + \cdots$. On the other hand, the FPS x is not invertible, since Lemma 3.2.15 shows that any product of x with an FPS must begin with a 0 (but the unity of $K[[x]]$ does not begin with a 0). (Strictly speaking, this is only true if the ring K is nontrivial – i.e., if not all elements of K are equal. If K is trivial, then $K[[x]]$ is trivial, and thus any FPS in $K[[x]]$ is invertible, but this does not make an interesting statement.)

It turns out that we can characterize invertible FPSs in $K[[x]]$ in a rather simple way:

Proposition 3.3.7. Let $a \in K[[x]]$. Then, the FPS a is invertible in $K[[x]]$ if and only if its constant term $[x^0]\, a$ is invertible in K.

Proof. $\Longrightarrow$: Assume that a is invertible in $K[[x]]$. That is, a has an inverse $b \in K[[x]]$. Consider this b. Since b is an inverse of a, we have $ab = ba = 1$ (where "1" means $\underline{1}$ by Convention 3.3.1). However, (22) (applied to $\mathbf{a} = a$ and $\mathbf{b} = b$) yields $[x^0]\,(ab) = [x^0]\, a \cdot [x^0]\, b$. Comparing this with $[x^0]\,\underbrace{(ab)}_{=1} = [x^0]\, 1 = 1$, we find $[x^0]\, a \cdot [x^0]\, b = 1$. Thus, $[x^0]\, b$ is an inverse of $[x^0]\, a$ in K (since $[x^0]\, b \cdot [x^0]\, a = [x^0]\, a \cdot [x^0]\, b = 1$, so that $[x^0]\, a \cdot [x^0]\, b = [x^0]\, b \cdot [x^0]\, a = 1$). Therefore, $[x^0]\, a$ is invertible in K (with inverse $[x^0]\, b$). This proves the "$\Longrightarrow$" direction of Proposition 3.3.7.

$\Longleftarrow$: Assume that $[x^0]\, a$ is invertible in K. Write the FPS a in the form $a = (a_0, a_1, a_2, \ldots)$. Thus, $[x^0]\, a = a_0$, so that a_0 is invertible in K (since $[x^0]\, a$ is invertible in K). Thus, its inverse a_0^{-1} is well-defined.

Now, we want to prove that a is invertible in $K[[x]]$. We thus try to find an inverse of a.

We work backwards at first: We assume that $b = (b_0, b_1, b_2, \ldots) \in K[[x]]$ is an inverse for a, and we try to figure out how this inverse looks like.

Since b is an inverse of a, we have $ab = \underline{1} = (1, 0, 0, 0, \ldots)$. However, from $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$, we have

$$\begin{aligned} ab &= (a_0, a_1, a_2, \ldots)\,(b_0, b_1, b_2, \ldots) \\ &= (a_0b_0,\ \ a_0b_1 + a_1b_0,\ \ a_0b_2 + a_1b_1 + a_2b_0,\ \ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0,\ \ \ldots) \end{aligned}$$

(by the definition of the product of FPSs). Comparing this with $ab = (1, 0, 0, 0, \ldots)$, we obtain

$$\begin{aligned} &(1, 0, 0, 0, \ldots) \\ &= (a_0b_0,\ \ a_0b_1 + a_1b_0,\ \ a_0b_2 + a_1b_1 + a_2b_0,\ \ a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0,\ \ \ldots). \end{aligned}$$

This can be rewritten as the following system of equations:

$$\begin{cases} 1 = a_0b_0, \\ 0 = a_0b_1 + a_1b_0, \\ 0 = a_0b_2 + a_1b_1 + a_2b_0, \\ 0 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0, \\ \ldots. \end{cases} \qquad (30)$$

I claim that this system of equations uniquely determines $(b_0, b_1, b_2, \ldots)$. Indeed, we can solve the first equation ($1 = a_0 b_0$) for b_0, thus obtaining $b_0 = a_0^{-1}$ (since a_0 is invertible). Having thus found b_0, we can solve the second equation ($0 = a_0 b_1 + a_1 b_0$) for b_1, thus obtaining $b_1 = -a_0^{-1} (a_1 b_0)$ (again because a_0 is invertible). Having thus found both b_0 and b_1, we can solve the third equation ($0 = a_0 b_2 + a_1 b_1 + a_2 b_0$) for b_2, thus obtaining $b_2 = -a_0^{-1} (a_1 b_1 + a_2 b_0)$. Proceeding like this, we obtain recursive expressions for all coefficients $b_0, b_1, b_2, \ldots$ of b, namely

$$\begin{cases} b_0 = a_0^{-1}, \\ b_1 = -a_0^{-1} (a_1 b_0), \\ b_2 = -a_0^{-1} (a_1 b_1 + a_2 b_0), \\ b_3 = -a_0^{-1} (a_1 b_2 + a_2 b_1 + a_3 b_0), \\ \ldots . \end{cases} \tag{31}$$

(This procedure for solving systems of linear equations is well-known from linear algebra – it is a form of Gaussian elimination, but a particularly simple one because our system is triangular with invertible coefficients on the diagonal. The only complication is that it has infinitely many variables and infinitely many equations.)

So we have shown that if b is an inverse of a, then the entries b_i of the FPS b are given recursively by (31). This yields that b is unique; alas, this is not what we want to prove. Instead, we want to prove that b exists.

Fortunately, we can achieve this by simply turning our above argument around: Forget that we fixed b. Instead, we define a sequence $(b_0, b_1, b_2, \ldots)$ of elements of K recursively by (31), and we define the FPS $b = (b_0, b_1, b_2, \ldots) \in K[[x]]$. Then, the equalities (30) hold (because they are just equivalent restatements of the equalities (31)). In other words, we have

$$\begin{aligned} &(1, 0, 0, 0, \ldots) \\ &= (a_0 b_0,\ \ a_0 b_1 + a_1 b_0,\ \ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \ a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0,\ \ \ldots). \end{aligned}$$

However, as before, we can show that

$$ab = (a_0 b_0,\ \ a_0 b_1 + a_1 b_0,\ \ a_0 b_2 + a_1 b_1 + a_2 b_0,\ \ a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0,\ \ \ldots).$$

Comparing these two equalities, we find $ab = (1, 0, 0, 0, \ldots) = \underline{1}$. Thus, $ba = ab = \underline{1}$, so that $ab = ba = \underline{1}$. This shows that b is an inverse of a, so that a is invertible. This proves the "$\Longleftarrow$" direction of Proposition 3.3.7. □

We note a particularly simple corollary of Proposition 3.3.7 when K is a field:

Corollary 3.3.8. Assume that K is a field. Let $a \in K[[x]]$. Then, the FPS a is invertible in $K[[x]]$ if and only if $[x^0]\, a \neq 0$.

Proof. An element of K is invertible in K if and only if it is nonzero (since K is a field). Hence, Corollary 3.3.8 follows from Proposition 3.3.7. □

3.3.4. Newton's binomial formula

Let us now return to considering specific FPSs. We have already seen that the FPS $1-x$ is invertible, with inverse $1+x+x^2+x^3+\cdots$. We shall now show an analogous result for the FPS $1+x$. Its invertibility follows from Proposition 3.3.7, but it is better to derive it by hand, as this also gives a formula for the inverse:

Proposition 3.3.9. The FPS $1+x \in K[[x]]$ is invertible, and its inverse is

$$(1+x)^{-1} = 1-x+x^2-x^3+x^4-x^5 \pm \cdots = \sum_{n\in\mathbb{N}} (-1)^n x^n.$$

First proof of Proposition 3.3.9. We have

$$\begin{aligned}
&(1+x)\cdot\left(1-x+x^2-x^3+x^4-x^5\pm\cdots\right)\\
&= \underbrace{1\cdot\left(1-x+x^2-x^3+x^4-x^5\pm\cdots\right)}_{=1-x+x^2-x^3+x^4-x^5\pm\cdots} + \underbrace{x\cdot\left(1-x+x^2-x^3+x^4-x^5\pm\cdots\right)}_{=x-x^2+x^3-x^4+x^5-x^6\pm\cdots}\\
&= \left(1-x+x^2-x^3+x^4-x^5\pm\cdots\right)+\left(x-x^2+x^3-x^4+x^5-x^6\pm\cdots\right)\\
&= 1
\end{aligned}$$

(since all powers of x other than 1 cancel out). This shows that $1-x+x^2-x^3+x^4-x^5\pm\cdots$ is an inverse of $1+x$ (since $K[[x]]$ is a commutative ring). Thus, $1+x$ is invertible, and its inverse is $(1+x)^{-1} = 1-x+x^2-x^3+x^4-x^5\pm\cdots = \sum_{n\in\mathbb{N}}(-1)^n x^n$. This proves Proposition 3.3.9. □

Second proof of Proposition 3.3.9. We have

$$\begin{aligned}
&(1+x)\cdot\left(1-x+x^2-x^3+x^4-x^5\pm\cdots\right)\\
&= \underbrace{(1+x)\cdot 1}_{=1+x} - \underbrace{(1+x)\cdot x}_{=x+x^2} + \underbrace{(1+x)\cdot x^2}_{=x^2+x^3} - \underbrace{(1+x)\cdot x^3}_{=x^3+x^4} + \underbrace{(1+x)\cdot x^4}_{=x^4+x^5} - \underbrace{(1+x)\cdot x^5}_{=x^5+x^6} \pm\cdots\\
&= (1+x)-\left(x+x^2\right)+\left(x^2+x^3\right)-\left(x^3+x^4\right)+\left(x^4+x^5\right)-\left(x^5+x^6\right)\pm\cdots\\
&= 1
\end{aligned}$$

(since we have a telescoping sum in front of us, in which all powers of x other than 1 cancel out). This shows that $1-x+x^2-x^3+x^4-x^5\pm\cdots$ is an inverse of $1+x$ (since $K[[x]]$ is a commutative ring). Thus, $1+x$ is invertible, and its inverse is $(1+x)^{-1} = 1-x+x^2-x^3+x^4-x^5\pm\cdots = \sum_{n\in\mathbb{N}}(-1)^n x^n$. This proves Proposition 3.3.9. □

Proposition 3.3.9 shows that the FPS $1+x$ is invertible; thus, its powers $(1+x)^n$ are defined for all $n \in \mathbb{Z}$ (by Definition 3.3.5 **(c)**). The following formula – known as *Newton's binomial theorem*[16] – describes these powers explicitly:

Theorem 3.3.10. For each $n \in \mathbb{Z}$, we have

$$(1+x)^n = \sum_{k \in \mathbb{N}} \binom{n}{k} x^k.$$

Note that the sum $\sum_{k \in \mathbb{N}} \binom{n}{k} x^k$ is summable for each $n \in \mathbb{N}$ (indeed, it equals the FPS $\left(\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots\right)$). If $n \in \mathbb{N}$, then it is essentially finite.

The reader may want to check that the particular case $n = -1$ of Theorem 3.3.10 agrees with Proposition 3.3.9. (Recall Example 2.0.2!)

Of course, Theorem 3.3.10 should look familiar – an identical-looking formula appears in real analysis under the same name. However, the result in real analysis is concerned with infinite sums of real numbers, while our Theorem 3.3.10 is an identity between FPSs over an arbitrary commutative ring. Thus, the two facts are not the same.

We will prove Theorem 3.3.10 in a somewhat roundabout way, since this gives us an opportunity to establish some auxiliary results that are of separate interest (and usefulness). The first of these auxiliary results is a fundamental property of binomial coefficients, known as the *upper negation formula* (see, e.g., [19fco, Proposition 1.3.7]):

Theorem 3.3.11. Let $n \in \mathbb{C}$ and $k \in \mathbb{Z}$. Then,

$$\binom{-n}{k} = (-1)^k \binom{k+n-1}{k}.$$

Proof of Theorem 3.3.11 (sketched). If $k < 0$, then this is trivial because both $\binom{-n}{k}$ and $\binom{k+n-1}{k}$ are 0 (by (1)). Thus, we WLOG assume that $k \geq 0$. Hence, $k \in \mathbb{N}$. Thus, (1) yields

$$\binom{-n}{k} = \frac{(-n)(-n-1)(-n-2)\cdots(-n-k+1)}{k!} \qquad \text{and}$$
$$\binom{k+n-1}{k} = \frac{(k+n-1)(k+n-2)(k+n-3)\cdots(k+n-k)}{k!}.$$

[16] or *Newton's binomial formula*

A moment of thought reveals that the right hand sides of these two equalities are equal up to a factor of $(-1)^k$. Thus, so are the left hand sides. In other words, $\dbinom{-n}{k} = (-1)^k \dbinom{k+n-1}{k}$. This proves Theorem 3.3.11. □

(Quick exercise: Rederive Example 2.0.2 from Theorem 3.3.11.)

Next, we show a formula for negative powers of $1+x$:

Proposition 3.3.12. For each $n \in \mathbb{N}$, we have

$$(1+x)^{-n} = \sum_{k\in\mathbb{N}} (-1)^k \binom{n+k-1}{k} x^k.$$

Proof of Proposition 3.3.12. We proceed by induction on n:

Induction base: Comparing

$$(1+x)^{-0} = (1+x)^0 = \underline{1} = (1,0,0,0,\ldots) = 1$$

with

$$\begin{aligned}
&\sum_{k\in\mathbb{N}} (-1)^k \binom{0+k-1}{k} x^k \\
&= \underbrace{(-1)^0}_{=1} \underbrace{\binom{0+0-1}{0}}_{=1} \underbrace{x^0}_{=1} + \sum_{\substack{k\in\mathbb{N};\\ k>0}} (-1)^k \underbrace{\binom{0+k-1}{k}}_{\substack{=\binom{k-1}{k}=0 \\ \text{(by Proposition 2.0.5} \\ \text{(applied to } m=k-1 \text{ and } n=k\text{),} \\ \text{since } k-1<k \text{ and } k-1\in\mathbb{N})}} x^k \\
&\qquad \text{(here, we have split off the addend for } k=0 \text{ from the sum)} \\
&= 1 + \underbrace{\sum_{\substack{k\in\mathbb{N};\\ k>0}} (-1)^k 0x^k}_{=0} = 1,
\end{aligned}$$

we obtain $(1+x)^{-0} = \sum_{k\in\mathbb{N}} (-1)^k \dbinom{0+k-1}{k} x^k$. In other words, Proposition 3.3.12 holds for $n=0$.

Induction step: Let $j \in \mathbb{N}$. Assume that Proposition 3.3.12 holds for $n=j$. We must prove that Proposition 3.3.12 holds for $n=j+1$.

We have assumed that Proposition 3.3.12 holds for $n=j$. In other words, we have

$$(1+x)^{-j} = \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k} x^k. \tag{32}$$

Now, we want to prove that Proposition 3.3.12 holds for $n = j+1$. In other words, we want to prove that

$$(1+x)^{-(j+1)} = \sum_{k\in\mathbb{N}} (-1)^k \binom{(j+1)+k-1}{k} x^k.$$

In view of $(1+x)^{-(j+1)} = (1+x)^{-j} \cdot (1+x)^{-1}$ and $(j+1)+k-1 = j+k$, this equality can be rewritten as

$$(1+x)^{-j} \cdot (1+x)^{-1} = \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k}{k} x^k.$$

Since $1+x$ is invertible, we can equivalently transform this equality by multiplying both sides with $1+x$; thus, it becomes

$$(1+x)^{-j} = \left(\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k}{k} x^k\right) \cdot (1+x).$$

So this is the equality we must prove.

We do this by simplifying its right hand side:

$$\begin{aligned}
&\left(\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k}{k} x^k\right)\cdot(1+x) \\
&= \sum_{k\in\mathbb{N}} \underbrace{(-1)^k \binom{j+k}{k} x^k (1+x)}_{\substack{=(-1)^k\binom{j+k}{k}\left(x^k+x^{k+1}\right) \\ =(-1)^k\binom{j+k}{k}x^k+(-1)^k\binom{j+k}{k}x^{k+1}}} \\
&= \sum_{k\in\mathbb{N}} \left((-1)^k \binom{j+k}{k} x^k + (-1)^k \binom{j+k}{k} x^{k+1}\right) \\
&= \sum_{k\in\mathbb{N}} (-1)^k \underbrace{\binom{j+k}{k}}_{\substack{=\binom{j+k-1}{k-1}+\binom{j+k-1}{k} \\ \text{(by Proposition 2.0.4,} \\ \text{applied to } m=j+k \text{ and } n=k\text{)}}} x^k + \underbrace{\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k}{k} x^{k+1}}_{\substack{=\sum_{k\geq 1}(-1)^{k-1}\binom{j+(k-1)}{k-1}x^k \\ \text{(here, we have substituted } k-1 \text{ for } k \\ \text{in the sum)}}} \\
&= \underbrace{\sum_{k\in\mathbb{N}} (-1)^k \left(\binom{j+k-1}{k-1}+\binom{j+k-1}{k}\right) x^k}_{=\sum_{k\in\mathbb{N}}(-1)^k\binom{j+k-1}{k-1}x^k+\sum_{k\in\mathbb{N}}(-1)^k\binom{j+k-1}{k}x^k} + \sum_{k\geq 1} \underbrace{(-1)^{k-1}}_{=-(-1)^k} \underbrace{\binom{j+(k-1)}{k-1}}_{=\binom{j+k-1}{k-1}} x^k \\
&= \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k-1} x^k + \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k} x^k + \sum_{k\geq 1} \left(-(-1)^k\right) \binom{j+k-1}{k-1} x^k \\
&= \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k-1} x^k + \sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k} x^k - \sum_{k\geq 1} (-1)^k \binom{j+k-1}{k-1} x^k \\
&= \underbrace{\left(\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k-1} x^k - \sum_{k\geq 1} (-1)^k \binom{j+k-1}{k-1} x^k\right)}_{\substack{=(-1)^0\binom{j+0-1}{0-1}x^0 \\ \text{(since the two sums differ only in their } k=0 \text{ addend)}}} + \underbrace{\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k-1}{k} x^k}_{\substack{=(1+x)^{-j} \\ \text{(by (32))}}} \\
&= (-1)^0 \underbrace{\binom{j+0-1}{0-1}}_{\substack{=0 \\ \text{(by (1), since } 0-1\notin\mathbb{N}\text{)}}} x^0 + (1+x)^{-j} = (1+x)^{-j}.
\end{aligned}$$

Multiplying both sides of this equality by $(1+x)^{-1}$, we obtain

$$\sum_{k\in\mathbb{N}} (-1)^k \binom{j+k}{k} x^k = (1+x)^{-j} \cdot (1+x)^{-1} = (1+x)^{(-j)+(-1)} = (1+x)^{-(j+1)},$$

so that

$$(1+x)^{-(j+1)} = \sum_{k\in\mathbb{N}} (-1)^k \underbrace{\binom{j+k}{k}}_{=\binom{(j+1)+k-1}{k}} x^k = \sum_{k\in\mathbb{N}} (-1)^k \binom{(j+1)+k-1}{k} x^k.$$

In other words, Proposition 3.3.12 holds for $n = j+1$. This completes the induction step. Thus, Proposition 3.3.12 is proved. □

We can rewrite Proposition 3.3.12 using negative binomial coefficients:

Corollary 3.3.13. For each $n \in \mathbb{N}$, we have

$$(1+x)^{-n} = \sum_{k\in\mathbb{N}} \binom{-n}{k} x^k.$$

Proof of Corollary 3.3.13. Proposition 3.3.12 yields

$$(1+x)^{-n} = \sum_{k\in\mathbb{N}} \underbrace{(-1)^k \binom{n+k-1}{k}}_{\substack{=(-1)^k \binom{k+n-1}{k} \\ =\binom{-n}{k} \\ \text{(by Theorem 3.3.11)}}} x^k = \sum_{k\in\mathbb{N}} \binom{-n}{k} x^k.$$

This proves Corollary 3.3.13. □

We can now easily prove Newton's binomial formula:

Proof of Theorem 3.3.10. Let $n \in \mathbb{Z}$. We must prove that $(1+x)^n = \sum_{k\in\mathbb{N}} \binom{n}{k} x^k$.

If $n \in \mathbb{N}$, then this follows by comparing

$$\begin{aligned}(1+x)^n = (x+1)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \underbrace{1^{n-k}}_{=1} \qquad \text{(by the binomial theorem)} \\ &= \sum_{k=0}^{n} \binom{n}{k} x^k\end{aligned}$$

with

$$\sum_{k\in\mathbb{N}} \binom{n}{k} x^k = \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k>n} \underbrace{\binom{n}{k}}_{\substack{=0 \\ \text{(by Proposition 2.0.5,} \\ \text{since } n<k\text{)}}} x^k = \sum_{k=0}^{n} \binom{n}{k} x^k + \underbrace{\sum_{k>n} 0x^k}_{=0}$$
$$= \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Hence, for the rest of this proof, we WLOG assume that $n \notin \mathbb{N}$.

Hence, n is a negative integer, so that $-n \in \mathbb{N}$. Thus, Corollary 3.3.13 (applied to $-n$ instead of n) yields

$$(1+x)^{-(-n)} = \sum_{k\in\mathbb{N}} \binom{-(-n)}{k} x^k.$$

Since $-(-n) = n$, this rewrites as $(1+x)^n = \sum\limits_{k\in\mathbb{N}} \binom{n}{k} x^k$. Thus, Theorem 3.3.10 is proven. □

We thus have a formula for $(1+x)^n$ for each **integer** n. We don't yet have such a formula for $(1+x)^{1/2}$ (nor do we have a proper definition of $(1+x)^{1/2}$), but this was clearly a step forward.

3.3.5. Dividing by x

Let us see how this all helps us justify our arguments in Section 3.1. Proposition 3.3.7 justifies the fractions that appear in (4), but it does not justify dividing by the FPS $2x$ in (10), since the constant term $\left[x^0\right](2x)$ is surely not invertible. And indeed, the FPS $2x$ is not invertible; the fraction $\frac{1}{2x}$ is not a well-defined FPS.

However, it is easy to see directly which FPSs can be divided by x (and thus by $2x$, if $K = \mathbb{Q}$), and what it means to divide them by x. In fact, Lemma 3.2.15 shows that multiplying an FPS by x means moving all its entries by one position to the right, and putting a 0 into the newly vacated starting position. Thus, it is rather clear what dividing by x should be:

Definition 3.3.14. Let $a = (a_0, a_1, a_2, \ldots)$ be an FPS whose constant term a_0 is 0. Then, $\frac{a}{x}$ is defined to be the FPS $(a_1, a_2, a_3, \ldots)$.

The following is almost trivial:

> **Proposition 3.3.15.** Let $a \in K[[x]]$ and $b \in K[[x]]$ be two FPSs. Then, $a = xb$ if and only if $\left([x^0] a = 0 \text{ and } b = \dfrac{a}{x} \right)$.

Proof. Exercise. □

Having defined $\dfrac{a}{x}$ in Definition 3.3.14 (when a has constant term 0), we can also define $\dfrac{a}{2x}$ when 2 is invertible in K (just set $\dfrac{a}{2x} = \dfrac{1}{2} \cdot \dfrac{a}{x}$). Thus, the fraction $\dfrac{1 \pm \sqrt{1-4x}}{2x}$ in (10) makes sense when the ± sign is a $-$ sign (but not when it is a $+$ sign), at least if we interpret the square root $\sqrt{1-4x}$ as $\sum\limits_{k \geq 0} \dbinom{1/2}{k} (-4x)^k$.

3.3.6. A few lemmas

Let us use this occasion to state two simple lemmas (vaguely related to Definition 3.3.14) that will be used later on:

> **Lemma 3.3.16.** Let $a \in K[[x]]$ be an FPS with $[x^0] a = 0$. Then, there exists an $h \in K[[x]]$ such that $a = xh$.

Proof of Lemma 3.3.16. Write the FPS a in the form $a = (a_0, a_1, a_2, \ldots)$. Thus, $a_0 = [x^0] a = 0$. Hence, the FPS $\dfrac{a}{x}$ is well-defined. Moreover, it is easy to see that $a = x \cdot \dfrac{a}{x}$ [17]. Hence, there exists an $h \in K[[x]]$ such that $a = xh$ (namely, $h = \dfrac{a}{x}$). This proves Lemma 3.3.16. □

> **Lemma 3.3.17.** Let $k \in \mathbb{N}$. Let $a \in K[[x]]$ be any FPS. Then, the first k coefficients of the FPS $x^k a$ are 0.

Proof of Lemma 3.3.17. We must show that $[x^m] (x^k a) = 0$ for any nonnegative integer $m < k$. But we can do this directly: If m is a nonnegative integer such that $m < k$, then (20) (applied to x^k, a and m instead of **a**, **b** and n) yields

$$[x^m] \left(x^k a\right) = \sum_{i=0}^{m} \underbrace{\left[x^i\right] \left(x^k\right)}_{\substack{=0 \\ \text{(since } i \leq m < k \\ \text{and thus } i \neq k)}} \cdot \left[x^{m-i}\right] a = \sum_{i=0}^{m} 0 \cdot \left[x^{m-i}\right] a = 0,$$

[17] *Proof.* We have $\frac{a}{x} = (a_1, a_2, a_3, \ldots)$ (by Definition 3.3.14). Thus, Lemma 3.2.15 (applied to $\frac{a}{x}$ and a_{i-1} instead of **a** and a_i) yields

$$\begin{aligned} x \cdot \frac{a}{x} &= (0, a_1, a_2, a_3, \ldots) = (a_0, a_1, a_2, a_3, \ldots) \qquad \text{(since } 0 = a_0\text{)} \\ &= (a_0, a_1, a_2, \ldots) = a. \end{aligned}$$

Thus, $a = x \cdot \frac{a}{x}$.

which is exactly what we wanted to show. Thus, Lemma 3.3.17 is proved.

(Alternatively, we could prove Lemma 3.3.17 by writing a in the form $a = (a_0, a_1, a_2, \ldots)$ and observing that $x^k a = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}, a_0, a_1, a_2, \ldots\right)$. This follows by applying Lemma 3.2.15 a total of k times, or more formally by induction on k.) □

Lemma 3.3.17 has a converse; here is a statement that combines it with this converse:

Lemma 3.3.18. Let $k \in \mathbb{N}$. Let $f \in K[[x]]$ be any FPS. Then, the first k coefficients of the FPS f are 0 if and only if f is a multiple of x^k.

Here, we use the following notation:

Definition 3.3.19. Let $g \in K[[x]]$ be an FPS. Then, a *multiple* of g means an FPS of the form ga with $a \in K[[x]]$.

(This is just a particular case of the usual concept of multiples in a commutative ring.)

Proof of Lemma 3.3.18. The statement we are proving is an "if and only if" statement. We shall prove its "only if" (i.e., "$\Longrightarrow$") and its "if" (i.e., "$\Longleftarrow$") directions separately:

$\Longrightarrow$: Assume that the first k coefficients of the FPS f are 0. We must show that f is a multiple of x^k.

Write f as $f = (f_0, f_1, f_2, \ldots)$. Then, the first k coefficients of the FPS f are $f_0, f_1, \ldots, f_{k-1}$. Hence, these k coefficients $f_0, f_1, \ldots, f_{k-1}$ are 0 (since we have assumed that the first k coefficients of the FPS f are 0). In other words, $f_n = 0$ for each $n \in \{0, 1, \ldots, k-1\}$. Hence, $\sum\limits_{n=0}^{k-1} \underbrace{f_n}_{=0} x^n = \sum\limits_{n=0}^{k-1} 0x^n = 0$.

Now,

$$f = (f_0, f_1, f_2, \ldots) = \sum_{n \in \mathbb{N}} f_n x^n = \underbrace{\sum_{n=0}^{k-1} f_n x^n}_{=0} + \sum_{n=k}^{\infty} f_n \underbrace{x^n}_{\substack{=x^k x^{n-k} \\ (\text{since } n \geq k)}} = \sum_{n=k}^{\infty} f_n x^k x^{n-k}$$
$$= x^k \sum_{n=k}^{\infty} f_n x^{n-k}.$$

In other words, $f = x^k a$ for $a = \sum\limits_{n=k}^{\infty} f_n x^{n-k}$. This shows that f is a multiple of x^k. Thus, the "$\Longrightarrow$" direction of Lemma 3.3.18 is proved.

$\Longleftarrow$: Assume that f is a multiple of x^k. In other words, $f = x^k a$ for some $a \in K[[x]]$. Consider this a. Now, Lemma 3.3.17 yields that the first k coefficients of the FPS $x^k a$ are 0. In other words, the first k coefficients of the FPS f are 0 (since $f = x^k a$). This proves the "$\Longleftarrow$" direction of Lemma 3.3.18.

The proof of Lemma 3.3.18 is now complete, as both directions have been proved. □

Another lemma that will prove its usefulness much later concerns FPSs that are equal up until a certain coefficient. It says that if f and g are two FPSs whose first $n+1$ coefficients agree (for a certain $n \in \mathbb{N}$), then the same is true of the FPSs af and ag whenever a is any further FPS. In more details:

Lemma 3.3.20. Let $a, f, g \in K[[x]]$ be three FPSs. Let $n \in \mathbb{N}$. Assume that

$$[x^m]\, f = [x^m]\, g \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{33}$$

Then,

$$[x^m]\,(af) = [x^m]\,(ag) \qquad \text{for each } m \in \{0, 1, \ldots, n\}.$$

Proof of Lemma 3.3.20. Let $m \in \{0, 1, \ldots, n\}$. Then, $m \leq n$. Hence, each $j \in \{0, 1, \ldots, m\}$ satisfies $j \leq m \leq n$ and thus $j \in \{0, 1, \ldots, n\}$ and therefore

$$\left[x^j\right] f = \left[x^j\right] g \tag{34}$$

(by (33), applied to j instead of m). However, (21) (applied to m, a and f instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields

$$[x^m]\,(af) = \sum_{j=0}^{m} \left[x^{m-j}\right] a \cdot \underbrace{\left[x^j\right] f}_{\substack{=[x^j]g \\ \text{(by (34))}}} = \sum_{j=0}^{m} \left[x^{m-j}\right] a \cdot \left[x^j\right] g.$$

On the other hand, (21) (applied to m, a and g instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields

$$[x^m]\,(ag) = \sum_{j=0}^{m} \left[x^{m-j}\right] a \cdot \left[x^j\right] g.$$

Comparing these two equalities, we obtain $[x^m]\,(af) = [x^m]\,(ag)$. This proves Lemma 3.3.20. □

A consequence of Lemma 3.3.20 is the following fact:

Lemma 3.3.21. Let $u, v \in K[[x]]$ be two FPSs such that v is a multiple of u. Let $n \in \mathbb{N}$. Assume that

$$[x^m]\, u = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{35}$$

Then,

$$[x^m]\, v = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\}.$$

Proof of Lemma 3.3.21. We have assumed that v is a multiple of u. In other words, $v = ua$ for some $a \in K[[x]]$. Consider this a.

For each $m \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} [x^m] u &= 0 \qquad \text{(by (35))} \\ &= [x^m] 0 \qquad \left(\text{since the FPS 0 satisfies } [x^m] 0 = 0\right). \end{aligned}$$

Hence, Lemma 3.3.20 (applied to $f = u$ and $g = 0$) yields that

$$[x^m](au) = [x^m](a \cdot 0) \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{36}$$

Now, for each $m \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} [x^m] v &= [x^m](au) \qquad (\text{since } v = ua = au) \\ &= [x^m] \underbrace{(a \cdot 0)}_{=0} \qquad \text{(by (36))} \\ &= [x^m] 0 = 0. \end{aligned}$$

This proves Lemma 3.3.21. □

We can derive a further useful consequence from Lemma 3.3.21:

Lemma 3.3.22. Let $a, b, c, d \in K[[x]]$ be four FPSs. Let $n \in \mathbb{N}$. Assume that

$$[x^m] a = [x^m] b \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{37}$$

Assume further that

$$[x^m] c = [x^m] d \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{38}$$

Then,

$$[x^m](ac) = [x^m](bd) \qquad \text{for each } m \in \{0, 1, \ldots, n\}.$$

Proof of Lemma 3.3.22. For each $m \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} [x^m](a - b) &= [x^m] a - [x^m] b \qquad \text{(by (19))} \\ &= 0 \qquad \text{(by (37))}. \end{aligned}$$

Moreover, the FPS $ac - bc$ is a multiple of $a - b$ (since $ac - bc = (a - b) c$). Hence, Lemma 3.3.21 (applied to $u = a - b$ and $v = ac - bc$) shows that

$$[x^m](ac - bc) = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\} \tag{39}$$

(since we have $[x^m](a - b) = 0$ for each $m \in \{0, 1, \ldots, n\}$).

For each $m \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} [x^m](c - d) &= [x^m] c - [x^m] d \qquad \text{(by (19))} \\ &= 0 \qquad \text{(by (38))}. \end{aligned}$$

Moreover, the FPS $bc - bd$ is a multiple of $c - d$ (since $bc - bd = b(c - d) = (c - d)b$). Hence, Lemma 3.3.21 (applied to $u = c - d$ and $v = bc - bd$) shows that

$$[x^m](bc - bd) = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\} \tag{40}$$

(since we have $[x^m](c - d) = 0$ for each $m \in \{0, 1, \ldots, n\}$).

Now, let $m \in \{0, 1, \ldots, n\}$. Then, (19) yields $[x^m](ac - bc) = [x^m](ac) - [x^m](bc)$. Comparing this with (39), we obtain $[x^m](ac) - [x^m](bc) = 0$. In other words, $[x^m](ac) = [x^m](bc)$. On the other hand, (19) yields $[x^m](bc - bd) = [x^m](bc) - [x^m](bd)$. Comparing this with (40), we obtain $[x^m](bc) - [x^m](bd) = 0$. In other words, $[x^m](bc) = [x^m](bd)$. Hence, $[x^m](ac) = [x^m](bc) = [x^m](bd)$. This proves Lemma 3.3.22. □

3.4. Polynomials

3.4.1. Definition

Let us take a little side trip to relate FPSs to polynomials. As should be clear enough from the definitions, we can think of an FPS as a "polynomial with (potentially) infinitely many nonzero coefficients". This can be easily made precise. Indeed, we can **define** polynomials as FPSs that have only finitely many nonzero coefficients:

> **Definition 3.4.1. (a)** An FPS $a \in K[[x]]$ is said to be a *polynomial* if all but finitely many $n \in \mathbb{N}$ satisfy $[x^n] a = 0$ (that is, if all but finitely many coefficients of a are 0).
>
> **(b)** We let $K[x]$ be the set of all polynomials $a \in K[[x]]$. This set $K[x]$ is a subring of $K[[x]]$ (according to Theorem 3.4.2 below), and is called the *univariate polynomial ring* over K.

For example, $2 + 3x + 7x^5$ is a polynomial, whereas $1 + x + x^2 + x^3 + \cdots$ is not (unless K is a trivial ring).

The definition of a "polynomial" that you have seen in your abstract algebra course might be superficially different from that in Definition 3.4.1; but it necessarily is equivalent. (In fact, Definition 3.4.1 **(a)** can be restated as "a polynomial means a K-linear combination of the monomials $x^0, x^1, x^2, \ldots$", and it is clear that the monomials $x^0, x^1, x^2, \ldots$ in $K[[x]]$ are K-linearly independent; thus, the polynomial ring $K[x]$ as we have defined it in Definition 3.4.1 **(b)** is a free K-module with basis $(x^0, x^1, x^2, \ldots)$. The same is true for the polynomial ring $K[x]$ that you know from abstract algebra. Moreover, the rules for adding, subtracting and multiplying polynomials known from abstract algebra agree with the formulas for $\mathbf{a} + \mathbf{b}$, $\mathbf{a} - \mathbf{b}$ and $\mathbf{a} \cdot \mathbf{b}$ that we gave in Definition 3.2.5.)

We owe a theorem:

Theorem 3.4.2. The set $K[x]$ is a subring of $K[[x]]$ (that is, it is closed under addition, subtraction and multiplication, and contains the zero $\underline{0}$ and the unity $\underline{1}$) and is a K-subalgebra of $K[[x]]$.

Proof of Theorem 3.4.2 (sketched). Exercise. (The hardest part is to show that $K[x]$ is closed under multiplication. But this, too, is easy: Let $a, b \in K[x]$. Then, all but finitely many $n \in \mathbb{N}$ satisfy $[x^n]\, a = 0$ (since $a \in K[x]$). In other words, there exists a finite subset I of $\mathbb{N}$ such that

$$\left[x^i\right] a = 0 \text{ for all } i \in \mathbb{N} \setminus I. \tag{41}$$

Similarly, there exists a finite subset J of $\mathbb{N}$ such that

$$\left[x^j\right] b = 0 \text{ for all } j \in \mathbb{N} \setminus J. \tag{42}$$

Consider these I and J. Now, let S be the subset $\{i + j \mid i \in I \text{ and } j \in J\}$ of $\mathbb{N}$. This set S is again finite (since I and J are finite), and we can easily see (using (20)) that

$$[x^n]\,(ab) = 0 \text{ for all } n \in \mathbb{N} \setminus S.$$

Thus, all but finitely many $n \in \mathbb{N}$ satisfy $[x^n]\,(ab) = 0$ (since S is finite). This shows that $ab \in K[x]$. Hence, we have shown that $K[x]$ is closed under multiplication. The remaining claims of Theorem 3.4.2 are similar but easier.) □

3.4.2. Evaluation

As we now know, polynomials are just a special case of FPSs. However, they have some features that FPSs don't have in general. The most important of these features is *substitution*. To wit, we can substitute an element of K, or more generally an element of any K-algebra, into a polynomial (but generally not into an FPS). Before we explain how, let us recall the notions of rings and K-algebras:

Definition 3.4.3. The notion of a *ring* (also known as a *noncommutative ring*) is defined in the exact same way as we defined the notion of a commutative ring in Definition 3.2.1, except that the "Commutativity of multiplication" axiom is removed.

Examples of noncommutative rings[18] abound in linear algebra:

- For any $n \in \mathbb{N}$, the matrix ring $\mathbb{R}^{n \times n}$ (that is, the ring of all $n \times n$-matrices with real entries) is a ring. This ring is commutative if $n \leq 1$, but not if $n > 1$.

  More generally, if K is any ring (commutative or not), then the matrix ring $K^{n \times n}$ is a ring for every $n \in \mathbb{N}$.

[18] Note that the word "noncommutative ring" does not imply that the ring is not commutative; it merely means that commutativity is not required. Thus, any commutative ring is a noncommutative ring.

- The ring $\mathbb{H}$ of quaternions is a ring that is not commutative.
- If M is an abelian group, then the ring of all endomorphisms of M (that is, the ring of all $\mathbb{Z}$-linear maps from M to M) is a noncommutative ring. (Its multiplication is composition of endomorphisms.)

Next, let us recall the notion of a K-algebra. Recall that K is a fixed commutative ring.

Definition 3.4.4. A *K-algebra* is a set A equipped with four maps

$$\begin{aligned} \oplus &: A \times A \to A, \\ \ominus &: A \times A \to A, \\ \odot &: A \times A \to A, \\ \rightharpoonup &: K \times A \to A \end{aligned}$$

and two elements $\overrightarrow{0} \in A$ and $\overrightarrow{1} \in A$ satisfying the following properties:

1. The set A, equipped with the maps $\oplus$, $\ominus$ and $\odot$ and the two elements $\overrightarrow{0}$ and $\overrightarrow{1}$, is a (noncommutative) ring.
2. The set A, equipped with the maps $\oplus$, $\ominus$ and $\rightharpoonup$ and the element $\overrightarrow{0}$, is a K-module.
3. We have
$$\lambda \rightharpoonup (a \odot b) = (\lambda \rightharpoonup a) \odot b = a \odot (\lambda \rightharpoonup b) \tag{43}$$
for all $\lambda \in K$ and $a, b \in A$.

(Thus, in a nutshell, a K-algebra is a set A that is simultaneously a ring and a K-module, with the property that the ring A and the K-module A have the same addition, the same subtraction and the same zero, and satisfy the additional compatibility property (43).)

Consequently, a K-algebra is automatically a ring and a K-module. Thus, all the notations and shorthands that we have introduced for rings and for K-modules will also be used for K-algebras. For example, if A is a K-algebra, then both maps $\odot : A \times A \to A$ and $\rightharpoonup: K \times A \to A$ will be denoted by $\cdot$ unless there is a risk of confusion. (There is rarely a risk of confusion, since the two maps act on different inputs: $a \cdot b$ means $a \odot b$ if a belongs to A, and means $a \rightharpoonup b$ if a belongs to K. Often, even when an element a belongs to both A and K, the elements $a \odot b$ and $a \rightharpoonup b$ are equal, so confusion cannot arise.)

Examples of K-algebras include:

- the ring K itself;

- the ring $K[[x]]$ of FPSs (we have defined the relevant maps in Definition 3.2.5, and claimed the relevant properties in Theorem 3.2.6);
- its subring $K[x]$ (all its maps are inherited from $K[[x]]$);
- the matrix ring $K^{n\times n}$ for each $n \in \mathbb{N}$;
- any quotient ring of K (that is, any ring of the form K/I where I is an ideal of K);
- any commutative ring that contains K as a subring.

We can now define what it means to substitute an element of a K-algebra into a polynomial:

Definition 3.4.5. Let $f \in K[x]$ be a polynomial. Let A be any K-algebra. Let $a \in A$ be any element. We then define an element $f[a] \in A$ as follows:

Write f in the form $f = \sum\limits_{n\in\mathbb{N}} f_n x^n$ with $f_0, f_1, f_2, \ldots \in K$. (That is, $f_n = [x^n] f$ for each $n \in \mathbb{N}$.) Then, set

$$f[a] := \sum_{n\in\mathbb{N}} f_n a^n.$$

(This sum is essentially finite, since f is a polynomial.)

The element $f[a]$ is also denoted by $f \circ a$ and is called the *value* of f at a (or the *evaluation* of f at a, or the *result of substituting* a for x in f).

Many people write $f(a)$ for the value $f[a]$ we have just defined. Unfortunately, this leads to ambiguities (for example, $f(x+1)$ could mean either the value of f at $x+1$, or the product of f with $x+1$). By writing $f[a]$ or $f \circ a$ instead, I will avoid these ambiguities.

For example, if $f = 4x^3 + 2x + 7$, then $f[a] = 4a^3 + 2a + 7$. For another example, if $f = (x+5)^3$, then $f[a] = (a+5)^3$ (although this is not obvious; it follows from Theorem 3.4.6 below).

If f and g are two polynomials in $K[x]$, then the value $f[g] = f \circ g$ (this is the value of f at g; it is well-defined because $K[x]$ is a K-algebra) is also known as the *composition* of f with g. We note that any polynomial $f \in K[x]$ satisfies

$$\begin{aligned}
&f[x] = f \qquad \text{and} \\
&f[0] = \left[x^0\right] f = (\text{the constant term of } f) \qquad \text{and} \\
&f[1] = \left[x^0\right] f + \left[x^1\right] f + \left[x^2\right] f + \cdots = (\text{the sum of all coefficients of } f).
\end{aligned}$$

It is fairly common to write $f[x]$ instead of f for a polynomial, just to stress the fact that it is a polynomial in an indeterminate called x. The equality $f[x] = f$ justifies this.

Definition 3.4.5 is rather versatile. For example, if $f \in \mathbb{Z}[x]$ is a polynomial with integer coefficients, then it allows evaluating f at integers, at complex numbers, at residue classes in $\mathbb{Z}/n$, at square matrices, at other polynomials and at FPSs. More generally, a polynomial $f \in \mathbb{Z}[x]$ can be evaluated at any element of any ring, since any ring is automatically a $\mathbb{Z}$-algebra. Evaluating polynomials at square matrices is an important idea in linear algebra (e.g., the Cayley–Hamilton theorem is concerned with the characteristic polynomial of a square matrix, evaluated at this matrix itself).

The following theorem ([19s, Theorem 7.6.3]) surveys the most basic properties of values of polynomials:

Theorem 3.4.6. Let A be a K-algebra. Let $a \in A$.

(a) Any $f, g \in K[x]$ satisfy

$$(f+g)[a] = f[a] + g[a] \qquad \text{and} \qquad (fg)[a] = f[a] \cdot g[a].$$

(b) Any $\lambda \in K$ and $f \in K[x]$ satisfy

$$(\lambda f)[a] = \lambda \cdot f[a].$$

(c) Any $\lambda \in K$ satisfies $\underline{\lambda}[a] = \lambda \cdot 1_A$, where 1_A is the unity of the ring A. (This is often written as "$\underline{\lambda}[a] = \lambda$", but keep in mind that the "λ" on the right hand side of this equality is understood to be "coerced into A", so it actually means "the element of A corresponding to λ", which is $\lambda \cdot 1_A$.)

(d) We have $x[a] = a$.

(e) We have $x^i[a] = a^i$ for each $i \in \mathbb{N}$.

3.5. Substitution and evaluation of power series

3.5.1. Defining substitution

Definition 3.4.5 shows that if $f \in K[x]$ is a polynomial, then almost anything (to be more precise: any element of a K-algebra) can be substituted into f.

In contrast, if $f \in K[[x]]$ is a FPS, then there are far fewer things that can be substituted into f. Even elements of K itself cannot always be substituted into f. For example, if we try to substitute 1 for x in the FPS $1 + x + x^2 + x^3 + \cdots$, then we get

$$1 + 1 + 1^2 + 1^3 + \cdots = 1 + 1 + 1 + 1 + \cdots,$$

which is undefined. Real analysis can help make sense of certain values of FPSs (for example, substituting $\frac{1}{2}$ for x into the FPS $1 + x + x^2 + x^3 + \cdots$ yields the convergent series $1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = 2$), but this is subtle and specific to certain numbers and certain FPSs.[19]

[19] For instance, it is not hard to see that there is no nonzero complex number that can be

Thus, polynomials have an advantage over FPSs.

However, not all is lost. **Some** things can be substituted into an FPS. For example:

- We can always substitute 0 for x in an FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. The result is
$$a_0 + a_1 0 + a_2 0^2 + a_3 0^3 + \cdots = a_0 + 0 + 0 + 0 + \cdots = a_0.$$

- We can always substitute x for x in an FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. The result is the same FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$ that we started with (obviously).

- We can always substitute $2x$ for x in an FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. The result is
$$a_0 + a_1 (2x) + a_2 (2x)^2 + a_3 (2x)^3 + \cdots = a_0 + 2a_1 x + 4a_2 x^2 + 8a_3 x^3 + \cdots.$$

- We can always substitute $x^2 + x$ for x in an FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$. This is less obvious, so let me explain why. If we try to substitute $x^2 + x$ for x in an FPS $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$, then we obtain
$$\begin{aligned}
&\left(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots\right)\left[x + x^2\right] \\
&= a_0 + a_1\left(x + x^2\right) + a_2\left(x + x^2\right)^2 + a_3\left(x + x^2\right)^3 + \cdots \\
&= a_0 + a_1\left(x + x^2\right) + a_2\left(x^2 + 2x^3 + x^4\right) + a_3\left(x^3 + 3x^4 + 3x^5 + x^6\right) + \cdots \\
&= a_0 + a_1 x + (a_1 + a_2)\, x^2 + (2a_2 + a_3)\, x^3 + (a_2 + 3a_3 + a_4)\, x^4 + \cdots.
\end{aligned}$$
I claim that the right hand side here is well-defined. To prove this, I need to show that for each $n \in \mathbb{N}$, the coefficient of x^n on this right hand side is a **finite** sum of a_i's. Indeed, fix $n \in \mathbb{N}$. Recall that the right hand side is obtained by expanding the infinite sum
$$a_0 + a_1\left(x + x^2\right) + a_2\left(x + x^2\right)^2 + a_3\left(x + x^2\right)^3 + \cdots.$$
Only the first $n+1$ addends of this infinite sum (i.e., only the addends $a_k\left(x + x^2\right)^k$ with $k \leq n$) can contribute to the coefficient of x^n, since any of the remaining addends is a multiple of x^{n+1} (because it has the form $a_k\left(x + x^2\right)^k = a_k\left(x\left(1 + x\right)\right)^k = a_k x^k \left(1 + x\right)^k$ with $k \geq n+1$) and thus has

substituted into the FPS $\sum\limits_{n \in \mathbb{N}} n! x^n$ to obtain a convergent result. Thus, even though some complex numbers can be substituted into some FPSs, there is no complex number other than 0 that can be substituted into **every** FPS.

a zero coefficient of x^n. Hence, the coefficient of x^n in this infinite sum equals the coefficient of x^n in the **finite** sum

$$a_0 + a_1\left(x+x^2\right) + a_2\left(x+x^2\right)^2 + a_3\left(x+x^2\right)^3 + \cdots + a_n\left(x+x^2\right)^n.$$

But the latter coefficient is clearly a **finite** sum of a_i's. Thus, my claim is proved, and it follows that the result of substituting $x^2 + x$ for x in an FPS $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$ is well-defined.

The idea of the last example can be generalized; there was nothing special about $x + x^2$ that we used other than the fact that $x + x^2$ is a multiple of x (that is, an FPS whose constant term is 0). Thus, generalizing our reasoning from this example, we can convince ourselves that any FPS g that is a multiple of x (that is, whose constant term is 0) can be substituted into any FPS. Let us introduce a notation for this, exactly like we did for substituting things into polynomials:

Definition 3.5.1. Let f and g be two FPSs in $K[[x]]$. Assume that $\left[x^0\right] g = 0$ (that is, $g = g_1x^1 + g_2x^2 + g_3x^3 + \cdots$ for some $g_1, g_2, g_3, \ldots \in K$).

We then define an FPS $f[g] \in K[[x]]$ as follows:

Write f in the form $f = \sum\limits_{n\in\mathbb{N}} f_nx^n$ with $f_0, f_1, f_2, \ldots \in K$. (That is, $f_n = [x^n] f$ for each $n \in \mathbb{N}$.) Then, set

$$f[g] := \sum_{n\in\mathbb{N}} f_ng^n. \qquad (44)$$

(This sum is well-defined, as we will see in Proposition 3.5.2 **(b)** below.)

This FPS $f[g]$ is also denoted by $f \circ g$, and is called the *composition* of f with g, or the result of *substituting* g for x in f.

Once again, it is not uncommon to see this FPS $f[g]$ denoted by $f(g)$, but I will eschew the latter notation (since it can be confused with a product).

In order to prove that Definition 3.5.1 makes sense, we need to ensure that the infinite sum $\sum\limits_{n\in\mathbb{N}} f_ng^n$ in (44) is well-defined. The proof of this fact is analogous to the reasoning I used in the last example; let me present it again in the general case:

Proposition 3.5.2. Let f and g be two FPSs in $K[[x]]$. Assume that $\left[x^0\right] g = 0$. Write f in the form $f = \sum\limits_{n\in\mathbb{N}} f_nx^n$ with $f_0, f_1, f_2, \ldots \in K$. Then:

(a) For each $n \in \mathbb{N}$, the first n coefficients of the FPS g^n are 0.

(b) The sum $\sum\limits_{n\in\mathbb{N}} f_ng^n$ is well-defined, i.e., the family $\left(f_ng^n\right)_{n\in\mathbb{N}}$ is summable.

(c) We have $\left[x^0\right]\left(\sum\limits_{n\in\mathbb{N}} f_ng^n\right) = f_0$.

Proof of Proposition 3.5.2. **(a)** This is easily proved by induction on n. Here is a shorter alternative argument:

The FPS g has constant term $\left[x^0\right] g = 0$. Hence, Lemma 3.3.16 (applied to $a = g$) yields that there exists an $h \in K[[x]]$ such that $g = xh$. Consider this h.

Now, let $n \in \mathbb{N}$. From $g = xh$, we obtain $g^n = (xh)^n = x^n h^n$. However, Lemma 3.3.17 (applied to $k = n$ and $a = h^n$) yields that the first n coefficients of the FPS $x^n h^n$ are 0. In other words, the first n coefficients of the FPS g^n are 0 (since $g^n = x^n h^n$). Thus, Proposition 3.5.2 **(a)** is proved.

(b) This follows from part **(a)**. Here are the details.

We must prove that the family $(f_n g^n)_{n\in\mathbb{N}}$ is summable. In other words, we must prove that the family $\left(f_i g^i\right)_{i\in\mathbb{N}}$ is summable (since $\left(f_i g^i\right)_{i\in\mathbb{N}} = (f_n g^n)_{n\in\mathbb{N}}$). In other words, we must prove that for each $n \in \mathbb{N}$, all but finitely many $i \in \mathbb{N}$ satisfy $[x^n]\left(f_i g^i\right) = 0$ (by the definition of "summable"). So let us prove this.

Fix $n \in \mathbb{N}$. We must prove that all but finitely many $i \in \mathbb{N}$ satisfy $[x^n]\left(f_i g^i\right) = 0$.

Indeed, let $i \in \mathbb{N}$ satisfy $i > n$. Then, $n < i$. Now, the first i coefficients of the FPS g^i are 0 (by Proposition 3.5.2 **(a)**, applied to i instead of n). However, the coefficient $[x^n]\left(g^i\right)$ of g^i is one of these first i coefficients (because $n < i$). Thus, this coefficient $[x^n]\left(g^i\right)$ must be 0. Now, $f_i \in K$; thus, (23) (applied to $\lambda = f_i$ and $\mathbf{a} = g^i$) yields $[x^n]\left(f_i g^i\right) = f_i \cdot \underbrace{[x^n]\left(g^i\right)}_{=0} = 0$.

Forget that we fixed i. We thus have shown that all $i \in \mathbb{N}$ satisfying $i > n$ satisfy $[x^n]\left(f_i g^i\right) = 0$. Hence, all but finitely many $i \in \mathbb{N}$ satisfy $[x^n]\left(f_i g^i\right) = 0$ (because all but finitely many $i \in \mathbb{N}$ satisfy $i > n$). This is precisely what we wanted to prove. Thus, Proposition 3.5.2 **(b)** is proved.

(c) Let n be a positive integer. We shall first show that $\left[x^0\right](f_n g^n) = 0$.

Indeed, Proposition 3.5.2 **(a)** shows that the first n coefficients of the FPS g^n are 0. However, the coefficient $\left[x^0\right](g^n)$ is one of these first n coefficients (since n is positive). Thus, this coefficient $\left[x^0\right](g^n)$ must be 0. Now, $f_n \in K$; thus, (23) (applied to f_n, g^n and 0 instead of λ, $\mathbf{a}$ and n) yields $\left[x^0\right](f_n g^n) = f_n \cdot \underbrace{\left[x^0\right](g^n)}_{=0} = 0$.

Forget that we fixed n. We thus have shown that

$$\left[x^0\right](f_n g^n) = 0 \qquad \text{for each positive integer } n. \tag{45}$$

Now,

$$\begin{aligned}
\left[x^0\right]\left(\sum_{n\in\mathbb{N}} f_n g^n\right) &= \sum_{n\in\mathbb{N}} \left[x^0\right](f_n g^n) \qquad \text{(by (25))} \\
&= \left[x^0\right]\left(f_0 \underbrace{g^0}_{=\underline{1}}\right) + \sum_{n>0} \underbrace{\left[x^0\right](f_n g^n)}_{\substack{=0 \\ \text{(by (45))}}} \\
&\qquad \left(\begin{array}{c}\text{here, we have split off the} \\ \text{addend for } n=0 \text{ from the sum}\end{array}\right) \\
&= \left[x^0\right] \underbrace{(f_0\underline{1})}_{\substack{=f_0(1,0,0,0,\ldots) \\ =(f_0,0,0,0,\ldots)}} + \underbrace{\sum_{n>0} 0}_{=0} = \left[x^0\right](f_0,0,0,0,\ldots) = f_0.
\end{aligned}$$

This proves Proposition 3.5.2 **(c)**. □

Example 3.5.3. The FPS $x+x^2$ has constant term $\left[x^0\right]\left(x+x^2\right)=0$. Hence, according to Definition 3.5.1, we can substitute it for x into $1+x+x^2+x^3+\cdots$. The result is

$$\begin{aligned}
&\left(1+x+x^2+x^3+\cdots\right)\left[x+x^2\right] \\
&= 1+\left(x+x^2\right)+\left(x+x^2\right)^2+\left(x+x^2\right)^3+\left(x+x^2\right)^4+\left(x+x^2\right)^5+\cdots \\
&= 1+x+2x^2+3x^3+5x^4+8x^5+\cdots.
\end{aligned}$$

The right hand side appears to be $f_1+f_2x+f_3x^2+f_4x^3+\cdots$, where $(f_0,f_1,f_2,\ldots)$ is the Fibonacci sequence (as defined in Section 3.1). Let me show that this indeed the case.

In Example 1 in Section 3.1, we had shown that

$$f_0+f_1x+f_2x^2+f_3x^3+\cdots = \frac{x}{1-x-x^2}.$$

Thus,

$$\begin{aligned}
\frac{x}{1-x-x^2} &= \underbrace{f_0}_{=0} + f_1x+f_2x^2+f_3x^3+\cdots \\
&= f_1x+f_2x^2+f_3x^3+f_4x^4+\cdots \\
&= x\left(f_1+f_2x+f_3x^2+f_4x^3+\cdots\right).
\end{aligned}$$

Cancelling x from this equality (this is indeed allowed – make sure you understand why!), we obtain

$$\frac{1}{1-x-x^2} = f_1+f_2x+f_3x^2+f_4x^3+\cdots.$$

However, it appears reasonable to expect that

$$\frac{1}{1-x-x^2} = \frac{1}{1-x}\left[x+x^2\right], \tag{46}$$

because substituting $x+x^2$ for x in the expression $\dfrac{1}{1-x}$ results in $\dfrac{1}{1-x-x^2}$. This is plausible but not obvious – after all, we defined $\dfrac{1}{1-x}\left[x+x^2\right]$ to be the result of substituting $x+x^2$ for x into the **expanded** version of $\dfrac{1}{1-x}$ (which is $1+x+x^2+x^3+\cdots$), not into the fractional expression $\dfrac{1}{1-x}$. Nevertheless, (46) is true (and will soon be proved). If we take this fact for granted, then our claim easily follows:

$$\begin{aligned} f_1+f_2x+f_3x^2+f_4x^3+\cdots &= \frac{1}{1-x-x^2} = \frac{1}{1-x}\left[x+x^2\right] \\ &= \left(1+x+x^2+x^3+\cdots\right)\left[x+x^2\right] \end{aligned}$$

(since $\dfrac{1}{1-x} = 1+x+x^2+x^3+\cdots$).

3.5.2. Laws of substitution

The plausible but nontrivial statement (46) that we have just used follows from part **(c)** of the following proposition:[20]

Proposition 3.5.4. Composition of FPSs satisfies the rules you would expect it to satisfy:

(a) If $f_1, f_2, g \in K[[x]]$ satisfy $\left[x^0\right]g = 0$, then $(f_1+f_2)\circ g = f_1\circ g + f_2\circ g$.

(b) If $f_1, f_2, g \in K[[x]]$ satisfy $\left[x^0\right]g = 0$, then $(f_1\cdot f_2)\circ g = (f_1\circ g)\cdot(f_2\circ g)$.

(c) If $f_1, f_2, g \in K[[x]]$ satisfy $\left[x^0\right]g = 0$, then $\dfrac{f_1}{f_2}\circ g = \dfrac{f_1\circ g}{f_2\circ g}$, as long as f_2 is invertible. (In particular, $f_2\circ g$ is automatically invertible under these assumptions.)

(d) If $f, g \in K[[x]]$ satisfy $\left[x^0\right]g = 0$, then $f^k\circ g = (f\circ g)^k$ for each $k\in\mathbb{N}$.

(e) If $f, g, h \in K[[x]]$ satisfy $\left[x^0\right]g = 0$ and $\left[x^0\right]h = 0$, then $\left[x^0\right](g\circ h) = 0$ and $(f\circ g)\circ h = f\circ(g\circ h)$.

(f) We have $\underline{a}\circ g = \underline{a}$ for each $a\in K$ and $g\in K[[x]]$.

(g) We have $x\circ g = g\circ x = g$ for each $g\in K[[x]]$.

[20] We are treating the symbol "$\circ$" similarly to the multiplication sign $\cdot$ in our PEMDAS convention. Thus, an expression like "$f_1\circ g+f_2\circ g$" is understood to mean $(f_1\circ g)+(f_2\circ g)$.

(h) If $(f_i)_{i\in I} \in K[[x]]^I$ is a summable family of FPSs, and if $g \in K[[x]]$ is an FPS satisfying $[x^0]\, g = 0$, then the family $(f_i \circ g)_{i\in I} \in K[[x]]^I$ is summable as well and we have $\left(\sum\limits_{i\in I} f_i\right) \circ g = \sum\limits_{i\in I} f_i \circ g$.

For our proof of Proposition 3.5.4, we will need the following lemma:

Lemma 3.5.5. Let $f, g \in K[[x]]$ satisfy $[x^0]\, g = 0$. Let $k \in \mathbb{N}$ be such that the first k coefficients of f are 0. Then, the first k coefficients of $f \circ g$ are 0.

Proof of Lemma 3.5.5. This is very similar to the proof of Proposition 3.5.2 **(a)**.

We have $[x^0]\, g = 0$. Hence, Lemma 3.3.16 (applied to $a = g$) yields that there exists an $h \in K[[x]]$ such that $g = xh$. Consider this h.

Write the FPS f in the form $f = (f_0, f_1, f_2, \ldots)$. Then, the first k coefficients of f are $f_0, f_1, \ldots, f_{k-1}$. Hence, these coefficients $f_0, f_1, \ldots, f_{k-1}$ are 0 (since the first k coefficients of f are 0). In other words,

$$f_n = 0 \qquad \text{for each } n < k. \tag{47}$$

Now, $f = (f_0, f_1, f_2, \ldots) = \sum\limits_{n\in\mathbb{N}} f_n x^n$ with $f_0, f_1, f_2, \ldots \in K$. Hence, Definition 3.5.1 yields

$$f[g] = \sum_{n\in\mathbb{N}} f_n g^n = \sum_{\substack{n\in\mathbb{N};\\ n<k}} \underbrace{f_n}_{\substack{=0\\ \text{(by (47))}}} g^n + \underbrace{\sum_{\substack{n\in\mathbb{N};\\ n\geq k}}}_{=\sum\limits_{\substack{n\in\mathbb{N};\\ k\leq n}}} f_n \underbrace{g^n}_{\substack{=(xh)^n\\ \text{(since } g=xh)}} = \underbrace{\sum_{\substack{n\in\mathbb{N};\\ n<k}} 0g^n}_{=0} + \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} f_n (xh)^n$$

$$= \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} f_n \underbrace{(xh)^n}_{=x^n h^n} = \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} f_n x^n h^n.$$

Thus,

$$f \circ g = f[g] = \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} \underbrace{f_n x^n}_{=x^n f_n} h^n = \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} x^n f_n h^n.$$

But this ensures that the first k coefficients of $f \circ g$ are 0 [21]. Thus, Lemma 3.5.5 follows. □

Our proof of Proposition 3.5.4 will furthermore use the *Kronecker delta notation*:

[21] *Proof.* We must show that $[x^m]\,(f \circ g) = 0$ for any nonnegative integer $m < k$. But we can do

Definition 3.5.6. If i and j are any objects, then $\delta_{i,j}$ means the element $\begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases}$ of K.

For example, $\delta_{2,2} = 1$ and $\delta_{3,8} = 0$.

Proof of Proposition 3.5.4. The proof is long and not particularly combinatorial. I am merely writing it down because it is so rarely explained in the literature.

(a) This is an easy consequence of the definitions, and also appears in [Loehr11, Theorem 7.62] and [Brewer14, Proposition 2.2.2].

Here are the details: Let $f_1, f_2, g \in K[[x]]$ satisfy $[x^0]\, g = 0$. Write the FPSs f_1 and f_2 as

$$f_1 = \sum_{n\in\mathbb{N}} f_{1,n} x^n \qquad \text{and} \qquad f_2 = \sum_{n\in\mathbb{N}} f_{2,n} x^n \tag{48}$$

with $f_{1,0}, f_{1,1}, f_{1,2}, \ldots \in K$ and $f_{2,0}, f_{2,1}, f_{2,2}, \ldots \in K$. Then, adding the two equalities in (48) together, we find

$$f_1 + f_2 = \sum_{n\in\mathbb{N}} f_{1,n} x^n + \sum_{n\in\mathbb{N}} f_{2,n} x^n = \sum_{n\in\mathbb{N}} \underbrace{\left(f_{1,n} x^n + f_{2,n} x^n\right)}_{=(f_{1,n}+f_{2,n})x^n} = \sum_{n\in\mathbb{N}} \left(f_{1,n} + f_{2,n}\right) x^n.$$

Thus, Definition 3.5.1 (applied to $f = f_1 + f_2$) yields

$$\left(f_1 + f_2\right)[g] = \sum_{n\in\mathbb{N}} \left(f_{1,n} + f_{2,n}\right) g^n \tag{49}$$

(since $f_{1,n} + f_{2,n} \in K$ for each $n \in \mathbb{N}$).

On the other hand, we have $f_1 = \sum\limits_{n\in\mathbb{N}} f_{1,n} x^n$. Thus, Definition 3.5.1 yields $f_1[g] = \sum\limits_{n\in\mathbb{N}} f_{1,n} g^n$ (since $f_{1,n} \in K$ for each $n \in \mathbb{N}$). Similarly, $f_2[g] = \sum\limits_{n\in\mathbb{N}} f_{2,n} g^n$.

this directly: If m is a nonnegative integer such that $m < k$, then

$$\begin{aligned} \left[x^m\right](f \circ g) &= \left[x^m\right]\left(\sum_{\substack{n\in\mathbb{N};\\ k\leq n}} x^n f_n h^n\right) \qquad \left(\text{since } f \circ g = \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} x^n f_n h^n\right) \\ &= \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} \underbrace{\left[x^m\right]\left(x^n f_n h^n\right)}_{\substack{=\sum\limits_{i=0}^{m}\left[x^i\right](x^n)\cdot\left[x^{m-i}\right](f_n h^n) \\ \text{(by (20),} \\ \text{applied to } x^n,\ f_n h^n \text{ and } m \\ \text{instead of } \mathbf{a},\ \mathbf{b} \text{ and } n)}} = \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} \sum_{i=0}^{m} \underbrace{\left[x^i\right](x^n)}_{\substack{=0 \\ \text{(since } i\leq m<k\leq n \\ \text{and thus } i\neq n)}} \cdot \left[x^{m-i}\right](f_n h^n) \\ &= \sum_{\substack{n\in\mathbb{N};\\ k\leq n}} \sum_{i=0}^{m} 0 \cdot \left[x^{m-i}\right](f_n h^n) = 0, \end{aligned}$$

exactly as we wanted to show.

Adding these two equalities together, we obtain

$$f_1[g]+f_2[g]=\sum_{n\in\mathbb{N}} f_{1,n}g^n+\sum_{n\in\mathbb{N}} f_{2,n}g^n=\sum_{n\in\mathbb{N}} \underbrace{\left(f_{1,n}g^n+f_{2,n}g^n\right)}_{=(f_{1,n}+f_{2,n})g^n}=\sum_{n\in\mathbb{N}}\left(f_{1,n}+f_{2,n}\right)g^n.$$

Comparing this with (49), we obtain $(f_1+f_2)[g]=f_1[g]+f_2[g]$. In other words, $(f_1+f_2)\circ g=f_1\circ g+f_2\circ g$ (since the notation $f\circ g$ is synonymous to $f[g]$). This proves Proposition 3.5.4 **(a)**.

(f) This is a near-trivial consequence of the definitions. To wit: Let $a\in K$. Then,

$$\begin{aligned}\sum_{n\in\mathbb{N}} a\delta_{n,0}x^n &= a\underbrace{\delta_{0,0}}_{\substack{=1\\ \text{(since }0=0)}}\underbrace{x^0}_{=\underline{1}}+\sum_{\substack{n\in\mathbb{N};\\ n\neq 0}} a\underbrace{\delta_{n,0}}_{\substack{=0\\ \text{(since }n\neq 0)}}x^n=a\cdot\underline{1}+\underbrace{\sum_{\substack{n\in\mathbb{N};\\ n\neq 0}} a\cdot 0x^n}_{=0}\\ &= a\cdot\underline{1}=a\cdot(1,0,0,0,\ldots)=(a\cdot 1,a\cdot 0,a\cdot 0,a\cdot 0,\ldots)\\ &=(a,0,0,0,\ldots)=\underline{a}. \qquad (50)\end{aligned}$$

Let $g\in K[[x]]$. We must prove that $\underline{a}\circ g=\underline{a}$. From (50), we obtain $\underline{a}=\sum\limits_{n\in\mathbb{N}} a\delta_{n,0}x^n$. Hence, Definition 3.5.1 (or Definition 3.4.5) yields $\underline{a}[g]=\sum\limits_{n\in\mathbb{N}} a\delta_{n,0}g^n$ (since $a\delta_{n,0}\in K$ for each $n\in\mathbb{N}$). Thus,

$$\begin{aligned}\underline{a}[g]=\sum_{n\in\mathbb{N}} a\delta_{n,0}g^n &= a\underbrace{\delta_{0,0}}_{\substack{=1\\ \text{(since }0=0)}}\underbrace{g^0}_{=\underline{1}}+\sum_{\substack{n\in\mathbb{N};\\ n\neq 0}} a\underbrace{\delta_{n,0}}_{\substack{=0\\ \text{(since }n\neq 0)}}g^n=a\cdot\underline{1}+\underbrace{\sum_{\substack{n\in\mathbb{N};\\ n\neq 0}} a\cdot 0g^n}_{=0}\\ &= a\cdot\underline{1}=\underline{a}.\end{aligned}$$

In other words, $\underline{a}\circ g=\underline{a}$ (since $\underline{a}\circ g$ is a synonym for $\underline{a}[g]$). This proves Proposition 3.5.4 **(f)**.

(g) This is easy, too. Indeed, we have

$$\begin{aligned}\sum_{n\in\mathbb{N}}\delta_{n,1}x^n &= \underbrace{\delta_{1,1}}_{\substack{=1\\ \text{(since }1=1)}}\underbrace{x^1}_{=x}+\sum_{\substack{n\in\mathbb{N};\\ n\neq 1}}\underbrace{\delta_{n,1}}_{\substack{=0\\ \text{(since }n\neq 1)}}x^n=x+\underbrace{\sum_{\substack{n\in\mathbb{N};\\ n\neq 1}} 0x^n}_{=0}\\ &= x. \qquad (51)\end{aligned}$$

Let $g\in K[[x]]$. We must prove that $x\circ g=g\circ x=g$. From (51), we obtain $x=\sum\limits_{n\in\mathbb{N}}\delta_{n,1}x^n$. Hence, Definition 3.5.1 (or Definition 3.4.5) yields $x[g]=\sum\limits_{n\in\mathbb{N}}\delta_{n,1}g^n$ (since $\delta_{n,1}\in K$ for each $n\in\mathbb{N}$). Thus,

$$x[g]=\sum_{n\in\mathbb{N}}\delta_{n,1}g^n=\underbrace{\delta_{1,1}}_{\substack{=1\\ \text{(since }1=1)}}\underbrace{g^1}_{=g}+\sum_{\substack{n\in\mathbb{N};\\ n\neq 1}}\underbrace{\delta_{n,1}}_{\substack{=0\\ \text{(since }n\neq 1)}}g^n=g+\underbrace{\sum_{\substack{n\in\mathbb{N};\\ n\neq 1}} 0g^n}_{=0}=g.$$

In other words, $x \circ g = g$ (since $x \circ g$ is a synonym for $x[g]$).

Next, let us write g in the form $g = \sum\limits_{n \in \mathbb{N}} g_n x^n$ for some $g_0, g_1, g_2, \ldots \in K$. Then, Definition 3.5.1 yields $g[x] = \sum\limits_{n \in \mathbb{N}} g_n x^n = g$. Thus, $g \circ x = g[x] = g$. Combining this with $x \circ g = g$, we obtain $x \circ g = g \circ x = g$. This proves Proposition 3.5.4 **(g)**.

(b) This appears in [Loehr11, Theorem 7.62] and [Brewer14, Proposition 2.2.2]. Here is the proof:

Let $f_1, f_2, g \in K[[x]]$ satisfy $[x^0]\, g = 0$. Write the FPSs f_1 and f_2 as

$$f_1 = \sum_{n \in \mathbb{N}} f_{1,n} x^n \qquad \text{and} \qquad f_2 = \sum_{n \in \mathbb{N}} f_{2,n} x^n \tag{52}$$

with $f_{1,0}, f_{1,1}, f_{1,2}, \ldots \in K$ and $f_{2,0}, f_{2,1}, f_{2,2}, \ldots \in K$. Thus, Definition 3.5.1 yields

$$f_1[x] = \sum_{n \in \mathbb{N}} f_{1,n} x^n = f_1 \qquad \text{and} \qquad f_2[x] = \sum_{n \in \mathbb{N}} f_{2,n} x^n = f_2$$

and

$$f_1[g] = \sum_{n \in \mathbb{N}} f_{1,n} g^n \qquad \text{and} \qquad f_2[g] = \sum_{n \in \mathbb{N}} f_{2,n} g^n.$$

Hence,

$$f_1[g] = \sum_{n \in \mathbb{N}} f_{1,n} g^n = \sum_{i \in \mathbb{N}} f_{1,i} g^i \qquad \text{and}$$
$$f_2[g] = \sum_{n \in \mathbb{N}} f_{2,n} g^n = \sum_{j \in \mathbb{N}} f_{2,j} g^j.$$

Multiplying these two equalities together, we find

$$\begin{aligned}
f_1[g] \cdot f_2[g] &= \left(\sum_{i \in \mathbb{N}} f_{1,i} g^i\right) \left(\sum_{j \in \mathbb{N}} f_{2,j} g^j\right) = \sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}} \underbrace{f_{1,i} g^i f_{2,j} g^j}_{\substack{= f_{1,i} f_{2,j} g^i g^j \\ = f_{1,i} f_{2,j} g^{i+j}}} \\
&= \underbrace{\sum_{i \in \mathbb{N}} \sum_{j \in \mathbb{N}}}_{= \sum\limits_{(i,j) \in \mathbb{N}^2}} f_{1,i} f_{2,j} g^{i+j} = \underbrace{\sum_{(i,j) \in \mathbb{N}^2}}_{= \sum\limits_{n \in \mathbb{N}} \sum\limits_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}}} f_{1,i} f_{2,j} g^{i+j} \\
&= \sum_{n \in \mathbb{N}} \sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}} f_{1,i} f_{2,j} \underbrace{g^{i+j}}_{\substack{= g^n \\ (\text{since } i+j=n)}} = \sum_{n \in \mathbb{N}} \sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}} f_{1,i} f_{2,j} g^n \\
&= \sum_{n \in \mathbb{N}} \left(\sum_{\substack{(i,j) \in \mathbb{N}^2; \\ i+j=n}} f_{1,i} f_{2,j} \right) g^n.
\end{aligned} \tag{53}$$

However, we can apply the same computations to x instead of g (since x is also an FPS with $\left[x^0\right] x = 0$). Thus, we obtain

$$f_1 \left[x\right] \cdot f_2 \left[x\right] = \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2;\\ i+j=n}} f_{1,i} f_{2,j} \right) x^n.$$

In view of $f_1 \left[x\right] = f_1$ and $f_2 \left[x\right] = f_2$, this rewrites as

$$f_1 \cdot f_2 = \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2;\\ i+j=n}} f_{1,i} f_{2,j} \right) x^n.$$

Hence, Definition 3.5.1 yields

$$\left(f_1 \cdot f_2\right) \left[g\right] = \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}^2;\\ i+j=n}} f_{1,i} f_{2,j} \right) g^n$$

(since $\sum\limits_{\substack{(i,j)\in\mathbb{N}^2;\\ i+j=n}} f_{1,i} f_{2,j} \in K$ for each $n \in \mathbb{N}$). Comparing this with (53), we obtain

$$\left(f_1 \cdot f_2\right) \left[g\right] = f_1 \left[g\right] \cdot f_2 \left[g\right].$$

In other words, $\left(f_1 \cdot f_2\right) \circ g = \left(f_1 \circ g\right) \cdot \left(f_2 \circ g\right)$ (since the notation $f \circ g$ is synonymous to $f \left[g\right]$). This proves Proposition 3.5.4 **(b)**.

Did you notice it? I have cheated. The above proof of Proposition 3.5.4 **(b)** relied on some manipulations of infinite sums that need to be justified. Namely, we replaced "$\sum\limits_{i\in\mathbb{N}} \sum\limits_{j\in\mathbb{N}}$" by "$\sum\limits_{(i,j)\in\mathbb{N}^2}$". This is an application of the "discrete Fubini rule", and as we said above, this rule can only be used if we know that the family $\left(f_{1,i} f_{2,j} g^{i+j}\right)_{(i,j)\in\mathbb{N}\times\mathbb{N}}$ is summable. In other words, we need to show the following statement:

> *Statement 1:* For each $m \in \mathbb{N}$, all but finitely many pairs $(i,j) \in \mathbb{N} \times \mathbb{N}$ satisfy $\left[x^m\right] \left(f_{1,i} f_{2,j} g^{i+j}\right) = 0$.

We shall achieve this by proving the following statement:

> *Statement 2:* For any three nonnegative integers m, i, j with $m < i + j$, we have $\left[x^m\right] \left(g^{i+j}\right) = 0$.

[*Proof of Statement 2:* Let m, i, j be three nonnegative integers with $m < i + j$. We must show that $\left[x^m\right] \left(g^{i+j}\right) = 0$.

We have $\left[x^0\right] g = 0$. Hence, Lemma 3.3.16 (applied to $a = g$) shows that there exists an $h \in K\left[\left[x\right]\right]$ such that $g = xh$. Consider this h.

Now, from $g = xh$, we obtain $g^{i+j} = (xh)^{i+j} = x^{i+j}h^{i+j}$. However, Lemma 3.3.17 (applied to $i + j$ and h^{i+j} instead of k and a) shows that the first $i + j$ coefficients of the FPS $x^{i+j}h^{i+j}$ are 0. In other words, the first $i + j$ coefficients of the FPS g^{i+j} are 0 (since $g^{i+j} = x^{i+j}h^{i+j}$). But $[x^m] \left(g^{i+j}\right)$ is one of these first $i + j$ coefficients (since $m < i + j$). Thus, we conclude that $[x^m] \left(g^{i+j}\right) = 0$. This proves Statement 2.]

[*Proof of Statement 1:* Let $m \in \mathbb{N}$. If $(i, j) \in \mathbb{N} \times \mathbb{N}$ is a pair satisfying $m < i + j$, then

$$\begin{aligned}[x^m] \left(f_{1,i}f_{2,j}g^{i+j}\right) &= f_{1,i}f_{2,j} \underbrace{[x^m] \left(g^{i+j}\right)}_{\substack{=0 \\ \text{(by Statement 2)}}} \qquad \text{(by (23))} \\ &= 0.\end{aligned}$$

Thus, all but finitely many pairs $(i, j) \in \mathbb{N} \times \mathbb{N}$ satisfy $[x^m] \left(f_{1,i}f_{2,j}g^{i+j}\right) = 0$ (because all but finitely many such pairs satisfy $m < i + j$). This proves Statement 1.]

As explained above, Statement 1 shows that the family $\left(f_{1,i}f_{2,j}g^{i+j}\right)_{(i,j)\in\mathbb{N}\times\mathbb{N}}$ is summable, and thus our interchange of summation signs made above is justified. This completes our proof of Proposition 3.5.4 **(b)**.

(c) This follows easily from parts **(b)** and **(f)**. In detail: Let $f_1, f_2, g \in K\left[\left[x\right]\right]$ be such that $\left[x^0\right] g = 0$. Assume that f_2 is invertible. Let us first show that $f_2 \circ g$ is invertible.

Indeed, consider the inverse f_2^{-1} of f_2. This inverse exists (since f_2 is invertible) and satisfies $f_2^{-1} \cdot f_2 = \underline{1}$. Now, Proposition 3.5.4 **(b)** (applied to f_2^{-1} instead of f_1) yields $\left(f_2^{-1} \cdot f_2\right) \circ g = \left(f_2^{-1} \circ g\right) \cdot (f_2 \circ g)$. Hence,

$$\left(f_2^{-1} \circ g\right) \cdot (f_2 \circ g) = \underbrace{\left(f_2^{-1} \cdot f_2\right)}_{=\underline{1}} \circ g = \underline{1} \circ g = \underline{1}$$

(by Proposition 3.5.4 **(f)**, applied to $a = 1$). Thus, the FPS $f_2^{-1} \circ g$ is an inverse of $f_2 \circ g$. Hence, $f_2 \circ g$ is invertible. The expression $\dfrac{f_1 \circ g}{f_2 \circ g}$ is therefore well-defined.

It now remains to prove that $\dfrac{f_1}{f_2} \circ g = \dfrac{f_1 \circ g}{f_2 \circ g}$. To this purpose, we argue as follows: The expression $\dfrac{f_1}{f_2}$ is well-defined, since f_2 is invertible. Proposition 3.5.4 **(b)** (applied to $\dfrac{f_1}{f_2}$ instead of f_1) yields $\left(\dfrac{f_1}{f_2} \cdot f_2\right) \circ g = \left(\dfrac{f_1}{f_2} \circ g\right) \cdot (f_2 \circ g)$. In view of $\dfrac{f_1}{f_2} \cdot f_2 = f_1$, this rewrites as $f_1 \circ g = \left(\dfrac{f_1}{f_2} \circ g\right) \cdot (f_2 \circ g)$. We can divide both sides of this equality by $f_2 \circ g$ (since $f_2 \circ g$ is invertible), and thus obtain $\dfrac{f_1 \circ g}{f_2 \circ g} = \dfrac{f_1}{f_2} \circ g$. In other words, $\dfrac{f_1}{f_2} \circ g = \dfrac{f_1 \circ g}{f_2 \circ g}$. Thus, Proposition 3.5.4 **(c)** is proven.

(d) Let $f, g \in K[[x]]$ satisfy $[x^0] g = 0$. We must prove that $f^k \circ g = (f \circ g)^k$ for each $k \in \mathbb{N}$.

We prove this by induction on k:

Induction base: We have $\underbrace{f^0}_{=\underline{1}} \circ g = \underline{1} \circ g = \underline{1}$ (by Proposition 3.5.4 **(f)**, applied to $a = 1$). Comparing this with $(f \circ g)^0 = \underline{1}$, we find $f^0 \circ g = (f \circ g)^0$. In other words, $f^k \circ g = (f \circ g)^k$ holds for $k = 0$.

Induction step: Let $m \in \mathbb{N}$. Assume that $f^k \circ g = (f \circ g)^k$ holds for $k = m$. We must prove that $f^k \circ g = (f \circ g)^k$ holds for $k = m + 1$.

We have assumed that $f^k \circ g = (f \circ g)^k$ holds for $k = m$. In other words, we have $f^m \circ g = (f \circ g)^m$. Now,

$$\begin{aligned}
\underbrace{f^{m+1}}_{=f \cdot f^m} \circ g &= (f \cdot f^m) \circ g = (f \circ g) \cdot \underbrace{(f^m \circ g)}_{=(f \circ g)^m} \\
&\qquad \left(\text{by Proposition 3.5.4 } \textbf{(b)}\text{, applied to } f_1 = f \text{ and } f_2 = f^m\right) \\
&= (f \circ g) \cdot (f \circ g)^m = (f \circ g)^{m+1}.
\end{aligned}$$

In other words, $f^k \circ g = (f \circ g)^k$ holds for $k = m + 1$. This completes the induction step. Thus, we have proven that $f^k \circ g = (f \circ g)^k$ for each $k \in \mathbb{N}$. Proposition 3.5.4 **(d)** is now proven.

(h) This is just a generalization of Proposition 3.5.4 **(a)** to (potentially) infinite sums. The proof follows the same method, but unfortunately requires some technical reasoning about summability. I will give the full proof for the sake of completeness, but be warned that it contains nothing of interest.

Let $(f_i)_{i \in I} \in K[[x]]^I$ be a summable family of FPSs. Let $g \in K[[x]]$ be an FPS satisfying $[x^0] g = 0$.

First, we shall prove that the family $(f_i \circ g)_{i \in I} \in K[[x]]^I$ is summable. Indeed, we recall that the family $(f_i)_{i \in I} \in K[[x]]^I$ is summable. In other words,

$$\text{for each } n \in \mathbb{N}\text{, all but finitely many } i \in I \text{ satisfy } [x^n] f_i = 0$$

(by the definition of "summable"). In other words, for each $n \in \mathbb{N}$, there exists a finite subset I_n of I such that

$$\text{all } i \in I \setminus I_n \text{ satisfy } [x^n] f_i = 0. \tag{54}$$

Consider this subset I_n. Thus, all the sets $I_0, I_1, I_2, \ldots$ are finite subsets of I.

Now, let $n \in \mathbb{N}$ be arbitrary. The set $I_0 \cup I_1 \cup \cdots \cup I_n$ is a union of $n + 1$ finite subsets of I (because all the sets $I_0, I_1, I_2, \ldots$ are finite subsets of I), and thus itself is a finite subset of I. Moreover,

$$\text{all } i \in I \setminus (I_0 \cup I_1 \cup \cdots \cup I_n) \text{ satisfy } [x^n] (f_i \circ g) = 0. \tag{55}$$

[*Proof of (55):* Let $i \in I \setminus (I_0 \cup I_1 \cup \cdots \cup I_n)$. We must show that $[x^n](f_i \circ g) = 0$.

Let $m \in \{0, 1, \ldots, n\}$. Then, $I_m \subseteq I_0 \cup I_1 \cup \cdots \cup I_n$, so that $I_0 \cup I_1 \cup \cdots \cup I_n \supseteq I_m$ and thus $I \setminus \underbrace{(I_0 \cup I_1 \cup \cdots \cup I_n)}_{\supseteq I_m} \subseteq I \setminus I_m$. Hence, $i \in I \setminus (I_0 \cup I_1 \cup \cdots \cup I_n) \subseteq I \setminus I_m$. Therefore, (54) (applied to m instead of n) yields $[x^m] f_i = 0$.

Forget that we fixed m. We thus have shown that $[x^m] f_i = 0$ for each $m \in \{0, 1, \ldots, n\}$. In other words, the first $n+1$ coefficients of f_i are 0. Hence, Lemma 3.5.5 (applied to f_i and $n+1$ instead of f and k) shows that the first $n+1$ coefficients of $f_i \circ g$ are 0. However, $[x^n](f_i \circ g)$ is one of these first $n+1$ coefficients (indeed, it is the last of them); thus, this coefficient $[x^n](f_i \circ g)$ must be 0. This proves (55).]

Now, recall that $I_0 \cup I_1 \cup \cdots \cup I_n$ is a finite subset of I. Hence, thanks to (55), we know that there exists a finite subset J of I such that all $i \in I \setminus J$ satisfy $[x^n](f_i \circ g) = 0$ (namely, $J = I_0 \cup I_1 \cup \cdots \cup I_n$). In other words, all but finitely many $i \in I$ satisfy $[x^n](f_i \circ g) = 0$.

Forget that we fixed n. We thus have shown that

$$\text{for each } n \in \mathbb{N}, \text{ all but finitely many } i \in I \text{ satisfy } [x^n](f_i \circ g) = 0.$$

In other words, the family $(f_i \circ g)_{i \in I} \in K[[x]]^I$ is summable (by the definition of "summable").

It now remains to prove that $\left(\sum\limits_{i \in I} f_i\right) \circ g = \sum\limits_{i \in I} f_i \circ g$.

For each $i \in I$, we write the FPS f_i in the form $f_i = \sum\limits_{n \in \mathbb{N}} f_{i,n} x^n$ with $f_{i,0}, f_{i,1}, f_{i,2}, \ldots \in K$. First, we shall show that

$$\text{the family } (f_{i,m} g^m)_{(i,m) \in I \times \mathbb{N}} \text{ is summable.} \tag{56}$$

[*Proof of (56):* Fix an $n \in \mathbb{N}$. Let J denote the set $I_0 \cup I_1 \cup \cdots \cup I_n$. Hence, J is a union of $n+1$ finite subsets of I (because all the sets $I_0, I_1, I_2, \ldots$ are finite subsets of I), and thus itself is a finite subset of I. The set $J \times \{0, 1, \ldots, n\}$ must be finite (since it is the product of the two finite sets J and $\{0, 1, \ldots, n\}$).

Now, let $(i, m) \in (I \times \mathbb{N}) \setminus (J \times \{0, 1, \ldots, n\})$. We shall prove that $[x^n](f_{i,m} g^m) = 0$.

We have $(i, m) \notin J \times \{0, 1, \ldots, n\}$ (since $(i, m) \in (I \times \mathbb{N}) \setminus (J \times \{0, 1, \ldots, n\})$).

We note that $f_{i,m} \in K$ and thus $[x^n](f_{i,m} g^m) = f_{i,m} \cdot [x^n](g^m)$ (by (23)). However, we have $[x^0] g = 0$. Thus, Proposition 3.5.2 **(a)** (applied to f_i and $f_{i,j}$ and m instead of f and f_j and n) yields that the first m coefficients of the FPS g^m are 0. In other words, we have

$$\left[x^k\right](g^m) = 0 \qquad \text{for each } k \in \{0, 1, \ldots, m-1\}. \tag{57}$$

Now, if we have $n \in \{0, 1, \ldots, m-1\}$, then we have $[x^n](g^m) = 0$ (by (57), applied to $k = n$) and therefore $[x^n](f_{i,m} g^m) = f_{i,m} \cdot \underbrace{[x^n](g^m)}_{=0} = 0$. Hence, $[x^n](f_{i,m} g^m) = 0$ is proved in the case when $n \in \{0, 1, \ldots, m-1\}$. Thus, for the rest of this proof of $[x^n](f_{i,m} g^m) = 0$, we WLOG assume that $n \notin \{0, 1, \ldots, m-1\}$. Hence, $n > m-1$ (since $n \in \mathbb{N}$), so that $n \geq m$ (since n and m are integers). Therefore, $m \leq n$, so that

$m \in \{0, 1, \ldots, n\}$ and therefore $I_m \subseteq I_0 \cup I_1 \cup \cdots \cup I_n = J$ (since we defined J to be $I_0 \cup I_1 \cup \cdots \cup I_n$).

If we had $i \in I_m$, then we would have $(i, m) \in J \times \{0, 1, \ldots, n\}$ (since $i \in I_m \subseteq J$ and $m \in \{0, 1, \ldots, n\}$), which would contradict the fact that $(i, m) \notin J \times \{0, 1, \ldots, n\}$. Thus, we cannot have $i \in I_m$. Hence, $i \notin I_m$, so that $i \in I \setminus I_m$ (since $i \in I$). Thus, (54) (applied to m instead of n) yields $[x^m] f_i = 0$. However, from $f_i = \sum\limits_{n \in \mathbb{N}} f_{i,n} x^n$, we see that $[x^m] f_i = f_{i,m}$. Thus, $f_{i,m} = [x^m] f_i = 0$. Consequently, $[x^n] (f_{i,m} g^m) = \underbrace{f_{i,m}}_{=0} \cdot [x^n] (g^m) = 0$.

Forget that we fixed (i, m). We thus have shown that

$$\text{all } (i, m) \in (I \times \mathbb{N}) \setminus (J \times \{0, 1, \ldots, n\}) \text{ satisfy } [x^n] (f_{i,m} g^m) = 0.$$

Therefore, all but finitely many $(i, m) \in I \times \mathbb{N}$ satisfy $[x^n] (f_{i,m} g^m) = 0$ (since $J \times \{0, 1, \ldots, n\}$ is a finite subset of $I \times \mathbb{N}$).

Forget that we fixed n. We thus have shown that

$$\text{for each } n \in \mathbb{N}, \text{ all but finitely many } (i, m) \in I \times \mathbb{N} \text{ satisfy } [x^n] (f_{i,m} g^m) = 0.$$

In other words, the family $(f_{i,m} g^m)_{(i,m) \in I \times \mathbb{N}}$ is summable. This proves (56).]

Now, we have shown that the family $(f_{i,m} g^m)_{(i,m) \in I \times \mathbb{N}}$ is summable. Renaming the index (i, m) as (i, n), we thus conclude that the family $(f_{i,n} g^n)_{(i,n) \in I \times \mathbb{N}}$ is summable. The same argument (but with g replaced by x) shows that the family $(f_{i,n} x^n)_{(i,n) \in I \times \mathbb{N}}$ is summable (since the FPS x satisfies $[x^0]\, x = 0$).

The proof of $\left(\sum\limits_{i \in I} f_i \right) \circ g = \sum\limits_{i \in I} f_i \circ g$ is now just a matter of computation: hen, summing the equalities $f_i = \sum\limits_{n \in \mathbb{N}} f_{i,n} x^n$ over all $i \in I$, we obtain

$$\sum_{i \in I} f_i = \sum_{i \in I} \sum_{n \in \mathbb{N}} f_{i,n} x^n = \sum_{n \in \mathbb{N}} \sum_{i \in I} f_{i,n} x^n$$

(here, we have been able to interchange the summation signs, since the family $(f_{i,n} x^n)_{(i,n) \in I \times \mathbb{N}}$ is summable). Thus,

$$\sum_{i \in I} f_i = \sum_{n \in \mathbb{N}} \sum_{i \in I} f_{i,n} x^n = \sum_{n \in \mathbb{N}} \left(\sum_{i \in I} f_{i,n} \right) x^n.$$

Hence, Definition 3.5.1 (applied to $f = \sum\limits_{i \in I} f_i$) yields

$$\left(\sum_{i \in I} f_i \right) [g] = \sum_{n \in \mathbb{N}} \left(\sum_{i \in I} f_{i,n} \right) g^n \tag{58}$$

(since $\sum\limits_{i \in I} f_{i,n} \in K$ for each $n \in \mathbb{N}$).

On the other hand, for each $i \in I$, we have $f_i[g] = \sum\limits_{n\in\mathbb{N}} f_{i,n} g^n$ (by Definition 3.5.1, since $f_i = \sum\limits_{n\in\mathbb{N}} f_{i,n} x^n$ with $f_{i,0}, f_{i,1}, f_{i,2}, \ldots \in K$). Summing these equalities over all $i \in I$, we find

$$\sum_{i\in I} f_i[g] = \sum_{i\in I} \sum_{n\in\mathbb{N}} f_{i,n} g^n = \sum_{n\in\mathbb{N}} \sum_{i\in I} f_{i,n} g^n$$

(again, we have been able to interchange the summation signs, since the family $(f_{i,n} g^n)_{(i,n)\in I\times\mathbb{N}}$ is summable). Thus,

$$\sum_{i\in I} f_i[g] = \sum_{n\in\mathbb{N}} \sum_{i\in I} f_{i,n} g^n = \sum_{n\in\mathbb{N}} \left(\sum_{i\in I} f_{i,n}\right) g^n.$$

Comparing this with (58), we find $\left(\sum\limits_{i\in I} f_i\right)[g] = \sum\limits_{i\in I} f_i[g]$. In other words, $\left(\sum\limits_{i\in I} f_i\right) \circ g = \sum\limits_{i\in I} f_i \circ g$ (since the notation $f \circ g$ is synonymous to $f[g]$). Thus, Proposition 3.5.4 **(h)** is proven.

(e) This is [Loehr11, Theorem 7.63] and [Brewer14, Proposition 2.2.5].[22] Again, let us give the proof:

Write the FPS g in the form $g = \sum\limits_{n\in\mathbb{N}} g_n x^n$ for some $g_0, g_1, g_2, \ldots \in K$. Then, $g_0 = [x^0]\, g = 0$. Moreover, $g \circ h = g[h] = \sum\limits_{n\in\mathbb{N}} g_n h^n$ (by Definition 3.5.1, because $g = \sum\limits_{n\in\mathbb{N}} g_n x^n$ with $g_0, g_1, g_2, \ldots \in K$). But Proposition 3.5.2 **(c)** (applied to g, h and g_n instead of f, g and f_n) yields $[x^0] \left(\sum\limits_{n\in\mathbb{N}} g_n h^n\right) = g_0 = 0$. In view of $g \circ h = \sum\limits_{n\in\mathbb{N}} g_n h^n$, this rewrites as $[x^0]\,(g \circ h) = 0$. Hence, the composition $f \circ (g \circ h)$ is well-defined.

It remains to show that $(f \circ g) \circ h = f \circ (g \circ h)$.

Write the FPS f in the form $f = \sum\limits_{n\in\mathbb{N}} f_n x^n$ for some $f_0, f_1, f_2, \ldots \in K$. Thus, Definition 3.5.1 yields

$$f[g] = \sum_{n\in\mathbb{N}} f_n g^n \qquad \text{and} \qquad f[g \circ h] = \sum_{n\in\mathbb{N}} f_n \cdot (g \circ h)^n.$$

Moreover, the family $(f_n g^n)_{n\in\mathbb{N}}$ is summable (by Proposition 3.5.2 **(b)**). Hence, Proposition 3.5.4 **(h)** (applied to $(f_n g^n)_{n\in\mathbb{N}}$ and h instead of $(f_i)_{i\in I}$ and g) yields that the family $((f_n g^n) \circ h)_{n\in\mathbb{N}} \in K[[x]]^{\mathbb{N}}$ is summable as well and that we have

$$\left(\sum_{n\in\mathbb{N}} f_n g^n\right) \circ h = \sum_{n\in\mathbb{N}} (f_n g^n) \circ h. \tag{59}$$

[22] See also [19s, Proposition 7.6.14] for a similar property for polynomials.

In view of $f \circ g = f[g] = \sum_{n \in \mathbb{N}} f_n g^n$, we can rewrite (59) as

$$(f \circ g) \circ h = \sum_{n \in \mathbb{N}} (f_n g^n) \circ h. \tag{60}$$

However, for each $n \in \mathbb{N}$, we have $f_n g^n = \underline{f_n} \cdot g^n$ (by Theorem 3.2.6 **(d)**, applied to $\lambda = f_n$ and $\mathbf{a} = g^n$) and thus

$$\begin{aligned}(f_n g^n) \circ h = \left(\underline{f_n} \cdot g^n\right) \circ h &= \underbrace{\left(\underline{f_n} \circ h\right)}_{\substack{=\underline{f_n} \\ \text{(by Proposition 3.5.4 (f),} \\ \text{applied to } f_n \text{ and } h \\ \text{instead of } a \text{ and } g)}} \cdot \underbrace{(g^n \circ h)}_{\substack{=(g \circ h)^n \\ \text{(by Proposition 3.5.4 (d),} \\ \text{applied to } g \text{ and } h \\ \text{instead of } f \text{ and } g)}} \\ &\qquad \left(\begin{array}{c}\text{by Proposition 3.5.4 (b),} \\ \text{applied to } \underline{f_n}, g^n \text{ and } h \text{ instead of } f_1, f_2 \text{ and } g\end{array}\right) \\ &= \underline{f_n} \cdot (g \circ h)^n = f_n \cdot (g \circ h)^n \end{aligned} \tag{61}$$

(since Theorem 3.2.6 **(d)** (applied to $\lambda = f_n$ and $\mathbf{a} = (g \circ h)^n$) yields $f_n \cdot (g \circ h)^n = \underline{f_n} \cdot (g \circ h)^n$). Thus, (60) becomes

$$\begin{aligned}(f \circ g) \circ h &= \sum_{n \in \mathbb{N}} \underbrace{(f_n g^n) \circ h}_{\substack{=f_n \cdot (g \circ h)^n \\ \text{(by (61))}}} = \sum_{n \in \mathbb{N}} f_n \cdot (g \circ h)^n \\ &= f[g \circ h] \qquad \left(\text{since } f[g \circ h] = \sum_{n \in \mathbb{N}} f_n \cdot (g \circ h)^n\right) \\ &= f \circ (g \circ h). \end{aligned}$$

This completes the proof of Proposition 3.5.4 **(e)**. □

Example 3.5.7. Let us use Proposition 3.5.4 **(c)** to justify the equality (46) that we used in Example 3.5.3. Indeed, we know that the FPS $1 - x$ is invertible. Thus, applying Proposition 3.5.4 **(c)** to $f_1 = 1$ and $f_2 = 1 - x$ and $g = x + x^2$, we obtain

$$\frac{1}{1-x} \circ \left(x + x^2\right) = \frac{1 \circ \left(x + x^2\right)}{(1-x) \circ (x + x^2)}.$$

Using the notation $f[g]$ instead of $f \circ g$, we can rewrite this as

$$\frac{1}{1-x}\left[x + x^2\right] = \frac{1\left[x + x^2\right]}{(1-x)\left[x + x^2\right]}.$$

In view of $1\left[x + x^2\right] = 1$ and $(1-x)\left[x + x^2\right] = 1 - \left(x + x^2\right) = 1 - x - x^2$, this rewrites as $\frac{1}{1-x}\left[x + x^2\right] = \frac{1}{1 - x - x^2}$. Thus, (46) is proved.

Let us summarize: If $f, g \in K[[x]]$ are two FPSs, then the composition $f[g]$ is not always defined. However, it is defined at least in the following two cases:

- in the case when f is a polynomial (that is, $f \in K[x]$), and
- in the case when g has constant term 0 (that is, $[x^0] g = 0$).

This justifies some more of the things we did back in Section 3.1; in particular, Example 1 from that section is now fully justified. But we still have not defined (e.g.) the square root of an FPS, which we used in Example 2.

Before I explain square roots, let me quickly survey differentiation of FPSs.

3.6. Derivatives of FPSs

Our definition of the derivative of a FPS copycats the well-known formula for the derivative of a power series in analysis:

> **Definition 3.6.1.** Let $f \in K[[x]]$ be an FPS. Then, the *derivative* f' of f is an FPS defined as follows: Write f as $f = \sum\limits_{n\in\mathbb{N}} f_n x^n$ (with $f_0, f_1, f_2, \ldots \in K$), and set
>
> $$f' := \sum_{n>0} n f_n x^{n-1}.$$

To make sure that this derivative behaves nicely, we need to check that it satisfies the familiar properties of derivatives. And indeed, it does:

> **Theorem 3.6.2.** **(a)** We have $(f+g)' = f' + g'$ for any $f, g \in K[[x]]$.
>
> **(b)** If $(f_i)_{i\in I}$ is a summable family of FPSs, then the family $(f_i')_{i\in I}$ is summable as well, and we have
>
> $$\left(\sum_{i\in I} f_i\right)' = \sum_{i\in I} f_i'.$$
>
> **(c)** We have $(cf)' = cf'$ for any $c \in K$ and $f \in K[[x]]$.
>
> **(d)** We have $(fg)' = f'g + fg'$ for any $f, g \in K[[x]]$. (This is known as the *Leibniz rule*.)
>
> **(e)** If $f, g \in K[[x]]$ are two FPSs such that g is invertible, then
>
> $$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$
>
> (This is known as the *quotient rule*.)
>
> **(f)** If $g \in K[[x]]$ is an FPS, then $(g^n)' = ng'g^{n-1}$ for any $n \in \mathbb{N}$ (where the expression $ng'g^{n-1}$ is to be understood as 0 if $n = 0$).

(g) Given two FPSs $f, g \in K[[x]]$, we have

$$(f \circ g)' = (f' \circ g) \cdot g'$$

if f is a polynomial or if $[x^0] g = 0$. (This is known as the *chain rule*.)

(h) If K is a $\mathbb{Q}$-algebra, and if two FPSs $f, g \in K[[x]]$ satisfy $f' = g'$, then $f - g$ is constant.

Theorem 3.6.2 justifies Example 4 in Section 3.1 (specifically, Theorem 3.6.2 **(e)** is the quotient rule that we used to compute $\left(\dfrac{1}{1-x}\right)'$).

Proof of Theorem 3.6.2 (sketched). **(a)** This is part of [19s-mt3s, Exercise 5 **(b)**] (specifically, it is Statement 1 in [19s-mt3s, solution to Exercise 5 **(b)**]). Anyway, the proof is very easy.

(b) This is just the natural generalization of Theorem 3.6.2 **(a)** to (potentially) infinite sums. The proof follows the same idea, but requires some straightforward technical verifications (mainly to check that the summation signs can be interchanged).

(c) This is part of [19s-mt3s, Exercise 5 **(b)**] (specifically, it is Statement 3 in [19s-mt3s, solution to Exercise 5 **(b)**]).

(d) This is [19s-mt3s, Exercise 5 **(c)**] and [Grinbe17, Proposition 0.2 **(c)**].

(e) Let $f, g \in K[[x]]$ be two FPSs such that g is invertible. Then, Theorem 3.6.2 **(d)** (applied to $\dfrac{f}{g}$ instead of f) yields $\left(\dfrac{f}{g} \cdot g\right)' = \left(\dfrac{f}{g}\right)' \cdot g + \dfrac{f}{g} \cdot g'$. In view of $\dfrac{f}{g} \cdot g = f$, this rewrites as $f' = \left(\dfrac{f}{g}\right)' \cdot g + \dfrac{f}{g} \cdot g'$. Solving this for $\left(\dfrac{f}{g}\right)'$, we find $\left(\dfrac{f}{g}\right)' = \dfrac{f'g - fg'}{g^2}$. This proves Theorem 3.6.2 **(e)**.

(f) This follows by induction on n, using part **(d)** (in the induction step) and $1' = 0$ (in the induction base).

(g) Let $f, g \in K[[x]]$ be two FPSs such that f is a polynomial or $[x^0] g = 0$. Write the FPS f in the form $f = \sum\limits_{n \in \mathbb{N}} f_n x^n$ with $f_0, f_1, f_2, \ldots \in K$. Then, either Definition 3.5.1 or Definition 3.4.5 (depending on whether we have $[x^0] g = 0$

or f is a polynomial) yields $f[g] = \sum\limits_{n\in\mathbb{N}} f_n g^n$. Hence,

$$\begin{aligned}(f[g])' &= \left(\sum_{n\in\mathbb{N}} f_n g^n\right)' = \sum_{n\in\mathbb{N}} \underbrace{(f_n g^n)'}_{\substack{=f_n(g^n)' \\ \text{(by Theorem 3.6.2 (c))}}} \qquad \text{(by Theorem 3.6.2 (b))} \\ &= \sum_{n\in\mathbb{N}} f_n (g^n)' = f_0 \underbrace{\left(g^0\right)'}_{=1'=0} + \sum_{n>0} f_n \underbrace{(g^n)'}_{\substack{=ng'g^{n-1} \\ \text{(by Theorem 3.6.2 (f))}}} = \underbrace{f_0 \cdot 0}_{=0} + \sum_{n>0} f_n n g' g^{n-1} \\ &= \sum_{n>0} f_n n \underbrace{g' g^{n-1}}_{=g^{n-1}g'} = \sum_{n>0} n f_n g^{n-1} g'. \end{aligned} \tag{62}$$

On the other hand, from $f = \sum\limits_{n\in\mathbb{N}} f_n x^n$, we obtain $f' = \sum\limits_{n>0} n f_n x^{n-1} = \sum\limits_{m\in\mathbb{N}} (m+1) f_{m+1} x^m$ (here, we have substituted $m+1$ for n in the sum). Hence, Definition 3.5.1 or Definition 3.4.5 (depending on whether we have $\left[x^0\right] g = 0$ or f is a polynomial) yields

$$f'[g] = \sum_{m\in\mathbb{N}} (m+1) f_{m+1} g^m = \sum_{n>0} n f_n g^{n-1}$$

(here, we have substituted $n-1$ for m in the sum). Multiplying both sides of this equality by g', we find

$$f'[g] \cdot g' = \left(\sum_{n>0} n f_n g^{n-1}\right) \cdot g' = \sum_{n>0} n f_n g^{n-1} g'.$$

Comparing this with (62), we find $(f[g])' = f'[g] \cdot g'$. In other words, $(f \circ g)' = (f' \circ g) \cdot g'$ (since $f \circ g$ is a synonym for $f[g]$). This proves Theorem 3.6.2 **(g)**. (Note that this proof is done in [Loehr11, proof of Theorem 7.57 (d)] in the case when f is a polynomial.)

(h) The proof is easy and can be found in [Grinbe17, Lemma 0.3]. Note that the condition that K be a $\mathbb{Q}$-algebra is crucial, since it allows dividing by positive integers. (For example, if K could be $\mathbb{Z}/2$, then we would easily get a counterexample, e.g., by taking $f = x^2$ and $g = 0$.) □

3.7. Exponentials and logarithms

Convention 3.7.1. Throughout Subsection 3.7, we assume that K is not just a commutative ring, but actually a commutative $\mathbb{Q}$-algebra.

This entails that elements of K can be divided by the positive integers $1, 2, 3, \ldots$. We can use this to define three specific (and particularly important) FPSs over K:

Definition 3.7.2. Define three FPS exp, $\overline{\log}$ and $\overline{\exp}$ in $K[[x]]$ by

$$\exp := \sum_{n\in\mathbb{N}} \frac{1}{n!} x^n,$$
$$\overline{\log} := \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n,$$
$$\overline{\exp} := \exp - 1 = \sum_{n\geq 1} \frac{1}{n!} x^n.$$

(The last equality sign here follows from $\exp = \sum_{n\in\mathbb{N}} \frac{1}{n!} x^n = \underbrace{\frac{1}{0!}}_{=1} \underbrace{x^0}_{=1} + \sum_{n\geq 1} \frac{1}{n!} x^n = 1 + \sum_{n\geq 1} \frac{1}{n!} x^n$.)

Note that the FPS exp is the usual exponential series from analysis, but now manifesting itself as a FPS. Likewise, $\overline{\log}$ is the Mercator series for $\log(1+x)$, where log stands for the natural logarithm function. The natural logarithm function itself cannot be interpreted as an FPS, since $\log 0$ is undefined.

I will prove that

$$\overline{\exp} \circ \overline{\log} = \overline{\log} \circ \overline{\exp} = x. \tag{63}$$

This is an algebraic analogue of the well-known fact from analysis which states that the exponential and logarithm functions are mutually inverse.

There is a short way of proving (63), which I will not take: Namely, one can show that any equality between holomorphic functions on an open disk around the origin leads to an equality between their Taylor series (viewed as FPSs). Thus, if you have proved in complex analysis that $\log \circ \exp = \operatorname{id}$ on an open disk around 0 and $\exp \circ \log = \operatorname{id}$ on an open disk around 1, then you automatically get (63) (indeed, $\overline{\exp}$ and $\overline{\log}$ are the Taylor series of the functions exp and log around 1, with the reservation that the point 1 has been moved to the origin by a shift). This approach uses nontrivial results from complex analysis, so I will not follow it and instead start from scratch.

The main tool in the proof of (63) will be the following useful proposition ([Grinbe17, Lemma 0.4]):

Proposition 3.7.3. Let $g \in K[[x]]$ with $[x^0]\, g = 0$. Then:

(a) We have

$$(\overline{\exp} \circ g)' = (\exp \circ g)' = (\exp \circ g) \cdot g'.$$

(b) We have

$$\left(\overline{\log} \circ g\right)' = (1+g)^{-1} \cdot g'.$$

Proof of Proposition 3.7.3. **(a)** Let us first show that $\overline{\exp}' = \exp' = \exp$. Indeed, $\overline{\exp} = \exp - 1$, so that $\exp = \overline{\exp} + 1$ and therefore

$$\begin{aligned} \exp' &= \left(\overline{\exp} + 1\right)' = \overline{\exp}' + \underbrace{1'}_{=0} \qquad \text{(by Theorem 3.6.2 **(a)**)} \\ &= \overline{\exp}'. \end{aligned} \tag{64}$$

Next, we recall that $\exp = \sum\limits_{n\in\mathbb{N}} \frac{1}{n!}x^n$. Hence, the definition of a derivative yields

$$\begin{aligned} \exp' &= \sum_{n\geq 1} \underbrace{n \cdot \frac{1}{n!}}_{\substack{=\frac{1}{(n-1)!} \\ \text{(since } n!=n\cdot(n-1)!\text{)}}} x^{n-1} = \sum_{n\geq 1} \frac{1}{(n-1)!} x^{n-1} = \sum_{n\in\mathbb{N}} \frac{1}{n!} x^n \\ &\qquad\qquad \text{(here, we have substituted } n \text{ for } n-1 \text{ in the sum)} \\ &= \exp. \end{aligned} \tag{65}$$

Comparing this with (64), we find

$$\overline{\exp}' = \exp. \tag{66}$$

Now, we can apply the chain rule (Theorem 3.6.2 **(g)**) to $f = \overline{\exp}$ (since $\left[x^0\right] g = 0$), and thus obtain

$$\left(\overline{\exp} \circ g\right)' = \left(\underbrace{\overline{\exp}'}_{=\exp} \circ g\right) \cdot g' = \left(\exp \circ g\right) \cdot g'.$$

The same computation (but with $\overline{\exp}$ replaced by $\exp$) yields $\left(\exp \circ g\right)' = \left(\exp \circ g\right) \cdot g'$. Combining these two formulas, we obtain $\left(\overline{\exp} \circ g\right)' = \left(\exp \circ g\right)' = \left(\exp \circ g\right) \cdot g'$. Thus, we have proved Proposition 3.7.3 **(a)**.

(b) We have $\overline{\log} = \sum\limits_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n$. Thus,

$$\begin{aligned} \overline{\log}' &= \left(\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n\right)' \\ &= \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} \underbrace{\left(x^n\right)'}_{\substack{=nx'x^{n-1} \\ \text{(by Theorem 3.6.2 **(f)**,} \\ \text{applied to } x \text{ instead of } g\text{)}}} \qquad \text{(by Theorem 3.6.2 **(b)**)} \\ &= \sum_{n\geq 1} \underbrace{\frac{(-1)^{n-1}}{n} n}_{=(-1)^{n-1}} \underbrace{x'}_{=1} x^{n-1} = \sum_{n\geq 1} (-1)^{n-1} x^{n-1} = \sum_{n\in\mathbb{N}} (-1)^n x^n \end{aligned}$$

(here, we have substituted n for $n-1$ in the sum). On the other hand, Proposition 3.3.7 yields $(1+x)^{-1} = \sum\limits_{n\in\mathbb{N}} (-1)^n x^n$. Comparing these two equalities, we find

$$\overline{\log}' = (1+x)^{-1}. \tag{67}$$

Now, we can apply the chain rule (Theorem 3.6.2 **(g)**) to $f = \overline{\log}$ (since $[x^0]\, g = 0$), and thus obtain

$$\left(\overline{\log} \circ g\right)' = \left(\underbrace{\overline{\log}'}_{=(1+x)^{-1}} \circ g\right) \cdot g' = \left((1+x)^{-1} \circ g\right) \cdot g'. \tag{68}$$

However, we claim that $(1+x)^{-1} \circ g = (1+g)^{-1}$. Indeed, Proposition 3.5.4 **(c)** (applied to $f_1 = 1$ and $f_2 = 1+x$) yields $\dfrac{1}{1+x} \circ g = \dfrac{1 \circ g}{(1+x) \circ g}$ (since the FPS $1+x$ is invertible). In view of $\dfrac{1}{1+x} = (1+x)^{-1}$ and

$$\underbrace{1}_{=\underline{1}} \circ g = \underline{1} \circ g = \underline{1} \qquad \text{(by Proposition 3.5.4 **(f)**, applied to } a = 1\text{)}$$

and

$$(1+x) \circ g = 1 + g \qquad \text{(this follows easily from Definition 3.5.1)},$$

this rewrites as $(1+x)^{-1} \circ g = \dfrac{\underline{1}}{1+g} = (1+g)^{-1}$. Hence, (68) becomes

$$\left(\overline{\log} \circ g\right)' = \underbrace{\left((1+x)^{-1} \circ g\right)}_{=(1+g)^{-1}} \cdot g' = (1+g)^{-1} \cdot g'.$$

Thus, we have proved Proposition 3.7.3 **(b)**. □

We will need a very simple lemma, which says (in particular) that if two FPSs have constant terms 0, then so does their composition:

Lemma 3.7.4. Let $f, g \in K[[x]]$ be two FPSs with $[x^0]\, g = 0$. Then, $[x^0]\,(f \circ g) = [x^0]\, f$.

Proof of Lemma 3.7.4. Write f in the form $f = \sum\limits_{n\in\mathbb{N}} f_n x^n$ with $f_0, f_1, f_2, \ldots \in K$. Thus, $f_0 = [x^0]\, f$. Now, Definition 3.5.1 yields $f[g] = \sum\limits_{n\in\mathbb{N}} f_n g^n$. However, Proposition 3.5.2 **(c)** yields $[x^0]\left(\sum\limits_{n\in\mathbb{N}} f_n g^n\right) = f_0 = [x^0]\, f$. In view of $f \circ g = f[g] = \sum\limits_{n\in\mathbb{N}} f_n g^n$, we can rewrite this as $[x^0]\,(f \circ g) = [x^0]\, f$. This proves Lemma 3.7.4. □

Now, we can prove the equalities we promised ([Grinbe17, Theorem 0.1]):

Theorem 3.7.5. We have

$$\overline{\exp} \circ \overline{\log} = x \qquad \text{and} \qquad \overline{\log} \circ \overline{\exp} = x.$$

Proof of Theorem 3.7.5. Let us first prove that $\overline{\log} \circ \overline{\exp} = x$.

Indeed, the idea of this proof is to show that $\overline{\log} \circ \overline{\exp}$ and x are two FPSs with the same constant term (namely, 0) and with the same derivative. Once this is proved, Theorem 3.6.2 **(h)** will easily yield that they are equal.

Let us fill in the details. We have $\left[x^0\right] \overline{\exp} = 0$ (since $\overline{\exp} = \sum\limits_{n \geq 1} \dfrac{1}{n!} x^n$). Hence, Lemma 3.7.4 (applied to $f = \overline{\log}$ and $g = \overline{\exp}$) yields $\left[x^0\right] \left(\overline{\log} \circ \overline{\exp}\right) = \left[x^0\right] \overline{\log} = 0$ (since $\overline{\log} = \sum\limits_{n \geq 1} \dfrac{(-1)^{n-1}}{n} x^n$). Now, (19) yields

$$\left[x^0\right] \left(\overline{\log} \circ \overline{\exp} - x\right) = \underbrace{\left[x^0\right] \left(\overline{\log} \circ \overline{\exp}\right)}_{=0} - \underbrace{\left[x^0\right] x}_{=0} = 0. \qquad (69)$$

However, $\overline{\exp} = \exp - 1$ and thus $1 + \overline{\exp} = \exp$. Now, Proposition 3.7.3 **(b)** (applied to $g = \overline{\exp}$) yields

$$\left(\overline{\log} \circ \overline{\exp}\right)' = \left(\underbrace{1 + \overline{\exp}}_{= \exp}\right)^{-1} \cdot \underbrace{\overline{\exp}'}_{\substack{= \exp \\ \text{(by (66))}}} = \exp^{-1} \cdot \exp = 1 = x'$$

(since $x' = 1$). Hence, Theorem 3.6.2 **(h)** (applied to $f = \overline{\log} \circ \overline{\exp}$ and $g = x$) yields that $\overline{\log} \circ \overline{\exp} - x$ is constant. In other words, $\overline{\log} \circ \overline{\exp} - x = \underline{a}$ for some $a \in K$. Consider this a. From $\overline{\log} \circ \overline{\exp} - x = \underline{a}$, we obtain $\left[x^0\right] \left(\overline{\log} \circ \overline{\exp} - x\right) = \left[x^0\right] \underline{a} = a$. Comparing this with (69), we find $a = 0$. Hence, $\overline{\log} \circ \overline{\exp} - x = \underline{a}$ rewrites as $\overline{\log} \circ \overline{\exp} - x = \underline{0}$. In other words, $\overline{\log} \circ \overline{\exp} = x$.

Now it remains to prove that $\overline{\exp} \circ \overline{\log} = x$. There are (at least) two ways to do this:

- *1st way:* A homework exercise (Exercise A.2.5.2) says that any FPS f with $\left[x^0\right] f = 0$ and with $\left[x^1\right] f$ invertible has a unique compositional inverse (i.e., there is a unique FPS g with $\left[x^0\right] g = 0$ and $f \circ g = g \circ f = x$). We can apply this to $f = \overline{\log}$ (since $\left[x^0\right] \overline{\log} = 0$ and since $\left[x^1\right] \overline{\log} = 1$ is invertible), and thus see that $\overline{\log}$ has a unique compositional inverse g.

This compositional inverse g must be $\overline{\exp}$, since $\overline{\log} \circ \overline{\exp} = x$ (indeed, comparing $\underbrace{\left(g \circ \overline{\log}\right)}_{=x} \circ \overline{\exp} = x \circ \overline{\exp} = \overline{\exp}$ with

$$\begin{aligned}\left(g \circ \overline{\log}\right) \circ \overline{\exp} &= g \circ \underbrace{\left(\overline{\log} \circ \overline{\exp}\right)}_{=x} \qquad \text{(by Proposition 3.5.4 \textbf{(e)})} \\ &= g \circ x = g\end{aligned}$$

yields $g = \overline{\exp}$). But this entails that $\overline{\exp} \circ \overline{\log} = x$ as well.

- *2nd way:* Here is a more direct argument. We shall first show that $\exp \circ \overline{\log} = 1 + x$.

  To wit: The FPS $1 + x$ is invertible (by Proposition 3.3.9). Thus, applying the quotient rule (Theorem 3.6.2 **(e)**) to $f = \exp \circ \overline{\log}$ and $g = 1 + x$, we obtain

$$\left(\frac{\exp \circ \overline{\log}}{1+x}\right)' = \frac{\left(\exp \circ \overline{\log}\right)' \cdot (1+x) - \left(\exp \circ \overline{\log}\right) \cdot (1+x)'}{(1+x)^2}.$$

  In view of

$$\begin{aligned}\left(\exp \circ \overline{\log}\right)' &= \left(\exp \circ \overline{\log}\right) \cdot \underbrace{\overline{\log}'}_{\substack{=(1+x)^{-1} \\ \text{(by (67))}}} \\ &\qquad \left(\text{by Proposition 3.7.3 \textbf{(a)}, applied to } g = \overline{\log}\right) \\ &= \left(\exp \circ \overline{\log}\right) \cdot (1+x)^{-1}\end{aligned}$$

  and $(1 + x)' = 1$, we can rewrite this as

$$\begin{aligned}\left(\frac{\exp \circ \overline{\log}}{1+x}\right)' &= \frac{\left(\exp \circ \overline{\log}\right) \cdot (1+x)^{-1} \cdot (1+x) - \left(\exp \circ \overline{\log}\right) \cdot 1}{(1+x)^2} \\ &= \frac{\left(\exp \circ \overline{\log}\right) - \left(\exp \circ \overline{\log}\right)}{(1+x)^2} = 0 = 0'.\end{aligned}$$

  Thus, Theorem 3.6.2 **(h)** (applied to $f = \frac{\exp \circ \overline{\log}}{1+x}$ and $g = 0$) yields that $\frac{\exp \circ \overline{\log}}{1+x} - 0$ is constant. In other words, $\frac{\exp \circ \overline{\log}}{1+x}$ is constant. In other words, $\dfrac{\exp \circ \overline{\log}}{1+x} = \underline{a}$ for some $a \in K$. Consider this a. From $\dfrac{\exp \circ \overline{\log}}{1+x} = \underline{a}$, we obtain $\exp \circ \overline{\log} = \underline{a}\,(1+x) = a\,(1+x)$. Thus,

$$\left[x^0\right] \left(\exp \circ \overline{\log}\right) = \left[x^0\right] \left(a\,(1+x)\right) = a.$$

However, it is easy to see that $\left[x^0\right] \left(\exp \circ \overline{\log}\right) = 1$ [23]. Comparing these two equalities, we find $a = 1$. Thus, $\exp \circ \overline{\log} = \underbrace{a}_{=1} (1+x) = 1 + x$.

Now, $\overline{\exp} = \exp - 1 = \exp + \underline{-1}$. Hence,

$$\begin{aligned}
&\overline{\exp} \circ \overline{\log} \\
&= \left(\exp + \underline{-1}\right) \circ \overline{\log} = \underbrace{\exp \circ \overline{\log}}_{=1+x} + \underbrace{\underline{-1} \circ \overline{\log}}_{\substack{=\underline{-1} \\ \text{(by Proposition 3.5.4 \textbf{(f)},} \\ \text{applied to } -1 \text{ and } \overline{\log} \text{ instead of } a \text{ and } g)}} \\
&\qquad \left(\begin{array}{c} \text{by Proposition 3.5.4 \textbf{(a)},} \\ \text{applied to } f_1 = \exp \text{ and } f_2 = \underline{-1} \text{ and } g = \overline{\log} \end{array}\right) \\
&= 1 + x + \underline{-1} = \underbrace{\left(1 + \underline{-1}\right)}_{=0} + x = x.
\end{aligned}$$

Either way, we have shown that $\overline{\exp} \circ \overline{\log} = x$. Thus, the proof of Theorem 3.7.5 is complete. □

In Definition 3.7.2, we have found algebraic versions of the exponential and logarithm functions as FPSs. Next, we shall define analogues of these functions as operators acting on FPSs (i.e., analogues not of the functions exp and log themselves, but rather of composition with these functions):

Definition 3.7.6. **(a)** We let $K\left[\left[x\right]\right]_0$ denote the set of all FPSs $f \in K\left[\left[x\right]\right]$ with $\left[x^0\right] f = 0$.

(b) We let $K\left[\left[x\right]\right]_1$ denote the set of all FPSs $f \in K\left[\left[x\right]\right]$ with $\left[x^0\right] f = 1$.

(c) We define two maps

$$\begin{aligned} \operatorname{Exp} : K\left[\left[x\right]\right]_0 &\to K\left[\left[x\right]\right]_1, \\ g &\mapsto \exp \circ g \end{aligned}$$

[23] *Proof.* Recall that $\left[x^0\right] \overline{\log} = 0$. Hence, Lemma 3.7.4 (applied to $f = \exp$ and $g = \overline{\log}$) yields

$$\begin{aligned} \left[x^0\right] \left(\exp \circ \overline{\log}\right) = \left[x^0\right] \exp &= \frac{1}{0!} \qquad \left(\text{since } \exp = \sum_{n \in \mathbb{N}} \frac{1}{n!} x^n\right) \\ &= \frac{1}{1} = 1. \end{aligned}$$

and

$$\begin{aligned} \operatorname{Log} : K[[x]]_1 &\to K[[x]]_0, \\ f &\mapsto \overline{\log} \circ (f-1). \end{aligned}$$

(These two maps are well-defined according to parts **(c)** and **(d)** of Lemma 3.7.7 below.)

The maps Exp and Log are algebraic analogues of the maps in complex analysis that take any holomorphic function f to its exponential and logarithm, respectively (at least within certain regions in which these things are well-defined). As one would hope, and as we will soon see, they are mutually inverse. Let us first check that their definition is justified:

Lemma 3.7.7. **(a)** For any $f, g \in K[[x]]_0$, we have $f \circ g \in K[[x]]_0$.

(b) For any $f \in K[[x]]_1$ and $g \in K[[x]]_0$, we have $f \circ g \in K[[x]]_1$.

(c) For any $g \in K[[x]]_0$, we have $\exp \circ g \in K[[x]]_1$.

(d) For any $f \in K[[x]]_1$, we have $f - 1 \in K[[x]]_0$ and $\overline{\log} \circ (f-1) \in K[[x]]_0$.

Proof of Lemma 3.7.7. **(a)** Let $f, g \in K[[x]]_0$. In view of the definition of $K[[x]]_0$, this entails that $[x^0] f = 0$ and $[x^0] g = 0$. Hence, Lemma 3.7.4 yields $[x^0](f \circ g) = [x^0] f = 0$. In other words, $f \circ g \in K[[x]]_0$ (by the definition of $K[[x]]_0$). This proves Lemma 3.7.7 **(a)**.

(b) This is analogous to the proof of Lemma 3.7.7 **(a)**.

(c) Let $g \in K[[x]]_0$. From $\exp = \sum\limits_{n \in \mathbb{N}} \dfrac{1}{n!} x^n$, we obtain $[x^0] \exp = \dfrac{1}{0!} = 1$, so that $\exp \in K[[x]]_1$. Hence, Lemma 3.7.7 **(b)** (applied to $f = \exp$) yields $\exp \circ g \in K[[x]]_1$. This proves Lemma 3.7.7 **(c)**.

(d) Let $f \in K[[x]]_1$. Thus, $[x^0] f = 1$. Now, (19) yields $[x^0](f-1) = \underbrace{[x^0] f}_{=1} - \underbrace{[x^0] 1}_{=1} = 1 - 1 = 0$, so that $f - 1 \in K[[x]]_0$. Furthermore, $[x^0] \overline{\log} = 0$ (since $\overline{\log} = \sum\limits_{n \geq 1} \dfrac{(-1)^{n-1}}{n} x^n$) and thus $\overline{\log} \in K[[x]]_0$. Hence, Lemma 3.7.7 **(a)** (applied to $\overline{\log}$ and $f - 1$ instead of f and g) yields $\overline{\log} \circ (f-1) \in K[[x]]_0$. Thus, Lemma 3.7.7 **(d)** is proven. □

Lemma 3.7.8. The maps Exp and Log are mutually inverse bijections between $K[[x]]_0$ and $K[[x]]_1$.

Proof of Lemma 3.7.8. First, we make a simple auxiliary observation: Each $g \in K[[x]]_0$ satisfies[24]

$$\exp \circ g = \overline{\exp} \circ g + 1. \tag{70}$$

[24] As before, the "$\circ$" operation behaves like multiplication in the sense of PEMDAS conventions. Thus, the expression "$\overline{\exp} \circ g + 1$" means $(\overline{\exp} \circ g) + 1$.

[*Proof of (70):* Let $g \in K[[x]]_0$. Recall that $\overline{\exp} = \exp - 1$, so that $\exp = \overline{\exp} + 1 = \overline{\exp} + \underline{1}$. Hence,

$$\exp \circ g = \left(\overline{\exp} + \underline{1}\right) \circ g = \overline{\exp} \circ g + \underline{1} \circ g$$

(by Proposition 3.5.4 **(a)**, applied to $f_1 = \overline{\exp}$ and $f_2 = \underline{1}$). However, Proposition 3.5.4 **(f)** (applied to $a = 1$) yields $\underline{1} \circ g = \underline{1} = 1$. Hence, $\exp \circ g = \overline{\exp} \circ g + \underbrace{\underline{1} \circ g}_{=1} = \overline{\exp} \circ g + 1$. This proves (70).]

Now, let us show that $\operatorname{Exp} \circ \operatorname{Log} = \operatorname{id}$. Indeed, we fix some $f \in K[[x]]_1$. Then, $f - 1 \in K[[x]]_0$ (by Lemma 3.7.7 **(d)**). Hence, Proposition 3.5.4 **(e)** (applied to $\overline{\exp}$, $\overline{\log}$ and $f - 1$ instead of f, g and h) yields $\left(\overline{\exp} \circ \overline{\log}\right) \circ (f-1) = \overline{\exp} \circ \left(\overline{\log} \circ (f-1)\right)$. Thus,

$$\overline{\exp} \circ \left(\overline{\log} \circ (f-1)\right) = \underbrace{\left(\overline{\exp} \circ \overline{\log}\right)}_{\substack{=x \\ \text{(by Theorem 3.7.5)}}} \circ (f-1) = x \circ (f-1) = f - 1 \tag{71}$$

(by Proposition 3.5.4 **(g)**, applied to $g = f - 1$). However,

$$\begin{aligned}
(\operatorname{Exp} \circ \operatorname{Log})(f) &= \operatorname{Exp}(\operatorname{Log} f) \\
&= \exp \circ (\operatorname{Log} f) \qquad \text{(by the definition of Exp)} \\
&= \overline{\exp} \circ \underbrace{(\operatorname{Log} f)}_{\substack{=\overline{\log} \circ (f-1) \\ \text{(by the definition of Log)}}} + 1 \\
&\qquad \text{(by (70), applied to } g = \operatorname{Log} f) \\
&= \underbrace{\overline{\exp} \circ \left(\overline{\log} \circ (f-1)\right)}_{\substack{=f-1 \\ \text{(by (71))}}} + 1 \\
&= (f-1) + 1 = f = \operatorname{id}(f).
\end{aligned}$$

Forget that we fixed f. We thus have shown that $(\operatorname{Exp} \circ \operatorname{Log})(f) = \operatorname{id}(f)$ for each $f \in K[[x]]_1$. In other words, $\operatorname{Exp} \circ \operatorname{Log} = \operatorname{id}$.

Using a similar argument, we can show that $\operatorname{Log} \circ \operatorname{Exp} = \operatorname{id}$. Indeed, let us fix some $g \in K[[x]]_0$. Hence, Proposition 3.5.4 **(e)** (applied to $\overline{\log}$, $\overline{\exp}$ and g instead of f, g and h) yields $\left(\overline{\log} \circ \overline{\exp}\right) \circ g = \overline{\log} \circ \left(\overline{\exp} \circ g\right)$. Thus,

$$\overline{\log} \circ \left(\overline{\exp} \circ g\right) = \underbrace{\left(\overline{\log} \circ \overline{\exp}\right)}_{\substack{=x \\ \text{(by Theorem 3.7.5)}}} \circ g = x \circ g = g \tag{72}$$

(by Proposition 3.5.4 **(g)**). But the definition of Exp yields $\operatorname{Exp} g = \exp \circ g = \overline{\exp} \circ g + 1$ (by (70)). Hence, $\operatorname{Exp} g - 1 = \overline{\exp} \circ g$. Now,

$$\begin{aligned}(\operatorname{Log} \circ \operatorname{Exp})(g) &= \operatorname{Log}(\operatorname{Exp} g) \\ &= \overline{\log} \circ (\operatorname{Exp} g - 1) \qquad \text{(by the definition of Log)} \\ &= \overline{\log} \circ (\overline{\exp} \circ g) \qquad \text{(since } \operatorname{Exp} g - 1 = \overline{\exp} \circ g\text{)} \\ &= g \qquad \text{(by (72))} \\ &= \operatorname{id}(g).\end{aligned}$$

Forget that we fixed g. We thus have shown that $(\operatorname{Log} \circ \operatorname{Exp})(g) = \operatorname{id}(g)$ for each $g \in K[[x]]_0$. In other words, $\operatorname{Log} \circ \operatorname{Exp} = \operatorname{id}$. Combining this with $\operatorname{Exp} \circ \operatorname{Log} = \operatorname{id}$, we see that the maps Exp and Log are mutually inverse bijections between $K[[x]]_0$ and $K[[x]]_1$. This proves Lemma 3.7.8. □

We will now prove another lemma, which says that the Exp and Log maps deserve their names:

Lemma 3.7.9. **(a)** For any $f, g \in K[[x]]_0$, we have

$$\operatorname{Exp}(f+g) = \operatorname{Exp} f \cdot \operatorname{Exp} g.$$

(b) For any $f, g \in K[[x]]_1$, we have

$$\operatorname{Log}(fg) = \operatorname{Log} f + \operatorname{Log} g.$$

Proof of Lemma 3.7.9 (sketched). **(a)** Like many of our arguments involving FPSs, this will be a short computation followed by lengthy technical arguments justifying the interchanges of summation signs. (In this aspect, our algebraic replica of the analysis of infinite sums doesn't differ that much from the original.) We begin with the computation; the justifying arguments will be sketched afterwards.

Let $f, g \in K[[x]]_0$. Thus, $[x^0] f = 0$ and $[x^0] g = 0$. Hence, $f + g \in K[[x]]_0$ (since (18) yields $[x^0](f+g) = \underbrace{[x^0] f}_{=0} + \underbrace{[x^0] g}_{=0} = 0$).

By the definition of Exp, we have

$$\operatorname{Exp} f = \exp \circ f = \exp[f] = \sum_{n \in \mathbb{N}} \frac{1}{n!} f^n$$

(by Definition 3.5.1, since $\exp = \sum_{n \in \mathbb{N}} \frac{1}{n!} x^n$). Similarly,

$$\operatorname{Exp} g = \sum_{n \in \mathbb{N}} \frac{1}{n!} g^n$$

and

$$\operatorname{Exp}(f+g) = \sum_{n\in\mathbb{N}} \frac{1}{n!}(f+g)^n .$$

Now, the latter equality becomes

$$\begin{aligned}
\operatorname{Exp}(f+g) &= \sum_{n\in\mathbb{N}} \frac{1}{n!} \underbrace{(f+g)^n}_{\substack{=\sum\limits_{k=0}^{n}\binom{n}{k} f^k g^{n-k} \\ \text{(by the binomial theorem)}}} = \sum_{n\in\mathbb{N}} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} f^k g^{n-k} \\
&= \sum_{n\in\mathbb{N}} \sum_{k=0}^{n} \underbrace{\frac{1}{n!}\binom{n}{k}}_{\substack{=\dfrac{1}{k!\,(n-k)!} \\ \text{(by (2))}}} f^k g^{n-k} = \underbrace{\sum_{n\in\mathbb{N}} \sum_{k=0}^{n}}_{\substack{=\sum\limits_{\substack{(n,k)\in\mathbb{N}\times\mathbb{N};\\ k\le n}} \\ =\sum\limits_{k\in\mathbb{N}}\ \sum\limits_{n\ge k}}} \frac{1}{k!\,(n-k)!} f^k g^{n-k} \\
&= \sum_{k\in\mathbb{N}} \sum_{n\ge k} \frac{1}{k!\,(n-k)!} f^k g^{n-k} = \sum_{k\in\mathbb{N}} \sum_{\ell\in\mathbb{N}} \frac{1}{k!\ell!} f^k g^\ell \\
&\qquad\qquad (\text{here, we have substituted } \ell \text{ for } n-k \text{ in the second sum}) .
\end{aligned}$$

Comparing this with

$$\begin{aligned}
\operatorname{Exp} f \cdot \operatorname{Exp} g &= \left(\sum_{k\in\mathbb{N}} \frac{1}{k!} f^k\right) \cdot \left(\sum_{\ell\in\mathbb{N}} \frac{1}{\ell!} g^\ell\right) \\
&\qquad \left(\begin{array}{c} \text{since } \operatorname{Exp} f = \sum\limits_{n\in\mathbb{N}} \dfrac{1}{n!} f^n = \sum\limits_{k\in\mathbb{N}} \dfrac{1}{k!} f^k \\ \text{and } \operatorname{Exp} g = \sum\limits_{n\in\mathbb{N}} \dfrac{1}{n!} g^n = \sum\limits_{\ell\in\mathbb{N}} \dfrac{1}{\ell!} g^\ell \end{array}\right) \\
&= \sum_{k\in\mathbb{N}} \sum_{\ell\in\mathbb{N}} \frac{1}{k!} f^k \cdot \frac{1}{\ell!} g^\ell = \sum_{k\in\mathbb{N}} \sum_{\ell\in\mathbb{N}} \frac{1}{k!\ell!} f^k g^\ell ,
\end{aligned}$$

we obtain $\operatorname{Exp}(f+g) = \operatorname{Exp} f \cdot \operatorname{Exp} g$.

This is sufficient to prove Lemma 3.7.9 **(a)** if we can justify the above manipulations of infinite sums. Actually, there is just one manipulation that we need to justify, and that is our replacement of "$\sum\limits_{n\in\mathbb{N}}\ \sum\limits_{k=0}^{n}$" by "$\sum\limits_{k\in\mathbb{N}}\ \sum\limits_{n\ge k}$". This is an application of the "discrete Fubini rule" (specifically, of a version thereof in which the summation is over all pairs $(n,k) \in \mathbb{N}\times\mathbb{N}$ satisfying $k \le n$). In order to justify this manipulation, we need to show that the family $\left(\dfrac{1}{k!\,(n-k)!} f^k g^{n-k}\right)_{(n,k)\in\mathbb{N}\times\mathbb{N} \text{ satisfying } k\le n}$ is summable. In other words, we need to show the following statement:

> *Statement 1:* For each $m \in \mathbb{N}$, all but finitely many pairs $(n,k) \in \mathbb{N}\times\mathbb{N}$ satisfying $k \le n$ satisfy $[x^m]\left(\dfrac{1}{k!\,(n-k)!} f^k g^{n-k}\right) = 0$.

We shall achieve this by proving the following statement:

> *Statement 2:* For any three nonnegative integers m, k, ℓ with $m < k + \ell$, we have $[x^m] \left(f^k g^\ell\right) = 0$.

[*Proof of Statement 2:* Let m, k, ℓ be three nonnegative integers with $m < k + \ell$. We must show that $[x^m] \left(f^k g^\ell\right) = 0$.

We have $\left[x^0\right] f = 0$. Hence, Lemma 3.3.16 (applied to $a = f$) shows that there exists an $h \in K[[x]]$ such that $f = xh$. Consider this h and denote it by u. Thus, $u \in K[[x]]$ and $f = xu$.

We have $\left[x^0\right] g = 0$. Hence, Lemma 3.3.16 (applied to $a = g$) shows that there exists an $h \in K[[x]]$ such that $g = xh$. Consider this h and denote it by v. Thus, $v \in K[[x]]$ and $g = xv$.

Now, from $f = xu$ and $g = xv$, we obtain $f^k g^\ell = (xu)^k (xv)^\ell = x^k u^k x^\ell v^\ell = x^{k+\ell} u^k v^\ell$. However, Lemma 3.3.17 (applied to $k + \ell$ and $u^k v^\ell$ instead of k and a) shows that the first $k + \ell$ coefficients of the FPS $x^{k+\ell} u^k v^\ell$ are 0. In other words, the first $k + \ell$ coefficients of the FPS $f^k g^\ell$ are 0 (since $f^k g^\ell = x^{k+\ell} u^k v^\ell$). But $[x^m] \left(f^k g^\ell\right)$ is one of these first $k + \ell$ coefficients (since $m < k + \ell$). Thus, we conclude that $[x^m] \left(f^k g^\ell\right) = 0$. This proves Statement 2.]

Note that Statement 2 entails that the family $\left(f^k g^\ell\right)_{(k,\ell) \in \mathbb{N} \times \mathbb{N}}$ is summable (because when $m \in \mathbb{N}$ is given, all but finitely many pairs $(k, \ell) \in \mathbb{N} \times \mathbb{N}$ satisfy $m < k + \ell$). However, we need to prove Statement 1, so let us do this:

[*Proof of Statement 1:* Let $m \in \mathbb{N}$. If $(n, k) \in \mathbb{N} \times \mathbb{N}$ is a pair satisfying $k \leq n$ and $m < n$, then

$$[x^m] \left(\frac{1}{k!\,(n-k)!} f^k g^{n-k}\right) = \frac{1}{k!\,(n-k)!} \underbrace{[x^m] \left(f^k g^{n-k}\right)}_{\substack{=0 \\ \text{(by Statement 2} \\ \text{(applied to } \ell = n-k\text{),} \\ \text{since } m < n = k + (n-k))}} \qquad \text{(by (23))}$$
$$= 0.$$

Thus, all but finitely many pairs $(n, k) \in \mathbb{N} \times \mathbb{N}$ satisfying $k \leq n$ satisfy $[x^m] \left(\frac{1}{k!\,(n-k)!} f^k g^{n-k}\right) = 0$ (because all but finitely many such pairs satisfy $m < n$). This proves Statement 1.]

As explained above, Statement 1 shows that the family $\left(\frac{1}{k!\,(n-k)!} f^k g^{n-k}\right)_{(n,k) \in \mathbb{N} \times \mathbb{N} \text{ satisfying } k \leq n}$ is summable, and thus our interchange of summation signs made above is justified. This completes our proof of Lemma 3.7.9 **(a)**.

(b) This easily follows from part **(a)**, since we know that Log is inverse to Exp. Here are the details:

Let $f, g \in K[[x]]_1$. Set $u = \operatorname{Log} f$ and $v = \operatorname{Log} g$; then, $u, v \in K[[x]]_0$ (since Log is a map from $K[[x]]_1$ to $K[[x]]_0$). Hence, Lemma 3.7.9 **(a)** (applied to u and v instead of f and g) yields $\operatorname{Exp}(u + v) = \operatorname{Exp} u \cdot \operatorname{Exp} v$.

However, Lemma 3.7.8 says that the maps Exp and Log are mutually inverse bijections between $K[[x]]_0$ and $K[[x]]_1$. Hence, $\operatorname{Exp} \circ \operatorname{Log} = \operatorname{id}$ and $\operatorname{Log} \circ \operatorname{Exp} = \operatorname{id}$.

Now, from $u = \operatorname{Log} f$, we obtain $\operatorname{Exp} u = \operatorname{Exp}(\operatorname{Log} f) = \underbrace{(\operatorname{Exp} \circ \operatorname{Log})}_{=\operatorname{id}}(f) = \operatorname{id}(f) = f$. Similarly, $\operatorname{Exp} v = g$. Multiplying these two equalities, we find $\operatorname{Exp} u \cdot \operatorname{Exp} v = fg$. Now, we have

$$\operatorname{Log}(\operatorname{Exp}(u+v)) = \underbrace{(\operatorname{Log} \circ \operatorname{Exp})}_{=\operatorname{id}}(u+v) = \operatorname{id}(u+v) = u+v = \operatorname{Log} f + \operatorname{Log} g$$

(since $u = \operatorname{Log} f$ and $v = \operatorname{Log} g$). In view of $\operatorname{Exp}(u+v) = \operatorname{Exp} u \cdot \operatorname{Exp} v = fg$, this rewrites as $\operatorname{Log}(fg) = \operatorname{Log} f + \operatorname{Log} g$. This proves Lemma 3.7.9 **(b)**. □

We can neatly pack the last few lemmas into a single theorem through the use of group isomorphisms. To this purpose, we need to observe that $K[[x]]_0$ is a group under addition and $K[[x]]_1$ is a group under multiplication:

Proposition 3.7.10. **(a)** The subset $K[[x]]_0$ of $K[[x]]$ is closed under addition and subtraction and contains 0, and thus forms a group $(K[[x]]_0, +, 0)$.

(b) The subset $K[[x]]_1$ of $K[[x]]$ is closed under multiplication and division and contains 1, and thus forms a group $(K[[x]]_1, \cdot, 1)$.

Proof of Proposition 3.7.10. **(a)** It is clear that the set $K[[x]]_0$ contains the FPS 0 (since $[x^0]\,0 = 0$). Thus, it remains to show that $K[[x]]_0$ is closed under addition and subtraction. But this is easy: If $f, g \in K[[x]]_0$, then $[x^0]\,f = 0$ and $[x^0]\,g = 0$, and therefore $f + g \in K[[x]]_0$ (since (18) yields $[x^0]\,(f+g) = \underbrace{[x^0]\,f}_{=0} + \underbrace{[x^0]\,g}_{=0} = 0$) and $f - g \in K[[x]]_0$ (by a similar argument using (19)). Thus, $K[[x]]_0$ is closed under addition and subtraction. This proves Proposition 3.7.10 **(a)**.

(b) Any $a \in K[[x]]_1$ is invertible in $K[[x]]$ (indeed, $a \in K[[x]]_1$ shows that $[x^0]\,a = 1$; thus, $[x^0]\,a$ is invertible in K; therefore, Proposition 3.3.7 entails that a is invertible in $K[[x]]$). Hence, $\dfrac{f}{g}$ is well-defined for any $f, g \in K[[x]]_1$.

Next, we claim that $K[[x]]_1$ is closed under multiplication. Indeed, if $f, g \in K[[x]]_1$, then $[x^0]\,f = 1$ and $[x^0]\,g = 1$, and therefore $fg \in K[[x]]_1$ (since (22) yields $[x^0]\,(fg) = \underbrace{[x^0]\,f}_{=1} \cdot \underbrace{[x^0]\,g}_{=1} = 1$). This shows that $K[[x]]_1$ is closed under multiplication.

It remains to prove that $K[[x]]_1$ is closed under division. Indeed, if $f, g \in K[[x]]_1$, then $[x^0]\,f = 1$ and $[x^0]\,g = 1$, and therefore $\dfrac{f}{g} \in K[[x]]_1$ (because we have $f = \dfrac{f}{g} \cdot g$ and thus

$$\begin{aligned}\left[x^0\right] f &= \left[x^0\right] \left(\frac{f}{g} \cdot g\right) = \left[x^0\right] \frac{f}{g} \cdot \underbrace{\left[x^0\right] g}_{=1} \qquad \text{(by (22))} \\ &= \left[x^0\right] \frac{f}{g}\end{aligned}$$

and thus $\left[x^0\right] \dfrac{f}{g} = \left[x^0\right] f = 1$, so that $\dfrac{f}{g} \in K\left[\left[x\right]\right]_1$). This shows that $K\left[\left[x\right]\right]_1$ is closed under division. Thus, Proposition 3.7.10 **(b)** is proven. □

The two groups in Proposition 3.7.10 can now be connected through Exp and Log:

Theorem 3.7.11. The maps

$$\operatorname{Exp} : \left(K\left[\left[x\right]\right]_0, +, 0\right) \to \left(K\left[\left[x\right]\right]_1, \cdot, 1\right)$$

and

$$\operatorname{Log} : \left(K\left[\left[x\right]\right]_1, \cdot, 1\right) \to \left(K\left[\left[x\right]\right]_0, +, 0\right)$$

are mutually inverse group isomorphisms.

Proof of Theorem 3.7.11 (sketched). Lemma 3.7.9 yields that these two maps are group homomorphisms[25]. Lemma 3.7.8 shows that they are mutually inverse. Combining these results, we conclude that these two maps are mutually inverse group isomorphisms. This proves Theorem 3.7.11. □

Theorem 3.7.11 helps us turn addition into multiplication and vice versa when it comes to FPSs, at least if the constant terms are the right ones. This will come useful rather soon.

3.8. Non-integer powers

3.8.1. Definition

Now, let us again recall Example 2 from Section 3.1. In order to fully justify that example, we still need to explain what $\sqrt{1-4x}$ is.

More generally, let us try to define non-integer powers of FPSs (since square roots are just 1/2-th powers). Thus, we are trying to solve the following problem:

[25] Here, we are using the following fact: If $(G, *, e_G)$ and $(H, *, e_H)$ are any two groups, and if $\Phi : G \to H$ is a map such that every $f, g \in G$ satisfy $\Phi(f * g) = \Phi(f) * \Phi(g)$, then Φ is a group homomorphism.

> *Problem:* Devise a reasonable definition of the c-th power f^c for any FPS $f \in K[[x]]$ and any $c \in K$.

Here, "reasonable" means that it should have some of the properties we would expect:

- It should not conflict with the existing notion of f^c for $c \in \mathbb{N}$. That is, if $c \in \mathbb{N}$, then our new definition of f^c should yield the same result as the existing meaning that f^c has in this case (namely, $\underbrace{ff\cdots f}_{c \text{ times}}$). The same should hold for $c \in \mathbb{Z}$ when f is invertible.
- Rules of exponents should hold: i.e., we should have
$$f^{a+b} = f^a f^b, \qquad (fg)^a = f^a g^a, \qquad (f^a)^b = f^{ab} \tag{73}$$
for all $a, b \in K$ and $f, g \in K[[x]]$.
- For any positive integer n and any FPS $f \in K[[x]]$, the $1/n$-th power $f^{1/n}$ should be an n-th root of f (that is, an FPS whose n-th power is f). (This actually follows from the previous two properties, since we can apply the rule $(f^a)^b = f^{ab}$ to $a = 1/n$ and $b = n$.)

Clearly, we cannot solve the above problem in full generality:

- The power 0^{-1} cannot be reasonably defined (unless K is trivial). Indeed, $0^{-1} \cdot 0^1$ would have to equal $0^{-1+1} = 0^0 = 1$, but this would contradict $0^{-1} \cdot 0^1 = 0^{-1} \cdot 0 = 0$.
- The power $x^{1/2}$ cannot be reasonably defined either (unless K is trivial). Indeed, there is no FPS whose square is x. This will be proved in Exercise A.2.8.1 **(a)**.
- Even the power $(-1)^{1/2}$ cannot always be defined: There is no guarantee that K contains a square root of -1 (and if K does not, then it is easy to see that $K[[x]]$ does neither).

However, all we want is to make sense of $\sqrt{1-4x}$, so let us restrict ourselves to FPSs whose constant term is 1. Using the notation from Definition 3.7.6 **(b)**, we are thus moving on to the following problem:

> *More realistic problem:* Devise a reasonable definition of the c-th power f^c for any FPS $f \in K[[x]]_1$ and any $c \in K$.

Besides imposing the above wishlist of properties, we want this c-th power f^c itself to belong to $K[[x]]_1$, since otherwise the iterated power $(f^a)^b$ in our rules of exponents might be undefined.

It turns out that this is still too much to ask. Indeed, if $K = \mathbb{Z}/2$, then the FPS $1 + x \in K[[x]]_1$ has no square root (you get to prove this in Exercise A.2.8.1 **(c)**), so its $1/2$-th power $(1+x)^{1/2}$ cannot be reasonably defined.

However, if we assume (as in Convention 3.7.1) that K is a commutative $\mathbb{Q}$-algebra, then we get lucky: Our "more realistic problem" can be solved in (at least) two ways:

1st solution: We define

$$(1+x)^c := \sum_{k\in\mathbb{N}} \binom{c}{k} x^k \qquad \text{for each } c \in K,$$

in order to make Newton's binomial formula (Theorem 3.3.10) hold for arbitrary exponents[26]. Subsequently, we define

$$f^c := (1+x)^c [f-1] \qquad \text{for any } f \in K[[x]]_1 \text{ and } c \in K \tag{74}$$

(in order to have $(1+g)^c = \sum\limits_{k\in\mathbb{N}} \binom{c}{k} g^k$ hold not only for $g = x$, but also for all $g \in K[[x]]_0$).

It is clear that the FPS f^c is well-defined in this way. However, proving that this definition satisfies all our wishlist (particularly the rules of exponents (73)) is highly nontrivial. Some of this is done in [Loehr11, §7.12], but it is still a lot of work.

Thus, we shall discard this definition of f^c, and instead take a different way:

2nd solution: Recall the mutually inverse group isomorphisms

$$\begin{aligned} &\operatorname{Exp} : (K[[x]]_0, +, 0) \to (K[[x]]_1, \cdot, 1) \qquad \text{and} \\ &\operatorname{Log} : (K[[x]]_1, \cdot, 1) \to (K[[x]]_0, +, 0) \end{aligned}$$

from Theorem 3.7.11. Thus, for any $f \in K[[x]]_1$ and any $c \in \mathbb{Z}$, the equation

$$\operatorname{Log}(f^c) = c \operatorname{Log} f$$

holds (since Log is a group homomorphism). This suggests that we define f^c for all $c \in K$ by the same equation. In other words, we define f^c for all $c \in K$ by setting $f^c = \operatorname{Exp}(c \operatorname{Log} f)$ (since the map Exp is inverse to Log). And this is what we shall do now:

[26] Note that $\dbinom{c}{k} = \dfrac{c(c-1)(c-2)\cdots(c-k+1)}{k!}$ is well-defined since K is a commutative $\mathbb{Q}$-algebra.

Definition 3.8.1. Assume that K is a commutative $\mathbb{Q}$-algebra. Let $f \in K[[x]]_1$ and $c \in K$. Then, we define an FPS

$$f^c := \operatorname{Exp}(c \operatorname{Log} f) \in K[[x]]_1 .$$

This definition of f^c does not conflict with our original definition of f^c when $c \in \mathbb{Z}$ because (as we said) the original definition of f^c already satisfies $\operatorname{Log}(f^c) = c \operatorname{Log} f$ and therefore $f^c = \operatorname{Exp}(c \operatorname{Log} f)$.

Moreover, Definition 3.8.1 makes the rules of exponents hold:

Theorem 3.8.2. Assume that K is a commutative $\mathbb{Q}$-algebra. For any $a, b \in K$ and $f, g \in K[[x]]_1$, we have

$$f^{a+b} = f^a f^b, \qquad (fg)^a = f^a g^a, \qquad (f^a)^b = f^{ab}.$$

Proof. Easy exercise (Exercise A.2.8.2). □

Now, let us return to Example 2 from Section 3.1. In that example, we had to solve the quadratic equation

$$C(x) = 1 + x(C(x))^2 \qquad \text{for an FPS } C(x) \in \mathbb{Q}[[x]] .$$

Let us write C for $C(x)$; thus, this quadratic equation becomes

$$C = 1 + xC^2.$$

By completing the square, we can rewrite this equation in the equivalent form

$$(1 - 2xC)^2 = 1 - 4x.$$

Taking both sides of this equation to the $1/2$-th power, we obtain

$$\left((1 - 2xC)^2\right)^{1/2} = (1 - 4x)^{1/2}$$

(since both sides are FPSs with constant term 1). However, the FPS $1 - 2xC$ has constant term 1; thus, the rules of exponents yield $\left((1 - 2xC)^2\right)^{1/2} = (1 - 2xC)^{2 \cdot 1/2} = 1 - 2xC$. Hence,

$$1 - 2xC = \left((1 - 2xC)^2\right)^{1/2} = (1 - 4x)^{1/2} .$$

This is a linear equation in C; solving it for C yields

$$C = \frac{1}{2x}\left(1 - (1 - 4x)^{1/2}\right).$$

This is precisely the "square-root" expression for $C = C(x)$ that we have obtained back in Section 3.1, but now we have proved it rigorously.

3.8.2. The Newton binomial formula for arbitrary exponents

Is Example 2 from Section 3.1 fully justified now? No, because we still need to prove the identity (12) that we used back there. Since we are defining powers in the 2nd way (i.e., using Definition 3.8.1 rather than using (74)), it is not immediately obvious. Nevertheless, it can be proved. More generally, we can prove the following:

Theorem 3.8.3 (Generalized Newton binomial formula)**.** Assume that K is a commutative $\mathbb{Q}$-algebra. Let $c \in K$. Then,

$$(1+x)^c = \sum_{k \in \mathbb{N}} \binom{c}{k} x^k.$$

The following proof illustrates a technique that will probably appear preposterous if you are seeing it for the first time, but is in fact both legitimate and rather useful.

Proof of Theorem 3.8.3 (sketched). The definition of Log yields

$$\operatorname{Log}(1+x) = \overline{\log} \circ \left(\underbrace{(1+x)-1}_{=x} \right) = \overline{\log} \circ x = \overline{\log}$$

(by Proposition 3.5.4 **(g)**, applied to $g = \overline{\log}$).

Now, let us obstinately compute $(1+x)^c$ using Definition 3.8.1 and the definitions of Exp and Log. To wit: Let $\mathbb{P}$ denote the set $\{1,2,3,\ldots\}$. By Definition 3.8.1, we have

$$\begin{aligned}
&(1+x)^c \\
&= \operatorname{Exp}(c \operatorname{Log}(1+x)) = \operatorname{Exp}\left(c\overline{\log}\right) \qquad \left(\text{since } \operatorname{Log}(1+x) = \overline{\log}\right) \\
&= \exp \circ \left(c\overline{\log}\right) \qquad (\text{by the definition of } \operatorname{Exp}) \\
&= \exp \circ \left(c \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} x^n\right) \qquad \left(\text{since } \overline{\log} = \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} x^n\right) \\
&= \exp \circ \left(\sum_{n \geq 1} \frac{(-1)^{n-1}}{n} c x^n\right) \\
&= \sum_{m \in \mathbb{N}} \frac{1}{m!} \left(\sum_{n \geq 1} \frac{(-1)^{n-1}}{n} c x^n\right)^m
\end{aligned} \tag{75}$$

(by Definition 3.5.1, since $\exp = \sum_{n \in \mathbb{N}} \frac{1}{n!} x^n = \sum_{m \in \mathbb{N}} \frac{1}{m!} x^m$).

Now, fix $m \in \mathbb{N}$. We shall expand $\left(\sum\limits_{n \geq 1} \dfrac{(-1)^{n-1}}{n} cx^n \right)^m$. Indeed, we can replace the " $\sum\limits_{n \geq 1}$ " sign by an " $\sum\limits_{n \in \mathbb{P}}$ " sign, since $\mathbb{P} = \{1, 2, 3, \ldots\}$. Thus,

$$\begin{aligned}
&\left(\sum_{n \geq 1} \frac{(-1)^{n-1}}{n} cx^n \right)^m \\
&= \left(\sum_{n \in \mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n \right)^m \\
&= \underbrace{\left(\sum_{n \in \mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n \right) \left(\sum_{n \in \mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n \right) \cdots \left(\sum_{n \in \mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n \right)}_{m \text{ times}} \\
&= \left(\sum_{n_1 \in \mathbb{P}} \frac{(-1)^{n_1-1}}{n_1} cx^{n_1} \right) \left(\sum_{n_2 \in \mathbb{P}} \frac{(-1)^{n_2-1}}{n_2} cx^{n_2} \right) \cdots \left(\sum_{n_m \in \mathbb{P}} \frac{(-1)^{n_m-1}}{n_m} cx^{n_m} \right) \\
&\qquad \text{(here, we have renamed the summation indices)} \\
&= \sum_{(n_1, n_2, \ldots, n_m) \in \mathbb{P}^m} \left(\frac{(-1)^{n_1-1}}{n_1} cx^{n_1} \right) \left(\frac{(-1)^{n_2-1}}{n_2} cx^{n_2} \right) \cdots \left(\frac{(-1)^{n_m-1}}{n_m} cx^{n_m} \right)
\end{aligned}$$

(by a product rule for the product of m sums[27]). Hence,

$$\begin{aligned}
&\left(\sum_{n\geq 1}\frac{(-1)^{n-1}}{n}cx^n\right)^m \\
&= \underbrace{\sum_{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m}}_{=\sum\limits_{k\in\mathbb{N}}\ \sum\limits_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}}} \underbrace{\left(\frac{(-1)^{n_1-1}}{n_1}cx^{n_1}\right)\left(\frac{(-1)^{n_2-1}}{n_2}cx^{n_2}\right)\cdots\left(\frac{(-1)^{n_m-1}}{n_m}cx^{n_m}\right)}_{=\frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m x^{n_1+n_2+\cdots+n_m}} \\
&= \sum_{k\in\mathbb{N}}\ \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m \underbrace{x^{n_1+n_2+\cdots+n_m}}_{\substack{=x^k\\ \text{(since } n_1+n_2+\cdots+n_m=k)}} \\
&= \sum_{k\in\mathbb{N}}\ \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m x^k. \qquad (76)
\end{aligned}$$

Now, forget that we fixed m. We thus have proved (76) for each $m \in \mathbb{N}$. Now, (75) becomes

$$\begin{aligned}
&(1+x)^c \\
&= \sum_{m\in\mathbb{N}}\frac{1}{m!}\left(\sum_{n\geq 1}\frac{(-1)^{n-1}}{n}cx^n\right)^m \\
&= \sum_{m\in\mathbb{N}}\frac{1}{m!}\sum_{k\in\mathbb{N}}\ \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m x^k \qquad \text{(by (76))} \\
&= \sum_{k\in\mathbb{N}}\ \sum_{m\in\mathbb{N}}\ \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{1}{m!}\cdot\frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m x^k \\
&= \sum_{k\in\mathbb{N}}\left(\sum_{m\in\mathbb{N}}\ \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{1}{m!}\cdot\frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m\right)x^k. \qquad (77)
\end{aligned}$$

[27] This product rule says that

$$\left(\sum_{n_1\in A_1}a_{1,n_1}\right)\left(\sum_{n_2\in A_2}a_{2,n_2}\right)\cdots\left(\sum_{n_m\in A_m}a_{m,n_m}\right) = \sum_{(n_1,n_2,\ldots,n_m)\in A_1\times A_2\times\cdots\times A_m} a_{1,n_1}a_{2,n_2}\cdots a_{m,n_m}$$

for any m sets $A_1, A_2, \ldots, A_m$ and any elements $a_{i,j} \in K$, provided that all the sums on the left hand side of this equality are summable. We leave it to the reader to convince himself of this rule (intuitively, it just says that we can expand a product of sums in the usual way, even when the sums are infinite) and to check that the sums we are applying it to are indeed summable.

Now, let $k \in \mathbb{N}$. Let us rewrite the "middle sum" $\sum\limits_{m\in\mathbb{N}} \sum\limits_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m$ on the right hand side as a finite sum. Indeed, a *composition* of k shall mean a tuple $(n_1,n_2,\ldots,n_m)$ of positive integers satisfying $n_1+n_2+\cdots+n_m=k$. (For example, $(1,3,1)$ is a composition of 5. We will study compositions in more detail in Section 3.9.) Let $\operatorname{Comp}(k)$ denote the set of all compositions of k. It is easy to see that this set $\operatorname{Comp}(k)$ is finite[28]. Now, we can rewrite the double summation sign "$\sum\limits_{m\in\mathbb{N}} \sum\limits_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}}$" as a single summation sign "$\sum\limits_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)}$" (since $\operatorname{Comp}(k)$ is precisely the set of all tuples $(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m$ satisfying $n_1+n_2+\cdots+n_m=k$). Hence, we obtain

$$\begin{aligned}&\sum_{m\in\mathbb{N}} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m \\ &= \sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m. \qquad (78)\end{aligned}$$

Forget that we fixed k. Thus, for each $k\in\mathbb{N}$, we have defined a finite set $\operatorname{Comp}(k)$ and shown that (78) holds.

[28] *Proof.* Let $(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)$. Thus, $(n_1,n_2,\ldots,n_m)$ is a composition of k. In other words, $(n_1,n_2,\ldots,n_m)$ is a finite tuple of positive integers satisfying $n_1+n_2+\cdots+n_m=k$. Hence, all its m entries $n_1,n_2,\ldots,n_m$ are positive integers and thus are ≥ 1; therefore, $n_1+n_2+\cdots+n_m \geq \underbrace{1+1+\cdots+1}_{m\text{ times}} = m$, so that $m \leq n_1+n_2+\cdots+n_m = k$. Thus, $m\in\{0,1,\ldots,k\}$.

Furthermore, the sum $n_1+n_2+\cdots+n_m$ is $\geq$ to each of its m addends (since its m addends $n_1,n_2,\ldots,n_m$ are positive). In other words, we have $n_1+n_2+\cdots+n_m \geq n_i$ for each $i\in\{1,2,\ldots,m\}$. Thus, for each $i\in\{1,2,\ldots,m\}$, we have $n_i \leq n_1+n_2+\cdots+n_m = k$ and therefore $n_i\in\{1,2,\ldots,k\}$ (since n_i is a positive integer). Hence,

$$(n_1,n_2,\ldots,n_m)\in\{1,2,\ldots,k\}^m \subseteq \bigcup_{\ell\in\{0,1,\ldots,k\}} \{1,2,\ldots,k\}^\ell$$

(since $m\in\{0,1,\ldots,k\}$).

Now, forget that we fixed $(n_1,n_2,\ldots,n_m)$. We thus have shown that $(n_1,n_2,\ldots,n_m) \in \bigcup\limits_{\ell\in\{0,1,\ldots,k\}} \{1,2,\ldots,k\}^\ell$ for each $(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)$. In other words, $\operatorname{Comp}(k) \subseteq \bigcup\limits_{\ell\in\{0,1,\ldots,k\}} \{1,2,\ldots,k\}^\ell$. Since the set $\bigcup\limits_{\ell\in\{0,1,\ldots,k\}} \{1,2,\ldots,k\}^\ell$ is clearly finite (having size $\sum\limits_{\ell\in\{0,1,\ldots,k\}} k^\ell$), this entails that the set $\operatorname{Comp}(k)$ is finite as well, qed.

(Incidentally, we will see in Section 3.9 that this set $\operatorname{Comp}(k)$ has size 2^{k-1} for $k\geq 1$, and size 1 for $k=0$.)

Using (78), we can rewrite (77) as

$$\begin{aligned}&(1+x)^c\\&=\sum_{k\in\mathbb{N}}\left(\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)}\frac{1}{m!}\cdot\frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m\right)x^k.\end{aligned}\tag{79}$$

Now, recall that our goal is to prove that this equals

$$\sum_{k\in\mathbb{N}}\binom{c}{k}x^k.$$

This is equivalent to proving that the equality

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)}\frac{1}{m!}\cdot\frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1n_2\cdots n_m}c^m=\binom{c}{k}\tag{80}$$

holds for each $k\in\mathbb{N}$ (because two FPSs $u=\sum\limits_{k\in\mathbb{N}}u_kx^k$ and $v=\sum\limits_{k\in\mathbb{N}}v_kx^k$ (with $u_k\in K$ and $v_k\in K$) are equal if and only if the equality $u_k=v_k$ holds for each $k\in\mathbb{N}$).

Thus, we have reduced our original goal (which was to prove $(1+x)^c=\sum\limits_{k\in\mathbb{N}}\binom{c}{k}x^k$) to the auxiliary goal of proving the equality (80) for each $k\in\mathbb{N}$. However, this doesn't look very useful, since (80) is too messy an equality to have a simple proof. We are seemingly stuck.

However, it turns out that we are almost there – we just need to take a bird's eye view. Here is the plan: We fix $k\in\mathbb{N}$. Instead of trying to prove the equality (80) directly, we observe that both sides of this equality are polynomials (with rational coefficients) in c. (Indeed, the left hand side is clearly a polynomial in c, since it is a finite sum of "rational number times a power of c" expressions. The right hand side is a polynomial in c because $\binom{c}{k}=\dfrac{c(c-1)(c-2)\cdots(c-k+1)}{k!}$.) Thus, the polynomial identity trick (which we learnt in Subsection 3.2.3) tells us that if we can prove this equality (80) for each $c\in\mathbb{N}$, then it will automatically hold for each $c\in K$ (since the two polynomials that yield its left and right hand sides will have to be equal, having infinitely many equal values). Hence, in order to prove (80) for each $c\in K$, it suffices to prove it for each $c\in\mathbb{N}$. Now, how can we prove it for each $c\in\mathbb{N}$? We forget that we fixed k, and we remember that the equality (80) (for all $k\in\mathbb{N}$) is just an equivalent restatement of the FPS equality $(1+x)^c=\sum\limits_{k\in\mathbb{N}}\binom{c}{k}x^k$ (that is, the equality we have originally set out to prove). However, we know for sure that this equality holds for each $c\in\mathbb{N}$ (by Theorem 3.3.10, applied to $n=c$).

Hence, the equality (80) also holds for each $c \in \mathbb{N}$ (and each $k \in \mathbb{N}$). And this is precisely what we needed to show!

Let me explain this argument in detail now, as it is somewhat vertigo-inducing. We forget that we fixed K and c. Now, fix $c \in \mathbb{N}$. Thus, $c \in \mathbb{N} \subseteq \mathbb{Z}$. Hence, in the ring $\mathbb{Q}[[x]]$, we have

$$(1+x)^c = \sum_{k\in\mathbb{N}} \binom{c}{k} x^k \qquad \text{(by Theorem 3.3.10, applied to } n = c\text{)}.$$

However, (79) (applied to $K = \mathbb{Q}$) shows that

$$(1+x)^c = \sum_{k\in\mathbb{N}} \left(\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} c^m \right) x^k.$$

Comparing these two equalities, we obtain

$$\sum_{k\in\mathbb{N}} \left(\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} c^m \right) x^k = \sum_{k\in\mathbb{N}} \binom{c}{k} x^k.$$

Comparing coefficients in this equality, we see that

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} c^m = \binom{c}{k} \tag{81}$$

for each $k \in \mathbb{N}$. This is an equality between two rational numbers.

Now, forget that we fixed c. We thus have shown that (81) holds for each $k \in \mathbb{N}$ and each $c \in \mathbb{N}$.

Let us now fix $k \in \mathbb{N}$. We have just shown that the equality (81) holds for each $c \in \mathbb{N}$. In other words, the two polynomials

$$f := \sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} x^m \in \mathbb{Q}[x]$$

and

$$g := \binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!} \in \mathbb{Q}[x]$$

satisfy $f[c] = g[c]$ for each $c \in \mathbb{N}$ (because $f[c]$ is the left hand side of (81), while $g[c]$ is the right hand side of (81)). Thus, each $c \in \mathbb{N}$ satisfies $(f-g)[c] = \underbrace{f[c]}_{=g[c]} - g[c] = g[c] - g[c] = 0$. In other words, each $c \in \mathbb{N}$ is a root of $f - g$. Hence, the polynomial $f - g$ has infinitely many roots in $\mathbb{Q}$ (since there are infinitely many $c \in \mathbb{N}$). Since $f - g$ is a polynomial with rational coefficients, this is impossible unless $f - g = 0$. We thus must have $f - g = 0$, so that $f = g$. In other words,

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} x^m = \binom{x}{k} \tag{82}$$

holds in the polynomial ring $\mathbb{Q}[x]$.

Now, forget that we fixed k. We thus have shown that the equality (82) holds for each $k \in \mathbb{N}$.

Now, fix a commutative $\mathbb{Q}$-algebra K and an arbitrary element $c \in K$. For each $k \in \mathbb{N}$, we then have

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{n_1+n_2+\cdots+n_m-m}}{n_1 n_2 \cdots n_m} c^m = \binom{c}{k} \tag{83}$$

(by substituting c for x on both sides of the equality (82)). Consequently, we can rewrite (79) as

$$(1+x)^c = \sum_{k\in\mathbb{N}} \binom{c}{k} x^k.$$

This proves Theorem 3.8.3. □

The method we used in the above proof is worth recapitulating in broad strokes:

- We had to prove a fairly abstract statement (namely, the identity $(1+x)^c = \sum\limits_{k\in\mathbb{N}} \binom{c}{k} x^k$).
- We translated this statement into an awkward but more concrete statement (namely, the equality (80)).
- We then argued that this concrete statement needs only to be proven in a special case (viz., for all $c \in \mathbb{N}$ rather than for all $c \in K$), because it is an equality between two polynomials with rational coefficients.
- To prove this concrete statement in this special case, we translated it back into the abstract language of FPSs, and realized that in this special case it is already known (as a consequence of Theorem 3.3.10).

Thus, by strategically switching between the abstract and the concrete, we have managed to use the advantages of both sides.

Now that Theorem 3.8.3 is proved, Example 2 from Section 3.1 is fully justified (since we can obtain (12) by applying Theorem 3.8.3 to $K = \mathbb{Q}$ and $c = 1/2$).

3.8.3. Another application

Let us show yet another application of powers with non-integer exponents and the generalized Newton formula. We shall show the following binomial identity:

Proposition 3.8.4. Let $n \in \mathbb{C}$ and $k \in \mathbb{N}$. Then,

$$\sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i} = \binom{n+k-1}{k}.$$

Proposition 3.8.4 can be proved in various ways. For example, a mostly combinatorial proof is found in [19fco, Exercise 2.10.7 and Exercise 2.10.8][29]. We shall give a proof using generating functions instead.

Proof of Proposition 3.8.4. Define two FPSs $f, g \in \mathbb{C}[[x]]$ by

$$f = \sum_{i \in \mathbb{N}} \binom{n+i-1}{i} x^{2i} \qquad (84)$$

$$\text{and} \qquad g = \sum_{j \in \mathbb{N}} \binom{n}{j} x^{j}. \qquad (85)$$

(We will soon see why we chose to define them this way.) Multiplying the two

[29] Specifically, [19fco, Exercise 2.10.7] proves Proposition 3.8.4 in the particular case when $n \in \mathbb{N}$; then, [19fco, Exercise 2.10.8] extends it to the case when $n \in \mathbb{R}$. However, the latter argument can just as well be used to extend it to arbitrary $n \in \mathbb{C}$.

equalities (84) and (85), we find

$$\begin{aligned}
fg &= \left(\sum_{i\in\mathbb{N}} \binom{n+i-1}{i} x^{2i}\right) \left(\sum_{j\in\mathbb{N}} \binom{n}{j} x^j\right) \\
&= \underbrace{\sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}}}_{=\sum_{(i,j)\in\mathbb{N}\times\mathbb{N}}} \underbrace{\binom{n+i-1}{i} x^{2i} \binom{n}{j} x^j}_{=\binom{n+i-1}{i}\binom{n}{j}x^{2i+j}} \\
&= \underbrace{\sum_{(i,j)\in\mathbb{N}\times\mathbb{N}}}_{=\sum_{m\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=m}}} \binom{n+i-1}{i}\binom{n}{j} x^{2i+j} \\
&= \sum_{m\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=m}} \binom{n+i-1}{i}\binom{n}{j} \underbrace{x^{2i+j}}_{\substack{=x^m \\ \text{(since } 2i+j=m)}} \\
&= \sum_{m\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=m}} \binom{n+i-1}{i}\binom{n}{j} x^m \\
&= \sum_{m\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=m}} \binom{n+i-1}{i}\binom{n}{j} \right) x^m.
\end{aligned}$$

Hence, the x^k-coefficient of this FPS fg is

$$\left[x^k\right](fg) = \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=k}} \binom{n+i-1}{i}\binom{n}{j}. \tag{86}$$

Now, a pair $(i,j) \in \mathbb{N}\times\mathbb{N}$ satisfying $2i+j=k$ is uniquely determined by its first entry i, since its second entry j is given by $j=k-2i$. Hence, we can substitute $(i,k-2i)$ for (i,j) in the sum $\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=k}} \binom{n+i-1}{i}\binom{n}{j}$, thus rewriting this sum as $\sum\limits_{\substack{i\in\mathbb{N};\\ k-2i\in\mathbb{N}}} \dbinom{n+i-1}{i}\dbinom{n}{k-2i}$. Hence,

$$\begin{aligned}
\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=k}} \binom{n+i-1}{i}\binom{n}{j} &= \sum_{\substack{i\in\mathbb{N};\\ k-2i\in\mathbb{N}}} \binom{n+i-1}{i}\binom{n}{k-2i} \\
&= \sum_{\substack{i\in\mathbb{N};\\ 2i\leq k}} \binom{n+i-1}{i}\binom{n}{k-2i} \\
&\qquad \left(\begin{array}{c}\text{since an } i\in\mathbb{N} \text{ satisfies } k-2i\in\mathbb{N}\\ \text{if and only if it satisfies } 2i\leq k\end{array}\right) \\
&= \sum_{\substack{i\in\mathbb{N};\\ i\leq k}} \binom{n+i-1}{i}\binom{n}{k-2i}
\end{aligned}$$

(here, we have replaced the condition "$2i \leq k$" under the summation sign by the weaker condition "$i \leq k$", thus extending the range of the sum; but this did not change the sum, since all the newly introduced addends are 0 because of the vanishing $\dbinom{n}{k-2i}$ factor). Thus, (86) becomes

$$\begin{aligned}
\left[x^k\right](fg) &= \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ 2i+j=k}} \binom{n+i-1}{i}\binom{n}{j} \\
&= \sum_{\substack{i\in\mathbb{N};\\ i\leq k}} \binom{n+i-1}{i}\binom{n}{k-2i} \\
&= \sum_{i=0}^{k} \binom{n+i-1}{i}\binom{n}{k-2i}. \qquad (87)
\end{aligned}$$

Note that the right hand side here is precisely the left hand side of the identity we are trying to prove. This is why we defined f and g as we did. With a bit of experience, the computation above can easily be reverse-engineered, and the definitions of f and g are essentially forced by the goal of making (87) hold.

Anyway, it is now clear that a simple expression for fg would move us forward. So let us try to simplify f and g. For g, the answer is easiest: We have

$$g = \sum_{j\in\mathbb{N}} \binom{n}{j} x^j = (1+x)^n,$$

because Theorem 3.8.3 (applied to $c = n$) yields $(1+x)^n = \sum\limits_{j\in\mathbb{N}} \dbinom{n}{j} x^j$. For f, we need a few more steps. Proposition 3.3.12 yields

$$(1+x)^{-n} = \sum_{i\in\mathbb{N}} (-1)^i \binom{n+i-1}{i} x^i. \tag{88}$$

Substituting $-x^2$ for x on both sides of this equality, we obtain

$$\begin{aligned}
\left(1-x^2\right)^{-n} &= \sum_{i\in\mathbb{N}} (-1)^i \binom{n+i-1}{i} \underbrace{\left(-x^2\right)^i}_{=(-1)^i x^{2i}} = \sum_{i\in\mathbb{N}} (-1)^i \binom{n+i-1}{i} (-1)^i x^{2i} \\
&= \sum_{i\in\mathbb{N}} \underbrace{(-1)^i (-1)^i}_{=1} \binom{n+i-1}{i} x^{2i} = \sum_{i\in\mathbb{N}} \binom{n+i-1}{i} x^{2i} = f
\end{aligned}$$

and thus $f = \left(1-x^2\right)^{-n}$. Multiplying this equality by $g = (1+x)^n$, we obtain

$$\begin{aligned}
fg &= \left(1-x^2\right)^{-n} (1+x)^n = \left(\frac{1+x}{1-x^2}\right)^n = \left(\frac{1-x^2}{1+x}\right)^{-n} \\
&= (1-x)^{-n} \qquad \left(\text{since } \frac{1-x^2}{1+x} = \frac{(1-x)(1+x)}{1+x} = 1-x\right) \\
&= \sum_{i\in\mathbb{N}} (-1)^i \binom{n+i-1}{i} \underbrace{(-x)^i}_{=(-1)^i x^i} \\
&\qquad\qquad (\text{this follows by substituting } -x \text{ for } x \text{ on both sides of (88)}) \\
&= \sum_{i\in\mathbb{N}} (-1)^i \binom{n+i-1}{i} (-1)^i x^i = \sum_{i\in\mathbb{N}} \underbrace{(-1)^i (-1)^i}_{=1} \binom{n+i-1}{i} x^i \\
&= \sum_{i\in\mathbb{N}} \binom{n+i-1}{i} x^i.
\end{aligned}$$

Hence, the x^k-coefficient in fg is $\left[x^k\right](fg) = \binom{n+k-1}{k}$. Comparing this with (87), we obtain

$$\sum_{i=0}^{k} \binom{n+i-1}{i} \binom{n}{k-2i} = \binom{n+k-1}{k}.$$

Thus, Proposition 3.8.4 is proved. □

3.9. Integer compositions

3.9.1. Compositions

Next, let us count certain simple combinatorial objects known as *integer compositions*. There are easy combinatorial ways to do this (see, e.g., [19fco, §2.10.1]), but we shall employ generating functions, in order to see one more example of how these can be used.

Definition 3.9.1. **(a)** An *(integer) composition* means a (finite) tuple of positive integers.

(b) The *size* of an integer composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is defined to be the integer $\alpha_1 + \alpha_2 + \cdots + \alpha_m$. It is written $|\alpha|$.

(c) The *length* of an integer composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is defined to be the integer m. It is written $\ell(\alpha)$.

(d) Let $n \in \mathbb{N}$. A *composition of n* means a composition whose size is n.

(e) Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. A *composition of n into k parts* is a composition whose size is n and whose length is k.

Example 3.9.2. The tuple $(3, 8, 6)$ is a composition with size $3 + 8 + 6 = 17$ and length 3. In other words, it is a composition of 17 into 3 parts.

The empty tuple $()$ is a composition of 0 into 0 parts. It is the only composition of 0, and also is the only composition with length 0.

The following **questions** arise quite naturally:

1. How many compositions of n exist for a given $n \in \mathbb{N}$?

2. How many compositions of n into k parts exist for given $n, k \in \mathbb{N}$?

Let us use generating functions to answer question 2.

Approach to question 2. Fix $k \in \mathbb{N}$, but don't fix n. Let

$$a_{n,k} = (\text{\# of compositions of } n \text{ into } k \text{ parts}). \tag{89}$$

We want to find $a_{n,k}$. We define the generating function

$$A_k := \sum_{n \in \mathbb{N}} a_{n,k} x^n = (a_{0,k}, a_{1,k}, a_{2,k}, \ldots) \in \mathbb{Q}[[x]]. \tag{90}$$

Let us write $\mathbb{P}$ for the set $\{1, 2, 3, \ldots\}$. Then, a composition of n into k parts is nothing but a k-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k$ satisfying $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$. Hence, (89) can be rewritten as

$$\begin{aligned} a_{n,k} &= \left(\text{\# of all } k\text{-tuples } (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k \text{ satisfying } \alpha_1 + \alpha_2 + \cdots + \alpha_k = n\right) \\ &= \sum_{\substack{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k; \\ \alpha_1 + \alpha_2 + \cdots + \alpha_k = n}} 1. \end{aligned} \tag{91}$$

Thus, we can rewrite the equality $A_k = \sum\limits_{n \in \mathbb{N}} a_{n,k} x^n$ as

$$\begin{aligned} A_k &= \sum_{n \in \mathbb{N}} \left(\sum_{\substack{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k; \\ \alpha_1 + \alpha_2 + \cdots + \alpha_k = n}} 1 \right) x^n = \sum_{n \in \mathbb{N}} \sum_{\substack{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k; \\ \alpha_1 + \alpha_2 + \cdots + \alpha_k = n}} \underbrace{x^n}_{\substack{= x^{\alpha_1 + \alpha_2 + \cdots + \alpha_k} \\ \text{(since } \alpha_1 + \alpha_2 + \cdots + \alpha_k = n)}} \\ &= \underbrace{\sum_{n \in \mathbb{N}} \sum_{\substack{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k; \\ \alpha_1 + \alpha_2 + \cdots + \alpha_k = n}}}_{= \sum\limits_{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k}} \underbrace{x^{\alpha_1 + \alpha_2 + \cdots + \alpha_k}}_{= x^{\alpha_1} x^{\alpha_2} \cdots x^{\alpha_k}} = \sum_{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k} x^{\alpha_1} x^{\alpha_2} \cdots x^{\alpha_k} \\ &= \left(\sum_{\alpha_1 \in \mathbb{P}} x^{\alpha_1} \right) \left(\sum_{\alpha_2 \in \mathbb{P}} x^{\alpha_2} \right) \cdots \left(\sum_{\alpha_k \in \mathbb{P}} x^{\alpha_k} \right) \\ &\qquad \left(\begin{array}{c} \text{by the same product rule that we used back} \\ \text{in the proof of Theorem 3.8.3} \end{array} \right) \\ &= \left(\sum_{n \in \mathbb{P}} x^n \right)^k \end{aligned}$$

(here, we have renamed all the k summation indices as n, and realized that all k sums are identical). Since

$$\sum_{n \in \mathbb{P}} x^n = x^1 + x^2 + x^3 + \cdots = x \underbrace{\left(1 + x + x^2 + \cdots\right)}_{= \frac{1}{1-x}} = x \cdot \frac{1}{1-x} = \frac{x}{1-x},$$

this can be rewritten further as

$$A_k = \left(\frac{x}{1-x} \right)^k = x^k (1-x)^{-k}. \tag{92}$$

In order to simplify this, we need to expand $(1-x)^{-k}$. This is routine by now: Theorem 3.3.10 (applied to $-k$ instead of n) yields

$$(1+x)^{-k} = \sum_{j \in \mathbb{N}} \binom{-k}{j} x^j.$$

Substituting $-x$ for x on both sides of this equality (i.e., applying the map

$f \mapsto f \circ (-x)$), we obtain

$$\begin{aligned}
(1-x)^{-k} &= \sum_{j\in\mathbb{N}} \underbrace{\binom{-k}{j}}_{\substack{=(-1)^j \binom{j+k-1}{j} \\ \text{(by Theorem 3.3.11,} \\ \text{applied to } k \text{ and } j \\ \text{instead of } n \text{ and } k\text{)}}} \underbrace{(-x)^j}_{=(-1)^j x^j} = \sum_{j\in\mathbb{N}} (-1)^j \binom{j+k-1}{j} \cdot (-1)^j x^j \\
&= \sum_{j\in\mathbb{N}} \underbrace{\left((-1)^j\right)^2}_{=1} \binom{j+k-1}{j} x^j = \sum_{j\in\mathbb{N}} \binom{j+k-1}{j} x^j \qquad (93) \\
&= \sum_{n\geq k} \binom{n-1}{n-k} x^{n-k}
\end{aligned}$$

(here, we have substituted $n-k$ for j in the sum). Hence, our above computation of A_k can be completed as follows:

$$\begin{aligned}
A_k &= x^k \underbrace{(1-x)^{-k}}_{=\sum\limits_{n\geq k} \binom{n-1}{n-k} x^{n-k}} = x^k \sum_{n\geq k} \binom{n-1}{n-k} x^{n-k} \\
&= \sum_{n\geq k} \binom{n-1}{n-k} \underbrace{x^k x^{n-k}}_{=x^n} = \sum_{n\geq k} \binom{n-1}{n-k} x^n = \sum_{n\in\mathbb{N}} \binom{n-1}{n-k} x^n
\end{aligned}$$

(here, we have extended the range of the summation from all $n \geq k$ to all $n \in \mathbb{N}$; this did not change the sum, since all the newly introduced addends with $n < k$ are 0). Comparing coefficients, we thus obtain

$$a_{n,k} = \binom{n-1}{n-k} \qquad \text{for each } n \in \mathbb{N}. \qquad (94)$$

If $n > 0$, then we can rewrite the right hand side of this equality as $\binom{n-1}{k-1}$ (using Theorem 2.0.6). However, if $n = 0$, then this right hand side equals $\delta_{k,0}$ instead (where we are using Definition 3.5.6). Thus, we can rewrite (94) as

$$a_{n,k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ \delta_{k,0}, & \text{if } n = 0 \end{cases} \qquad \text{for each } n \in \mathbb{N}. \qquad (95)$$

□

We have thus answered our Question 2. Let us summarize the two answers we have found ((94) and (95)) in the following theorem ([19fco, Theorem 2.10.1]):

Theorem 3.9.3. Let $n, k \in \mathbb{N}$. Then, the # of compositions of n into k parts is

$$\binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ \delta_{k,0}, & \text{if } n = 0. \end{cases}$$

This theorem has other proofs as well. See [19fco, Proof of Theorem 2.10.1] for a proof by bijection and [19fco, solution to Exercise 2.10.2] for a proof by induction.

As an easy consequence of Theorem 3.9.3, we can now answer Question 1 as well:

Theorem 3.9.4. Let $n \in \mathbb{N}$. Then, the # of compositions of n is

$$\begin{cases} 2^{n-1}, & \text{if } n > 0; \\ 1, & \text{if } n = 0. \end{cases}$$

Proof of Theorem 3.9.4 (sketched). If $n = 0$, then the # of compositions of n is 1 (since the empty tuple $()$ is the only composition of 0). Thus, for the rest of this proof, we WLOG assume that $n \neq 0$. Hence, we must prove that the # of compositions of n is 2^{n-1}.

If $(n_1, n_2, \ldots, n_m)$ is a composition of n, then $m \in \{1, 2, \ldots, n\}$ (why?). In other words, any composition of n is a composition of n into k parts for some $k \in \{1, 2, \ldots, n\}$. Hence,

$$\begin{aligned} &(\text{\# of compositions of } n) \\ &= \sum_{k \in \{1,2,\ldots,n\}} \underbrace{(\text{\# of compositions of } n \text{ into } k \text{ parts})}_{\substack{= \binom{n-1}{n-k} \\ \text{(by Theorem 3.9.3)}}} \\ &= \sum_{k \in \{1,2,\ldots,n\}} \binom{n-1}{n-k} = \sum_{k=1}^{n} \binom{n-1}{n-k} = \sum_{k=0}^{n-1} \binom{n-1}{k} \end{aligned}$$

(here, we have substituted k for $n-k$ in the sum). Comparing this with

$$\begin{aligned} 2^{n-1} &= (1+1)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} \underbrace{1^k 1^{n-1-k}}_{=1} \qquad \text{(by the binomial theorem)} \\ &= \sum_{k=0}^{n-1} \binom{n-1}{k}, \end{aligned}$$

we obtain (# of compositions of n) $= 2^{n-1}$. This proves Theorem 3.9.4. □

3.9.2. Weak compositions

A variant of compositions are the *weak compositions*. These are like compositions, but their entries have to only be nonnegative rather than positive. For the sake of completeness, let us give their definition in full:[30]

Definition 3.9.5. (a) An *(integer) weak composition* means a (finite) tuple of nonnegative integers.

(b) The *size* of a weak composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is defined to be the integer $\alpha_1 + \alpha_2 + \cdots + \alpha_m$. It is written $|\alpha|$.

(c) The *length* of a weak composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ is defined to be the integer m. It is written $\ell(\alpha)$.

(d) Let $n \in \mathbb{N}$. A *weak composition of n* means a weak composition whose size is n.

(e) Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. A *weak composition of n into k parts* is a weak composition whose size is n and whose length is k.

Example 3.9.6. The tuple $(3, 0, 1, 2)$ is a weak composition with size $3 + 0 + 1 + 2 = 6$ and length 4. In other words, it is a weak composition of 6 into 4 parts. It is not a composition, since one of its entries is a 0.

Weak compositions are a rather natural analogue of compositions, but behave dissimilarly in one important way: Any $n \in \mathbb{N}$ has infinitely many weak compositions. Indeed, all the tuples (n), $(n, 0)$, $(n, 0, 0)$, $(n, 0, 0, 0)$, $\ldots$ are weak compositions of n (and of course, there are many more weak compositions of n, unless $n = 0$). Thus, it makes no sense to look for an analogue of Theorem 3.9.4 for weak compositions. However, an analogue of Theorem 3.9.3 does exist:

Theorem 3.9.7. Let $n, k \in \mathbb{N}$. Then, the # of weak compositions of n into k parts is

$$\dbinom{n+k-1}{n} = \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ \delta_{n,0}, & \text{if } k = 0. \end{cases}$$

Proof of Theorem 3.9.7 (sketched). (See [19fco, Theorem 2.10.5] for details and alternative proofs.) Adding 1 to a nonnegative integer yields a positive integer. Furthermore, if we add 1 to each entry of a k-tuple, then the sum of all entries of the k-tuple increases by k.

Thus, if $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ is a weak composition of n into k parts, then $(\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_k + 1)$ is a composition of $n + k$ into k parts. Hence, we can define a map

$$\{\text{weak compositions of } n \text{ into } k \text{ parts}\} \to \{\text{compositions of } n+k \text{ into } k \text{ parts}\},$$
$$(\alpha_1, \alpha_2, \ldots, \alpha_k) \mapsto (\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_k + 1).$$

[30] Beware that the word "weak composition" does not have a unique meaning in the literature.

Furthermore, it is easy to see that this map is a bijection (indeed, its inverse is rather easy to construct). Thus, by the bijection principle, we have

$$\begin{aligned}
&\left|\left\{\text{weak compositions of } n \text{ into } k \text{ parts}\right\}\right| \\
&= \left|\left\{\text{compositions of } n+k \text{ into } k \text{ parts}\right\}\right| \\
&= \left(\text{\# of compositions of } n+k \text{ into } k \text{ parts}\right) \\
&= \binom{n+k-1}{n+k-k} \qquad \left(\begin{array}{c}\text{by the first equality sign in Theorem 3.9.3,} \\ \text{applied to } n+k \text{ instead of } n\end{array}\right) \\
&= \binom{n+k-1}{n}.
\end{aligned}$$

Thus, we have shown that the # of weak compositions of n into k parts is $\binom{n+k-1}{n}$. It remains to prove that this equals $\begin{cases}\binom{n+k-1}{k-1}, & \text{if } k>0; \\ \delta_{n,0}, & \text{if } k=0\end{cases}$ as well. This is similar to how we obtained (95): If $k = 0$, then it is clear by inspection; otherwise it follows from Theorem 2.0.6. Theorem 3.9.7 is proven. □

3.9.3. Weak compositions with entries from $\{0,1,\ldots,p-1\}$

Theorems 3.9.3 and 3.9.7 may stir up hopes that other tuple-counting problems also have simple answers. Let us see if this hope holds up.

An attempt. We fix three nonnegative integers n, k and p. We are looking for the # of k-tuples $(\alpha_1,\alpha_2,\ldots,\alpha_k) \in \{0,1,\ldots,p-1\}^k$ satisfying $\alpha_1+\alpha_2+\cdots+\alpha_k = n$. In other words, we are looking for the # of all weak compositions of n into k parts with the property that each entry is $< p$. Let us denote this # by $w_{n,k,p}$.

Just as when counting compositions, we invoke a generating function. Forget that we fixed n, and define the FPS

$$W_{k,p} := \sum_{n\in\mathbb{N}} w_{n,k,p} x^n \in \mathbb{Q}\left[\left[x\right]\right].$$

For each $n \in \mathbb{N}$, we have

$$\begin{aligned}
w_{n,k,p} &= \Big(\text{\# of all } k\text{-tuples } (\alpha_1,\alpha_2,\ldots,\alpha_k) \in \{0,1,\ldots,p-1\}^k \\
&\qquad\qquad \text{satisfying } \alpha_1+\alpha_2+\cdots+\alpha_k = n\Big) \\
&= \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k; \\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}} 1.
\end{aligned}$$

Thus, we can rewrite the equality $W_{k,p} = \sum\limits_{n\in\mathbb{N}} w_{n,k,p}x^n$ as

$$\begin{aligned}
W_{k,p} &= \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k;\\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}} 1 \right) x^n \\
&= \sum_{n\in\mathbb{N}} \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k;\\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}} \underbrace{x^n}_{\substack{=x^{\alpha_1+\alpha_2+\cdots+\alpha_k}\\ \text{(since } \alpha_1+\alpha_2+\cdots+\alpha_k=n)}} \\
&= \underbrace{\sum_{n\in\mathbb{N}} \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k;\\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}}}_{=\sum\limits_{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k}} \underbrace{x^{\alpha_1+\alpha_2+\cdots+\alpha_k}}_{=x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_k}} \\
&= \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k} x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_k} \\
&= \left(\sum_{\alpha_1\in\{0,1,\ldots,p-1\}} x^{\alpha_1} \right) \left(\sum_{\alpha_2\in\{0,1,\ldots,p-1\}} x^{\alpha_2} \right) \cdots \left(\sum_{\alpha_k\in\{0,1,\ldots,p-1\}} x^{\alpha_k} \right) \\
&\qquad \left(\begin{array}{c}\text{by the same product rule that we used back}\\ \text{in the proof of Theorem 3.8.3}\end{array} \right) \\
&= \left(\sum_{n\in\{0,1,\ldots,p-1\}} x^n \right)^k
\end{aligned}$$

(here, we have renamed all the k summation indices as n, and realized that all k sums are identical). Since

$$\sum_{n\in\{0,1,\ldots,p-1\}} x^n = x^0 + x^1 + \cdots + x^{p-1} = \frac{1-x^p}{1-x}$$

(the last equality sign here is easy to check[31]), this can be rewritten further as

$$W_{k,p} = \left(\frac{1-x^p}{1-x} \right)^k = (1-x^p)^k (1-x)^{-k}. \qquad (96)$$

In order to expand the right hand side, let us expand $(1-x^p)^k$ and $(1-x)^{-k}$ separately.

[31] Just show that $(1-x)\left(x^0+x^1+\cdots+x^{p-1}\right) = 1-x^p$.

The binomial theorem yields

$$\begin{aligned}(1-x^p)^k &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \underbrace{(x^p)^j}_{=x^{pj}} = \sum_{j=0}^{k} (-1)^j \binom{k}{j} x^{pj} \\ &= \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} x^{pj}\end{aligned}$$

(here, we have extended the range of the summation from $j \in \{0, 1, \ldots, k\}$ to all $j \in \mathbb{N}$; this did not change the sum, since all the newly introduced addends are 0). Multiplying this by (93), we obtain

$$\begin{aligned}&(1-x^p)^k (1-x)^{-k} \\ &= \left(\sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} x^{pj}\right) \left(\sum_{j\in\mathbb{N}} \binom{j+k-1}{j} x^j\right) \\ &= \left(\sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} x^{pj}\right) \left(\sum_{i\in\mathbb{N}} \binom{i+k-1}{i} x^i\right) \\ &\qquad \left(\begin{array}{c}\text{here, we have renamed the summation index } j \\ \text{as } i \text{ in the second sum}\end{array}\right) \\ &= \underbrace{\sum_{(i,j)\in\mathbb{N}\times\mathbb{N}}}_{=\sum_{n\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}}} (-1)^j \binom{k}{j} \binom{i+k-1}{i} x^{pj+i} \\ &= \sum_{n\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}} (-1)^j \binom{k}{j} \binom{i+k-1}{i} \underbrace{x^{pj+i}}_{\substack{=x^n \\ (\text{since } pj+i=n)}} \\ &= \sum_{n\in\mathbb{N}} \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}} (-1)^j \binom{k}{j} \binom{i+k-1}{i} x^n \\ &= \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}} (-1)^j \binom{k}{j} \binom{i+k-1}{i}\right) x^n.\end{aligned}$$

Thus, (96) becomes

$$W_{k,p} = (1-x^p)^k (1-x)^{-k} = \sum_{n\in\mathbb{N}} \left(\sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}} (-1)^j \binom{k}{j} \binom{i+k-1}{i}\right) x^n.$$

Comparing coefficients in this equality, we find that each $n \in \mathbb{N}$ satisfies

$$\begin{aligned}
w_{n,k,p} &= \sum_{\substack{(i,j)\in\mathbb{N}\times\mathbb{N};\\ pj+i=n}} (-1)^j \binom{k}{j}\binom{i+k-1}{i} \\
&= \sum_{\substack{j\in\mathbb{N};\\ pj\leq n}} (-1)^j \binom{k}{j}\binom{n-pj+k-1}{n-pj} \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (n-pj,j) \text{ for } (i,j) \text{ in the sum,}\\ \text{since any pair } (i,j)\in\mathbb{N}\times\mathbb{N} \text{ satisfying } pj+i=n\\ \text{is uniquely determined by its second entry } j\end{array}\right) \\
&= \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j}\binom{n-pj+k-1}{n-pj} \\
&\qquad \left(\begin{array}{c}\text{here, we have extended the range of summation by}\\ \text{dropping the ``} pj\leq n \text{'' requirement; this does not change}\\ \text{the sum, since all newly introduced addends are } 0\end{array}\right) \\
&= \sum_{j=0}^{k} (-1)^j \binom{k}{j}\binom{n-pj+k-1}{n-pj}
\end{aligned}$$

(here, we have removed all addends with $j > k$ from the sum; this does not change the sum, since all these addends are 0). □

Thus, we have proved the following fact:

Theorem 3.9.8. Let $n, k, p \in \mathbb{N}$. Then, the # of k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1, \ldots, p-1\}^k$ satisfying $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ is

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j}\binom{n-pj+k-1}{n-pj}.$$

In general, this expression is the simplest we can get. A combinatorial proof of Theorem 3.9.8 can be found in [19fco, Exercise 2.10.6].

However, the particular case when $p = 2$ is worth exploring, as it allows for a much simpler expression. Indeed, the k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1\}^k$ are just the "*binary k-strings*", i.e., the k-tuples formed of 0s and 1s. Imposing the condition $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ on such a k-tuple is tantamount to requiring that it contain exactly n many 1s. Therefore, the # of all k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1\}^k$ satisfying $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ is $\dbinom{k}{n}$, since we have to choose which n of its k positions will be occupied by 1s (and then all remaining $k - n$ positions will be occupied by 0s). However, Theorem 3.9.8 (applied to $p = 2$) yields that this # equals $\sum\limits_{j=0}^{k} (-1)^j \dbinom{k}{j} \dbinom{n-2j+k-1}{n-2j}$. Comparing these two results, we obtain the following identity:

Proposition 3.9.9. Let $n, k \in \mathbb{N}$. Then,

$$\binom{k}{n} = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-2j+k-1}{n-2j}.$$

3.10. x^n-equivalence

We now return to general properties of FPSs.

Definition 3.10.1. Let $n \in \mathbb{N}$. Let $f, g \in K[[x]]$ be two FPSs. We write $f \overset{x^n}{\equiv} g$ if and only if

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] f = [x^m] g.$$

Thus, we have defined a binary relation $\overset{x^n}{\equiv}$ on the set $K[[x]]$. We say that an FPS f is *x^n-equivalent* to an FPS g if and only if $f \overset{x^n}{\equiv} g$.

Thus, an FPS f is x^n-equivalent to an FPS g if and only if the first $n+1$ coefficients of f agree with the first $n+1$ coefficients of g. Here are some examples:

Example 3.10.2. (a) We have $(1+x)^3 \overset{x^1}{\equiv} \dfrac{1}{1-3x}$, since each $m \in \{0, 1\}$ satisfies $[x^m]\left((1+x)^3\right) = [x^m] \dfrac{1}{1-3x}$ (indeed, $[x^0]\left((1+x)^3\right) = 1 = [x^0] \dfrac{1}{1-3x}$ and $[x^1]\left((1+x)^3\right) = 1 = [x^1] \dfrac{1}{1-3x}$). Of course, this also shows that $(1+x)^3 \overset{x^0}{\equiv} \dfrac{1}{1-3x}$. However, we don't have $(1+x)^3 \overset{x^2}{\equiv} \dfrac{1}{1-3x}$ (at least not for $K = \mathbb{Z}$), since $[x^2]\left((1+x)^3\right) = 3$ does not equal $[x^2] \dfrac{1}{1-3x} = 9$.

(b) More generally, $(1+x)^n \overset{x^1}{\equiv} \dfrac{1}{1-nx}$ and $(1+x)^n \overset{x^1}{\equiv} 1 + nx$ for each $n \in \mathbb{Z}$.

(c) If $f \in K[[x]]$ is any FPS, and if $n \in \mathbb{N}$, then there exists a polynomial $p \in K[x]$ such that $f \overset{x^n}{\equiv} p$. Indeed, we can take $p = \sum\limits_{k=0}^{n} \left([x^k] f\right) \cdot x^k$.

One way to get an intuition for the relation $\overset{x^n}{\equiv}$ is to think of it as a kind of "approximate equality" up to degree n. (This makes the most sense if one thinks of x as an infinitesimal quantity, in which case a term λx^k (with $\lambda \in K$) is the more "important" the lower k is. From this viewpoint, $f \overset{x^n}{\equiv} g$ means that the FPSs f and g agree in their $n+1$ most "important" terms and differ at most in their "error terms".) For this reason, the statement "$f \overset{x^n}{\equiv} g$" is sometimes written as "$f = g + o\left(x^n\right)$" (an algebraic imitation of Landau's little-o notation from asymptotic analysis). Another intuition comes from elementary number theory: The relation $\overset{x^n}{\equiv}$ is similar to congruence of integers modulo a given integer. This is more than a similarity; the relation $\overset{x^n}{\equiv}$ can in fact be restated as a divisibility in the same fashion as for congruences of integers (see Proposition 3.10.4 below). For this reason, the statement "$f \overset{x^n}{\equiv} g$" is sometimes written as "$f \equiv g \operatorname{mod} x^{n+1}$". We shall, however, eschew both of these alternative notations, and use the original notation "$f \overset{x^n}{\equiv} g$" from Definition 3.10.1, as both intuitions (while useful) would distract from the simplicity of Definition 3.10.1[32].

Here are some basic properties of the relation $\overset{x^n}{\equiv}$ (some of which will be used without explicit reference):

Theorem 3.10.3. Let $n \in \mathbb{N}$.

(a) The relation $\overset{x^n}{\equiv}$ on $K\left[\left[x\right]\right]$ is an equivalence relation. In other words:

- This relation is reflexive (i.e., we have $f \overset{x^n}{\equiv} f$ for each $f \in K\left[\left[x\right]\right]$).
- This relation is transitive (i.e., if three FPSs $f, g, h \in K\left[\left[x\right]\right]$ satisfy $f \overset{x^n}{\equiv} g$ and $g \overset{x^n}{\equiv} h$, then $f \overset{x^n}{\equiv} h$).
- This relation is symmetric (i.e., if two FPSs $f, g \in K\left[\left[x\right]\right]$ satisfy $f \overset{x^n}{\equiv} g$, then $g \overset{x^n}{\equiv} f$).

(b) If $a, b, c, d \in K\left[\left[x\right]\right]$ are four FPSs satisfying $a \overset{x^n}{\equiv} b$ and $c \overset{x^n}{\equiv} d$, then we also have

$$a + c \overset{x^n}{\equiv} b + d; \tag{97}$$

$$a - c \overset{x^n}{\equiv} b - d; \tag{98}$$

$$ac \overset{x^n}{\equiv} bd. \tag{99}$$

[32] Case in point: Definition 3.10.1 can be generalized to multivariate FPSs, but the two intuitions are no longer available (or, worse, give the "wrong" concepts) when extended to this generality.

(c) If $a, b \in K[[x]]$ are two FPSs satisfying $a \overset{x^n}{\equiv} b$, then $\lambda a \overset{x^n}{\equiv} \lambda b$ for each $\lambda \in K$.

(d) If $a, b \in K[[x]]$ are two invertible FPSs satisfying $a \overset{x^n}{\equiv} b$, then $a^{-1} \overset{x^n}{\equiv} b^{-1}$.

(e) Let S be a finite set. Let $(a_s)_{s\in S} \in K[[x]]^S$ and $(b_s)_{s\in S} \in K[[x]]^S$ be two families of FPSs such that

$$\text{each } s \in S \text{ satisfies } a_s \overset{x^n}{\equiv} b_s. \tag{100}$$

Then, we have

$$\sum_{s\in S} a_s \overset{x^n}{\equiv} \sum_{s\in S} b_s; \tag{101}$$

$$\prod_{s\in S} a_s \overset{x^n}{\equiv} \prod_{s\in S} b_s. \tag{102}$$

Proof of Theorem 3.10.3 (sketched). All of these properties are analogous to familiar properties of integer congruences, except for Theorem 3.10.3 **(d)**, which is moot for integers (since there are not many integers that are invertible in $\mathbb{Z}$). The proofs are similarly simple (using (18), (19), (20) and (23)). Thus, we shall only give some hints for the proof of Theorem 3.10.3 **(d)** here; detailed proofs of all parts of Theorem 3.10.3 can be found in Section B.1.

(d) Let $a, b \in K[[x]]$ be two invertible FPSs satisfying $a \overset{x^n}{\equiv} b$. We want to show that $a^{-1} \overset{x^n}{\equiv} b^{-1}$.

The FPS a is invertible; thus, its constant term $[x^0]\, a$ is invertible in K (by Proposition 3.3.7).

Recall that $a \overset{x^n}{\equiv} b$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m]\, a = [x^m]\, b. \tag{103}$$

Now, we want to prove that $a^{-1} \overset{x^n}{\equiv} b^{-1}$. In other words, we want to prove that each $m \in \{0, 1, \ldots, n\}$ satisfies $[x^m]\,(a^{-1}) = [x^m]\,(b^{-1})$. We shall prove this by strong induction on m: We fix some $k \in \{0, 1, \ldots, n\}$, and we assume (as an induction hypothesis) that

$$[x^m]\left(a^{-1}\right) = [x^m]\left(b^{-1}\right) \qquad \text{for each } m \in \{0, 1, \ldots, k-1\}. \tag{104}$$

We must now prove that $[x^k]\,(a^{-1}) = [x^k]\,(b^{-1})$. We know that

$$\begin{aligned}
\left[x^k\right]\left(aa^{-1}\right) &= \sum_{i=0}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right]\left(a^{-1}\right) \qquad \text{(by (20))} \\
&= \left[x^0\right] a \cdot \left[x^k\right]\left(a^{-1}\right) + \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right]\left(a^{-1}\right)
\end{aligned}$$

(here, we have split off the addend for $i = 0$ from the sum). Thus,

$$\left[x^0\right] a \cdot \left[x^k\right] \left(a^{-1}\right) + \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right] \left(a^{-1}\right) = \left[x^k\right] \underbrace{\left(aa^{-1}\right)}_{=1} = \left[x^k\right] 1.$$

We can solve this equation for $\left[x^k\right] \left(a^{-1}\right)$ (since $\left[x^0\right] a$ is invertible), and thus obtain

$$\left[x^k\right] \left(a^{-1}\right) = \frac{1}{\left[x^0\right] a} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right] \left(a^{-1}\right)\right).$$

The same argument (applied to b instead of a) yields

$$\left[x^k\right] \left(b^{-1}\right) = \frac{1}{\left[x^0\right] b} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] b \cdot \left[x^{k-i}\right] \left(b^{-1}\right)\right).$$

The right hand sides of the latter two equalities are equal (since each $i \in \{1, 2, \ldots, k\}$ satisfies $\left[x^i\right] a = \left[x^i\right] b$ as a consequence of (103), and satisfies $\left[x^{k-i}\right] \left(a^{-1}\right) = \left[x^{k-i}\right] \left(b^{-1}\right)$ as a consequence of (104), and since we have $\left[x^0\right] a = \left[x^0\right] b$ as a consequence of (103)). Hence, the left hand sides must also be equal. In other words, $\left[x^k\right] \left(a^{-1}\right) = \left[x^k\right] \left(b^{-1}\right)$, which is precisely what we wanted to prove. Thus, the induction step is complete, so that $a^{-1} \overset{x^n}{\equiv} b^{-1}$ is proved. Thus, Theorem 3.10.3 **(d)** is proved. (See Section B.1 for more details.) □

Let us next characterize x^n-equivalence of FPSs in terms of divisibility:

Proposition 3.10.4. Let $n \in \mathbb{N}$. Let $f, g \in K[[x]]$ be two FPSs. Then, we have $f \overset{x^n}{\equiv} g$ if and only if the FPS $f - g$ is a multiple of x^{n+1}.

Proof of Proposition 3.10.4. See Section B.1 for this proof (a simple consequence of Lemma 3.3.18). □

Finally, here is a subtler property of x^n-equivalence similar to the ones in Theorem 3.10.3 **(b)**:

Proposition 3.10.5. Let $n \in \mathbb{N}$. Let $a, b, c, d \in K[[x]]$ be four FPSs satisfying $a \overset{x^n}{\equiv} b$ and $c \overset{x^n}{\equiv} d$ and $\left[x^0\right] c = 0$ and $\left[x^0\right] d = 0$. Then,

$$a \circ c \overset{x^n}{\equiv} b \circ d.$$

Proof of Proposition 3.10.5 (sketched). Write a and b as $a = \sum_{i \in \mathbb{N}} a_i x^i$ and $b = \sum_{i \in \mathbb{N}} b_i x^i$ (with $a_i, b_i \in K$). Then, $a \overset{x^n}{\equiv} b$ means that $a_i = b_i$ for all $i \leq n$. Combine this with $c^i \overset{x^n}{\equiv} d^i$ (which holds for all $i \in \mathbb{N}$ as a consequence of $c \overset{x^n}{\equiv} d$ and of (102)) to obtain the relation $a_i c^i \overset{x^n}{\equiv} b_i d^i$ for all $i \leq n$. But this relation also holds for all $i > n$, since all such i satisfy $[x^m]\left(c^i\right) = [x^m]\left(d^i\right) = 0$ for all $m \in \{0, 1, \ldots, n\}$ (a consequence of Lemma 3.3.18 using $\left[x^0\right] c = 0$ and $\left[x^0\right] d = 0$). Thus, the relation $a_i c^i \overset{x^n}{\equiv} b_i d^i$ holds for all $i \in \mathbb{N}$. Summing over all i, we find $a \circ c \overset{x^n}{\equiv} b \circ d$.

See Section B.1 for the details of this argument. □

3.11. Infinite products

Let us now extend our FPS playground somewhat. We have made sense of infinite sums. What about infinite products?

3.11.1. An example

We start with a **motivating example** (due to Euler, in [Euler48, §328–329]), which we shall first discuss informally.

Assume (for the time being) that the infinite product

$$\prod_{i \in \mathbb{N}} \left(1 + x^{2^i}\right) = \left(1 + x^1\right)\left(1 + x^2\right)\left(1 + x^4\right)\left(1 + x^8\right) \cdots \qquad (105)$$

in the ring $K[[x]]$ is meaningful, and that such products behave as nicely as finite products. Can we simplify this product?

We can observe that each $i \in \mathbb{N}$ satisfies $1 + x^{2^i} = \dfrac{1 - x^{2^{i+1}}}{1 - x^{2^i}}$ (since $1 - x^{2^{i+1}} = 1 - \left(x^{2^i}\right)^2 = \left(1 - x^{2^i}\right)\left(1 + x^{2^i}\right)$). Multiplying these equalities over all $i \in \mathbb{N}$, we obtain

$$\prod_{i \in \mathbb{N}} \left(1 + x^{2^i}\right) = \prod_{i \in \mathbb{N}} \frac{1 - x^{2^{i+1}}}{1 - x^{2^i}} = \frac{1 - x^2}{1 - x^1} \cdot \frac{1 - x^4}{1 - x^2} \cdot \frac{1 - x^8}{1 - x^4} \cdot \frac{1 - x^{16}}{1 - x^8} \cdot \cdots .$$

The product on the right hand side here is a *telescoping product* – meaning that each numerator is cancelled by the denominator of the following fraction. Assuming (somewhat plausibly, but far from rigorously) that we are allowed to cancel infinitely many factors from an infinite product, we thus end up with a single $1 - x^1$ factor in the denominator. That is, our product simplifies to $\dfrac{1}{1 - x^1}$. Thus, we obtain

$$\prod_{i \in \mathbb{N}} \left(1 + x^{2^i}\right) = \frac{1}{1 - x^1} = \frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots . \qquad (106)$$

This was not very rigorous, so let us try to compute the product $\prod_{i\in\mathbb{N}}\left(1+x^{2^i}\right)$ in a different way. Namely, we recall a simple fact about finite products: If $a_0, a_1, \ldots, a_m$ are finitely many elements of a commutative ring, then the product

$$\prod_{i=0}^{m}(1+a_i) = (1+a_0)(1+a_1)\cdots(1+a_m) \qquad (107)$$

equals the sum[33]

$$\sum_{i_1<i_2<\cdots<i_k\leq m} a_{i_1}a_{i_2}\cdots a_{i_k}$$

of all the 2^{m+1} "sub-products" of the product $a_0a_1\cdots a_m$ (because this sum is what we obtain if we expand $\prod_{i=0}^{m}(1+a_i)$ by repeatedly applying distributivity). For example, for $m=2$, this is saying that

$$\begin{aligned}&(1+a_0)(1+a_1)(1+a_2)\\&=1+a_0+a_1+a_2+a_0a_1+a_0a_2+a_1a_2+a_0a_1a_2.\end{aligned}$$

Now, it is plausible to expect the same formula $\prod_{i=0}^{m}(1+a_i) = \sum_{I\subseteq\{0,1,\ldots,m\}}\prod_{i\in I}a_i$ to hold if "m is ∞" (that is, if the product ranges over all $i\in\mathbb{N}$), provided that the product is meaningful. In other words, it is plausible to expect that

$$\prod_{i\in\mathbb{N}}(1+a_i) = \sum_{i_1<i_2<\cdots<i_k} a_{i_1}a_{i_2}\cdots a_{i_k} \qquad (108)$$

for any infinite sequence $a_0, a_1, a_2, \ldots$ as long as $\prod_{i\in\mathbb{N}}(1+a_i)$ makes sense. (It's a little bit more complicated than that, but we aren't trying to be fully rigorous yet. The correct condition is that the sequence $(a_0, a_1, a_2, \ldots)$ is summable.) If we now apply (108) to $a_i = x^{2^i}$, then we obtain

$$\begin{aligned}\prod_{i\in\mathbb{N}}\left(1+x^{2^i}\right) &= \sum_{i_1<i_2<\cdots<i_k} x^{2^{i_1}}x^{2^{i_2}}\cdots x^{2^{i_k}} = \sum_{i_1<i_2<\cdots<i_k} x^{2^{i_1}+2^{i_2}+\cdots+2^{i_k}}\\&=\sum_{n\in\mathbb{N}} q_nx^n, \qquad (109)\end{aligned}$$

where q_n is the # of ways to write the integer n as a sum $2^{i_1}+2^{i_2}+\cdots+2^{i_k}$ with nonnegative integers $i_1, i_2, \ldots, i_k$ satisfying $i_1<i_2<\cdots<i_k$. Comparing this with (106), we obtain

$$\sum_{n\in\mathbb{N}} q_nx^n = 1+x+x^2+x^3+\cdots = \sum_{n\in\mathbb{N}} x^n,$$

[33] The indices $i_1, i_2, \ldots, i_k$ of the sum are supposed to be nonnegative integers.

at least if our assumptions were valid. Comparing coefficients, this would mean that $q_n = 1$ for each $n \in \mathbb{N}$. In other words, each $n \in \mathbb{N}$ can be written in **exactly one** way as a sum $2^{i_1} + 2^{i_2} + \cdots + 2^{i_k}$ with nonnegative integers $i_1, i_2, \ldots, i_k$ satisfying $i_1 < i_2 < \cdots < i_k$. In other words, each $n \in \mathbb{N}$ can be written uniquely as a finite sum of distinct powers of 2.

Is this true? Yes, because this is just saying that each $n \in \mathbb{N}$ has a unique binary representation. For example, $21 = 2^4 + 2^2 + 2^0$ corresponds to the binary representation $21 = (10101)_2$.

Thus, the two results we have obtained in (106) and (109) are actually equal, which is reassuring. Yet, this does not replace a formal definition of infinite products that rigorously justifies the above arguments.

3.11.2. A rigorous definition

One way of rigorously defining infinite products of FPSs can be found in [Loehr11, §7.5]. However, this definition only defines infinite products of the form $\prod_{i\in\mathbb{N}}$ or $\prod_{i=1}^{\infty}$, but not (for example) of the form $\prod_{I\subseteq\mathbb{N}}$ or $\prod_{(i,j)\in\mathbb{N}\times\mathbb{N}}$. Another definition of infinite products uses the Log and Exp bijections from Definition 3.7.6 to turn products into sums; but this requires K to be a $\mathbb{Q}$-algebra (since Log and Exp aren't defined otherwise). Thus, we shall give a different definition here.

We recall our definition of infinite sums of FPSs (Definition 3.2.9):

> **Definition 3.2.9 (repeated).** A (possibly infinite) family $(\mathbf{a}_i)_{i\in I}$ of FPSs is said to be *summable* if
>
> for each $n \in \mathbb{N}$, all but finitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$.
>
> In this case, the sum $\sum_{i\in I} \mathbf{a}_i$ is defined to be the FPS with
>
> $$[x^n]\left(\sum_{i\in I}\mathbf{a}_i\right) = \underbrace{\sum_{i\in I}[x^n]\,\mathbf{a}_i}_{\substack{\text{an essentially}\\ \text{finite sum}}} \qquad \text{for all } n \in \mathbb{N}.$$

This is how we defined infinite sums of FPSs. We cannot use the same definition for infinite products, because usually

$$\text{we **don't** expect to have } [x^n]\left(\prod_{i\in I}\mathbf{a}_i\right) = \prod_{i\in I}[x^n]\,\mathbf{a}_i$$

(after all, multiplication of FPSs is not defined coefficientwise). The condition "all but finitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$" is therefore not what we are looking for.

Let us instead go back to the idea behind Definition 3.2.9. Let us fix some $n \in \mathbb{N}$. What was the actual purpose of the "all but finitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$" condition? The purpose was to ensure that the coefficient $[x^n]\left(\sum\limits_{i\in I}\mathbf{a}_i\right)$ is determined by **finitely many** of the $\mathbf{a}_i$'s. In other words, the purpose was to ensure that there is a **finite** partial sum of $\sum\limits_{i\in I}\mathbf{a}_i$ such that if we add any further $\mathbf{a}_i$'s to this partial sum, then the coefficient of x^n does not change any more. Here is a way to restate this condition more rigorously: There is a **finite** subset M of I such that every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\sum_{i\in M}\mathbf{a}_i\right) = [x^n]\left(\sum_{i\in J}\mathbf{a}_i\right).$$

(The subset M here is the indexing set of our finite partial sum, and the set J is what it becomes if we add some further $\mathbf{a}_i$'s to this partial sum.)

This condition is a mouthful; this is why we found it easier to boil it down to the simple "all but finitely many $i \in I$ satisfy $[x^n]\,\mathbf{a}_i = 0$" condition in the case of infinite sums. However, in the case of infinite products, we cannot boil it down to something this simple; thus, we have to live with it.

Fortunately, we can simplify our life by giving this condition a name:

Definition 3.11.1. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a (possibly infinite) family of FPSs. Let $n \in \mathbb{N}$. Let M be a finite subset of I.

(a) We say that M *determines the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$* if every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\sum_{i\in J}\mathbf{a}_i\right) = [x^n]\left(\sum_{i\in M}\mathbf{a}_i\right).$$

(You can think of this condition as saying "If you add any further $\mathbf{a}_i$s to the sum $\sum\limits_{i\in M}\mathbf{a}_i$, then the x^n-coefficient stays unchanged", or, more informally: "If you want to know the x^n-coefficient of $\sum\limits_{i\in I}\mathbf{a}_i$, it suffices to take the partial sum over all $i \in M$".)

(b) We say that M *determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$* if every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\prod_{i\in J}\mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M}\mathbf{a}_i\right).$$

(You can think of this condition as saying "If you multiply any further $\mathbf{a}_i$s to the product $\prod\limits_{i\in M}\mathbf{a}_i$, then the x^n-coefficient stays unchanged", or, more informally: "If you want to know the x^n-coefficient of $\prod\limits_{i\in I}\mathbf{a}_i$, it suffices to take the partial product over all $i \in M$".)

Example 3.11.2. **(a)** Consider the family

$$\begin{aligned}
&\left(\left(x+x^2\right)^i\right)_{i\in\mathbb{N}} \\
&= \left(\left(x+x^2\right)^0,\ \left(x+x^2\right)^1,\ \left(x+x^2\right)^2,\ \left(x+x^2\right)^3,\ \left(x+x^2\right)^4,\ \ldots\right) \\
&= \left(1,\ \ x+x^2,\ \ x^2+2x^3+x^4,\ \ x^3+3x^4+3x^5+x^6,\ \ x^4+4x^5+6x^6+4x^7+x^8,\ \ \ldots\right)
\end{aligned}$$

of FPSs. The subset $\{1,2,3\}$ of $\mathbb{N}$ determines the x^3-coefficient in the sum of this family $\left(\left(x+x^2\right)^i\right)_{i\in\mathbb{N}}$, because every finite subset J of $\mathbb{N}$ satisfying $\{1,2,3\} \subseteq J \subseteq \mathbb{N}$ satisfies

$$\left[x^3\right]\left(\sum_{i\in J}\left(x+x^2\right)^i\right) = \left[x^3\right]\left(\sum_{i\in\{1,2,3\}}\left(x+x^2\right)^i\right)$$

(this is simply a consequence of the fact that the only three entries of our family that have a nonzero x^3-coefficient are the entries $\left(x+x^2\right)^i$ for $i \in \{1,2,3\}$). Thus, any finite subset of $\mathbb{N}$ that contains $\{1,2,3\}$ as a subset determines the x^3-coefficient in the sum of this family $\left(\left(x+x^2\right)^i\right)_{i\in\mathbb{N}}$.

(b) Consider the family

$$\left(1+x^i\right)_{i\in\mathbb{N}} = \left(1+1,\ \ 1+x,\ \ 1+x^2,\ \ 1+x^3,\ \ 1+x^4,\ \ \ldots\right)$$

of FPSs. The subset $\{0,1,2,3\}$ of $\mathbb{N}$ determines the x^3-coefficient in the product of this family $\left(1+x^i\right)_{i\in\mathbb{N}}$, because every finite subset J of $\mathbb{N}$ satisfying $\{0,1,2,3\} \subseteq J \subseteq \mathbb{N}$ satisfies

$$\left[x^3\right]\left(\prod_{i\in J}\left(1+x^i\right)\right) = \left[x^3\right]\left(\prod_{i\in\{0,1,2,3\}}\left(1+x^i\right)\right).$$

(This is because multiplying an FPS by any of the polynomials $1+x^4$, $1+x^5$, $1+x^6$, $\ldots$ leaves its x^3-coefficient unchanged.) Thus, any finite subset of $\mathbb{N}$ that contains $\{0,1,2,3\}$ as a subset determines the x^3-coefficient in the product of this family $\left(1+x^i\right)_{i\in\mathbb{N}}$.

On the other hand, the subset $\{0,3\}$ of $\mathbb{N}$ does **not** determine the x^3-coefficient in the product of $\left(1+x^i\right)_{i\in\mathbb{N}}$. To see this, it suffices to notice that

$$\underbrace{\left[x^3\right]\left(\prod_{i\in\{0,1,2,3\}}\left(1+x^i\right)\right)}_{=4} \neq \underbrace{\left[x^3\right]\left(\prod_{i\in\{0,3\}}\left(1+x^i\right)\right)}_{=2}.$$

(The philosophical reason is that, even though the monomial x^3 itself does not appear in any of the entries $1+x^1$ and $1+x^2$, it does emerge in the product of these two entries with the constant term of $\prod\limits_{i\in\{0,3\}} \left(1+x^i\right) = (1+1)\left(1+x^3\right)$.)

Definition 3.11.3. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a (possibly infinite) family of FPSs. Let $n \in \mathbb{N}$.

(a) We say that *the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$ is finitely determined* if there is a finite subset M of I that determines the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$.

(b) We say that *the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined* if there is a finite subset M of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$.

Using these concepts, we can now reword our definition of infinite sums as follows:

Proposition 3.11.4. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a (possibly infinite) family of FPSs. Then:

(a) The family $(\mathbf{a}_i)_{i\in I}$ is summable if and only if each coefficient in its sum is finitely determined (i.e., for each $n \in \mathbb{N}$, the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$ is finitely determined).

(b) If the family $(\mathbf{a}_i)_{i\in I}$ is summable, then its sum $\sum\limits_{i\in I} \mathbf{a}_i$ is the FPS whose x^n-coefficient (for any $n \in \mathbb{N}$) can be computed as follows: If $n \in \mathbb{N}$, and if M is a finite subset of I that determines the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$, then

$$\left[x^n\right]\left(\sum_{i\in I} \mathbf{a}_i\right) = \left[x^n\right]\left(\sum_{i\in M} \mathbf{a}_i\right).$$

Proof. Easy and LTTR. □

The rest of Chapter 3 needs more details.
TODO: Push this border stone further down this chapter.

Inspired by Proposition 3.11.4, we can now define infinite products of FPSs at last:

Definition 3.11.5. Let $(\mathbf{a}_i)_{i\in I}$ be a (possibly infinite) family of FPSs. Then:

(a) The family $(\mathbf{a}_i)_{i\in I}$ is said to be *multipliable* if and only if each coefficient in its product is finitely determined.

(b) If the family $(\mathbf{a}_i)_{i\in I}$ is multipliable, then its *product* $\prod\limits_{i\in I} \mathbf{a}_i$ is defined to be the FPS whose x^n-coefficient (for any $n \in \mathbb{N}$) can be computed as follows: If $n \in \mathbb{N}$, and if M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$, then

$$[x^n]\left(\prod_{i\in I} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M} \mathbf{a}_i\right).$$

Proposition 3.11.6. This definition of $\prod\limits_{i\in I} \mathbf{a}_i$ is well-defined – i.e., the coefficient $[x^n]\left(\prod\limits_{i\in M} \mathbf{a}_i\right)$ does not depend on M (as long as M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$).

Proof. Let $n \in \mathbb{N}$. We need to check that the coefficient $[x^n]\left(\prod\limits_{i\in M} \mathbf{a}_i\right)$ does not depend on M (as long as M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$). In other words, we need to check that if M_1 and M_2 are two finite subsets of I that each determine the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$, then

$$[x^n]\left(\prod_{i\in M_1} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M_2} \mathbf{a}_i\right). \tag{110}$$

So let us prove this. Let M_1 and M_2 be two finite subsets of I that each determine the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$. Thus, in particular, M_1 determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$. In other words, every finite subset J of I satisfying $M_1 \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\prod_{i\in J} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M_1} \mathbf{a}_i\right).$$

Applying this to $J = M_1 \cup M_2$, we obtain

$$[x^n]\left(\prod_{i\in M_1\cup M_2} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M_1} \mathbf{a}_i\right) \tag{111}$$

(since $M_1 \cup M_2$ is a subset of I satisfying $M_1 \subseteq M_1 \cup M_2 \subseteq I$). The same argument (with the roles of M_1 and M_2 swapped) yields

$$[x^n]\left(\prod_{i\in M_2\cup M_1} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M_2} \mathbf{a}_i\right). \tag{112}$$

The left hand sides of the equalities (111) and (112) are equal (since $M_1 \cup M_2 = M_2 \cup M_1$). Thus, the right hand sides are equal as well. In other words, $[x^n]\left(\prod\limits_{i\in M_1} \mathbf{a}_i\right) = [x^n]\left(\prod\limits_{i\in M_2} \mathbf{a}_i\right)$. Thus, we have proved (110), and with it Proposition 3.11.6. □

The attentive (and pedantic) reader might notice that there is one more thing that needs to be checked in order to make sure that Definition 3.11.5 **(b)** is legitimate. In fact, this definition does not merely define (some) infinite products $\prod\limits_{i\in I} \mathbf{a}_i$ of FPSs, but also "accidentally" gives a new meaning to **finite** products $\prod\limits_{i\in I} \mathbf{a}_i$ (since a finite family $(\mathbf{a}_i)_{i\in I}$ of FPSs is always multipliable). We therefore need to check that this new meaning does not conflict with the original definition of a finite product of elements of a commutative ring. In other words, we need to prove the following:

> **Proposition 3.11.7.** Let $(\mathbf{a}_i)_{i\in I}$ be a finite family of FPSs. Then, the product $\prod\limits_{i\in I} \mathbf{a}_i$ defined according to Definition 3.11.5 **(b)** equals the finite product $\prod\limits_{i\in I} \mathbf{a}_i$ defined in the usual way (i.e., defined as in any commutative ring).

Proof. Argue that I itself is a subset of I that determines all coefficients in the product of $(\mathbf{a}_i)_{i\in I}$. See Section B.2 for a detailed proof. □

Let us now see that this legitimizes our product $\prod\limits_{i\in\mathbb{N}} \left(1 + x^{2^i}\right)$ from Subsection 3.11.1. Indeed,

$$\prod_{i\in\mathbb{N}} \left(1 + x^{2^i}\right) = \left(1 + x^1\right)\left(1 + x^2\right)\left(1 + x^4\right)\left(1 + x^8\right)\cdots.$$

If you want to compute the x^6-coefficient in this product, you only need to multiply the first 3 factors $(1 + x^1)(1 + x^2)(1 + x^4)$; none of the other factors will change this coefficient in any way, because multiplying an FPS by $1 + x^m$ (for some $m > 0$) does not change its first m coefficients[34]. Likewise, if you want to compute the x^{13}-coefficient of the above product, then you only need to multiply the first 4 factors; none of the others will have any effect on this coefficient. The same logic applies to the x^n-coefficient for any $n \in \mathbb{N}$; it is determined by the first $\lfloor \log_2 n \rfloor + 1$ factors of the product. Thus, each coefficient

[34] For example, let us check this for $m = 3$: If we multiply an FPS $a_0x^0 + a_1x^1 + a_2x^2 + \cdots$ by $1 + x^3$, then we obtain

$$\begin{aligned}&\left(a_0x^0 + a_1x^1 + a_2x^2 + \cdots\right)\left(1 + x^3\right)\\ &= a_0x^0 + a_1x^1 + a_2x^2 + (a_3 + a_0)\,x^3 + (a_4 + a_1)\,x^4 + (a_5 + a_2)\,x^5 + \cdots,\end{aligned}$$

and so the first 3 coefficients are left unchanged.

in the product is finitely determined. This means that the family is multipliable; thus, its product makes sense.

In contrast, the product

$$(1+0x)(1+1x)(1+2x)(1+3x)(1+4x)\cdots = \prod_{i\in\mathbb{N}} (1+ix)$$

does not make sense. Indeed, its x^1-coefficient is not finitely determined (any of the factors other than $1+0x$ affects it), so the family $(1+ix)_{i\in\mathbb{N}}$ is not multipliable.

Recall our reasoning that we used above to prove that the family $\left(1+x^{2^i}\right)_{i\in\mathbb{N}}$ is multipliable. The core of this reasoning was the observation that multiplying an FPS by $1+x^m$ (for some $m>0$) does not change its first m coefficients. This can be generalized: If $f\in K[[x]]$ is an FPS whose first m coefficients are 0 (for example, f can be x^m, in which case we recover the statement in our preceding sentence), then multiplying an FPS a by $1+f$ does not change its first m coefficients (that is, the first m coefficients of $a(1+f)$ are the first m coefficients of a). This is a useful fact, so let us state it as a lemma (renaming m as $n+1$):

Lemma 3.11.8. Let $a,f\in K[[x]]$ be two FPSs. Let $n\in\mathbb{N}$. Assume that

$$[x^m] f = 0 \qquad \text{for each } m\in\{0,1,\ldots,n\}. \tag{113}$$

Then,

$$[x^m](a(1+f)) = [x^m] a \qquad \text{for each } m\in\{0,1,\ldots,n\}.$$

Proof of Lemma 3.11.8. The FPS af is a multiple of f (since $af=fa$). Hence, Lemma 3.3.21 (applied to $u=f$ and $v=af$) yields that

$$[x^m](af) = 0 \qquad \text{for each } m\in\{0,1,\ldots,n\} \tag{114}$$

(since we have assumed that $[x^m] f = 0$ for each $m\in\{0,1,\ldots,n\}$).

Now, for each $m\in\{0,1,\ldots,n\}$, we have

$$\begin{aligned}[x^m]\left(\underbrace{a(1+f)}_{=a+af}\right) &= [x^m](a+af) = [x^m]a + \underbrace{[x^m](af)}_{\substack{=0\\ \text{(by (114))}}} \qquad \text{(by (18))}\\ &= [x^m]a.\end{aligned}$$

This proves Lemma 3.11.8. □

For convenience, let us extend Lemma 3.11.8 to products of several factors:

Lemma 3.11.9. Let $a \in K[[x]]$ be an FPS. Let $(f_i)_{i \in J} \in K[[x]]^J$ be a finite family of FPSs. Let $n \in \mathbb{N}$. Assume that each $i \in J$ satisfies

$$[x^m](f_i) = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \tag{115}$$

Then,

$$[x^m]\left(a \prod_{i \in J}(1 + f_i)\right) = [x^m]\, a \qquad \text{for each } m \in \{0, 1, \ldots, n\}.$$

Proof of Lemma 3.11.9. This is just Lemma 3.11.8, applied several times (specifically, $|J|$ many times). See Section B.2 for a detailed proof. □

Now, using Lemma 3.11.9, we can obtain the following convenient criterion for multipliability:

Theorem 3.11.10. Let $(f_i)_{i \in I} \in K[[x]]^I$ be a (possibly infinite) summable family of FPSs. Then, the family $(1 + f_i)_{i \in I}$ is multipliable.

Proof of Theorem 3.11.10. This is an easy consequence of Lemma 3.11.9. See Section B.2 for a detailed proof. □

We notice two simple sufficient (if rarely satisfied) criteria for multipliability:

Proposition 3.11.11. If all but finitely many entries of a family $(\mathbf{a}_i)_{i \in I} \in K[[x]]^I$ equal 1 (that is, if all but finitely many $i \in I$ satisfy $\mathbf{a}_i = 1$), then this family is multipliable.

Proof. LTTR. (See Section B.2 for a detailed proof.) □

Remark 3.11.12. If a family $(\mathbf{a}_i)_{i \in I} \in K[[x]]^I$ contains 0 as an entry (i.e., if there exists an $i \in I$ such that $\mathbf{a}_i = 0$), then this family is automatically multipliable, and its product is 0.

Proof. Assume that the family $(\mathbf{a}_i)_{i \in I}$ contains 0 as an entry. That is, there exists some $j \in I$ such that $\mathbf{a}_j = 0$. Consider this j. Now, it is easy to see that the subset $\{j\}$ of I determines all coefficients in the product of $(\mathbf{a}_i)_{i \in I}$. The details are LTTR. □

Working with multipliable families gets slightly easier using the following notion:

Definition 3.11.13. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a family of FPSs. Let $n \in \mathbb{N}$. An *x^n-approximator* for $(\mathbf{a}_i)_{i\in I}$ means a finite subset M of I that determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i\in I}$. (In other words, M has to determine the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ for each $m \in \{0,1,\ldots,n\}$.)

The name "x^n-approximator" is supposed to hint at the fact that if M is an x^n-approximator for a multipliable family $(\mathbf{a}_i)_{i\in I}$, then the (finite) subproduct $\prod\limits_{i\in M} \mathbf{a}_i$ "approximates" the full product $\prod\limits_{i\in I} \mathbf{a}_i$ up until the x^n-coefficient (i.e., the first $n+1$ coefficients of $\prod\limits_{i\in M} \mathbf{a}_i$ equal the respective coefficients of $\prod\limits_{i\in I} \mathbf{a}_i$). See Proposition 3.11.16 **(b)** below for the precise statement of this fact.

Clearly, an x^n-approximator for a family $(\mathbf{a}_i)_{i\in I}$ always determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$. But the converse is not true, as the following example shows:

Example 3.11.14. Consider the family

$$\left(1+x^{2^i}\right)_{i\in\mathbb{N}} = \left(1+x^1,\ 1+x^2,\ 1+x^4,\ 1+x^8,\ \ldots\right)$$

of FPSs. The finite subset $\{1,2\}$ of $\mathbb{N}$ determines the x^6-coefficient in the product of this family (indeed, the x^6-coefficient of the product $(1+x^2)(1+x^4)$ is 1, and this does not change if we multiply any further factors onto this product), but is not an x^6-approximator for this family (since, e.g., it does not determine the x^5-coefficient in its product).

Lemma 3.11.15. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a multipliable family of FPSs. Let $n \in \mathbb{N}$. Then, there exists an x^n-approximator for $(\mathbf{a}_i)_{i\in I}$.

Proof of Lemma 3.11.15 (sketched). This is an easy consequence of the fact that a union of finitely many finite sets is finite. A detailed proof can be found in Section B.2. □

As promised above, we can use x^n-approximators to "approximate" infinite products of FPSs (in the sense of: compute the first $n+1$ coefficients of these products). Here is why this works:[35]

Proposition 3.11.16. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a family of FPSs. Let $n \in \mathbb{N}$. Let M be an x^n-approximator for $(\mathbf{a}_i)_{i\in I}$. Then:

(a) Every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$\prod_{i\in J} \mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in M} \mathbf{a}_i.$$

[35] See Definition 3.10.1 for the meaning of the symbol "$\overset{x^n}{\equiv}$" appearing in this proposition.

(b) If the family $(\mathbf{a}_i)_{i\in I}$ is multipliable, then

$$\prod_{i\in I}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in M}\mathbf{a}_i.$$

Proof. This follows easily from Definition 3.11.13 and Definition 3.11.5 **(b)**. See Section B.2 for a detailed proof. □

Here are some further properties of multipliable families:

Proposition 3.11.17. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a family of FPSs. Let J be a subset of I. Assume that the subfamilies $(\mathbf{a}_i)_{i\in J}$ and $(\mathbf{a}_i)_{i\in I\setminus J}$ are multipliable. Then:

(a) The entire family $(\mathbf{a}_i)_{i\in I}$ is multipliable.

(b) We have

$$\prod_{i\in I}\mathbf{a}_i = \left(\prod_{i\in J}\mathbf{a}_i\right)\cdot\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right).$$

Proof of Proposition 3.11.17 (sketched). Here is the idea: Fix $n \in \mathbb{N}$. Lemma 3.11.15 (applied to J instead of I) shows that there exists an x^n-approximator U for $(\mathbf{a}_i)_{i\in J}$. Consider this U. Lemma 3.11.15 (applied to J instead of I) shows that there exists an x^n-approximator V for $(\mathbf{a}_i)_{i\in I\setminus J}$. Consider this V. Note that $U\cup V$ is finite (since U and V are finite). Now, it is not hard to see that $U\cup V$ determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ (indeed, it is not much harder to see that $U\cup V$ is an x^n-approximator for $(\mathbf{a}_i)_{i\in I}$). Hence, the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined (since $U\cup V$ is finite). Now, forget that we fixed n, and conclude that the family $(\mathbf{a}_i)_{i\in I}$ is multipliable. This proves part **(a)**. Part **(b)** easily follows using Proposition 3.11.16 **(b)**.

The details of this proof can be found in Section B.2. □

Proposition 3.11.18. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ and $(\mathbf{b}_i)_{i\in I} \in K[[x]]^I$ be two multipliable families of FPSs. Then:

(a) The family $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is multipliable.

(b) We have

$$\prod_{i\in I}(\mathbf{a}_i\mathbf{b}_i) = \left(\prod_{i\in I}\mathbf{a}_i\right)\cdot\left(\prod_{i\in I}\mathbf{b}_i\right).$$

Proof of Proposition 3.11.18 (sketched). Here is the idea: Fix $n \in \mathbb{N}$. Lemma 3.11.15 shows that there exists an x^n-approximator U for $(\mathbf{a}_i)_{i\in I}$. Consider this U. Lemma 3.11.15 (applied to $\mathbf{b}_i$ instead of $\mathbf{a}_i$) shows that there exists an x^n-approximator V for $(\mathbf{b}_i)_{i\in I}$. Consider this V. Note that $U\cup V$ is finite (since U

and V are finite). Now, it is not hard to see that $U \cup V$ is an x^n-approximator for $(\mathbf{a}_i \mathbf{b}_i)_{i \in I}$. From here, proceed as in the proof of Proposition 3.11.17.

The details of this proof can be found in Section B.2. □

Proposition 3.11.19. Let $(\mathbf{a}_i)_{i \in I} \in K[[x]]^I$ be a multipliable family of invertible FPSs. Then, any subfamily of $(\mathbf{a}_i)_{i \in I}$ is multipliable.

Proof of Proposition 3.11.19 (sketched). This is another proof in the tradition of the proofs of Proposition 3.11.17 and Proposition 3.11.18. We must show that the family $(\mathbf{a}_i)_{i \in J}$ is multipliable whenever J is a subset of I. The idea is to show that if U is an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$, then $U \cap J$ determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in J}$ (and, in fact, is an x^n-approximator for $(\mathbf{a}_i)_{i \in J}$). This relies on the invertibility of $\prod\limits_{i \in M \setminus J} \mathbf{a}_i$; this is why the FPS $\mathbf{a}_i$ are required to be invertible in the proposition.

The details of this proof can be found in Section B.2. □

Remark 3.11.20. Proposition 3.11.19 would not hold if we did not assume that the $\mathbf{a}_i$ are invertible. For example, the family $(0, 1, 2, 3, \ldots)$ is multipliable, but its subfamily $(1, 2, 3, \ldots)$ is not.

To justify our work from Subsection 3.11.1, we still need to argue that the products we have defined are well-behaved – i.e., satisfy the usual rules that finite products satisfy, with some minor caveats. To stay on the safe side, we state them only for products of invertible FPSs, to avoid the nasty surprises we know from Remark 3.11.20:

Proposition 3.11.21. Products of multipliable families of FPSs satisfy the usual rules for products, as long as we assume that our families consist of invertible FPSs. For example, the following facts hold:

- Let $(\mathbf{a}_s)_{s \in S} \in K[[x]]^S$ and $(\mathbf{b}_s)_{s \in S} \in K[[x]]^S$ be two multipliable families of invertible FPSs. Then, the family $(\mathbf{a}_s \mathbf{b}_s)_{s \in S}$ is multipliable as well, and satisfies
$$\prod_{s \in S} (\mathbf{a}_s \mathbf{b}_s) = \left(\prod_{s \in S} \mathbf{a}_s \right) \cdot \left(\prod_{s \in S} \mathbf{b}_s \right).$$
- Let $(\mathbf{a}_s)_{s \in S} \in K[[x]]^S$ be a multipliable family of invertible FPSs. Let X and Y be two subsets of S such that $X \cap Y = \varnothing$ and $X \cup Y = S$. Then,
$$\prod_{s \in S} \mathbf{a}_s = \left(\prod_{s \in X} \mathbf{a}_s \right) \cdot \left(\prod_{s \in Y} \mathbf{a}_s \right).$$

- Let $(\mathbf{a}_s)_{s\in S} \in K[[x]]^S$ be a multipliable family of invertible FPSs. Let W be a set. Let $f : S \to W$ be a map. Then,

$$\prod_{s\in S} \mathbf{a}_s = \prod_{w\in W} \prod_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s.$$

(In particular, the right hand side is well-defined – i.e., the family $(\mathbf{a}_s)_{s\in S;\ f(s)=w}$ is multipliable for each $w \in W$, and the family $\left(\prod_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s\right)_{w\in W}$ is also multipliable.)

- Let I and J be two sets. Let $\left(\mathbf{a}_{(i,j)}\right)_{(i,j)\in I\times J} \in K[[x]]^{I\times J}$ be a multipliable family of invertible FPSs. Then,

$$\prod_{i\in I} \prod_{j\in J} \mathbf{a}_{(i,j)} = \prod_{(i,j)\in I\times J} \mathbf{a}_{(i,j)} = \prod_{j\in J} \prod_{i\in I} \mathbf{a}_{(i,j)}.$$

(In particular, all the products appearing in this equality are well-defined.)

Proof. In essence, all of these facts can be proved by reducing them to the corresponding properties of finite products. This relies on the fact that all coefficients in multipliable products are finitely determined (conveniently using x^n-approximators, which determine several coefficients at the same time).

TODO: Add details! □

Proposition 3.11.21 justifies most of our manipulations in Subsection 3.11.1 (except possibly for the telescope principle, which is somewhat subtle and needs some qualifications[36]; it is better to argue using more fundamental rules[37]).

[36] Here is an example of how not to use the telescope principle:

$$\frac{1}{2} \cdot \frac{2}{2} \cdot \frac{2}{2} \cdot \frac{2}{2} \cdot \cdots \neq 1.$$

The infinitely many 2's don't factor each other out completely.

[37] To wit, we can argue as follows: We have

$$\prod_{i\in\mathbb{N}} \left(1 + x^{2^i}\right) = \prod_{i\in\mathbb{N}} \frac{1 - x^{2^{i+1}}}{1 - x^{2^i}} = \frac{\prod_{i\in\mathbb{N}} \left(1 - x^{2^{i+1}}\right)}{\prod_{i\in\mathbb{N}} \left(1 - x^{2^i}\right)},$$

where the last step used the fact that both families $\left(1 - x^{2^{i+1}}\right)_{i\in\mathbb{N}}$ and $\left(1 - x^{2^i}\right)_{i\in\mathbb{N}}$ are multipliable (this is important, but very easy to check in this case) and that the product

The only thing we still need to justify is the equality (108). This is what we will do next.

3.11.3. Product rules (generalized distributive laws)

The equality (108) is an instance of a *product rule* – a statement of the form "a product of sums can be expanded into one big sum". The simplest product rules are the distributive laws $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ (here, one of the sums being multiplied is a one-addend sum); one of the next-simplest is $(a+b)(c+d) = ac+ad+bc+bd$. As far as finite sums and finite products are concerned, the following product rule is one of the most general:[38]

> **Proposition 3.11.22.** Let L be a commutative ring. For every $n \in \mathbb{N}$, let $[n]$ denote the set $\{1,2,\ldots,n\}$.
>
> Let $n \in \mathbb{N}$. For every $i \in [n]$, let $p_{i,1}, p_{i,2}, \ldots, p_{i,m_i}$ be finitely many elements of L. Then,
>
> $$\prod_{i=1}^{n} \sum_{k=1}^{m_i} p_{i,k} = \sum_{(k_1,k_2,\ldots,k_n) \in [m_1]\times[m_2]\times\cdots\times[m_n]} \prod_{i=1}^{n} p_{i,k_i}. \tag{116}$$

We can rewrite (116) in a less abstract way as follows:

$$\begin{aligned}&\left(p_{1,1}+p_{1,2}+\cdots+p_{1,m_1}\right)\left(p_{2,1}+p_{2,2}+\cdots+p_{2,m_2}\right)\cdots\left(p_{n,1}+p_{n,2}+\cdots+p_{n,m_n}\right)\\&= p_{1,1}p_{2,1}\cdots p_{n,1} + p_{1,1}p_{2,1}\cdots p_{n-1,1}p_{n,2} + \cdots + p_{1,m_1}p_{2,m_2}\cdots p_{n,m_n},\end{aligned}$$

$\prod_{i\in\mathbb{N}}\left(1-x^{2^i}\right)$ is invertible (indeed, its constant term is 1). However, splitting off the factor for $i=0$ from the product $\prod_{i\in\mathbb{N}}\left(1-x^{2^i}\right)$, we obtain

$$\prod_{i\in\mathbb{N}}\left(1-x^{2^i}\right) = \underbrace{\left(1-x^{2^0}\right)}_{=1-x^1=1-x} \cdot \underbrace{\prod_{i>0}\left(1-x^{2^i}\right)}_{\substack{=\prod_{i\in\mathbb{N}}\left(1-x^{2^{i+1}}\right)\\ \text{(here, we substituted } i+1\\ \text{for } i \text{ in the product)}}} = (1-x)\cdot\prod_{i\in\mathbb{N}}\left(1-x^{2^{i+1}}\right),$$

so that

$$\frac{\prod_{i\in\mathbb{N}}\left(1-x^{2^{i+1}}\right)}{\prod_{i\in\mathbb{N}}\left(1-x^{2^i}\right)} = \frac{1}{1-x}.$$

Hence, $\prod_{i\in\mathbb{N}}\left(1+x^{2^i}\right) = \frac{\prod_{i\in\mathbb{N}}\left(1-x^{2^{i+1}}\right)}{\prod_{i\in\mathbb{N}}\left(1-x^{2^i}\right)} = \frac{1}{1-x}$. So we don't need the telescope principle to justify this equality.

[38] Keep in mind that an empty Cartesian product (i.e., a Cartesian product of 0 sets) is always a 1-element set; its only element is the 0-tuple $()$. Thus, a sum ranging over an empty Cartesian product has exactly 1 addend.

where the right hand side is the sum of all $m_1 m_2 \cdots m_n$ many ways to multiply one addend from each of the factors on the left hand side.

See [Grinbe15, solution to Exercise 6.9] for a formal proof of Proposition 3.11.22. (The idea is to reduce it to the case $n = 2$ by induction, then to use the discrete Fubini rule.)

Let us now move on to product rules for infinite sums and products. First, let us extend Proposition 3.11.22 to a finite product of infinite sums (which are now required to be in $K[[x]]$ in order to have a notion of summability):

Proposition 3.11.23. For every $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \ldots, n\}$.

Let $n \in \mathbb{N}$. For every $i \in [n]$, let $(p_{i,k})_{k \in S_i}$ be a summable family of elements of $K[[x]]$. Then,

$$\prod_{i=1}^{n} \sum_{k \in S_i} p_{i,k} = \sum_{(k_1,k_2,\ldots,k_n) \in S_1 \times S_2 \times \cdots \times S_n} \prod_{i=1}^{n} p_{i,k_i}. \tag{117}$$

In particular, the family $\left(\prod\limits_{i=1}^{n} p_{i,k_i} \right)_{(k_1,k_2,\ldots,k_n) \in S_1 \times S_2 \times \cdots \times S_n}$ is summable.

Proof. Same method as for Proposition 3.11.22, but now using the discrete Fubini rule for infinite sums. □

Proposition 3.11.23 is rather general, but is only concerned with **finite** products. Thus, it cannot be directly used to justify (108), since the product in (108) is infinite. Thus, we need a product rule for infinite products of sums. Such rules are subtle and require particular care: Not only do our sums have to be summable and our product multipliable, but we also must avoid cases like $(1-1)(1-1)(1-1)\cdots$, which would produce non-summable infinite sums when expanded (despite being multipliable). We also need on come clear about what addends we get when we expand our products: For example, when expanding the product

$$(1 + a_0)(1 + a_1)(1 + a_2)(1 + a_3)(1 + a_4)\cdots,$$

we should get addends like $a_0 \cdot 1 \cdot a_2 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1s}}$ or $1 \cdot a_1 \cdot a_2 \cdot 1 \cdot a_4 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1s}}$, but not addends like $a_0 \cdot a_1 \cdot a_2 \cdot a_3 \cdot \cdots$; otherwise, the right hand side of (108) would have to include infinite products of a_i's. To filter out the latter kind of addends, let us define the notion of "essentially finite" sequences or families:

Definition 3.11.24. **(a)** A sequence $(k_1, k_2, k_3, \ldots)$ is said to be *essentially finite* if all but finitely many $i \in \{1, 2, 3, \ldots\}$ satisfy $k_i = 0$.

(b) A family $(k_i)_{i \in I}$ is said to be *essentially finite* if all but finitely many $i \in I$ satisfy $k_i = 0$.

For example, the sequence $(2,4,1,0,0,0,0,\ldots)$ is essentially finite, whereas the sequence $(0,1,0,1,0,1,\ldots)$ (which alternates between 0s and 1s) is not.

Of course, Definition 3.11.24 **(a)** is a particular case of Definition 3.11.24 **(b)**, since a sequence $(k_1,k_2,k_3,\ldots)$ is the same as a family $(k_i)_{i\in\{1,2,3,\ldots\}}$ indexed by the positive integers. We also remark that Definition 3.2.8 **(a)** is a particular case of Definition 3.11.24 **(b)**, since a family of elements of K is one particular type of family.

Now, we can finally state a version of the product rule for infinite products of potentially infinite sums. This will help us derive (108) (even though the sums being multiplied in (108) are finite).

Proposition 3.11.25. Let $S_1,S_2,S_3,\ldots$ be infinitely many sets that all contain the number 0. Set

$$\overline{S}=\{(i,k)\ \mid\ i\in\{1,2,3,\ldots\}\text{ and }k\in S_i\text{ and }k\neq 0\}.$$

For any $i\in\{1,2,3,\ldots\}$ and any $k\in S_i$, let $p_{i,k}$ be an element of $K[[x]]$. Assume that

$$p_{i,0}=1\qquad\text{for any }i\in\{1,2,3,\ldots\}. \tag{118}$$

Assume further that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable. Then, the product $\prod\limits_{i=1}^{\infty}\ \sum\limits_{k\in S_i}p_{i,k}$ is well-defined (i.e., the family $(p_{i,k})_{k\in S_i}$ is summable for each $i\in\{1,2,3,\ldots\}$, and the family $\left(\sum\limits_{k\in S_i}p_{i,k}\right)_{i\in\{1,2,3,\ldots\}}$ is multipliable), and we have

$$\prod_{i=1}^{\infty}\ \sum_{k\in S_i}p_{i,k}=\sum_{\substack{(k_1,k_2,k_3,\ldots)\in S_1\times S_2\times S_3\times\cdots\\ \text{is essentially finite}}}\ \prod_{i=1}^{\infty}p_{i,k_i}. \tag{119}$$

In particular, the family $\left(\prod\limits_{i=1}^{\infty}p_{i,k_i}\right)_{(k_1,k_2,k_3,\ldots)\in S_1\times S_2\times S_3\times\cdots\text{ is essentially finite}}$ is summable.

Note that the assumption (118) in Proposition 3.11.25 ensures that each of the sums being multiplied contains an addend that equals 1 (and that this addend is indexed by 0; but this clearly does not restrict the generality of the proposition). The equality (119) shows how we can expand an infinite product of such sums. The result is a huge sum of products (the right hand side of (119)); each of these products is formed by picking an addend from each sum $\sum\limits_{k\in S_i}p_{i,k}$ (just as in the finite case). The picking has to be done in such a way that the addend 1 gets picked from all but finitely many of our sums (for instance, when expanding $(1+x^1)(1+x^2)(1+x^3)\cdots$, we don't want to pick the x^i's from all sums, as this would lead to $x^1x^2x^3\cdots=$"x^∞"); this is why the sum on the right hand side of (119) is ranging only over the **essentially finite** sequences $(k_1, k_2, k_3, \ldots) \in S_1 \times S_2 \times S_3 \times \cdots$. Finally, the condition that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ be summable is our way of ruling out cases like $(1-1)(1-1)(1-1)\cdots$, which cannot be expanded. Proposition 3.11.25 is not the most general version of the product rule, but it is sufficient for many of our needs (and we will see some more general versions below).

The rest of this subsection should probably be skipped at first reading – it is largely a succession of technical arguments about finite and infinite sets in service of making rigorous what is already intuitively clear.

Before we sketch a proof of Proposition 3.11.25, let us show how (108) can be derived from it:

Proof of (108) using Proposition 3.11.25. Let $(a_0, a_1, a_2, \ldots) = (a_n)_{n\in\mathbb{N}}$ be a summable sequence of FPSs in $K[[x]]$. We must prove the equality (108).

Set $S_i = \{0,1\}$ for each $i \in \{1,2,3,\ldots\}$. Thus,

$$S_1 \times S_2 \times S_3 \times \cdots = \{0,1\} \times \{0,1\} \times \{0,1\} \times \cdots = \{0,1\}^{\infty}.$$

Define the set $\overline{S}$ as in Proposition 3.11.25. Then, $\overline{S} = \{(1,1),\ (2,1),\ (3,1),\ \ldots\}$. Now, set $p_{i,k} = a_{i-1}^k$ for each $i \in \{1,2,3,\ldots\}$ and each $k \in \{0,1\}$. Thus, the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable[39], and the statement (118) holds as well (indeed, we have $p_{i,0} = a_{i-1}^0 = 1$ for any $i \in \{1,2,3,\ldots\}$). Hence, Proposition 3.11.25 can be applied.

Moreover, for each $i \in \{1,2,3,\ldots\}$, we have $S_i = \{0,1\}$. Thus, for each $i \in \{1,2,3,\ldots\}$, we have

$$\sum_{k\in S_i} p_{i,k} = \sum_{k\in\{0,1\}} p_{i,k} = \underbrace{p_{i,0}}_{=a_{i-1}^0=1} + \underbrace{p_{i,1}}_{=a_{i-1}^1=a_{i-1}} = 1 + a_{i-1}.$$

Hence,

$$\prod_{i=1}^{\infty} \underbrace{\sum_{k\in S_i} p_{i,k}}_{=1+a_{i-1}} = \prod_{i=1}^{\infty} (1 + a_{i-1}) = \prod_{i\in\mathbb{N}} (1 + a_i)$$

[39] Indeed, this family can be rewritten as $(p_{1,1}, p_{2,1}, p_{3,1}, \ldots) = (a_0^1, a_1^1, a_2^1, \ldots) = (a_0, a_1, a_2, \ldots)$, but we have assumed that the latter family is summable.

(here, we have substituted i for $i-1$ in the product). Thus,

$$\begin{aligned}
\prod_{i\in\mathbb{N}}(1+a_i) &= \prod_{i=1}^{\infty}\ \sum_{k\in S_i} p_{i,k} \\
&= \underbrace{\sum_{\substack{(k_1,k_2,k_3,\ldots)\in S_1\times S_2\times S_3\times\cdots \\ \text{is essentially finite}}}}_{\substack{=\sum\limits_{\substack{(k_1,k_2,k_3,\ldots)\in\{0,1\}^\infty \\ \text{is essentially finite}}} \\ (\text{since } S_1\times S_2\times S_3\times\cdots=\{0,1\}^\infty)}}\ \prod_{i=1}^{\infty}\underbrace{p_{i,k_i}}_{=a_{i-1}^{k_i}} \qquad \text{(by (119))} \\
&= \sum_{\substack{(k_1,k_2,k_3,\ldots)\in\{0,1\}^\infty \\ \text{is essentially finite}}}\ \prod_{i=1}^{\infty} a_{i-1}^{k_i} = \sum_{\substack{(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty \\ \text{is essentially finite}}}\ \underbrace{\prod_{i=1}^{\infty} a_{i-1}^{k_{i-1}}}_{=\prod\limits_{i\in\mathbb{N}} a_i^{k_i}} \\
&\qquad\left(\begin{array}{c}\text{here, we have renamed the summation} \\ \text{index } (k_1,k_2,k_3,\ldots) \text{ as } (k_0,k_1,k_2,\ldots)\end{array}\right) \\
&= \sum_{\substack{(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty \\ \text{is essentially finite}}}\ \prod_{i\in\mathbb{N}} a_i^{k_i}. \qquad (120)
\end{aligned}$$

Now, an essentially finite sequence $(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty$ is just an infinite sequence of 0s and 1s that contains only finitely many 1s. Thus, such a sequence is uniquely determined by the positions of the 1s in it, and these positions form a finite set, so they can be uniquely labeled as $i_1,i_2,\ldots,i_k$ with $i_1<i_2<\cdots<i_k$. To put this more formally: There is a bijection

$$\begin{aligned}
&\text{from } \left\{\text{essentially finite sequences } (k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty\right\} \\
&\text{to } \{\text{finite lists } (i_1,i_2,\ldots,i_k) \text{ of nonnegative integers such that } i_1<i_2<\cdots<i_k\}
\end{aligned}$$

that sends each sequence $(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty$ to the list of all $i\in\mathbb{N}$ satisfying $k_i=1$ (written in increasing order). Furthermore, if this bijection sends an essentially finite sequence $(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty$ to a finite list $(i_1,i_2,\ldots,i_k)$, then

$$\begin{aligned}
\prod_{i\in\mathbb{N}} a_i^{k_i} &= \left(\prod_{\substack{i\in\mathbb{N};\\ k_i=0}}\underbrace{a_i^{k_i}}_{=a_i^0=1}\right)\left(\prod_{\substack{i\in\mathbb{N};\\ k_i=1}}\underbrace{a_i^{k_i}}_{=a_i^1=a_i}\right) \qquad (\text{since each } k_i \text{ is either 0 or 1}) \\
&= \underbrace{\left(\prod_{\substack{i\in\mathbb{N};\\ k_i=0}} 1\right)}_{=1}\left(\prod_{\substack{i\in\mathbb{N};\\ k_i=1}} a_i\right) = \prod_{\substack{i\in\mathbb{N};\\ k_i=1}} a_i = a_{i_1}a_{i_2}\cdots a_{i_k}
\end{aligned}$$

(since $(i_1, i_2, \ldots, i_k)$ is the list of all $i \in \mathbb{N}$ satisfying $k_i = 1$). Thus, we can use this bijection to re-index the sum on the right hand side of (120); we obtain

$$\sum_{\substack{(k_0,k_1,k_2,\ldots)\in\{0,1\}^\infty \\ \text{is essentially finite}}} \prod_{i\in\mathbb{N}} a_i^{k_i} = \sum_{i_1<i_2<\cdots<i_k} a_{i_1}a_{i_2}\cdots a_{i_k}.$$

Thus, (120) rewrites as

$$\prod_{i\in\mathbb{N}} (1+a_i) = \sum_{i_1<i_2<\cdots<i_k} a_{i_1}a_{i_2}\cdots a_{i_k}.$$

This proves (108). □

We note that (108) can be rewritten as

$$\prod_{i\in\mathbb{N}} (1+a_i) = \sum_{\substack{J \text{ is a finite} \\ \text{subset of } \mathbb{N}}} \prod_{i\in J} a_i. \tag{121}$$

Indeed, the right hand side of this equality is precisely the right hand side of (108).

We will prove Proposition 3.11.25 soon. First, however, let us generalize Proposition 3.11.25 to products indexed by arbitrary sets instead of $\{1, 2, 3, \ldots\}$:

Proposition 3.11.26. Let I be a set. For any $i \in I$, let S_i be a set that contains the number 0. Set

$$\overline{S} = \{(i,k) \mid i \in I \text{ and } k \in S_i \text{ and } k \neq 0\}.$$

For any $i \in I$ and any $k \in S_i$, let $p_{i,k}$ be an element of $K[[x]]$. Assume that

$$p_{i,0} = 1 \qquad \text{for any } i \in I. \tag{122}$$

Assume further that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable. Then, the product $\prod\limits_{i\in I} \sum\limits_{k\in S_i} p_{i,k}$ is well-defined (i.e., the family $(p_{i,k})_{k\in S_i}$ is summable for each $i \in I$, and the family $\left(\sum\limits_{k\in S_i} p_{i,k}\right)_{i\in I}$ is multipliable), and we have

$$\prod_{i\in I} \sum_{k\in S_i} p_{i,k} = \sum_{\substack{(k_i)_{i\in I}\in\prod\limits_{i\in I} S_i \\ \text{is essentially finite}}} \prod_{i\in I} p_{i,k_i}. \tag{123}$$

In particular, the family $\left(\prod\limits_{i\in I} p_{i,k_i}\right)_{(k_i)_{i\in I}\in\prod\limits_{i\in I} S_i \text{ is essentially finite}}$ is summable.

Clearly, Proposition 3.11.25 is the particular case of Proposition 3.11.26 for $I = \{1, 2, 3, \ldots\}$. The proof of Proposition 3.11.26 is a long-winded reduction to the finite case; nothing substantial is going on in it. Thus, I recommend skipping it unless specifically interested. For the sake of convenience, before proving Proposition 3.11.26, let me restate Proposition 3.11.23 in a form that makes it particularly easy to use:

Proposition 3.11.27. Let N be a finite set. For any $i \in N$, let $(p_{i,k})_{k \in S_i}$ be a summable family of elements of $K[[x]]$. Then,

$$\prod_{i \in N} \sum_{k \in S_i} p_{i,k} = \sum_{(k_i)_{i \in N} \in \prod_{i \in N} S_i} \prod_{i \in N} p_{i,k_i}. \qquad (124)$$

In particular, the family $\left(\prod_{i \in N} p_{i,k_i} \right)_{(k_i)_{i \in N} \in \prod_{i \in N} S_i}$ is summable.

Proof of Proposition 3.11.27. This is just Proposition 3.11.23, with the indexing set $\{1, 2, \ldots, n\}$ replaced by N. It can be proved by reindexing the products (or directly by induction on $|N|$). □

Let me furthermore state an infinite version of Lemma 3.11.9, which will be used in the proof of Proposition 3.11.26 given below:

Lemma 3.11.28. Let $a \in K[[x]]$ be an FPS. Let $(f_i)_{i \in J} \in K[[x]]^J$ be a summable family of FPSs. Let $n \in \mathbb{N}$. Assume that each $i \in J$ satisfies

$$[x^m](f_i) = 0 \qquad \text{for each } m \in \{0, 1, \ldots, n\}. \qquad (125)$$

Then,

$$[x^m]\left(a \prod_{i \in J} (1 + f_i) \right) = [x^m]\, a \qquad \text{for each } m \in \{0, 1, \ldots, n\}.$$

Proof of Lemma 3.11.28 (sketched). The idea here is to argue that the first $n+1$ coefficients of $a \prod_{i \in J} (1 + f_i)$ agree with those of $a \prod_{i \in M} (1 + f_i)$ for some finite subset M of J. Then, apply Lemma 3.11.9 to this subset M. The details of this argument can be found in Section B.2. □

With this lemma proved, we have all necessary prerequisites for the proof of Proposition 3.11.26. The proof, however, is rather long due to the bookkeeping required, and therefore has been banished to the appendix (Section B.2, to be specific).

We notice that Proposition 3.11.26 (and thus also Proposition 3.11.25) can be generalized slightly by lifting the requirement that all sets S_i contain 0 (this means that the sums being multiplied no longer need to contain 1 as an addend). See Exercise A.2.11.5 for this generalization. This lets us expand products such as $x\left(1+x^1\right)\left(1+x^2\right)\left(1+x^3\right)\cdots$ (but of course, we could just as well expand this particular product by splitting off the x factor and applying Proposition 3.11.25).

3.11.4. Another example

As another bit of practice with infinite products of FPSs, let us prove the following identity by Euler ([Euler48, §326]):

> **Proposition 3.11.29** (Euler)**.** We have
> $$\prod_{i>0}\left(1-x^{2i-1}\right)^{-1}=\prod_{k>0}\left(1+x^k\right).$$

Proof. For each $k>0$, we have $1+x^k=\dfrac{1-x^{2k}}{1-x^k}$ (since $1-x^{2k}=1-\left(x^k\right)^2=\left(1-x^k\right)\left(1+x^k\right)$). Thus,

$$\begin{aligned}\prod_{k>0}\underbrace{\left(1+x^k\right)}_{=\dfrac{1-x^{2k}}{1-x^k}}&=\prod_{k>0}\frac{1-x^{2k}}{1-x^k}=\frac{\prod\limits_{k>0}\left(1-x^{2k}\right)}{\prod\limits_{k>0}\left(1-x^k\right)}\\&=\frac{\left(1-x^2\right)\left(1-x^4\right)\left(1-x^6\right)\left(1-x^8\right)\cdots}{\left(1-x^1\right)\left(1-x^2\right)\left(1-x^3\right)\left(1-x^4\right)\cdots}\\&=\frac{1}{\left(1-x^1\right)\left(1-x^3\right)\left(1-x^5\right)\cdots}\\&\qquad\left(\begin{array}{c}\text{since all }1-x^i\text{ factors with }i\text{ even}\\\text{cancel out}\end{array}\right)\\&=\left(1-x^1\right)^{-1}\left(1-x^3\right)^{-1}\left(1-x^5\right)^{-1}\cdots=\prod_{i>0}\left(1-x^{2i-1}\right)^{-1}.\end{aligned}$$

This proves Proposition 3.11.29. □

Let us try to interpret Proposition 3.11.29 combinatorially, by expanding both sides.

First, we use (108) to expand the right hand side:

$$\begin{aligned}\prod_{k>0}\left(1+x^k\right) &= \left(1+x^1\right)\left(1+x^2\right)\left(1+x^3\right)\left(1+x^4\right)\cdots \\ &= \sum_{\substack{i_1,i_2,\ldots,i_k\in\{1,2,3,\ldots\};\\ i_1<i_2<\cdots<i_k}} x^{i_1}x^{i_2}\cdots x^{i_k} \\ &= \sum_{n\in\mathbb{N}} d_n x^n,\end{aligned}$$

where d_n is the # of all strictly increasing tuples $(i_1 < i_2 < \cdots < i_k)$ of positive integers such that $n = i_1 + i_2 + \cdots + i_k$. We can rewrite this definition as follows: d_n is the # of ways to write n as a sum of distinct positive integers, with no regard for the order[40].

Now the left hand side: Since $(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots$, we have

$$\begin{aligned}&\prod_{i>0}\left(1-x^{2i-1}\right)^{-1} \\ &= \prod_{i>0}\left(1+x^{2i-1}+\left(x^{2i-1}\right)^2+\left(x^{2i-1}\right)^3+\cdots\right) \\ &= \prod_{i>0}\left(1+x^{2i-1}+x^{2(2i-1)}+x^{3(2i-1)}+\cdots\right) \\ &= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \\ \text{is essentially finite}}} \underbrace{x^{u_1\cdot 1}x^{u_2\cdot 3}x^{u_3\cdot 5}\cdots}_{=x^{u_1\cdot 1+u_2\cdot 3+u_3\cdot 5+\cdots}} \qquad \text{(by Proposition 3.11.25)} \\ &= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \\ \text{is essentially finite}}} x^{u_1\cdot 1+u_2\cdot 3+u_3\cdot 5+\cdots} \\ &= \sum_{n\in\mathbb{N}} o_n x^n,\end{aligned}$$

where o_n is the # of all essentially finite sequences $(u_1, u_2, u_3, \ldots) \in \mathbb{N}^\infty$ such that $u_1 \cdot 1 + u_2 \cdot 3 + u_3 \cdot 5 + \cdots = n$. I claim that o_n is the # of ways to write n as a sum of (not necessarily distinct) odd positive integers, without regard to the order. (Why? Because if we write n as a sum of u_1 many 1s, u_2 many 3s, u_3 many 5s and so on, then $u_1 \cdot 1 + u_2 \cdot 3 + u_3 \cdot 5 + \cdots = n$, and vice versa.)

Proposition 3.11.29 tells us that

$$\sum_{n\in\mathbb{N}} d_n x^n = \prod_{k>0}\left(1+x^k\right) = \prod_{i>0}\left(1-x^{2i-1}\right)^{-1} = \sum_{n\in\mathbb{N}} o_n x^n.$$

Therefore, $d_n = o_n$ for each $n \in \mathbb{N}$. Thus, we have proven the following purely combinatorial statement:

[40] "No regard for the order" means that, for example, $3+4+1$ and $1+3+4$ count as the same way of writing 8 as a sum of distinct integers.

Theorem 3.11.30 (Euler)**.** Let $n \in \mathbb{N}$. Then, $d_n = o_n$, where

- d_n is the # of ways to write n as a sum of distinct positive integers, without regard to the order;
- o_n is the # of ways to write n as a sum of (not necessarily distinct) odd positive integers, without regard to the order.

Example 3.11.31. Let $n = 6$. Then, $d_n = 4$, because the ways to write $n = 6$ as a sum of distinct positive integers are

$$6 = 6 = 1 + 5 = 2 + 4 = 1 + 2 + 3.$$

On the other hand, $o_n = 4$, because the ways to write $n = 6$ as a sum of odd positive integers are

$$6 = 1 + 5 = 3 + 3 = 3 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1 + 1.$$

We will soon learn a bijective proof of Theorem 3.11.30 (see the Second proof of Theorem 4.1.13 below).

3.11.5. Infinite products and substitution

Proposition 3.5.4 **(h)** has an analogue for products instead of sums:

Proposition 3.11.32. If $(f_i)_{i \in I} \in K[[x]]^I$ is a multipliable family of FPSs, and if $g \in K[[x]]$ is an FPS satisfying $[x^0]\, g = 0$, then the family $(f_i \circ g)_{i \in I} \in K[[x]]^I$ is multipliable as well and we have $\left(\prod\limits_{i \in I} f_i \right) \circ g = \prod\limits_{i \in I} (f_i \circ g)$.

Proof of Proposition 3.11.32 (sketched). See Section B.2. □

3.12. The generating function of a weighted set

So far, we have built a theory of FPSs, but their application to combinatorics (via generating functions) was a trick. I will now explain one way to make this latter trick into a theory as well. This theory isn't magic – it is just rewriting our arguments in a more uniform way; but it makes some of them easier to manage.

I will briefly survey this theory (as it isn't a focus of this course), following Fink's introduction [Fink17, §3.3–§3.4] (but speaking of *finite-type weighted sets* where Fink speaks of "combinatorial classes").

3.12.1. The theory

Definition 3.12.1. (a) A *weighted set* is a set A equipped with a function $w : A \rightarrow \mathbb{N}$, which is called the *weight function* of this weighted set. For each $a \in A$, the value $w(a)$ is denoted $|a|$ and is called the *weight* of a (in our weighted set).

Usually, instead of explicitly specifying the weight function w as a function, we will simply specify the weight $|a|$ for each $a \in A$. The weighted set consisting of the set A and the weight function w will be called (A, w) or simply A when the weight function w is clear from the context.

(b) A weighted set A is said to be *finite-type* if for each $n \in \mathbb{N}$, there are only finitely many $a \in A$ having weight $|a| = n$.

(c) If A is a finite-type weighted set, then the *weight generating function* of A is defined to be the FPS

$$\sum_{a \in A} x^{|a|} = \sum_{n \in \mathbb{N}} (\text{\# of } a \in A \text{ having weight } n) \cdot x^n \in \mathbb{Z}[[x]].$$

This FPS is denoted by $\overline{A}$.

(d) An *isomorphism* between two weighted sets A and B means a bijection $\rho : A \rightarrow B$ that preserves the weight (i.e., each $a \in A$ satisfies $|\rho(a)| = |a|$).

(e) We say that two weighted sets A and B are *isomorphic* (this is written $A \cong B$) if there exists an isomorphism between A and B.

Example 3.12.2. Let B be the weighted set of all *binary strings*, i.e., finite tuples consisting of 0s and 1s. Thus,

$$B = \{(),\ (0),\ (1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (0,0,0),\ (0,0,1),\ \ldots\}.$$

The weight of a k-tuple is defined to be k. This weighted set B is finite-type, since for each $k \in \mathbb{N}$, there are only finitely many binary strings of length k (namely, there are 2^k such strings). The weight generating function of B is

$$\begin{aligned}\overline{B} &= \sum_{n \in \mathbb{N}} \underbrace{(\text{\# of } a \in B \text{ having weight } n)}_{\substack{=(\text{\# of binary strings of length } n) \\ =2^n}} \cdot x^n \\ &= \sum_{n \in \mathbb{N}} 2^n x^n = \frac{1}{1-2x}.\end{aligned}$$

Proposition 3.12.3. Let A and B be two isomorphic finite-type weighted sets. Then, $\overline{A} = \overline{B}$.

Proof. This is almost trivial: The weighted sets A and B are isomorphic; thus, there exists an isomorphism $\rho : A \rightarrow B$. Consider this ρ. Then, ρ is a bijection and preserves the weight (since ρ is an isomorphism of weighted sets). The latter property says that we have

$$|\rho(a)| = |a| \qquad \text{for each } a \in A. \tag{126}$$

Now, the definition of $\overline{B}$ yields

$$\overline{B} = \sum_{b\in B} x^{|b|} = \sum_{a\in A} \underbrace{x^{|\rho(a)|}}_{\substack{=x^{|a|} \\ \text{(by (126))}}} \qquad \left(\begin{array}{c}\text{here, we have substituted } \rho(a) \text{ for } b \\ \text{in the sum, since } \rho \text{ is a bijection}\end{array}\right)$$
$$= \sum_{a\in A} x^{|a|}.$$

Comparing this with

$$\overline{A} = \sum_{a\in A} x^{|a|} \qquad \left(\text{by the definition of } \overline{A}\right),$$

we obtain $\overline{A} = \overline{B}$. This proves Proposition 3.12.3. □

Note that Proposition 3.12.3 has a converse: If $\overline{A} = \overline{B}$, then $A \cong B$.

Recall that the *disjoint union* of two sets A and B is "the union of A and B where we pretend that A and B are disjoint even if they aren't". Formally, it is defined as the set $(\{0\} \times A) \cup (\{1\} \times B)$, but we think of the elements $(0, a)$ of this set as copies of the respective elements $a \in A$, and we think of the elements $(1, b)$ of this set as copies of the respective elements $b \in B$. If A and B are two finite sets, then their disjoint union always has size $|A| + |B|$.

Definition 3.12.4. Let A and B be two finite-type weighted sets. Then, the weighted set $A + B$ is defined to be the disjoint union of A and B, with the weight function inherited from A and B (meaning that each element of A has the same weight that it had in A, and each element of B has the same weight that it had in B). Formally speaking, this means that $A + B$ is the set $(\{0\} \times A) \cup (\{1\} \times B)$, with the weight function given by

$$|(0, a)| = |a| \qquad \text{for each } a \in A \tag{127}$$

and

$$|(1, b)| = |b| \qquad \text{for each } b \in B. \tag{128}$$

Proposition 3.12.5. Let A and B be two finite-type weighted sets. Then, $A + B$ is finite-type, too, and satisfies $\overline{A + B} = \overline{A} + \overline{B}$.

Proof. The formal definition of $A + B$ says that $A + B = (\{0\} \times A) \cup (\{1\} \times B)$. Thus, the set $A + B$ is the union of the two disjoint sets $\{0\} \times A$ and $\{1\} \times B$ (indeed, these two sets are clearly disjoint, since $0 \neq 1$).

Let us first check that $A+B$ is finite-type.

For each $n \in \mathbb{N}$, there are only finitely many $a \in A$ having weight $|a| = n$ (since A is finite-type), and there are only finitely many $b \in B$ having weight $|b| = n$ (since B is finite-type). Hence, there are only finitely many $c \in A+B$ having weight $|c| = n$ (because any such c either has the form $(0,a)$ for some $a \in A$ having weight $|a| = n$, or has the form $(1,b)$ for some $b \in B$ having weight $|b| = n$). In other words, the weighted set $A+B$ is finite-type.

Let us now check that $\overline{A+B} = \overline{A} + \overline{B}$. Indeed, the definition of $\overline{A+B}$ yields

$$\begin{aligned}
\overline{A+B} &= \sum_{c\in A+B} x^{|c|} \\
&= \underbrace{\sum_{c\in\{0\}\times A} x^{|c|}}_{\substack{=\sum_{a\in A} x^{|(0,a)|} \\ \text{(here, we have substituted } (0,a) \\ \text{for } c \text{ in the sum, since the} \\ \text{map } A\to\{0\}\times A,\ a\mapsto(0,a) \text{ is a bijection)}}} + \underbrace{\sum_{c\in\{1\}\times B} x^{|c|}}_{\substack{=\sum_{b\in B} x^{|(1,b)|} \\ \text{(here, we have substituted } (1,b) \\ \text{for } c \text{ in the sum, since the} \\ \text{map } B\to\{1\}\times B,\ b\mapsto(1,b) \text{ is a bijection)}}} \\
&\qquad \left(\begin{array}{c}\text{here, we have split the sum, since the}\\ \text{set } A+B \text{ is the union of the two disjoint}\\ \text{sets } \{0\}\times A \text{ and } \{1\}\times B\end{array}\right) \\
&= \sum_{a\in A} \underbrace{x^{|(0,a)|}}_{\substack{=x^{|a|}\\ \text{(by (127))}}} + \sum_{b\in B} \underbrace{x^{|(1,b)|}}_{\substack{=x^{|b|}\\ \text{(by (128))}}} = \underbrace{\sum_{a\in A} x^{|a|}}_{=\overline{A}} + \underbrace{\sum_{b\in B} x^{|b|}}_{=\overline{B}} = \overline{A} + \overline{B}.
\end{aligned}$$

Thus, the proof of Proposition 3.12.5 is complete. □

We can easily extend Definition 3.12.4 and Proposition 3.12.5 to disjoint unions of any number (even infinite) of weighted sets. (However, in the case of infinite disjoint unions, we need to require the disjoint union to be finite-type in order for Proposition 3.12.5 to make sense.)

Definition 3.12.6. Let A and B be two weighted sets. Then, the weighted set $A \times B$ is defined to be the Cartesian product of A and B (that is, the set $\{(a,b) \mid a \in A \text{ and } b \in B\}$), with the weight function defined as follows: For any $(a,b) \in A \times B$, we set

$$|(a,b)| = |a| + |b| . \qquad (129)$$

Proposition 3.12.7. Let A and B be two finite-type weighted sets. Then, $A \times B$ is finite-type, too, and satisfies $\overline{A \times B} = \overline{A} \cdot \overline{B}$.

Proof of Proposition 3.12.7 (sketched). The proof that $A \times B$ is finite-type is left to the reader.

The definition of $\overline{A \times B}$ yields

$$\begin{aligned}
\overline{A \times B} &= \sum_{(a,b) \in A \times B} \underbrace{x^{|(a,b)|}}_{\substack{= x^{|a|+|b|} \\ \text{(by (129))}}} \qquad \left(\begin{array}{c} \text{since all elements of } A \times B \text{ have} \\ \text{the form } (a,b) \text{ for some } a \text{ and } b \end{array} \right) \\
&= \sum_{(a,b) \in A \times B} \underbrace{x^{|a|+|b|}}_{= x^{|a|} \cdot x^{|b|}} \\
&= \sum_{(a,b) \in A \times B} x^{|a|} \cdot x^{|b|} = \underbrace{\left(\sum_{a \in A} x^{|a|} \right)}_{= \overline{A}} \underbrace{\left(\sum_{b \in B} x^{|b|} \right)}_{= \overline{B}} = \overline{A} \cdot \overline{B}.
\end{aligned}$$

The proof of Proposition 3.12.7 is thus complete. □

We can easily extend Definition 3.12.6 and Proposition 3.12.7 to Cartesian products of k weighted sets. In particular, we obtain Cartesian powers when we multiply k copies of the same weighted set:

Definition 3.12.8. Let A be a weighted set. Then, A^k (for $k \in \mathbb{N}$) means the weighted set $\underbrace{A \times A \times \cdots \times A}_{k \text{ times}}$.

Proposition 3.12.9. Let A be a finite-type weighted set. Let $k \in \mathbb{N}$. Then, A^k is finite-type, too, and satisfies $\overline{A^k} = \overline{A}^k$.

Note that the 0-th Cartesian power A^0 of a weighted set A always consists of a single element – namely, the empty 0-tuple $()$, which has weight 0.

3.12.2. Examples

Now, let us use this theory to revisit some of the things we have already counted:

- Fix $k \in \mathbb{N}$, and let

$$\begin{aligned}
C_k &= \{\text{compositions of length } k\} \\
&= \{(a_1, a_2, \ldots, a_k) \mid a_1, a_2, \ldots, a_k \text{ are positive integers}\} \\
&= \mathbb{P}^k \qquad (\text{where } \mathbb{P} = \{1, 2, 3, \ldots\}).
\end{aligned}$$

  This becomes a finite-type weighted set if we set $|(a_1, a_2, \ldots, a_k)| = a_1 + a_2 + \cdots + a_k$ for every $(a_1, a_2, \ldots, a_k) \in C_k$. What is its weight generating function $\overline{C_k}$? We can turn $\mathbb{P}$ itself into a weighted set, by defining the weight of a positive integer n by $|n| = n$. Then, $C_k = \mathbb{P}^k$ not just as sets, but as weighted sets. Hence,

$$\begin{aligned}
\overline{C_k} = \overline{\mathbb{P}^k} = \overline{\mathbb{P}}^k & \qquad \text{(by Proposition 3.12.9)} \\
= \left(x^1 + x^2 + x^3 + \cdots\right)^k & \qquad \left(\text{since } \overline{\mathbb{P}} = x^1 + x^2 + x^3 + \cdots\right) \\
= \left(\frac{x}{1-x}\right)^k & \qquad \left(\text{since } x^1 + x^2 + x^3 + \cdots = \frac{x}{1-x}\right).
\end{aligned}$$

This recovers the equality (92).

- Recall the notion of Dyck paths (as defined in Example 2 in Section 3.1), as well as the Catalan numbers $c_0, c_1, c_2, \ldots$ (defined in the same place). Let

$$D = \{\text{Dyck paths from } (0,0) \text{ to } (2n,0) \text{ for some } n \in \mathbb{N}\}.$$

This set D becomes a finite-type weighted set if we set

$$|P| = n \qquad \text{whenever } P \text{ is a Dyck path from } (0,0) \text{ to } (2n,0).$$

Thus,

$$\overline{D} = \sum_{n\in\mathbb{N}} \underbrace{(\#\text{ of Dyck paths from } (0,0) \text{ to } (2n,0))}_{=c_n} x^n = \sum_{n\in\mathbb{N}} c_n x^n.$$

This is the generating function we called $C(x)$ in Example 2 of Section 3.1.

Recall that there is only one Dyck path from $(0,0)$ to $(0,0)$, namely the trivial path. All the other Dyck paths in D are nontrivial. We let

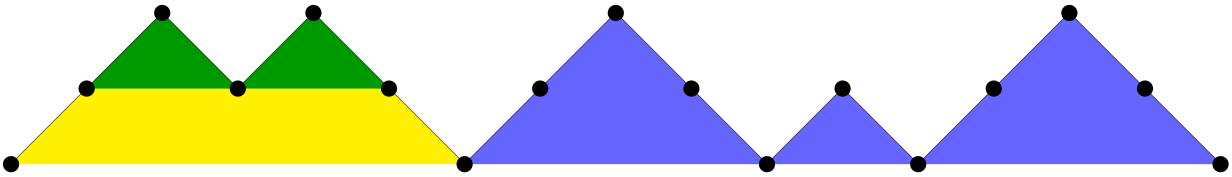
$$\begin{aligned}
D_{\text{triv}} &= \{\text{trivial Dyck paths in } D\} \qquad \text{and} \\
D_{\text{non}} &= \{\text{nontrivial Dyck paths in } D\}.
\end{aligned}$$

These two sets D_{triv} and D_{non} are subsets of D, and thus are weighted sets themselves (we define their weight functions by restricting the one of D). The set D_{triv} consists of a single Dyck path, which has weight 0; thus, its weight generating function is

$$\overline{D_{\text{triv}}} = x^0 = 1.$$

In Example 2 of Section 3.1, we have seen that any nontrivial Dyck path π has the following structure:[41]

[41] The colors are referring to the following picture:



- a NE-step,
- followed by a (diagonally shifted) Dyck path (drawn in green),
- followed by a SE-step,
- followed by another (horizontally shifted) Dyck path (drawn in purple).

If we denote the green Dyck path by α and the purple Dyck path by β, then we thus obtain a bijection

$$\begin{aligned} D_{\text{non}} &\to D \times D, \\ \pi &\mapsto (\alpha, \beta) . \end{aligned}$$

Alas, this bijection is not an isomorphism of weighted sets, since it fails to preserve the weight. Indeed, $|(\alpha, \beta)| = |\alpha| + |\beta| = |\pi| - 1 \neq |\pi|$.

Fortunately, we can fix this rather easily. Define a weighted set

$$X := \{1\} \qquad \text{with } |1| = 1.$$

This is a one-element set, so the only real difference between the weighted sets $X \times D \times D$ and $D \times D$ is in the weights. Indeed, the sets $D \times D$ and $X \times D \times D$ are in bijection (any pair $(\alpha, \beta) \in D \times D$ corresponds to the triple $(1, \alpha, \beta) \in X \times D \times D$), but the weights of corresponding elements differ by 1 (namely, $|(1, \alpha, \beta)| = \underbrace{|1|}_{=1} + \underbrace{|\alpha| + |\beta|}_{=|(\alpha,\beta)|} = 1 + |(\alpha, \beta)|$).

Thus, by replacing $D \times D$ by $X \times D \times D$, we can fix the degrees in our above bijection. We thus obtain a bijection

$$\begin{aligned} D_{\text{non}} &\to X \times D \times D, \\ \pi &\mapsto (1, \alpha, \beta) \end{aligned}$$

that does preserve the weight. This bijection is thus an isomorphism of weighted sets. Hence, $D_{\text{non}} \cong X \times D \times D$.

Each Dyck path is either trivial or nontrivial. Hence,

$$D \cong D_{\text{triv}} + \underbrace{D_{\text{non}}}_{\cong X \times D \times D} \cong D_{\text{triv}} + X \times D \times D,$$

so that

$$\begin{aligned} \overline{D} &= \overline{D_{\text{triv}} + X \times D \times D} && \text{(by Proposition 3.12.3)} \\ &= \underbrace{\overline{D_{\text{triv}}}}_{=1} + \underbrace{\overline{X}}_{=x} \cdot \underbrace{\overline{D} \cdot \overline{D}}_{=\overline{D}^2} && \text{(by Proposition 3.12.5 and Proposition 3.12.7)} \\ &= 1 + x \cdot \overline{D}^2 . \end{aligned}$$

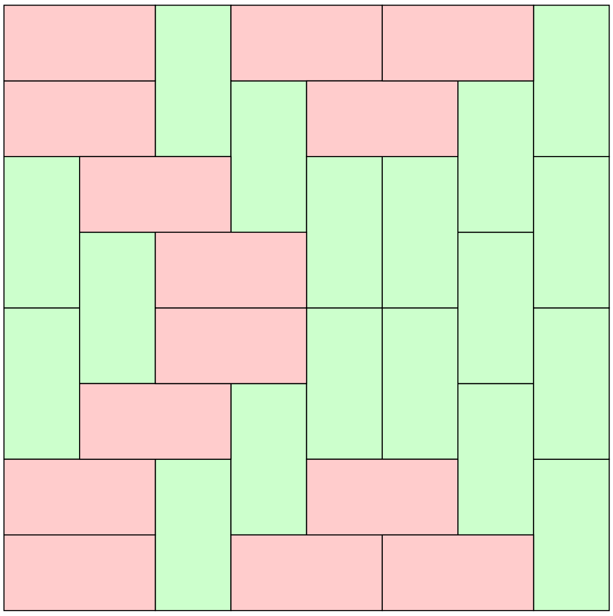
This is precisely the quadratic equation $C(x) = 1 + x(C(x))^2$ that we obtained in Section 3.1. This time, we obtained it from a more abstract technique.

3.12.3. Domino tilings

Let us now apply the theory of weight generating functions to something we haven't already counted. Namely, we shall count the domino tilings of a rectangle. Informally, these are defined as follows:

- For any $n, m \in \mathbb{N}$, we let $R_{n,m}$ be a rectangle with width n and height m.
- A *domino* means a rectangle that is an $R_{1,2}$ or an $R_{2,1}$.
- A *domino tiling* of a shape S means a tiling of S by dominos (i.e., a set of dominos that cover S and whose interiors don't intersect).

For example, here is a domino tiling of $R_{8,8}$:



(note that the colors are purely ornamental here: we are coloring a domino pink if it lies horizontally and green if it stands vertically, for the sake of convenience).

This sounds geometric, but actually is a combinatorial object hiding behind geometric language. Our rectangles and dominos all align to a square grid. Thus, rectangles can be modeled simply as finite sets of grid squares, and dominos are unordered pairs of adjacent grid squares. This allows us to redefine domino tilings combinatorially as follows:

Definition 3.12.10. **(a)** A *shape* means a subset of $\mathbb{Z}^2$.

We draw each $(i,j) \in \mathbb{Z}^2$ as a unit square with center at the point (i,j) (in Cartesian coordinates); thus, a shape can be drawn as a cluster of squares.

(b) For any $n, m \in \mathbb{N}$, the shape $R_{n,m}$ (called the *$n \times m$-rectangle*) is defined to be

$$\{1,2,\ldots,n\} \times \{1,2,\ldots,m\} = \left\{(i,j) \in \mathbb{Z}^2 \mid 1 \leq i \leq n \text{ and } 1 \leq j \leq m\right\}.$$

(c) A *domino* means a size-2 shape of the form

$$\begin{array}{ll} \{(i,j)\,,\ (i+1,j)\} \text{ (a "\textit{horizontal domino}")} & \text{or} \\ \{(i,j)\,,\ (i,j+1)\} \text{ (a "\textit{vertical domino}")} & \end{array}$$

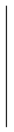
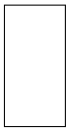
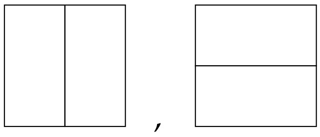
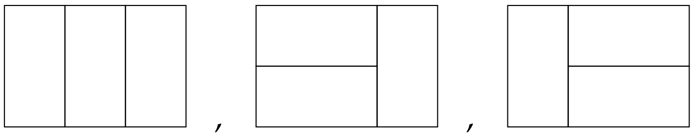
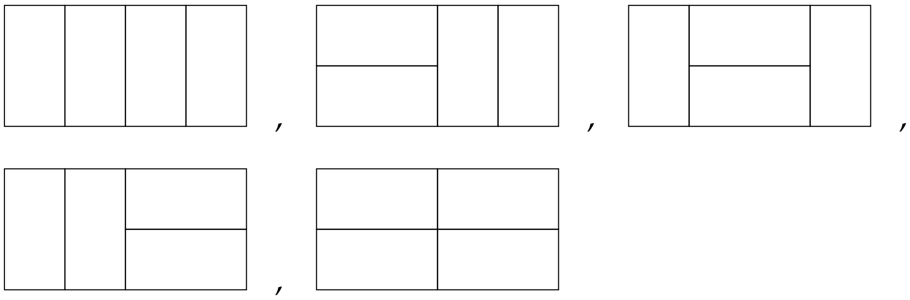
for some $(i,j) \in \mathbb{Z}^2$.

(d) A *domino tiling* of a shape S is a set partition of S into dominos (i.e., a set of disjoint dominos whose union is S).

(e) For any $n, m \in \mathbb{N}$, let $d_{n,m}$ be the # of domino tilings of $R_{n,m}$.

Can we compute $d_{n,m}$?
The case $m = 1$ is a bit too simple (do it!), so let us start with the case $m = 2$.

Here are the $d_{n,2}$ for $n \in \{0, 1, \ldots, 4\}$:

n	$d_{n,2}$	domino tilings
0	$d_{0,2} = 1$	
1	$d_{1,2} = 1$	
2	$d_{2,2} = 2$	
3	$d_{3,2} = 3$	
4	$d_{4,2} = 5$	

.

What do we expect $d_{n,2}$ to be in general?

A *height-*2 *rectangle* shall mean a rectangle of the form $R_{n,2}$ with $n \in \mathbb{N}$. Let us define the weighted set

$$\begin{aligned} D &:= \{\text{domino tilings of height-2 rectangles}\} \\ &= \{\text{domino tilings of } R_{n,2} \text{ with } n \in \mathbb{N}\}. \end{aligned}$$

We define the weight of a tiling T of $R_{n,2}$ to be $|T| := n$ (that is, the width of the rectangle tiled by this tiling).

Thus, D is a finite-type weighted set, with generating function

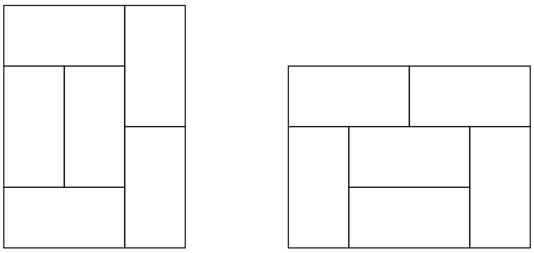
$$\overline{D} = \sum_{n \in \mathbb{N}} d_{n,2} x^n.$$

So we want to compute $\overline{D}$. Let us define a new weighted set that will help us at that.

Namely, we say that a *fault* of a domino tiling T is a vertical line ℓ such that

- each domino of T lies either left of ℓ or right of ℓ (but does not straddle ℓ), and
- there is at least one domino of T that lies left of ℓ, and at least domino of T that lies right of ℓ.

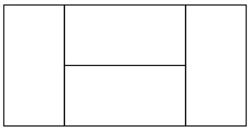
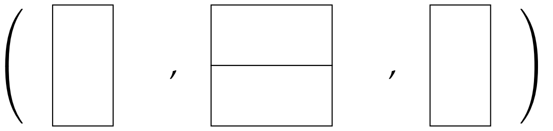
For example, in the following picture:



,

you see two domino tilings. The tiling on the left has a fault (namely, the vertical line separating the 2nd from the 3rd column), but the tiling on the right has none (a fault must be a vertical line by definition; a horizontal line doesn't count).

A domino tiling will be called *faultfree* if it is nonempty and has no fault. So the tiling on the right is faultfree.

> **Observation:** Any domino tiling of a height-2 rectangle can be decomposed uniquely into a tuple of faultfree tilings of (usually smaller) height-2 rectangles, by cutting it along the faults. For example:
>
> 
>
> decomposes as
>
> 
>
> .
>
> (Note that if the original tiling was faultfree, then this will be a 1-tuple. If the original tiling was empty, then this will be a 0-tuple.)
>
> Moreover, the sum of the weights of the faultfree tilings in the tuple is the weight of the original tiling.

Thus, if we define a new weighted set

$$F := \{\textbf{faultfree} \text{ domino tilings of } R_{n,2} \text{ with } n \in \mathbb{N}\}$$

(with the same weights as in D), then

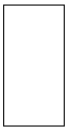
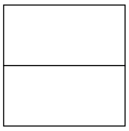
$$D \cong F^0 + F^1 + F^2 + F^3 + \cdots$$

(here, the right hand side is an infinite disjoint union). Thus,

$$\overline{D} = \overline{F^0 + F^1 + F^2 + F^3 + \cdots} = \overline{F}^0 + \overline{F}^1 + \overline{F}^2 + \overline{F}^3 + \cdots$$
$$\text{(by the infinite analogue of Proposition 3.12.5 and by Proposition 3.12.9)}$$
$$= \frac{1}{1-\overline{F}} \qquad \left(\text{by (5), with } \overline{F} \text{ substituted for } x\right).$$

Thus, if we can compute $\overline{F}$, then we can compute $\overline{D}$.

In order to compute $\overline{F}$, let us see how a faultfree domino tiling of a height-2 rectangle looks like. Here are two such tilings:

 and  .

I claim that these two tilings are the **only** faultfree tilings of height-2 rectangles. Indeed, consider any faultfree tiling of a height-2 rectangle. In this tiling, look at the domino that covers the box $(1,1)$. If it is a vertical domino, then this vertical domino must constitute the entire tiling, since otherwise there would be a fault to its right. If it is a horizontal domino, then there must be a second horizontal domino stacked atop it, and these two dominos must then constitute the entire tiling, since otherwise there would be a fault to their right. This leads to the two options we just named.

Thus, the weighted set F consists of just the two tilings shown above: one tiling of weight 1 and one tiling of weight 2. Hence, its weight generating function is $\overline{F} = x + x^2$. So

$$\overline{D} = \frac{1}{1-\overline{F}} = \frac{1}{1-(x+x^2)} = \frac{1}{1-x-x^2} = f_1 + f_2 x + f_3 x^2 + f_4 x^3 + \cdots,$$

where $(f_0, f_1, f_2, \ldots)$ is the Fibonacci sequence. Thus, comparing coefficients, we find

$$d_{n,2} = f_{n+1} \qquad \text{for each } n \in \mathbb{N}.$$

There are, of course, more elementary proofs of this (see [19fco, Proposition 1.1.11]).

Remark: There is an alternative argument for $\overline{D} = \dfrac{1}{1-\overline{F}}$ that runs as follows:

Any tiling in D is either empty, or can be uniquely split into a pair of a faultfree tiling and an arbitrary tiling (just split it along its leftmost fault, or along the right end if there is no fault). Thus,

$$D \cong 1 + F \times D.$$

Hence,

$$\overline{D} = \overline{1 + F \times D} = 1 + \overline{F} \cdot \overline{D}.$$

Solving this for $\overline{D}$, we find

$$\overline{D} = \frac{1}{1 - \overline{F}}.$$

Now, let us try to solve the analogous problem for height-3 rectangles. Forget about the D and F we defined above. Instead, define a new weighted set

$$\begin{aligned} D &:= \{\text{domino tilings of height-3 rectangles}\} \\ &= \{\text{domino tilings of } R_{n,3} \text{ with } n \in \mathbb{N}\}. \end{aligned}$$

The weight of a tiling T of $R_{n,3}$ is defined as before (i.e., it is $|T| = n$). Thus, D is a finite-type weighted set, with generating function

$$\overline{D} = \sum_{n \in \mathbb{N}} d_{n,3} x^n.$$

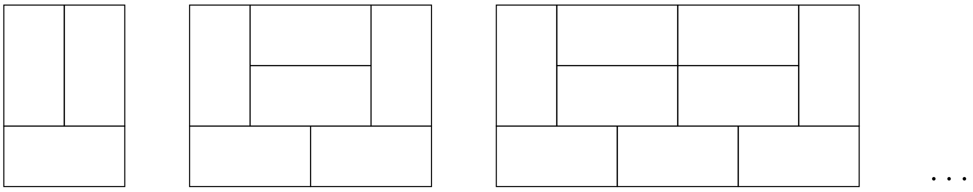
We want to compute this $\overline{D}$.

Set

$$F := \{\textbf{faultfree} \text{ domino tilings of } R_{n,3} \text{ with } n \in \mathbb{N}\}.$$

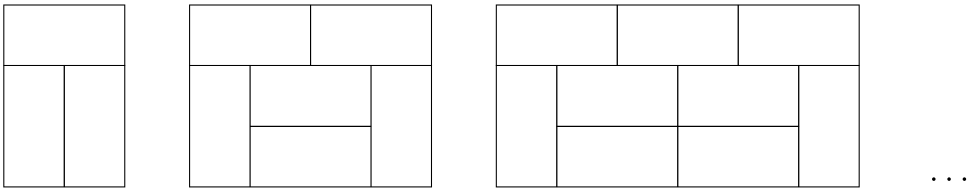
How does a faultfree domino tiling of a height-3 rectangle look like? Again, let us distinguish cases according to the kind of dominos that occupy the first column of the tiling:

- The faultfree domino tilings of a height-3 rectangle that contain a vertical domino in the **top** two cells of the first column are

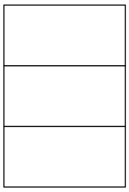
  (this is an infinite sequence of tilings, each obtained from the previous by inserting two columns in the middle by a fairly self-explanatory procedure). The weights of these tilings are $2, 4, 6, \ldots$, so their total contribution to the weight generating function $\overline{F}$ of F is $x^2 + x^4 + x^6 + \cdots$.

- The faultfree domino tilings of a height-3 rectangle that contain a vertical domino in the **bottom** two cells of the first column are

  (these are the top-down mirror images of the previously classified tilings). The weights of these tilings are $2, 4, 6, \ldots$, so their total contribution to the weight generating function $\overline{F}$ of F is $x^2 + x^4 + x^6 + \cdots$.

- The faultfree domino tilings of a height-3 rectangle that contain **no** vertical domino in the first column are



(yes, there is only one such tiling). The weight of this tiling is 2, so its total contribution to the weight generating function $\overline{F}$ of F is x^2.

This classification of faultfree domino tilings entails

$$\begin{aligned}\overline{F} &= \left(x^2+x^4+x^6+\cdots\right)+\left(x^2+x^4+x^6+\cdots\right)+x^2 \\ &= x^2\cdot\frac{1}{1-x^2}+x^2\cdot\frac{1}{1-x^2}+x^2 \qquad \left(\text{since } x^2+x^4+x^6+\cdots=x^2\cdot\frac{1}{1-x^2}\right) \\ &= \frac{3x^2-x^4}{1-x^2}.\end{aligned}$$

Thus,

$$\begin{aligned}\overline{D} = \frac{1}{1-\overline{F}} &= \frac{1}{1-\dfrac{3x^2-x^4}{1-x^2}} = \frac{1-x^2}{1-4x^2+x^4} \\ &= 1+3x^2+11x^4+41x^6+153x^8+\cdots.\end{aligned}$$

One thing you see right away is that only even powers of x appear in this FPS. In other words,

$$d_{n,3}=0 \text{ when } n \text{ is odd.}$$

This is not surprising, since if n is odd, then the rectangle $R_{n,3}$ has an odd # of squares, and thus cannot be tiled by dominos.

But we can also compute $d_{n,3}$ for even n. Indeed, using the same method (partial fractions) that we used for the Fibonacci sequence in Section 3.1, we can expand $\dfrac{1-x^2}{1-4x^2+x^4}$ as a sum of geometric series. Thus, after some computation, we find

$$d_{n,3}=\frac{3+\sqrt{3}}{6}\left(2+\sqrt{3}\right)^{n/2}+\frac{3-\sqrt{3}}{6}\left(2-\sqrt{3}\right)^{n/2} \qquad \text{for any even } n.$$

Now, what about computing $d_{n,m}$ in general? The above reasoning leading up to $\overline{D}=\dfrac{1}{1-\overline{F}}$ can be applied for any $m\in\mathbb{N}$, but describing F becomes harder and harder as m grows larger. The generating function $\overline{D}$ is still a quotient of two polynomials for any m (see, e.g., [KlaPol79]), but this requires more insight to prove. For $m \geq 6$, it appears that there is no formula for $d_{n,m}$ that requires only quadratic irrationalities.

Let me mention a different formula for $d_{n,m}$, found by Kasteleyn in 1961 (motivated by a theoretical physics model):

Theorem 3.12.11 (Kasteleyn's formula)**.** Assume that m is even and $n \geq 1$. Then,

$$d_{n,m} = 2^{mn/2} \prod_{j=1}^{m/2} \prod_{k=1}^{n} \sqrt{\left(\cos \frac{j\pi}{m+1}\right)^2 + \left(\cos \frac{k\pi}{n+1}\right)^2}.$$

See [Loehr11, Theorem 12.85] or [Stucky15] for proofs of this formula. Note that it can indeed be used for exact computation of $d_{n,m}$ (as there are algorithms for exact manipulation of "cyclotomic integers" such as $\cos \frac{j\pi}{m+1}$); for example, it yields $d_{8,8} = 12\,988\,816$.

3.13. Limits of FPSs

Next, I will discuss limits of sequences of FPSs. I will follow [Loehr11, §7.5]. As a bonus, this will give a simpler definition of infinite products, at least if products of the form $\prod_{i \in \mathbb{N}} f_i$ are enough for you.

We start with the stupidest kind of limit ever: the limit of an eventually constant sequence.

Definition 3.13.1. Let $(a_i)_{i \in \mathbb{N}} = (a_0, a_1, a_2, \ldots) \in K^{\mathbb{N}}$ be a sequence of elements of K. Let $a \in K$.

We say that $(a_i)_{i \in \mathbb{N}}$ *stabilizes to a as $i \to \infty$* (this is written "$a_i \to a$ as $i \to \infty$") if there exists some $N \in \mathbb{N}$ such that all integers $i \geq N$ satisfy $a_i = a$.

Note that this is equivalent to "$(a_i)_{i \in \mathbb{N}}$ converges to a in the discrete topology".

We often omit the words "if $i \to \infty$" from the phrase "$(a_i)_{i \in \mathbb{N}}$ stabilizes to a as $i \to \infty$" (so we just say "$(a_i)_{i \in \mathbb{N}}$ stabilizes to a").

If a_i stabilizes to a as $i \to \infty$, then we write $\lim_{i \to \infty} a_i = a$ and say that a is the *limit* (or *eventual value*) of $(a_i)_{i \in \mathbb{N}}$ (or, less precisely, that a is the limit of the a_i). This is legitimate, since a is uniquely determined by the sequence $(a_i)_{i \in \mathbb{N}}$.

We can replace $\mathbb{N}$ by $\mathbb{Z}_{\geq q} = \{q, q+1, q+2, \ldots\}$ in this definition, where q is any integer.

For example, the sequence

$$\left(\left\lfloor \frac{5}{i} \right\rfloor\right)_{i \geq 1} = \left(\left\lfloor \frac{5}{1} \right\rfloor, \left\lfloor \frac{5}{2} \right\rfloor, \left\lfloor \frac{5}{3} \right\rfloor, \ldots\right) = (5, 2, 1, 1, 1, 0, 0, 0, 0, \ldots)$$

stabilizes to 0.

On the other hand, the sequence $\left(\frac{5}{i}\right)_{i\geq 1}$ does not stabilize to anything. (It does converge to 0 in the sense of real analysis, but stabilization would be a stronger statement.)

Definition 3.13.2. Let $(f_i)_{i\in\mathbb{N}} \in K[[x]]^{\mathbb{N}}$ be a sequence of FPSs over K. Let $f \in K[[x]]$ be an FPS.

We say that $(f_i)_{i\in\mathbb{N}}$ *coefficientwise stabilizes to f as $i \to \infty$* (this is written "$f_i \to f$ as $i \to \infty$") if for each $n \in \mathbb{N}$, the sequence $([x^n] f_i)_{i\in\mathbb{N}}$ stabilizes to $[x^n] f$ as $i \to \infty$.

Note that this is equivalent to "$(f_i)_{i\in\mathbb{N}}$ converges to f in the product topology, where we regard $K[[x]]$ as $K \times K \times K \times \cdots$ with each K having the discrete topology".

If f_i coefficientwise stabilizes to f as $i \to \infty$, then we write $\lim\limits_{i\to\infty} f_i = f$ and say that f is the *limit* of $(f_i)_{i\in\mathbb{N}}$ (or, less precisely, that f is the limit of the f_i). This is legitimate, because f is uniquely determined by the sequence $(f_i)_{i\in\mathbb{N}}$.

Again, we can replace $\mathbb{N}$ by $\mathbb{Z}_{\geq q} = \{q, q+1, q+2, \ldots\}$ in this definition, where q is any integer.

Example 3.13.3. (a) We have $x^i \to 0$ as $i \to \infty$. Indeed, for each $n \in \mathbb{N}$, the sequence $\left([x^n]\left(x^i\right)\right)_{i\in\mathbb{N}}$ consists of a single 1 and infinitely many 0s; thus, this sequence stabilizes to 0.

(b) We **don't** have $\frac{1}{i}x \to 0$ as $i \to \infty$. Indeed, the x^1-coefficients never stabilize, so $\frac{1}{i}x$ has no limit as $i \to \infty$.

(c) We have

$$\left(1+x^1\right)\left(1+x^2\right)\cdots\left(1+x^i\right) \to \prod_{k=1}^{\infty}\left(1+x^k\right) \qquad \text{as } i \to \infty.$$

Indeed, the x^n-coefficient stabilizes after the n-th factor.

(d) It would be nice to have $\left(1+\frac{x}{n}\right)^n \to \exp$ as $n \to \infty$, as in real analysis. Unfortunately, this is not the case. Note that the binomial formula yields

$$\left(1+\frac{x}{n}\right)^n = 1 + \underbrace{n \cdot \frac{x}{n}}_{=x} + \binom{n}{2} \cdot \left(\frac{x}{n}\right)^2 + \cdots = 1 + x + \frac{\binom{n}{2}}{n^2}x^2 + \cdots.$$

This shows that the x^0-coefficient and the x^1-coefficient stabilize, but the x^2-coefficient does not.

Our definition of limit, alas, does not support $\lim\limits_{n\to\infty}\left(1+\frac{x}{n}\right)^n$.

Theorem 3.13.4. Let $(f_i)_{i\in\mathbb{N}} \in K[[x]]^{\mathbb{N}}$ be a sequence of FPSs. Assume that for each $n \in \mathbb{N}$, there exists some $g_n \in K$ such that the sequence $([x^n] f_i)_{i\in\mathbb{N}}$ stabilizes to g_n. Then, $f_i \to \sum\limits_{n\in\mathbb{N}} g_n x^n$ as $i \to \infty$.

Proof. Obvious. □

The following proposition is an analogue of the classical "limits respect sums and products" theorem from real analysis:

Proposition 3.13.5. Assume that $(f_i)_{i\in\mathbb{N}}$ and $(g_i)_{i\in\mathbb{N}}$ are two sequences of FPSs, and that f and g are two FPSs such that

$$f_i \to f \qquad \text{and} \qquad g_i \to g \qquad \text{as } i \to \infty.$$

Then,

$$f_i + g_i \to f + g \qquad \text{and} \qquad f_i g_i \to fg \qquad \text{as } i \to \infty.$$

Proof. Pretty easy. Left as a homework exercise (Exercise A.2.13.1). □

Corollary 3.13.6. Let $k \in \mathbb{N}$. For each $i \in \{1, 2, \ldots, k\}$, let f_i be an FPS, and let $(f_{i,n})_{n\in\mathbb{N}}$ be a sequence of FPSs such that

$$f_{i,n} \to f_i \qquad \text{as } n \to \infty.$$

Then,

$$\sum_{i=1}^{k} f_{i,n} \to \sum_{i=1}^{k} f_i \qquad \text{and} \qquad \prod_{i=1}^{k} f_{i,n} \to \prod_{i=1}^{k} f_i \qquad \text{as } n \to \infty.$$

Proof. Follows by induction on k, using Proposition 3.13.5. □

Here are a few more simple facts (the proofs are omitted but quite easy):

Proposition 3.13.7. Assume that $(f_i)_{i\in\mathbb{N}}$ and $(g_i)_{i\in\mathbb{N}}$ are two sequences of FPSs, and that f and g are two FPSs such that

$$f_i \to f \qquad \text{and} \qquad g_i \to g \qquad \text{as } i \to \infty.$$

Assume that each FPS g_i has constant term 1, and so does the FPS g.

Then,

$$\frac{f_i}{g_i} \to \frac{f}{g} \qquad \text{as } i \to \infty.$$

Proof. Pretty easy. Left as a homework exercise (Exercise A.2.13.1). □

Theorem 3.13.8. Let $(f_n)_{n\in\mathbb{N}}$ be a summable sequence of FPSs. Then,

$$\sum_{n=0}^{i} f_n \to \sum_{n\in\mathbb{N}} f_n \qquad \text{as } i \to \infty.$$

In other words, the infinite sum $\sum\limits_{n\in\mathbb{N}} f_n$ is the limit of the finite partial sums $\sum\limits_{n=0}^{i} f_n$.

Theorem 3.13.9. Let $(f_n)_{n\in\mathbb{N}}$ be a multipliable sequence of FPSs. Then,

$$\prod_{n=0}^{i} f_n \to \prod_{n\in\mathbb{N}} f_n \qquad \text{as } i \to \infty.$$

In other words, the infinite product $\prod\limits_{n\in\mathbb{N}} f_n$ is the limit of the finite partial products $\prod\limits_{n=0}^{i} f_n$.

Corollary 3.13.10. Each FPS is a limit of a sequence of polynomials. Indeed, if $a = \sum\limits_{n\in\mathbb{N}} a_n x^n$ (with $a_n \in K$), then

$$a = \lim_{i\to\infty} \sum_{n=0}^{i} a_n x^n.$$

This corollary can be rewritten as "the polynomials are dense in the FPSs" (more formally: $K[x]$ is dense in $K[[x]]$). This is useful, because it allows you to restrict yourself to polynomials when proving some properties of FPSs. That is, sometimes, if you want to prove that some identity holds for FPSs, it suffices to prove it for polynomials, and then use a limiting argument.

3.14. Laurent power series

Let us now try to extend the concept of FPSs to allow negative powers of x. As a motivating example, we recall the binary positional system:

Definition 3.14.1. A *binary representation* of an integer n means an essentially finite sequence $(b_i)_{i\in\mathbb{N}} = (b_0, b_1, b_2, \ldots) \in \{0,1\}^{\mathbb{N}}$ such that

$$n = \sum_{i\in\mathbb{N}} b_i 2^i.$$

(Recall: "Essentially finite" means "all but finitely many $i \in \mathbb{N}$ satisfy $b_i = 0$".)

The following theorem is well-known (and has been proved in Subsection 3.11.1):

Theorem 3.14.2. Each $n \in \mathbb{N}$ has a unique binary representation.

Note that we are encoding the digits (actually, bits) of a binary representation as essentially finite sequences instead of finite tuples. This way, we don't have to worry about leading zeros breaking the uniqueness in Theorem 3.14.2.

Let us now define a variation of binary representation:

Definition 3.14.3. A *balanced ternary representation* of an integer n means an essentially finite sequence $(b_i)_{i\in\mathbb{N}} = (b_0, b_1, b_2, \ldots) \in \{0, 1, -1\}^{\mathbb{N}}$ such that

$$n = \sum_{i\in\mathbb{N}} b_i 3^i.$$

Examples:

- The integer 19 has a balanced ternary representation $(1, 0, -1, 1, 0, 0, 0, \ldots)$, because
$$19 = 1 - 9 + 27 = 3^0 - 3^2 + 3^3 = 1 \cdot 3^0 + (-1) \cdot 3^2 + 1 \cdot 3^3.$$
- The integer 42 has a balanced ternary representation $(0, -1, -1, -1, 1, 0, 0, 0, \ldots)$, because
$$42 = 81 - 27 - 9 - 3 = 3^4 - 3^3 - 3^2 - 3^1.$$

Note that (unlike with binary representations) even negative integers can have balanced ternary representations.

In the Soviet Union of the 1960s/70s, balanced ternary representations have been used as a foundation for computers (see the Setun computer). The idea was shelved in the 1970s, but a noticeable amount of algorithms have been invented for working with balanced ternary representations. (See [Knuth2, §4.1] for some discussion of these.) The following theorem (which goes back to Fibonacci) is crucial for making balanced ternary representations useful:

Theorem 3.14.4. Each integer n has a unique balanced ternary representation.

There are various ways to prove this (see, e.g., [20f, solution to Exercise 3.7.8] for an elementary one). Let us here try to prove it using FPSs (imitating our proof of Theorem 3.14.2 in Subsection 3.11.1). Since the b_i can be -1s, we must allow for negative powers of x.

Let us first argue informally and see later whether we can make sense of what we have done.

Here is the idea[42]: We shall compute the product

$$\left(1+x+x^{-1}\right)\left(1+x^{3}+x^{-3}\right)\left(1+x^{9}+x^{-9}\right)\cdots=\prod_{i\geq 0}\left(1+x^{3^i}+x^{-3^i}\right)$$

in two ways:

- On the one hand, this product equals

$$\begin{aligned}
&\prod_{i\geq 0}\underbrace{\left(1+x^{3^i}+x^{-3^i}\right)}_{=\sum\limits_{b\in\{0,1,-1\}} x^{b\cdot 3^i}} \\
&=\prod_{i\geq 0}\ \sum_{b\in\{0,1,-1\}} x^{b\cdot 3^i} \\
&=\sum_{\substack{(b_0,b_1,b_2,\ldots)\in\{0,1,-1\}^{\mathbb{N}} \\ \text{essentially finite}}} x^{b_0 3^0} x^{b_1 3^1} x^{b_2 3^2}\cdots \\
&\qquad\qquad \text{(here, we have just expanded the product)} \\
&=\sum_{\substack{(b_0,b_1,b_2,\ldots)\in\{0,1,-1\}^{\mathbb{N}} \\ \text{essentially finite}}} x^{b_0 3^0+b_1 3^1+b_2 3^2+\cdots} \\
&=\sum_{n\in\mathbb{Z}} \left(\text{\# of balanced ternary representations of } n\right)\cdot x^n, \qquad (130)
\end{aligned}$$

  since a balanced ternary representation of n is precisely an essentially finite sequence $(b_0, b_1, b_2, \ldots) \in \{0, 1, -1\}^{\mathbb{N}}$ satisfying $b_0 3^0 + b_1 3^1 + b_2 3^2 + \cdots = n$.

- On the other hand, we have $1+x+x^{-1}=\dfrac{1-x^3}{x\,(1-x)}$. Substituting x^{3^i} for x in this equality, we obtain

$$1+x^{3^i}+x^{-3^i}=\frac{1-x^{3^{i+1}}}{x^{3^i}\left(1-x^{3^i}\right)}\qquad\text{for each } i\geq 0.$$

[42] which, again, goes back to Euler [Euler48, §331]

Hence,

$$\begin{aligned}
&\prod_{i\geq 0}\left(1+x^{3^i}+x^{-3^i}\right)\\
&=\prod_{i\geq 0}\frac{1-x^{3^{i+1}}}{x^{3^i}\left(1-x^{3^i}\right)}\\
&=\frac{1-x^3}{x\left(1-x\right)}\cdot\frac{1-x^9}{x^3\left(1-x^3\right)}\cdot\frac{1-x^{27}}{x^9\left(1-x^9\right)}\cdot\frac{1-x^{81}}{x^{27}\left(1-x^{27}\right)}\cdot\cdots\\
&=\underbrace{\frac{1}{xx^3x^9x^{27}\cdots}}_{\substack{=x^{-\infty}\\ \text{(whatever this means)}}}\cdot\underbrace{\frac{1}{1-x}}_{=1+x+x^2+x^3+\cdots}\\
&\qquad\qquad\text{(by a somewhat daring use of the telescope principle)}\\
&=x^{-\infty}\left(1+x+x^2+x^3+\cdots\right)\\
&=\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\\
&\qquad\qquad\left(\begin{array}{c}\text{with some artistic license,}\\ \text{since } x^i\left(1+x+x^2+x^3+\cdots\right)=x^i+x^{i+1}+x^{i+2}+\cdots\\ \text{for each } i\in\mathbb{Z}\end{array}\right)\\
&=\sum_{n\in\mathbb{Z}}x^n. \qquad (131)
\end{aligned}$$

Comparing (130) with (131), we find

$$\sum_{n\in\mathbb{Z}}(\#\text{ of balanced ternary representations of } n)\cdot x^n=\sum_{n\in\mathbb{Z}}x^n.$$

Comparing coefficients, we thus conclude that

$$(\#\text{ of balanced ternary representations of } n)=1$$

for each $n\in\mathbb{Z}$. This "proves" Theorem 3.14.4; we just need to make our computations rigorous – i.e., define the ring in which we have been computing, explain what x is, and justify the well-definedness of our infinite products and sums.

Let us first play around a bit further. We have

$$\begin{aligned}
&(1-x)\left(\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\right)\\
&=\left(\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\right)-\underbrace{x\left(\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\right)}_{\substack{=\cdots+x^{-1}+x^0+x^1+x^2+x^3+\cdots\\ =\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots}}\\
&=\left(\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\right)-\left(\cdots+x^{-2}+x^{-1}+x^0+x^1+x^2+\cdots\right)\\
&=0.
\end{aligned}$$

Thus, dividing by $1-x$, we obtain

$$\cdots + x^{-2} + x^{-1} + x^0 + x^1 + x^2 + \cdots = 0.$$

Comparing coefficients, we conclude that

$$1 = 0 \qquad \text{for each } n \in \mathbb{Z}.$$

Oops! Looks like we have overtaxed our artistic license.

So we need to be careful with negative powers of x. Not everything that looks like a valid computation actually is one. So let us try to be rigorous and delimit what can and what cannot be done with negative powers of x.

Let us try to define "FPSs with negative powers of x" formally. First, let's define the largest possible space of such FPSs:

> **Definition 3.14.5.** Let $K\left[\left[x^{\pm}\right]\right]$ be the K-module $K^{\mathbb{Z}}$ of all families $\left(a_n\right)_{n\in\mathbb{Z}} = \left(\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots\right)$ of elements of K. Its addition and its scaling are defined entrywise:
>
> $$\begin{aligned} \left(a_n\right)_{n\in\mathbb{Z}} + \left(b_n\right)_{n\in\mathbb{Z}} &= \left(a_n + b_n\right)_{n\in\mathbb{Z}}; \\ \lambda \left(a_n\right)_{n\in\mathbb{Z}} &= \left(\lambda a_n\right)_{n\in\mathbb{Z}} \qquad \text{for each } \lambda \in K. \end{aligned}$$
>
> An element of $K\left[\left[x^{\pm}\right]\right]$ will be called a *doubly infinite power series*. This name is justified by the fact that we will later use the notation $\sum\limits_{n\in\mathbb{Z}} a_n x^n$ for a family $\left(a_n\right)_{n\in\mathbb{Z}} \in K\left[\left[x^{\pm}\right]\right]$.

Now, let us try to define a multiplication on this K-module $K\left[\left[x^{\pm}\right]\right]$, in order to turn it into a K-algebra (like $K\left[\left[x\right]\right]$). This multiplication should satisfy

$$\left(a_n\right)_{n\in\mathbb{Z}} \cdot \left(b_n\right)_{n\in\mathbb{Z}} = \left(c_n\right)_{n\in\mathbb{Z}}, \qquad \text{where} \qquad c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}$$

(since this is what we would get if we expanded $\left(\sum\limits_{n\in\mathbb{Z}} a_n x^n\right)\left(\sum\limits_{n\in\mathbb{Z}} b_n x^n\right)$ and combined like powers of x). Unfortunately, the sum $\sum\limits_{i\in\mathbb{Z}} a_i b_{n-i}$ is now infinite (unlike for $K\left[\left[x\right]\right]$), and is not always defined. Hence, $K\left[\left[x^{\pm}\right]\right]$ is not a K-algebra (even though it is a K-module). In general, we cannot multiply its elements. This explains why our above computations have led us astray.

If we cannot multiply two arbitrary elements of $K\left[\left[x^{\pm}\right]\right]$, can we perhaps restrict ourselves to a smaller K-submodule of $K\left[\left[x^{\pm}\right]\right]$ whose elements can be multiplied? Of course, $K\left[\left[x\right]\right]$ is such a submodule, but there are some others. Here is one:

Definition 3.14.6. Let $K\left[x^{\pm}\right]$ be the K-submodule of $K\left[\left[x^{\pm}\right]\right]$ consisting of all **essentially finite** families $\left(a_n\right)_{n\in\mathbb{Z}}$. This is indeed a K-submodule (check it!). It should be thought of as an analogue of the ring of polynomials $K\left[x\right]$, but now allowing for negative powers of x.

The elements of $K\left[x^{\pm}\right]$ are called *Laurent polynomials* in the indeterminate x over K.

We define a multiplication on $K\left[x^{\pm}\right]$ by setting

$$\left(a_n\right)_{n\in\mathbb{Z}} \cdot \left(b_n\right)_{n\in\mathbb{Z}} = \left(c_n\right)_{n\in\mathbb{Z}}, \qquad \text{where} \qquad c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

Note that the sum $\sum\limits_{i\in\mathbb{Z}} a_i b_{n-i}$ is now well-defined, because it is essentially finite.

We define an element $x \in K\left[x^{\pm}\right]$ by $x = \left(\delta_{i,1}\right)_{i\in\mathbb{Z}}$.

Theorem 3.14.7. The K-module $K\left[x^{\pm}\right]$, equipped with the multiplication we just defined, is a commutative K-algebra. Its unity is $\left(\delta_{i,0}\right)_{i\in\mathbb{Z}}$. The element x is invertible in this K-algebra.

This K-algebra $K\left[x^{\pm}\right]$ is called the *Laurent polynomial ring* in one indeterminate x over K. It is often denoted by $K\left[x^{\pm 1}\right]$ or $K\left[x, x^{-1}\right]$ as well.

Proposition 3.14.8. Any doubly infinite power series $a = \left(a_i\right)_{i\in\mathbb{Z}} \in K\left[\left[x^{\pm}\right]\right]$ satisfies

$$a = \sum_{i\in\mathbb{Z}} a_i x^i.$$

Here, the powers x^i are taken in the Laurent polynomial ring $K\left[x^{\pm}\right]$, but the infinite sum $\sum\limits_{i\in\mathbb{Z}} a_i x^i$ is taken in the K-module $K\left[\left[x^{\pm}\right]\right]$. (The notions of summable families and infinite sums are defined in $K\left[\left[x^{\pm}\right]\right]$ in the same way as they are defined in $K\left[\left[x\right]\right]$.)

Examples of Laurent polynomials are

- any polynomial in $K\left[x\right]$;
- x^{-15};
- $x^2 + 3 + 7x^{-3}$.

There are other, equivalent ways to define the Laurent polynomial ring $K\left[x^{\pm}\right]$:

- as the group algebra of the cyclic group $\mathbb{Z}$ over K;
- as the localization of the polynomial ring $K\left[x\right]$ at the powers of x.

(These are done in some textbooks on abstract algebra – e.g., see [Ford21, Exercise 3.6.31] for a quick overview.)

Now let us see if we can make our above proof of Theorem 3.14.4 rigorous using Laurent polynomials. Unfortunately, $K\left[x^{\pm}\right]$ is "too small" to contain the infinite product $\prod\limits_{i\geq 0}\left(1+x^{3^i}+x^{-3^i}\right)$. However, we can try using its partial products, which are finite. For each $k\in\mathbb{N}$, we have

$$\begin{aligned}
&\prod_{i=0}^{k}\left(1+x^{3^i}+x^{-3^i}\right)\\
&=\left(1+x+x^{-1}\right)\left(1+x^{3}+x^{-3}\right)\cdots\left(1+x^{3^k}+x^{-3^k}\right)\\
&=\frac{1-x^3}{x\left(1-x\right)}\cdot\frac{1-x^9}{x^3\left(1-x^3\right)}\cdot\cdots\cdot\frac{1-x^{3^{k+1}}}{x^{3^k}\left(1-x^{3^k}\right)}\\
&\qquad\qquad\left(\begin{array}{c}\text{this is somewhat unrigorous, since } 1-x^{3^i} \text{ are not invertible}\\ \text{in } K\left[x^{\pm}\right]\text{, but this will soon be made rigorous}\end{array}\right)\\
&=\underbrace{\frac{1}{xx^3x^9\cdots x^{3^k}}}_{=x^{-\left(3^0+3^1+\cdots+3^k\right)}}\cdot\underbrace{\frac{1-x^{3^{k+1}}}{1-x}}_{=1+x+x^2+\cdots+x^{3^{k+1}-1}}\\
&=x^{-\left(3^0+3^1+\cdots+3^k\right)}\cdot\left(1+x+x^2+\cdots+x^{3^{k+1}-1}\right)\\
&=x^{-\left(3^0+3^1+\cdots+3^k\right)}\cdot\left(1+x+x^2+\cdots+x^{2\left(3^0+3^1+\cdots+3^k\right)}\right)\\
&\qquad\qquad\left(\text{since } 3^{k+1}-1=2\cdot\left(3^0+3^1+\cdots+3^k\right)\text{ (check this!)}\right)\\
&=x^{-\left(3^0+3^1+\cdots+3^k\right)}+x^{-\left(3^0+3^1+\cdots+3^k\right)+1}+x^{-\left(3^0+3^1+\cdots+3^k\right)+2}+\cdots+x^{3^0+3^1+\cdots+3^k}\\
&=\sum_{\substack{n\in\mathbb{Z};\\ \left|n\right|\leq 3^0+3^1+\cdots+3^k}}x^n.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\prod_{i=0}^{k} \underbrace{\left(1 + x^{3^i} + x^{-3^i}\right)}_{= \sum\limits_{b\in\{0,1,-1\}} x^{b\cdot 3^i}} \\
&= \prod_{i=0}^{k} \sum_{b\in\{0,1,-1\}} x^{b\cdot 3^i} \\
&= \sum_{(b_0,b_1,\ldots,b_k)\in\{0,1,-1\}^{k+1}} x^{b_0 3^0} x^{b_1 3^1} \cdots x^{b_k 3^k} \qquad \left(\begin{array}{c}\text{by expanding the product} \\ \text{using Proposition 3.11.22}\end{array}\right) \\
&= \sum_{(b_0,b_1,\ldots,b_k)\in\{0,1,-1\}^{k+1}} x^{b_0 3^0 + b_1 3^1 + \cdots + b_k 3^k} \\
&= \sum_{n\in\mathbb{Z}} (\#\text{ of } k\text{-bounded balanced ternary representations of } n) \cdot x^n,
\end{aligned}$$

where a balanced ternary representation $(b_0, b_1, b_2, \ldots)$ is said to be *k-bounded* if $b_{k+1} = b_{k+2} = b_{k+3} = \cdots = 0$. Comparing the two results, we find

$$\begin{aligned}
&\sum_{n\in\mathbb{Z}} (\#\text{ of } k\text{-bounded balanced ternary representations of } n) \cdot x^n \\
&= \sum_{\substack{n\in\mathbb{Z};\\ |n|\leq 3^0+3^1+\cdots+3^k}} x^n.
\end{aligned}$$

Comparing coefficients, we thus see that each $n \in \mathbb{Z}$ satisfying $|n| \leq 3^0 + 3^1 + \cdots + 3^k$ has a unique k-bounded balanced ternary representation. Letting $k \to \infty$ now quickly yields Theorem 3.14.4 (because any balanced ternary representation is k-bounded for a sufficiently large k).

Thus we have proved Theorem 3.14.4 up to the fact that we have divided by the polynomials $1 - x, 1 - x^3, 1 - x^9, \ldots$, which are not invertible in the Laurent polynomial ring $K[x^{\pm}]$. In order to fill this gap, we need a new K-algebra: The Laurent polynomial ring $K[x^{\pm}]$ is too small, whereas the original K-module $K[[x^{\pm}]]$ is not a ring. We need some kind of middle ground: some K-module lying between $K[x^{\pm}]$ and $K[[x^{\pm}]]$ that is a ring but allows division by $1 - x$, $1 - x^3, 1 - x^9, \ldots$ (and, more generally, by $1 - x^i$ for each positive integer i).

This middle ground is called $K((x))$ and is defined as follows:

Definition 3.14.9. We let $K((x))$ be the subset of $K[[x^{\pm}]]$ consisting of all families $(a_i)_{i\in\mathbb{Z}} \in K[[x^{\pm}]]$ such that the sequence $(a_{-1}, a_{-2}, a_{-3}, \ldots)$ is essentially finite – i.e., such that all sufficiently low $i \in \mathbb{Z}$ satisfy $a_i = 0$.

The elements of $K((x))$ are called *Laurent series* in one indeterminate x over K.

For example (for $K = \mathbb{Z}$):

- the "series" $x^{-3}+x^{-2}+x^{-1}+x^{0}+x^{1}+\cdots$ belongs to $K((x))$;
- the "series" $1+x^{-1}+x^{-2}+x^{-3}+\cdots$ does not belong to $K((x))$;
- the "series" $\sum\limits_{n\in\mathbb{Z}} x^n = \cdots + x^{-2}+x^{-1}+x^{0}+x^{1}+x^{2}+\cdots$ does not belong to $K((x))$.

Theorem 3.14.10. The subset $K((x))$ is a K-submodule of $K[[x^{\pm}]]$. But it has a multiplication (unlike $K[[x^{\pm}]]$). This multiplication is given by the same rule as the multiplication of $K[x^{\pm}]$: namely,

$$(a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}} = (c_n)_{n\in\mathbb{Z}}, \qquad \text{where} \qquad c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

The sum $\sum\limits_{i\in\mathbb{Z}} a_i b_{n-i}$ here is well-defined, because it is essentially finite (indeed, for all sufficiently low $i\in\mathbb{Z}$, we have $a_i=0$ and thus $a_i b_{n-i}=0$; on the other hand, for all sufficiently high $i\in\mathbb{Z}$, we have $b_{n-i}=0$ and thus $a_i b_{n-i}=0$).

Now, the ring $K((x))$ contains both the FPS ring $K[[x]]$ and the Laurent polynomial ring $K[x^{\pm}]$ as subrings (and actually as K-subalgebras). This makes it one of the most convenient places for formal manipulation of FPSs. (However, it has a disadvantage compared to the FPS ring $K[[x]]$: Namely, you cannot easily substitute something for x in a Laurent series $f\in K((x))$.)

Now, our above computation of $\prod\limits_{i=0}^{k}\left(1+x^{3^i}+x^{-3^i}\right)$ makes perfect sense in the Laurent series ring $K((x))$ (indeed, for each positive integer i, the power series $1-x^i$ is invertible in $K[[x]]$ and thus also invertible in $K((x))$). Hence, at last, we have a rigorous proof of Theorem 3.14.4.

Actually, you **could** also make sense of our original argument for proving Theorem 3.14.4, with the infinite product $\prod\limits_{i\geq 0}\left(1+x^{3^i}+x^{-3^i}\right)$, as long as you made sure to interpret it correctly: First, compute the finite products $\prod\limits_{i=0}^{k}\left(1+x^{3^i}+x^{-3^i}\right)$ in the ring $K((x))$. Then, take their limit $\lim\limits_{k\to\infty}\prod\limits_{i=0}^{k}\left(1+x^{3^i}+x^{-3^i}\right)$ in $K[[x^{\pm}]]$ (this is not a ring, but the notion of a limit in $K[[x^{\pm}]]$ is defined just as it was in $K[[x]]$).

More can be said about the K-algebra $K((x))$ when K is a field: Indeed, in this case, it is a field itself! This fact (whose proof is Exercise A.2.14.2) is not very useful in combinatorics, but quite so in abstract algebra.

One more remark. As we have explained, $K[[x^{\pm}]]$ is not a ring. However, some semblance of multiplication can be restored in $K[[x^{\pm}]]$. Namely, a "doubly infinite power series" $\sum\limits_{n\in\mathbb{Z}} a_n x^n = (a_n)_{n\in\mathbb{Z}} \in K[[x^{\pm}]]$ can be multiplied by a Laurent polynomial $\sum\limits_{n\in\mathbb{Z}} b_n x^n = (b_n)_{n\in\mathbb{Z}} \in K[x^{\pm}]$, because in this case the sums

$\sum\limits_{i\in\mathbb{Z}} a_i b_{n-i}$ will be essentially finite. Thus, while we cannot always multiply two elements of $K\left[\left[x^{\pm}\right]\right]$, we can always multiply an element of $K\left[\left[x^{\pm}\right]\right]$ with an element of $K\left[x^{\pm}\right]$. This makes $K\left[\left[x^{\pm}\right]\right]$ into a $K\left[x^{\pm}\right]$-module. The equality

$$(1-x)\left(\cdots+x^{-2}+x^{-1}+x^{0}+x^{1}+x^{2}+\cdots\right)=0$$

reveals that this module has torsion.

3.15. Multivariate FPSs

Multivariate FPSs are just FPSs in several variables. Their theory is mostly analogous to the theory of univariate FPSs (which is what we have been studying above), but requires more subscripts. I will just discuss the main differences.

For instance, FPSs in two variables x and y have the form $\sum\limits_{i,j\in\mathbb{N}} a_{i,j}x^iy^j$, where the summation sign $\sum\limits_{i,j\in\mathbb{N}}$ means $\sum\limits_{(i,j)\in\mathbb{N}^2}$ of course. Formally, such an FPS is a family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ of elements of K. The indeterminates x and y are defined by

$$x=\left(\delta_{(i,j),(1,0)}\right)_{(i,j)\in\mathbb{N}^2} \qquad \text{and} \qquad y=\left(\delta_{(i,j),(0,1)}\right)_{(i,j)\in\mathbb{N}^2}$$

(so that each indeterminate has exactly one coefficient equal to 1, while all other coefficients are 0). The rules for addition, subtraction, scaling and multiplication are essentially as they are for univariate FPSs, except that now the indexing set is $\mathbb{N}^2$ instead of $\mathbb{N}$. For example, multiplication of FPSs in x and y is defined by the formula

$$\left[x^ny^m\right](ab)=\sum_{\substack{(i,j),\ (k,\ell)\in\mathbb{N}^2;\\ i+k=n;\\ j+\ell=m}}\left[x^iy^j\right]a\cdot\left[x^ky^\ell\right]b$$

(for any two FPSs a and b and any $n,m\in\mathbb{N}$).

More generally, for any $k\in\mathbb{N}$, the FPSs in k variables $x_1,x_2,\ldots,x_k$ are defined to be the families $\left(a_{\mathbf{i}}\right)_{\mathbf{i}\in\mathbb{N}^k}$ of elements of K indexed by k-tuples $\mathbf{i}=(i_1,i_2,\ldots,i_k)\in\mathbb{N}^k$. Addition, subtraction and scaling of such families is defined entrywise. Multiplication is defined by the formula

$$\left[\mathbf{x}^{\mathbf{n}}\right](ab)=\sum_{\substack{\mathbf{i},\mathbf{j}\in\mathbb{N}^k;\\ \mathbf{i}+\mathbf{j}=\mathbf{n}}}\left[\mathbf{x}^{\mathbf{i}}\right]a\cdot\left[\mathbf{x}^{\mathbf{j}}\right]b$$

(for any two FPSs a and b and any $\mathbf{n}\in\mathbb{N}^k$), where

- the sum $\mathbf{i}+\mathbf{j}$ means the entrywise sum of the k-tuples $\mathbf{i}$ and $\mathbf{j}$ (that is, $\mathbf{i}+\mathbf{j}=(i_1+j_1,i_2+j_2,\ldots,i_k+j_k)$, where $\mathbf{i}=(i_1,i_2,\ldots,i_k)$ and $\mathbf{j}=(j_1,j_2,\ldots,j_k)$);

- if $\mathbf{m} \in \mathbb{N}^k$ and h is an FPS in $x_1, x_2, \ldots, x_k$, then $[\mathbf{x}^{\mathbf{m}}]\, h$ is the $\mathbf{m}$-th entry of the family h. Just as in the univariate case, this entry $[\mathbf{x}^{\mathbf{m}}]\, h$ is called the *coefficient of the monomial* $\mathbf{x}^{\mathbf{m}} := x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}$ in h (where $\mathbf{m} = (m_1, m_2, \ldots, m_k)$).

With this notation, the formula for ab doesn't look any more complicated than the analogous formula in the univariate case. We just are using k-tuples of nonnegative integers instead of nonnegative integers themselves to index the monomials and the coefficients.

The indeterminates $x_1, x_2, \ldots, x_k$ are defined by

$$x_i = \left(\delta_{\mathbf{n},(0,0,\ldots,0,1,0,0,\ldots,0)}\right)_{\mathbf{n}\in\mathbb{N}^k},$$

where the tuple $(0,0,\ldots,0,1,0,0,\ldots,0)$ is a k-tuple with a lone 1 in its i-th position. Thus, if $\mathbf{m} = (m_1, m_2, \ldots, m_k) \in \mathbb{N}^k$, then

$$x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} = \left(\delta_{\mathbf{n},\mathbf{m}}\right)_{\mathbf{n}\in\mathbb{N}^k},$$

so that each FPS $f = (f_{\mathbf{m}})_{\mathbf{m}\in\mathbb{N}^k}$ satisfies

$$f = \sum_{\mathbf{m}=(m_1,m_2,\ldots,m_k)\in\mathbb{N}^k} f_{\mathbf{m}} x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}.$$

Most of what we have said about FPSs in one variable applies similarly to FPSs in multiple variables. The proofs are similar but more laborious due to the need for subscripts. Instead of the derivative of an FPS, there are now k derivatives (one for each variable); they are called *partial derivatives*. One needs to be somewhat careful with substitution – e.g., one cannot substitute non-commuting elements into a multivariate polynomial. For example, you cannot substitute two non-commuting matrices A and B for x and y into the polynomial xy, at least not without sacrificing the rule that a value of the product of two polynomials should be the product of their values (since $\underbrace{x[A,B]}_{=A} \cdot \underbrace{y[A,B]}_{=B} = AB$ would have to equal $\underbrace{y[A,B]}_{=B} \cdot \underbrace{x[A,B]}_{=A} = BA$). But you can still substitute k commuting elements for the k indeterminates in a k-variable polynomial. You can also compose multivariate FPSs as long as appropriate summability conditions are satisfied.

Definition 3.15.1. Let $k \in \mathbb{N}$. The K-algebra of all FPSs in k variables $x_1, x_2, \ldots, x_k$ over K will be denoted by $K[[x_1, x_2, \ldots, x_k]]$.

Sometimes we will use different names for our variables. For example, if we work with 2 variables, we will commonly call them x and y instead of x_1 and x_2. Correspondingly, we will use the notation $K[[x,y]]$ (instead of $K[[x_1, x_2]]$) for the K-algebra of FPSs in these two variables.

Let me give an example of working with multivariate FPSs.

Let us work in $K[[x,y]]$. On the one hand, we have

$$\begin{aligned}
\sum_{n,k\in\mathbb{N}} \binom{n}{k} x^n y^k &= \sum_{n\in\mathbb{N}} \sum_{k\in\mathbb{N}} \binom{n}{k} x^n y^k = \sum_{n\in\mathbb{N}} x^n \underbrace{\sum_{k\in\mathbb{N}} \binom{n}{k} y^k}_{\substack{=(1+y)^n \\ \text{(by the binomial formula)}}} \\
&= \sum_{n\in\mathbb{N}} x^n (1+y)^n = \sum_{n\in\mathbb{N}} (x(1+y))^n = \frac{1}{1-x(1+y)} \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } x(1+y) \text{ for } x \text{ in} \\ \text{the formula } \sum\limits_{n\in\mathbb{N}} x^n = \dfrac{1}{1-x}; \\ \text{this is allowed since } x(1+y) \text{ has constant term } 0 \end{array}\right) \\
&= \frac{1}{1-x} \cdot \frac{1}{1-\dfrac{x}{1-x}y} \qquad \text{(easy to check by computation)} \\
&= \frac{1}{1-x} \cdot \sum_{k\in\mathbb{N}} \left(\frac{x}{1-x}y\right)^k \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } \dfrac{x}{1-x}y \text{ for } x \\ \text{in the formula } \dfrac{1}{1-x} = \sum\limits_{k\in\mathbb{N}} x^k \end{array}\right) \\
&= \frac{1}{1-x} \cdot \sum_{k\in\mathbb{N}} \frac{x^k}{(1-x)^k} y^k = \sum_{k\in\mathbb{N}} \frac{x^k}{(1-x)^{k+1}} y^k.
\end{aligned}$$

On the other hand, we have

$$\sum_{n,k\in\mathbb{N}} \binom{n}{k} x^n y^k = \sum_{k\in\mathbb{N}} \sum_{n\in\mathbb{N}} \binom{n}{k} x^n y^k = \sum_{k\in\mathbb{N}} \left(\sum_{n\in\mathbb{N}} \binom{n}{k} x^n \right) y^k.$$

Comparing these two equalities, we find

$$\sum_{k\in\mathbb{N}} \frac{x^k}{(1-x)^{k+1}} y^k = \sum_{k\in\mathbb{N}} \left(\sum_{n\in\mathbb{N}} \binom{n}{k} x^n \right) y^k. \tag{132}$$

Now, comparing coefficients in front of $x^i y^k$ in (132), we conclude that

$$\frac{x^k}{(1-x)^{k+1}} = \sum_{n\in\mathbb{N}} \binom{n}{k} x^n \qquad \text{for each } k \in \mathbb{N}. \tag{133}$$

Let me explain in a bit more detail what I mean by "comparing coefficients in front of $x^i y^k$". What we have used is the following simple fact:

Proposition 3.15.2. Let $f_0, f_1, f_2, \ldots$ and $g_0, g_1, g_2, \ldots$ be FPSs in a single variable x such that

$$\sum_{k\in\mathbb{N}} f_k y^k = \sum_{k\in\mathbb{N}} g_k y^k \qquad \text{in } K\left[\left[x,y\right]\right]. \tag{134}$$

Then, $f_k = g_k$ for each $k \in \mathbb{N}$.

Proof. For each $k \in \mathbb{N}$, let us write the two FPSs f_k and g_k as $f_k = \sum\limits_{n\in\mathbb{N}} f_{k,n} x^n$ and $g_k = \sum\limits_{n\in\mathbb{N}} g_{k,n} x^n$ with $f_{k,n}, g_{k,n} \in K$. Then, the equality (134) can be rewritten as

$$\sum_{k\in\mathbb{N}} \sum_{n\in\mathbb{N}} f_{k,n} x^n y^k = \sum_{k\in\mathbb{N}} \sum_{n\in\mathbb{N}} g_{k,n} x^n y^k.$$

Now, comparing coefficients in front of $x^n y^k$ in this equality, we obtain $f_{k,n} = g_{k,n}$ for each $k, n \in \mathbb{N}$. Therefore, $f_k = g_k$ for each $k \in \mathbb{N}$. This proves Proposition 3.15.2. □

Now, because of (132), we can apply Proposition 3.15.2 to $f_k = \dfrac{x^k}{\left(1-x\right)^{k+1}}$ and $g_k = \sum\limits_{n\in\mathbb{N}} \dbinom{n}{k} x^n$. Thus, we obtain the equality

$$\frac{x^k}{\left(1-x\right)^{k+1}} = \sum_{n\in\mathbb{N}} \binom{n}{k} x^n \qquad \text{for each } k \in \mathbb{N}.$$

This is an equality between **univariate** FPSs, even though we have obtained it by manipulating **bivariate** FPSs (i.e., FPSs in two variables x and y). As a homework exercise (Exercise A.2.15.1), you can prove this equality in a more elementary, univariate way. But the idea to introduce extra variables (in our case, in order to discover an equality) is highly useful in many situations (some of which we will see later in this course).

4. Integer partitions and q-binomial coefficients

We have previously counted compositions of an $n \in \mathbb{N}$. These are (roughly speaking) ways to write n as a sum of finitely many positive integers, where the order matters. For example, $3 = 3 = 2+1 = 1+2 = 1+1+1$, so 3 has 4 compositions. Formally, compositions are tuples of positive integers.

Now, let us disregard the order. There are two ways to make this rigorous: either we replace tuples by multisets, or we require the tuples to be weakly decreasing. These result in the same count, but we will use the 2nd way, just because tuples are easier to work with than multisets. This will lead to the notion of *integer partitions*.

4.1. Partition basics

The following definition is built in analogy to Definition 3.9.1:

Definition 4.1.1. **(a)** An *(integer) partition* means a (finite) weakly decreasing tuple of positive integers – i.e., a finite tuple $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ of positive integers such that $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m$.

Thus, partitions are the same as weakly decreasing compositions. Hence, the notions of *size* and *length* of a partition are automatically defined, since we have defined them for compositions (in Definition 3.9.1).

(b) The *parts* of a partition $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ are simply its entries $\lambda_1, \lambda_2, \ldots, \lambda_m$.

(c) Let $n \in \mathbb{Z}$. A *partition of n* means a partition whose size is n.

(d) Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. A *partition of n into k parts* is a partition whose size is n and whose length is k.

Example 4.1.2. The partitions of 5 are

$$(5), \quad (4,1), \quad (3,2), \quad (3,1,1), \quad (2,2,1), \quad (2,1,1,1), \quad (1,1,1,1,1).$$

Definition 4.1.3. **(a)** Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$. Then, we set

$$p_k(n) := (\text{\# of partitions of } n \text{ into } k \text{ parts}).$$

(b) Let $n \in \mathbb{Z}$. Then, we set

$$p(n) := (\text{\# of partitions of } n).$$

This is called the *n-th partition number*.

Example 4.1.4. Our above list of partitions of 5 reveals that

$$\begin{aligned}
p_0(5) &= 0; \\
p_1(5) &= 1; \\
p_2(5) &= 2; \\
p_3(5) &= 2; \\
p_4(5) &= 1; \\
p_5(5) &= 1; \\
p_k(5) &= 0 \qquad \text{for any } k > 5;
\end{aligned}$$

and finally $p(5) = 7$.

Here are the values of $p(n)$ for the first 15 nonnegative integers n:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$p(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135

.

The sequence $(p(0), p(1), p(2), \ldots)$ is remarkable for being an integer sequence that grows faster than polynomially, but still considerably slower than exponentially. (See (154) for an asymptotic expansion.) This not-too-fast growth (for instance, $p(100) = 190\,569\,292$ is far smaller than 2^{100}) makes integer partitions rather convenient for computer experiments.

We will next state some elementary properties of $p_k(n)$ and $p(n)$, but first we introduce a few very basic notations:

Definition 4.1.5. We will use the *Iverson bracket notation*: If $\mathcal{A}$ is a logical statement, then $[\mathcal{A}]$ means the *truth value* of $\mathcal{A}$; this is the integer $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false.} \end{cases}$

For example, $[2+2=4] = 1$ and $[2+2=5] = 0$.

Note that the Kronecker delta notation is a particular case of the Iverson bracket: We have

$$\delta_{i,j} = [i = j] \qquad \text{for any objects } i \text{ and } j.$$

Definition 4.1.6. Let a be a real number.

Then, $\lfloor a \rfloor$ (called the *floor* of a) means the largest integer that is $\leq a$.

Likewise, $\lceil a \rceil$ (called the *ceiling* of a) means the smallest integer that is $\geq a$.

For example, the number $\pi \approx 3.14$ satisfies $\lfloor \pi \rfloor = 3$ and $\lceil \pi \rceil = 4$ and $\lfloor -\pi \rfloor = -4$ and $\lceil -\pi \rceil = -3$. For another example, $\lfloor n \rfloor = \lceil n \rceil = n$ for each $n \in \mathbb{Z}$.

The following proposition collects various basic properties of the numbers introduced in Definition 4.1.3:

Proposition 4.1.7. Let $n \in \mathbb{Z}$ and $k \in \mathbb{N}$.

(a) We have $p_k(n) = 0$ whenever $n < 0$ and $k \in \mathbb{N}$.

(b) We have $p_k(n) = 0$ whenever $k > n$.

(c) We have $p_0(n) = [n = 0]$.

(d) We have $p_1(n) = [n > 0]$.

(e) We have $p_k(n) = p_k(n-k) + p_{k-1}(n-1)$ whenever $k > 0$.

(f) We have $p_2(n) = \lfloor n/2 \rfloor$ whenever $n \in \mathbb{N}$.

(g) We have $p(n) = p_0(n) + p_1(n) + \cdots + p_n(n)$ whenever $n \in \mathbb{N}$.

(h) We have $p(n) = 0$ whenever $n < 0$.

Proof of Proposition 4.1.7 (sketched). **(a)** The size of a partition is always nonnegative (being a sum of positive integers). Thus, a negative number n has no partitions whatsoever. Thus, $p_k(n) = 0$ whenever $n < 0$ and $k \in \mathbb{N}$.

(b) If $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a partition, then $\lambda_i \geq 1$ for each $i \in \{1, 2, \ldots, k\}$ (because a partition is a tuple of positive integers, i.e., of integers ≥ 1). Hence, if $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a partition of n into k parts, then

$$\begin{aligned} n &= \lambda_1 + \lambda_2 + \cdots + \lambda_k && \left(\text{since } (\lambda_1, \lambda_2, \ldots, \lambda_k) \text{ is a partition of } n\right) \\ &\geq \underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} && \left(\text{since } \lambda_i \geq 1 \text{ for each } i \in \{1, 2, \ldots, k\}\right) \\ &= k. \end{aligned}$$

Thus, a partition of n into k parts cannot satisfy $k > n$. Thus, no such partitions exist if $k > n$. In other words, $p_k(n) = 0$ if $k > n$.

(c) The integer 0 has a unique partition into 0 parts, namely the empty tuple $()$. A nonzero integer n cannot have any partitions into 0 parts, since the empty tuple has size $0 \neq n$. Thus, $p_0(n)$ equals 1 for $n = 0$ and equals 0 for $n \neq 0$. In other words, $p_0(n) = [n = 0]$.

(d) Any positive integer n has a unique partition into 1 part – namely, the 1-tuple (n). On the other hand, if n is not positive, then this 1-tuple is not a partition, so in this case n has no partition into 1 part. Thus, $p_1(n)$ equals 1 if n is positive and equals 0 otherwise. In other words, $p_1(n) = [n > 0]$.

(e) Assume that $k > 0$. We must prove that $p_k(n) = p_k(n-k) + p_{k-1}(n-1)$.

We consider all partitions of n into k parts. We classify these partitions into two types:

- *Type 1* consists of all partitions that have 1 as a part.
- *Type 2* consists of all partitions that don't.

For example, here are the partitions of 5 along with their types:

$$\underbrace{(4,1), \quad (3,1,1), \quad (2,2,1), \quad (2,1,1,1), \quad (1,1,1,1,1)}_{\text{Type 1}}, \quad \underbrace{(5), \quad (3,2)}_{\text{Type 2}}.$$

Let us count the type-1 partitions and the type-2 partitions separately.

Any type-1 partition has 1 as a part, therefore as its last part (because it is weakly decreasing). Hence, any type-1 partition has the form $(\lambda_1, \lambda_2, \ldots, \lambda_{k-1}, 1)$. If $(\lambda_1, \lambda_2, \ldots, \lambda_{k-1}, 1)$ is a type-1 partition (of n into k parts), then $(\lambda_1, \lambda_2, \ldots, \lambda_{k-1})$ is a partition of $n-1$ into $k-1$ parts. Thus, we have a map

$$\begin{gathered} \{\text{type-1 partitions of } n \text{ into } k \text{ parts}\} \to \{\text{partitions of } n-1 \text{ into } k-1 \text{ parts}\}, \\ (\lambda_1, \lambda_2, \ldots, \lambda_{k-1}, 1) \mapsto (\lambda_1, \lambda_2, \ldots, \lambda_{k-1}). \end{gathered}$$

This map is a bijection (since it has an inverse map, which simply inserts a 1 at the end of a partition). Thus, the bijection principle shows that

$$\begin{aligned}&(\text{\# of type-1 partitions of } n \text{ into } k \text{ parts})\\&=(\text{\# of partitions of } n-1 \text{ into } k-1 \text{ parts})=p_{k-1}(n-1)\end{aligned}$$

(by the definition of $p_{k-1}(n-1)$).

Now let us count type-2 partitions. A type-2 partition does not have 1 as a part; hence, all its parts are larger than 1 (because all its parts are positive integers), and therefore we can subtract 1 from each part and still have a partition in front of us. To be more specific: If $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a type-2 partition of n into k parts, then subtracting 1 from each of its parts produces the k-tuple $(\lambda_1 - 1, \lambda_2 - 1, \ldots, \lambda_k - 1)$, which is a partition of $n-k$ into k parts. Hence, we have a map

$$\begin{aligned}\{\text{type-2 partitions of } n \text{ into } k \text{ parts}\} &\to \{\text{partitions of } n-k \text{ into } k \text{ parts}\},\\(\lambda_1, \lambda_2, \ldots, \lambda_k) &\mapsto (\lambda_1 - 1, \lambda_2 - 1, \ldots, \lambda_k - 1).\end{aligned}$$

This map is a bijection (since it has an inverse map, which simply adds 1 to each entry of a partition). Thus, the bijection principle shows that

$$\begin{aligned}&(\text{\# of type-2 partitions of } n \text{ into } k \text{ parts})\\&=(\text{\# of partitions of } n-k \text{ into } k \text{ parts})=p_k(n-k)\end{aligned}$$

(by the definition of $p_k(n-k)$).

Since any partition of n into k parts is either type-1 or type-2 (but not both at the same time), we now have

$$\begin{aligned}&(\text{\# of partitions of } n \text{ into } k \text{ parts})\\&=\underbrace{(\text{\# of type-1 partitions of } n \text{ into } k \text{ parts})}_{=p_{k-1}(n-1)}+\underbrace{(\text{\# of type-2 partitions of } n \text{ into } k \text{ parts})}_{=p_k(n-k)}\\&=p_{k-1}(n-1)+p_k(n-k)=p_k(n-k)+p_{k-1}(n-1).\end{aligned}$$

Since the left hand side of this equality is $p_k(n)$, we thus have proved that $p_k(n) = p_k(n-k) + p_{k-1}(n-1)$.

(f) Let $n \in \mathbb{N}$. The partitions of n into 2 parts are

$$(n-1,1), \quad (n-2,2), \quad (n-3,3), \quad \ldots, \quad \left(\underbrace{n-\lfloor n/2\rfloor}_{=\lceil n/2\rceil}, \lfloor n/2\rfloor\right).$$

Thus there are $\lfloor n/2\rfloor$ of them. In other words, $p_2(n) = \lfloor n/2\rfloor$.

(g) Let $n \in \mathbb{N}$. Any partition of n must have k parts for some $k \in \mathbb{N}$. Thus,

$$\begin{aligned} p(n) &= \sum_{k\in\mathbb{N}} p_k(n) = \sum_{k=0}^{n} p_k(n) + \sum_{k=n+1}^{\infty} \underbrace{p_k(n)}_{\substack{=0 \\ \text{(by Proposition 4.1.7 \textbf{(b)})}}} \\ &= \sum_{k=0}^{n} p_k(n) = p_0(n) + p_1(n) + \cdots + p_n(n). \end{aligned}$$

(h) Same argument as for **(a)**. □

Proposition 4.1.7 **(e)** is a recursive formula that makes it not too hard to compute $p_k(n)$ for reasonably small values of n and k. Then, using Proposition 4.1.7 **(g)**, we can compute $p(n)$ from these $p_k(n)$'s. However, one might want a better, faster method.

To get there, let me first express the generating function of the numbers $p(n)$:

Theorem 4.1.8. In the FPS ring $\mathbb{Z}[[x]]$, we have

$$\sum_{n\in\mathbb{N}} p(n)\, x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

(The product on the right hand side is well-defined, since multiplying a FPS by $\frac{1}{1-x^k}$ does not affect its first k coefficients.)

Example 4.1.9. Let us check the above equality "up to x^5", i.e., let us compare the coefficients of x^i for $i < 5$. (In doing so, we can ignore all powers of x higher than x^4.) We have

$$\begin{aligned} \prod_{k=1}^{\infty} \frac{1}{1-x^k} &= \frac{1}{1-x^1} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdot \frac{1}{1-x^4} \cdot \cdots \\ &= \quad \left(1 + x + x^2 + x^3 + x^4 + \cdots\right) \\ &\quad \cdot \left(1 + x^2 + x^4 + \cdots\right) \\ &\quad \cdot \left(1 + x^3 + \cdots\right) \\ &\quad \cdot \left(1 + x^4 + \cdots\right) \\ &\quad \cdot (1 + \cdots) \\ &\quad \cdot (1 + \cdots) \\ &\quad \cdots \\ &= 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots \\ &= p(0) + p(1)\,x + p(2)\,x^2 + p(3)\,x^3 + p(4)\,x^4 + \cdots. \end{aligned}$$

Proof of Theorem 4.1.8. We have

$$\begin{aligned}
&\prod_{k=1}^{\infty} \underbrace{\frac{1}{1-x^k}}_{=1+x^k+x^{2k}+x^{3k}+\cdots} \\
&= \prod_{k=1}^{\infty} \underbrace{\left(1+x^k+x^{2k}+x^{3k}+\cdots\right)}_{=\sum\limits_{u\in\mathbb{N}} x^{ku}} = \prod_{k=1}^{\infty} \sum_{u\in\mathbb{N}} x^{ku} \\
&= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ is} \\ \text{essentially finite}}} x^{1u_1}x^{2u_2}x^{3u_3}\cdots \qquad \left(\begin{array}{c}\text{here, we expanded the product} \\ \text{using Proposition 3.11.25}\end{array}\right) \\
&= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ is} \\ \text{essentially finite}}} x^{1u_1+2u_2+3u_3+\cdots} \\
&= \sum_{n\in\mathbb{N}} |Q_n|\, x^n,
\end{aligned}$$

where

$$Q_n = \{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ essentially finite } \mid 1u_1+2u_2+3u_3+\cdots = n\}.$$

Thus, it will suffice to show that

$$|Q_n| = p(n) \qquad \text{for each } n\in\mathbb{N}.$$

Let us fix $n \in \mathbb{N}$. We want to construct a bijection from Q_n to {partitions of n}. Here is how to do this: For any $(u_1,u_2,u_3,\ldots)\in Q_n$, define a partition

$$\begin{aligned}
\pi(u_1,u_2,u_3,\ldots) &:= (\text{the partition that contains each } i \text{ exactly } u_i \text{ times}) \\
&= \left(\ldots, \underbrace{3,3,\ldots,3}_{u_3 \text{ times}}, \underbrace{2,2,\ldots,2}_{u_2 \text{ times}}, \underbrace{1,1,\ldots,1}_{u_1 \text{ times}}\right).
\end{aligned}$$

This is a partition of n, since its size is $1u_1+2u_2+3u_3+\cdots = n$ (because $(u_1,u_2,u_3,\ldots)\in Q_n$). Thus, we have defined a partition $\pi(u_1,u_2,u_3,\ldots)$ of n for each $(u_1,u_2,u_3,\ldots)\in Q_n$. In other words, we have defined a map

$$\pi : Q_n \to \{\text{partitions of } n\}.$$

It remains to show that this map π is a bijection. We define a map

$$\rho : \{\text{partitions of } n\} \to Q_n$$

that sends each partition λ of n to the sequence

$$(\#\text{ of 1's in } \lambda,\ \#\text{ of 2's in } \lambda,\ \#\text{ of 3's in } \lambda,\ \ldots)\in Q_n$$

(this is indeed a sequence in Q_n, since

$$\sum_{i=1}^{\infty} i\left(\#\text{ of } i\text{'s in } \lambda\right) = \left(\text{the sum of all entries of } \lambda\right) = \left|\lambda\right| = n$$

because λ is a partition of n). It is now easy to check that the maps π and ρ are mutually inverse, so that π is a bijection. The bijection principle therefore yields $\left|Q_n\right| = \left(\#\text{ of partitions of } n\right) = p\left(n\right)$; but this is precisely what we wanted to show. The proof of Theorem 4.1.8 is thus complete. □

Theorem 4.1.8 has a "finite" analogue (finite in the sense that the product $\prod\limits_{k=1}^{\infty} \dfrac{1}{1-x^k}$ is replaced by a finite product; the FPSs are still infinite):

Theorem 4.1.10. Let $m \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $p_{\text{parts}\leq m}\left(n\right)$ be the # of partitions λ of n such that all parts of λ are $\leq m$. Then,

$$\sum_{n\in\mathbb{N}} p_{\text{parts}\leq m}\left(n\right) x^n = \prod_{k=1}^{m} \frac{1}{1-x^k}.$$

Proof of Theorem 4.1.10. This proof is mostly analogous to the above proof of Theorem 4.1.8, and to some extent even simpler because it uses m-tuples instead of infinite sequences.

We have

$$\begin{aligned}
&\prod_{k=1}^{m} \underbrace{\frac{1}{1-x^k}}_{=1+x^k+x^{2k}+x^{3k}+\cdots} \\
&= \prod_{k=1}^{m} \underbrace{\left(1+x^k+x^{2k}+x^{3k}+\cdots\right)}_{=\sum\limits_{u\in\mathbb{N}} x^{ku}} = \prod_{k=1}^{m} \sum_{u\in\mathbb{N}} x^{ku} \\
&= \sum_{(u_1,u_2,\ldots,u_m)\in\mathbb{N}^m} x^{1u_1}x^{2u_2}\cdots x^{mu_m} \qquad \left(\begin{array}{c}\text{here, we expanded the product}\\ \text{using Proposition 3.11.23}\end{array}\right) \\
&= \sum_{(u_1,u_2,\ldots,u_m)\in\mathbb{N}^m} x^{1u_1+2u_2+\cdots+mu_m} = \sum_{n\in\mathbb{N}} \left|Q_n\right| x^n,
\end{aligned}$$

where

$$Q_n = \left\{\left(u_1,u_2,\ldots,u_m\right) \in \mathbb{N}^m \ \mid \ 1u_1+2u_2+\cdots+mu_m = n\right\}.$$

Thus, it will suffice to show that

$$\left|Q_n\right| = p_{\text{parts}\leq m}\left(n\right) \qquad \text{for each } n \in \mathbb{N}.$$

Let us fix $n \in \mathbb{N}$. We want to construct a bijection from Q_n to the set $\{$partitions λ of n such that all parts of λ are $\leq m\}$.

Here is how to do this: For any $(u_1, u_2, \ldots, u_m) \in Q_n$, define a partition

$$\begin{aligned}\pi\left(u_1, u_2, \ldots, u_m\right) &:= (\text{the partition that contains each } i \text{ exactly } u_i \text{ times})\\ &= \left(\underbrace{m, m, \ldots, m}_{u_m \text{ times}}, \ldots, \underbrace{2, 2, \ldots, 2}_{u_2 \text{ times}}, \underbrace{1, 1, \ldots, 1}_{u_1 \text{ times}}\right).\end{aligned}$$

Thus, we have defined a map

$$\pi : Q_n \to \{\text{partitions } \lambda \text{ of } n \text{ such that all parts of } \lambda \text{ are } \leq m\}.$$

It is easy to see that this map π is a bijection[43]. The bijection principle therefore yields

$$|Q_n| = (\text{\# of partitions } \lambda \text{ of } n \text{ such that all parts of } \lambda \text{ are } \leq m) = p_{\text{parts}\leq m}(n);$$

but this is precisely what we wanted to show. The proof of Theorem 4.1.10 is thus complete. □

Next, we shall state a result of Euler that we have already discovered in a different language.

Definition 4.1.11. Let $n \in \mathbb{Z}$.

(a) A *partition of n into odd parts* means a partition of n whose all parts are odd.

(b) A *partition of n into distinct parts* means a partition of n whose parts are distinct.

(c) Let

$$\begin{aligned}p_{\text{odd}}(n) &:= (\text{\# of partitions of } n \text{ into odd parts}) \qquad \text{and}\\ p_{\text{dist}}(n) &:= (\text{\# of partitions of } n \text{ into distinct parts}).\end{aligned}$$

Example 4.1.12. We have

$$\begin{aligned}p_{\text{odd}}(7) &= |\{(7),\ (5,1,1),\ (3,3,1),\ (3,1,1,1,1),\ (1,1,1,1,1,1,1)\}| = 5;\\ p_{\text{dist}}(7) &= |\{(7),\ (6,1),\ (5,2),\ (4,3),\ (4,2,1)\}| = 5.\end{aligned}$$

Theorem 4.1.13 (Euler's odd-distinct identity)**.** We have $p_{\text{odd}}(n) = p_{\text{dist}}(n)$ for each $n \in \mathbb{N}$.

[43] The argument is analogous to the one used in the proof of Theorem 4.1.8.

We have already encountered this theorem before (as Theorem 3.11.30, albeit in less precise language), and we have proved it using the generating function identity

$$\prod_{i>0}\left(1-x^{2i-1}\right)^{-1}=\prod_{k>0}\left(1+x^{k}\right).$$

Let me outline a different, bijective proof.

Second proof of Theorem 4.1.13 (sketched). Let $n \in \mathbb{N}$. We want to construct a bijection

$$A : \{\text{partitions of } n \text{ into odd parts}\} \to \{\text{partitions of } n \text{ into distinct parts}\}.$$

We shall do this as follows: Given a partition λ of n into odd parts, we repeatedly merge pairs of equal parts in λ until no more equal parts appear. The final result will be $A(\lambda)$. Here are two examples:

- To compute $A(5,5,3,1,1,1)$, we compute[44]

  $$\left(\underline{5,5},3,1,1,1\right) \to \left(10,3,1,\underline{1,1}\right) \to (10,3,2,1).$$

  Thus, $A(5,5,3,1,1,1) = (10,3,2,1)$.

- To compute $A(5,3,1,1,1,1)$, we compute

  $$\left(5,3,1,1,\underline{1,1}\right) \to \left(5,3,2,\underline{1,1}\right) \to \left(5,3,\underline{2,2}\right) \to (5,4,3).$$

  Thus, $A(5,3,1,1,1,1) = (5,4,3)$.

Why is this map A well-defined? We only specified the sort of steps we are allowed to take when computing $A(\lambda)$; however, there is often a choice involved in taking these steps (since there are often several pairs of equal parts).[45] So we have specified a non-deterministic algorithm. Why is the resulting partition independent of the choices we make?

One way to prove this is using the *diamond lemma*, which is a general tool for proving that certain non-deterministic algorithms have unique final outcomes (independent of the choices taken). We will hopefully learn more about it later on.

For the map A, we can also proceed differently, by analyzing the algorithm that we used to define A. Namely, we observe what is really going on when we are merging equal parts. Let us say our original partition λ has p many 1s.

[44] The two entries underlined are the two equal entries that are going to get merged in the next step. Note that there are usually several candidates, and we just pick one pair at will.

[45] For example, we could have also computed $A(5,5,3,1,1,1)$ as follows:

$$\left(5,5,3,\underline{1},1,\underline{1}\right) \to \left(\underline{5,5},3,2,1\right) \to (10,3,2,1).$$

Let us first merge them in pairs, so that we get $\lfloor p/2 \rfloor$ many 2s and maybe one single 1. Then, let us merge the 2s in pairs, so that we get $\lfloor \lfloor p/2 \rfloor /2 \rfloor$ many 4s, maybe a single 2, and maybe a single 1. Proceed until no more than one 1, no more than one 2, no more than one 4, no more than one 8, and so on remain. This clears out any duplicate parts of the form 2^k. Next do the same with parts of the form $3 \cdot 2^k$ (that is, with parts equal to 3, 6, 12, 24, and so on), then with parts of the form $5 \cdot 2^k$, and so on.

The nice thing about this way of proceeding is that we can explicitly describe the final outcome. Indeed, if the original partition λ (a partition of n into odd parts) contains an odd part k precisely m many times, and if the binary representation of m is $m = (m_i m_{i-1} \cdots m_1 m_0)_2$ (that is, if $m_0, m_1, \ldots, m_i \in \{0, 1\}$ satisfy $m = \sum\limits_{j=0}^{i} m_j 2^j$), then the partition $A(\lambda)$ will contain the number $2^0 k$ exactly m_0 times, the number $2^1 k$ exactly m_1 times, the number $2^2 k$ exactly m_2 times, and so on. Since the binary digits $m_0, m_1, \ldots, m_i$ are all ≤ 1, this partition $A(\lambda)$ will therefore not contain any number more than once, i.e., it will be a partition into distinct parts.

It is not hard to check that this map A is indeed a bijection. Indeed, in order to see this, we construct a map B that will turn out to be its inverse. Here, we start with a partition λ of n into distinct parts. Let us represent each part of this partition in the form $k \cdot 2^i$ for some odd $k \geq 1$ and some integer $i \geq 0$. (Recall that any positive integer can be represented uniquely in this form.) Now, replace this part $k \cdot 2^i$ by 2^i many k's. The resulting partition (once all parts have been replaced) will usually have many equal parts, but all its parts are odd. We define $B(\lambda)$ to be this resulting partition. Alternatively, $B(\lambda)$ can also be constructed step-by-step by a non-deterministic algorithm: Starting with λ, keep "breaking even parts into halves" (i.e., whenever you see an even part m, replace it by two parts $\dfrac{m}{2}$ and $\dfrac{m}{2}$), until no even parts remain any more. The result is $B(\lambda)$. It is not hard to see that both descriptions of $B(\lambda)$ describe the same partition. It is furthermore easy to see that this map B is indeed an inverse of A, so that A is indeed a bijection. Thus, the bijection principle yields

$$|\{\text{partitions of } n \text{ into odd parts}\}| = |\{\text{partitions of } n \text{ into distinct parts}\}| .$$

In other words, $p_{\text{odd}}(n) = p_{\text{dist}}(n)$. This proves Theorem 4.1.13. □

Here is another situation in which two kinds of partitions are equinumerous:

Proposition 4.1.14. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$p_k(n) = (\# \text{ of partitions of } n \text{ whose largest part is } k) .$$

Here and in the following, we use the following convention:

Convention 4.1.15. We agree to say that the largest part of the empty partition $()$ is 0 (even though this partition has no parts).

Example 4.1.16. For $n = 4$ and $k = 3$, we have

$$p_k(n) = p_3(4) = 1 \qquad \text{(due to the partition } (2,1,1))$$

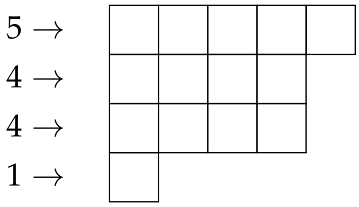
and

$$\begin{aligned} &(\text{\# of partitions of } n \text{ whose largest part is } k) \\ &= (\text{\# of partitions of } 4 \text{ whose largest part is } 3) \\ &= 1 \qquad (\text{due to the partition } (3,1)). \end{aligned}$$

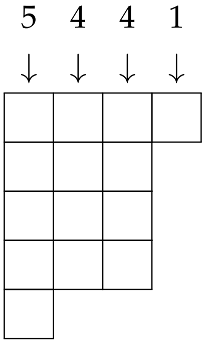
Thus, Proposition 4.1.14 holds for $n = 4$ and $k = 3$.

Proof of Proposition 4.1.14 (sketched). We do a "proof by picture" (it can be made rigorous – see Exercise A.3.1.1 for this). We pick $n = 14$ and $k = 4$ for example, and we start with the partition $\lambda = (5,4,4,1)$ of n into k parts.

We draw a table of k left-aligned rows, where the length of each row equals the corresponding part of λ (that is, the i-th row from the top has λ_i boxes, where $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$):



Now, let us flip this table across the "main diagonal" (i.e., the diagonal that goes from the top-left corner to the bottom-right corner)[46]:



The lengths of the rows of the resulting table again form a partition of n. (In our case, this new partition is $(4,3,3,3,1)$.) Moreover, the largest part of this new partition is k (because the original table had k rows, so the flipped table

[46] This kind of flip is precisely how you would transpose a matrix.

has k columns, and this means that its top row has k boxes). This procedure (i.e., turning a partition into a table, then flipping the table across the "main diagonal", and then reading the lengths of the rows of the resulting table again as a partition) therefore gives a map from

$$\{\text{partitions of } n \text{ into } k \text{ parts}\}$$

to

$$\{\text{partitions of } n \text{ whose largest part is } k\}.$$

Moreover, this map is a bijection (indeed, its inverse can be effected in the exact same way, by flipping the table). This bijection is called *conjugation* of partitions, and will be studied in more detail later.

Here are some pointers to how this proof can be formalized (see Exercise A.3.1.1 for much more): For any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we define the *Young diagram* of λ to be the set

$$Y(\lambda) := \left\{(i,j) \in \mathbb{Z}^2 \mid 1 \leq i \leq k \text{ and } 1 \leq j \leq \lambda_i\right\}.$$

This Young diagram is precisely the table that we drew above, as long as we agree to identify each pair $(i,j) \in Y(\lambda)$ with the box in row i and column j. Now, the *conjugate* of the partition λ is the partition λ^t uniquely determined by

$$Y\left(\lambda^t\right) = \operatorname{flip}(Y(\lambda)) = \{(j,i) \mid (i,j) \in Y(\lambda)\}.$$

Explicitly, λ^t can be defined by $\lambda^t = \left(\mu_1, \mu_2, \ldots, \mu_p\right)$, where p is the largest part of λ and where

$$\mu_i = (\# \text{ of parts of } \lambda \text{ that are } \geq i) \qquad \text{for each } i \in \{1, 2, \ldots, p\}.$$

(This conjugate λ^t is also often called λ'.) Now, it is not hard to show that $\left|\lambda^t\right| = |\lambda|$ and $\left(\lambda^t\right)^t = \lambda$ for each partition λ, and that the largest part of λ^t equals the length of λ. Using these observations (which are proved in Exercise A.3.1.1), we see that the map

$$\{\text{partitions of } n \text{ into } k \text{ parts}\} \to \{\text{partitions of } n \text{ whose largest part is } k\},$$
$$\lambda \mapsto \lambda^t$$

is well-defined and is a bijection; thus, the above proof of Proposition 4.1.14 becomes fully rigorous. □

The word "Young" in "Young diagram" (and, later, "Young tableau") does not imply any novelty (Young diagrams have been around in some form or another since the 19th century – if often in the superficially different guise of "Ferrers diagrams"), but rather honors Alfred Young, who built up the representation theory of symmetric groups (and significantly forwarded invariant theory) using these objects.

Corollary 4.1.17. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Then,

$$\begin{aligned} & p_0(n) + p_1(n) + \cdots + p_k(n) \\ & = (\text{\# of partitions of } n \text{ whose largest part is } \leq k). \end{aligned}$$

Proof of Corollary 4.1.17. We have

$$\begin{aligned} & p_0(n) + p_1(n) + \cdots + p_k(n) \\ & = \sum_{i=0}^{k} \underbrace{p_i(n)}_{\substack{=(\text{\# of partitions of } n \text{ whose largest part is } i) \\ \text{(by Proposition 4.1.14,} \\ \text{applied to } i \text{ instead of } k)}} \\ & = \sum_{i=0}^{k} (\text{\# of partitions of } n \text{ whose largest part is } i) \\ & = (\text{\# of partitions of } n \text{ whose largest part is } \leq k). \end{aligned}$$

This proves Corollary 4.1.17. □

Corollary 4.1.17 leads to yet another FPS identity:

Theorem 4.1.18. Let $m \in \mathbb{N}$. Then,

$$\sum_{n \in \mathbb{N}} (p_0(n) + p_1(n) + \cdots + p_m(n)) x^n = \prod_{k=1}^{m} \frac{1}{1 - x^k}.$$

Proof of Theorem 4.1.18. For each $n \in \mathbb{N}$, we have

$$\begin{aligned} & p_0(n) + p_1(n) + \cdots + p_m(n) \\ & = (\text{\# of partitions of } n \text{ whose largest part is } \leq m) \qquad \text{(by Corollary 4.1.17)} \\ & = (\text{\# of partitions of } n \text{ whose all parts are } \leq m) \\ & \qquad \left(\begin{array}{c} \text{because the condition ``the largest part is } \leq m\text{'' for a} \\ \text{partition is clearly equivalent to ``all parts are } \leq m\text{''} \end{array} \right) \\ & = p_{\text{parts} \leq m}(n), \end{aligned}$$

where $p_{\text{parts} \leq m}(n)$ is defined as in Theorem 4.1.10. Hence,

$$\sum_{n \in \mathbb{N}} \underbrace{(p_0(n) + p_1(n) + \cdots + p_m(n))}_{= p_{\text{parts} \leq m}(n)} x^n = \sum_{n \in \mathbb{N}} p_{\text{parts} \leq m}(n) x^n = \prod_{k=1}^{m} \frac{1}{1 - x^k}$$

(by Theorem 4.1.10). This proves Theorem 4.1.18. □

4.2. Euler's pentagonal number theorem

The following definition looks somewhat quaint; why define a notation for a specific quadratic function?

Definition 4.2.1. For any $k \in \mathbb{Z}$, define a nonnegative integer $w_k \in \mathbb{N}$ by

$$w_k = \frac{(3k-1)\,k}{2}.$$

This is called the *k-th pentagonal number*.

Here is a table of these pentagonal numbers:

k	$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	4	5	$\cdots$
w_k	$\cdots$	40	26	15	7	2	0	1	5	12	22	35	$\cdots$

.

Note that w_k really is a nonnegative integer for any $k \in \mathbb{Z}$ (check this!). The name "pentagonal numbers" is historically motivated (see the Wikipedia page for details); the only thing we need to know about them (beside their definition) is the fact that they are nonnegative integers and grow quadratically with n in both directions (i.e., when $n \to \infty$ and when $n \to -\infty$). The latter fact ensures that the infinite sum $\sum\limits_{k\in\mathbb{Z}} (-1)^k x^{w_k}$ is a well-defined FPS in $\mathbb{Z}[[x]]$. Rather surprisingly, this infinite sum coincides with a particularly simple infinite product:

Theorem 4.2.2 (Euler's pentagonal number theorem)**.** We have

$$\prod_{k=1}^{\infty} \left(1 - x^k\right) = \sum_{k\in\mathbb{Z}} (-1)^k x^{w_k}.$$

Let us write this out concretely:

$$\begin{aligned}
&\prod_{k=1}^{\infty} \left(1 - x^k\right) \\
&= \sum_{k\in\mathbb{Z}} (-1)^k x^{w_k} \\
&= \cdots + x^{w_{-4}} - x^{w_{-3}} + x^{w_{-2}} - x^{w_{-1}} + x^{w_0} - x^{w_1} + x^{w_2} - x^{w_3} + x^{w_4} - x^{w_5} \pm \cdots \\
&= \cdots + x^{26} - x^{15} + x^7 - x^2 + 1 - x + x^5 - x^{12} + x^{22} - x^{35} \pm \cdots \\
&= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} \pm \cdots .
\end{aligned}$$

We will prove Theorem 4.2.2 in the next section (as a particular case of Jacobi's Triple Product Identity).[47] First, let us use it to derive the following recursive formula for the partition numbers $p(n)$:

[47] See [Bell06] for the history of Theorem 4.2.2.

Corollary 4.2.3. For each positive integer n, we have

$$\begin{aligned} p\left(n\right) &= \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^{k-1} p\left(n-w_k\right) \\ &= p\left(n-1\right)+p\left(n-2\right)-p\left(n-5\right)-p\left(n-7\right) \\ &\qquad + p\left(n-12\right)+p\left(n-15\right)-p\left(n-22\right)-p\left(n-26\right)\pm\cdots . \end{aligned}$$

Proof of Corollary 4.2.3 using Theorem 4.2.2. We have

$$\sum_{m\in\mathbb{N}} p\left(m\right)x^m = \sum_{n\in\mathbb{N}} p\left(n\right)x^n = \prod_{k=1}^{\infty}\frac{1}{1-x^k}$$

(by Theorem 4.1.8) and

$$\sum_{k\in\mathbb{Z}} \left(-1\right)^k x^{w_k} = \prod_{k=1}^{\infty}\left(1-x^k\right)$$

(by Theorem 4.2.2). Multiplying these two equalities, we obtain

$$\begin{aligned} \left(\sum_{m\in\mathbb{N}} p\left(m\right)x^m\right)\cdot\left(\sum_{k\in\mathbb{Z}}\left(-1\right)^k x^{w_k}\right) &= \left(\prod_{k=1}^{\infty}\frac{1}{1-x^k}\right)\cdot\left(\prod_{k=1}^{\infty}\left(1-x^k\right)\right) \\ &= \prod_{k=1}^{\infty}\underbrace{\left(\frac{1}{1-x^k}\cdot\left(1-x^k\right)\right)}_{=1} \\ &= 1. \end{aligned} \tag{135}$$

Now, let us fix a positive integer n. We shall compare the x^n-coefficients on both sides of (4.2.3).

The x^n-coefficient on the left hand side of (4.2.3) is

$$\begin{aligned}
\sum_{\substack{m\in\mathbb{N};\\ k\in\mathbb{Z};\\ m+w_k=n}} p\left(m\right)\cdot\left(-1\right)^k &= \sum_{\substack{k\in\mathbb{Z};\\ n-w_k\geq 0}} p\left(n-w_k\right)\cdot\left(-1\right)^k \\
&\qquad \left(\begin{array}{c}\text{here, we have replaced } m \text{ by } n-w_k \\ \text{in the sum, since the condition } m+w_k=n \\ \text{forces } m \text{ to be } n-w_k\end{array}\right) \\
&= \sum_{k\in\mathbb{Z}} p\left(n-w_k\right)\cdot\left(-1\right)^k \\
&\qquad \left(\begin{array}{c}\text{here, we have extended the range of} \\ \text{summation; this does not change the sum,} \\ \text{since } p\left(n-w_k\right)=0 \text{ whenever } n-w_k<0\end{array}\right) \\
&= \sum_{k\in\mathbb{Z}} \left(-1\right)^k p\left(n-w_k\right) \\
&= \underbrace{\left(-1\right)^0}_{=1} p\left(n-\underbrace{w_0}_{=0}\right) + \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right) \\
&= p\left(n\right) + \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right).
\end{aligned}$$

But the x^n-coefficient on the right hand side of (4.2.3) is 0 (since n is positive). Hence, comparing the coefficients yields

$$p\left(n\right) + \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right) = 0.$$

Solving this for $p\left(n\right)$, we find

$$p\left(n\right) = -\sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right) = \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^{k-1} p\left(n-w_k\right).$$

Corollary 4.2.3 is thus proved. □

4.3. Jacobi's triple product identity

Instead of proving Theorem 4.2.2 directly, we shall prove a stronger result: *Jacobi's triple product identity*. This identity can be stated as follows:

$$\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right) = \sum_{\ell\in\mathbb{Z}} q^{\ell^2}z^{\ell}. \tag{136}$$

What are q and z here? It appears that (136) should be an identity between multivariate Laurent series (in the indeterminates q and z), but I have never defined such a thing[48]. However, it is not hard to see that any negative power of z in (136) is "compensated" by a positive power of q. For example, the $q^{2n-1}z^{-1}$ term on the left hand side will always have total degree ≥ 0, and so will the $q^{\ell^2}z^{\ell}$ term on the right hand side. So this is not as bad as Laurent series in general.

One natural ring in which the identity (136) can be placed is $(\mathbb{Z}[z^{\pm}])[[q]]$ (that is, the ring of FPSs in the indeterminate q whose coefficients are Laurent polynomials over $\mathbb{Z}$ in the indeterminate z). In other words, we state the following:

Theorem 4.3.1 (Jacobi's triple product identity, take 1)**.** In the ring $(\mathbb{Z}[z^{\pm}])[[q]]$, we have

$$\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right)=\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}.$$

However, we aren't just planning to view this identity as a formal identity between power series; instead, we will later evaluate both sides at certain powers of another indeterminate x (i.e., we will set $q = x^a$ and $z = x^b$ for some positive integers a and b). Alas, this is not an operation defined on the whole ring $(\mathbb{Z}[z^{\pm}])[[q]]$. For example, setting $q = x$ and $z = x$ in the sum $\sum\limits_{\ell\in\mathbb{Z}} q^{\ell}z^{-\ell} \in (\mathbb{Z}[z^{\pm}])[[q]]$ yields the nonsensical sum $\sum\limits_{\ell\in\mathbb{Z}} x^{\ell}x^{-\ell} = \sum\limits_{\ell\in\mathbb{Z}} 1$.

Thus, Theorem 4.3.1 is not a version of Jacobi's triple product identity that we can use for our purposes. Instead, let us interpret the identity (136) in a different way: Instead of treating q and z as indeterminates, I will set them to be powers of a single indeterminate x (more precisely, scalar multiples of such powers). This leads us to the following version of the identity:

Theorem 4.3.2 (Jacobi's triple product identity, take 2)**.** Let a and b be two integers such that $a > 0$ and $a \geq |b|$. Let $u, v \in \mathbb{Q}$ be rational numbers with $v \neq 0$. In the ring $\mathbb{Q}((x))$, set $q = ux^a$ and $z = vx^b$. Then,

$$\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right)=\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}.$$

Before we start proving this theorem, let us check that the infinite product on its left hand side and the infinite sum on its right are well-defined:

[48] Multivariate Laurent series can indeed be defined, but this is not as easy as the univariate case and involves some choices. See [ApaKau13] for details.

- The infinite product is

$$\begin{aligned}&\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right)\\&=\prod_{n>0}\left(\left(1+\left(ux^{a}\right)^{2n-1}\left(vx^{b}\right)\right)\left(1+\left(ux^{a}\right)^{2n-1}\left(vx^{b}\right)^{-1}\right)\left(1-\left(ux^{a}\right)^{2n}\right)\right)\\&=\prod_{n>0}\left(\left(1+u^{2n-1}vx^{(2n-1)a+b}\right)\left(1+u^{2n-1}v^{-1}x^{(2n-1)a-b}\right)\left(1-u^{2n}x^{2na}\right)\right).\end{aligned}$$

  All factors in this product belong to the ring $\mathbb{Q}[[x]]$ (not just to $\mathbb{Q}((x))$), since the exponents $(2n-1)a+b$ and $(2n-1)a-b$ and $2na$ are always nonnegative for any $n>0$ (indeed, for any $n>0$, we have $\underbrace{(2n-1)}_{\geq 1}\underbrace{a}_{\geq |b|}+b\geq |b|+b\geq 0$ and $\underbrace{(2n-1)}_{\geq 1}\underbrace{a}_{\geq |b|}-b\geq |b|-b\geq 0$ and $2n\underbrace{a}_{>0}>0$). Moreover, this product is multipliable, because

  - $(2n-1)a+b$ grows linearly when $n\to\infty$ (since $a>0$);
  - $(2n-1)a-b$ grows linearly when $n\to\infty$ (since $a>0$);
  - $2na$ grows linearly when $n\to\infty$ (since $a>0$).

  Thus, the infinite product is well-defined.

- The infinite sum is

$$\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}=\sum_{\ell\in\mathbb{Z}}\left(ux^{a}\right)^{\ell^2}\left(vx^{b}\right)^{\ell}=\sum_{\ell\in\mathbb{Z}}u^{\ell^2}v^{\ell}x^{a\ell^2+b\ell}.$$

  All addends in this sum belong to the ring $\mathbb{Q}[[x]]$ (not just to $\mathbb{Q}((x))$), since the exponent $a\ell^2+b\ell$ is always nonnegative for any $\ell\in\mathbb{Z}$ (indeed, we have $\underbrace{a}_{\geq |b|}\underbrace{\ell^2}_{=|\ell|^2}+\underbrace{b\ell}_{\geq -|b\ell|=-|b|\cdot|\ell|}\geq |b|\cdot|\ell|^2-|b|\cdot|\ell|=\underbrace{|b|}_{\geq 0}\cdot\underbrace{|\ell|\cdot(|\ell|-1)}_{\geq 0}\geq 0$ for any $\ell\in\mathbb{Z}$). Moreover, this sum is summable, because $a\ell^2+b\ell$ grows quadratically when $\ell\to+\infty$ or $\ell\to-\infty$ (since $a>0$).

We will give a proof of Jacobi's triple product identity that works equally for both versions of it (Theorem 4.3.1 and Theorem 4.3.2). But first, let us see how it yields Euler's pentagonal number theorem as a particular case.

Proof of Theorem 4.2.2 using Theorem 4.3.2. Set $q=x^3$ and $z=-x$ in Theorem 4.3.2. (This means that we apply Theorem 4.3.2 to $a=3$ and $b=1$ and $u=1$ and $v=-1$). We get

$$\begin{aligned}&\prod_{n>0}\left(\left(1+\left(x^3\right)^{2n-1}(-x)\right)\left(1+\left(x^3\right)^{2n-1}(-x)^{-1}\right)\left(1-\left(x^3\right)^{2n}\right)\right)\\&=\sum_{\ell\in\mathbb{Z}}\left(x^3\right)^{\ell^2}(-x)^{\ell}.\end{aligned}\qquad(137)$$

The left hand side of this equality simplifies as follows:

$$\begin{aligned}
&\prod_{n>0}\left(\left(1+\underbrace{\left(x^3\right)^{2n-1}(-x)}_{\substack{=-x^{3(2n-1)+1}\\ =-x^{6n-2}}}\right)\left(1+\underbrace{\left(x^3\right)^{2n-1}(-x)^{-1}}_{\substack{=-x^{3(2n-1)-1}\\ =-x^{6n-4}}}\right)\left(1-\underbrace{\left(x^3\right)^{2n}}_{=x^{6n}}\right)\right)\\
&=\prod_{n>0}\left(\left(1-\underbrace{x^{6n-2}}_{=(x^2)^{3n-1}}\right)\left(1-\underbrace{x^{6n-4}}_{=(x^2)^{3n-2}}\right)\left(1-\underbrace{x^{6n}}_{=(x^2)^{3n}}\right)\right)\\
&=\prod_{n>0}\left(\left(1-\left(x^2\right)^{3n-1}\right)\left(1-\left(x^2\right)^{3n-2}\right)\left(1-\left(x^2\right)^{3n}\right)\right)\\
&=\prod_{k>0}\left(1-\left(x^2\right)^k\right),
\end{aligned}$$

since each positive integer k can be uniquely represented as $3n-1$ or $3n-2$ or $3n$ for some positive integer n.

Comparing this with (137), we obtain

$$\begin{aligned}
&\prod_{k>0}\left(1-\left(x^2\right)^k\right)\\
&=\sum_{\ell\in\mathbb{Z}}\underbrace{\left(x^3\right)^{\ell^2}(-x)^{\ell}}_{=(-1)^{\ell}x^{3\ell^2-\ell}}=\sum_{\ell\in\mathbb{Z}}(-1)^{\ell}\underbrace{x^{3\ell^2-\ell}}_{\substack{=x^{2w_\ell}\\ \text{(since } 3\ell^2-\ell=(3\ell-1)\ell=2w_\ell\\ \text{(because } w_\ell \text{ is defined}\\ \text{as } (3\ell-1)\ell/2))}}=\sum_{\ell\in\mathbb{Z}}(-1)^{\ell}\underbrace{x^{2w_\ell}}_{=(x^2)^{w_\ell}}\\
&=\sum_{\ell\in\mathbb{Z}}(-1)^{\ell}\left(x^2\right)^{w_\ell}=\sum_{k\in\mathbb{Z}}(-1)^{k}\left(x^2\right)^{w_k}.
\end{aligned}\tag{138}$$

Now, let us "substitute x for x^2" in this equality (see below for how this works). As a result, we obtain

$$\prod_{k>0}\left(1-x^k\right)=\sum_{k\in\mathbb{Z}}(-1)^k x^{w_k}.$$

This is Euler's pentagonal number theorem (Theorem 4.2.2). □

What did I mean by "substituting x for x^2"? I meant using the following simple fact:

Lemma 4.3.3. Let K be a commutative ring. Let f and g be two FPSs in $K[[x]]$. Assume that $f\left[x^2\right]=g\left[x^2\right]$. Then, $f=g$.

Proof. This is easy: Write f and g as $f = \sum_{n\in\mathbb{N}} f_n x^n$ and $g = \sum_{n\in\mathbb{N}} g_n x^n$ where $f_0, f_1, f_2, \ldots \in K$ and $g_0, g_1, g_2, \ldots \in K$. Then, $f\left[x^2\right] = \sum_{n\in\mathbb{N}} f_n \left(x^2\right)^n = \sum_{n\in\mathbb{N}} f_n x^{2n}$ and similarly $g\left[x^2\right] = \sum_{n\in\mathbb{N}} g_n x^{2n}$. Thus, our assumption $f\left[x^2\right] = g\left[x^2\right]$ rewrites as $\sum_{n\in\mathbb{N}} f_n x^{2n} = \sum_{n\in\mathbb{N}} g_n x^{2n}$. Comparing x^{2n}-coefficients in this equality, we conclude that $f_n = g_n$ for each $n \in \mathbb{N}$. Hence, $\sum_{n\in\mathbb{N}} \underbrace{f_n}_{=g_n} x^n = \sum_{n\in\mathbb{N}} g_n x^n$. In other words, $f = g$ (since $f = \sum_{n\in\mathbb{N}} f_n x^n$ and $g = \sum_{n\in\mathbb{N}} g_n x^n$). This proves Lemma 4.3.3. □

Lemma 4.3.3 justifies our "substituting x for x^2" in the above proof; indeed, we can apply Lemma 4.3.3 to $K = \mathbb{Q}$ and $f = \prod_{k>0} \left(1 - x^k\right)$ and $g = \sum_{k\in\mathbb{Z}} (-1)^k x^{w_k}$ (because (138) says that these two FPSs f and g satisfy $f\left[x^2\right] = g\left[x^2\right]$), and consequently obtain $\prod_{k>0} \left(1 - x^k\right) = \sum_{k\in\mathbb{Z}} (-1)^k x^{w_k}$. Thus, Theorem 4.2.2 is proved using Theorem 4.3.2. It therefore remains to prove the latter.

The following proof is due to Borcherds, and I have taken it from [Camero16, §8.3] (note that [Loehr11, §11.2] gives essentially the same proof, albeit in a different language).

Proof of Theorem 4.3.1 and Theorem 4.3.2. The following argument applies equally to Theorem 4.3.1 and to Theorem 4.3.2. (The meanings of q and z differ between these two theorems, but all the infinite sums and products considered below are well-defined in either case.)

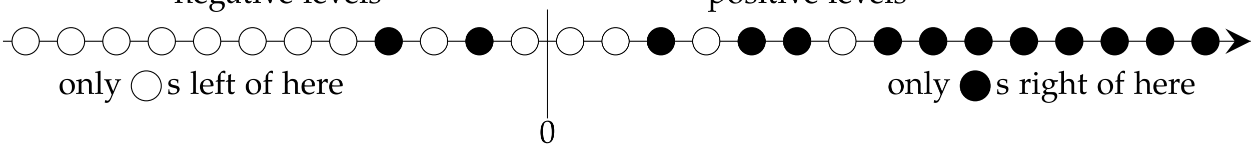
We will use a somewhat physics-inspired language:

- A *level* will mean a number of the form $p + \dfrac{1}{2}$ with $p \in \mathbb{Z}$. (Thus, there is exactly one level midway between any two consecutive integers.)
- A *state* will mean a set of levels that contains
  - all but finitely many negative levels, and
  - only finitely many positive levels.

Here is an example of a state:

$$\left\{\frac{-5}{2}, \frac{-1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{7}{2}, \frac{13}{2}\right\} \cup \left\{\text{all levels } \leq \frac{-9}{2}\right\}.$$

Visually, it can be represented as follows:



where

- A white (=hollow) circle ○ means a level that is contained in the state (you can think of it as an "electron").
- A black (=filled) circle ● means a level that is not contained in the state (think of it as a "hole").

For any state S,

- we define the *energy* of S to be

$$\operatorname{energy} S := \sum_{\substack{p>0;\\ p\in S}} \underbrace{2p}_{>0} - \sum_{\substack{p<0;\\ p\notin S}} \underbrace{2p}_{<0} \in \mathbb{N}$$

(where the summation index p in the first sum runs over the finitely many positive levels contained in S, while the summation index p in the second sum runs over the finitely many negative levels not contained in S).

- we define the *particle number* of S to be

$$\begin{aligned}\operatorname{parnum} S := {} & (\# \text{ of levels } p > 0 \text{ such that } p \in S) \\ & - (\# \text{ of levels } p < 0 \text{ such that } p \notin S) \in \mathbb{Z}.\end{aligned}$$

For instance, in the above example, we have

$$\operatorname{energy} S = 1 + 3 + 7 + 13 - (-3) - (-7) = 34$$

and

$$\operatorname{parnum} S = 4 - 2 = 2.$$

We want to prove the identity

$$\prod_{n>0} \left(\left(1 + q^{2n-1} z\right) \left(1 + q^{2n-1} z^{-1}\right) \left(1 - q^{2n}\right) \right) = \sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^{\ell}.$$

We will first transform this identity into an equivalent one: Namely, we move the $\left(1 - q^{2n}\right)$ factors from the left hand side to the right hand side by multiplying both sides with $\prod\limits_{n>0} \left(1 - q^{2n}\right)^{-1}$. Thus, we can rewrite our identity as

$$\prod_{n>0} \left(\left(1 + q^{2n-1} z\right) \left(1 + q^{2n-1} z^{-1}\right) \right) = \left(\sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^{\ell} \right) \prod_{n>0} \left(1 - q^{2n}\right)^{-1}.$$

We will prove this new identity by showing that both of its sides are

$$\sum_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}.$$

Left hand side: We have

$$\begin{aligned}
&\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\right)\\
&=\left(\prod_{n>0}\left(1+q^{2n-1}z\right)\right)\left(\prod_{n>0}\left(1+q^{2n-1}z^{-1}\right)\right)\\
&=\left(\prod_{p\text{ is a positive level}}\left(1+q^{2p}z\right)\right)\left(\prod_{p\text{ is a negative level}}\left(1+q^{-2p}z^{-1}\right)\right)\\
&\qquad\qquad\left(\begin{array}{c}\text{here, we have substituted } p+\dfrac{1}{2}\text{ for } n \text{ in the first product,}\\ \text{and have substituted } -p+\dfrac{1}{2}\text{ for } n \text{ in the second product}\end{array}\right)\\
&=\left(\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\prod_{p\in P}\left(q^{2p}z\right)\right)\left(\sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}}\prod_{p\in N}\left(q^{-2p}z^{-1}\right)\right)\\
&\qquad\qquad(\text{here, we have expanded both products using (121)})\\
&=\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\ \sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}}\underbrace{\prod_{p\in P}\left(q^{2p}z\right)\prod_{p\in N}\left(q^{-2p}z^{-1}\right)}_{=q^{2(\text{sum of elements of }P)-2(\text{sum of elements of }N)}z^{|P|-|N|}}\\
&=\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\ \sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}} q^{2(\text{sum of elements of }P)-2(\text{sum of elements of }N)}z^{|P|-|N|}\\
&=\sum_{S\text{ is a state}}\underbrace{q^{2(\text{sum of positive levels in }S)-2(\text{sum of negative levels not in }S)}}_{\substack{=q^{\operatorname{energy}S}\\ (\text{by the definition of }\operatorname{energy}S)}}\\
&\qquad\qquad\underbrace{z^{(\text{number of positive levels in }S)-(\text{number of negative levels not in }S)}}_{\substack{=z^{\operatorname{parnum}S}\\ (\text{by the definition of }\operatorname{parnum}S)}}\\
&\qquad\qquad\left(\begin{array}{c}\text{here, we have combined } P \text{ and } N\\ \text{into a single state } S:=P\cup\overline{N},\\ \text{where } \overline{N}=\{\text{all negative levels}\}\setminus N\end{array}\right)\\
&=\sum_{S\text{ is a state}} q^{\operatorname{energy}S}z^{\operatorname{parnum}S}. \qquad (139)
\end{aligned}$$

Right hand side: Recall that

$$\begin{aligned}
\prod_{n>0}\left(1-x^n\right)^{-1}&=\prod_{n>0}\frac{1}{1-x^n}=\sum_{n\in\mathbb{N}}p\left(n\right)x^n \qquad (\text{by Theorem 4.1.8})\\
&=\sum_{\substack{\lambda\text{ is a}\\ \text{partition}}}x^{|\lambda|}
\end{aligned}$$

(because the sum $\sum\limits_{\substack{\lambda \text{ is a} \\ \text{partition}}} x^{|\lambda|}$ contains each monomial x^n precisely $p(n)$ times). Substituting q^2 for x in this equality, we find

$$\prod_{n>0} \left(1 - \left(q^2\right)^n\right)^{-1} = \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} \left(q^2\right)^{|\lambda|}.$$

In other words,

$$\prod_{n>0} \left(1 - q^{2n}\right)^{-1} = \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{2|\lambda|}.$$

Multiplying both sides of this equality by $\sum\limits_{\ell \in \mathbb{Z}} q^{\ell^2} z^\ell$, we obtain

$$\begin{aligned}\left(\sum_{\ell \in \mathbb{Z}} q^{\ell^2} z^\ell\right) \prod_{n>0} \left(1 - q^{2n}\right)^{-1} &= \left(\sum_{\ell \in \mathbb{Z}} q^{\ell^2} z^\ell\right) \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{2|\lambda|} \\ &= \sum_{\ell \in \mathbb{Z}} \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{\ell^2 + 2|\lambda|} z^\ell. \qquad (140)\end{aligned}$$

We want to show that this equals $\sum\limits_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}$. In order to do this, we will find a bijection

$$\Phi_\ell : \{\text{partitions}\} \to \{\text{states with particle number } \ell\}$$

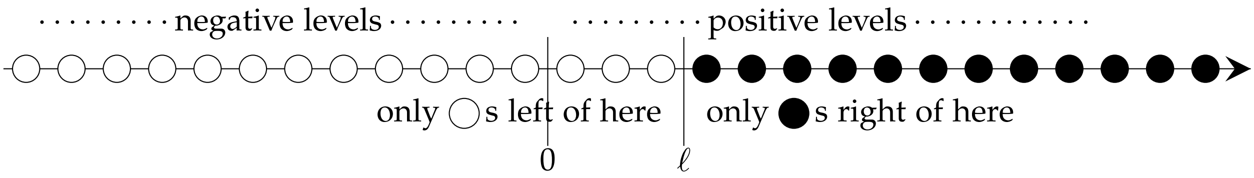
for each $\ell \in \mathbb{Z}$, and we will show that this bijection satisfies

$$\operatorname{energy}\left(\Phi_\ell(\lambda)\right) = \ell^2 + 2|\lambda| \qquad \text{for each } \ell \in \mathbb{Z} \text{ and } \lambda \in \{\text{partitions}\}.$$

Let us do this. Fix $\ell \in \mathbb{Z}$. We define the state G_ℓ (called the "ℓ-ground state") by

$$G_\ell := \{\text{all levels } < \ell\} = \left\{\ell - \frac{1}{2},\ \ell - \frac{3}{2},\ \ell - \frac{5}{2},\ \ldots\right\}.$$

Here is how it looks like (for ℓ positive):


· · · · · · · · · negative levels · · · · · · · · ·
· · · · · · · · · positive levels · · · · · · · · · · · ·
only ○s left of here
only ●s right of here
0
ℓ

If $\ell \geq 0$, then this state G_ℓ has energy

$$\operatorname{energy} G_\ell = 1 + 3 + 5 + \cdots + (2\ell - 1) = \ell^2$$

and particle number

$$\operatorname{parnum} G_\ell = \ell - 0 = \ell.$$

If $\ell < 0$, then it has energy

$$\operatorname{energy} G_\ell = -(-1) - (-3) - (-5) - \cdots - (2\ell+1) = \ell^2$$

and particle number

$$\operatorname{parnum} G_\ell = 0 - (-\ell) = \ell.$$

Note that the answers are the same in both cases. Thus, whatever sign ℓ has, we have

$$\operatorname{energy} G_\ell = \ell^2 \qquad \text{and} \qquad \operatorname{parnum} G_\ell = \ell.$$

If S is a state, and if $p \in S$, and if q is a positive integer such that $p+q \notin S$, then we define a new state

$$\operatorname{jump}_{p,q} S := (S \setminus \{p\}) \cup \{p+q\}.$$

We say that this state $\operatorname{jump}_{p,q} S$ is obtained from S by letting the electron at level p *jump* q steps to the right. Note that $\operatorname{jump}_{p,q} S$ has the same particle number as S (check this![49]), whereas its energy is $2q$ higher than that of S (check this![50]). Thus, a jumping electron raises the energy but keeps the particle number unchanged.

For any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we define the state $E_{\ell,\lambda}$ (called an "excited state") by starting with the ℓ-ground state G_ℓ, and then successively letting the k electrons at the highest levels (which are – from highest to lowest – the levels $\ell - 1 + \frac{1}{2},\ \ \ell - 2 + \frac{1}{2},\ \ \ldots,\ \ \ell - k + \frac{1}{2}$) jump $\lambda_1, \lambda_2, \ldots, \lambda_k$ steps to the right, respectively (starting with the rightmost electron). In other words,

$$\begin{aligned} E_{\ell,\lambda} &:= \operatorname{jump}_{\ell-k+1/2,\ \lambda_k}\left(\cdots\left(\operatorname{jump}_{\ell-2+1/2,\ \lambda_2}\left(\operatorname{jump}_{\ell-1+1/2,\ \lambda_1}(G_\ell)\right)\right)\right) \\ &= \{\text{all levels } < \ell - k\} \cup \left\{\ell - i + \frac{1}{2} + \lambda_i \ \mid\ i \in \{1, 2, \ldots, k\}\right\}. \end{aligned}$$

(Check that these jumps are well-defined – i.e., that each electron jumps to an unoccupied state.)

[Example: Let $\ell = 3$ and $k = 4$ and $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = (4, 2, 2, 1)$. Then,

$$E_{\ell,\lambda} = \{\text{all levels } < -1\} \cup \left\{\frac{3}{2},\ \frac{7}{2},\ \frac{9}{2},\ \frac{13}{2}\right\}.$$

[49] There are three cases:

Case 1: We have $p > 0$ (that is, the particle jumps from a positive level to a positive level).

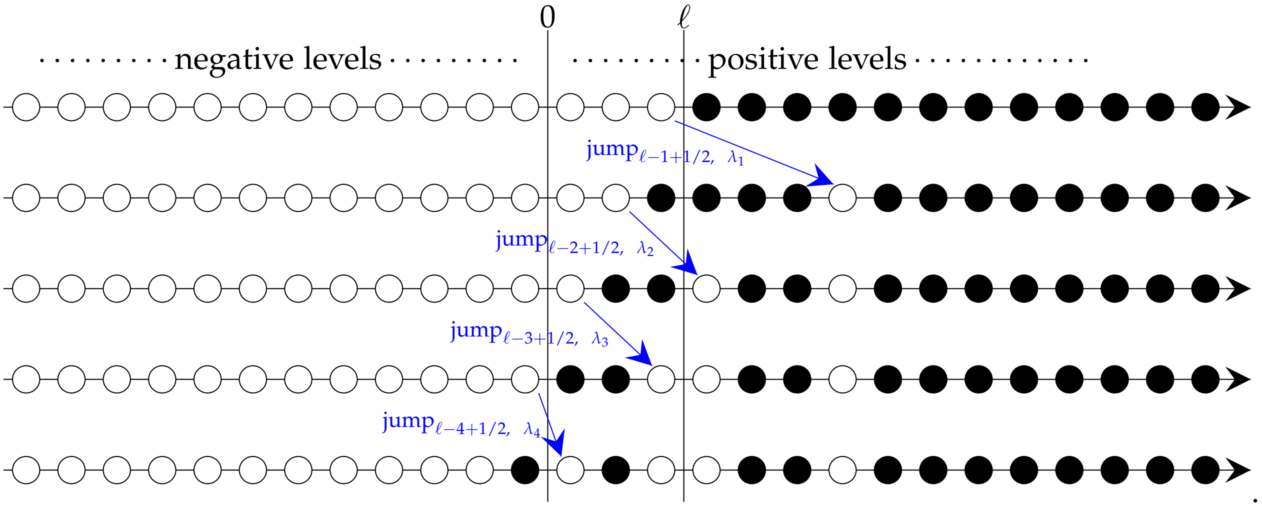
Case 2: We have $p < 0$ and $p + q > 0$ (that is, the particle jumps from a negative level to a positive level).

Case 3: We have $p + q < 0$ (that is, the particle jumps from a negative level to a negative level).

Each case is easy to check.

[50] Again, the same three cases are to be considered.

Here is a picture of this state $E_{\ell,\lambda}$ and how it is constructed by a sequence of electron jumps (the top state is G_ℓ; the bottom state is $E_{\ell,\lambda}$):


0
ℓ
negative levels
positive levels
$\text{jump}_{\ell-1+1/2,\ \lambda_1}$
$\text{jump}_{\ell-2+1/2,\ \lambda_2}$
$\text{jump}_{\ell-3+1/2,\ \lambda_3}$
$\text{jump}_{\ell-4+1/2,\ \lambda_4}$

Note how the order of the electrons after the jumps is the same as before – i.e., the electron in the rightmost position before the jumps is still the rightmost one after the jumps, etc.]

Recall that the ℓ-ground state G_ℓ has energy ℓ^2 and particle number ℓ. The state $E_{\ell,\lambda}$ that we have just defined is obtained from this ℓ-ground state G_ℓ by k jumps, which are jumps by $\lambda_1, \lambda_2, \ldots, \lambda_k$ steps respectively. Recall that a jump by q steps raises the energy by $2q$ but keeps the particle number unchanged. Thus, the "excited state" $E_{\ell,\lambda}$ has energy $\ell^2 + \underbrace{2\lambda_1 + 2\lambda_2 + \cdots + 2\lambda_k}_{=2|\lambda|} = \ell^2 + 2|\lambda|$ and particle number ℓ. Furthermore, every state with particle number ℓ can be written as $E_{\ell,\lambda}$ for a unique partition λ (check this![51]).

Thus, we obtain a bijection

$$\begin{aligned} \Phi_\ell : \{\text{partitions}\} &\to \{\text{states with particle number } \ell\}, \\ \lambda &\mapsto E_{\ell,\lambda}. \end{aligned}$$

This bijection satisfies

$$\text{energy}\left(\Phi_\ell(\lambda)\right) = \text{energy}\, E_{\ell,\lambda} = \ell^2 + 2|\lambda| \qquad \text{for every partition } \lambda.$$

[51] Here is how to obtain this λ: For each $i \in \{1, 2, 3, \ldots\}$, let u_i be the i-th largest level in the state, and let $\lambda_i = u_i - \ell + i - \dfrac{1}{2}$. Then, $(\lambda_1, \lambda_2, \lambda_3, \ldots)$ is a weakly decreasing sequence of nonnegative integers, and all but finitely many of its entries are 0 (since the state has particle number ℓ, so that it is not hard to see that $u_i = \ell - i + \dfrac{1}{2}$ for any sufficiently large i). Removing all 0s from this sequence $(\lambda_1, \lambda_2, \lambda_3, \ldots)$ thus results in a finite tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k)$, which is precisely the partition λ whose corresponding $E_{\ell,\lambda}$ is our state.

Hence,

$$\sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} \underbrace{q^{\ell^2+2|\lambda|}}_{\substack{=q^{\operatorname{energy}(\Phi_\ell(\lambda))} \\ \text{(since } \operatorname{energy}(\Phi_\ell(\lambda))=\ell^2+2|\lambda|)}} = \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{\operatorname{energy}(\Phi_\ell(\lambda))} = \sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}} q^{\operatorname{energy} S} \tag{141}$$

(here, we have substituted S for $\Phi_\ell(\lambda)$ in the sum, since the map Φ_ℓ is a bijection).

Forget that we fixed ℓ. We thus have proved (141) for each $\ell \in \mathbb{Z}$.

Now, (140) becomes

$$\begin{aligned}\left(\sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^\ell\right) \prod_{n>0} \left(1-q^{2n}\right)^{-1} &= \sum_{\ell\in\mathbb{Z}} \underbrace{\sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{\ell^2+2|\lambda|}}_{\substack{=\sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}} q^{\operatorname{energy} S} \\ \text{(by (141))}}} z^\ell \\
&= \sum_{\ell\in\mathbb{Z}} \sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}} q^{\operatorname{energy} S} \underbrace{z^\ell}_{\substack{=z^{\operatorname{parnum} S} \\ \text{(since } \ell=\operatorname{parnum} S)}} \\
&= \underbrace{\sum_{\ell\in\mathbb{Z}} \sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}}}_{=\sum_{S \text{ is a state}}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S} \\
&= \sum_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}.\end{aligned}$$

Comparing this with (139), we obtain

$$\prod_{n>0} \left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\right) = \left(\sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^\ell\right) \prod_{n>0} \left(1-q^{2n}\right)^{-1}.$$

Multiplying both sides of this identity with $\prod_{n>0}\left(1-q^{2n}\right)$, we find

$$\prod_{n>0} \left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right) = \sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^\ell.$$

This proves Jacobi's Triple Product Identity (Theorem 4.3.1 and Theorem 4.3.2). □

Other proofs of Jacobi's Triple Product Identity can be found in [Aigner07, §3.4], [Wagner08, Theorem 10.2] and [Hirsch17, §1.3 and §1.4].

We note that proving Theorem 4.2.2 using Theorem 4.3.2 can be viewed as a kind of overkill; there are more direct proofs of Theorem 4.2.2 as well (see, e.g., [Zabroc03] or [Koch16, §10] or [18f-mt3s, Exercise 5] or [Bell06, §3]).

4.4. q-binomial coefficients

Next, we shall study *q-binomial coefficients* (also known as *Gaussian binomial coefficients*, due to their origins in Gauss's number-theoretical research [Gauss08, §5]). While we will define them as generating functions for certain kinds of partitions, they are sufficiently elementary to have relevance to various other subjects. We will scratch the surface; more can be found in [KacChe02, Chapters 5–7], [KliSch97, Chapter 2], [Wagner08, Chapter 5], [Wagner20, §11.3–11.11], [Stanle11, spread across the text], [GouJac83, §2.6], [Johnso20] and other sources. (The book [Johnso20] is particularly recommended as a leisurely introduction to q-binomial coefficients and related power series.)

4.4.1. Motivation

For any $n \in \mathbb{N}$, we have

$$p\left(n\right) = \left(\text{\# of partitions of } n\right).$$

For any $n, k \in \mathbb{N}$, we have

$$\begin{aligned} p_k\left(n\right) &= \left(\text{\# of partitions of } n \text{ into } k \text{ parts}\right) \\ &= \left(\text{\# of partitions of } n \text{ with largest part } k\right) \qquad \left(\text{by Theorem 4.1.14}\right). \end{aligned}$$

Thus, for any $n, k \in \mathbb{N}$, we have

$$\begin{aligned} p_0\left(n\right) + p_1\left(n\right) + \cdots + p_k\left(n\right) &= \left(\text{\# of partitions of } n \text{ into } \textbf{at most } k \text{ parts}\right) \\ &= \left(\text{\# of partitions of } n \text{ with largest part } \leq k\right) \end{aligned}$$

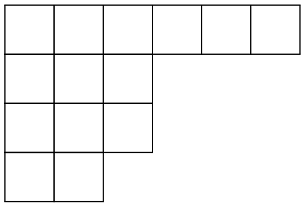
(by Corollary 4.1.17).

So far, so good. But how to count partitions of n that both have a fixed # of parts (say, k parts) and a fixed largest part (say, largest part ℓ) ?

Let us first drop the size requirement – i.e., we replace "partitions of n" by just "partitions".

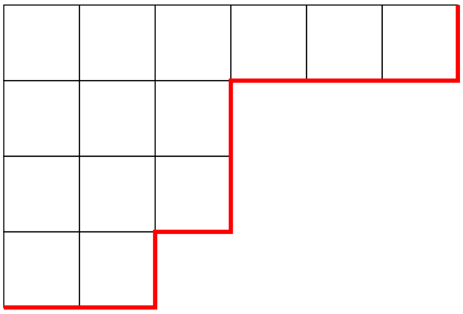
For example, how many partitions have 4 parts and largest part 6 ?

As in the proof of Theorem 4.1.14, let us draw the Young diagram of such a partition: For example, the partition $(6, 3, 3, 2)$ has Young diagram



.

Consider the lower boundary of this Young diagram – i.e., the "irregular" southeastern border between what is in the diagram and what is outside of it. Let me mark it in thick red:

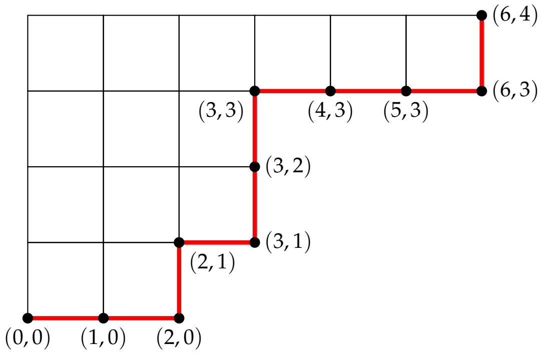


.

This lower boundary can be viewed as a lattice path from the point $(0,0)$ to the point $(6,4)$ (where we are using Cartesian coordinates to label the intersections of grid lines, so that the southwesternmost point in our diagram is $(0,0)$; note that this is completely unrelated to our labeling of cells used in defining the Young diagram![52]). This lattice path consists of east-steps (i.e., steps $(i,j) \rightarrow (i+1,j)$) and north-steps (i.e., steps $(i,j) \rightarrow (i,j+1)$); moreover, it begins with an east-step (since otherwise, our partition would have fewer than 4 parts) and ends with a north-step (since otherwise, our partition would have largest part < 6). Moreover, the Young diagram (and thus the partition) is uniquely determined by this lattice path, since its cells are precisely the cells "northwest" of this lattice path. Conversely, any lattice path from $(0,0)$ to $(6,4)$ that consists of east-steps and north-steps and begins with an east step and ends with a north-step uniquely determines a Young diagram and therefore a partition. Therefore, in order to count the partitions that have 4 parts and largest part 6, we only need to count such lattice paths.

To count them, we notice that any such lattice path has precisely 10 steps (since any step increases the sum of the coordinates by 1; but this sum must increase from $0+0=0$ to $6+4=10$). The first and the last steps are predetermined; it remains to decide which of the remaining 8 steps are north-steps.

[52] For additional clarity, here are the Cartesian coordinates of all grid points on our lattice path:



.

The # of ways to do this is $\dbinom{8}{3}$, because we want precisely 3 of our 8 non-predetermined steps to be north-steps (in order to end up at $(6,4)$ rather than some other point).

As a consequence of this all, we find

$$(\text{\# of partitions with 4 parts and largest part 6}) = \dbinom{8}{3}.$$

More generally, by the same argument, we obtain the following:

Proposition 4.4.1. For any positive integers k and ℓ, we have

$$(\text{\# of partitions with } k \text{ parts and largest part } \ell) = \dbinom{k+\ell-2}{k-1}.$$

Note two things:

- This is a finite number, even without fixing the size of the partition. This is not surprising, since you have only finitely many parts and only finitely many options for each part.
- The number is symmetric in k and ℓ. This, too, is not surprising, because conjugation (as defined in the proof of Theorem 4.1.14) gives a bijection

$$\begin{aligned}&\text{from } \{\text{partitions with } k \text{ parts and largest part } \ell\}\\ &\text{to } \{\text{partitions with } \ell \text{ parts and largest part } k\}.\end{aligned}$$

Now, let us integrate the size of the partition back into our count – i.e., let us try to count the partitions of a given $n \in \mathbb{N}$ with k parts and largest part ℓ. No simple formula (like Proposition 4.4.1) exists for this number any more, so we switch our focus to the generating function of such numbers (for fixed k and ℓ). In other words, we try to compute the FPS

$$\begin{aligned}&\sum_{n\in\mathbb{N}} (\text{\# of partitions of } n \text{ with } k \text{ parts and largest part } \ell)\, x^n\\ &= \sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \ell\\ \text{and length } k}} x^{|\lambda|}.\end{aligned}$$

For reasons of convenience, history and simplicity, we modify this problem slightly (without changing its essence). To wit,

- we rename ℓ as $n-k$ (note that n will no longer stand for the size of the partition);

- we replace "largest part $n-k$ and length k" by "largest part $\leq n-k$ and length $\leq k$" (this changes the results of our counts, but we can easily recover the answer to the original question from an answer to the new question; e.g., in order to count the length-k partitions, it suffices to subtract the # of length-($\leq k-1$)-partitions from the # of length-($\leq k$) partitions);
- we rename the indeterminate x as q.

4.4.2. Definition

Convention 4.4.2. In this section, we will mostly be using FPSs in the indeterminate q. That is, we call the indeterminate q rather than x. Thus, e.g., our formula

$$\prod_{n>0} \left(1-x^n\right)^{-1} = \prod_{n>0} \frac{1}{1-x^n} = \sum_{n\in\mathbb{N}} p\left(n\right) x^n = \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} x^{\left|\lambda\right|}$$

becomes

$$\prod_{n>0} \left(1-q^n\right)^{-1} = \prod_{n>0} \frac{1}{1-q^n} = \sum_{n\in\mathbb{N}} p\left(n\right) q^n = \sum_{\substack{\lambda \text{ is a} \\ \text{partition}}} q^{\left|\lambda\right|}.$$

The ring of FPSs in the indeterminate q over a commutative ring K will be denoted by $K\left[\left[q\right]\right]$. The ring of polynomials in the indeterminate q over K will be denoted by $K\left[q\right]$.

Definition 4.4.3. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

(a) The *q-binomial coefficient* (or *Gaussian binomial coefficient*) $\dbinom{n}{k}_q$ is defined to be the polynomial

$$\sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{\left|\lambda\right|} \in \mathbb{Z}\left[q\right].$$

This is also denoted by $\begin{bmatrix} n \\ k \end{bmatrix}$ (but this notation has other meanings, too, and suppresses q).

(b) If a is any element of a ring A, then we set

$$\begin{aligned}\binom{n}{k}_a &:= \binom{n}{k}_q [a] \\ &\qquad \left(\text{this means the result of substituting } a \text{ for } q \text{ in } \binom{n}{k}_q\right) \\ &= \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} a^{|\lambda|} \in A.\end{aligned}$$

Remark 4.4.4. The $\binom{n}{k}_q$ we defined in Definition 4.4.3 **(a)** is really a polynomial, not merely a FPS, because (for any given n and k) there are only finitely many partitions with largest part $\leq n-k$ and length $\leq k$.

Remark 4.4.5. The notation $\binom{n}{k}_q$ (and the name "q-binomial coefficient") suggests a similarity to the usual binomial coefficient $\binom{n}{k}$. And indeed, we will soon see that $\binom{n}{k}_1 = \binom{n}{k}$.

Note, however, that $\binom{n}{k}_q$ is only defined for $n, k \in \mathbb{N}$ (unlike $\binom{n}{k}$, which we defined for arbitrary $n, k \in \mathbb{C}$). It is possible to extend it to negative integers n, but this will result in a Laurent polynomial. (See Exercise A.3.4.4 for this extension.)

Example 4.4.6. We have

$$\begin{aligned}\binom{3}{2}_q &= \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq 1 \\ \text{and length } \leq 2}} q^{|\lambda|} = q^{|(1,1)|} + q^{|(1)|} + q^{|()|} \\ &\qquad \left(\begin{array}{c}\text{since the partitions with largest part } \leq 1 \\ \text{and length } \leq 2 \text{ are } (1,1),\ (1) \text{ and } ()\end{array}\right) \\ &= q^2 + q^1 + q^0 = q^2 + q + 1\end{aligned}$$

and

$$\begin{aligned}\binom{4}{2}_q &= \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq 2 \\ \text{and length } \leq 2}} q^{|\lambda|} \\ &= q^{|(2,2)|} + q^{|(2,1)|} + q^{|(2)|} + q^{|(1,1)|} + q^{|(1)|} + q^{|()|} \\ &= q^4 + q^3 + q^2 + q^2 + q^1 + q^0 = q^4 + q^3 + 2q^2 + q + 1.\end{aligned}$$

4.4.3. Basic properties

Let us show two slightly different (but equivalent) ways to express q-binomial coefficients:

Proposition 4.4.7. Let $n, k \in \mathbb{N}$.

(a) We have

$$\binom{n}{k}_q = \sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n-k} q^{i_1 + i_2 + \cdots + i_k}.$$

Here, the sum ranges over all weakly increasing k-tuples $(i_1, i_2, \ldots, i_k) \in \{0, 1, \ldots, n-k\}^k$. If $k > n$, then this is an empty sum (since the set $\{0, 1, \ldots, n-k\}$ is empty in this case, and thus its k-th power $\{0, 1, \ldots, n-k\}^k$ is also empty because $k > n \geq 0$).

(b) Set $\operatorname{sum} S = \sum_{s \in S} s$ for any finite set S of integers. (For example, $\operatorname{sum}\{2, 4, 5\} = 2 + 4 + 5 = 11$.) Then, we have

$$\binom{n}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S| = k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

(c) We have

$$\binom{n}{k}_1 = \binom{n}{k}.$$

Example 4.4.8. For example, let us compute $\binom{5}{2}_q$ using Proposition 4.4.7

(b). Namely, applying Proposition 4.4.7 **(b)** to $n = 5$ and $k = 2$, we obtain

$$\begin{aligned}
\binom{5}{2}_q &= \sum_{\substack{S \subseteq \{1,2,\ldots,5\};\\ |S|=2}} q^{\operatorname{sum} S - (1+2)} \\
&= q^{(1+2)-(1+2)} + q^{(1+3)-(1+2)} + q^{(1+4)-(1+2)} + q^{(1+5)-(1+2)} \\
&\qquad + q^{(2+3)-(1+2)} + q^{(2+4)-(1+2)} + q^{(2+5)-(1+2)} \\
&\qquad + q^{(3+4)-(1+2)} + q^{(3+5)-(1+2)} + q^{(4+5)-(1+2)} \\
&\qquad\qquad \left(\begin{array}{c} \text{since the 2-element subsets of } \{1,2,\ldots,5\} \text{ are} \\ \{1,2\},\ \{1,3\},\ \{1,4\},\ \{1,5\},\ \{2,3\},\ \{2,4\}, \\ \{2,5\},\ \{3,4\},\ \{3,5\},\ \{4,5\} \end{array} \right) \\
&= q^0 + q^1 + q^2 + q^3 + q^2 + q^3 + q^4 + q^4 + q^5 + q^6 \\
&= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6.
\end{aligned}$$

Proof of Proposition 4.4.7. **(a)** The definition of $\binom{n}{k}_q$ yields

$$\binom{n}{k}_q = \sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{|\lambda|} = \sum_{\ell=0}^{k} \sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k \\ \text{and length } \ell}} q^{|\lambda|}. \tag{142}$$

Now, let us simplify the inner sum on the right hand side.

Fix $\ell \in \{0, 1, \ldots, k\}$. Then, any partition λ with length ℓ has the form $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ for some nonnegative integers $\lambda_1, \lambda_2, \ldots, \lambda_\ell$ satisfying $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$ (by the definitions of "partition" and "length"). Moreover, this partition λ has largest part $\leq n - k$ if and only if its entries satisfy $n - k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0$. Finally, the size $|\lambda|$ of this partition equals $\lambda_1 + \lambda_2 + \cdots + \lambda_\ell$. Hence, we can rewrite the sum

$$\sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k \\ \text{and length } \ell}} q^{|\lambda|} \qquad \text{as} \qquad \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_\ell) \in \mathbb{N}^\ell;\\ n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell}.$$

In other words, we have

$$\sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k \\ \text{and length } \ell}} q^{|\lambda|} = \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_\ell) \in \mathbb{N}^\ell;\\ n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell > 0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell}. \tag{143}$$

Next, for any k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$, let us define $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k)$ to be the number of positive entries of this k-tuple (i.e., the number of $i \in$

$\{1,2,\ldots,k\}$ satisfying $\lambda_i > 0$). For example, $\operatorname{numpos}(4,2,2,0) = 3$ and $\operatorname{numpos}(4,2,2,1) = 4$ and $\operatorname{numpos}(0,0,0,0) = 0$. The following is easy but important:

> *Observation 1:* Let $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$ be any k-tuple satisfying $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$ and $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$. Then:
>
> **(a)** The first ℓ entries of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ are positive (i.e., we have $\lambda_i > 0$ for all $i \in \{1,2,\ldots,\ell\}$).
>
> **(b)** The last $k-\ell$ entries of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ are 0 (i.e., we have $\lambda_i = 0$ for all $i \in \{\ell+1, \ell+2, \ldots, k\}$).
>
> **(c)** We have $\lambda_1 + \lambda_2 + \cdots + \lambda_\ell = \lambda_1 + \lambda_2 + \cdots + \lambda_k$.
>
> **(d)** The ℓ-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ is a partition.

[*Proof of Observation 1:* We have $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$. In other words, the k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ has exactly ℓ positive entries. Since this k-tuple is weakly decreasing (because $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$), these ℓ positive entries must be concentrated at the beginning of the k-tuple; i.e., they must be the first ℓ entries of the k-tuple. Hence, the first ℓ entries of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ are positive. This proves Observation 1 **(a)**.

We have shown that the k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ has exactly ℓ positive entries, and they are the first ℓ entries of this k-tuple. Hence, the remaining $k-\ell$ entries of this k-tuple are nonpositive. Since these entries are nonnegative as well (because $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$), we thus conclude that they are 0. In other words, the last $k-\ell$ entries of $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ are 0. This proves Observation 1 **(b)**.

Furthermore,

$$\lambda_1 + \lambda_2 + \cdots + \lambda_k = (\lambda_1 + \lambda_2 + \cdots + \lambda_\ell) + \underbrace{(\lambda_{\ell+1} + \lambda_{\ell+2} + \cdots + \lambda_k)}_{\substack{=0+0+\cdots+0 \\ \text{(by Observation 1 (b))}}}$$
$$= (\lambda_1 + \lambda_2 + \cdots + \lambda_\ell) + (0+0+\cdots+0) = \lambda_1 + \lambda_2 + \cdots + \lambda_\ell.$$

This proves Observation 1 **(c)**.

(d) The ℓ-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ is weakly decreasing (since $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$ entails $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell$) and consists of positive integers (since Observation 1 **(a)** says that we have $\lambda_i > 0$ for all $i \in \{1,2,\ldots,\ell\}$). Thus, it is a weakly decreasing tuple of positive integers, i.e., a partition. This proves Observation 1 **(d)**.]

Let us recall that $\ell \in \{0,1,\ldots,k\}$, so that $\ell \leq k$. Hence, any ℓ-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_\ell) \in \mathbb{N}^\ell$ can be extended to a k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$ by inserting $k-\ell$ zeroes at the end (i.e., by setting $\lambda_{\ell+1} = \lambda_{\ell+2} = \cdots = \lambda_k = 0$). [53] If the original ℓ-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_\ell) \in \mathbb{N}^\ell$ was a partition with largest part $\leq n-k$, then the extended k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) = \left(\lambda_1, \lambda_2, \ldots, \lambda_\ell, \underbrace{0, 0, \ldots, 0}_{k-\ell \text{ zeroes}}\right)$ will satisfy

[53] For example, if $\ell = 3$ and $k = 5$, then the ℓ-tuple $(4,2,2)$ gets extended to the k-tuple $(4,2,2,0,0)$.

$n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$ (since $n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell$ and $\lambda_\ell \geq 0 = \lambda_{\ell+1} = \lambda_{\ell+2} = \cdots = \lambda_k \geq 0$) and $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$ (since its first ℓ entries are positive whereas its remaining $k-\ell$ entries are 0).

Conversely, if $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$ is a k-tuple satisfying $n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$ and $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$, then $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ is a partition[54] with largest part $\leq n-k$ [55] and length ℓ. Thus, we obtain a map

$$\begin{aligned} &\text{from } \Big\{ k\text{-tuples } (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k \text{ satisfying } n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0 \\ &\qquad\qquad \text{and } \operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell \Big\} \\ &\text{to } \{\text{partitions with largest part } \leq n-k \text{ and length } \ell\} \end{aligned}$$

which sends any k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ to the partition $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$. On the other hand, we have a map

$$\begin{aligned} &\text{from } \{\text{partitions with largest part } \leq n-k \text{ and length } \ell\} \\ &\text{to } \Big\{ k\text{-tuples } (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k \text{ satisfying } n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0 \\ &\qquad\qquad \text{and } \operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell \Big\} \end{aligned}$$

which sends any partition $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ to the k-tuple $\Bigg(\lambda_1, \lambda_2, \ldots, \lambda_\ell, \underbrace{0, 0, \ldots, 0}_{k-\ell \text{ zeroes}}\Bigg)$ [56]. These two maps are mutually inverse[57], and therefore are bijections. In particular, this shows that the first map is a bijection. This bijection allows us to replace our partitions $(\lambda_1, \lambda_2, \ldots, \lambda_\ell) \in \mathbb{N}^\ell$ by k-tuples $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$ in

[54] because of Observation 1 **(d)**

[55] since all parts $\lambda_1, \lambda_2, \ldots, \lambda_\ell$ of this partition are $\leq n-k$ (because $n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k$)

[56] because we have shown in the previous paragraph that if $(\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ is a partition with largest part $\leq n-k$, then we can extend it to a k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) = \Bigg(\lambda_1, \lambda_2, \ldots, \lambda_\ell, \underbrace{0, 0, \ldots, 0}_{k-\ell \text{ zeroes}}\Bigg)$ by inserting $k-\ell$ zeroes at the end, and this extended k-tuple will satisfy $n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$ and $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$

[57] Indeed, the first map removes the last $k-\ell$ entries from a k-tuple, whereas the second map inserts $k-\ell$ zeroes at the end of the partition. Thus, if we apply the first map after the second map, we clearly recover the partition that we started with. If we apply the second map after the first map, then we end up replacing the last $k-\ell$ entries of our k-tuple by zeroes. However, if $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}^k$ is any k-tuple satisfying $n-k \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$ and $\operatorname{numpos}(\lambda_1, \lambda_2, \ldots, \lambda_k) = \ell$, then the last $k-\ell$ entries of this k-tuple are 0 (by Observation 1 **(b)**), and therefore the k-tuple does not change if we replace these $k-\ell$ entries by zeroes.

the sum $\sum\limits_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_\ell)\in\mathbb{N}^\ell;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_\ell>0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell}$; we thus find

$$\begin{aligned}\sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_\ell)\in\mathbb{N}^\ell;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_\ell>0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell} &= \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0;\\ \operatorname{numpos}(\lambda_1,\lambda_2,\ldots,\lambda_k)=\ell}} \underbrace{q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell}}_{\substack{=q^{\lambda_1+\lambda_2+\cdots+\lambda_k}\\ \text{(by Observation 1 } \textbf{(c)}\text{)}}} \\ &= \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0;\\ \operatorname{numpos}(\lambda_1,\lambda_2,\ldots,\lambda_k)=\ell}} q^{\lambda_1+\lambda_2+\cdots+\lambda_k}.\end{aligned}$$

Now, (143) becomes

$$\begin{aligned}\sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k\\ \text{and length } \ell}} q^{|\lambda|} &= \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_\ell)\in\mathbb{N}^\ell;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_\ell>0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_\ell} \\ &= \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0;\\ \operatorname{numpos}(\lambda_1,\lambda_2,\ldots,\lambda_k)=\ell}} q^{\lambda_1+\lambda_2+\cdots+\lambda_k}. \qquad (144)\end{aligned}$$

Now, forget that we fixed ℓ. We thus have proved (144) for each $\ell \in \{0,1,\ldots,k\}$. Now, (142) becomes

$$\begin{aligned}\binom{n}{k}_q &= \sum_{\ell=0}^{k} \underbrace{\sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k\\ \text{and length } \ell}} q^{|\lambda|}}_{\substack{=\sum\limits_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0;\\ \operatorname{numpos}(\lambda_1,\lambda_2,\ldots,\lambda_k)=\ell}} q^{\lambda_1+\lambda_2+\cdots+\lambda_k}\\ \text{(by (144))}}} = \underbrace{\sum_{\ell=0}^{k} \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0;\\ \operatorname{numpos}(\lambda_1,\lambda_2,\ldots,\lambda_k)=\ell}}}_{=\sum\limits_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0}}} q^{\lambda_1+\lambda_2+\cdots+\lambda_k} \\ &= \sum_{\substack{(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k;\\ n-k\geq\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_k\geq 0}} q^{\lambda_1+\lambda_2+\cdots+\lambda_k} = \sum_{\substack{(i_1,i_2,\ldots,i_k)\in\mathbb{N}^k;\\ 0\leq i_1\leq i_2\leq\cdots\leq i_k\leq n-k}} \underbrace{q^{i_k+i_{k-1}+\cdots+i_1}}_{=q^{i_1+i_2+\cdots+i_k}} \\ &\qquad \left(\begin{array}{c}\text{here, we have reversed the } k\text{-tuple } (\lambda_1,\lambda_2,\ldots,\lambda_k)\text{,}\\ \text{i.e., we have substituted } (i_k,i_{k-1},\ldots,i_1) \text{ for } (\lambda_1,\lambda_2,\ldots,\lambda_k)\\ \text{in our sum}\end{array}\right) \\ &= \sum_{\substack{(i_1,i_2,\ldots,i_k)\in\mathbb{N}^k;\\ 0\leq i_1\leq i_2\leq\cdots\leq i_k\leq n-k}} q^{i_1+i_2+\cdots+i_k} = \sum_{0\leq i_1\leq i_2\leq\cdots\leq i_k\leq n-k} q^{i_1+i_2+\cdots+i_k}.\end{aligned}$$

This proves Proposition 4.4.7 **(a)**.

(b) There is a bijection

$$\text{from } \left\{\text{weakly increasing } k\text{-tuples } (i_1, i_2, \ldots, i_k) \in \{0, 1, \ldots, n-k\}^k\right\}$$
$$\text{to } \left\{\text{strictly increasing } k\text{-tuples } (s_1, s_2, \ldots, s_k) \in \{1, 2, \ldots, n\}^k\right\}$$

that sends each weakly increasing k-tuple $(i_1, i_2, \ldots, i_k)$ to $(i_1 + 1,\ i_2 + 2,\ \ldots,\ i_k + k)$ (you can think of it as "spacing the i_js apart", i.e., increasing the distance between any two consecutive i_j's by 1 and also increasing i_1 by 1). The inverse of this bijection sends each strictly increasing k-tuple $(s_1, s_2, \ldots, s_k)$ to $(s_1 - 1,\ s_2 - 2,\ \ldots,\ s_k - k)$. Thus, we can substitute $(s_1 - 1,\ s_2 - 2,\ \ldots,\ s_k - k)$ for $(i_1, i_2, \ldots, i_k)$ in the sum

$$\sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n-k} q^{i_1 + i_2 + \cdots + i_k}.$$

Hence we obtain

$$\begin{aligned}\sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n-k} q^{i_1 + i_2 + \cdots + i_k} &= \sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq n} \underbrace{q^{(s_1 - 1) + (s_2 - 2) + \cdots + (s_k - k)}}_{= q^{(s_1 + s_2 + \cdots + s_k) - (1 + 2 + \cdots + k)}} \\ &= \sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq n} q^{(s_1 + s_2 + \cdots + s_k) - (1 + 2 + \cdots + k)}.\end{aligned}$$

On the other hand, there is a bijection

$$\text{from } \left\{\text{strictly increasing } k\text{-tuples } (s_1, s_2, \ldots, s_k) \in \{1, 2, \ldots, n\}^k\right\}$$
$$\text{to } \{k\text{-element subsets of } \{1, 2, \ldots, n\}\}$$

that sends each k-tuple $(s_1, s_2, \ldots, s_k)$ to the subset $\{s_1, s_2, \ldots, s_k\}$. (This map is indeed a bijection, because any k-element subset of $\{1, 2, \ldots, n\}$ can be written as $\{s_1, s_2, \ldots, s_k\}$ for a unique strictly increasing k-tuple $(s_1, s_2, \ldots, s_k) \in \{1, 2, \ldots, n\}^k$; in fact, this is simply saying that there is a unique way of listing the elements of this subset in increasing order.)

Because of this bijection, we have

$$\sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq n} q^{(s_1 + s_2 + \cdots + s_k) - (1 + 2 + \cdots + k)} = \sum_{\substack{S \subseteq \{1, 2, \ldots, n\}; \\ |S| = k}} q^{\operatorname{sum} S - (1 + 2 + \cdots + k)}$$

(because $s_1 + s_2 + \cdots + s_k = \operatorname{sum} \{s_1, s_2, \ldots, s_k\}$ for any strictly increasing k-tuple $(s_1, s_2, \ldots, s_k) \in \{1, 2, \ldots, n\}^k$).

Now, Proposition 4.4.7 **(a)** yields

$$\begin{aligned}\binom{n}{k}_q &= \sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n-k} q^{i_1 + i_2 + \cdots + i_k} = \sum_{1 \leq s_1 < s_2 < \cdots < s_k \leq n} q^{(s_1 + s_2 + \cdots + s_k) - (1 + 2 + \cdots + k)} \\ &= \sum_{\substack{S \subseteq \{1, 2, \ldots, n\}; \\ |S| = k}} q^{\operatorname{sum} S - (1 + 2 + \cdots + k)}.\end{aligned}$$

This proves Proposition 4.4.7 **(b)**.

(c) Proposition 4.4.7 **(b)** yields

$$\binom{n}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S|=k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

Substituting 1 for q in this equality, we find

$$\begin{aligned}\binom{n}{k}_1 &= \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S|=k}} \underbrace{1^{\operatorname{sum} S - (1+2+\cdots+k)}}_{=1} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S|=k}} 1 \\ &= (\text{\# of subsets } S \subseteq \{1,2,\ldots,n\} \text{ satisfying } |S| = k) \\ &= (\text{\# of } k\text{-element subsets of } \{1,2,\ldots,n\}) = \binom{n}{k}.\end{aligned}$$

This proves Proposition 4.4.7 **(c)**. □

The following property of q-binomial coefficients generalizes Proposition 2.0.5:

Proposition 4.4.9. Let $n, k \in \mathbb{N}$ satisfy $k > n$. Then, $\binom{n}{k}_q = 0$.

Proof. From $k > n$, we obtain $n - k < 0$. The definition of $\binom{n}{k}_q$ yields

$$\binom{n}{k}_q = \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{|\lambda|}. \tag{145}$$

The sum on the right hand side is an empty sum, since there exists no partition with largest part $\leq n - k$ (because $n - k < 0$). Thus, (145) rewrites as $\binom{n}{k}_q = (\text{empty sum}) = 0$, and this proves Proposition 4.4.9. □

Proposition 4.4.10. We have $\binom{n}{0}_q = \binom{n}{n}_q = 1$ for each $n \in \mathbb{N}$.

Proof. This is easy and left as a homework exercise (Exercise A.3.4.1 **(a)**). □

The next convention mirrors a convention we made for the (usual) binomial coefficients:

Convention 4.4.11. Let $n \in \mathbb{N}$. For any $k \notin \mathbb{N}$, we set $\dbinom{n}{k}_q := 0$.

The following theorem gives not one, but two analogues ("q-analogues") of the recurrence relation $\dbinom{n}{k} = \dbinom{n-1}{k-1} + \dbinom{n-1}{k}$ (from Proposition 2.0.4):

Theorem 4.4.12. Let n be a positive integer. Let $k \in \mathbb{N}$. Then:

(a) We have

$$\binom{n}{k}_q = q^{n-k} \binom{n-1}{k-1}_q + \binom{n-1}{k}_q .$$

(b) We have

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q .$$

Proof. **(a)** This is similar to the combinatorial proof of the recurrence relation for binomial coefficients.

If $k = 0$, then the claim we are proving boils down to $1 = q^{n-k} 0 + 1$ (because Proposition 4.4.10 yields $\dbinom{n}{0}_q = 1$ and $\dbinom{n-1}{0}_q = 1$, and because Convention 4.4.11 yields $\dbinom{n-1}{-1}_q = 0$). Hence, we WLOG assume that $k > 0$. Thus, $k - 1 \in \mathbb{N}$.

Proposition 4.4.7 **(b)** says that

$$\binom{n}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S| = k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}. \tag{146}$$

Proposition 4.4.7 **(b)** (applied to $n-1$ and $k-1$ instead of n and k) yields

$$\binom{n-1}{k-1}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n-1\}; \\ |S| = k-1}} q^{\operatorname{sum} S - (1+2+\cdots+(k-1))}. \tag{147}$$

Proposition 4.4.7 **(b)** (applied to $n-1$ instead of n) yields

$$\binom{n-1}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n-1\}; \\ |S| = k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}. \tag{148}$$

Let us now make two definitions:

- A *type-1 subset* will mean a k-element subset of $\{1, 2, \ldots, n\}$ that contains n;

- A *type-2 subset* will mean a k-element subset of $\{1, 2, \ldots, n\}$ that does not contain n.

Each k-element subset of $\{1, 2, \ldots, n\}$ is either type-1 or type-2 (but not both at the same time). Thus,

$$\begin{aligned} & \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} q^{\operatorname{sum} S-(1+2+\cdots+k)} \\ &= \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-1}}} q^{\operatorname{sum} S-(1+2+\cdots+k)} + \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-2}}} q^{\operatorname{sum} S-(1+2+\cdots+k)}. \end{aligned}$$

The type-2 subsets are precisely the k-element subsets of $\{1, 2, \ldots, n-1\}$. Hence,

$$\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-2}}} q^{\operatorname{sum} S-(1+2+\cdots+k)} = \sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k}} q^{\operatorname{sum} S-(1+2+\cdots+k)} = \binom{n-1}{k}_q$$

(by (148)).

The type-1 subsets are just the $(k-1)$-element subsets of $\{1, 2, \ldots, n-1\}$ with an n inserted into them; i.e., the map

$$\begin{aligned} \{(k-1)\text{-element subsets of } \{1,2,\ldots,n-1\}\} &\to \{\text{type-1 subsets}\}, \\ S &\mapsto S\cup\{n\} \end{aligned}$$

is a bijection. Hence, substituting $S \cup \{n\}$ for S in the sum, we find

$$\begin{aligned}
\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-1}}} q^{\operatorname{sum}S-(1+2+\cdots+k)} &= \sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} \underbrace{q^{\operatorname{sum}(S\cup\{n\})-(1+2+\cdots+k)}}_{\substack{=q^{\operatorname{sum}S+n-(1+2+\cdots+k)}\\ \text{(since } S\subseteq\{1,2,\ldots,n-1\}\text{ entails } n\notin S\\ \text{and thus } \operatorname{sum}(S\cup\{n\})=\operatorname{sum}S+n)}} \\
&= \sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} \underbrace{q^{\operatorname{sum}S+n-(1+2+\cdots+k)}}_{\substack{=q^{\operatorname{sum}S+n-(1+2+\cdots+(k-1))-k}\\ =q^{n-k}q^{\operatorname{sum}S-(1+2+\cdots+(k-1))}}} \\
&= \sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} q^{n-k}q^{\operatorname{sum}S-(1+2+\cdots+(k-1))} \\
&= q^{n-k} \underbrace{\sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} q^{\operatorname{sum}S-(1+2+\cdots+(k-1))}}_{\substack{=\binom{n-1}{k-1}_q\\ \text{(by (147))}}} \\
&= q^{n-k}\binom{n-1}{k-1}_q .
\end{aligned}$$

All that's left to do is combining what we have found:

$$\begin{aligned}
\binom{n}{k}_q &= \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} q^{\operatorname{sum}S-(1+2+\cdots+k)} \qquad \text{(by (146))} \\
&= \underbrace{\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-1}}} q^{\operatorname{sum}S-(1+2+\cdots+k)}}_{=q^{n-k}\binom{n-1}{k-1}_q} + \underbrace{\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ S\text{ is type-2}}} q^{\operatorname{sum}S-(1+2+\cdots+k)}}_{=\binom{n-1}{k}_q} \\
&= q^{n-k}\binom{n-1}{k-1}_q + \binom{n-1}{k}_q .
\end{aligned}$$

This proves Theorem 4.4.12 **(a)**.

(b) This is somewhat similar to Theorem 4.4.12 **(a)** (but a little bit more complicated). It is left as a homework exercise (Exercise A.3.4.1 **(b)**). □

Next, we shall derive a q-analogue of the formula $\dbinom{n}{k} = \dfrac{n(n-1)\cdots(n-k+1)}{k!} = \dfrac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$:

Theorem 4.4.13. Let $n, k \in \mathbb{N}$ satisfy $n \geq k$. Then:

(a) We have

$$\left(1-q^{k}\right)\left(1-q^{k-1}\right)\cdots\left(1-q^{1}\right)\cdot\binom{n}{k}_{q} = \left(1-q^{n}\right)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right).$$

(b) We have

$$\binom{n}{k}_{q} = \frac{\left(1-q^{n}\right)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right)}{\left(1-q^{k}\right)\left(1-q^{k-1}\right)\cdots\left(1-q^{1}\right)}$$

(in the ring $\mathbb{Z}[[q]]$ or in the field of rational functions over $\mathbb{Q}$).

Note that part **(b)** of Theorem 4.4.13 is the more intuitive statement, but part **(a)** is easier to substitute things in (because substituting something for q in part **(b)** requires showing that the denominator remains invertible, whereas part **(a)** has no denominators and thus requires no such diligence).

Proof of Theorem 4.4.13. This is left as a homework exercise (Exercise A.3.4.1 **(c)**). (Use induction on n and Theorem 4.4.12.) □

Remark 4.4.14. If I just gave you the fraction $\dfrac{\left(1-q^{n}\right)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right)}{\left(1-q^{k}\right)\left(1-q^{k-1}\right)\cdots\left(1-q^{1}\right)}$, you would be surprised to hear that it is a polynomial (i.e., that the denominator divides the numerator) and has nonnegative coefficients. But given the way we defined $\dbinom{n}{k}_{q}$, you are now getting this for free from Theorem 4.4.13.

Theorem 4.4.13 **(b)** can be rewritten in a somewhat simpler way using the following notations:

Definition 4.4.15. (a) For any $n \in \mathbb{N}$, define the *q-integer* $[n]_q$ to be

$$[n]_q := q^0 + q^1 + \cdots + q^{n-1} \in \mathbb{Z}[q].$$

(b) For any $n \in \mathbb{N}$, define the *q-factorial* $[n]_q!$ to be

$$[n]_q! := [1]_q [2]_q \cdots [n]_q \in \mathbb{Z}[q].$$

(c) As usual, if a is an element of a ring A, then $[n]_a$ and $[n]_a!$ will mean the results of substituting a for q in $[n]_q$ and $[n]_q!$, respectively. Thus, explicitly, $[n]_a = a^0 + a^1 + \cdots + a^{n-1}$ and $[n]_a! = [1]_a [2]_a \cdots [n]_a$.

Remark 4.4.16. For any $n \in \mathbb{N}$, we have

$$[n]_q = \frac{1-q^n}{1-q} \qquad \text{(in } \mathbb{Z}[[q]] \text{ or in the ring of rational functions over } \mathbb{Q}\text{)}$$

and

$$[n]_1 = n \qquad \text{and} \qquad [n]_1! = n!.$$

Proof of Remark 4.4.16. Let $n \in \mathbb{N}$. We have

$$[n]_q := q^0 + q^1 + \cdots + q^{n-1} = \frac{1-q^n}{1-q},$$

since

$$\begin{aligned}(1-q)\left(q^0+q^1+\cdots+q^{n-1}\right) &= \left(q^0+q^1+\cdots+q^{n-1}\right) - q\left(q^0+q^1+\cdots+q^{n-1}\right)\\ &= \left(q^0+q^1+\cdots+q^{n-1}\right) - \left(q^1+q^2+\cdots+q^n\right)\\ &= \underbrace{q^0}_{=1} - q^n = 1-q^n.\end{aligned}$$

Furthermore, substituting 1 for q in the equality $[n]_q = q^0 + q^1 + \cdots + q^{n-1}$, we obtain

$$[n]_1 = 1^0 + 1^1 + \cdots + 1^{n-1} = \underbrace{1+1+\cdots+1}_{n \text{ times}} = n. \qquad (149)$$

Substituting 1 for q in the equality $[n]_q! = [1]_q [2]_q \cdots [n]_q$, we obtain

$$[n]_1! = \underbrace{[1]_1}_{\substack{=1\\ \text{(by (149))}}} \underbrace{[2]_1}_{\substack{=2\\ \text{(by (149))}}} \cdots \underbrace{[n]_1}_{\substack{=n\\ \text{(by (149))}}} = 1 \cdot 2 \cdot \cdots \cdot n = n!.$$

□

Theorem 4.4.17. Let $n, k \in \mathbb{N}$ with $n \geq k$. Then,

$$\binom{n}{k}_q = \frac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q!} = \frac{[n]_q!}{[k]_q! \cdot [n-k]_q!}$$

(in the ring $\mathbb{Z}[[q]]$ or in the ring of rational functions over $\mathbb{Q}$).

Proof. This is left as a homework exercise (Exercise A.3.4.1 **(d)**). □

A consequence of this theorem is the following symmetry property of q-binomial coefficients:

Proposition 4.4.18. Let $n, k \in \mathbb{N}$. Then,

$$\binom{n}{k}_q = \binom{n}{n-k}_q.$$

Proof. This is left as a homework exercise (Exercise A.3.4.1 **(e)**). □

4.4.4. q-binomial formulas

The properties we have seen so far are suggesting that q-binomial coefficients not only generalize binomial coefficients, but also share most of their properties in a somewhat modified form. In other words, we start expecting most properties of binomial coefficients to generalize to q-binomial coefficients, often in several ways (e.g., the recurrence of the binomial coefficients generalized in two ways).

Let us see how this expectation holds up for the most famous property of binomial coefficients: the binomial formula

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

This formula holds whenever a and b are two elements of a commutative ring, or even more generally, whenever a and b are two commuting elements of an arbitrary ring. If we want to integrate a q into this formula, we need to

- either change the structure of the formula,
- or modify the commutativity assumption.

This gives rise to two different "q-analogues" of the binomial formula. Both are important (one for the theory of partitions, and another for the theory of quantum groups). Here is the first one:

Theorem 4.4.19 (1st q-binomial theorem)**.** Let K be a commutative ring. Let $a, b \in K$ and $n \in \mathbb{N}$. In the polynomial ring $K[q]$, we have

$$\left(aq^0 + b\right)\left(aq^1 + b\right)\cdots\left(aq^{n-1} + b\right) = \sum_{k=0}^{n} q^{k(k-1)/2} \binom{n}{k}_q a^k b^{n-k}.$$

Note that setting $q = 1$ in Theorem 4.4.19 (i.e., substituting 1 for q) recovers the good old binomial formula, since all the n factors on the left hand side become $a + b$.

There is a straightforward way to prove Theorem 4.4.19 by induction on n (see Exercise A.3.4.2 **(a)**). Let us instead give a nicer argument. This argument will rely on the following general fact:

Lemma 4.4.20. Let L be a commutative ring. Let $n \in \mathbb{N}$. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. Let $a_1, a_2, \ldots, a_n$ be n elements of L. Let $b_1, b_2, \ldots, b_n$ be n further elements of L. Then,

$$\prod_{i=1}^{n} (a_i + b_i) = \sum_{S \subseteq [n]} \left(\prod_{i \in S} a_i \right) \left(\prod_{i \in [n] \setminus S} b_i \right). \tag{150}$$

Lemma 4.4.20 is well-known and intuitively clear: When expanding the product $\prod_{i=1}^{n} (a_i + b_i) = (a_1 + b_1)(a_2 + b_2) \cdots (a_n + b_n)$, you obtain a sum of 2^n terms, each of which is a product of one addend chosen from each of the n sums $a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n$. This is precisely what the right hand side of (150) is. A rigorous proof of Lemma 4.4.20 can be found in [Grinbe15, Exercise 6.1 **(a)**].

Proof of Theorem 4.4.19. Let $[n]$ denote the set $\{1,2,\ldots,n\}$. We have

$$\left(aq^0+b\right)\left(aq^1+b\right)\cdots\left(aq^{n-1}+b\right)=\prod_{i=1}^{n}\left(aq^{i-1}+b\right)$$

$$=\sum_{S\subseteq[n]}\underbrace{\left(\prod_{i\in S}\left(aq^{i-1}\right)\right)}_{=a^{|S|}\prod\limits_{i\in S}q^{i-1}}\underbrace{\left(\prod_{i\in[n]\setminus S}b\right)}_{=b^{|[n]\setminus S|}}$$

$$\left(\text{by Lemma 4.4.20, applied to } L=K\left[q\right],\ a_i=aq^{i-1} \text{ and } b_i=b\right)$$

$$=\underbrace{\sum_{S\subseteq[n]}}_{=\sum\limits_{k=0}^{n}\ \sum\limits_{\substack{S\subseteq[n];\\|S|=k}}} a^{|S|}\underbrace{\left(\prod_{i\in S}q^{i-1}\right)}_{\substack{=q^{\operatorname{sum}S-|S|}\\ \text{(since the sum of the exponents } i-1\\ \text{over all } i\in S \text{ is precisely } \operatorname{sum}S-|S|)}} b^{|[n]\setminus S|}$$

$$=\sum_{k=0}^{n}\ \sum_{\substack{S\subseteq[n];\\|S|=k}}\underbrace{a^{|S|}}_{\substack{=a^k\\ \text{(since } |S|=k)}}\underbrace{q^{\operatorname{sum}S-|S|}}_{\substack{=q^{\operatorname{sum}S-k}\\ \text{(since } |S|=k)}}\underbrace{b^{|[n]\setminus S|}}_{\substack{=b^{n-k}\\ \text{(since } S \text{ is a } k\text{-element}\\ \text{subset of the } n\text{-element}\\ \text{set } [n]\text{, and thus we}\\ \text{have } |[n]\setminus S|=n-k)}}$$

$$=\sum_{k=0}^{n}\ \sum_{\substack{S\subseteq[n];\\|S|=k}} a^k \underbrace{q^{\operatorname{sum}S-k}}_{\substack{=q^{\operatorname{sum}S-(1+2+\cdots+k)}q^{1+2+\cdots+(k-1)}\\ =q^{\operatorname{sum}S-(1+2+\cdots+k)}q^{k(k-1)/2}\\ \text{(since } 1+2+\cdots+(k-1)=k(k-1)/2)}} b^{n-k}$$

$$=\sum_{k=0}^{n}\ \sum_{\substack{S\subseteq[n];\\|S|=k}} a^k q^{\operatorname{sum}S-(1+2+\cdots+k)}q^{k(k-1)/2}b^{n-k}$$

$$=\sum_{k=0}^{n}q^{k(k-1)/2}\underbrace{\left(\sum_{\substack{S\subseteq[n];\\|S|=k}}q^{\operatorname{sum}S-(1+2+\cdots+k)}\right)}_{\substack{=\dbinom{n}{k}_q\\ \text{(by Proposition 4.4.7 }\textbf{(b)}\text{,}\\ \text{since } [n]=\{1,2,\ldots,n\})}}a^kb^{n-k}=\sum_{k=0}^{n}q^{k(k-1)/2}\binom{n}{k}_q a^kb^{n-k}.$$

This proves Theorem 4.4.19. □

The 2nd q-binomial theorem grows out of noncommutativity:

Theorem 4.4.21 (2nd q-binomial theorem, aka Potter's binomial theorem)**.** Let L be a commutative ring. Let $\omega \in L$. Let A be a noncommutative L-algebra. Let $a, b \in A$ be such that $ba = \omega ab$. Then,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}_{\omega} a^k b^{n-k}.$$

The condition $ba = \omega ab$ looks somewhat artificial – do such elements a, b actually exist in the wild? Indeed they do, as the following examples show:

Example 4.4.22. Let $L = \mathbb{Z}$ and $\omega = -1$ and $A = \mathbb{Z}^{2\times 2}$ (the ring of 2×2-matrices with integer entries). Let

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

It is easy to check that these two matrices satisfy $ba = -ab$, that is, $ba = \omega ab$. Thus, Theorem 4.4.21 predicts that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k}_{\omega} a^k b^{n-k}.$$

And this is indeed true (check it for $n = 3$).

Example 4.4.23. Let $L = \mathbb{R}$. Let A be the ring of $\mathbb{R}$-linear operators on $C^\infty(\mathbb{R}) = \{\text{smooth functions from } \mathbb{R} \text{ to } \mathbb{R}\}$. Let ω be any real number.

Let $b \in A$ be the differentiation operator (sending each $f \in C^\infty(\mathbb{R})$ to f').

Let $a \in A$ be the operator that substitutes ωx for x in the function (in other words, it shrinks the plot of the function by ω in the x-direction).

Then, you can check that $ba = \omega ab$. (Indeed, $(f(\omega x))' = \omega f'(\omega x)$.)

The proof of Theorem 4.4.21 is again a homework exercise (Exercise A.3.4.2 **(b)**).

The two q-binomial theorems are not entirely unrelated: Theorem 4.4.19 can be obtained from Theorem 4.4.21. (See Exercise A.3.4.14 for the details.)

4.4.5. Counting subspaces of vector spaces

We have introduced the q-binomial coefficient $\binom{n}{k}_q$ as a generating function for a certain sort of partitions – i.e., a "weighted number" of partitions, where each partition λ has weight $q^{|\lambda|}$. However, for certain integers a, the number $\binom{n}{k}_a$ has other interpretations, too. A particularly striking one can be found when a is the size of a finite field.

Let us recall a few things about finite fields:

- For any prime power p^k, there is a finite field of size p^k; it is unique up to isomorphism, and is therefore often called the "Galois field of size p^k" and denoted by $\mathbb{F}_{p^k}$. The finite fields $\mathbb{F}_{p^1}$ are easiest to construct – they are just the quotient rings $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p$ (that is, the rings of integers modulo p). Higher prime powers are more complicated. For example, the finite field $\mathbb{F}_{p^2}$ can be obtained by starting with $\mathbb{Z}/p$ and adjoining a square root of an element that is not a square. It is not $\mathbb{Z}/p^2$, since $\mathbb{Z}/p^2$ is not a field!

- Linear algebra (i.e., the notions of vector spaces, subspaces, linear independence, bases, matrices, Gaussian elimination, etc.) can be done over any field. In fact, many of its concepts can be defined over any commutative ring, but only over fields do they behave as nicely as they do over the real numbers. Thus, much of the linear algebra that you have learned over the real numbers remains valid over any field. (Exceptions are some properties that rely on positivity or on characteristic 0.)

Thus, it makes sense to talk about finite-dimensional vector spaces over finite fields. Such spaces are finite as sets, and thus can be viewed as combinatorial objects. An n-dimensional vector space over a finite field F has size $|F|^n$.

Now, we might wonder how many k-dimensional subspaces such an n-dimensional vector space has. The answer is given by the following theorem:

> **Theorem 4.4.24.** Let F be a finite field. Let $n, k \in \mathbb{N}$. Let V be an n-dimensional F-vector space. Then,
>
> $$\binom{n}{k}_{|F|} = (\text{\# of } k\text{-dimensional vector subspaces of } V)\,.$$

Compare this with the classical fact that if S is an n-element set, then

$$\binom{n}{k} = (\text{\# of } k\text{-element subsets of } S)\,.$$

This hints at an analogy between finite sets and finite-dimensional vector spaces. Such an analogy does indeed exist; the expository paper [Cohn04] gives a great overview over its reach.

The easiest proof of Theorem 4.4.24 uses three lemmas. The first one is a classical fact from linear algebra, which holds for any vector space (not necessarily finite-dimensional) over any field (not necessarily finite):

Lemma 4.4.25. Let F be a field. Let V be an F-vector space. Let $(v_1, v_2, \ldots, v_k)$ be a k-tuple of vectors in V. Then, $(v_1, v_2, \ldots, v_k)$ is linearly independent if and only if each $i \in \{1, 2, \ldots, k\}$ satisfies $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$ (where the span $\operatorname{span}()$ of an empty list is understood to be the set $\{\mathbf{0}\}$ consisting only of the zero vector $\mathbf{0}$). In other words, $(v_1, v_2, \ldots, v_k)$ is linearly independent if and only if we have

$$\begin{aligned}
& v_1 \notin \underbrace{\operatorname{span}()}_{=\{\mathbf{0}\}} && \text{and} \\
& v_2 \notin \operatorname{span}(v_1) && \text{and} \\
& v_3 \notin \operatorname{span}(v_1, v_2) && \text{and} \\
& \cdots && \text{and} \\
& v_k \notin \operatorname{span}(v_1, v_2, \ldots, v_{k-1}).
\end{aligned}$$

Proof of Lemma 4.4.25. We must prove that $(v_1, v_2, \ldots, v_k)$ is linearly independent if and only if each $i \in \{1, 2, \ldots, k\}$ satisfies $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$. This is an "if and only if" statement; we shall prove its "only if" (i.e., "$\Longrightarrow$") and "if" (i.e., "$\Longleftarrow$") directions separately:

$\Longrightarrow$: Assume that the k-tuple $(v_1, v_2, \ldots, v_k)$ is linearly independent. Let $i \in \{1, 2, \ldots, k\}$. If we had $v_i \in \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$, then we could write v_i in the form $v_i = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{i-1} v_{i-1}$ for some coefficients $\alpha_1, \alpha_2, \ldots, \alpha_{i-1} \in F$, and therefore these coefficients $\alpha_1, \alpha_2, \ldots, \alpha_{i-1}$ would satisfy

$$\begin{aligned}
& \underbrace{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_{i-1} v_{i-1}}_{=v_i} + \underbrace{(-1) v_i}_{=-v_i} + \underbrace{0 v_{i+1} + 0 v_{i+2} + \cdots + 0 v_k}_{=\mathbf{0}} \\
& = v_i + (-v_i) + \mathbf{0} = \mathbf{0},
\end{aligned}$$

which would be a nontrivial linear dependence relation between $(v_1, v_2, \ldots, v_k)$ (nontrivial because v_i appears in it with the nonzero coefficient -1); this would contradict the linear independence of $(v_1, v_2, \ldots, v_k)$. Hence, we cannot have $v_i \in \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$. In other words, we have $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$.

Forget that we fixed i. We thus have shown that each $i \in \{1, 2, \ldots, k\}$ satisfies $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$. This proves the "$\Longrightarrow$" direction of our claim.

$\Longleftarrow$: Assume that each $i \in \{1, 2, \ldots, k\}$ satisfies $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$. We must prove that the k-tuple $(v_1, v_2, \ldots, v_k)$ is linearly independent. Indeed, assume the contrary. Thus, this k-tuple is linearly dependent. In other words, there exist coefficients $\beta_1, \beta_2, \ldots, \beta_k \in F$ that satisfy $\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k = \mathbf{0}$ and that are not all zero. Consider these $\beta_1, \beta_2, \ldots, \beta_k$. At least one $i \in \{1, 2, \ldots, k\}$ satisfies $\beta_i \neq 0$ (since the coefficients $\beta_1, \beta_2, \ldots, \beta_k$ are not all zero).

Pick the **largest** such i. Thus, $\beta_i \neq 0$ but $\beta_{i+1} = \beta_{i+2} = \cdots = \beta_k = 0$. Hence,

$$\begin{aligned}
&\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k \\
&= \left(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{i-1} v_{i-1}\right) + \beta_i v_i + \underbrace{\left(\beta_{i+1} v_{i+1} + \beta_{i+2} v_{i+2} + \cdots + \beta_k v_k\right)}_{\substack{=0v_{i+1}+0v_{i+2}+\cdots+0v_k \\ =\mathbf{0}}} \\
&= \left(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{i-1} v_{i-1}\right) + \beta_i v_i,
\end{aligned}$$

so that

$$\begin{aligned}
\beta_i v_i &= \underbrace{\left(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_k v_k\right)}_{=\mathbf{0}} - \left(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{i-1} v_{i-1}\right) \\
&= -\left(\beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_{i-1} v_{i-1}\right) \\
&= \left(-\beta_1\right) v_1 + \left(-\beta_2\right) v_2 + \cdots + \left(-\beta_{i-1}\right) v_{i-1} \\
&\in \operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right).
\end{aligned}$$

Since $\beta_i \neq 0$, we thus obtain $v_i \in \operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right)$ (since $\operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right)$ is an F-vector subspace of V and thus preserved under scaling). This contradicts our assumption that $v_i \notin \operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right)$. This contradiction shows that our assumption was wrong, and thus completes our proof of the "$\Longleftarrow$" direction of our claim.

Thus, both directions of our claim are proved. This concludes the proof of Lemma 4.4.25. □

The next lemma we are going to use is itself an answer to a rather natural counting problem. Indeed, it is well-known that (see, e.g., [19fco, Proposition 2.7.2]) if X is an n-element set, and if $k \in \mathbb{N}$, then the

$$\begin{aligned}
&(\text{\# of } k\text{-tuples of distinct elements of } X) \\
&= n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right) = \prod_{i=0}^{k-1}\left(n-i\right).
\end{aligned} \tag{151}$$

The following lemma is a "linear analogue" of this combinatorial fact: The n-element set X is replaced by an n-dimensional vector space V, and "distinct elements" are replaced by "linearly independent vectors". The answer is rather similar:

Lemma 4.4.26. Let F be a finite field. Let $n, k \in \mathbb{N}$. Let V be an n-dimensional F-vector space. Then,

$$\begin{aligned}
&(\text{\# of linearly independent } k\text{-tuples of vectors in } V) \\
&= \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right) = \prod_{i=0}^{k-1}\left(|F|^n - |F|^i\right).
\end{aligned}$$

Proof of Lemma 4.4.26. We have $|V| = |F|^n$ (since V is an n-dimensional F-vector space).

Lemma 4.4.25 says that a k-tuple $(v_1, v_2, \ldots, v_k)$ of vectors in V is linearly independent if and only if it satisfies

$$\begin{aligned} & v_1 \notin \underbrace{\operatorname{span}()}_{=\{\mathbf{0}\}} \qquad \text{and} \\ & v_2 \notin \operatorname{span}(v_1) \qquad \text{and} \\ & v_3 \notin \operatorname{span}(v_1, v_2) \qquad \text{and} \\ & \quad \cdots \qquad \text{and} \\ & v_k \notin \operatorname{span}(v_1, v_2, \ldots, v_{k-1}). \end{aligned}$$

Thus, we can construct a linearly independent k-tuple $(v_1, v_2, \ldots, v_k)$ of vectors in V as follows, proceeding entry by entry:

- First, we choose v_1. This has to be a vector in $V \setminus \underbrace{\operatorname{span}()}_{=\{\mathbf{0}\}}$ (because it has to satisfy $v_1 \notin \operatorname{span}()$); thus, there are $|V \setminus \operatorname{span}()| = |V| - \underbrace{|\operatorname{span}()|}_{=1} = |V| - 1$ options for it.

  Once v_1 has been chosen, we have obtained a linearly independent singleton list (v_1). Hence, its span $\operatorname{span}(v_1)$ has dimension 1 (as an F-vector space) and thus size $|F|^1$. In other words, $|\operatorname{span}(v_1)| = |F|^1$.

- Next, we choose v_2. This has to be a vector in $V \setminus \operatorname{span}(v_1)$ (because it has to satisfy $v_2 \notin \operatorname{span}(v_1)$); thus, there are $|V| - \underbrace{|\operatorname{span}(v_1)|}_{=|F|^1} = |V| - |F|^1$ options for it.

  Once v_2 has been chosen, we have obtained a linearly independent list (v_1, v_2). Hence, its span $\operatorname{span}(v_1, v_2)$ has dimension 2 (as an F-vector space) and thus size $|F|^2$. In other words, $|\operatorname{span}(v_1, v_2)| = |F|^2$.

- Next, we choose v_3. This has to be a vector in $V \setminus \operatorname{span}(v_1, v_2)$ (because it has to satisfy $v_3 \notin \operatorname{span}(v_1, v_2)$); thus, there are $|V| - \underbrace{|\operatorname{span}(v_1, v_2)|}_{=|F|^2} = |V| - |F|^2$ options for it.

  Once v_3 has been chosen, we have obtained a linearly independent list (v_1, v_2, v_3). Hence, its span $\operatorname{span}(v_1, v_2, v_3)$ has dimension 3 (as an F-vector space) and thus size $|F|^3$. In other words, $|\operatorname{span}(v_1, v_2, v_3)| = |F|^3$.

- And so on, until the last vector v_k in our list has been chosen.

The total # of ways to perform this construction is

$$(|V|-1)\left(|V|-|F|^1\right)\left(|V|-|F|^2\right)\cdots\left(|V|-|F|^{k-1}\right).$$

Hence,

$$\begin{aligned}&(\text{\# of linearly independent } k\text{-tuples of vectors in } V)\\&=(|V|-1)\left(|V|-|F|^1\right)\left(|V|-|F|^2\right)\cdots\left(|V|-|F|^{k-1}\right)\\&=\prod_{i=0}^{k-1}\left(|V|-|F|^i\right)=\prod_{i=0}^{k-1}\left(|F|^n-|F|^i\right)\end{aligned}$$

(since $|V|=|F|^n$). This proves Lemma 4.4.26. □

Another lemma we will need is a basic combinatorial principle (often illustrated by the saying "to count a flock of sheep, count the legs and divide by 4"):

Lemma 4.4.27 (Multijection principle)**.** Let A and B be two finite sets. Let $m\in\mathbb{N}$. Let $f:A\to B$ be any map. Assume that each $b\in B$ has exactly m preimages under f (that is, for each $b\in B$, there are exactly m many elements $a\in A$ such that $f(a)=b$). Then,

$$|A|=m\cdot|B|.$$

Proof. Easy and LTTR. □

We note that a map $f:A\to B$ satisfying the assumption of Lemma 4.4.27 is often called an *m-to-1 map*.

Proof of Theorem 4.4.24. First of all, we notice that if $k>n$, then $\binom{n}{k}_{|F|}=0$ (by Proposition 4.4.9) and $(\text{\# of } k\text{-dimensional vector subspaces of } V)=0$ (since the dimension of a subspace of V is never larger than the dimension of V). Thus, Theorem 4.4.24 is true when $k>n$. Hence, for the rest of this proof, we WLOG assume that $k\leq n$.

We will use the shorthand "linind" for the words "linearly independent".

If $(v_1,v_2,\ldots,v_k)$ is a linind k-tuple of vectors in V, then $\operatorname{span}(v_1,v_2,\ldots,v_k)$ is a k-dimensional vector subspace of V. Hence, we can define a map

$$\begin{aligned}f:\{\text{linind } k\text{-tuples of vectors in } V\}&\to\{k\text{-dimensional vector subspaces of } V\},\\(v_1,v_2,\ldots,v_k)&\mapsto\operatorname{span}(v_1,v_2,\ldots,v_k).\end{aligned}$$

Consider this map f. We claim the following:

Observation 1: Each k-dimensional vector subspace of V has exactly

$$\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)$$

preimages under f.

[*Proof of Observation 1:* Let W be a k-dimensional vector subspace of V. We must prove that

$$(\text{\# of preimages of } W \text{ under } f) = \left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right).$$

A preimage of W under f is a k-tuple of vectors in V that spans W (by the very definition of f). Obviously, all the k vectors in such a k-tuple must belong to W. Thus, a preimage of W under f is a k-tuple of vectors in W that spans W. However, the vector space W is k-dimensional. Thus, a k-tuple of vectors in W spans W if and only if this k-tuple is linind[58]. Therefore, a preimage of W under f is a linind k-tuple of vectors in W. Hence,

$$\begin{aligned}&(\text{\# of preimages of } W \text{ under } f)\\ &= (\text{\# of linearly independent } k\text{-tuples of vectors in } W)\\ &= \left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)\end{aligned}$$

(by Lemma 4.4.26, applied to W and k instead of V and n). This proves Observation 1.]

Now, Observation 1 shows that each k-dimensional vector subspace of V has exactly $\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)$ preimages under f. Hence, Lemma 4.4.27 (applied to $A = \{\text{linind } k\text{-tuples of vectors in } V\}$ and $B = \{k\text{-dimensional vector subspaces of } V\}$ and $m = \left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)$) shows that

$$\begin{aligned}&(\text{\# of linind } k\text{-tuples of vectors in } V)\\ &= \left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)\\ &\qquad \cdot (\text{\# of } k\text{-dimensional vector subspaces of } V).\end{aligned}$$

However, Lemma 4.4.26 yields

$$\begin{aligned}&(\text{\# of linind } k\text{-tuples of vectors in } V)\\ &= \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right).\end{aligned}$$

[58] Again, we are using a simple fact from linear algebra here, which is true over any field (not necessarily finite): A k-tuple of vectors in a k-dimensional vector space spans the space if and only if it is linind.

Comparing these two equalities, we obtain

$$\begin{aligned}
&\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right) \\
&\qquad\qquad \cdot (\text{\# of } k\text{-dimensional vector subspaces of } V) \\
&= \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&(\text{\# of } k\text{-dimensional vector subspaces of } V) \\
&= \frac{\left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right)}{\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)} \\
&= \frac{\prod\limits_{i=0}^{k-1}\left(|F|^n - |F|^i\right)}{\prod\limits_{i=0}^{k-1}\left(|F|^k - |F|^i\right)} = \prod_{i=0}^{k-1} \underbrace{\frac{|F|^n - |F|^i}{|F|^k - |F|^i}}_{\substack{=\frac{|F|^i\left(|F|^{n-i}-1\right)}{|F|^i\left(|F|^{k-i}-1\right)}=\frac{|F|^{n-i}-1}{|F|^{k-i}-1} \\ =\frac{1-|F|^{n-i}}{1-|F|^{k-i}}}} = \prod_{i=0}^{k-1} \frac{1-|F|^{n-i}}{1-|F|^{k-i}} \\
&= \frac{\prod\limits_{i=0}^{k-1}\left(1 - |F|^{n-i}\right)}{\prod\limits_{i=0}^{k-1}\left(1 - |F|^{k-i}\right)} = \frac{\left(1-|F|^n\right)\left(1-|F|^{n-1}\right)\cdots\left(1-|F|^{n-k+1}\right)}{\left(1-|F|^k\right)\left(1-|F|^{k-1}\right)\cdots\left(1-|F|^1\right)} \\
&= \binom{n}{k}_{|F|}
\end{aligned}$$

(since substituting $|F|$ for q in Theorem 4.4.13 **(b)** yields $\binom{n}{k}_{|F|} = \dfrac{\left(1-|F|^n\right)\left(1-|F|^{n-1}\right)\cdots\left(1-|F|^{n-k+1}\right)}{\left(1-|F|^k\right)\left(1-|F|^{k-1}\right)\cdots\left(1-|F|^1\right)}$). This proves Theorem 4.4.24. □

4.4.6. Limits of q-binomial coefficients

There is much more to say about q-binomial coefficients, but let us just briefly focus on their limiting behavior. This is not analogous to anything known from usual binomial coefficients; indeed, the limit $\lim\limits_{n\to\infty}\dbinom{n}{k}$ does not exist for any positive integer k. However, q-binomial coefficients behave much better in this regard.

Indeed, consider the q-binomial coefficients $\dbinom{n}{2}_q$ for various values of n:

$$\begin{aligned}
\binom{0}{2}_q &= 0, \\
\binom{1}{2}_q &= 0, \\
\binom{2}{2}_q &= 1, \\
\binom{3}{2}_q &= 1 + q + q^2, \\
\binom{4}{2}_q &= 1 + q + 2q^2 + q^3 + q^4, \\
\binom{5}{2}_q &= 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6, \\
\binom{6}{2}_q &= 1 + q + 2q^2 + 2q^3 + 3q^4 + 2q^5 + 2q^6 + q^7 + q^8.
\end{aligned}$$

It appears from these examples that the sequence $\left(\dbinom{n}{2}_q\right)_{n\in\mathbb{N}}$ coefficientwise stabilizes[59] to

$$1 + q + 2q^2 + 2q^3 + 3q^4 + 3q^5 + \cdots = \sum_{n\in\mathbb{N}} \left(1 + \left\lfloor \frac{n}{2} \right\rfloor\right) q^n.$$

And this is indeed the case:

Proposition 4.4.28. Let $k \in \mathbb{N}$ be fixed. Then,

$$\lim_{n\to\infty} \binom{n}{k}_q = \sum_{n\in\mathbb{N}} \left(p_0\left(n\right) + p_1\left(n\right) + \cdots + p_k\left(n\right)\right) q^n = \prod_{i=1}^{k} \frac{1}{1-q^i}.$$

(See Definition 4.1.3 **(a)** for the meaning of $p_i\left(n\right)$.)

[59] Recall Definition 3.13.2 for the notion of "coefficientwise stabilizing".

First proof of Proposition 4.4.28 (sketched). For each integer $n \geq k$, we have

$$\begin{aligned}\dbinom{n}{k}_q &= \frac{(1-q^n)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right)}{\left(1-q^k\right)\left(1-q^{k-1}\right)\cdots\left(1-q^1\right)} \qquad \text{(by Theorem 4.4.13 \textbf{(b)})} \\ &= \frac{\left(1-q^{n-k+1}\right)\left(1-q^{n-k+2}\right)\cdots\left(1-q^n\right)}{\left(1-q^1\right)\left(1-q^2\right)\cdots\left(1-q^k\right)} \\ &\qquad \text{(here, we have turned both products upside down)} \\ &= \frac{\prod\limits_{i=1}^{k}\left(1-q^{n-k+i}\right)}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} = \frac{1}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} \cdot \prod_{i=1}^{k}\left(1-q^{n-k+i}\right).\end{aligned}$$

However, we have $q^n \to 0$ as $n \to \infty$ (check this![60]). Thus, for each $i \in \{1,2,\ldots,k\}$, we have

$$q^{n-k+i} \to 0 \qquad \text{as } n \to \infty$$

(since the family $\left(q^{n-k+i}\right)_{n \geq k-i}$ is just a reindexing of the family $(q^n)_{n \geq 0}$), and therefore

$$1 - q^{n-k+i} \to 1 \qquad \text{as } n \to \infty.$$

Hence, Corollary 3.13.6 (applied to $f_{i,n} = 1 - q^{n-k+i}$ and $f_i = 1$) yields that

$$\sum_{i=1}^{k}\left(1-q^{n-k+i}\right) \to \sum_{i=1}^{k} 1 \qquad \text{and} \qquad \prod_{i=1}^{k}\left(1-q^{n-k+i}\right) \to \prod_{i=1}^{k} 1 \qquad \text{as } n \to \infty.$$

Thus, in particular, $\prod\limits_{i=1}^{k}\left(1-q^{n-k+i}\right) \to \prod\limits_{i=1}^{k} 1$ as $n \to \infty$. In other words,

$$\lim_{n\to\infty}\prod_{i=1}^{k}\left(1-q^{n-k+i}\right) = \prod_{i=1}^{k} 1 = 1.$$

Now, recall that each integer $n \geq k$ satisfies

$$\dbinom{n}{k}_q = \frac{1}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} \cdot \prod_{i=1}^{k}\left(1-q^{n-k+i}\right).$$

[60] This is a matter of understanding Definition 3.13.2.

Hence,

$$\begin{aligned}\lim_{n\to\infty}\dbinom{n}{k}_q &= \lim_{n\to\infty}\left(\frac{1}{\prod\limits_{i=1}^{k}(1-q^i)}\cdot\prod_{i=1}^{k}\left(1-q^{n-k+i}\right)\right)\\ &= \frac{1}{\prod\limits_{i=1}^{k}(1-q^i)}\cdot\underbrace{\lim_{n\to\infty}\prod_{i=1}^{k}\left(1-q^{n-k+i}\right)}_{=1} = \frac{1}{\prod\limits_{i=1}^{k}(1-q^i)}\\ &= \prod_{i=1}^{k}\frac{1}{1-q^i}. \qquad (152)\end{aligned}$$

Finally, Theorem 4.1.18 (with the letters x, m and k renamed as q, k and i) says that

$$\sum_{n\in\mathbb{N}}\left(p_0(n)+p_1(n)+\cdots+p_k(n)\right)q^n = \prod_{i=1}^{k}\frac{1}{1-q^i}.$$

Combining this with (152), we obtain

$$\lim_{n\to\infty}\dbinom{n}{k}_q = \sum_{n\in\mathbb{N}}\left(p_0(n)+p_1(n)+\cdots+p_k(n)\right)q^n = \prod_{i=1}^{k}\frac{1}{1-q^i}.$$

This proves Proposition 4.4.28. □

Second proof of Proposition 4.4.28 (sketched). For each $n\in\mathbb{N}$, we have

$$\dbinom{n}{k}_q = \sum_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k\\ \text{and length } \leq k}} q^{|\lambda|} \qquad (153)$$

(by the definition of $\dbinom{n}{k}_q$).

However, for each $n\in\mathbb{N}$, the sum $\sum\limits_{\substack{\lambda \text{ is a partition}\\ \text{with largest part } \leq n-k\\ \text{and length } \leq k}} q^{|\lambda|}$ is a partial sum of the sum $\sum\limits_{\substack{\lambda \text{ is a partition}\\ \text{with length } \leq k}} q^{|\lambda|}$, and this partial sum grows by more and more addends as n increases; each addend of the sum $\sum\limits_{\substack{\lambda \text{ is a partition}\\ \text{with length } \leq k}} q^{|\lambda|}$ gets eventually included in this partial sum (for sufficiently large n). From these observations, it is easy to obtain that

$$\sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{|\lambda|} \to \sum_{\substack{\lambda \text{ is a partition} \\ \text{with length } \leq k}} q^{|\lambda|} \qquad \text{as } n \to \infty.$$

In view of (153), this rewrites as

$$\binom{n}{k}_q \to \sum_{\substack{\lambda \text{ is a partition} \\ \text{with length } \leq k}} q^{|\lambda|} \qquad \text{as } n \to \infty.$$

Hence,

$$\begin{aligned} \lim_{n\to\infty} \binom{n}{k}_q &= \sum_{\substack{\lambda \text{ is a partition} \\ \text{with length } \leq k}} q^{|\lambda|} = \sum_{n\in\mathbb{N}} \underbrace{(\text{\# of partitions of } n \text{ having length } \leq k)}_{\substack{=p_0(n)+p_1(n)+\cdots+p_k(n) \\ \text{(by Definition 4.1.3 \textbf{(a)})}}} q^n \\ &= \sum_{n\in\mathbb{N}} \left(p_0(n) + p_1(n) + \cdots + p_k(n)\right) q^n = \prod_{i=1}^{k} \frac{1}{1-q^i} \end{aligned}$$

(by Theorem 4.1.18, with the letters x, m and k renamed as q, k and i). Thus, Proposition 4.4.28 is proved again. □

4.5. References

Thus ends our foray into integer partitions and related FPSs. We will partially revisit this topic later, as we discuss symmetric functions. Here are just a few things we are omitting:

- In 1919, Ramanujan discovered the following three congruences for $p(n)$:

$$\begin{aligned} p(n) &\equiv 0 \bmod 5 && \text{if } n \equiv 4 \bmod 5; \\ p(n) &\equiv 0 \bmod 7 && \text{if } n \equiv 5 \bmod 7; \\ p(n) &\equiv 0 \bmod 11 && \text{if } n \equiv 6 \bmod 11. \end{aligned}$$

  The first of these follows from the FPS equality

$$\sum_{n\in\mathbb{N}} p(5n+4)\, x^n = 5 \prod_{i=1}^{\infty} \frac{\left(1-x^{5i}\right)^5}{\left(1-x^i\right)^6},$$

  whose proof is far from straightforward. All of these results (and some rather subtle generalizations) are shown in [Berndt06, Chapter 2] and [Hirsch17, Chapters 3 and 5]; see also [Aigner07, Chapter 3, Highlight] for a proof of the latter equality.

- An asymptotic expansion for $p\left(n\right)$ (found by Hardy and Ramanujan in 1918) is
$$p\left(n\right)\sim\frac{1}{4n\sqrt{3}}\exp\left(\pi\sqrt{\frac{2n}{3}}\right)\qquad\text{as } n\to\infty. \tag{154}$$
See [Erdos42] for a proof.

- In 1770, Lagrange proved that every nonnegative integer n can be written as a sum of four perfect squares. In 1829, Jacobi strengthened this to a counting formula: If n is a positive integer, then the number of quadruples $\left(a,b,c,d\right)$ of integers satisfying $n=a^2+b^2+c^2+d^2$ is 8 times the sum of positive divisors of n that are not divisible by 4. The most elementary proofs of this striking result use partition-related FPSs and the Jacobi Triple Product Identity. (See [Hirsch87] for a self-contained proof; see also [Hirsch17, Chapter 2] and [Berndt06, Chapter 3] for various related results.)

- The Rogers–Ramanujan identities
$$\sum_{k\in\mathbb{N}}\frac{x^{k^2}}{\left(1-x^1\right)\left(1-x^2\right)\cdots\left(1-x^k\right)}=\prod_{i\in\mathbb{N}}\frac{1}{\left(1-x^{5i+1}\right)\left(1-x^{5i+4}\right)}\qquad\text{and}$$
$$\sum_{k\in\mathbb{N}}\frac{x^{k(k+1)}}{\left(1-x^1\right)\left(1-x^2\right)\cdots\left(1-x^k\right)}=\prod_{i\in\mathbb{N}}\frac{1}{\left(1-x^{5i+2}\right)\left(1-x^{5i+3}\right)}$$
can be used to count partitions into parts that are congruent to $\pm1\operatorname{mod}5$ or congruent to $\pm2\operatorname{mod}5$, respectively. These surprising identities can be proved using Proposition 4.4.28 and the Jacobi Triple Product Identity; see [Doyle19] for a self-contained writeup of this proof.

Here is a list of references for further reading on partitions:

- The book [AndEri04] by Andrews and Eriksson is a beautiful (if not always fully precise) introduction to integer partitions and related topics.

- Pak's [Pak06] is a survey of identities between partition numbers (and related FPSs) with occasionally outlined proofs. (Beware: the writing is very terse and teems with typos.)

- Hirschhorn's [Hirsch17] (subtitled "a personal journey", not meant to be comprehensive) studies partitions through the lens of (mostly purely algebraic) manipulation of FPSs.

- Berndt's [Berndt06] is another (more analytic and number-theoretical) study of partition-related FPSs, with applications to number theory.

5. Permutations

We now come back to the foundations of combinatorics: We will study permutations of finite sets. I will assume that you know their most basic properties (see, e.g., [Strick13, Appendix B] and [Goodma15, §1.5] for refreshers; see also [Grinbe15, Chapter 5] for many more details on inversions), and will show some more advanced results. For deeper treatments, see [Bona12], [Sagan01] and [Stanle11, Chapter 1].

5.1. Basic definitions

Definition 5.1.1. Let X be a set.

(a) A *permutation* of X means a bijection from X to X.

(b) It is known that the set of all permutations of X is a group under composition. This group is called the *symmetric group* of X, and is denoted by S_X. Its neutral element is the identity map $\operatorname{id}_X : X \to X$. Its size is $|X|!$ when X is finite.

(Alternative notations for S_X include $\operatorname{Sym}(X)$ and Σ_X and $\mathfrak{S}_X$ and $\mathcal{S}_X$.)

(c) As usual in group theory, we will write $\alpha\beta$ for the composition $\alpha \circ \beta$ when $\alpha, \beta \in S_X$. This is the map that sends each $x \in X$ to $\alpha(\beta(x))$.

(d) If $\alpha \in S_X$ and $i \in \mathbb{Z}$, then α^i shall denote the i-th power of α in the group S_X. Note that $\alpha^i = \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{i \text{ times}}$ if $i \geq 0$. Also, $\alpha^0 = \operatorname{id}_X$. Also, α^{-1} is the inverse of α in the group S_X, that is, the inverse of the map α.

Definition 5.1.2. Let $n \in \mathbb{Z}$. Then, $[n]$ shall mean the set $\{1, 2, \ldots, n\}$. This is an n-element set if $n \geq 0$, and is an empty set if $n \leq 0$.

The symmetric group $S_{[n]}$ (consisting of all permutations of $[n]$) will be denoted S_n and called the *n-th symmetric group*. Its size is $n!$ (when $n \geq 0$).

For instance, S_3 is the group of all 6 permutations of the set $[3] = \{1, 2, 3\}$.

If two sets X and Y are in bijection, then their symmetric groups S_X and S_Y are isomorphic. Intuitively, this is clear (just think of Y as a "copy" of X with all elements relabelled, and use this to reinterpret each permutation of X as a permutation of Y). We can formalize this as the following proposition:

Proposition 5.1.3. Let X and Y be two sets, and let $f : X \to Y$ be a bijection. Then, for each permutation σ of X, the map $f \circ \sigma \circ f^{-1} : Y \to Y$ is a permutation of Y. Furthermore, the map

$$\begin{aligned} S_f : S_X &\to S_Y, \\ \sigma &\mapsto f \circ \sigma \circ f^{-1} \end{aligned}$$

is a group isomorphism; thus, we obtain $S_X \cong S_Y$.

Proof. Easy and LTTR. □

Because of Proposition 5.1.3, if you want to understand the symmetric groups of finite sets, you only need to understand S_n for all $n \in \mathbb{N}$ (because if X is a finite set of size n, then there is a bijection $f : X \to [n]$ and therefore a group isomorphism $S_f : S_X \to S_{[n]}$). Thus, we will focus mostly on S_n in this chapter.

Remark 5.1.4. If $Y = X$ in Proposition 5.1.3, then the group isomorphism S_f is conjugation by f in the group S_X.

Next, let us define three ways to represent a permutation:

Definition 5.1.5. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. We introduce three notations for σ:

(a) A *two-line notation* of σ means a $2 \times n$-array $\left(\begin{array}{cccc} p_1 & p_2 & \cdots & p_n \\ \sigma(p_1) & \sigma(p_2) & \cdots & \sigma(p_n) \end{array}\right)$, where the entries $p_1, p_2, \ldots, p_n$ of the top row are the n elements of $[n]$ in some order. Note that this is a standard notation for any kind of map from a finite set. Commonly, we pick $p_i = i$, so we get the array $\left(\begin{array}{cccc} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{array}\right)$.

(b) The *one-line notation* (short, *OLN*) of σ means the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$.

It is common to omit the commas and the parentheses when writing down the OLN of σ. Thus, one simply writes $\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n)$ instead of $(\sigma(1), \sigma(2), \ldots, \sigma(n))$. Note that this omission can make the notation ambiguous if some of the $\sigma(i)$ have more than one digit (for example, the OLN 1112345678910 can mean two different permutations of $[11]$, depending on whether you read the "111" part as "1, 11" or as "11, 1"). However, if $n \leq 10$, then this ambiguity does not occur, and the notation is unproblematic (even without commas and parentheses).

(c) The *cycle digraph* of σ is defined (informally) as follows:

- For each $i \in [n]$, draw a point ("node") labelled i.
- For each $i \in [n]$, draw an arrow ("arc") from the node labelled i to the node labelled $\sigma(i)$.

The resulting picture is called the cycle digraph of σ.

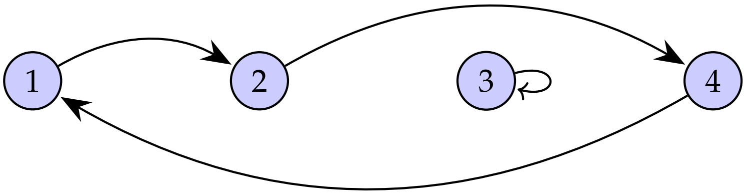
Using the concept of *digraphs* (= directed graphs), this definition can be restated formally as follows: The *cycle digraph* of σ is the directed graph with vertices $1, 2, \ldots, n$ and arcs $i \to \sigma(i)$ for all $i \in [n]$.

Example 5.1.6. Let $\sigma : [4] \to [4]$ be the map that sends the elements $1, 2, 3, 4$ to $2, 4, 3, 1$, respectively. Then, σ is a bijection, thus a permutation of $[4]$.

(a) A two-line notation of σ is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. Another is $\begin{pmatrix} 3 & 1 & 4 & 2 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Another is $\begin{pmatrix} 4 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$. There are 24 two-line notations of σ in total, since we can freely choose the order in which the elements of $[4]$ appear in the top row.

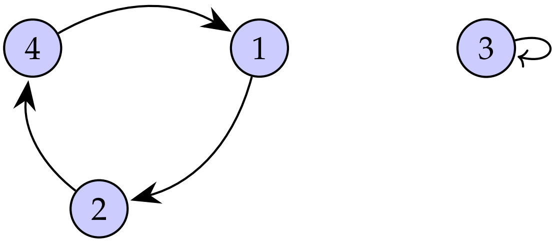
(b) The one-line notation of σ is $(2, 4, 3, 1)$. Omitting the commas and the parentheses, we can rewrite this as 2431.

(c) One way to draw the cycle digraph of σ is



.

Another is



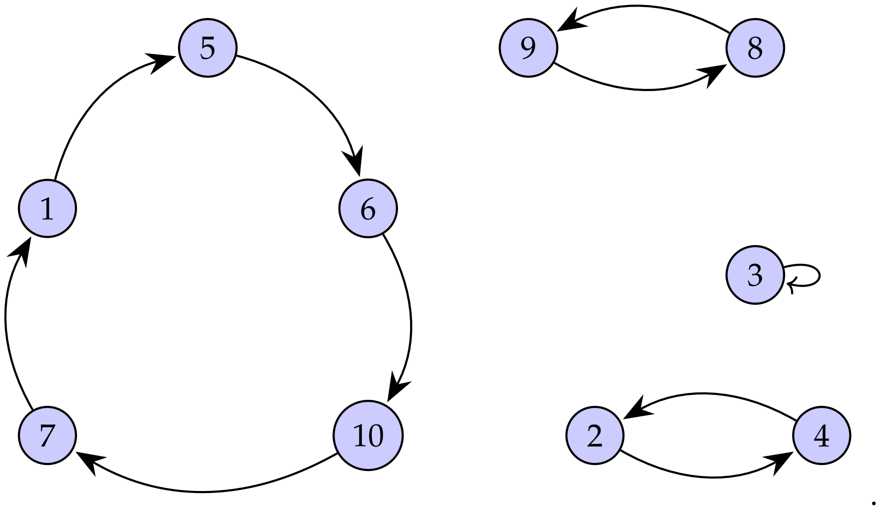
.

(When drawing cycle digraphs, one commonly tries to place the nodes in such a way as to make the arcs as short as possible. Thus, it is natural to keep the cycles separate in the picture. But formally speaking, any picture is fine, as long as the nodes and arcs don't overlap.)

Example 5.1.7. Let $\sigma : [10] \to [10]$ be the map that sends the elements $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ to $5, 4, 3, 2, 6, 10, 1, 9, 8, 7$, respectively. Then, σ is a bijection, hence a permutation of $[10]$. The one-line notation of σ is $(5, 4, 3, 2, 6, 10, 1, 9, 8, 7)$. If we omit the commas and the parentheses, then this becomes

$$5\,4\,3\,2\,6\ \ (10)\ \ 1\,9\,8\,7.$$

(We have put the 10 in parentheses to make its place clearer.) The cycle digraph of σ is



.

5.2. Transpositions and cycles

We shall now define some important families of permutations.

5.2.1. Transpositions

Definition 5.2.1. Let i and j be two distinct elements of a set X.

Then, the *transposition* $t_{i,j}$ is the permutation of X that sends i to j, sends j to i, and leaves all other elements of X unchanged.

Strictly speaking, the notation $t_{i,j}$ is somewhat ambiguous, since it suppresses X. However, most of the times we will use it, the set X will be either clear from the context or irrelevant.

Example 5.2.2. The permutation $t_{2,4}$ of the set $[7]$ sends the elements $1,2,3,4,5,6,7$ to $1,4,3,2,5,6,7$, respectively. Its one-line notation (with commas and parentheses omitted) is therefore 1432567.

Note that $t_{i,j} = t_{j,i}$ for any two distinct elements i and j of a set X.

Definition 5.2.3. Let $n \in \mathbb{N}$ and $i \in [n-1]$. Then, the *simple transposition* s_i is defined by

$$s_i := t_{i,i+1} \in S_n.$$

Thus, a simple transposition is a transposition that swaps two consecutive integers. Again, the notation s_i suppresses n, but this won't usually be a problem.

Example 5.2.4. The permutation s_2 of the set $[7]$ sends the elements $1,2,3,4,5,6,7$ to $1,3,2,4,5,6,7$, respectively. Its one-line notation is therefore 1324567.

Here are some very basic properties of simple transpositions:[61]

Proposition 5.2.5. Let $n \in \mathbb{N}$.

(a) We have $s_i^2 = \operatorname{id}$ for all $i \in [n-1]$. In other words, we have $s_i = s_i^{-1}$ for all $i \in [n-1]$.

(b) We have $s_i s_j = s_j s_i$ for any $i,j \in [n-1]$ with $|i-j| > 1$.

(c) We have $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ for any $i \in [n-2]$.

Proof. To prove that two permutations α and β of $[n]$ are identical, it suffices to show that $\alpha(k) = \beta(k)$ for each $k \in [n]$. Using this strategy, we can prove all three parts of Proposition 5.2.5 straightforwardly (distinguishing cases corresponding to the relative positions of k, i, $i+1$, j and $j+1$). This is done in detail for Proposition 5.2.5 **(c)** in [Grinbe15, solution to Exercise 5.1 **(a)**]; the proofs of parts **(a)** and **(b)** are easier and LTTR. □

5.2.2. Cycles

The following definition can be viewed as a generalization of Definition 5.2.1:

Definition 5.2.6. Let X be a set. Let $i_1, i_2, \ldots, i_k$ be k distinct elements of X. Then,

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$$

means the permutation of X that sends

$$\begin{aligned} &i_1 \text{ to } i_2, \\ &i_2 \text{ to } i_3, \\ &i_3 \text{ to } i_4, \\ &\ldots, \\ &i_{k-1} \text{ to } i_k, \\ &i_k \text{ to } i_1 \end{aligned}$$

and leaves all other elements of X unchanged. In other words, $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ means the permutation of X that satisfies

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k}(p) = \begin{cases} i_{j+1}, & \text{if } p = i_j \text{ for some } j \in \{1,2,\ldots,k\}; \\ p, & \text{otherwise} \end{cases} \qquad \text{for every } p \in X,$$

where i_{k+1} means i_1.

This permutation is called a *k-cycle*.

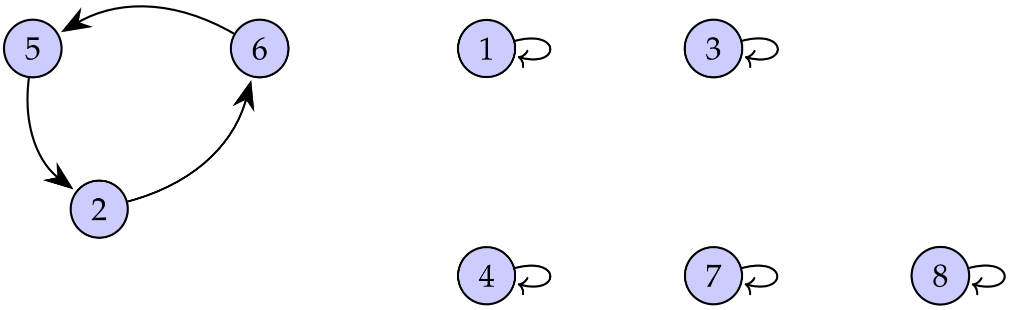
[61] Recall Definition 5.1.1. Thus, for example, s_i^2 means $s_i s_i = s_i \circ s_i$, whereas $s_i s_j$ means $s_i \circ s_j$.

The name "k-cycle" harkens back to the cycle digraph of $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$, which consists of a cycle of length k (containing the nodes $i_1, i_2, \ldots, i_k$ in this order) along with $|X| - k$ isolated nodes (more precisely, each of the elements of $X \setminus \{i_1, i_2, \ldots, i_k\}$ has an arrow from itself to itself in the cycle digraph of σ). Here is an example:

Example 5.2.7. Let $X = [8]$. Then, the permutation $\operatorname{cyc}_{2,6,5}$ of X sends

2 to 6,
6 to 5,
5 to 2

and leaves all other elements of X unchanged. Thus, this permutation has OLN 16342578 and cycle digraph



Example 5.2.8. Let X be a set. If i and j are two distinct elements of X, then $\operatorname{cyc}_{i,j} = t_{i,j}$. Thus, the 2-cycles in S_X are precisely the transpositions in S_X, so there are $\dbinom{|X|}{2}$ many of them (since any 2-element subset $\{i, j\}$ of X gives rise to a transposition $t_{i,j}$, and this assignment of transpositions to 2-element subsets is bijective).

Note that the k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is often denoted by $(i_1, i_2, \ldots, i_k)$, but I will not use this notation here, since it clashes with the standard notation for k-tuples.

Exercise 5.2.2.1. Let $n \in \mathbb{N}$ and let $k \in [n]$. Let X be an n-element set. How many k-cycles exist in S_X ?

Solution to Exercise 5.2.2.1 (sketched). First, we note that there is exactly one 1-cycle in S_X (for $n > 0$), since a 1-cycle is just the identity map. This should be viewed as a degenerate case; thus, we WLOG assume that $k > 1$.

For any k distinct elements $i_1, i_2, \ldots, i_k$ of X, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \operatorname{cyc}_{i_2,i_3,\ldots,i_k,i_1} = \operatorname{cyc}_{i_3,i_4,\ldots,i_k,i_1,i_2} = \cdots = \operatorname{cyc}_{i_k,i_1,i_2,\ldots,i_{k-1}}.$$

That is, $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ does not change if we cyclically rotate the list $(i_1, i_2, \ldots, i_k)$.

Any k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ uniquely determines the elements $i_1, i_2, \ldots, i_k$ up to cyclic rotation (since $k > 1$). Indeed, if $\sigma = \operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is a k-cycle, then the elements $i_1, i_2, \ldots, i_k$ are precisely the elements of X that are not fixed by σ (it is here that we use our assumption $k > 1$), and furthermore, if we know which of these elements is i_1, then we can reconstruct the remaining elements $i_2, i_3, \ldots, i_k$ recursively by

$$i_2 = \sigma(i_1), \qquad i_3 = \sigma(i_2), \qquad i_4 = \sigma(i_3), \qquad \ldots, \qquad i_k = \sigma(i_{k-1})$$

(that is, $i_2, i_3, \ldots, i_k$ are obtained by iteratively applying σ to i_1). Therefore, if $\sigma \in S_X$ is a k-cycle, then there are precisely k lists $(i_1, i_2, \ldots, i_k)$ for which $\sigma = \operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ (coming from the k possibilities for which of the k non-fixed points of σ should be i_1).

Hence, the map

$$\begin{aligned} f : \{k\text{-tuples of distinct elements of } X\} &\to \{k\text{-cycles in } S_X\}, \\ (i_1, i_2, \ldots, i_k) &\mapsto \operatorname{cyc}_{i_1,i_2,\ldots,i_k} \end{aligned}$$

is a k-to-1 map (i.e., each k-cycle in S_X has precisely k preimages under this map). Therefore, Lemma 4.4.27 (applied to $m = k$ and
$A = \{k\text{-tuples of distinct elements of } X\}$ and $B = \{k\text{-cycles in } S_X\}$) yields

$$(\#\text{ of } k\text{-tuples of distinct elements of } X) = k \cdot (\#\text{ of } k\text{-cycles in } S_X).$$

Therefore,

$$\begin{aligned} (\#\text{ of } k\text{-cycles in } S_X) &= \frac{1}{k} \cdot \underbrace{(\#\text{ of } k\text{-tuples of distinct elements of } X)}_{\substack{=n(n-1)(n-2)\cdots(n-k+1) \\ \text{(by (151), since } X \text{ is an } n\text{-element set)}}} \\ &= \frac{1}{k} \cdot n(n-1)(n-2)\cdots(n-k+1) \\ &= \binom{n}{k} \cdot (k-1)! \qquad \text{(by a bit of simple algebra)}. \end{aligned}$$

This is the answer to Exercise 5.2.2.1 in the case $k > 1$. Hence, Exercise 5.2.2.1 is solved. □

5.3. Inversions, length and Lehmer codes

5.3.1. Inversions and lengths

Let us define some features of arbitrary permutations of $[n]$:

Definition 5.3.1. Let $n \in \mathbb{N}$ and $\sigma \in S_n$.

(a) An *inversion* of σ means a pair (i, j) of elements of $[n]$ such that $i < j$ and $\sigma(i) > \sigma(j)$.

(b) The *length* (also known as the *Coxeter length*) of σ is the # of inversions of σ. It is called $\ell(\sigma)$. (Some authors call it $\operatorname{inv}\sigma$ instead.)

(In LaTeX, the symbol "ℓ" is obtained by typing "`\ell`". If you just type "`l`", you will get "l".)

An inversion of a permutation σ can thus be viewed as a pair of elements of $[n]$ whose relative order changes when σ is applied to them. (We require this pair (i, j) to satisfy $i < j$ in order not to count each such pair doubly.)

Example 5.3.2. Let $\pi \in S_4$ be the permutation with OLN 3142. The inversions of π are

$$(1,2) \qquad \left(\text{since } 1 < 2 \text{ and } \underbrace{\pi(1)}_{=3} > \underbrace{\pi(2)}_{=1}\right) \qquad \text{and}$$

$$(1,4) \qquad \left(\text{since } 1 < 4 \text{ and } \underbrace{\pi(1)}_{=3} > \underbrace{\pi(4)}_{=2}\right) \qquad \text{and}$$

$$(3,4) \qquad \left(\text{since } 3 < 4 \text{ and } \underbrace{\pi(3)}_{=4} > \underbrace{\pi(4)}_{=2}\right).$$

Thus, the length of π is 3.

For a given $n \in \mathbb{N}$ and a given $k \in \mathbb{N}$, how many permutations $\sigma \in S_n$ have length k ? The following proposition gives a partial answer:

Proposition 5.3.3. Let $n \in \mathbb{N}$.

(a) For any $\sigma \in S_n$, we have $\ell(\sigma) \in \left\{0, 1, \ldots, \dbinom{n}{2}\right\}$.

(b) We have

$$(\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = 0) = 1.$$

Indeed, the only permutation $\sigma \in S_n$ with $\ell(\sigma) = 0$ is the identity map id.

(c) We have

$$\left(\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = \binom{n}{2}\right) = 1.$$

Indeed, the only permutation $\sigma \in S_n$ with $\ell(\sigma) = \dbinom{n}{2}$ is the permutation with OLN $n(n-1)(n-2)\cdots 21$. (This permutation is often called w_0.)

(d) We have

$$(\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = 1) = n - 1.$$

Indeed, the only permutations $\sigma \in S_n$ with $\ell(\sigma) = 1$ are the simple transpositions s_i with $i \in [n-1]$.

(e) We have

$$(\# \text{ of } \sigma \in S_n \text{ with } \ell(\sigma) = 2) = \frac{(n-2)(n+1)}{2}.$$

Indeed, the only permutations $\sigma \in S_n$ with $\ell(\sigma) = 2$ are the products $s_i s_j$ with $1 \leq i < j < n$ as well as the products $s_i s_{i-1}$ with $i \in \{2, 3, \ldots, n-1\}$. There are $\frac{(n-2)(n+1)}{2}$ such products (and they are all distinct).

(f) For any $k \in \mathbb{Z}$, we have

$$(\# \text{ of } \sigma \in S_n \text{ with } \ell(\sigma) = k) = \left(\# \text{ of } \sigma \in S_n \text{ with } \ell(\sigma) = \binom{n}{2} - k\right).$$

Proof. Exercise A.4.3.1. □

What about the general case? Alas, there is no explicit formula for the # of $\sigma \in S_n$ with $\ell(\sigma) = k$. However, there is a nice formula for the generating function

$$\sum_{k \in \mathbb{N}} (\# \text{ of } \sigma \in S_n \text{ with } \ell(\sigma) = k)\, x^k = \sum_{\sigma \in S_n} x^{\ell(\sigma)}.$$

Let us first sound it out on the case $n = 3$:

Example 5.3.4. Written in one-line notation, the permutations of the set $[3]$ are 123, 132, 213, 231, 312, and 321. Their lengths are

$$\begin{aligned} &\ell(123) = 0, && \ell(132) = 1, && \ell(213) = 1, \\ &\ell(231) = 2, && \ell(312) = 2, && \ell(321) = 3. \end{aligned}$$

Thus,

$$\begin{aligned} \sum_{\sigma \in S_3} x^{\ell(\sigma)} &= x^{\ell(123)} + x^{\ell(132)} + x^{\ell(213)} + x^{\ell(231)} + x^{\ell(312)} + x^{\ell(321)} \\ &\qquad\qquad (\text{where we are writing each } \sigma \in S_3 \text{ in OLN}) \\ &= x^0 + x^1 + x^1 + x^2 + x^2 + x^3 = 1 + 2x + 2x^2 + x^3 \\ &= (1+x)\left(1 + x + x^2\right). \end{aligned}$$

This suggests the following general result:

Proposition 5.3.5. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}
&\sum_{\sigma \in S_n} x^{\ell(\sigma)} \\
&= \prod_{i=1}^{n-1} \left(1 + x + x^2 + \cdots + x^i\right) \\
&= (1+x)\left(1+x+x^2\right)\left(1+x+x^2+x^3\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right) \\
&= [n]_x!.
\end{aligned}$$

(Here, we are using Definition 4.4.15, so that $[n]_x!$ means the result of substituting x for q in the q-factorial $[n]_q!$.)

5.3.2. Lehmer codes

We will prove this proposition using the so-called *Lehmer code* of a permutation, which is defined as follows:

Definition 5.3.6. Let $n \in \mathbb{N}$. The following notations will be used throughout Section 5.3:

(a) For each $\sigma \in S_n$ and $i \in [n]$, we set

$$\begin{aligned}
\ell_i(\sigma) &:= (\text{\# of all } j \in [n] \text{ satisfying } i < j \text{ and } \sigma(i) > \sigma(j)) \\
&= (\text{\# of all } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j)).
\end{aligned}$$

(The last equality sign here is clear, since the $j \in [n]$ satisfying $i < j$ are precisely the $j \in \{i+1, i+2, \ldots, n\}$.)

(b) For each $m \in \mathbb{Z}$, we let $[m]_0$ denote the set $\{0, 1, \ldots, m\}$. (This is an empty set when $m < 0$.)

(c) We let H_n denote the set

$$\begin{aligned}
&[n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0 \\
&= \{(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n \mid j_i \leq n - i \text{ for each } i \in [n]\}.
\end{aligned}$$

This set H_n has size

$$\begin{aligned}
|H_n| &= |[n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0| \\
&= \underbrace{|[n-1]_0|}_{=n} \cdot \underbrace{|[n-2]_0|}_{=n-1} \cdot \cdots \cdot \underbrace{|[n-n]_0|}_{=1} \\
&= n(n-1)\cdots 1 = n!.
\end{aligned}$$

(d) We define the map

$$\begin{aligned}
L : S_n &\to H_n, \\
\sigma &\mapsto (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)).
\end{aligned}$$

(This map is well-defined, since each $\sigma \in S_n$ and each $i \in [n]$ satisfy $\ell_i(\sigma) \in \{0, 1, \ldots, n-i\} = [n-i]_0$.)

(e) If $\sigma \in S_n$ is a permutation, then the n-tuple $L(\sigma) = (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))$ is called the *Lehmer code* (or just the *code*) of σ.

Example 5.3.7. **(a)** If $n = 6$, and if $\sigma \in S_6$ is the permutation with one-line notation 451263, then $\ell_2(\sigma) = 3$ (because the numbers $j \in [n]$ satisfying $2 < j$ and $\sigma(2) > \sigma(j)$ are precisely 3, 4 and 6, so that there are 3 of them) and likewise $\ell_1(\sigma) = 3$ and $\ell_3(\sigma) = 0$ and $\ell_4(\sigma) = 0$ and $\ell_5(\sigma) = 1$ and $\ell_6(\sigma) = 0$, and thus $L(\sigma) = (3, 3, 0, 0, 1, 0) \in H_6$.

(b) Here is a table of all 6 permutations $\sigma \in S_3$ (written in one-line notation) and their respective Lehmer codes $L(\sigma)$:

σ	$L(\sigma)$
123	$(0,0,0)$
132	$(0,1,0)$
213	$(1,0,0)$
231	$(1,1,0)$
312	$(2,0,0)$
321	$(2,1,0)$

.

The Lehmer code $L(\sigma)$ of a permutation σ is a refinement of its length $\ell(\sigma)$, in the sense that it gives finer information (i.e., we can reconstruct $\ell(\sigma)$ from $L(\sigma)$):

Proposition 5.3.8. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then, $\ell(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma)$.

Proof. This follows from the definitions of $\ell(\sigma)$ and $\ell_i(\sigma)$. □

The main property of Lehmer codes is that they uniquely determine permutations, and in fact are in bijection with them (cf. Example 5.3.7 **(b)**):

Theorem 5.3.9. Let $n \in \mathbb{N}$. Then, the map $L : S_n \to H_n$ is a bijection.

We shall sketch two ways of proving this theorem.

First proof of Theorem 5.3.9 (sketched). Let $\sigma \in S_n$. Let $i \in [n]$. Recall that the OLN of σ is the n-tuple $\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n)$. The definition of $\ell_i(\sigma)$ can be rewritten as follows:

$$\begin{aligned}\ell_i(\sigma) &= (\text{\# of all } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j)) \\ &= (\text{\# of all entries in the OLN of } \sigma \text{ that appear} \\ &\qquad\qquad \text{after } \sigma(i) \text{ but are smaller than } \sigma(i)) \\ &= (\text{\# of elements of } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i)\} \\ &\qquad\qquad \text{that are smaller than } \sigma(i))\end{aligned}$$

(since the elements of $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i)\}$ are precisely the entries that appear after $\sigma(i)$ in the OLN of σ). We can replace the set $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i)\}$ by $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$ in this equality[62] (this will not change the # of elements of this set that are smaller than $\sigma(i)$, because it only inserts the element $\sigma(i)$ into the set, and obviously this element $\sigma(i)$ is not smaller than $\sigma(i)$). Thus, we obtain

$$\begin{aligned}\ell_i(\sigma) = (\text{\# of elements of } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\} \\ \text{that are smaller than } \sigma(i)).\end{aligned} \tag{155}$$

Therefore,

$$\begin{aligned}\sigma(i) = (\text{the } (\ell_i(\sigma)+1)\text{-st smallest element of} \\ \text{the set } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\})\end{aligned} \tag{156}$$

(since $\sigma(i)$ is an element of $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$).

Forget that we fixed i. We thus have proved the equality (156) for each $i \in [n]$. This equality (156) allows us to find $\sigma(i)$ if $\ell_i(\sigma)$ and $\sigma(1), \sigma(2), \ldots, \sigma(i-1)$ are known. This can be used to recover σ from $L(\sigma)$. Let us perform this recovery in an example: Let $n = 5$, and let $\sigma \in S_5$ satisfy $L(\sigma) = (3, 1, 2, 1, 0)$. What is σ ?

From $L(\sigma) = (3, 1, 2, 1, 0)$, we obtain $\ell_1(\sigma) = 3$ and $\ell_2(\sigma) = 1$ and $\ell_3(\sigma) = 2$ and $\ell_4(\sigma) = 1$ and $\ell_5(\sigma) = 0$.

Applying (156) to $i = 1$, we find

$$\begin{aligned}\sigma(1) &= \left(\text{the } (\ell_1(\sigma)+1)\text{-st smallest element of} \right. \\ &\qquad\qquad \left. \text{the set } [n] \setminus \underbrace{\{\sigma(1), \sigma(2), \ldots, \sigma(1-1)\}}_{=\varnothing}\right) \\ &= (\text{the } (3+1)\text{-st smallest element of the set } [5]) \\ &\qquad\qquad (\text{since } \ell_1(\sigma) = 3 \text{ and } n = 5) \\ &= (\text{the 4-th smallest element of the set } [5]) = 4.\end{aligned}$$

[62] If $i = 1$, then the set $\{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$ is empty, so that we have $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\} = [n]$ in this case.

Applying (156) to $i = 2$, we find

$$\begin{aligned}\sigma(2) &= \left(\text{the } (\ell_2(\sigma)+1)\text{-st smallest element of}\right.\\ &\qquad\left.\text{the set } [n] \setminus \underbrace{\{\sigma(1), \sigma(2), \ldots, \sigma(2-1)\}}_{=\{\sigma(1)\}}\right)\\ &= \left(\text{the } (1+1)\text{-st smallest element of the set } [5] \setminus \{4\}\right)\\ &\qquad (\text{since } \ell_2(\sigma) = 1 \text{ and } n = 5 \text{ and } \sigma(1) = 4)\\ &= \left(\text{the 2-nd smallest element of the set } [5] \setminus \{4\}\right) = 2.\end{aligned}$$

Applying (156) to $i = 3$, we find

$$\begin{aligned}\sigma(3) &= \left(\text{the } (\ell_3(\sigma)+1)\text{-st smallest element of}\right.\\ &\qquad\left.\text{the set } [n] \setminus \underbrace{\{\sigma(1), \sigma(2), \ldots, \sigma(3-1)\}}_{=\{\sigma(1), \sigma(2)\}}\right)\\ &= \left(\text{the } (2+1)\text{-st smallest element of the set } [5] \setminus \{4, 2\}\right)\\ &\qquad (\text{since } \ell_3(\sigma) = 2 \text{ and } n = 5 \text{ and } \sigma(1) = 4 \text{ and } \sigma(2) = 2)\\ &= \left(\text{the 3-rd smallest element of the set } [5] \setminus \{4, 2\}\right) = 5\end{aligned}$$

(since $[5] \setminus \{4, 2\} = \{1, 3, 5\}$).

Continuing like this, we find $\sigma(4) = 3$ and $\sigma(5) = 1$. Thus, the OLN of σ is $\sigma(1)\ \sigma(2)\ \sigma(3)\ \sigma(4)\ \sigma(5) = 42531$.

This method allows us to reconstruct any $\sigma \in S_n$ from $L(\sigma)$ (and thus shows that the map L is injective). We shall now see what happens if we apply it to an **arbitrary** n-tuple $\mathbf{j} = (j_1, j_2, \ldots, j_n) \in H_n$ instead of $L(\sigma)$ (that is, we replace $\ell_i(\sigma)$ by j_i).

Thus, we define a map

$$M : H_n \to S_n$$

as follows: If $\mathbf{j} = (j_1, j_2, \ldots, j_n) \in H_n$, then $M(\mathbf{j})$ is the map $\sigma : [n] \to [n]$ whose values $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are defined recursively by the rule

$$\begin{aligned}\sigma(i) = &\left(\text{the } (j_i+1)\text{-st smallest element of}\right.\\ &\qquad\left.\text{the set } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}\right). \qquad (157)\end{aligned}$$

This map σ

- is always well-defined (indeed, we never run out of values in the process of constructing σ, because of the following argument: each $i \in$

$[n]$ satisfies $j_i \leq n-i$ [63], and thus the $(n-i+1)$-element set $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$ has a (j_i+1)-st smallest element[64]), and

- always is a permutation of $[n]$ (indeed, our definition of $\sigma(i)$ ensures that $\sigma(i) \in [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$, so that $\sigma(i) \notin \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$, and therefore the map σ has no two equal values; thus, σ is injective; therefore, by the Pigeonhole Principle for Injections[65], the map σ must also be bijective, i.e., a permutation of $[n]$).

Thus, the map M is well-defined.

We claim that the maps L and M are mutually inverse. Indeed, we already know that M undoes L (since applying M to $L(\sigma)$ produces precisely our above-discussed algorithm for reconstructing σ from $L(\sigma)$); in other words, we have $M \circ L = \text{id}$. It is also easy to see that $L \circ M = \text{id}$. Thus, the maps L and M are inverse, so that L is bijective. This proves Theorem 5.3.9. □

Our second proof of Theorem 5.3.9 will be less algorithmic, but it provides a good illustration for the use of total orders. We will only outline it; the details can be found in [Grinbe15, solution to Exercise 5.18].

This second proof relies on a total order that can be defined on the set $\mathbb{Z}^n$ of n-tuples of integers:

Definition 5.3.10. Let $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ be two n-tuples of integers. We say that

$$(a_1, a_2, \ldots, a_n) <_{\text{lex}} (b_1, b_2, \ldots, b_n) \qquad (158)$$

if and only if

- there exists some $k \in [n]$ such that $a_k \neq b_k$, and
- the **smallest** such k satisfies $a_k < b_k$.

For example, $(4,1,2,5) <_{\text{lex}} (4,1,3,0)$ and $(1,1,0,1) <_{\text{lex}} (2,0,0,0)$. The relation (158) is usually pronounced as "$(a_1, a_2, \ldots, a_n)$ is *lexicographically smaller*

[63] because $(j_1, j_2, \ldots, j_n) \in H_n = [n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0$ entails $j_i \in [n-i]_0$

[64] To be fully precise: We don't know yet that $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$ is an $(n-i+1)$-element set, since we haven't yet shown that the $i-1$ elements $\sigma(1), \sigma(2), \ldots, \sigma(i-1)$ are distinct. However, if they are not distinct, then the set $[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}$ has more than $n-i+1$ elements, which is just as good for our argument.

[65] The *Pigeonhole Principle for Injections* says the following two things:

- If $f : X \to Y$ is an injective map between two finite sets X and Y, then $|X| \leq |Y|$.
- If $f : X \to Y$ is an injective map between two finite sets X and Y of the same size, then f is bijective.

We are here using the second statement.

than $(b_1, b_2, \ldots, b_n)$"; the word "lexicographic" comes from the idea that if numbers were letters, then a "word" $a_1 a_2 \cdots a_n$ would appear earlier in a dictionary than $b_1 b_2 \cdots b_n$ if and only if $(a_1, a_2, \ldots, a_n) <_{\text{lex}} (b_1, b_2, \ldots, b_n)$.

Now, the following is easy to see:

Proposition 5.3.11. If $\mathbf{a}$ and $\mathbf{b}$ are two distinct n-tuples of integers, then we have either $\mathbf{a} <_{\text{lex}} \mathbf{b}$ or $\mathbf{b} <_{\text{lex}} \mathbf{a}$.

Actually, it is not hard to show that the relation $<_{\text{lex}}$ is a total order on the set $\mathbb{Z}^n$ (known as the *lexicographic order*); however, Proposition 5.3.11 is the only part of this statement that we will need.

Proposition 5.3.12. Let $\sigma \in S_n$ and $\tau \in S_n$ be such that

$$(\sigma(1), \sigma(2), \ldots, \sigma(n)) <_{\text{lex}} (\tau(1), \tau(2), \ldots, \tau(n)). \tag{159}$$

Then,

$$(\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)) <_{\text{lex}} (\ell_1(\tau), \ell_2(\tau), \ldots, \ell_n(\tau)). \tag{160}$$

(In other words, $L(\sigma) <_{\text{lex}} L(\tau)$.)

Proof of Proposition 5.3.12 (sketched). (See [Grinbe15, solution to Exercise 5.18, proof of Proposition 5.50] for details.) The assumption (159) shows that there exists some $k \in [n]$ such that $\sigma(k) \neq \tau(k)$, and that the **smallest** such k satisfies $\sigma(k) < \tau(k)$. Consider this smallest k. Thus, $\sigma(i) = \tau(i)$ for each $i \in [k-1]$ (since k is smallest with $\sigma(k) \neq \tau(k)$). Hence, using (155), we can easily see that

$$\ell_i(\sigma) = \ell_i(\tau) \qquad \text{for each } i \in [k-1]. \tag{161}$$

Let Z be the set

$$[n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(k-1)\} = [n] \setminus \{\tau(1), \tau(2), \ldots, \tau(k-1)\}.$$

Then, (155) (applied to $i = k$) yields that

$$\ell_k(\sigma) = (\text{\# of elements of } Z \text{ that are smaller than } \sigma(k)),$$

and similarly we have

$$\ell_k(\tau) = (\text{\# of elements of } Z \text{ that are smaller than } \tau(k)).$$

From these two equalities, we can easily see that $\ell_k(\sigma) < \ell_k(\tau)$. (In fact, any element of Z that is smaller than $\sigma(k)$ must also be smaller than $\tau(k)$ (since $\sigma(k) < \tau(k)$), but there is at least one element of Z that is smaller than $\tau(k)$ but not smaller than $\sigma(k)$ (namely, the element $\sigma(k)$). Hence, there are fewer elements of Z that are smaller than $\sigma(k)$ than there are elements of Z that are smaller than $\tau(k)$.)

Combining (161) with $\ell_k(\sigma) < \ell_k(\tau)$, we obtain $(\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)) <_{\text{lex}} (\ell_1(\tau), \ell_2(\tau), \ldots, \ell_n(\tau))$ (by Definition 5.3.10). This proves Proposition 5.3.12. □

Now, we can easily finish our second proof of Theorem 5.3.9:

Second proof of Theorem 5.3.9 (sketched). We shall first show that the map L is injective.

Indeed, let σ and τ be two distinct permutations in S_n. Then, the two n-tuples $(\sigma(1), \sigma(2), \ldots, \sigma(n))$ and $(\tau(1), \tau(2), \ldots, \tau(n))$ (that is, the OLNs of σ and τ) are distinct as well. Hence, Proposition 5.3.11 yields that we have either $(\sigma(1), \sigma(2), \ldots, \sigma(n)) <_{\text{lex}} (\tau(1), \tau(2), \ldots, \tau(n))$ or $(\tau(1), \tau(2), \ldots, \tau(n)) <_{\text{lex}} (\sigma(1), \sigma(2), \ldots, \sigma(n))$. In the first case, we obtain $L(\sigma) <_{\text{lex}} L(\tau)$ (by Proposition 5.3.12); in the second case, we likewise obtain $L(\tau) <_{\text{lex}} L(\sigma)$. In either case, we thus conclude that $L(\sigma) \neq L(\tau)$.

Forget that we fixed σ and τ. We thus have shown that if σ and τ are two distinct permutations in S_n, then $L(\sigma) \neq L(\tau)$. In other words, the map $L : S_n \to H_n$ is injective. However, L is a map between two finite sets of the same size (indeed, $|S_n| = n! = |H_n|$). Thus, the Pigeonhole Principle for Injections shows that L is bijective (since L is injective). This proves Theorem 5.3.9 again. □

Now, we can prove Proposition 5.3.5 at last:

Proof of Proposition 5.3.5. Each $\sigma \in S_n$ satisfies

$$\begin{aligned}\ell(\sigma) &= \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma) \qquad \text{(by Proposition 5.3.8)} \\ &= (\text{sum of the entries of } L(\sigma))\end{aligned}$$

(since $L(\sigma) = (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma))$). Thus,

$$\begin{aligned}
\sum_{\sigma \in S_n} x^{\ell(\sigma)} &= \sum_{\sigma \in S_n} x^{(\text{sum of the entries of } L(\sigma))} = \sum_{(j_1, j_2, \ldots, j_n) \in H_n} \underbrace{x^{(\text{sum of the entries of } (j_1, j_2, \ldots, j_n))}}_{= x^{j_1 + j_2 + \cdots + j_n} = x^{j_1} x^{j_2} \cdots x^{j_n}} \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } (j_1, j_2, \ldots, j_n) \text{ for } L(\sigma) \text{ in} \\ \text{the sum, since the map } L : S_n \to H_n \text{ is a bijection} \end{array} \right) \\
&= \sum_{(j_1, j_2, \ldots, j_n) \in H_n} x^{j_1} x^{j_2} \cdots x^{j_n} = \sum_{(j_1, j_2, \ldots, j_n) \in [n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0} x^{j_1} x^{j_2} \cdots x^{j_n} \\
&\qquad (\text{since } H_n = (j_1, j_2, \ldots, j_n) \in [n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0) \\
&= \left(\sum_{j_1 \in [n-1]_0} x^{j_1} \right) \left(\sum_{j_2 \in [n-2]_0} x^{j_2} \right) \cdots \left(\sum_{j_n \in [n-n]_0} x^{j_n} \right) \\
&\qquad (\text{by the product rule (116)}) \\
&= \left(\sum_{j_1 = 0}^{n-1} x^{j_1} \right) \left(\sum_{j_2 = 0}^{n-2} x^{j_2} \right) \cdots \left(\sum_{j_n = 0}^{n-n} x^{j_n} \right) \\
&\qquad (\text{since } [m]_0 = \{0, 1, \ldots, m\} \text{ for any } m \in \mathbb{Z}) \\
&= \left(1 + x + x^2 + \cdots + x^{n-1}\right) \left(1 + x + x^2 + \cdots + x^{n-2}\right) \cdots (1 + x)(1) \\
&= \left(1 + x + x^2 + \cdots + x^{n-1}\right) \left(1 + x + x^2 + \cdots + x^{n-2}\right) \cdots (1 + x) \\
&= (1 + x) \left(1 + x + x^2\right) \left(1 + x + x^2 + x^3\right) \cdots \left(1 + x + x^2 + \cdots + x^{n-1}\right) \\
&= \prod_{i=1}^{n-1} \left(1 + x + x^2 + \cdots + x^i\right) = [n]_x!
\end{aligned}$$

(the last equality sign here is easy to check). This proves Proposition 5.3.5. □

5.3.3. More about lengths and simples

Let us continue studying lengths of permutations.

Proposition 5.3.13. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then, $\ell\left(\sigma^{-1}\right) = \ell(\sigma)$.

Proof of Proposition 5.3.13 (sketched). (See [Grinbe15, Exercise 5.2 **(f)**] for details.)

Recall that $\ell(\sigma)$ is the # of inversions of σ, while $\ell\left(\sigma^{-1}\right)$ is the # of inversions of σ^{-1}.

Recall also that an inversion of σ is a pair $(i, j) \in [n] \times [n]$ such that $i < j$ and $\sigma(i) > \sigma(j)$. Likewise, an inversion of σ^{-1} is a pair $(u, v) \in [n] \times [n]$ such that $u < v$ and $\sigma^{-1}(u) > \sigma^{-1}(v)$.

Thus, if (i, j) is an inversion of σ, then $(\sigma(j), \sigma(i))$ is an inversion of σ^{-1}.

Hence, we obtain a map

$$\begin{aligned} \{\text{inversions of } \sigma\} &\to \left\{\text{inversions of } \sigma^{-1}\right\}, \\ (i,j) &\mapsto (\sigma(j), \sigma(i)). \end{aligned}$$

This map is furthermore bijective (indeed, it has an inverse map, which sends each $(u,v) \in \left\{\text{inversions of } \sigma^{-1}\right\}$ to $\left(\sigma^{-1}(v), \sigma^{-1}(u)\right)$). Thus, the bijection principle yields

$$(\#\text{ of inversions of } \sigma) = \left(\#\text{ of inversions of } \sigma^{-1}\right).$$

In other words, $\ell(\sigma) = \ell\left(\sigma^{-1}\right)$. This proves Proposition 5.3.13. □

The following lemma is crucial for understanding lengths of permutations:

> **Lemma 5.3.14** (single swap lemma)**.** Let $n \in \mathbb{N}$, $\sigma \in S_n$ and $k \in [n-1]$. Then:
>
> **(a)** We have
>
> $$\ell(\sigma s_k) = \begin{cases} \ell(\sigma)+1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma(k) > \sigma(k+1). \end{cases}$$
>
> **(b)** We have
>
> $$\ell(s_k\sigma) = \begin{cases} \ell(\sigma)+1, & \text{if } \sigma^{-1}(k) < \sigma^{-1}(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma^{-1}(k) > \sigma^{-1}(k+1). \end{cases}$$
>
> [**Note:** If $i \in [n]$, then $\sigma(i)$ is the **entry** in position i of the one-line notation of σ, whereas $\sigma^{-1}(i)$ is the **position** in which the number i appears in the one-line notation of σ. For example, if $\sigma = 512364$ in one-line notation, then $\sigma(6) = 4$ and $\sigma^{-1}(6) = 5$.]

We will only outline the proof of Lemma 5.3.14; a detailed proof can be found in [Grinbe15, Exercise 5.2 **(a)**] (although not completely the same proof).

Proof of Lemma 5.3.14 (sketched). **(b)** The OLN[66] of $s_k\sigma$ is obtained from the OLN of σ by swapping the two entries k and $k+1$. This is best seen on an example: For example, if $\sigma = 512364$ (in OLN), then $s_3\sigma = 512463$. In general, this follows by observing that

$$(s_k\sigma)(i) = s_k(\sigma(i)) = \begin{cases} k+1, & \text{if } \sigma(i) = k; \\ k, & \text{if } \sigma(i) = k+1; \\ \sigma(i), & \text{otherwise} \end{cases} \qquad \text{for each } i \in [n].$$

[66] Recall that "OLN" means "one-line notation".

Let us now use this observation to see how the inversions of $s_k\sigma$ differ from the inversions of σ. Indeed, let us call an inversion (i,j) of a permutation τ *exceptional* if we have $\tau(i) = k+1$ and $\tau(j) = k$. All other inversions of τ will be called *non-exceptional*.

Now, we make the following observation:

> *Observation 1:* If (i,j) is any non-exceptional inversion of σ, then (i,j) is still a non-exceptional inversion of $s_k\sigma$.

[*Proof of Observation 1:* Let (i,j) be a non-exceptional inversion of σ. Thus, we have the inequality $\sigma(i) > \sigma(j)$ (since (i,j) is an inversion of σ). This inequality cannot get reversed by applying s_k to both its sides (i.e., we cannot have $s_k(\sigma(i)) < s_k(\sigma(j))$), since the only pair $(u,v) \in [n] \times [n]$ satisfying $u > v$ and $s_k(u) < s_k(v)$ is the pair $(k+1,k)$ (but our pair $(\sigma(i), \sigma(j))$ cannot equal this pair $(k+1,k)$, since the inversion (i,j) of σ is non-exceptional). Hence, we have $s_k(\sigma(i)) \geq s_k(\sigma(j))$. In other words, $(s_k\sigma)(i) \geq (s_k\sigma)(j)$. Since the map $s_k\sigma$ is injective (being a permutation of $[n]$), we thus obtain $(s_k\sigma)(i) > (s_k\sigma)(j)$ (since $i \neq j$). Thus, the pair (i,j) is an inversion of $s_k\sigma$. Moreover, this inversion (i,j) is non-exceptional (since otherwise we would have $(s_k\sigma)(i) = k+1$ and $(s_k\sigma)(j) = k$, which would lead to $\sigma(i) = k$ and $\sigma(j) = k+1$, which would contradict $\sigma(i) > \sigma(j)$). Thus, we have shown that (i,j) is still a non-exceptional inversion of $s_k\sigma$. This proves Observation 1.]

Similarly to Observation 1, we can prove the following:

> *Observation 2:* If (i,j) is any non-exceptional inversion of $s_k\sigma$, then (i,j) is still a non-exceptional inversion of σ.

(Alternatively, we can obtain Observation 2 by applying Observation 1 to $s_k\sigma$ instead of σ, since we have $\underbrace{s_k s_k}_{=s_k^2=\operatorname{id}} \sigma = \sigma$.)

Combining Observation 1 with Observation 2, we see that the non-exceptional inversions of $s_k\sigma$ are precisely the non-exceptional inversions of σ. Hence,

$$\begin{aligned} &(\text{\# of non-exceptional inversions of } s_k\sigma) \\ &= (\text{\# of non-exceptional inversions of } \sigma). \end{aligned} \tag{162}$$

What about the exceptional inversions? A permutation $\tau \in S_n$ has a unique exceptional inversion if k appears after $k+1$ in the OLN of τ (that is, if we have $\tau^{-1}(k) > \tau^{-1}(k+1)$); otherwise, it has none. Thus:

- If $\sigma^{-1}(k) < \sigma^{-1}(k+1)$, then the permutation $s_k\sigma$ has a unique exceptional inversion, whereas the permutation σ has none.
- If $\sigma^{-1}(k) > \sigma^{-1}(k+1)$, then the permutation σ has a unique exceptional inversion, whereas the permutation $s_k\sigma$ has none.

Thus,

$$\begin{aligned}&(\text{\# of exceptional inversions of } s_k\sigma)\\&=(\text{\# of exceptional inversions of } \sigma)\\&\qquad+\begin{cases}1, & \text{if } \sigma^{-1}(k)<\sigma^{-1}(k+1);\\ -1, & \text{if } \sigma^{-1}(k)>\sigma^{-1}(k+1).\end{cases}\end{aligned} \tag{163}$$

Now, recall that each inversion of a permutation $\tau \in S_n$ is either exceptional or non-exceptional (and cannot be both at the same time). Thus, adding together the two equalities (163) and (162), we obtain

$$\begin{aligned}&(\text{\# of inversions of } s_k\sigma)\\&=(\text{\# of inversions of } \sigma)+\begin{cases}1, & \text{if } \sigma^{-1}(k)<\sigma^{-1}(k+1);\\ -1, & \text{if } \sigma^{-1}(k)>\sigma^{-1}(k+1)\end{cases}\\&=\begin{cases}(\text{\# of inversions of } \sigma)+1, & \text{if } \sigma^{-1}(k)<\sigma^{-1}(k+1);\\ (\text{\# of inversions of } \sigma)-1, & \text{if } \sigma^{-1}(k)>\sigma^{-1}(k+1).\end{cases}\end{aligned}$$

In other words,

$$\ell(s_k\sigma)=\begin{cases}\ell(\sigma)+1, & \text{if } \sigma^{-1}(k)<\sigma^{-1}(k+1);\\ \ell(\sigma)-1, & \text{if } \sigma^{-1}(k)>\sigma^{-1}(k+1)\end{cases}$$

(since $\ell(\tau)$ denotes the # of inversions of any permutation τ). This proves Lemma 5.3.14 **(b)**.

(a) Applying Lemma 5.3.14 **(b)** to σ^{-1} instead of σ, we obtain

$$\begin{aligned}\ell\left(s_k\sigma^{-1}\right)&=\begin{cases}\ell\left(\sigma^{-1}\right)+1, & \text{if } \left(\sigma^{-1}\right)^{-1}(k)<\left(\sigma^{-1}\right)^{-1}(k+1);\\ \ell\left(\sigma^{-1}\right)-1, & \text{if } \left(\sigma^{-1}\right)^{-1}(k)>\left(\sigma^{-1}\right)^{-1}(k+1)\end{cases}\\&=\begin{cases}\ell(\sigma)+1, & \text{if } \sigma(k)<\sigma(k+1);\\ \ell(\sigma)-1, & \text{if } \sigma(k)>\sigma(k+1)\end{cases}\end{aligned} \tag{164}$$

(since $\left(\sigma^{-1}\right)^{-1}=\sigma$, and since Proposition 5.3.13 yields $\ell\left(\sigma^{-1}\right)=\ell(\sigma)$). However, Proposition 5.3.13 (applied to σs_k instead of σ) yields $\ell\left((\sigma s_k)^{-1}\right)=\ell(\sigma s_k)$. In view of $(\sigma s_k)^{-1}=\underbrace{s_k^{-1}}_{=s_k}\sigma^{-1}=s_k\sigma^{-1}$, this rewrites as $\ell\left(s_k\sigma^{-1}\right)=\ell(\sigma s_k)$. Comparing this with (164), we obtain

$$\ell(\sigma s_k)=\begin{cases}\ell(\sigma)+1, & \text{if } \sigma(k)<\sigma(k+1);\\ \ell(\sigma)-1, & \text{if } \sigma(k)>\sigma(k+1).\end{cases}$$

This proves Lemma 5.3.14 **(a)**. □

Lemma 5.3.14 answers what happens to the length of a permutation when we compose it (from the left or the right) with a simple transposition s_k. What happens when we compose it with a non-simple transposition? The situation is more complicated, but it is still true that the length decreases or increases depending on whether the two entries that are being swapped formed an inversion or not. Here is the exact answer (stated only for $\sigma t_{i,j}$, but a version for $t_{i,j}\sigma$ can easily be derived from it):

Proposition 5.3.15. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Let i and j be two elements of $[n]$ such that $i < j$. Then:

(a) We have $\ell\left(\sigma t_{i,j}\right) < \ell\left(\sigma\right)$ if $\sigma\left(i\right) > \sigma\left(j\right)$. We have $\ell\left(\sigma t_{i,j}\right) > \ell\left(\sigma\right)$ if $\sigma\left(i\right) < \sigma\left(j\right)$.

(b) We have

$$\ell\left(\sigma t_{i,j}\right) = \begin{cases} \ell\left(\sigma\right) - 2\left|Q\right| - 1, & \text{if } \sigma\left(i\right) > \sigma\left(j\right); \\ \ell\left(\sigma\right) + 2\left|R\right| + 1, & \text{if } \sigma\left(i\right) < \sigma\left(j\right), \end{cases}$$

where

$$Q = \left\{k \in \left\{i+1, i+2, \ldots, j-1\right\} \mid \sigma\left(i\right) > \sigma\left(k\right) > \sigma\left(j\right)\right\} \qquad \text{and}$$
$$R = \left\{k \in \left\{i+1, i+2, \ldots, j-1\right\} \mid \sigma\left(i\right) < \sigma\left(k\right) < \sigma\left(j\right)\right\}.$$

Proof of Proposition 5.3.15 (sketched). **(b)** This follows by a diligent analysis of the possible interactions between an inversion and composition by $t_{i,j}$. To be more concrete:

- The fact that $\ell\left(\sigma t_{i,j}\right) = \ell\left(\sigma\right) - 2\left|Q\right| - 1$ when $\sigma\left(i\right) > \sigma\left(j\right)$ is [Grinbe15, Exercise 5.20]. A straightforward solution was given by Elafandi in [18f-hw4se]. (The solution given in [Grinbe15, Exercise 5.20] is more circuitous, as it uses summation tricks to bypass case distinctions.)

- The fact that $\ell\left(\sigma t_{i,j}\right) = \ell\left(\sigma\right) + 2\left|R\right| + 1$ when $\sigma\left(i\right) < \sigma\left(j\right)$ follows by applying the previous fact to $\sigma t_{i,j}$ instead of σ. (Indeed, if $\sigma\left(i\right) < \sigma\left(j\right)$, then $\left(\sigma t_{i,j}\right)\left(i\right) = \sigma\left(j\right) > \sigma\left(i\right) = \left(\sigma t_{i,j}\right)\left(j\right)$ and $\sigma \underbrace{t_{i,j} t_{i,j}}_{=t_{i,j}^2 = \operatorname{id}} = \sigma$. Moreover, when we replace σ by $\sigma t_{i,j}$, the sets Q and R trade places.)

(a) This follows immediately from part **(b)**. □

Now we come to one of the main facts about permutations of a finite set.

Convention 5.3.16. We recall that a *simple transposition* in S_n means one of the $n-1$ transpositions $s_1, s_2, \ldots, s_{n-1}$. We shall occasionally abbreviate "simple transposition" as "*simple*".

Theorem 5.3.17 (1st reduced word theorem for the symmetric group)**.** Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then:

(a) We can write σ as a composition (i.e., product) of $\ell(\sigma)$ simples.

(b) The number $\ell(\sigma)$ is the smallest $p \in \mathbb{N}$ such that we can write σ as a composition of p simples.

[**Keep in mind:** The composition of 0 simples is id, since id is the neutral element of the group S_n.]

Example 5.3.18. Let $\sigma \in S_4$ be the permutation 4132 (in OLN). How can we write σ as a composition of simples? There are several ways to do this; for example,

$$\sigma = \underbrace{s_2 s_3 s_2}_{= s_3 s_2 s_3} s_1 = s_3 s_2 \underbrace{s_3 s_1}_{= s_1 s_3} = s_3 s_2 s_1 s_3 = s_2 s_1 s_1 s_3 s_2 s_1 = s_2 s_1 s_3 s_1 s_2 s_1 = \cdots .$$

The shortest of these representations involve 4 simples, precisely as predicted by Theorem 5.3.17 (since $\ell(\sigma) = 4$).

Before we prove Theorem 5.3.17, let me mention a geometric visualization of the symmetric group that will not be used in what follows, but sheds some light on the theorem and on the role of simple transpositions:

Remark 5.3.19. Let $n \in \mathbb{N}$. Then, the permutations of $[n]$ can be represented as the vertices of an $(n-1)$-dimensional polytope in n-dimensional space.

Namely, each permutation σ of $[n]$ gives rise to the point

$$V_\sigma := (\sigma(1), \sigma(2), \ldots, \sigma(n)) \in \mathbb{R}^n.$$

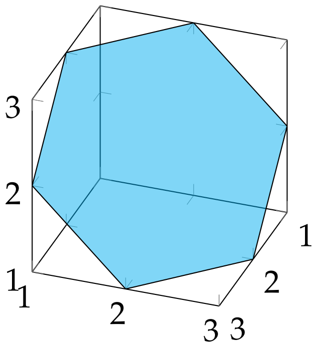
The convex hull of all these $n!$ many points V_σ (for $\sigma \in S_n$) is a polytope (i.e., a bounded convex polyhedron in $\mathbb{R}^n$). This polytope is known as the permutahedron (corresponding to n). It is actually $(n-1)$-dimensional, since all its vertices lie on the hyperplane with equation $x_1 + x_2 + \cdots + x_n = 1 + 2 + \cdots + n$. It can be shown (see, e.g., [GaiGup77]) that:

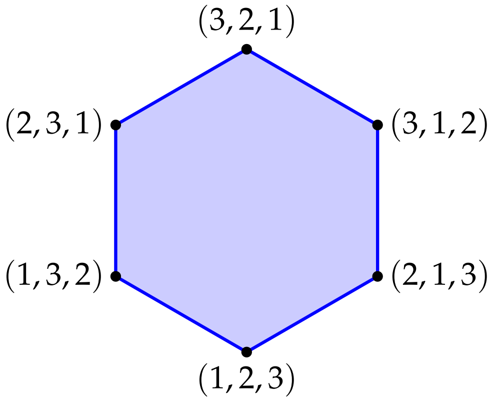
- The vertices of this polytope are precisely the $n!$ points V_σ with $\sigma \in S_n$.
- Two vertices V_σ and V_τ are joined by an edge if and only if $\sigma = s_k \tau$ for some $k \in [n-1]$.

The (intuitively obvious) fact that any two vertices of a polytope can be connected by a sequence of edges therefore yields that any $\sigma \in S_n$ can be written as a product of simples. This is a weaker version of Theorem 5.3.17 **(a)**.

We refer to textbooks on discrete geometry and geometric combinatorics for more about polytopes and permutahedra in particular. Let me here just show the permutahedra for $n = 3$ and for $n = 4$ (note that the permutahedron for $n = 2$ is a boring line segment in $\mathbb{R}^2$):

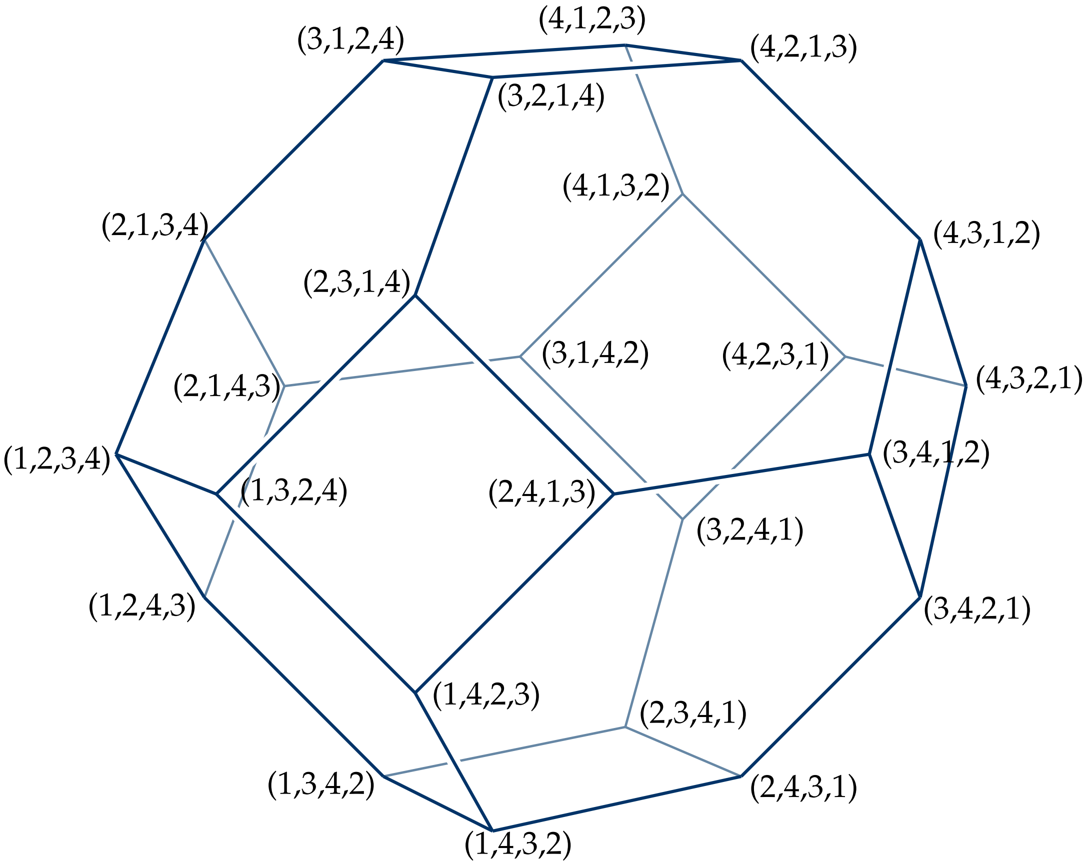
- The permutahedron for $n = 3$ is a regular hexagon:





The picture on the left (courtesy of tex.stackexchange user Jake, released under the MIT license) shows the permutahedron embedded in $\mathbb{R}^3$; the picture on the right is a view from an orthogonal direction.

- The permutahedron for $n = 4$ is a truncated octahedron:



(picture courtesy of David Eppstein on the Wikipedia).

Let us now outline a proof of Theorem 5.3.17.

Proof of Theorem 5.3.17 (sketched). **(a)** (See [Grinbe15, Exercise 5.2 **(e)**] for details.)

We proceed by induction on $\ell\left(\sigma\right)$:

Induction base: If $\ell\left(\sigma\right)=0$, then $\sigma=\operatorname{id}$, so that we can write σ as a composition of 0 simples.

Induction step: Fix $h\in\mathbb{N}$. Assume (as the IH[67]) that Theorem 5.3.17 **(a)** holds for $\ell\left(\sigma\right)=h$.

Now, let $\sigma\in S_n$ be such that $\ell\left(\sigma\right)=h+1$. We must prove that we can write σ as a composition of $\ell\left(\sigma\right)$ simples.

We have $\ell\left(\sigma\right)=h+1>h\geq 0$; hence, σ has at least one inversion. Thus, we cannot have $\sigma\left(1\right)\leq\sigma\left(2\right)\leq\cdots\leq\sigma\left(n\right)$. In other words, there exists some $k\in\left[n-1\right]$ such that $\sigma\left(k\right)>\sigma\left(k+1\right)$. Let us fix such a k.

Lemma 5.3.14 **(a)** yields

$$\begin{aligned}\ell\left(\sigma s_k\right)&=\begin{cases}\ell\left(\sigma\right)+1, & \text{if } \sigma\left(k\right)<\sigma\left(k+1\right);\\ \ell\left(\sigma\right)-1, & \text{if } \sigma\left(k\right)>\sigma\left(k+1\right)\end{cases}\\ &=\ell\left(\sigma\right)-1 \qquad \left(\text{since } \sigma\left(k\right)>\sigma\left(k+1\right)\right)\\ &=h \qquad \left(\text{since } \ell\left(\sigma\right)=h+1\right).\end{aligned}$$

Thus, the IH tells us that we can apply Theorem 5.3.17 **(a)** to σs_k instead of σ. We conclude that we can write σs_k as a composition of $\ell\left(\sigma s_k\right)$ simples. In other words, we can write σs_k as a composition of h simples (since $\ell\left(\sigma s_k\right)=h$). That is, we have

$$\sigma s_k=s_{i_1}s_{i_2}\cdots s_{i_h} \qquad \text{for some } i_1,i_2,\ldots,i_h\in\left[n-1\right].$$

Consider these $i_1,i_2,\ldots,i_h$. Now,

$$\sigma=\underbrace{\sigma s_k}_{=s_{i_1}s_{i_2}\cdots s_{i_h}}\underbrace{s_k^{-1}}_{=s_k}=s_{i_1}s_{i_2}\cdots s_{i_h}s_k.$$

This shows that we can write σ as a composition of $h+1$ simples. In other words, we can write σ as a composition of $\ell\left(\sigma\right)$ simples (since $\ell\left(\sigma\right)=h+1$). Thus, Theorem 5.3.17 **(a)** holds for $\ell\left(\sigma\right)=h+1$. This completes the induction step, and so Theorem 5.3.17 **(a)** is proved by induction.

(b) (See [Grinbe15, Exercise 5.2 **(g)**] for details.)

We already know from Theorem 5.3.17 **(a)** that we can write σ as a composition of $\ell\left(\sigma\right)$ simples. It thus remains to show that we cannot write σ as a composition of fewer than $\ell\left(\sigma\right)$ simples.

This will clearly follow if we can show that

$$\ell\left(s_{i_1}s_{i_2}\cdots s_{i_g}\right)\leq g \tag{165}$$

[67] "IH" means "induction hypothesis".

for any $i_1, i_2, \ldots, i_g \in [n-1]$.

In order to prove (5.3.17), we first make a simple observation: For any $\sigma \in S_n$ and any $k \in [n-1]$, we have

$$\ell(\sigma s_k) \leq \ell(\sigma) + 1. \tag{166}$$

(This follows from Lemma 5.3.14 **(a)**, since both numbers $\ell(\sigma) + 1$ and $\ell(\sigma) - 1$ are $\leq \ell(\sigma) + 1$.) Now, for any $i_1, i_2, \ldots, i_g \in [n-1]$, we have

$$\begin{aligned}
&\ell\left(s_{i_1} s_{i_2} \cdots s_{i_g}\right) \\
&\leq \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-1}}\right) + 1 \qquad \text{(by (166))} \\
&\leq \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-2}}\right) + 2 \\
&\qquad \left(\text{since (166) yields } \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-1}}\right) \leq \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-2}}\right) + 1\right) \\
&\leq \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-3}}\right) + 3 \\
&\qquad \left(\text{since (166) yields } \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-2}}\right) \leq \ell\left(s_{i_1} s_{i_2} \cdots s_{i_{g-3}}\right) + 1\right) \\
&\leq \cdots \\
&\leq \underbrace{\ell(\mathrm{id})}_{=0} + g \qquad \text{(since the product of 0 simples is id)} \\
&= g.
\end{aligned}$$

This proves (165), and thus concludes our proof of Theorem 5.3.17 **(b)**. □

Corollary 5.3.20. Let $n \in \mathbb{N}$.

(a) We have $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \bmod 2$ for all $\sigma \in S_n$ and $\tau \in S_n$.

(b) We have $\ell(\sigma\tau) \leq \ell(\sigma) + \ell(\tau)$ for all $\sigma \in S_n$ and $\tau \in S_n$.

(c) Let $k_1, k_2, \ldots, k_q \in [n-1]$, and let $\sigma = s_{k_1} s_{k_2} \cdots s_{k_q}$. Then, $q \geq \ell(\sigma)$ and $q \equiv \ell(\sigma) \bmod 2$.

Example 5.3.21. Let $n = 4$. Consider the two permutations $\sigma = 3214$ and $\tau = 3142$ (both written in one-line notation). Then, $\ell(\sigma) = 3$ and $\ell(\tau) = 3$. Now, the permutation $\sigma\tau = 1342$ has length $\ell(\sigma\tau) = 2$.

Corollary 5.3.20 **(a)** says $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \bmod 2$. In other words, $2 \equiv 3 + 3 \bmod 2$.

Corollary 5.3.20 **(b)** says $\ell(\sigma\tau) \leq \ell(\sigma) + \ell(\tau)$. In other words, $2 \leq 3 + 3$.

Proof of Corollary 5.3.20 (sketched). **(a)** (See [Grinbe15, Exercise 5.2 **(b)**] for details.)

For any $\sigma \in S_n$ and any $k \in [n-1]$, we have

$$\ell(\sigma s_k) \equiv \ell(\sigma) + 1 \bmod 2. \tag{167}$$

(This follows from Lemma 5.3.14 **(a)**, since both numbers $\ell(\sigma)+1$ and $\ell(\sigma)-1$ are congruent to $\ell(\sigma)+1$ modulo 2.)

Now, let $\sigma \in S_n$ and $\tau \in S_n$. Theorem 5.3.17 **(a)** yields that we can write τ as a composition of $\ell(\tau)$ simples. In other words, we can write τ as $\tau = s_{k_1}s_{k_2}\cdots s_{k_q}$ for some $k_1, k_2, \ldots, k_q \in [n-1]$, where $q = \ell(\tau)$. Consider these $k_1, k_2, \ldots, k_q$. Now,

$$\begin{aligned}
\ell(\sigma\tau) &= \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_q}\right) \qquad \left(\text{since } \tau = s_{k_1}s_{k_2}\cdots s_{k_q}\right)\\
&\equiv \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-1}}\right)+1 \qquad (\text{by (167)})\\
&\equiv \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right)+2\\
&\qquad \left(\text{since (167) yields } \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-1}}\right) \equiv \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right)+1 \bmod 2\right)\\
&\equiv \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-3}}\right)+3\\
&\qquad \left(\text{since (167) yields } \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right) \equiv \ell\left(\sigma s_{k_1}s_{k_2}\cdots s_{k_{q-3}}\right)+1 \bmod 2\right)\\
&\equiv \cdots\\
&\equiv \ell(\sigma) + \underbrace{q}_{=\ell(\tau)} = \ell(\sigma)+\ell(\tau) \bmod 2.
\end{aligned}$$

This proves Corollary 5.3.20 **(a)**.

(b) (See [Grinbe15, Exercise 5.2 **(c)**] for details.)

This is analogous to the proof of Corollary 5.3.20 **(a)** (but using inequalities instead of congruences, and using (166) instead of (167)).

(c) Let $k_1, k_2, \ldots, k_q \in [n-1]$, and let $\sigma = s_{k_1}s_{k_2}\cdots s_{k_q}$. We must prove that $q \geq \ell(\sigma)$ and $q \equiv \ell(\sigma) \bmod 2$.

From $\sigma = s_{k_1}s_{k_2}\cdots s_{k_q}$, we obtain

$$\begin{aligned}
\ell(\sigma) &= \ell\left(s_{k_1}s_{k_2}\cdots s_{k_q}\right)\\
&\equiv \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-1}}\right)+1 \qquad (\text{by (167)})\\
&\equiv \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right)+2\\
&\qquad \left(\text{since (167) yields } \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-1}}\right) \equiv \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right)+1 \bmod 2\right)\\
&\equiv \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-3}}\right)+3\\
&\qquad \left(\text{since (167) yields } \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-2}}\right) \equiv \ell\left(s_{k_1}s_{k_2}\cdots s_{k_{q-3}}\right)+1 \bmod 2\right)\\
&\equiv \cdots\\
&\equiv \underbrace{\ell(\mathrm{id})}_{=0} + q \qquad (\text{since the product of 0 simples is } \mathrm{id})\\
&= q \bmod 2.
\end{aligned}$$

In other words, $q \equiv \ell(\sigma) \bmod 2$. A similar argument (but using inequalities instead of congruences, and using (166) instead of (167)) shows that $q \geq \ell(\sigma)$. Thus, Corollary 5.3.20 **(c)** is proved. □

Corollary 5.3.22. Let $n \in \mathbb{N}$. Then, the group S_n is generated by the simples $s_1, s_2, \ldots, s_{n-1}$.

Proof. This follows directly from Theorem 5.3.17 **(a)**. □

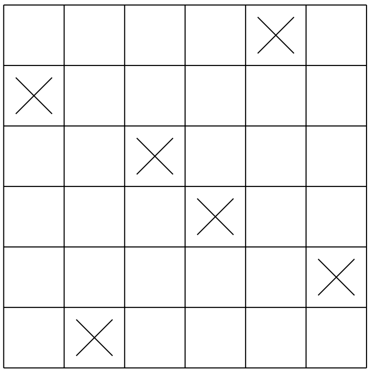
Theorem 5.3.17 **(a)** shows that every permutation $\sigma \in S_n$ can be represented as a product of $\ell(\sigma)$ simples (and in most cases, this can be done in many different ways). It turns out that there is a rather explicit way to find such a representation:

Remark 5.3.23. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Let us represent the Lehmer code of σ visually as follows:

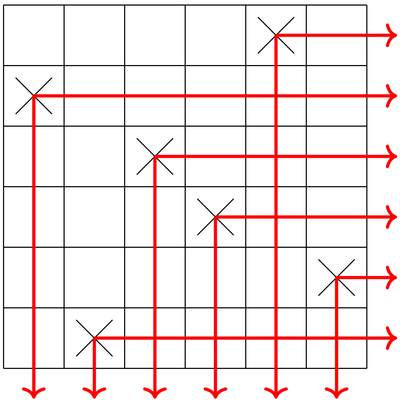
We draw an (empty) $n \times n$-matrix.

For each $i \in [n]$, we put a cross × into the cell $(i, \sigma(i))$ of the matrix.

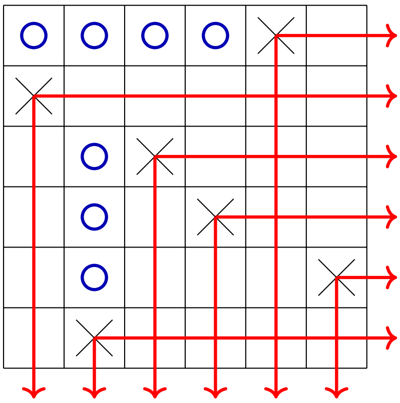
In the following, I will use the case $n = 6$ and $\sigma = 513462$ (in one-line notation) as a running example. In this case, the matrix looks as follows:



Now, starting from each ×, we draw a vertical ray downwards and a horizontal ray eastwards. I will call these two rays the *Lehmer lasers*. Here is how the rays look like in our running example:



Now, we draw a little circle $\circ$ into each cell that is not hit by any laser. Here is where the circles end up in our example:



This picture is called the *Rothe diagram* of σ.

Explicitly, a cell (i,j) has a $\circ$ in it if and only if

$$\sigma(i) > j \text{ and } \sigma^{-1}(j) > i$$

(indeed, the vertical laser in column j hits cell (i,j) if and only if $\sigma^{-1}(j) \leq i$, whereas the horizontal laser in row i hits cell (i,j) if and only if $\sigma(i) \leq j$).

If we substitute $\sigma(j)$ for j in this statement, then we obtain the following: A cell $(i, \sigma(j))$ has a $\circ$ in it if and only if

$$\sigma(i) > \sigma(j) \quad \text{and } j > i.$$

In other words, a cell $(i, \sigma(j))$ has a $\circ$ in it if and only if (i,j) is an inversion of σ.

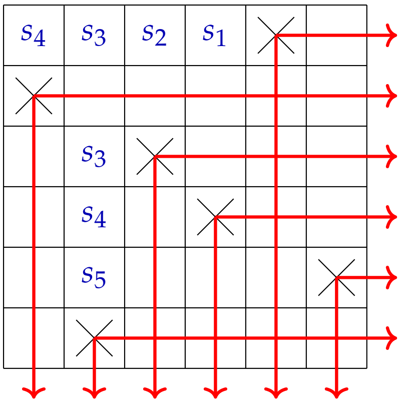
Thus,

$$\ell(\sigma) = (\# \text{ of inversions of } \sigma) = (\# \text{ of } \circ\text{'s}),$$

and

$$\ell_i(\sigma) = (\# \text{ of } \circ\text{'s in row } i) \qquad \text{for each } i \in [n].$$

Finally, let us label the $\circ$'s as follows: For each $i \in [n]$, we label the $\circ$'s in row i from right to left by the simple transpositions $s_i, s_{i+1}, s_{i+2}, \ldots, s_{i'-1}$ where $i' = i + \ell_i(\sigma)$. (This works, since there are precisely $\ell_i(\sigma) = i' - i$ many $\circ$'s in row i.) Here is how this labeling looks in our running example:



Finally, read the matrix row by row, starting with the top row, and reading each row from left to right. The result, in our running example, is

$$s_4 s_3 s_2 s_1 s_3 s_4 s_5.$$

Reading this as a product, we obtain a product of $\ell(\sigma)$ simples that equals σ.

The claim of Remark 5.3.23 can be restated in a more direct (if less visual) fashion:

Proposition 5.3.24. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. For each $i \in [n]$, we set

$$a_i := \operatorname{cyc}_{i', i'-1, i'-2, \ldots, i} = s_{i'-1} s_{i'-2} s_{i'-3} \cdots s_i, \tag{168}$$

where $i' = i + \ell_i(\sigma)$. Then, $\sigma = a_1 a_2 \cdots a_n$. (The second equality sign in (168) is not hard to check. Note that $a_n = \operatorname{id}$.)

We refer to [Grinbe15, Exercise 5.21 parts **(b)** and **(c)**] for a (detailed, but annoyingly long) proof of Proposition 5.3.24. (You are probably better off proving it yourself.)

5.4. Signs of permutations

The notion of the *sign* (aka *signature*) of a permutation is a simple consequence of that of its length; moreover, it is rather well-known, due to its role in the definition of a determinant. Thus we will survey its properties quickly and without proofs. More can be found in [Grinbe15, §5.3 and §5.6] and [Strick13, Appendix B].

Definition 5.4.1. Let $n \in \mathbb{N}$. The *sign* of a permutation $\sigma \in S_n$ is defined to be the integer $(-1)^{\ell(\sigma)}$.

It is denoted by $(-1)^{\sigma}$ or $\operatorname{sgn}(\sigma)$ or $\operatorname{sign}(\sigma)$ or $\varepsilon(\sigma)$. It is also known as the *signature* of σ.

Proposition 5.4.2. Let $n \in \mathbb{N}$.

(a) The sign of the permutation $\operatorname{id} \in S_n$ is $(-1)^{\operatorname{id}} = 1$.

(b) For any two distinct elements i and j of $[n]$, the transposition $t_{i,j} \in S_n$ has sign $(-1)^{t_{i,j}} = -1$.

(c) For any positive integer k and any distinct elements $i_1, i_2, \ldots, i_k \in [n]$, the k-cycle $\operatorname{cyc}_{i_1, i_2, \ldots, i_k}$ has sign $(-1)^{\operatorname{cyc}_{i_1, i_2, \ldots, i_k}} = (-1)^{k-1}$.

(d) We have $(-1)^{\sigma\tau} = (-1)^{\sigma} \cdot (-1)^{\tau}$ for any $\sigma \in S_n$ and $\tau \in S_n$.

(e) We have $(-1)^{\sigma_1 \sigma_2 \cdots \sigma_p} = (-1)^{\sigma_1} (-1)^{\sigma_2} \cdots (-1)^{\sigma_p}$ for any $\sigma_1, \sigma_2, \ldots, \sigma_p \in S_n$.

(f) We have $(-1)^{\sigma^{-1}} = (-1)^{\sigma}$ for any $\sigma \in S_n$. (The left hand side here has to be understood as $(-1)^{\left(\sigma^{-1}\right)}$.)

(g) We have

$$(-1)^{\sigma} = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \qquad \text{for each } \sigma \in S_n.$$

(The product sign "$\prod\limits_{1 \leq i < j \leq n}$" means a product over all pairs (i, j) of integers satisfying $1 \leq i < j \leq n$. There are $\dbinom{n}{2}$ such pairs.)

(h) If $x_1, x_2, \ldots, x_n$ are any elements of some commutative ring, and if $\sigma \in S_n$, then

$$\prod_{1 \leq i < j \leq n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right) = (-1)^{\sigma} \prod_{1 \leq i < j \leq n} \left(x_i - x_j\right).$$

Proof of Proposition 5.4.2 (sketched). Most of this follows easily from what we have proved above, but here are references to complete proofs:

(a) This is [Grinbe15, Proposition 5.15 **(a)**], and follows easily from $\ell(\mathrm{id}) = 0$.

(d) This is [Grinbe15, Proposition 5.15 **(c)**], and follows easily from Corollary 5.3.20 **(a)**. A different proof appears in [Strick13, Proposition B.13].

(b) This is [Grinbe15, Exercise 5.10 **(b)**], and follows easily from Exercise A.4.3.2 **(a)**.

(c) This is [Grinbe15, Exercise 5.17 **(d)**], and follows easily from Exercise A.4.2.1 **(a)** and Exercise A.4.3.2 **(b)** using Proposition 5.4.2 **(d)**.

(e) This is [Grinbe15, Proposition 5.28], and follows by induction from Proposition 5.4.2 **(d)**.

(f) This is [Grinbe15, Proposition 5.15 **(d)**], and follows easily from Proposition 5.4.2 **(d)** or from Proposition 5.3.13.

(h) This is [Grinbe15, Exercise 5.13 **(a)**] (or, rather, the straightforward generalization of [Grinbe15, Exercise 5.13 **(a)**] to arbitrary commutative rings). The proof is fairly easy: Each factor $x_{\sigma(i)} - x_{\sigma(j)}$ on the left hand side appears also on the right hand side, albeit with a different sign if (i, j) is an inversion of σ. Thus, the products on both sides agree up to a sign, which is precisely $(-1)^{\ell(\sigma)} = (-1)^{\sigma}$.

(g) This is [Grinbe15, Exercise 5.13 **(c)**], and is a particular case of Proposition 5.4.2 **(h)**. □

Corollary 5.4.3. Let $n \in \mathbb{N}$. The map

$$\begin{aligned} S_n &\to \{1, -1\}, \\ \sigma &\mapsto (-1)^{\sigma} \end{aligned}$$

is a group homomorphism from the symmetric group S_n to the order-2 group $\{1,-1\}$. (Of course, $\{1,-1\}$ is a group with respect to multiplication.)

This map is known as the *sign homomorphism*.

Proof of Corollary 5.4.3 (sketched). Proposition 5.4.2 **(d)** shows that this map respects multiplication (i.e., sends products to products). However, if a map between two groups respects multiplication, then it is automatically a group homomorphism. Thus, Corollary 5.4.3 follows. □

Definition 5.4.4. Let $n \in \mathbb{N}$. A permutation $\sigma \in S_n$ is said to be

- *even* if $(-1)^\sigma = 1$ (that is, if $\ell(\sigma)$ is even);
- *odd* if $(-1)^\sigma = -1$ (that is, if $\ell(\sigma)$ is odd).

The sign and the "parity" (i.e., evenness/oddness) of a permutation has applications throughout mathematics (in the definition of determinants and the construction of exterior powers) as well as in the solution of *permutation puzzles* (such as Rubik's cube and the 15-game; see [Mulhol21, Chapters 7–8 and Theorem 20.2.1] for example). Even permutations are also crucial in group theory, as they form a group:

Corollary 5.4.5. Let $n \in \mathbb{N}$. The set of all even permutations in S_n is a normal subgroup of S_n.

This subgroup is known as the *n-th alternating group* (commonly called A_n). If $n \geq 5$, then this group is a simple group (meaning that it has no normal subgroups besides itself and the trivial group)[68], and this fact has been used by Galois to prove that the general 5-th degree polynomial equation cannot be solved using radicals.

Proof of Corollary 5.4.5 (sketched). The set of all even permutations in S_n is the kernel of the group homomorphism $S_n \to \{1,-1\}$ from Corollary 5.4.3. Thus, it is a normal subgroup of S_n (since any kernel is a normal subgroup). □

Corollary 5.4.6. Let $n \geq 2$. Then,

$$(\text{\# of even permutations } \sigma \in S_n) = (\text{\# of odd permutations } \sigma \in S_n) = n!/2.$$

[68] See, e.g., `https://groupprops.subwiki.org/wiki/Alternating_groups_are_simple` or [Goodma15, Theorem 10.3.4] for a proof.

Proof of Corollary 5.4.6 (sketched). The symmetric group S_n contains the simple transposition s_1 (since $n \geq 2$). If $\sigma \in S_n$, then

$$\begin{aligned}(-1)^{\sigma s_1} &= (-1)^{\sigma} \cdot \underbrace{(-1)^{s_1}}_{\substack{=-1 \\ \text{(by Proposition 5.4.2 \textbf{(b)},} \\ \text{since } s_1 = t_{1,2})}} \qquad \text{(by Proposition 5.4.2 \textbf{(d)})} \\ &= -(-1)^{\sigma}.\end{aligned}$$

Hence, a permutation $\sigma \in S_n$ is even if and only if the permutation σs_1 is odd. Hence, the map

$$\{\text{even permutations } \sigma \in S_n\} \to \{\text{odd permutations } \sigma \in S_n\}, \\ \sigma \mapsto \sigma s_1$$

is well-defined. This map is furthermore a bijection (since S_n is a group). Thus, the bijection principle yields

$$(\# \text{ of even permutations } \sigma \in S_n) = (\# \text{ of odd permutations } \sigma \in S_n).$$

Both sides of this equality must furthermore equal to $n!/2$, since they add up to $|S_n| = n!$. This proves Corollary 5.4.6. (See [Grinbe15, Exercise 5.4] for details.) □

As a consequence of Corollary 5.4.6, we see that

$$\sum_{\sigma \in S_n} (-1)^{\sigma} = 0 \qquad \text{for each } n \geq 2. \tag{169}$$

(Indeed, the sum $\sum_{\sigma \in S_n} (-1)^{\sigma}$ can be rewritten as

$$(\# \text{ of even permutations } \sigma \in S_n) - (\# \text{ of odd permutations } \sigma \in S_n),$$

since the addends corresponding to the even permutations $\sigma \in S_n$ are equal to 1 whereas the addends corresponding to the odd permutations $\sigma \in S_n$ are equal to -1.)

We note that the sign can be defined not only for a permutation $\sigma \in S_n$, but also for any permutation of any finite set X (even if the set X has no chosen total order on it, as the set $[n]$ has). Here is one way to do so:

Proposition 5.4.7. Let X be a finite set. We want to define the sign of any permutation of X.

Fix a bijection $\phi : X \to [n]$ for some $n \in \mathbb{N}$. (Such a bijection always exists, since X is finite.) For every permutation σ of X, set

$$(-1)^{\sigma}_{\phi} := (-1)^{\phi \circ \sigma \circ \phi^{-1}}.$$

Here, the right hand side is well-defined, since $\phi \circ \sigma \circ \phi^{-1}$ is a permutation of $[n]$. Now:

(a) This number $(-1)^{\sigma}_{\phi}$ depends only on the permutation σ, but not on the bijection ϕ. (In other words, if ϕ_1 and ϕ_2 are two bijections from X to $[n]$, then $(-1)^{\sigma}_{\phi_1} = (-1)^{\sigma}_{\phi_2}$.)

Thus, we shall denote $(-1)^{\sigma}_{\phi}$ by $(-1)^{\sigma}$ from now on. We refer to this number $(-1)^{\sigma}$ as the *sign* of the permutation $\sigma \in S_X$. (When $X = [n]$, this notation does not clash with Definition 5.4.1, since we can pick the bijection $\phi = \operatorname{id}$ and obtain $(-1)^{\sigma}_{\phi} = (-1)^{\operatorname{id} \circ \sigma \circ \operatorname{id}^{-1}} = (-1)^{\sigma}$.)

(b) The identity permutation $\operatorname{id} : X \to X$ satisfies $(-1)^{\operatorname{id}} = 1$.

(c) We have $(-1)^{\sigma\tau} = (-1)^{\sigma} \cdot (-1)^{\tau}$ for any two permutations σ and τ of X.

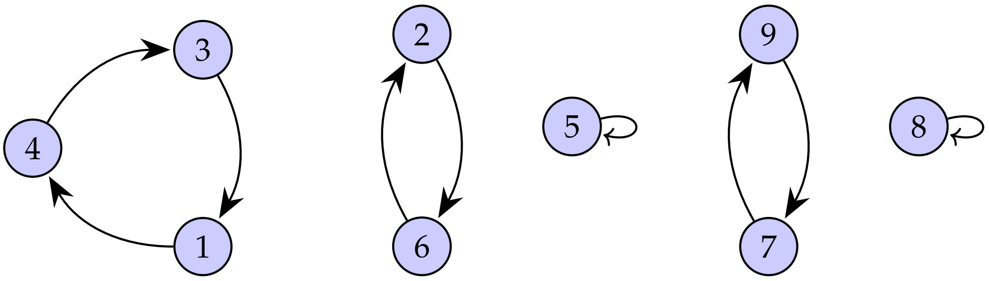
Proof of Proposition 5.4.7 (sketched). This all follows quite easily from Proposition 5.4.2 **(d)**. See [Grinbe15, Exercise 5.12] for a detailed proof. □

5.5. The cycle decomposition

Next, we shall discuss the *cycle decomposition* (or *disjoint cycle decomposition*) of a permutation. Again, this is a fairly well-known and elementary tool, so we will restrict ourselves to the basic properties and omit the details.

We begin with an introductory example:

Example 5.5.1. Let $\sigma \in S_9$ be the permutation with one-line notation 461352987. Here is its cycle digraph:



(where we have strategically arranged the cycles apart horizontally). This digraph consists of five node-disjoint cycles (i.e., cycles that share no nodes); thus, we can view the permutation σ as acting on the five subsets $\{1,4,3\}$, $\{2,6\}$, $\{5\}$, $\{7,9\}$ and $\{8\}$ of $[9]$ separately. On the first of these five subsets, σ acts as the 3-cycle $\operatorname{cyc}_{1,4,3}$ (in the sense that $\sigma(k) = \operatorname{cyc}_{1,4,3}(k)$ for each $k \in \{1,4,3\}$). On the second, it acts as the 2-cycle $\operatorname{cyc}_{2,6}$. On the third, it acts as the 1-cycle cyc_5 (which, of course, is the identity map). On the fourth, it acts as the 2-cycle $\operatorname{cyc}_{7,9}$. On the fifth, it acts as the 1-cycle cyc_8 (which, again, is just the identity map). Combining these observations, we conclude that

$$\sigma(k) = \left(\operatorname{cyc}_{1,4,3} \circ \operatorname{cyc}_{2,6} \circ \operatorname{cyc}_5 \circ \operatorname{cyc}_{7,9} \circ \operatorname{cyc}_8\right)(k) \qquad \text{for each } k \in [9]$$

(because, when we apply the composed permutation $\operatorname{cyc}_{1,4,3} \circ \operatorname{cyc}_{2,6} \circ \operatorname{cyc}_5 \circ \operatorname{cyc}_{7,9} \circ \operatorname{cyc}_8$ to an element of $[9]$, then four of the five cycles $\operatorname{cyc}_{1,4,3}, \operatorname{cyc}_{2,6}, \operatorname{cyc}_5, \operatorname{cyc}_{7,9}, \operatorname{cyc}_8$ will leave this element unchanged, whereas the remaining one will move it one step forward along the appropriate cycle of the above digraph – which is precisely what the permutation σ does to our element). This entails that

$$\sigma = \operatorname{cyc}_{1,4,3} \circ \operatorname{cyc}_{2,6} \circ \operatorname{cyc}_5 \circ \operatorname{cyc}_{7,9} \circ \operatorname{cyc}_8 . \tag{170}$$

In Example 5.5.1, we have represented our permutation $\sigma \in S_9$ as a composition of five cycles with the property that each element of $[9]$ appears in exactly one of these cycles. This is not specific to the permutation σ chosen in Example 5.5.1. Indeed, for any finite set X, any permutation $\sigma \in S_X$ can be written as a composition of finitely many cycles $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ with the property that each element of X appears in exactly one of these cycles. Moreover, this representation of σ is unique up to

- swapping the cycles (for example, we could have replaced $\operatorname{cyc}_{1,4,3} \circ \operatorname{cyc}_{2,6}$ by $\operatorname{cyc}_{2,6} \circ \operatorname{cyc}_{1,4,3}$ in (170)), and
- rotating each cycle (for example, we could have replaced $\operatorname{cyc}_{1,4,3}$ by $\operatorname{cyc}_{4,3,1}$ or by $\operatorname{cyc}_{3,1,4}$ in (170)).

Let us state this in a more rigorous fashion:

Theorem 5.5.2 (disjoint cycle decomposition of permutations)**.** Let X be a finite set. Let σ be a permutation of X. Then:

(a) There is a list

$$\begin{aligned} \Big(& (a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}), \\ & (a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}), \\ & \ldots, \\ & (a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}) \Big) \end{aligned}$$

of lists of elements of X such that:

- each element of X appears exactly once in the composite list

$$\begin{aligned} (& a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}, \\ & a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}, \\ & \ldots, \\ & a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}), \end{aligned}$$

and

- we have

$$\sigma = \operatorname{cyc}_{a_{1,1},a_{1,2},\ldots,a_{1,n_1}} \circ \operatorname{cyc}_{a_{2,1},a_{2,2},\ldots,a_{2,n_2}} \circ \cdots \circ \operatorname{cyc}_{a_{k,1},a_{k,2},\ldots,a_{k,n_k}}.$$

Such a list is called a *disjoint cycle decomposition* (or short *DCD*) of σ. Its entries (which themselves are lists of elements of X) are called the *cycles* of σ.

(b) Any two DCDs of σ can be obtained from each other by (repeatedly) swapping the cycles with each other, and rotating each cycle (i.e., replacing $(a_{i,1}, a_{i,2}, \ldots, a_{i,n_i})$ by $(a_{i,2}, a_{i,3}, \ldots, a_{i,n_i}, a_{i,1})$).

(c) Now assume that X is a set of integers (or, more generally, any totally ordered finite set). Then, there is a unique DCD

$$\Big((a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}), \\ (a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}), \\ \ldots, \\ (a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}) \Big)$$

of σ that satisfies the additional requirements that

- we have $a_{i,1} \leq a_{i,p}$ for each $i \in [k]$ and each $p \in [n_i]$ (that is, each cycle in this DCD is written with its smallest entry first), and
- we have $a_{1,1} > a_{2,1} > \cdots > a_{k,1}$ (that is, the cycles appear in this DCD in the order of decreasing first entries).

Example 5.5.3. Let $\sigma \in S_9$ be the permutation from Example 5.5.1. Then, the representation (170) shows that

$$\Big((1,4,3), \ (2,6), \ (5), \ (7,9), \ (8) \Big)$$

is a DCD of σ. By swapping the five cycles of this DCD, and by rotating each cycle, we can produce various other DCDs of σ, such as

$$\Big((7,9), \ (6,2), \ (3,1,4), \ (8), \ (5) \Big).$$

The unique DCD of σ that satisfies the two additional requirements of Theorem 5.5.2 **(c)** is

$$\Big((8), \ (7,9), \ (5), \ (2,6), \ (1,4,3) \Big).$$

Proof of Theorem 5.5.2 (sketched). This is a classical result with an easy proof;

sadly, this easy proof does not present well in writing. I will try to be as clear as the situation allows. Some familiarity with digraphs (= directed graphs) is recommended[69].

(a) Let $\mathcal{D}$ be the cycle digraph of σ, as in Example 5.5.1. This cycle digraph $\mathcal{D}$ has the following two properties:

- *Outbound uniqueness:* For each node i, there is exactly one arc outgoing from i. (Indeed, this is the arc from i to $\sigma(i)$, as should be clear from the construction of $\mathcal{D}$.)

- *Inbound uniqueness:* For each node i, there is exactly one arc incoming into i. (Indeed, this is the arc from $\sigma^{-1}(i)$ to i, since σ is a permutation and therefore invertible.)

Using these two properties, we will now show that the cycle digraph $\mathcal{D}$ consists of several node-disjoint cycles (i.e., several cycles that pairwise share no nodes).

Indeed, let us first observe the following: If two cycles C and D of $\mathcal{D}$ have a node in common, then they are identical[70] (because the outbound uniqueness property prevents these cycles from ever separating after meeting at the common node). In other words, any two cycles C and D of $\mathcal{D}$ are either identical or node-disjoint (i.e., share no nodes with each other).

Now, let i be any node of $\mathcal{D}$. Then, if we start at i and follow the outgoing arcs, then we obtain an infinite walk

$$\sigma^0(i) \to \sigma^1(i) \to \sigma^2(i) \to \sigma^3(i) \to \cdots$$

along our digraph $\mathcal{D}$. Since X is finite, the Pigeonhole Principle guarantees that this walk will eventually revisit a node it has already been to; i.e., there exist two integers $u, v \in \mathbb{N}$ with $u < v$ and $\sigma^u(i) = \sigma^v(i)$. Let us pick two such integers u, v with the **smallest** possible v. Thus,

$$\text{the } v \text{ nodes } \sigma^0(i), \sigma^1(i), \ldots, \sigma^{v-1}(i) \text{ are distinct} \tag{171}$$

(since otherwise, v would not be smallest possible). Now, σ is a permutation and thus has an inverse σ^{-1}. Applying the map σ^{-1} to both sides of the equality $\sigma^u(i) = \sigma^v(i)$, we obtain $\sigma^{u-1}(i) = \sigma^{v-1}(i)$. However, if we had $u \geq 1$, then (171) would entail $\sigma^{u-1}(i) \neq \sigma^{v-1}(i)$ (because $0 \leq \underbrace{u}_{<v} -1 < v-1$), which would contradict $\sigma^{u-1}(i) = \sigma^{v-1}(i)$. Thus, we cannot have $u \geq 1$. Hence, $u < 1$, so that $u = 0$. Therefore, $\sigma^u(i) = \sigma^0(i)$, so that $\sigma^0(i) = \sigma^u(i) = \sigma^v(i)$. This shows that our walk $\sigma^0(i) \to \sigma^1(i) \to \sigma^2(i) \to \sigma^3(i) \to \cdots$ is circular: it

[69] See, e.g., [Guicha20, §5.11] or [Loehr11, §3.5] for brief introductions to digraphs.

[70] Here, we identify any cycle with its cyclic rotations. For example, if $a \to b \to c \to a$ is a cycle, then we consider $b \to c \to a \to b$ to be the same cycle.

comes back to its starting node $\sigma^0(i) = i$ after v steps. We have thus found a cycle in our digraph $\mathcal{D}$:

$$\sigma^0(i) \to \sigma^1(i) \to \sigma^2(i) \to \cdots \to \sigma^v(i) = \sigma^0(i).$$

(This is indeed a cycle, since (171) shows that its first v nodes are distinct.) This shows that the node i lies on a cycle C_i of $\mathcal{D}$ (namely, the cycle that we just found).

Now, forget that we fixed i. We thus have shown that each node i of $\mathcal{D}$ lies on a cycle C_i. The cycles C_i for all nodes $i \in X$ will be called the *chosen cycles*.

Any arc of our digraph $\mathcal{D}$ must belong to one of these chosen cycles. Indeed, if a is an arc from a node i to a node j, then a must be the only arc outgoing from i (by the outbound uniqueness property); but this means that this arc a belongs to the chosen cycle C_i.

Now, let us look back at what we have shown:

- Any node i of $\mathcal{D}$ lies on one of our chosen cycles (namely, on C_i).
- Some of the chosen cycles may be identical, but apart from that, the chosen cycles are pairwise node-disjoint (since any two cycles of $\mathcal{D}$ are either identical or node-disjoint).
- Any arc of $\mathcal{D}$ must belong to one of these chosen cycles.

Combining these facts, we conclude that $\mathcal{D}$ consists of several node-disjoint cycles. Let us label these cycles as

$$\begin{aligned}
&(a_{1,1} \to a_{1,2} \to \cdots \to a_{1,n_1} \to a_{1,1}), \\
&(a_{2,1} \to a_{2,2} \to \cdots \to a_{2,n_2} \to a_{2,1}), \\
&\ldots, \\
&(a_{k,1} \to a_{k,2} \to \cdots \to a_{k,n_k} \to a_{k,1})
\end{aligned}$$

(making sure to label each cycle only once). Then, each element of X appears exactly once in the composite list

$$\begin{aligned}
(&a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}, \\
&a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}, \\
&\ldots, \\
&a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}),
\end{aligned}$$

and we have

$$\sigma = \operatorname{cyc}_{a_{1,1},a_{1,2},\ldots,a_{1,n_1}} \circ \operatorname{cyc}_{a_{2,1},a_{2,2},\ldots,a_{2,n_2}} \circ \cdots \circ \operatorname{cyc}_{a_{k,1},a_{k,2},\ldots,a_{k,n_k}}$$

(since σ moves any node $i \in X$ one step forward along its chosen cycle). This proves Theorem 5.5.2 **(a)**.

Alternative proofs of Theorem 5.5.2 **(a)** can be found (e.g.) in [Goodma15, Theorem 1.5.3] or in [Bourba74, Chapter I, §5.7, Proposition 7] or in [Sagan19, §1.9, proof of Theorem 1.5.1] (this is essentially our proof) or in `https://proofwiki.org/wiki/Existence_and_Uniqueness_of_Cycle_Decomposition` (see also [17f-hw7s, Exercise 7 **(e)** and **(d)**] for a rather formalized proof). Note that some of these sources work with a slightly modified concept of a DCD, in which they throw away the 1-cycles (i.e., they replace "appears exactly once" by "appears at most once", and require all cycle lengths $n_1, n_2, \ldots, n_k$ to be > 1). For instance, the DCD (170) becomes

$$\sigma = \operatorname{cyc}_{1,4,3} \circ \operatorname{cyc}_{2,6} \circ \operatorname{cyc}_{7,9}$$

if we use this modified notion of a DCD.

(b) See [Goodma15, Theorem 1.5.3] or [Bourba74, Chapter I, §5.7, Proposition 7]. The idea is fairly simple: Let

$$\begin{aligned} \Big(& \left(a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}\right), \\ & \left(a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}\right), \\ & \ldots, \\ & \left(a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}\right) \Big) \end{aligned}$$

be a DCD of σ. Then, for each $i \in [n]$, the cycle of this DCD that contains i is uniquely determined by σ and i up to cyclic rotation (indeed, it is a rotated version of the list $\left(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{r-1}(i)\right)$, where r is the smallest positive integer satisfying $\sigma^r(i) = i$). Therefore, all cycles of this DCD are uniquely determined by σ up to cyclic rotation and up to the relative order in which these cycles appear in the DCD. But this is precisely the claim of Theorem 5.5.2 **(b)**.

(c) In order to obtain a DCD of σ that satisfies these two requirements, it suffices to

- start with an arbitrary DCD of σ,
- then rotate each cycle of this DCD so that it begins with its smallest entry, and
- then repeatedly swap these cycles so they appear in the order of decreasing first entries.

It is clear that the result of this procedure is uniquely determined (a consequence of Theorem 5.5.2 **(b)**). Thus, Theorem 5.5.2 **(c)** is proven. □

Definition 5.5.4. Let X be a finite set. Let σ be a permutation of X.

(a) The *cycles* of σ are defined to be the cycles in the DCD of σ (as defined in Theorem 5.5.2 **(a)**). (This includes 1-cycles, if there are any in the DCD of σ.)

We shall equate a cycle of σ with any of its cyclic rotations; thus, for example, $(3,1,4)$ and $(1,4,3)$ shall be regarded as being the same cycle (but $(3,1,4)$ and $(3,4,1)$ shall not).

(b) The *cycle lengths partition* of σ shall denote the partition of $|X|$ obtained by writing down the lengths of the cycles of σ in weakly decreasing order.

Example 5.5.5. Let $\sigma \in S_9$ be the permutation from Example 5.5.1. Then, the cycles of σ are

$$(1,4,3), \ (2,6), \ (5), \ (7,9), \ (8).$$

Their lengths are $3,2,1,2,1$. Hence, the cycle lengths partition of σ is $(3,2,2,1,1)$.

The following is obvious:

Proposition 5.5.6. Let X be a finite set. Let $i,j \in X$. Let σ be a permutation of X. Then, we have the following chain of equivalences:

$$\begin{aligned} & (i \text{ and } j \text{ belong to the same cycle of } \sigma) \\ \Longleftrightarrow\ & (i = \sigma^p(j) \ \text{ for some } p \in \mathbb{N}) \\ \Longleftrightarrow\ & (j = \sigma^p(i) \ \text{ for some } p \in \mathbb{N}). \end{aligned}$$

The number of cycles of a permutation determines its sign. Let us state this for permutations of $[n]$ in particular (the reader can easily extend this to the general case using Proposition 5.4.7):

Proposition 5.5.7. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $k \in \mathbb{N}$ be such that σ has exactly k cycles (including the 1-cycles). Then, $(-1)^\sigma = (-1)^{n-k}$.

Proof of Proposition 5.5.7 (sketched). Let

$$\begin{aligned} & \left(a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}\right), \\ & \left(a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}\right), \\ & \ldots, \\ & \left(a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}\right) \end{aligned}$$

be the k cycles of σ. Thus,

$$\begin{aligned}\Big(&\left(a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}\right), \\ &\left(a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}\right), \\ &\ldots, \\ &\left(a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}\right) \Big)\end{aligned} \tag{172}$$

is the DCD of σ. Therefore,

$$\begin{aligned}\sigma &= \operatorname{cyc}_{a_{1,1},a_{1,2},\ldots,a_{1,n_1}} \circ \operatorname{cyc}_{a_{2,1},a_{2,2},\ldots,a_{2,n_2}} \circ \cdots \circ \operatorname{cyc}_{a_{k,1},a_{k,2},\ldots,a_{k,n_k}} \\ &= (\text{an } n_1\text{-cycle}) \circ (\text{an } n_2\text{-cycle}) \circ \cdots \circ (\text{an } n_k\text{-cycle}),\end{aligned}$$

so that

$$\begin{aligned}(-1)^{\sigma} &= (-1)^{(\text{an } n_1\text{-cycle})\circ(\text{an } n_2\text{-cycle})\circ\cdots\circ(\text{an } n_k\text{-cycle})} \\ &= (-1)^{(\text{an } n_1\text{-cycle})} \cdot (-1)^{(\text{an } n_2\text{-cycle})} \cdot \cdots \cdot (-1)^{(\text{an } n_k\text{-cycle})} \\ &\qquad (\text{by Proposition 5.4.2 } \textbf{(e)}) \\ &= (-1)^{n_1-1} \cdot (-1)^{n_2-1} \cdot \cdots \cdot (-1)^{n_k-1} \\ &\qquad \left(\begin{array}{c}\text{since Proposition 5.4.2 } \textbf{(c)} \text{ yields } (-1)^{(\text{a } p\text{-cycle})} = (-1)^{p-1} \\ \text{for any } p > 0\end{array}\right) \\ &= (-1)^{(n_1-1)+(n_2-1)+\cdots+(n_k-1)}.\end{aligned} \tag{173}$$

However, recall that (172) is a DCD of σ. Thus, each element of $[n]$ appears exactly once in the composite list

$$\begin{aligned}(&a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}, \\ &a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}, \\ &\ldots, \\ &a_{k,1}, a_{k,2}, \ldots, a_{k,n_k}).\end{aligned}$$

Therefore, the length $n_1 + n_2 + \cdots + n_k$ of this composite list equals the size $|[n]| = n$ of the set $[n]$. In other words, $n_1 + n_2 + \cdots + n_k = n$. Hence,

$$(n_1 - 1) + (n_2 - 1) + \cdots + (n_k - 1) = \underbrace{(n_1 + n_2 + \cdots + n_k)}_{=n} - k = n - k.$$

Thus, (173) rewrites as $(-1)^{\sigma} = (-1)^{n-k}$. This proves Proposition 5.5.7. □

5.6. References

We end our discussion of permutations here, although we will revisit it every once in a while. Much more about permutations can be found in [Bona12], [Kitaev11] (focussing on permutation patterns), [Sagan01] (focussing on the representation theory of the symmetric group) and various other texts.

It is worth mentioning that the symmetric groups S_n are a particular case of *Coxeter groups* – a class of groups highly significant to algebra, combinatorics and geometry. One of the most combinatorial introductions to this subject (which sheds new light on the combinatorics of symmetric groups) is the highly readable text [BjoBre05]. Other texts include [Cohen08] and (for the particularly resolute) [Bourba02, Chapter IV].

6. Alternating sums, signed counting and determinants

This chapter is not concerned with any specific combinatorial objects like partitions or permutations, but rather with a set of simple ideas that appear often (and not just in combinatorics). The main objects of study here are *alternating sums* – i.e., sums with a $(-1)^{\text{something}}$ factor in them. A poster child is the determinant of a matrix. Such sums are often simplified by the cancellation that occurs in them, with positive addends cancelling negative addends. Frequently, understanding this cancellation is key to computing the sums. As a rule of thumb, alternating sums are more likely to have simple closed-form answers than non-alternating sums. For example, each $n \in \mathbb{N}$ satisfies

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3 = \begin{cases} (-1)^{n/2} \dfrac{(3n/2)!}{(n/2)!^3}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}$$

(see Exercise A.2.15.5 **(g)**), but there is no closed form for

$$\sum_{k=0}^{n} \binom{n}{k}^3 .$$

The use of cancellations to simplify alternating sums is old, but systematic surveys of applications of this technique have not appeared until recently ([Stanle11, Chapter 2], [Aigner07, Chapter 5], [BenQui03, Chapter 6], [BenQui08], [Sagan19, Chapter 2], [Grinbe20]).

6.1. Cancellations in alternating sums

We begin with a simple binomial identity:

Proposition 6.1.1 (Negative hockey-stick identity)**.** Let $n \in \mathbb{C}$ and $m \in \mathbb{N}$. Then,

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}. \qquad (174)$$

There are easy proofs of this proposition by induction on m or by the telescope principle (see, e.g., [18f-hw2s, Exercise 4] and [19fco, Exercise 2.1.1 **(a)** and §7.27]). However, let us try to prove the proposition combinatorially. For a bijective proof, the $(-1)^k$ and $(-1)^m$ factors would be gamestoppers, as there is no way to get a negative number (let alone a number of variable sign) by counting something. However, if we think of the $(-1)^k$ as an opportunity for cancelling addends, then we can use combinatorics pretty well:

Combinatorial proof of Proposition 6.1.1 (sketched). We need to prove the equality (174). Both sides of this equality are polynomial functions in n. Thus, we can WLOG assume that n is a positive integer (because of the polynomial identity trick that we saw in Subsection 3.2.3). Assume this.

Set $[n] := \{1, 2, \ldots, n\}$. We shall now introduce some notations tailored for this particular proof.

Define an *acceptable set* to be a subset of $[n]$ that has size $\leq m$. Clearly,

$$(\#\text{ of acceptable sets}) = \sum_{k=0}^{m} \binom{n}{k} \tag{175}$$

(since the # of k-element subsets of $[n]$ equals $\binom{n}{k}$ for each $k \in \mathbb{Z}$). Incidentally, we note that there is no closed form for this sum – another instance of the phenomenon in which alternating sums are simpler than non-alternating ones.

Define the *sign* of a finite set I to be $(-1)^{|I|}$. Then,

$$\begin{aligned}&(\text{the sum of the signs of all acceptable sets})\\ &= \sum_{k=0}^{m} (-1)^k \binom{n}{k}.\end{aligned} \tag{176}$$

(This can be shown just like (175).)

However, the sum of the signs of all acceptable sets is a sum of 1s and -1s. Let us try to cancel as many of these 1s and -1s against each other as we can, hoping that what remains will be precisely $(-1)^m \binom{n-1}{m}$.

In order to cancel two addends, we need to pair up two finite sets I that have opposite signs. How do we find such pairs? One way to do so is to pick some set I that does not contain the element 1, and pair it up with $I \cup \{1\}$. Alternatively, we can pick some set I that contains the element 1, and pair it up with $I \setminus \{1\}$. In other words, we pair up a finite set I with either $I \setminus \{1\}$ or $I \cup \{1\}$, depending on whether $1 \in I$ or $1 \notin I$.

Let us do this systematically for all finite sets: For each finite set I, we define the *partner* of I to be the set

$$I' := \begin{cases} I \setminus \{1\}, & \text{if } 1 \in I; \\ I \cup \{1\}, & \text{if } 1 \notin I \end{cases} = I \bigtriangleup \{1\},$$

where the notation $X \bigtriangleup Y$ means the symmetric difference $(X \cup Y) \setminus (X \cap Y)$ of two sets X and Y (as in Subsection 3.2.1). It is easy to see that each finite set I satisfies $I'' = I$ and $|I'| = |I| \pm 1$, so that $(-1)^{|I'|} = -(-1)^{|I|}$. Thus, if both I and I' are acceptable sets, then their contributions to the sum of the signs of all acceptable sets cancel each other out.

This does not mean that all addends in this sum cancel. Indeed, while each finite set has a partner, it may happen that an acceptable set has a non-acceptable partner, and then the contribution of the former to the sum does not get cancelled (since the partner does not contribute to the sum). Thus, in order to see what remains of the sum after the cancellations, we need to study the acceptable sets that have non-acceptable partners.

Fortunately, this is easy: In order for an acceptable set I to have a non-acceptable partner, it needs to satisfy $1 \notin I$ and $|I| = m$. Better yet, this is an "if and only if" statement:

> *Claim 1:* Let I be an acceptable set. Then, the partner I' of I is non-acceptable if and only if $(1 \notin I$ and $|I| = m)$.

[*Proof of Claim 1:* The "if" direction is easy: If $1 \notin I$ and $|I| = m$, then the partner I' of I is defined by $I' = I \cup \{1\}$ and thus has size $|I'| = |I| + 1 > |I| = m$, which shows that it is non-acceptable.

It remains to prove the converse, i.e., the "only if" direction. Thus, we assume that the partner I' of I is non-acceptable. We must show that $1 \notin I$ and $|I| = m$.

Since I is acceptable, we have $I \subseteq [n]$ and $|I| \leq m$. If we had $1 \in I$, then we would have $I' = I \setminus \{1\} \subseteq I \subseteq [n]$ and furthermore $|I'| \leq |I|$ (since $I' \subseteq I$), so that $|I'| \leq |I| \leq m$. This would entail that I' is acceptable (since $I' \subseteq [n]$ and $|I'| \leq m$), which would contradict our assumption that I' be non-acceptable. Hence, we cannot have $1 \in I$. Thus, $1 \notin I$ is proved. Hence, $I' = I \cup \{1\}$. However, $1 \in [n]$ (since $n \geq 1$), and $I' = I \cup \{1\} \subseteq [n]$ (since $I \subseteq [n]$ and $1 \in [n]$). Moreover, from $I' = I \cup \{1\}$, we obtain $|I'| = |I \cup \{1\}| = |I| + 1$. Now, if we had $|I| \leq m - 1$, then we would obtain $|I'| = |I| + 1 \leq m$ (since $|I| \leq m - 1$), which would entail that I' is acceptable (since $I' \subseteq [n]$), which again would contradict our assumption. Thus, we cannot have $|I| \leq m - 1$. Hence, $|I| > m - 1$, so that $|I| \geq m$ and therefore $|I| = m$ (since $|I| \leq m$). Thus, we have shown that $1 \notin I$ and $|I| = m$. This proves the "only if" direction and thus completes the proof of Claim 1.]

Now, recall our line of reasoning: We start with the sum of the signs of all acceptable sets, and we cancel any two addends that correspond to an acceptable set and its acceptable partner. What remains are the addends corresponding to the acceptable sets that have non-acceptable partners. According to Claim 1, these are precisely the acceptable sets I that satisfy $(1 \notin I$ and $|I| = m)$. In other words, these are precisely the m-element subsets of $[n]$ that do not contain 1. In other words, these are precisely the m-element subsets of $[n] \setminus \{1\}$ (since a subset of $[n]$ that does not contain 1 is the same as a subset of $[n] \setminus \{1\}$).

Thus, there are precisely $\dbinom{n-1}{m}$ of these subsets (since $[n] \setminus \{1\}$ is an $(n-1)$-element set), and each of them has sign $(-1)^m$. Hence, there are precisely $\dbinom{n-1}{m}$ addends left in the sum after our cancellations, and each of these addends is $(-1)^m$. Hence,

$$(\text{the sum of the signs of all acceptable sets}) = (-1)^m \dbinom{n-1}{m}.$$

Comparing this with (176), we obtain

$$\sum_{k=0}^{m} (-1)^k \dbinom{n}{k} = (-1)^m \dbinom{n-1}{m}.$$

This proves Proposition 6.1.1. □

Let me outline how to formalize this argument without using vague notions like "cancelling" and "pairing up". We let

$$\mathcal{A} := \{\text{acceptable sets}\}$$

and

$$\begin{aligned}\mathcal{X} &:= \{\text{acceptable sets whose partner is acceptable}\} \\ &= \{I \subseteq [n] \ \mid \ |I| \leq m \text{ but not } (|I| = m \text{ and } 1 \notin I)\}\end{aligned}$$

(by Claim 1 in the above proof). Now, we define a map

$$\begin{aligned} f : \mathcal{X} &\to \mathcal{X}, \\ I &\mapsto I'. \end{aligned}$$

This map f is a bijection, since each $I \in \mathcal{X}$ satisfies $I'' = I$ and thus $I' \in \mathcal{X}$. This bijection f is furthermore *sign-reversing*, meaning that $(-1)^{|f(I)|} = -(-1)^{|I|}$ for all $I \in \mathcal{X}$. We claim that this automatically guarantees

$$\begin{aligned}&(\text{the sum of the signs of all acceptable sets}) \\ &= (\text{the sum of the signs of all acceptable sets } \textbf{not} \text{ belonging to } \mathcal{X}).\end{aligned}$$

The reason for this equality is that in the sum of the signs of all acceptable sets, the contributions of the sets that belong to $\mathcal{X}$ (that is, of the acceptable sets that have acceptable partners) cancel each other out. This principle is worth generalizing and stating as a lemma:

Lemma 6.1.2 (Cancellation principle, take 1)**.** Let $\mathcal{A}$ be a finite set. Let $\mathcal{X}$ be a subset of $\mathcal{A}$.

For each $I \in \mathcal{A}$, let $\operatorname{sign} I$ be a real number (not necessarily 1 or -1). Let $f : \mathcal{X} \to \mathcal{X}$ be a bijection with the property that

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I \qquad \text{for all } I \in \mathcal{X}. \tag{177}$$

(Such a bijection f is called *sign-reversing*.) Then,

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

Note that we did **not** require that $f \circ f = \mathrm{id}$ in Lemma 6.1.2; we only required that f is a bijection. That said, most examples that I know do have $f \circ f = \mathrm{id}$.

Proof of Lemma 6.1.2. Intuitively, this is clear: The contributions of all $I \in \mathcal{X}$ to the sum $\sum_{I \in \mathcal{A}} \operatorname{sign} I$ cancel out, to the extent they are not already zero. However, rather than formalize this cancellation, let us give an even slicker argument:

We have

$$\begin{aligned} \sum_{I \in \mathcal{X}} \operatorname{sign} I &= \sum_{I \in \mathcal{X}} \underbrace{\operatorname{sign}(f(I))}_{\substack{= -\operatorname{sign} I \\ \text{(by (177))}}} \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } f(I) \text{ for } I \\ \text{in the sum, since } f : \mathcal{X} \to \mathcal{X} \text{ is a bijection} \end{array}\right) \\ &= \sum_{I \in \mathcal{X}} (-\operatorname{sign} I) = -\sum_{I \in \mathcal{X}} \operatorname{sign} I. \end{aligned}$$

Adding $\sum_{I \in \mathcal{X}} \operatorname{sign} I$ to both sides of this equality, we obtain $2 \cdot \sum_{I \in \mathcal{X}} \operatorname{sign} I = 0$. Hence, $\sum_{I \in \mathcal{X}} \operatorname{sign} I = 0$ (since any real number a satisfying $2a = 0$ must satisfy $a = 0$).

Now, $\mathcal{X} \subseteq \mathcal{A}$; hence, we can split the sum $\sum_{I \in \mathcal{A}} \operatorname{sign} I$ as follows:

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \underbrace{\sum_{I \in \mathcal{X}} \operatorname{sign} I}_{=0} + \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

This proves Lemma 6.1.2. □

In the proof of Proposition 6.1.1, we applied Lemma 6.1.2 to

$$\begin{aligned} \mathcal{A} &= \{\text{acceptable sets}\} \qquad \text{and} \\ \mathcal{X} &= \{\text{acceptable sets whose partner is acceptable}\} \qquad \text{and} \end{aligned}$$

$$\operatorname{sign} I = (-1)^{|I|}.$$

But there are many other situations in which Lemma 6.1.2 can be applied. For example, $\mathcal{A}$ can be some set of permutations, and $\operatorname{sign}\sigma$ can be the sign of σ (as in Definition 5.4.1).

Let us observe that Lemma 6.1.2 can be generalized. Indeed, in Lemma 6.1.2, we can replace "real number" by "element of any $\mathbb{Q}$-vector space" or even by "element of any additive abelian group with the property that $2a = 0$ implies $a = 0$". We cannot, however, remove this requirement entirely. Indeed, if all the signs $\operatorname{sign} I$ were the element $\overline{1}$ of $\mathbb{Z}/2$, then the sign-reversing condition (177) would hold automatically (since $\overline{1} = -\overline{1}$ in $\mathbb{Z}/2$), but the claim of Lemma 6.1.2 would not necessarily be true.

However, if we replace the word "bijection" by "involution with no fixed points", then Lemma 6.1.2 holds even without any requirements on the group:

Lemma 6.1.3 (Cancellation principle, take 2)**.** Let $\mathcal{A}$ be a finite set. Let $\mathcal{X}$ be a subset of $\mathcal{A}$.

For each $I \in \mathcal{A}$, let $\operatorname{sign} I$ be an element of some additive abelian group. Let $f : \mathcal{X} \to \mathcal{X}$ be an involution (i.e., a map satisfying $f \circ f = \operatorname{id}$) that has no fixed points. Assume that

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I \qquad \text{for all } I \in \mathcal{X}.$$

Then,

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

Proof. The idea is that all addends corresponding to the $I \in \mathcal{X}$ cancel out from the sum $\sum\limits_{I \in \mathcal{A}} \operatorname{sign} I$ (because they come in pairs of addends with opposite signs). See Section B.3 for a detailed proof. □

A more general version of Lemma 6.1.3 allows for f to have fixed points, as long as these fixed points have sign 0:

Lemma 6.1.4 (Cancellation principle, take 3)**.** Let $\mathcal{A}$ be a finite set. Let $\mathcal{X}$ be a subset of $\mathcal{A}$.

For each $I \in \mathcal{A}$, let $\operatorname{sign} I$ be an element of some additive abelian group. Let $f : \mathcal{X} \to \mathcal{X}$ be an involution (i.e., a map satisfying $f \circ f = \operatorname{id}$). Assume that

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I \qquad \text{for all } I \in \mathcal{X}.$$

Assume furthermore that

$$\operatorname{sign} I = 0 \qquad \text{for all } I \in \mathcal{X} \text{ satisfying } f(I) = I.$$

Then,

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

Proof. This is similar to Lemma 6.1.3, except that the addends corresponding to the $I \in \mathcal{X}$ satisfying $f(I) = I$ don't cancel (but are already zero and thus can be removed right away). See Section B.3 for a detailed proof. □

Let us try to use this idea in another setting. Recall the notion of q-binomial coefficients, and specifically their values (Definition 4.4.3 **(b)**).

Exercise 6.1.0.1. Let $n, k \in \mathbb{N}$. Simplify $\dbinom{n}{k}_{-1}$.

Example 6.1.5. Let us compute $\dbinom{4}{2}_{-1}$. Theorem 4.4.13 **(b)** yields

$$\binom{4}{2}_q = \frac{(1-q^4)(1-q^3)}{(1-q^2)(1-q^1)}.$$

We cannot substitute -1 for q in this formula directly, since both numerator and denominator would become 0 if we did. However, we can first simplify the fraction and then substitute -1 for q: We have

$$\binom{4}{2}_q = \frac{(1-q^4)(1-q^3)}{(1-q^2)(1-q^1)} = q^4 + q^3 + 2q^2 + q + 1,$$

so that (by substituting -1 for q) we obtain

$$\binom{4}{2}_{-1} = (-1)^4 + (-1)^3 + 2(-1)^2 + (-1) + 1 = 2.$$

Solution of Exercise 6.1.0.1 (sketched). Proposition 4.4.7 **(b)** yields

$$\binom{n}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n\};\\ |S|=k}} q^{\operatorname{sum} S - (1+2+\cdots+k)},$$

where $\operatorname{sum} S$ denotes the sum of the elements of a finite set S of integers. Substituting -1 for q in this equality, we find

$$\binom{n}{k}_{-1} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\};\\ |S|=k}} (-1)^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

Using the shorthand $[n]$ for the set $\{1, 2, \ldots, n\}$, we can rewrite this as

$$\binom{n}{k}_{-1} = \sum_{\substack{S \subseteq [n];\\ |S|=k}} (-1)^{\operatorname{sum} S - (1+2+\cdots+k)}. \qquad (178)$$

Let us analyze the sum on the right hand side using sign-reversing involutions. Thus, we set

$$\mathcal{A} := \{S \subseteq [n] \ \mid \ |S| = k\} = \{k\text{-element subsets of } [n]\}$$

and

$$\operatorname{sign} S := (-1)^{\operatorname{sum} S - (1+2+\cdots+k)} \qquad \text{for every } S \in \mathcal{A}.$$

Hence, (178) rewrites as

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A}} \operatorname{sign} S. \tag{179}$$

Now, we seek a reasonable subset $\mathcal{X} \subseteq \mathcal{A}$ and a sign-reversing bijection $f : \mathcal{X} \to \mathcal{X}$ in order to cancel addends in the sum $\sum\limits_{S \in \mathcal{A}} \operatorname{sign} S$.

To wit, let us try to construct f as a partial map first, and then (as an afterthought) define $\mathcal{X}$ to be the set of all $S \in \mathcal{A}$ for which $f(S)$ is defined.

Consider a k-element subset S of $[n]$. What is a way to transform S that leaves its size $|S| = k$ unchanged, but flips its sign (i.e., flips the parity of sum S) ? One thing we can do is *switching* 1 *with* 2. By this I mean the following operation:

- If $1 \in S$ and $2 \notin S$, then we replace 1 by 2 in S.
- Otherwise, if $2 \in S$ and $1 \notin S$, then we replace 2 by 1 in S.
- If none of 1 and 2 is in S, or if both are in S, then we leave S unchanged for now.

Thus, switching 1 with 2 means replacing S by

$$\operatorname{switch}_{1,2}(S) := \begin{cases} (S \setminus \{1\}) \cup \{2\}, & \text{if } 1 \in S \text{ and } 2 \notin S; \\ (S \setminus \{2\}) \cup \{1\}, & \text{if } 1 \notin S \text{ and } 2 \in S; \\ S, & \text{otherwise.} \end{cases}$$

For example,

$$\begin{aligned} \operatorname{switch}_{1,2}(\{1,3,5\}) &= \{2,3,5\}; \\ \operatorname{switch}_{1,2}(\{2,3,5\}) &= \{1,3,5\}; \\ \operatorname{switch}_{1,2}(\{1,2,5\}) &= \{1,2,5\}; \\ \operatorname{switch}_{1,2}(\{3,4,5\}) &= \{3,4,5\}. \end{aligned}$$

Notice that the definition of switching 1 with 2 can be restated in a somewhat simpler way using symmetric differences (see Subsection 3.2.1 for the definition of symmetric differences):

$$\operatorname{switch}_{1,2}(S) := \begin{cases} S \triangle \{1,2\}, & \text{if } |S \cap \{1,2\}| = 1; \\ S, & \text{otherwise.} \end{cases}$$

Indeed, the condition "$|S \cap \{1,2\}| = 1$" is equivalent to having either $(1 \in S \text{ and } 2 \notin S)$ or $(1 \notin S \text{ and } 2 \in S)$; and in this case, the symmetric difference $S \bigtriangleup \{1,2\}$ is precisely the set we need (i.e., the set $(S \setminus \{1\}) \cup \{2\}$ if we have $(1 \in S \text{ and } 2 \notin S)$, and the set $(S \setminus \{2\}) \cup \{1\}$ if we have $(1 \notin S \text{ and } 2 \in S)$).

This map $\operatorname{switch}_{1,2} : \mathcal{A} \to \mathcal{A}$ is certainly a bijection (and, in fact, an involution). It is not sign-reversing on the entire set $\mathcal{A}$; however, it has the property that the sign of $\operatorname{switch}_{1,2}(S)$ is opposite to the sign of S whenever we have $(1 \in S \text{ and } 2 \notin S)$ or $(1 \notin S \text{ and } 2 \in S)$ (because in these two cases, $\operatorname{sum} S$ either increases by 1 or decreases by 1, respectively). We can restate this property as follows: The sign of $\operatorname{switch}_{1,2}(S)$ is opposite to the sign of S whenever we have $|S \cap \{1,2\}| = 1$. Thus, we can use $\operatorname{switch}_{1,2}$ to cancel many addends from our sum $\sum\limits_{S \in \mathcal{A}} \operatorname{sign} S$. Still, many other addends (of different signs) remain, and the result is far from simple.

Thus, we need a "Plan B" if the map $\operatorname{switch}_{1,2}$ does not succeed. Assuming that $|S \cap \{1,2\}| \neq 1$ (that is, the set $S \in \mathcal{A}$ contains none or both of 1 and 2), we gain nothing by switching 1 with 2 in S, but maybe we get lucky switching 2 with 3 in S (which is defined in the same way as switching 1 with 2, but with the obvious changes)? If that, too, fails, we can try to switch 3 with 4. If that fails as well, we can try to switch 4 with 5, and so on, until we get to the end of the set $[n]$.

In other words, we try to define a bijection $f : \mathcal{A} \to \mathcal{A}$ as follows: For any $S \in \mathcal{A}$, we pick the **smallest** $i \in [n-1]$ such that $|S \cap \{i, i+1\}| = 1$ (in other words, the **smallest** $i \in [n-1]$ such that exactly one of the two elements i and $i+1$ belongs to S); and we switch i with $i+1$ in S (that is, we replace S by $S \bigtriangleup \{i, i+1\}$). This produces a new subset S' of $[n]$ that has the same size as S but has the opposite sign (actually, we have $\operatorname{sum} S' = \operatorname{sum} S \pm 1$), except for the two cases when $S = \varnothing$ and when $S = [n]$ (these are the cases where we cannot find any $i \in [n-1]$ such that $|S \cap \{i, i+1\}| = 1$). We set $f(S) := S \bigtriangleup \{i, i+1\}$.

Here are some examples (for $n = 4$ and $k = 2$):

$$\begin{aligned}
f(\{1,3\}) &= \{2,3\} && (\text{here, the smallest } i \text{ is } 1);\\
f(\{1,4\}) &= \{2,4\} && (\text{here, the smallest } i \text{ is } 1);\\
f(\{3,4\}) &= \{2,4\} && (\text{here, the smallest } i \text{ is } 2).
\end{aligned}$$

Alas, the last two of these examples show that f is not injective (as $f(\{1,4\}) = \{2,4\} = f(\{3,4\})$). Thus, f is not a bijection. The underlying problem is that the i that was picked in the construction of $f(S)$ is not uniquely recoverable from $f(S)$. Hence, our map f does not work for us – we cannot use it to cancel addends, since we cannot cancel (e.g.) a single 1 against multiple -1s.

How can we salvage this argument? We change our map f to "space" our switches apart. That is, we again start by trying to switch 1 with 2; if this fails, we jump straight to trying to switch 3 with 4; if this fails too, we jump further to trying to switch 5 with 6; and so on, until we either succeed at some switch or run out of pairs to switch. For the explicit description of f, this means that instead of picking the **smallest** $i \in [n-1]$ such that $|S \cap \{i, i+1\}| = 1$, we pick the **smallest odd** $i \in [n-1]$ such that $|S \cap \{i, i+1\}| = 1$; and then we set $f(S) := S \triangle \{i, i+1\}$ as before.

In other words, we define our new map $f : \mathcal{A} \to \mathcal{A}$ as follows: For any $S \in \mathcal{A}$, we set

$$f(S) := S \triangle \{i, i+1\},$$

where i is the **smallest odd** element of $[n-1]$ such that $|S \cap \{i, i+1\}| = 1$. If no such i exists, we just set $f(S) := S$. (We will soon see when this happens.)

Here are some examples (for $n = 8$ and $k = 3$):

$$\begin{aligned}
f(\{1,3,4\}) &= \{2,3,4\} && \text{(here, the smallest odd } i \text{ is } 1)\,; \\
f(\{2,4,5\}) &= \{3,4,5\} && \text{(here, the smallest odd } i \text{ is } 3)\,; \\
f(\{3,4,5\}) &= \{2,4,5\} && \text{(here, the smallest odd } i \text{ is } 3)\,; \\
f(\{5,6,7\}) &= \{5,6,8\} && \text{(here, the smallest odd } i \text{ is } 7)\,.
\end{aligned}$$

And here are two more examples (for $n = 8$ and $k = 4$):

$$\begin{aligned}
f(\{1,2,5,7\}) &= \{1,2,6,7\} && \text{(here, the smallest odd } i \text{ is } 5)\,; \\
f(\{1,2,5,6\}) &= \{1,2,5,6\} && \text{(here, there is no appropriate odd } i)\,.
\end{aligned}$$

Once again, it is clear that the set $f(S)$ has size k whenever S does. Hence, $f : \mathcal{A} \to \mathcal{A}$ is at least a well-defined map. This time, the map f is furthermore an involution (that is, $f \circ f = \operatorname{id}$). Here is a quick argument for this (details are left to the reader): Since we have "spaced" the switches apart, they don't interfere with each other. Thus, the i that gets chosen in the construction of $f(S)$ will again get chosen in the construction of $f(f(S))$ (since the elements of $f(S)$ that are smaller than this i will not have changed from S). Thus, the switch that happens in the construction of $f(f(S))$ undoes the switch made in the construction of $f(S)$, and as a result, the set $f(f(S))$ will be S again. This shows that $f \circ f = \operatorname{id}$.

Thus, f is an involution, hence a bijection. Moreover, $\operatorname{sign}(f(S)) = -\operatorname{sign} S$ holds whenever $f(S) \neq S$ (because $f(S) \neq S$ implies that $f(S) = S \triangle \{i, i+1\}$ for some i satisfying $|S \cap \{i, i+1\}| = 1$, and therefore $\operatorname{sum}(f(S)) = \operatorname{sum} S \pm 1$). Thus, we set

$$\mathcal{X} := \{S \in \mathcal{A} \mid f(S) \neq S\},$$

and we restrict f to a map $\mathcal{X} \to \mathcal{X}$ (this is well-defined, since it is easy to see from $f \circ f = \operatorname{id}$ that $f(S) \in \mathcal{X}$ for each $S \in \mathcal{X}$). Then, the map f becomes a sign-reversing bijection from $\mathcal{X}$ to $\mathcal{X}$. Hence, Lemma 6.1.2 yields

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

Renaming the index I as S, we can rewrite this equality as

$$\sum_{S \in \mathcal{A}} \operatorname{sign} S = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S.$$

Hence, (179) becomes

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A}} \operatorname{sign} S = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S. \tag{180}$$

Now, what is $\mathcal{A} \setminus \mathcal{X}$? In other words, what addends are left behind uncancelled?

In order to answer this question, we need to consider the case when n is even and the case when n is odd separately. We begin with the case when n is even.

A k-element subset S of $[n]$ belongs to $\mathcal{A} \setminus \mathcal{X}$ if and only if it satisfies $f(S) = S$. In other words, S belongs to $\mathcal{A} \setminus \mathcal{X}$ if and only if there exists no odd $i \in [n-1]$ such that $|S \cap \{i, i+1\}| = 1$ (because f has been defined in such a way that $f(S) = S$ in this case, while $f(S) = S \bigtriangleup \{i, i+1\} \neq S$ in the other case). In other words, S belongs to $\mathcal{A} \setminus \mathcal{X}$ if and only if for each odd $i \in [n-1]$, the size $|S \cap \{i, i+1\}|$ is either 0 or 2. This is equivalent to saying that if we break up the n elements $1, 2, \ldots, n$ into $n/2$ "blocks"

$$\{1,2\}, \quad \{3,4\}, \quad \{5,6\}, \quad \ldots, \quad \{n-1, n\}$$

(this can be done, since n is even), then the intersection of S with each block has size 0 or 2. In other words, this is saying that the set S consists of entire blocks (i.e., each block is either fully included in S or is disjoint from S). In other words, this is saying that the set S is a union (possibly empty) of blocks. We call a subset S of $[n]$ *blocky* if it satisfies this condition.[71] Thus, a k-element subset S of $[n]$ belongs to $\mathcal{A} \setminus \mathcal{X}$ if and only if it is blocky. In other words, $\mathcal{A} \setminus \mathcal{X}$ is the set of all blocky k-element subsets of $[n]$.

How many blocky k-element subsets does $[n]$ have, and what are their signs? Any blocky subset of $[n]$ has the form[72]

$$\{i_1, i_1 + 1\} \sqcup \{i_2, i_2 + 1\} \sqcup \cdots \sqcup \{i_p, i_p + 1\}$$

for some odd elements $i_1 < i_2 < \cdots < i_p$ of $[n-1]$. Thus, this subset has size $2p$, which entails that its size is even. Hence, if k is odd, there are no blocky k-element subsets of $[n]$ at all. In other words, if k is odd, then there are no $S \in \mathcal{A} \setminus \mathcal{X}$ (since $\mathcal{A} \setminus \mathcal{X}$ is the set of all blocky k-element subsets of $[n]$). Therefore, if k is odd, then the sum $\sum\limits_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S$ is empty, and thus (180) simplifies to

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = (\text{empty sum}) = 0. \tag{181}$$

Let us now consider the case when k is even. In this case, again, any blocky subset S of $[n]$ has the form

$$\{i_1, i_1 + 1\} \sqcup \{i_2, i_2 + 1\} \sqcup \cdots \sqcup \{i_p, i_p + 1\}$$

[71] For example, $\{3,4,5,6,9,10\}$ is a blocky subset of $[10]$, whereas $\{2,3,5,6\}$ is not (since it neither fully includes nor is disjoint from the block $\{1,2\}$).

[72] The symbol "$\sqcup$" means "disjoint union" (in our case, a union of disjoint sets).

for some odd elements $i_1 < i_2 < \cdots < i_p$ of $[n-1]$. Moreover, again, this subset has size $2p$. Thus, if S has size k, then we must have $2p = k$, so that $p = k/2$. Thus, any blocky k-element subset S of $[n]$ has the form

$$\{i_1, i_1+1\} \sqcup \{i_2, i_2+1\} \sqcup \cdots \sqcup \{i_{k/2}, i_{k/2}+1\}$$

for some odd elements $i_1 < i_2 < \cdots < i_{k/2}$ of $[n-1]$. Hence, there are $\dbinom{n/2}{k/2}$ such subsets S (since there are precisely $\dbinom{n/2}{k/2}$ choices for these odd elements $i_1 < i_2 < \cdots < i_{k/2}$ [73]). Moreover, any such subset S satisfies

$$\begin{aligned} \operatorname{sum} S &= \underbrace{i_1 + (i_1+1)}_{\equiv 1 \bmod 2} + \underbrace{i_2 + (i_2+1)}_{\equiv 1 \bmod 2} + \cdots + \underbrace{i_{k/2} + (i_{k/2}+1)}_{\equiv 1 \bmod 2} \\ &\equiv \underbrace{1 + 1 + \cdots + 1}_{k/2 \text{ times}} = k/2 \bmod 2 \end{aligned}$$

and therefore

$$\underbrace{\operatorname{sum} S}_{\equiv k/2 \bmod 2} - \underbrace{(1+2+\cdots+k)}_{=\dfrac{k(k+1)}{2}} \equiv k/2 - \frac{k(k+1)}{2} = -k^2/2 \equiv 0 \bmod 2$$

(since k is even, so that $-k^2/2$ is even), and

$$\operatorname{sign} S = (-1)^{\operatorname{sum} S - (1+2+\cdots+k)} = 1 \tag{182}$$

(since $\operatorname{sum} S - (1+2+\cdots+k) \equiv 0 \bmod 2$). Hence, the sum $\sum\limits_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S$ has $\dbinom{n/2}{k/2}$ addends (because $\mathcal{A} \setminus \mathcal{X}$ is the set of all blocky k-element subsets of $[n]$, and we have just shown that there are $\dbinom{n/2}{k/2}$ such subsets), and each of these addends is 1 (by (182)). Thus, this sum simplifies to

$$\sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{n/2}{k/2} \cdot 1 = \binom{n/2}{k/2}.$$

Hence, (180) becomes

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{n/2}{k/2}. \tag{183}$$

Thus, we have computed $\dbinom{n}{k}_{-1}$

[73] because the set $[n-1]$ has $n/2$ odd elements

- in the case when n is even and k is odd (obtaining (181)), and
- in the case when n is even and k is even (obtaining (183)).

It remains to handle the case when n is odd. This case is different in that the n elements $1, 2, \ldots, n$ are now subdivided into $(n+1)/2$ "blocks"

$$\{1,2\}, \quad \{3,4\}, \quad \{5,6\}, \quad \ldots, \quad \{n-2, n-1\}, \quad \{n\},$$

with the last of these blocks having size 1. As a consequence, this time, a blocky subset of $[n]$ can have odd size. Moreover, the parity of k determines whether a blocky k-element subset of $[n]$ will contain n:

- If k is even, then no blocky k-element subset of $[n]$ can contain n (because if it did, then it would have odd size, since all non-$\{n\}$ blocks have even size).
- If k is odd, then every blocky k-element subset of $[n]$ must contain n (because if it didn't, then it would have even size, since all non-$\{n\}$ blocks have even size).

Thus, when classifying the blocky k-element subsets of $[n]$, we can either dismiss n immediately (if k is even) or take n for granted (if k is odd); in either case, the problem gets reduced to classifying the blocky k-element or $(k-1)$-element subsets of $[n-1]$, which we already know how to do (since $n-1$ is even). The result is that the # of blocky k-element subsets of $[n]$ (in the case when n is odd) is

$$\begin{cases} \dbinom{(n-1)/2}{k/2}, & \text{if } k \text{ is even;} \\ \dbinom{(n-1)/2}{(k-1)/2}, & \text{if } k \text{ is odd} \end{cases} = \dbinom{(n-1)/2}{\lfloor k/2 \rfloor},$$

and their signs are always 1. Hence, we obtain

$$\sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{(n-1)/2}{\lfloor k/2 \rfloor} \cdot 1 = \binom{(n-1)/2}{\lfloor k/2 \rfloor}.$$

Thus, (180) becomes

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{(n-1)/2}{\lfloor k/2 \rfloor}. \qquad (184)$$

This is the answer to our exercise in the case when n is odd.

Returning to the general case, we can now combine the formulas (183), (181) and (184) into a single equality that holds in all cases:

$$\binom{n}{k}_{-1} = \begin{cases} 0, & \text{if } n \text{ is even and } k \text{ is odd;} \\ \dbinom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor}, & \text{otherwise.} \end{cases} \tag{185}$$

□

This formula (185) can be generalized. Indeed, here is a generalization of the number -1:

Definition 6.1.6. Let K be a field. Let d be a positive integer.

(a) A *d-th root of unity* in K means an element ω of K satisfying $\omega^d = 1$. In other words, a d-th root of unity in K means an element of K whose d-th power is 1.

(b) A *primitive d-th root of unity* in K means an element ω of K satisfying

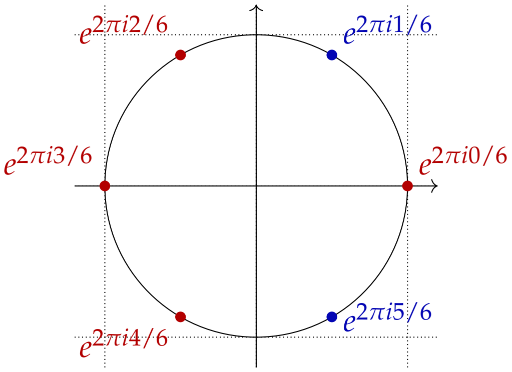
$$\omega^d = 1$$

but

$$\omega^i \neq 1 \qquad \text{for each } i \in \{1, 2, \ldots, d-1\}.$$

In other words, a primitive d-th root of unity in K means an element of the multiplicative group $K^\times$ whose order is d.

For $K = \mathbb{C}$, the d-th roots of unity are the d complex numbers $e^{2\pi i 0/d}, e^{2\pi i 1/d}, e^{2\pi i 2/d}, \ldots, e^{2\pi i (d-1)/d}$ (which are the vertices of a regular d-gon inscribed in the unit circle, with one vertex at 1), whereas the primitive d-th roots of unity are the numbers $e^{2\pi i g/d}$ for all $g \in [d]$ satisfying $\gcd(g, d) = 1$. In particular, the 2-nd roots of unity in $\mathbb{C}$ are 1 and -1, and the only primitive 2-nd root of unity is -1. The following picture shows the six 6-th roots of unity in $\mathbb{C}$ (with the two primitive 6-th roots colored blue, and the remaining four roots colored red):



.

We can now generalize (185) by replacing -1 by primitive roots of unity:

Theorem 6.1.7 (q-Lucas theorem)**.** Let K be a field. Let d be a positive integer. Let ω be a primitive d-th root of unity in K. Let $n, k \in \mathbb{N}$. Let q and u be the quotients obtained when dividing n and k by d with remainder, and let r and v be the respective remainders. Then,

$$\binom{n}{k}_{\omega} = \binom{q}{u} \cdot \binom{r}{v}_{\omega}. \tag{186}$$

Note that the equality (186) contains two ω-binomial coefficients and one regular binomial coefficient.

It is not hard to check that (185) is the particular case of Theorem 6.1.7 for $d = 2$ and $\omega = -1$. Indeed, the only possible remainders of an integer upon division by 2 are 0 and 1, and the ω-binomial coefficients $\binom{r}{v}_{\omega}$ for $r, v \in \{0, 1\}$ are

$$\binom{0}{0}_{\omega} = 1, \qquad \binom{0}{1}_{\omega} = 0, \qquad \binom{1}{0}_{\omega} = 1, \qquad \binom{1}{1}_{\omega} = 1.$$

Theorem 6.1.7 can be proved using a generalization of sign-reversing involutions to d-cycles instead of pairs[74]. A more algebraic proof – using "noncommutative generating functions" – is given in Exercise A.5.1.3.

6.2. The principles of inclusion and exclusion

We have so far been applying the "yoga" of sign-reversing involutions directly to alternating sums. However, some of its essence can also be crystallized into useful theorems. Most famous among such theorems are the *principles of inclusion and exclusion* (also known as *Sylvester sieve theorems* or *Poincaré's theorems*)[75].

6.2.1. The size version

The simplest such principle answers the following question: Assume that you have a finite set U, and some subsets $A_1, A_2, \ldots, A_n$ of U. Assume that, for each selection of some of these subsets, you know how many elements of U belong to all selected sets at the same time. (For instance, you know how many elements of U belong to A_2, A_3 and A_5 at the same time.) Does this help you

[74] In our proofs so far, we have been using the equality $1 + (-1) = 0$ to cancel addends in alternating sums. This equality can be generalized as follows: If ω is a primitive d-th root of unity for $d > 1$, then $1 + \omega + \omega^2 + \cdots + \omega^{d-1} = 0$. This equality can be used to cancel addends in sums that involve powers of ω. The *discrete Fourier transform* (see, e.g., [OlvSha18, §5.6]) and the *roots-of-unity filter* (see, e.g., [Knuth1, §1.2.9.D]) are applications of this idea.

[75] People typically use the singular forms ("principle" and "theorem" rather than "principles" and "theorems"), but often mean different things.

count the elements of U that belong to **none** of the n subsets (i.e., that don't belong to $A_1 \cup A_2 \cup \cdots \cup A_n$) ?

The answer is "yes", and there is an explicit formula for this count:

> **Theorem 6.2.1** (size version of the PIE)**.** Let $n \in \mathbb{N}$. Let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Then,
>
> $$\begin{aligned}&(\text{\# of } u \in U \text{ that satisfy } u \notin A_i \text{ for all } i \in [n]) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I).\end{aligned}$$

Some explanations are in order:

- Here and in the following, we are using the notation $[n]$ for the set $\{1, 2, \ldots, n\}$, as defined in Definition 5.1.2.
- The summation sign " $\sum\limits_{I \subseteq [n]}$ " means a sum over all subsets I of $[n]$. More generally, if S is a given set, then the summation sign " $\sum\limits_{I \subseteq S}$ " shall always mean a sum over all subsets I of S.
- The shorthand "*PIE*" in the name of Theorem 6.2.1 is short for "*Principle of Inclusion and Exclusion*".

In one form or another, Theorem 6.2.1 appears in almost any text on combinatorics (e.g., in [Sagan19, Theorem 2.1.1], in [Loehr11, §4.11], in [Strick20, Theorem 5.3], in [19fco, Theorem 2.9.7], or – in almost the same form as above – in [20f, Theorem 7.8.6]). Most commonly, its claim is stated in the shorter (if less transparent) form

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|,$$

where $\bigcap\limits_{i \in I} A_i$ denotes the set $\{u \in U \mid u \in A_i \text{ for all } i \in I\}$ whenever I is a subset of $[n]$ [76]. This form is indeed equivalent to the claim of Theorem 6.2.1,

[76] This notation should be taken with a grain of salt. When I is a **nonempty** subset of $[n]$, it is indeed true that the set $\bigcap\limits_{i \in I} A_i$ as we just defined it (i.e., the set $\{u \in U \mid u \in A_i \text{ for all } i \in I\}$) is the intersection of the sets A_i over all $i \in I$ (that is, if $I = \{i_1, i_2, \ldots, i_k\}$, then $\bigcap\limits_{i \in I} A_i = A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}$). However, if I is the **empty** set, then the literal intersection of the sets A_i over all $i \in I$ is not well-defined (indeed, by common sense, such an intersection should contain every object whatsoever; but there is no set that does this), whereas the set we just called $\bigcap\limits_{i \in I} A_i$ is simply the set U. This is still justified, since we should think of the sets A_i not as arbitrary sets but rather as subsets of U (so that any intersections are to be taken within U). This, incidentally, is the reason for the choice of the letter "U": We think of U as the "universe" in which our objects live.

since we have

$$\begin{aligned}
&\left|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)\right| \\
&= (\text{\# of } u \in U \text{ that satisfy } u \notin A_1 \cup A_2 \cup \cdots \cup A_n) \\
&= (\text{\# of } u \in U \text{ that satisfy } u \notin A_i \text{ for all } i \in [n])
\end{aligned}$$

and since (for each subset I of $[n]$) we have

$$\left|\bigcap_{i\in I} A_i\right| = (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I)$$

(by the definition of $\bigcap\limits_{i\in I} A_i$ that we just gave).

Rather than prove Theorem 6.2.1 directly, we shall soon derive it from more general results (in order to avoid duplicating arguments). First, however, let us give an interpretation that makes Theorem 6.2.1 a little bit more intuitive, and sketch four applications (more can be found in textbooks – e.g., [Sagan19, §2.1], [Stanle11, Chapter 2], [Wildon19, Chapter 3], [AndFen04, Chapter 6], [19fco, §2.9]).

> **“Rule-breaking” interpretation of Theorem 6.2.1.** Assume that we are given a finite set U, and we are given n rules (labelled $1, 2, \ldots, n$) that each element of U may or may not satisfy. (For instance, one element of U might satisfy all of these rules; another might satisfy none; yet another might satisfy rules 1 and 3 only. A rule can be something like “thou shalt be divisible by 5” (if the elements of U are numbers) or “thou shalt be a nonempty set” (if the elements of U are sets).)
>
> Assume that, for each $I \subseteq [n]$, we know how many elements $u \in U$ satisfy all rules in I (but may or may not satisfy the remaining rules). For example, this means that we know how many elements $u \in U$ satisfy rules $2, 3, 5$ (simultaneously). Then, we can compute the # of elements $u \in U$ that violate all n rules $1, 2, \ldots, n$ by the following formula:
>
> $$\begin{aligned}
> &(\text{\# of elements } u \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\
> &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of elements } u \in U \text{ that satisfy all rules in } I).
> \end{aligned}$$
>
> Indeed, this formula is precisely what we obtain if we apply Theorem 6.2.1 to the n subsets $A_1, A_2, \ldots, A_n$ defined by setting
>
> $$A_i := \{u \in U \mid u \text{ satisfies rule } i\} \qquad \text{for each } i \in [n].$$

Thus, if you have a counting problem that can be restated as "count things that violate a bunch of rules", then you can apply Theorem 6.2.1 (in the interpretation we just gave) to "turn the problem positive", i.e., to make it about counting rule-followers instead of rule-violators. If the "positive" problem is easier, then this is a useful technique. We will now witness this on four examples.

6.2.2. Examples

Example 1. Let $n, m \in \mathbb{N}$. Let us compute the # of surjective maps from $[m]$ to $[n]$. (We will outline the argument here; details can be found in [20f, §7.8.2] or [19fco, §2.9.4].)

What are surjective maps? They are maps that take each element of the target set as a value. Thus, in particular, a map $f : [m] \to [n]$ is surjective if and only if it takes each $i \in [n]$ as a value.

Hence, if we impose n rules $1, 2, \ldots, n$ on a map $f : [m] \to [n]$, where rule i says "thou shalt not take i as a value", then the surjective maps $f : [m] \to [n]$ are precisely the maps $f : [m] \to [n]$ that violate all n rules. Hence,

$$\begin{aligned}
&(\text{\# of surjective maps } f : [m] \to [n]) \\
&= (\text{\# of maps } f : [m] \to [n] \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of maps } f : [m] \to [n] \text{ that satisfy all rules in } I)
\end{aligned}$$

(by the "rule-breaking" interpretation of Theorem 6.2.1).

Now, fix some subset I of $[n]$. What is the # of maps $f : [m] \to [n]$ that satisfy all rules in I ? A map $f : [m] \to [n]$ satisfies all rules in I if and only if it takes none of the $i \in I$ as a value, i.e., if all its values belong to $[n] \setminus I$. Thus, the maps $f : [m] \to [n]$ that satisfy all rules in I are nothing but the maps from $[m]$ to $[n] \setminus I$. The # of such maps is therefore $|[n] \setminus I|^{|[m]|} = (n - |I|)^m$ (since $I \subseteq [n]$ entails $|[n] \setminus I| = |[n]| - |I| = n - |I|$, and since $|[m]| = m$).

Forget that we fixed I. We thus have shown that for each subset I of $[n]$, we have

$$\begin{aligned}
&(\text{\# of maps } f : [m] \to [n] \text{ that satisfy all rules in } I) \\
&= (n - |I|)^m .
\end{aligned} \tag{187}$$

Substituting this into the above computation, we find

$$\begin{aligned}
&(\text{\# of surjective maps } f : [m] \to [n]) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\text{\# of maps } f : [m] \to [n] \text{ that satisfy all rules in } I)}_{\substack{=(n-|I|)^m \\ \text{(by (187))}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)^m = \sum_{k=0}^{n} \sum_{\substack{I \subseteq [n]; \\ |I|=k}} \underbrace{(-1)^{|I|} (n-|I|)^m}_{\substack{=(-1)^k (n-k)^m \\ \text{(since } |I|=k)}} \\
&\qquad \left(\begin{array}{c}\text{here, we have split the sum according to} \\ \text{the value of } |I|\end{array}\right) \\
&= \sum_{k=0}^{n} \underbrace{\sum_{\substack{I \subseteq [n]; \\ |I|=k}} (-1)^k (n-k)^m}_{\substack{=\binom{n}{k}(-1)^k(n-k)^m \\ \text{(since this is a sum of } \binom{n}{k} \\ \text{many equal addends)}}} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)^m \\
&= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m .
\end{aligned}$$

Thus, we have proved the following theorem:

Theorem 6.2.2. Let $n, m \in \mathbb{N}$. Then,

$$(\text{\# of surjective maps } f : [m] \to [n]) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m .$$

This is the simplest expression for this number. It has no product formula (unlike the # of injective maps $f : [m] \to [n]$, which is $n(n-1)(n-2)\cdots(n-m+1)$).

Before we move on to the next example, let us draw a few consequences from Theorem 6.2.2:

Corollary 6.2.3. Let $n \in \mathbb{N}$. Then:

(a) We have $\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m = 0$ for any $m \in \mathbb{N}$ satisfying $m < n$.

(b) We have $\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n = n!$.

(c) We have $\sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \geq 0$ for each $m \in \mathbb{N}$.

(d) We have $n! \mid \sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^m$ for each $m \in \mathbb{N}$.

Proof of Corollary 6.2.3 (sketched). **(a)** Let $m \in \mathbb{N}$ satisfy $m < n$. Theorem 6.2.2 shows that the sum $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^m$ equals the # of surjective maps $f : [m] \to [n]$. However, there are no such maps (by the Pigeonhole Principle for Surjections)[77]; hence, this # is 0. Therefore, the sum is 0. In other words, $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^m = 0$. This proves Corollary 6.2.3 **(a)**.

(b) Theorem 6.2.2 (applied to $m = n$) shows that the sum $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^n$ equals the # of surjective maps $f : [n] \to [n]$. However, these maps are precisely the permutations of $[n]$ (by the Pigeonhole Principle for Surjections)[78]; therefore, this # is $n!$. Therefore, this sum is $n!$. This proves Corollary 6.2.3 **(b)**.

(c) Let $m \in \mathbb{N}$. Theorem 6.2.2 shows that the sum $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^m$ equals the # of surjective maps $f : [m] \to [n]$. Hence, this sum is ≥ 0. This proves Corollary 6.2.3 **(c)**.

(d) Let $m \in \mathbb{N}$. Theorem 6.2.2 shows that the sum $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^m$ equals the # of surjective maps $f : [m] \to [n]$. Let

$$U := \{\text{surjective maps } f : [m] \to [n]\}.$$

Thus, this sum equals $|U|$. Hence, it remains to show that $n! \mid |U|$.

The argument that follows will use the language of group actions (although it could be restated combinatorially)[79]. If $\sigma \in S_n$ is any permutation and $f : [m] \to [n]$ is a surjective map, then the composition $\sigma \circ f : [m] \to [n]$ is again a surjective map. In other words, any $\sigma \in S_n$ and $f \in U$ satisfy $\sigma \circ f \in U$. Hence, the symmetric group S_n acts on the set U by the rule[80]

$$\sigma \cdot f = \sigma \circ f \qquad \text{for all } \sigma \in S_n \text{ and } f \in U.$$

[77] Indeed, the Pigeonhole Principle for Surjections shows that there are no surjective maps from a smaller set to a larger set. Thus, in particular, there are no surjective maps from $[m]$ to $[n]$ (since $m < n$).

[78] Indeed, the Pigeonhole Principle for Surjections shows that any surjective map between two finite sets of the same size is bijective. Thus, any surjective map $f : [n] \to [n]$ is bijective, and hence is a permutation of $[n]$. The converse is true as well (i.e., any permutation of $[n]$ is a surjective map $f : [n] \to [n]$). Thus, the surjective maps $f : [n] \to [n]$ are precisely the permutations of $[n]$.

[79] For a refresher on group actions, see (e.g.) [Quinla21, §3.2] or [Loehr11, §9.11–§9.15] or [Artin10, §6.7–§6.9] or [Armstr19, Fall 2018, Weeks 8–10] or [Aigner07, §6.1]. When G is a group, we use the word "*G-set*" to mean a set on which G acts.

[80] This is called "acting by post-composition" (since $\sigma \circ f$ is obtained from f by composing with σ "after" f).

(This is a well-defined group action, since composition of maps is associative.)

This turns U into an S_n-set. It is not hard to see that this action of S_n on U is free – i.e., the stabilizer of each $f \in U$ is the trivial subgroup $\{\text{id}\}$ of S_n [81]. Thus, the Orbit-Stabilizer Theorem (see, e.g., [Quinla21, Theorem 3.2.5]) shows that each orbit of this action has size

$$[S_n : \{\text{id}\}] = \underbrace{|S_n|}_{=n!} / \underbrace{|\{\text{id}\}|}_{=1} = n!/1 = n!.$$

However, the orbits of this action form a partition of U (since each element of U belongs to exactly one orbit). Thus, we have

$$|U| = (\text{the sum of the sizes of the orbits}) = (\# \text{ of orbits}) \cdot n!$$

(since each orbit has size $n!$). This entails $n! \mid |U|$, which is exactly what we wanted to show. This proves Corollary 6.2.3 **(d)**. □

We note that parts **(a)** and **(b)** of Corollary 6.2.3 can also be proved algebraically (see, e.g., [20f, Exercise 5.4.2 **(d)**] for an algebraic generalization of Corollary 6.2.3 **(a)**); but this is harder for Corollary 6.2.3 **(d)** and (to my knowledge) impossible for Corollary 6.2.3 **(c)**.

Example 2. (See [19fco, §2.9.5] for details.) We will use the following definition:

Definition 6.2.4. A *derangement* of a set X means a permutation of X that has no fixed points.

Now, let $n \in \mathbb{N}$. How many derangements does $[n]$ have?

Before answering this question, we establish notations and a few examples.

Let D_n be the # of derangements of $[n]$. For example:

- The identity permutation $\text{id} \in S_0$ is a derangement, since it has no fixed points (since $[0] = \varnothing$ has no elements to begin with). Thus, $D_0 = 1$.
- The identity permutation $\text{id} \in S_1$ is **not** a derangement, since $\text{id}(1) = 1$. Thus, $D_1 = 0$.

[81] *Proof.* Let $f \in U$. We must prove that the stabilizer of f is $\{\text{id}\}$.

Let σ belong to the stabilizer of f. Thus, $\sigma \circ f = f$. Now, let $j \in [n]$. Recall that $f \in U$; hence, f is surjective. Thus, there exists some $i \in [m]$ such that $j = f(i)$. Consider this i. Now, from $j = f(i)$, we obtain $\sigma(j) = \sigma(f(i)) = \underbrace{(\sigma \circ f)}_{=f}(i) = f(i) = j$. Now, forget that we fixed j. We thus have shown that $\sigma(j) = j$ for each $j \in [n]$. In other words, $\sigma = \text{id}$.

Forget that we fixed σ. We thus have shown that any σ in the stabilizer of f satisfies $\sigma = \text{id}$. In other words, the stabilizer of f is a subset of $\{\text{id}\}$. Therefore, the stabilizer of f must be $\{\text{id}\}$ (since id is clearly in the stabilizer of f).

- In the symmetric group S_2, the identity is **not** a derangement, but the transposition $s_1 = t_{1,2}$ is one. Thus, $D_2 = 1$.
- In the symmetric group S_3, the derangements are the 3-cycles $\operatorname{cyc}_{1,2,3}$ and $\operatorname{cyc}_{1,3,2}$. Thus, $D_3 = 2$.

Here is a table of early values of D_n:

n	0	1	2	3	4	5	6	7	8	9	10
D_n	1	0	1	2	9	44	265	1854	14 833	133 496	1 334 961

.

Note: The number D_n is also called the *subfactorial* of n and is sometimes denoted by $!n$. Be careful with that notation: what is 2!2 ?

Let us now try to compute D_n in general. Fix $n \in \mathbb{N}$, and set $U := S_n = \{\text{permutations of } [n]\}$. We impose n rules $1, 2, \ldots, n$ on a permutation $\sigma \in U$, with rule i being "thou shalt leave the element i fixed" (in other words, rule i requires a permutation $\sigma \in U$ to satisfy $\sigma(i) = i$). Now,

$$\begin{aligned} D_n &= (\text{\# of derangements of } [n]) \\ &= (\text{\# of permutations } u \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of permutations } u \in U \text{ that satisfy all rules in } I) \end{aligned}$$

(by the "rule-breaking" interpretation of Theorem 6.2.1).

Now, let I be a subset of $[n]$. What is the # of permutations $u \in U$ that satisfy all rules in I ? These permutations are the permutations of $[n]$ that leave each $i \in I$ fixed (but can do whatever they want with the remaining elements of $[n]$). Clearly, there are $(n - |I|)!$ such permutations, since they are essentially the permutations of the $(n - |I|)$-element set $[n] \setminus I$ (with the elements of I tacked on as fixed points). (See [19fco, Corollary 2.9.16] for the technical details of this intuitively obvious argument.)

Forget that we fixed I. We thus have shown that

$$\begin{aligned} &(\text{\# of permutations } u \in U \text{ that satisfy all rules in } I) \\ &= (n - |I|)! \end{aligned} \tag{188}$$

for any subset I of $[n]$.

Thus, the above computation becomes

$$\begin{aligned}
D_n &= \sum_{I\subseteq[n]} (-1)^{|I|} \underbrace{(\text{\# of permutations } u \in U \text{ that satisfy all rules in } I)}_{\substack{=(n-|I|)! \\ \text{(by (188))}}} \\
&= \underbrace{\sum_{I\subseteq[n]}}_{=\sum\limits_{k=0}^{n} \sum\limits_{\substack{I\subseteq[n];\\ |I|=k}}} (-1)^{|I|} (n-|I|)! = \sum_{k=0}^{n} \sum_{\substack{I\subseteq[n];\\ |I|=k}} \underbrace{(-1)^{|I|} (n-|I|)!}_{\substack{=(-1)^k(n-k)! \\ \text{(since } |I|=k)}} \\
&= \sum_{k=0}^{n} \underbrace{\sum_{\substack{I\subseteq[n];\\ |I|=k}} (-1)^k (n-k)!}_{=\binom{n}{k}(-1)^k(n-k)!} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)! \\
&= \sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k} (n-k)!}_{\substack{=\dfrac{n!}{k!} \\ \text{(by (2))}}} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.
\end{aligned}$$

Let us summarize our results as a theorem:

Theorem 6.2.5. Let $n \in \mathbb{N}$. Then, the # of derangements of $[n]$ is

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Remark 6.2.6. The sum on the right hand side is a partial sum of the well-known infinite series $\sum\limits_{k=0}^{\infty} \dfrac{(-1)^k}{k!} = e^{-1}$ (where $e = 2.718\ldots$ is Euler's number). This is quite helpful in approximating D_n; indeed, it is easy to see (using some simple estimates) that

$$D_n = \operatorname{round} \frac{n!}{e} \qquad \text{for each } n > 0,$$

where $\operatorname{round} x$ means the result of rounding a real number x to the nearest integer (fortunately, since e is irrational, we never get a tie).

See Exercise A.5.2.2 and [Wildon19, Chapter 1] for more about derangements.

Example 3. Like many other things in these lectures, the following elementary number-theoretical result is due to Euler:

Theorem 6.2.7. Let c be a positive integer with prime factorization $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, where $p_1, p_2, \ldots, p_n$ are distinct primes, and where $a_1, a_2, \ldots, a_n$ are positive integers. Then,

$$(\text{\# of all } u \in [c] \text{ that are coprime to } c) = c \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{n} \left(p_i^{a_i} - p_i^{a_i - 1}\right).$$

Note that the # of all $u \in [c]$ that are coprime to c is usually denoted by $\phi(c)$ in number theory, and the map $\phi : \{1, 2, 3, \ldots\} \to \mathbb{N}$ that sends each c to $\phi(c)$ is called *Euler's totient function*.

Theorem 6.2.7 can be proved in many ways (and a proof can be found in almost any text on elementary number theory). Probably the most transparent proof relies on the PIE:

Proof of Theorem 6.2.7 (sketched). (See [19fco, proof of Theorem 2.9.19] for the details of this argument.) Let $U = [c]$. A number $u \in U$ is coprime to c if and only if it is not divisible by any of the prime factors $p_1, p_2, \ldots, p_n$ of c. Again, this means that u breaks all n rules $1, 2, \ldots, n$, where rule i says "thou shalt be divisible by p_i". Thus, by the "rule-breaking" interpretation of Theorem 6.2.1, we obtain

$$\begin{aligned}
&(\text{\# of all } u \in [c] \text{ that are coprime to } c) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\text{\# of all } u \in [c] \text{ that are divisible by all } p_i \text{ with } i \in I)}_{\substack{= \frac{c}{\prod_{i \in I} p_i} \\ \text{(this is not hard to prove)}}} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \frac{c}{\prod_{i \in I} p_i} = c \cdot \underbrace{\sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \frac{1}{p_i}}_{\substack{= \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) \\ \text{(an easy consequence of (150))}}} \\
&= \underbrace{c}_{\substack{= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ = \prod_{i=1}^{n} p_i^{a_i}}} \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \left(\prod_{i=1}^{n} p_i^{a_i}\right) \cdot \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) \\
&= \prod_{i=1}^{n} \underbrace{\left(p_i^{a_i} \left(1 - \frac{1}{p_i}\right)\right)}_{= p_i^{a_i} - p_i^{a_i - 1}} = \prod_{i=1}^{n} \left(p_i^{a_i} - p_i^{a_i - 1}\right).
\end{aligned}$$

This proves Theorem 6.2.7. □

Example 4. (This one is taken from [Sagan19, Theorem 2.3.3].) Recall Theorem 4.1.13, which states that each $n \in \mathbb{N}$ satisfies

$$p_{\text{odd}}(n) = p_{\text{dist}}(n),$$

where

$$\begin{aligned} p_{\text{odd}}(n) &:= (\text{\# of partitions of } n \text{ into odd parts}) \qquad \text{and} \\ p_{\text{dist}}(n) &:= (\text{\# of partitions of } n \text{ into distinct parts}). \end{aligned}$$

We have already proved this twice, but let us prove it again.

Third proof of Theorem 4.1.13 (sketched). Let $n \in \mathbb{N}$. We set $U := \{\text{partitions of } n\}$.

In this proof, the word "partition" will always mean "partition of n". Thus, a partition cannot contain any of the entries $n+1, n+2, n+3, \ldots$ (because any of these entries would cause the partition to have size $> n$).

We want to frame the partitions of n into distinct parts as rule-breakers. We observe that

$$\begin{aligned} &\{\text{partitions of } n \text{ into distinct parts}\} \\ &= \{\text{partitions that contain none of the entries } 1, 2, 3, \ldots \text{ twice}\} \\ &\qquad \left(\begin{array}{c}\text{here and in the following, the word "twice"} \\ \text{means "at least twice"}\end{array}\right) \\ &= \{\text{partitions that contain none of the entries } 1, 2, \ldots, n \text{ twice}\} \end{aligned}$$

(since a partition cannot contain any of the entries $n+1, n+2, n+3, \ldots$). In other words, the partitions of n into distinct parts are precisely the partitions that break all rules $1, 2, \ldots, n$, where rule i says "thou shalt contain the entry i twice"[82].

Thus, applying the PIE (specifically, the "rule-breaking" interpretation of Theorem 6.2.1), we obtain

$$\begin{aligned} &p_{\text{dist}}(n) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that satisfy all rules in } I) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that contain each of the entries } i \in I \text{ twice}). \end{aligned} \tag{189}$$

[82] Once again, "twice" means "at least twice".

We can play the same game with $p_{\text{odd}}(n)$. This time, rule i says "thou shalt contain the entry $2i$". Thus, again applying the PIE, we obtain

$$p_{\text{odd}}(n) = \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that contain the entry } 2i \text{ for each } i \in I). \tag{190}$$

Now, comparing these two equalities, we see that in order to prove that $p_{\text{dist}}(n) = p_{\text{odd}}(n)$, it will suffice to show that

$$\begin{aligned} & (\text{\# of partitions that contain each of the entries } i \in I \text{ twice}) \\ & = (\text{\# of partitions that contain the entry } 2i \text{ for each } i \in I) \end{aligned}$$

for any subset I of $[n]$.

So let I be a subset of $[n]$. We are looking for a bijection

$$\begin{aligned} & \text{from } \{\text{partitions that contain each of the entries } i \in I \text{ twice}\} \\ & \text{to } \{\text{partitions that contain the entry } 2i \text{ for each } i \in I\}. \end{aligned}$$

Such a bijection can be obtained as follows: For each $i \in I$ (from highest to lowest[83]), we remove two copies of i from the partition, and insert a $2i$ into the partition in their stead. For example, if $I = \{2, 4, 5\}$ and $n = 33$, then our bijection sends the partition

$$(5, 5, 4, 4, 3, 3, 2, 2, 2, 2, 1) \text{ to } (10, 8, 4, 3, 3, 2, 2, 1).$$

(Note that the 4 in the resulting partition is not one of the original two 4s, but rather a new 4 that was inserted when we removed two copies of 2. On the other hand, the two 2s in the resulting partition are inherited from the original partition, because (unlike the bijection A in our Second proof of Theorem 4.1.13 above) our bijection only removes two copies of each $i \in I$.)

It is easy to see that this purported bijection really is a bijection[84]. Thus, we have found our bijection. The bijection principle therefore yields

$$\begin{aligned} & (\text{\# of partitions that contain each of the entries } i \in I \text{ twice}) \\ & = (\text{\# of partitions that contain the entry } 2i \text{ for each } i \in I). \end{aligned}$$

We have proved this equality for all $I \subseteq [n]$. Hence, the right hand sides of the equalities (189) and (190) are equal. Thus, their left hand sides are equal as well. In other words, $p_{\text{dist}}(n) = p_{\text{odd}}(n)$. This proves Theorem 4.1.13 again. □

[83] Actually, a bit of thought reveals that the order in which we go through the $i \in I$ does not affect the result; this becomes particularly clear if we identify each partition with the multiset of its entries. Thus, me saying "from highest to lowest" is unnecessary.

[84] Its inverse, of course, does what you would expect: For each $i \in I$, we remove a $2i$ from the partition, and insert two copies of i in its stead.

Remark 6.2.8. It is worth contrasting the above four examples (in which we applied the PIE to solve a counting problem, obtaining an alternating sum as a result) with our arguments in Section 6.1 (in which we computed alternating sums using sign-reversing involutions). Sign-reversing involutions help turn alternating sums into combinatorial problems, while the PIE moves us in the opposite direction. The two techniques are thus, in some way, inverse to each other. This will become less mysterious once we prove the PIE itself using a sign-reversing involution. The PIE can also be used backwards, to turn an alternating sign into a counting problem, which is how we proved Corollary 6.2.3 above.

6.2.3. The weighted version

The main rule of algebra is to never turn down nature's gifts. The PIE (in the shape of Theorem 6.2.1) can be generalized with zero effort, so let us do it ([20f, Theorem 7.8.9]):

Theorem 6.2.9 (weighted version of the PIE). Let $n \in \mathbb{N}$, and let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Let A be any additive abelian group (such as $\mathbb{R}$, or any vector space, or any ring). Let $w : U \to A$ be any map (i.e., let $w(u)$ be an element of A for each $u \in U$). Then,

$$\sum_{\substack{u \in U; \\ u \notin A_i \text{ for all } i \in [n]}} w(u) = \sum_{I \subseteq [n]} (-1)^{|I|} \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in I}} w(u). \qquad (191)$$

We can think of each value $w(u)$ in Theorem 6.2.9 as a kind of "weight" of the respective element u. Thus, the left hand side of the equality (191) is the total weight of all "rule-breaking" $u \in U$ (that is, of all $u \in U$ that satisfy ($u \notin A_i$ for all $i \in [n]$)), whereas the inner sum $\sum\limits_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in I}} w(u)$ on the right hand side is the total weight of all $u \in U$ that satisfy ($u \in A_i$ for all $i \in I$). This is why we call Theorem 6.2.9 the *weighted version of the PIE* (or just the *weighted PIE*).

Theorem 6.2.1 can be obtained from Theorem 6.2.9 by taking w to be constantly 1 (that is, by setting $w(u) = 1$ for each $u \in U$). Indeed, a sum of a bunch of 1s equals the # of 1s being summed, so that sums generalize cardinalities.

With Theorem 6.2.9, we can take any of our above four examples from Subsection 6.2.2, and introduce weights into them – i.e., instead of asking for a number, we sum certain "weights". Little question (cf. the homework): What do you get?

But we have no time for this now. Another generalization is calling!

6.2.4. Boolean Möbius inversion

This generalization (we will soon see why it is a generalization) is our third "Principle of Inclusion and Exclusion", but is probably best referred to as the *Boolean Möbius inversion formula* (or the *Möbius inversion formula for the Boolean lattice*):

Theorem 6.2.10 (Boolean Möbius inversion)**.** Let S be a finite set. Let A be any additive abelian group.

For each subset I of S, let a_I and b_I be two elements of A.

Assume that

$$b_I = \sum_{J \subseteq I} a_J \qquad \text{for all } I \subseteq S. \tag{192}$$

Then, we also have

$$a_I = \sum_{J \subseteq I} (-1)^{|I \setminus J|} b_J \qquad \text{for all } I \subseteq S. \tag{193}$$

Example 6.2.11. Let $S = [2] = \{1,2\}$. Then, the assumptions of Theorem 6.2.10 state that

$$\begin{aligned} b_\varnothing &= a_\varnothing; \\ b_{\{1\}} &= a_\varnothing + a_{\{1\}}; \\ b_{\{2\}} &= a_\varnothing + a_{\{2\}}; \\ b_{\{1,2\}} &= a_\varnothing + a_{\{1\}} + a_{\{2\}} + a_{\{1,2\}}. \end{aligned}$$

The claim of Theorem 6.2.10 then states that

$$\begin{aligned} a_\varnothing &= b_\varnothing; \\ a_{\{1\}} &= -b_\varnothing + b_{\{1\}}; \\ a_{\{2\}} &= -b_\varnothing + b_{\{2\}}; \\ a_{\{1,2\}} &= b_\varnothing - b_{\{1\}} - b_{\{2\}} + b_{\{1,2\}}. \end{aligned}$$

These four equalities can be verified easily. For instance, let us check the last of them:

$$\begin{aligned} &\underbrace{b_\varnothing}_{=a_\varnothing} - \underbrace{b_{\{1\}}}_{=a_\varnothing + a_{\{1\}}} - \underbrace{b_{\{2\}}}_{=a_\varnothing + a_{\{2\}}} + \underbrace{b_{\{1,2\}}}_{=a_\varnothing + a_{\{1\}} + a_{\{2\}} + a_{\{1,2\}}} \\ &= a_\varnothing - \left(a_\varnothing + a_{\{1\}}\right) - \left(a_\varnothing + a_{\{2\}}\right) + \left(a_\varnothing + a_{\{1\}} + a_{\{2\}} + a_{\{1,2\}}\right) \\ &= a_{\{1,2\}}. \end{aligned}$$

Before we prove Theorem 6.2.10, let us show that the weighted PIE (Theorem 6.2.9) is a particular case of it:

Proof of Theorem 6.2.9 using Theorem 6.2.10. Let $S = [n]$. We note that the map

$$\begin{aligned} \{\text{subsets of } S\} &\to \{\text{subsets of } S\}, \\ J &\mapsto S \setminus J \end{aligned}$$

is a bijection. (Indeed, this map is an involution, since each subset J of S satisfies $S \setminus (S \setminus J) = J$.)

For each $u \in U$, define a subset $\operatorname{Viol} u$ of S by

$$\operatorname{Viol} u := \{i \in S \ \mid \ u \notin A_i\}.$$

(In terms of the "rule-breaking" interpretation, $\operatorname{Viol} u$ is the set of all rules that u violates.) Now, for each subset I of $[n]$, we set

$$a_I := \sum_{\substack{u \in U; \\ \operatorname{Viol} u = I}} w(u) \qquad \text{and} \qquad b_I := \sum_{\substack{u \in U; \\ \operatorname{Viol} u \subseteq I}} w(u).$$

Then, for each subset I of S, we have

$$\begin{aligned} b_I &= \sum_{\substack{u \in U; \\ \operatorname{Viol} u \subseteq I}} w(u) = \sum_{J \subseteq I} \underbrace{\sum_{\substack{u \in U; \\ \operatorname{Viol} u = J}} w(u)}_{\substack{= a_J \\ \text{(by the definition of } a_J)}} \qquad \left(\begin{array}{c} \text{here, we have split} \\ \text{the sum according to} \\ \text{the value of } \operatorname{Viol} u \end{array}\right) \\ &= \sum_{J \subseteq I} a_J. \end{aligned}$$

Thus, we can apply Theorem 6.2.10. This gives us

$$a_I = \sum_{J \subseteq I} (-1)^{|I \setminus J|} b_J \qquad \text{for all } I \subseteq S. \tag{194}$$

However, if J is any subset of S, then the definition of b_J yields

$$b_J = \sum_{\substack{u \in U; \\ \operatorname{Viol} u \subseteq J}} w(u) = \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in S \setminus J}} w(u) \tag{195}$$

(because the elements $u \in U$ that satisfy $\operatorname{Viol} u \subseteq J$ are precisely the elements $u \in U$ that satisfy $(u \in A_i \text{ for all } i \in S \setminus J)$ [85]).

[85] *Proof.* Let $u \in U$. We must prove that the condition "$\operatorname{Viol} u \subseteq J$" is equivalent to "$u \in A_i$ for all $i \in S \setminus J$".

We have $\operatorname{Viol} u = \{i \in S \mid u \notin A_i\}$ (by the definition of $\operatorname{Viol} u$). Hence, we have the

Now, applying (194) to $I = S$, we obtain

$$\begin{aligned} a_S &= \sum_{J \subseteq S} (-1)^{|S \setminus J|} b_J = \sum_{J \subseteq S} (-1)^{|S \setminus J|} \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in S \setminus J}} w(u) \qquad \text{(by (195))} \\ &= \sum_{I \subseteq S} (-1)^{|I|} \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in I}} w(u) \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } I \text{ for } S \setminus J \text{ in the sum, since} \\ \text{the map } \{\text{subsets of } S\} \to \{\text{subsets of } S\},\ J \mapsto S \setminus J \\ \text{is a bijection} \end{array} \right) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in I}} w(u) \qquad (\text{since } S = [n]) . \end{aligned}$$

On the other hand, the definition of a_S yields

$$a_S = \sum_{\substack{u \in U; \\ \operatorname{Viol} u = S}} w(u) = \sum_{\substack{u \in U; \\ u \notin A_i \text{ for all } i \in [n]}} w(u)$$

(since the elements $u \in U$ that satisfy $\operatorname{Viol} u = S$ are precisely the elements $u \in U$ that satisfy $(u \notin A_i \text{ for all } i \in [n])$ [86]).

Comparing these two equalities, we obtain

$$\sum_{\substack{u \in U; \\ u \notin A_i \text{ for all } i \in [n]}} w(u) = \sum_{I \subseteq [n]} (-1)^{|I|} \sum_{\substack{u \in U; \\ u \in A_i \text{ for all } i \in I}} w(u) .$$

following chain of equivalences:

$$\begin{aligned} (\operatorname{Viol} u \subseteq J) &\iff (\{i \in S \mid u \notin A_i\} \subseteq J) \\ &\iff (\text{each } i \in S \text{ satisfying } u \notin A_i \text{ belongs to } J) \\ &\iff (\text{each } i \in S \text{ that does not belong to } J \text{ must satisfy } u \in A_i) \\ &\qquad\qquad (\text{by contraposition}) \\ &\iff (\text{each } i \in S \setminus J \text{ must satisfy } u \in A_i) \\ &\iff (u \in A_i \text{ for all } i \in S \setminus J) . \end{aligned}$$

Hence, the condition "$\operatorname{Viol} u \subseteq J$" is equivalent to "$u \in A_i$ for all $i \in S \setminus J$".

[86] *Proof.* Let $u \in U$. We must prove that the condition "$\operatorname{Viol} u = S$" is equivalent to "$u \notin A_i$ for all $i \in [n]$".

We have $\operatorname{Viol} u = \{i \in S \mid u \notin A_i\}$ (by the definition of $\operatorname{Viol} u$). Hence, we have the following chain of equivalences:

$$\begin{aligned} (\operatorname{Viol} u = S) &\iff (\{i \in S \mid u \notin A_i\} = S) \\ &\iff (\text{each } i \in S \text{ satisfies } u \notin A_i) \\ &\iff (u \notin A_i \text{ for all } i \in S) \\ &\iff (u \notin A_i \text{ for all } i \in [n]) \qquad (\text{since } S = [n]) . \end{aligned}$$

Hence, the condition "$\operatorname{Viol} u = S$" is equivalent to "$u \notin A_i$ for all $i \in [n]$".

Thus, Theorem 6.2.9 has been proved, assuming Theorem 6.2.10. □

It remains to prove the latter:

Proof of Theorem 6.2.10. Fix a subset Q of S. We shall prove that

$$a_Q = \sum_{I \subseteq Q} (-1)^{|Q \setminus I|} b_I.$$

We begin by rewriting the right hand side:

$$\sum_{I \subseteq Q} (-1)^{|Q \setminus I|} \underbrace{b_I}_{\substack{= \sum_{J \subseteq I} a_J \\ \text{(by (192))}}} = \sum_{I \subseteq Q} (-1)^{|Q \setminus I|} \underbrace{\sum_{J \subseteq I} a_J}_{= \sum_{P \subseteq I} a_P} = \sum_{I \subseteq Q} (-1)^{|Q \setminus I|} \sum_{P \subseteq I} a_P$$
$$= \sum_{I \subseteq Q} \sum_{P \subseteq I} (-1)^{|Q \setminus I|} a_P. \tag{196}$$

The two summation signs "$\sum_{I \subseteq Q} \sum_{P \subseteq I}$" on the right hand side of this equality result in a sum over all pairs (I, P) of subsets of Q satisfying $P \subseteq I \subseteq Q$. The same result can be obtained by the two summation signs "$\sum_{P \subseteq Q} \sum_{\substack{I \subseteq Q; \\ P \subseteq I}}$" (indeed, the only difference between "$\sum_{I \subseteq Q} \sum_{P \subseteq I}$" and "$\sum_{P \subseteq Q} \sum_{\substack{I \subseteq Q; \\ P \subseteq I}}$" is the order in which the two subsets I and P are chosen). Thus, we can replace "$\sum_{I \subseteq Q} \sum_{P \subseteq I}$" by "$\sum_{P \subseteq Q} \sum_{\substack{I \subseteq Q; \\ P \subseteq I}}$" on the right hand side of (196). Hence, (196) rewrites as follows:

$$\sum_{I \subseteq Q} (-1)^{|Q \setminus I|} b_I = \sum_{P \subseteq Q} \sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q \setminus I|} a_P$$
$$= \sum_{P \subseteq Q} \left(\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q \setminus I|} \right) a_P. \tag{197}$$

We want to prove that this equals a_Q. Since the a_P's are arbitrary elements of an abelian group, the only way this can possibly be achieved is by showing that the sum on the right hand side simplifies to a_Q **formally** – i.e., that the coefficient $\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q \setminus I|}$ in front of a_P is 0 whenever $P \neq Q$, and is 1 whenever $P = Q$. Thus, we now set out to prove this. Using Definition A.1.5, we can restate this goal as follows: We want to prove that every subset P of Q satisfies

$$\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q \setminus I|} = [P = Q]. \tag{198}$$

We shall prove this soon (in Lemma 6.2.12 **(b)** below). For now, let us explain how the proof of Theorem 6.2.10 can be completed if (198) is known to be true. Indeed, (197) becomes

$$\begin{aligned}
\sum_{I\subseteq Q}(-1)^{|Q\setminus I|}b_I &= \sum_{P\subseteq Q}\underbrace{\left(\sum_{\substack{I\subseteq Q;\\ P\subseteq I}}(-1)^{|Q\setminus I|}\right)}_{\substack{=[P=Q]\\ \text{(by (198))}}}a_P = \sum_{P\subseteq Q}[P=Q]\,a_P \\
&= \underbrace{[Q=Q]}_{\substack{=1\\ \text{(since } Q=Q)}}a_Q + \sum_{\substack{P\subseteq Q;\\ P\neq Q}}\underbrace{[P=Q]}_{\substack{=0\\ \text{(since } P\neq Q)}}a_P \\
&\qquad \left(\begin{array}{c}\text{here, we have split off the addend for } P=Q\\ \text{from the sum (since } Q\subseteq Q)\end{array}\right) \\
&= a_Q + \underbrace{\sum_{\substack{P\subseteq Q;\\ P\neq Q}}0a_P}_{=0} = a_Q.
\end{aligned}$$

In other words, $a_Q = \sum\limits_{I\subseteq Q}(-1)^{|Q\setminus I|}b_I$.

Forget that we fixed Q. We thus have shown that

$$a_Q = \sum_{I\subseteq Q}(-1)^{|Q\setminus I|}b_I \qquad \text{for all } Q\subseteq S.$$

Renaming the indices Q and I as I and J in this statement, we obtain the following:

$$a_I = \sum_{J\subseteq I}(-1)^{|I\setminus J|}b_J \qquad \text{for all } I\subseteq S.$$

Thus, Theorem 6.2.10 is proved (assuming that (198) is known to be true). □

It now remains to prove (198). We shall do this as part of the following lemma:

Lemma 6.2.12. Let Q be a finite set. Let P be a subset of Q. Then:

(a) We have

$$\sum_{\substack{I\subseteq Q;\\ P\subseteq I}}(-1)^{|I|} = (-1)^{|P|}[P=Q]. \tag{199}$$

(b) We have

$$\sum_{\substack{I\subseteq Q;\\ P\subseteq I}}(-1)^{|Q\setminus I|} = [P=Q]. \tag{200}$$

As promised, Lemma 6.2.12 **(b)** (once proved) will yield (198) and thus will complete our above proof of Theorem 6.2.10 (and, with it, the proofs of Theorem 6.2.9 and Theorem 6.2.1).

Proof of Lemma 6.2.12. **(a)** There are many ways to prove this (in particular, a simple one using the binomial theorem – do you see it?); but staying true to the spirit of this chapter, we pick one using a sign-reversing involution. (A variant of this proof can be found in [19fco, solution to Exercise 2.9.1].[87])

We must prove the equality (199). If $P = Q$, then this equality is easily seen to hold[88]. Hence, for the rest of this proof, we WLOG assume that $P \neq Q$. Thus, $[P = Q] = 0$.

Now, P is a **proper** subset of Q (since P is a subset of Q and satisfies $P \neq Q$). Hence, there exists some $q \in Q$ such that $q \notin P$. Fix such a q.

Let

$$\mathcal{A} := \{I \subseteq Q \ \mid \ P \subseteq I\},$$

and let

$$\operatorname{sign} I := (-1)^{|I|} \qquad \text{for each } I \in \mathcal{A}.$$

Then,

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{\substack{I \subseteq Q;\\ P \subseteq I}} (-1)^{|I|}. \tag{202}$$

We shall now construct an involution $f : \mathcal{A} \to \mathcal{A}$ on the set $\mathcal{A}$; this will allow us to apply Lemma 6.1.3 (to $\mathcal{X} = \mathcal{A}$), and easily conclude that $\sum\limits_{I \in \mathcal{A}} \operatorname{sign} I = 0$ (see below for the details).

Indeed, if I is a subset of Q, then $I \cup \{q\}$ is also a subset of Q (because $q \in Q$). Thus, if $I \in \mathcal{A}$, then $I \cup \{q\} \in \mathcal{A}$ (because $P \subseteq I$ implies $P \subseteq I \subseteq I \cup \{q\}$).

[87] Our sets Q and P are called S and T in [19fco, solution to Exercise 2.9.1].

[88] *Proof.* Assume that $P = Q$. Then, the only subset I of Q that satisfies $P \subseteq I$ is the set Q itself (since any such subset I has to satisfy both $Q = P \subseteq I$ and $I \subseteq Q$, which in combination entail $I = Q$). Thus, the sum $\sum\limits_{\substack{I \subseteq Q;\\ P \subseteq I}} (-1)^{|I|}$ has only one addend, namely the addend for $I = Q$. Consequently, this sum simplifies as follows:

$$\sum_{\substack{I \subseteq Q;\\ P \subseteq I}} (-1)^{|I|} = (-1)^{|Q|}. \tag{201}$$

On the other hand, from $P = Q$, we obtain

$$(-1)^{|P|} [P = Q] = (-1)^{|Q|} \underbrace{[Q = Q]}_{\substack{=1\\ (\text{since } Q = Q)}} = (-1)^{|Q|}.$$

Comparing this with (201), we obtain $\sum\limits_{\substack{I \subseteq Q;\\ P \subseteq I}} (-1)^{|I|} = (-1)^{|P|} [P = Q]$. Thus, we have shown that (199) holds under the assumption that $P = Q$.

On the other hand, if I is a set satisfying $P \subseteq I$, then the set $I \setminus \{q\}$ also satisfies $P \subseteq I \setminus \{q\}$ (since $q \notin P$). Thus, if $I \in \mathcal{A}$, then $I \setminus \{q\} \in \mathcal{A}$ (since $I \subseteq Q$ implies $I \setminus \{q\} \subseteq I \subseteq Q$).

Now, we define a map $f : \mathcal{A} \to \mathcal{A}$ by setting[89]

$$f(I) := I \triangle \{q\} = \begin{cases} I \setminus \{q\}, & \text{if } q \in I; \\ I \cup \{q\}, & \text{if } q \notin I \end{cases} \qquad \text{for each } I \in \mathcal{A}.$$

This map f is well-defined, because (as we have just shown in the two paragraphs above) every $I \in \mathcal{A}$ satisfies $I \cup \{q\} \in \mathcal{A}$ and $I \setminus \{q\} \in \mathcal{A}$. Moreover, this map f is an involution[90]. This involution f has no fixed points (because if $I \in \mathcal{A}$, then $f(I) = I \triangle \{q\} \neq I$). Furthermore, if $I \in \mathcal{A}$, then the set $f(I) = I \triangle \{q\}$ differs from I in exactly one element (namely, q), and thus satisfies $|f(I)| = |I| \pm 1$, so that

$$(-1)^{|f(I)|} = -(-1)^{|I|},$$

or, equivalently,

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I$$

(since the definition of $\operatorname{sign} I$ yields $\operatorname{sign} I = (-1)^{|I|}$, and similarly $\operatorname{sign}(f(I)) = (-1)^{|f(I)|}$). Thus, Lemma 6.1.3 (applied to $\mathcal{X} = \mathcal{A}$) shows that

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{A}} \operatorname{sign} I = (\text{empty sum}) \qquad (\text{since } \mathcal{A} \setminus \mathcal{A} = \varnothing)$$
$$= 0.$$

Comparing this with (202), we find

$$\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|I|} = 0 = (-1)^{|P|} [P = Q] \qquad \left(\text{since } (-1)^{|P|} \underbrace{[P = Q]}_{=0} = 0\right).$$

Thus, (199) is proved. This proves Lemma 6.2.12 **(a)**.

(b) If I is any subset of Q, then $|Q \setminus I| = |Q| - |I| \equiv |Q| + |I| \bmod 2$ and thus

$$(-1)^{|Q \setminus I|} = (-1)^{|Q| + |I|} = (-1)^{|Q|} (-1)^{|I|}.$$

Hence,

$$\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} \underbrace{(-1)^{|Q \setminus I|}}_{=(-1)^{|Q|}(-1)^{|I|}} = \sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q|} (-1)^{|I|} = (-1)^{|Q|} \underbrace{\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|I|}}_{\substack{=(-1)^{|P|}[P=Q] \\ (\text{by Lemma 6.2.12 } \textbf{(a)})}}$$
$$= (-1)^{|Q|} (-1)^{|P|} [P = Q].$$

[89] Here, the notation $X \triangle Y$ means the symmetric difference $(X \cup Y) \setminus (X \cap Y)$ of two sets X and Y (as in Subsection 3.2.1).

[90] Indeed, the map f merely removes q from a set I if q is contained in I, and inserts it into I otherwise; but this is clearly an operation that undoes itself when performed a second time.

However, it is easy to see that

$$(-1)^{|Q|} (-1)^{|P|} [P = Q] = [P = Q] \tag{203}$$

[91]. Thus,

$$\sum_{\substack{I \subseteq Q; \\ P \subseteq I}} (-1)^{|Q \setminus I|} = (-1)^{|Q|} (-1)^{|P|} [P = Q] = [P = Q] .$$

This proves Lemma 6.2.12 **(b)**. □

As said above, this completes the proofs of Theorem 6.2.10, of Theorem 6.2.9 and of Theorem 6.2.1.

While Theorem 6.2.10 has played the part of the ultimate generalization to us, it can be generalized further. Indeed, it is merely a particular case of *Möbius inversion for arbitrary posets* (see, e.g., [Stanle11, Proposition 3.7.1] or [Martin21, Theorem 2.3.1] or [Sagan19, Theorem 5.5.5] or [Sam21, Theorem 6.10] or [Wagner20, Theorem 14.6.4]).

6.3. More subtractive methods

TODO: Here should be a proof of the # of all-even d-tuples, and more generally of d-tuples in which each number appears with a given parity. For now, see [18f-hw4s, solution to Exercise 7] for this.

6.4. Determinants

Determinants were introduced by Leibniz in the 17th century, and quickly became one of the most powerful tools in mathematics. They remained so until the early 20th century. There is a 5-volume book by Thomas Muir [Muir30] that merely summarizes the results found on determinants... until 1920.

Most of these old results are still interesting and nontrivial. The relative role of determinants in mathematics has declined mainly because other parts of mathematics have "caught up" and have produced easier ways to many of the places that were previously only accessible through the study of determinants.

As with anything else, we will just present some of the most basic results and methods related to determinants. For more, see [MuiMet60], [Zeilbe85], [Grinbe15, Chapter 6], [Prasol94, Chapter I] and various other sources. A good introduction to the most fundamental properties is [Strick13].

[91] *Proof of (203):* If $P \neq Q$, then the equality (203) boils down to $(-1)^{|Q|} (-1)^{|P|} \cdot 0 = 0$ (since $P \neq Q$ entails $[P = Q] = 0$), which is obviously true. Hence, (203) is proved if $P \neq Q$. Thus, for the rest of this proof, we WLOG assume that $P = Q$. Hence, $(-1)^{|Q|} (-1)^{|P|} = (-1)^{|Q|} (-1)^{|Q|} = (-1)^{|Q|+|Q|} = 1$ (since $|Q| + |Q| = 2|Q|$ is even). Therefore, $\underbrace{(-1)^{|Q|} (-1)^{|P|}}_{=1} [P = Q] = [P = Q]$. This proves (203).

Convention 6.4.1. For the rest of Section 6.4, we fix a commutative ring K. In most examples, K will be $\mathbb{Z}$ or $\mathbb{Q}$ or a polynomial ring.

Convention 6.4.2. Let $n, m \in \mathbb{N}$.

(a) If A is an $n \times m$-matrix, then $A_{i,j}$ shall mean the (i, j)-th entry of A, that is, the entry of A in row i and column j.

(b) If $a_{i,j}$ is an element of K for each $i \in [n]$ and each $j \in [m]$, then

$$\left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m}$$

shall denote the $n \times m$-matrix whose (i, j)-th entry is $a_{i,j}$ for all $i \in [n]$ and $j \in [m]$. Explicitly:

$$\left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}.$$

Note that the letters "i" and "j" in the notation "$\left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq m}$" are not carved in stone. We could just as well use any other letters instead, and write $\left(a_{x,y}\right)_{1\leq x\leq n,\ 1\leq y\leq m}$ or (somewhat misleadingly, but technically correctly) $\left(a_{j,i}\right)_{1\leq j\leq n,\ 1\leq i\leq m}$ for the exact same matrix. (However, $\left(a_{j,i}\right)_{1\leq i\leq m,\ 1\leq j\leq n}$ is a different matrix. Whichever index is mentioned first in the subscript after the closing parenthesis is used to index rows; the other index is used to index columns.)

(c) We let $K^{n\times m}$ denote the set of all $n \times m$-matrices with entries in K. This is a K-module. If $n = m$, this is also a K-algebra.

(d) Let $A \in K^{n\times m}$ be an $n \times m$-matrix. The *transpose* A^T of A is defined to be the $m \times n$-matrix whose entries are given by

$$\left(A^T\right)_{i,j} = A_{j,i} \qquad \text{for all } i \in [m] \text{ and } j \in [n].$$

6.4.1. Definition

There are several ways to define the determinant of a square matrix. The following is the most direct one:

Definition 6.4.3. Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be an $n \times n$-matrix. The *determinant* $\det A$ of A is defined to be the element

$$\sum_{\sigma\in S_n} (-1)^\sigma \underbrace{A_{1,\sigma(1)}A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}}_{=\prod_{i=1}^{n} A_{i,\sigma(i)}}$$

of K. Here, as before:

- we let S_n denote the n-th symmetric group (i.e., the group of permutations of $[n] = \{1, 2, \ldots, n\}$);
- we let $(-1)^\sigma$ denote the sign of the permutation σ (as defined in Definition 5.4.1).

Example 6.4.4. For $n = 2$, we have

$$\begin{aligned}\det A &= \sum_{\sigma \in S_2} (-1)^\sigma A_{1,\sigma(1)} A_{2,\sigma(2)} \\ &= \underbrace{(-1)^{\operatorname{id}}}_{=1} \underbrace{A_{1,\operatorname{id}(1)}}_{=A_{1,1}} \underbrace{A_{2,\operatorname{id}(2)}}_{=A_{2,2}} + \underbrace{(-1)^{s_1}}_{=-1} \underbrace{A_{1,s_1(1)}}_{=A_{1,2}} \underbrace{A_{2,s_1(2)}}_{=A_{2,1}} \\ &\qquad \left(\begin{array}{c}\text{since the two elements of } S_2 \text{ are the identity} \\ \text{map } \operatorname{id} \text{ and the simple transposition } s_1 = t_{1,2}\end{array}\right) \\ &= A_{1,1}A_{2,2} - A_{1,2}A_{2,1}.\end{aligned}$$

Using less cumbersome notations, we can rewrite this as follows: For any $a, b, a', b' \in K$, we have

$$\det \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} = ab' - ba'.$$

Similarly, for $n = 3$, we obtain

$$\det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = ab'c'' - ac'b'' - ba'c'' + bc'a'' + ca'b'' - cb'a''.$$

(The six addends on the right hand side here correspond to the six permutations in S_3, which in one-line notation are 123, 132, 213, 231, 312, and 321, respectively.)

Similarly, for $n = 1$, we obtain that the determinant of the 1×1-matrix $\begin{pmatrix} a \end{pmatrix}$ is

$$\det \begin{pmatrix} a \end{pmatrix} = a.$$

Here, the "$\begin{pmatrix} a \end{pmatrix}$" on the left hand side is a 1×1-matrix.

Finally, for $n = 0$, we obtain that the determinant of the 0×0-matrix $()$ (this is an empty matrix, with no rows and no columns) is

$$\det () = (\text{empty product}) = 1.$$

Some (particularly, older) texts use the notation $|A|$ instead of $\det A$ for the determinant of the matrix A.

The above definition of the determinant is purely combinatorial: it is an alternating sum over the n-th symmetric group S_n. Typically, when computing determinants, this definition is not in itself very useful (e.g., because S_n gets rather large when n is large). However, in some cases, it suffices. Here are a few examples:

> **Example 6.4.5.** Let $a, b, c, d, e, \ldots, p$ be 16 elements of K. Prove that
>
> $$\det \begin{pmatrix} a & b & c & d & e \\ p & 0 & 0 & 0 & f \\ o & 0 & 0 & 0 & g \\ n & 0 & 0 & 0 & h \\ m & l & k & j & i \end{pmatrix} = 0.$$
>
> (The "o" is a letter "oh", not a zero. Not that it matters much...)

Proof of Example 6.4.5. Let A be the 5×5-matrix whose determinant we are trying to identify as 0; thus, $A_{1,1} = a$ and $A_{1,2} = b$ and $A_{3,2} = 0$ and so on. Notice that

$$A_{i,j} = 0 \qquad \text{whenever } i, j \in \{2,3,4\} \tag{204}$$

(since A has a "hollow core", i.e., a 3×3-square consisting entirely of zeroes in its middle). We must prove that $\det A = 0$.

Our definition of $\det A$ yields

$$\det A = \sum_{\sigma \in S_5} (-1)^{\sigma} \prod_{i=1}^{5} A_{i,\sigma(i)}. \tag{205}$$

Now, I claim that each of the addends in the sum on the right hand side is 0. In other words, I claim that $\prod\limits_{i=1}^{5} A_{i,\sigma(i)} = 0$ for each $\sigma \in S_5$.

To prove this, fix $\sigma \in S_5$. The three numbers $\sigma(2), \sigma(3), \sigma(4)$ are three distinct elements of $[5]$ (distinct because σ is injective), so they cannot all belong to the 2-element set $\{1,5\}$ (since there are no three distinct elements in a 2-element set). Hence, at least one of them must belong to the complement $\{2,3,4\}$ of this set. In other words, there exists some $i \in \{2,3,4\}$ such that $\sigma(i) \in \{2,3,4\}$. This i must then satisfy $A_{i,\sigma(i)} = 0$ (by (204), applied to $j = \sigma(i)$). Thus, we have shown that there exists some $i \in \{2,3,4\}$ such that $A_{i,\sigma(i)} = 0$.

This shows that at least one factor of the product $\prod\limits_{i=1}^{5} A_{i,\sigma(i)}$ is 0. Thus, the entire product is 0.

Forget that we fixed σ. We thus have proved that $\prod\limits_{i=1}^{5} A_{i,\sigma(i)} = 0$ for each

$\sigma \in S_5$. Hence,

$$\det A = \sum_{\sigma \in S_5} (-1)^{\sigma} \underbrace{\prod_{i=1}^{5} A_{i,\sigma(i)}}_{=0} = 0,$$

and thus Example 6.4.5 is proved.

[We note that there are various alternative proofs, e.g., using Laplace expansion. Also, if K is a field, you can argue that $\det A = 0$ using rank arguments. See [Grinbe15, Exercise 6.47 **(a)**] for a generalization of Example 6.4.5.] □

Example 6.4.6. Let $n \in \mathbb{N}$, and let $x_1, x_2, \ldots, x_n \in K$ and $y_1, y_2, \ldots, y_n \in K$. Compute

$$\det\left(\left(x_i y_j\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = \det \begin{pmatrix} x_1 y_1 & x_1 y_2 & \cdots & x_1 y_n \\ x_2 y_1 & x_2 y_2 & \cdots & x_2 y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & x_n y_2 & \cdots & x_n y_n \end{pmatrix}.$$

Let us experiment with small n's:

$$\begin{aligned} \det () &= 1; \\ \det \begin{pmatrix} x_1 y_1 \end{pmatrix} &= x_1 y_1; \\ \det \begin{pmatrix} x_1 y_1 & x_1 y_2 \\ x_2 y_1 & x_2 y_2 \end{pmatrix} &= 0; \\ \det \begin{pmatrix} x_1 y_1 & x_1 y_2 & x_1 y_3 \\ x_2 y_1 & x_2 y_2 & x_2 y_3 \\ x_3 y_1 & x_3 y_2 & x_3 y_3 \end{pmatrix} &= 0. \end{aligned}$$

This makes us suspect the following:

Proposition 6.4.7. Let $n \in \mathbb{N}$ be such that $n \geq 2$. Let $x_1, x_2, \ldots, x_n \in K$ and $y_1, y_2, \ldots, y_n \in K$. Then,

$$\det\left(\left(x_i y_j\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = 0.$$

Proof of Proposition 6.4.7 (sketched). The definition of the determinant yields

$$\begin{aligned}
\det\left(\left(x_i y_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) &= \sum_{\sigma\in S_n} (-1)^\sigma \underbrace{\left(x_1 y_{\sigma(1)}\right)\left(x_2 y_{\sigma(2)}\right)\cdots\left(x_n y_{\sigma(n)}\right)}_{=\left(x_1x_2\cdots x_n\right)\left(y_{\sigma(1)}y_{\sigma(2)}\cdots y_{\sigma(n)}\right)} \\
&= \sum_{\sigma\in S_n} (-1)^\sigma \left(x_1x_2\cdots x_n\right) \underbrace{\left(y_{\sigma(1)}y_{\sigma(2)}\cdots y_{\sigma(n)}\right)}_{\substack{=y_1y_2\cdots y_n \\ \text{(since } \sigma \text{ is a bijection } [n]\to[n])}} \\
&= \sum_{\sigma\in S_n} (-1)^\sigma \left(x_1x_2\cdots x_n\right)\left(y_1y_2\cdots y_n\right) \\
&= \left(x_1x_2\cdots x_n\right)\left(y_1y_2\cdots y_n\right) \underbrace{\sum_{\sigma\in S_n} (-1)^\sigma}_{\substack{=0 \\ \text{(by (169))}}} = 0.
\end{aligned}$$

Thus, Proposition 6.4.7 is proved. □

As a consequence of Proposition 6.4.7 (applied to $x_i = x$ and $y_j = 1$), we see that

$$\underbrace{\det\begin{pmatrix} x & x & \cdots & x \\ x & x & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x \end{pmatrix}}_{\text{an } n\times n\text{-matrix with } n\geq 2} = 0 \qquad (206)$$

for any $x \in K$. In other words, if all entries of a square matrix of size ≥ 2 are equal, then the determinant of this matrix is 0.

> **Example 6.4.8.** Let $n \in \mathbb{N}$, and let $x_1, x_2, \ldots, x_n \in K$ and $y_1, y_2, \ldots, y_n \in K$. Compute
>
> $$\det\left(\left(x_i + y_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \det\begin{pmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_n \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n+y_1 & x_n+y_2 & \cdots & x_n+y_n \end{pmatrix}.$$

Let us experiment with small n's:

$$\begin{aligned}
\det () &= 1; \\
\det \left(\begin{array}{c} x_1 + y_1 \end{array} \right) &= x_1 + y_1; \\
\det \left(\begin{array}{cc} x_1 + y_1 & x_1 + y_2 \\ x_2 + y_1 & x_2 + y_2 \end{array} \right) &= -\left(x_1 - x_2\right)\left(y_1 - y_2\right); \\
\det \left(\begin{array}{ccc} x_1 + y_1 & x_1 + y_2 & x_1 + y_3 \\ x_2 + y_1 & x_2 + y_2 & x_2 + y_3 \\ x_3 + y_1 & x_3 + y_2 & x_3 + y_3 \end{array} \right) &= 0.
\end{aligned}$$

So we suspect the following:

Proposition 6.4.9. Let $n \in \mathbb{N}$ be such that $n \geq 3$. Let $x_1, x_2, \ldots, x_n \in K$ and $y_1, y_2, \ldots, y_n \in K$. Then,

$$\det \left(\left(x_i + y_j\right)_{1 \leq i \leq n,\ 1 \leq j \leq n} \right) = 0.$$

Proof of Proposition 6.4.9 (sketched). (See [Grinbe15, Example 6.7] for more details.) The definition of the determinant yields

$$\begin{aligned}
&\det \left(\left(x_i + y_j\right)_{1 \leq i \leq n,\ 1 \leq j \leq n} \right) \\
&= \sum_{\sigma \in S_n} (-1)^\sigma \underbrace{\left(x_1 + y_{\sigma(1)}\right) \left(x_2 + y_{\sigma(2)}\right) \cdots \left(x_n + y_{\sigma(n)}\right)}_{\substack{= \prod_{i=1}^{n} \left(x_i + y_{\sigma(i)}\right) = \sum_{I \subseteq [n]} \left(\prod_{i \in I} x_i\right) \left(\prod_{i \in [n] \setminus I} y_{\sigma(i)}\right) \\ \text{(by (150), applied to } a_i = x_i \text{ and } b_i = y_{\sigma(i)}\text{)}}} \\
&= \sum_{\sigma \in S_n} (-1)^\sigma \sum_{I \subseteq [n]} \left(\prod_{i \in I} x_i\right) \left(\prod_{i \in [n] \setminus I} y_{\sigma(i)}\right) \\
&= \sum_{I \subseteq [n]} \sum_{\sigma \in S_n} (-1)^\sigma \left(\prod_{i \in I} x_i\right) \left(\prod_{i \in [n] \setminus I} y_{\sigma(i)}\right) \\
&= \sum_{I \subseteq [n]} \left(\prod_{i \in I} x_i\right) \sum_{\sigma \in S_n} (-1)^\sigma \prod_{i \in [n] \setminus I} y_{\sigma(i)}.
\end{aligned}$$

Now, I claim that the inner sum is 0 for each I. In other words, I claim that

$$\sum_{\sigma \in S_n} (-1)^\sigma \prod_{i \in [n] \setminus I} y_{\sigma(i)} = 0 \qquad \text{for each } I \subseteq [n]. \tag{207}$$

For instance, for $I = \{1, 2\}$, this is claiming that

$$\sum_{\sigma \in S_n} (-1)^\sigma y_{\sigma(3)} y_{\sigma(4)} \cdots y_{\sigma(n)} = 0.$$

[*Proof of (207):* Fix a subset I of $[n]$. We shall show that all addends in the sum $\sum\limits_{\sigma \in S_n} (-1)^{\sigma} \prod\limits_{i \in [n] \setminus I} y_{\sigma(i)}$ cancel each other – i.e., that for each addend in this sum, there is a different addend with the same product of y_j's but a different sign $(-1)^{\sigma}$. To achieve this, we need to pair up each $\sigma \in S_n$ with a different permutation $\sigma' = \sigma t_{u,v} \in S_n$ that satisfies $\prod\limits_{i \in [n] \setminus I} y_{\sigma'(i)} = \prod\limits_{i \in [n] \setminus I} y_{\sigma(i)}$ but $(-1)^{\sigma'} = -(-1)^{\sigma}$. (Indeed, this pairing will then produce the required cancellations: the addend for each σ will cancel the addend for the corresponding σ'. To be more rigorous, we are here applying Lemma 6.1.3 to $\mathcal{A} = S_n$, $\mathcal{X} = S_n$ and $\operatorname{sign} \sigma = (-1)^{\sigma} \prod\limits_{i \in [n] \setminus I} y_{\sigma(i)}$ (of course, this should not be confused for the notation $\operatorname{sign} \sigma$ for $(-1)^{\sigma}$) and
$f =$ (the map $S_n \to S_n$ that sends each $\sigma \in S_n$ to the corresponding σ').)

So let us construct our pairing. Indeed, from $I \subseteq [n]$, we obtain $|I| + |[n] \setminus I| = |[n]| = n \geq 3$; hence, at least one of the two sets I and $[n] \setminus I$ has size > 1. In other words, must be in one of the following two cases:

Case 1: We have $|I| > 1$.

Case 2: We have $|[n] \setminus I| > 1$.

Let us first consider Case 1. In this case, we have $|I| > 1$. Thus, $|I| \geq 2$. Pick two distinct elements u and v of I. (These exist, since $|I| \geq 2$.) Now, for each permutation $\sigma \in S_n$, we set $\sigma' := \sigma t_{u,v} \in S_n$. Then, each $\sigma \in S_n$ satisfies $\sigma'' = \underbrace{\sigma'}_{=\sigma t_{u,v}} t_{u,v} = \sigma \underbrace{t_{u,v} t_{u,v}}_{=t_{u,v}^2 = \operatorname{id}} = \sigma$. Hence, we can pair up each $\sigma \in S_n$ with $\sigma' \in S_n$. Any two permutations σ and σ' that are paired with each other have different signs (indeed, if $\sigma \in S_n$, then $\sigma' = \sigma t_{u,v}$ and thus $(-1)^{\sigma'} = (-1)^{\sigma t_{u,v}} = (-1)^{\sigma} \underbrace{(-1)^{t_{u,v}}}_{=-1} = -(-1)^{\sigma}$), but the corresponding products $\prod\limits_{i \in [n] \setminus I} y_{\sigma(i)}$ and $\prod\limits_{i \in [n] \setminus I} y_{\sigma'(i)}$ are equal (indeed, the permutations σ and $\sigma' = \sigma t_{u,v}$ differ only in their values at u and v, but neither of these two values appears in any of our two products, since $u, v \in I$). This shows that our pairing has precisely the properties we want: Each $\sigma \in S_n$ satisfies $\prod\limits_{i \in [n] \setminus I} y_{\sigma'(i)} = \prod\limits_{i \in [n] \setminus I} y_{\sigma(i)}$ but $(-1)^{\sigma'} = -(-1)^{\sigma}$ (and thus $\sigma' \neq \sigma$). As explained above, this completes the proof of (207) in Case 1.

Let us now consider Case 2. In this case, we have $|[n] \setminus I| > 1$. Thus, $|[n] \setminus I| \geq 2$. Pick two distinct elements u and v of $[n] \setminus I$. (These exist, since $|[n] \setminus I| \geq 2$.) We now proceed just as we did in Case 1: For each permutation $\sigma \in S_n$, we set $\sigma' := \sigma t_{u,v} \in S_n$. Then, each $\sigma \in S_n$ satisfies $\sigma'' = \underbrace{\sigma'}_{=\sigma t_{u,v}} t_{u,v} = \sigma \underbrace{t_{u,v} t_{u,v}}_{=t_{u,v}^2 = \operatorname{id}} = \sigma$. Hence, we can pair up each $\sigma \in S_n$ with $\sigma' \in S_n$. Any two permutations σ and σ' that are paired with each other have different signs (this can be seen as in Case 1), but the corresponding products $\prod_{i\in[n]\setminus I} y_{\sigma(i)}$ and $\prod_{i\in[n]\setminus I} y_{\sigma'(i)}$ are equal (indeed, the permutation $\sigma' = \sigma t_{u,v}$ can be obtained from σ by swapping the values at u and v (so that $\sigma'(u) = \sigma(v)$ and $\sigma'(v) = \sigma(u)$); thus, the products $\prod_{i\in[n]\setminus I} y_{\sigma(i)}$ and $\prod_{i\in[n]\setminus I} y_{\sigma'(i)}$ differ only in the order in which their factors $y_{\sigma(u)}$ and $y_{\sigma(v)}$ appear in them[92]; hence, these products are equal, since K is commutative). Again, this shows that our pairing has the properties we want, and thus the proof of (207) is complete in Case 2.

Thus, (207) is proved in both cases.]

Now, we can finish our computation of the original determinant:

$$\det\left(\left(x_i+y_j\right)_{1\le i\le n,\ 1\le j\le n}\right) = \sum_{I\subseteq[n]}\left(\prod_{i\in I} x_i\right)\underbrace{\sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i\in[n]\setminus I} y_{\sigma(i)}}_{\substack{=0\\ \text{(by (207))}}} = 0.$$

This proves Proposition 6.4.9. □

6.4.2. Basic properties

The examples above show that pedestrian proofs of facts about determinants (using just the definition) are possible, but become cumbersome fairly quickly. Fortunately, determinants have a lot of properties that, once proved, provide new methods for computing determinants.

Let us first recall a few basic facts that should (ideally) be known from a good course on linear algebra. Recall that the transpose of a matrix A is denoted by A^T.

Theorem 6.4.10 (Transposes preserve determinants)**.** Let $n \in \mathbb{N}$. If $A \in K^{n\times n}$ is any $n\times n$-matrix, then $\det\left(A^T\right) = \det A$.

Proof. See [Strick13, Corollary B.16] or [Grinbe15, Exercise 6.4] or [Laue15, §5.3.2]. □

Theorem 6.4.11 (Determinants of triangular matrices)**.** Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be a triangular (i.e., lower-triangular or upper-triangular) $n\times n$-matrix. Then, the determinant of the matrix A is the product of its diagonal entries. That is,

$$\det A = A_{1,1}A_{2,2}\cdots A_{n,n}.$$

Proof. See [Strick13, Proposition B.11] or [Grinbe15, Exercise 6.3 and the paragraph after Exercise 6.4]. □

[92] Both factors $y_{\sigma(u)}$ and $y_{\sigma(v)}$ do indeed appear in these products, since u and v belong to $[n]\setminus I$.

As a consequence of Theorem 6.4.11, we see that the determinant of a diagonal matrix is the product of its diagonal entries (since any diagonal matrix is triangular).

Theorem 6.4.12 (Row operation properties)**.** Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Then:

(a) If we swap two rows of A, then $\det A$ gets multiplied by -1.

(b) If A has a zero row (i.e., a row that consists entirely of zeroes), then $\det A = 0$.

(c) If A has two equal rows, then $\det A = 0$.

(d) Let $\lambda \in K$. If we multiply a row of A by λ (that is, we multiply all entries of this one row by λ, while leaving all other entries of A unchanged), then $\det A$ gets multiplied by λ.

(e) If we add a row of A to another row of A (that is, we add each entry of the former row to the corresponding entry of the latter), then $\det A$ stays unchanged.

(f) Let $\lambda \in K$. If we add λ times a row of A to another row of A (that is, we add λ times each entry of the former row to the corresponding entry of the latter), then $\det A$ stays unchanged.

(g) Let $B, C \in K^{n \times n}$ be two further $n \times n$-matrices. Let $k \in [n]$. Assume that

$$(\text{the } k\text{-th row of } C) = (\text{the } k\text{-th row of } A) + (\text{the } k\text{-th row of } B),$$

whereas each $i \neq k$ satisfies

$$(\text{the } i\text{-th row of } C) = (\text{the } i\text{-th row of } A) = (\text{the } i\text{-th row of } B).$$

Then,

$$\det C = \det A + \det B.$$

Example 6.4.13. Let us see what Theorem 6.4.12 is saying in some particular cases (specifically, for 3×3-matrices):

(a) One instance of Theorem 6.4.12 **(a)** is

$$\det \begin{pmatrix} a & b & c \\ a'' & b'' & c'' \\ a' & b' & c' \end{pmatrix} = -\det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}.$$

(b) One instance of Theorem 6.4.12 **(b)** is

$$\det \begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ a'' & b'' & c'' \end{pmatrix} = 0.$$

(c) One instance of Theorem 6.4.12 **(c)** is

$$\det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a & b & c \end{pmatrix} = 0.$$

(d) One instance of Theorem 6.4.12 **(d)** is

$$\det \begin{pmatrix} a & b & c \\ \lambda a' & \lambda b' & \lambda c' \\ a'' & b'' & c'' \end{pmatrix} = \lambda \det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}.$$

(e) One instance of Theorem 6.4.12 **(e)** is

$$\det \begin{pmatrix} a & b & c \\ a' + a'' & b' + b'' & c' + c'' \\ a'' & b'' & c'' \end{pmatrix} = \det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}.$$

(f) One instance of Theorem 6.4.12 **(f)** is

$$\det \begin{pmatrix} a & b & c \\ a' + \lambda a'' & b' + \lambda b'' & c' + \lambda c'' \\ a'' & b'' & c'' \end{pmatrix} = \det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}.$$

(g) One instance of Theorem 6.4.12 **(g)** is

$$\underbrace{\det \begin{pmatrix} a & b & c \\ d+d' & e+e' & f+f' \\ g & h & i \end{pmatrix}}_{\text{this is } C} = \det \underbrace{\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}}_{\text{this is } A} + \det \underbrace{\begin{pmatrix} a & b & c \\ d' & e' & f' \\ g & h & i \end{pmatrix}}_{\text{this is } B}.$$

(Specifically, this is the particular case of Theorem 6.4.12 **(g)** for $n = 3$ and $k = 2$.)

Parts **(b)**, **(d)** and **(g)** of Theorem 6.4.12 are commonly summarized under the mantle of *"multilinearity of the determinant"* or *"linearity of the determinant in the k-th row"*. In fact, they say that (for any given $n \in \mathbb{N}$ and $k \in [n]$) if we hold all rows other than the k-th row of an $n \times n$-matrix A fixed, then $\det A$ depends K-linearly on the k-th row of A.

Proof of Theorem 6.4.12. **(a)** See [Grinbe15, Exercise 6.7 **(a)**]. This is also a particular case of [Strick13, Corollary B.19].

(b) See [Grinbe15, Exercise 6.7 **(c)**]. This is also near-obvious from Definition 6.4.3.

(c) See [Grinbe15, Exercise 6.7 **(e)**] or [Laue15, §5.3.3, property (iii)] or [19fla, 2019-10-23 blackboard notes, Theorem 1.3.3].[93]

(d) See [Grinbe15, Exercise 6.7 **(g)**] or [Laue15, §5.3.3, property (ii)]. This is also a particular case of [Strick13, Corollary B.19].

(f) See [Grinbe15, Exercise 6.8 **(a)**]. This is also a particular case of [Strick13, Corollary B.19].

(e) This is the particular case of part **(f)** for $\lambda = 1$.

(g) See [Grinbe15, Exercise 6.7 **(i)**] or [Laue15, §5.3.3, property (i)] or [19fla, 2019-10-30 blackboard notes, Theorem 1.2.3]. □

Theorem 6.4.14 (Column operation properties)**.** Theorem 6.4.12 also holds if we replace "row" by "column" throughout it.

Proof. Theorem 6.4.10 shows that the determinant of a matrix does not change when we replace it by its transpose; however, the rows of this transpose A^T are the transposes of the columns of A. Thus, Theorem 6.4.14 follows by applying Theorem 6.4.12 to the transposes of all the matrices involved. (See [Grinbe15, Exercises 6.7 and 6.8] for the details.) □

Corollary 6.4.15. Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ and $\tau \in S_n$. Then,

$$\det\left(\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^{\tau}\cdot\det A \tag{208}$$

and

$$\det\left(\left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^{\tau}\cdot\det A. \tag{209}$$

In words: When we permute the rows or the columns of a matrix, its determinant gets multiplied by the sign of the permutation.

Proof of Corollary 6.4.15. Let us first prove (209).

The definition of $\det A$ yields

$$\begin{aligned}\det A &= \sum_{\sigma\in S_n}(-1)^{\sigma}\underbrace{A_{1,\sigma(1)}A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}}_{=\prod_{i=1}^{n}A_{i,\sigma(i)}}\\ &= \sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\sigma(i)}.\end{aligned} \tag{210}$$

[93] *Warning:* Several authors claim to give an easy proof of part **(c)** using part **(a)**. This "proof" goes as follows: If A has two equal rows, then swapping these rows leaves A unchanged, but (because of Theorem 6.4.12) flips the sign of $\det A$. Hence, in this case, we have $\det A = -\det A$, so that $2\det A = 0$ and therefore $\det A = 0$, right? Not so fast! In order to obtain $\det A = 0$ from $2\det A = 0$, we need the element 2 of K to be invertible or at least be a non-zero-divisor (since we have to divide by 2). This is true when K is one of the "high-school rings" $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, but it is not true when K is the field $\mathbb{F}_2$ with 2 elements (or, more generally, any field of characteristic 2). This slick argument can be salvaged, but in the form just given it is incomplete.

The definition of $\det\left(\left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)$ yields

$$\det\left(\left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \sum_{\sigma\in S_n}(-1)^{\sigma}\underbrace{A_{1,\tau(\sigma(1))}A_{2,\tau(\sigma(2))}\cdots A_{n,\tau(\sigma(n))}}_{=\prod_{i=1}^{n}A_{i,\tau(\sigma(i))}}$$
$$= \sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\tau(\sigma(i))}. \qquad (211)$$

However, S_n is a group. Thus, the map

$$S_n \to S_n,$$
$$\sigma \mapsto \tau^{-1}\sigma$$

is a bijection. Hence, we can substitute $\tau^{-1}\sigma$ for σ in the sum $\sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\tau(\sigma(i))}$. Thus, we obtain

$$\sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\tau(\sigma(i))}$$
$$= \sum_{\sigma\in S_n}\underbrace{(-1)^{\tau^{-1}\sigma}}_{\substack{=(-1)^{\tau^{-1}}\cdot(-1)^{\sigma} \\ \text{(by Proposition 5.4.2 \textbf{(d)},} \\ \text{applied to } \tau^{-1} \text{ and } \sigma \text{ instead of } \sigma \text{ and } \tau)}}\prod_{i=1}^{n}\underbrace{A_{i,\tau\left(\left(\tau^{-1}\sigma\right)(i)\right)}}_{\substack{=A_{i,\sigma(i)} \\ \text{(since } \tau\left(\left(\tau^{-1}\sigma\right)(i)\right)=\left(\tau\tau^{-1}\sigma\right)(i)=\sigma(i) \\ \text{(because } \tau\tau^{-1}\sigma=\sigma))}}$$
$$= \sum_{\sigma\in S_n}(-1)^{\tau^{-1}}\cdot(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\sigma(i)} = \underbrace{(-1)^{\tau^{-1}}}_{\substack{=(-1)^{\tau} \\ \text{(by Proposition 5.4.2 \textbf{(f)},} \\ \text{applied to } \tau^{-1} \text{ instead of } \sigma)}}\cdot\underbrace{\sum_{\sigma\in S_n}(-1)^{\sigma}\prod_{i=1}^{n}A_{i,\sigma(i)}}_{\substack{=\det A \\ \text{(by (210))}}}$$
$$= (-1)^{\tau}\cdot\det A.$$

In view of this, we can rewrite (211) as

$$\det\left(\left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^{\tau}\cdot\det A.$$

This proves (209).

Now, we can easily derive (208) by using the transpose. Indeed, applying (209) to A^T instead of A, we obtain

$$\det\left(\left(\left(A^T\right)_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^{\tau}\cdot\underbrace{\det\left(A^T\right)}_{\substack{=\det A \\ \text{(by Theorem 6.4.10)}}}$$
$$= (-1)^{\tau}\cdot\det A. \qquad (212)$$

However, each $(i,j) \in [n]^2$ satisfies

$$\left(A^T\right)_{i,\tau(j)} = A_{\tau(j),i} \qquad \left(\text{by the definition of } A^T\right).$$

Thus,

$$\left(\left(A^T\right)_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \left(A_{\tau(j),i}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \left(\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)^T$$

(again by the definition of the transpose). Therefore,

$$\begin{aligned}\det\left(\left(\left(A^T\right)_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) &= \det\left(\left(\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)^T\right)\\ &= \det\left(\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)\end{aligned}$$

(by Theorem 6.4.10, applied to $\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ instead of A). Hence,

$$\det\left(\left(A_{\tau(i),j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \det\left(\left(\left(A^T\right)_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^\tau \cdot \det A$$

(by (212)). This proves (208). Thus, the proof of Corollary 6.4.15 is complete. □

The following is probably the most remarkable property of determinants:

Theorem 6.4.16 (Multiplicativity of the determinant)**.** Let $n \in \mathbb{N}$. Let $A, B \in K^{n\times n}$ be two $n \times n$-matrices. Then,

$$\det(AB) = \det A \cdot \det B.$$

Proof. See [Strick13, Theorem B.17] or [Grinbe15, Theorem 6.23] or [Zeilbe85, §5] or [Ford21, Lemma 4.5.5 (1)] or [Laue15, Theorem 5.7]. (Many of these proofs are at least partly combinatorial, but the one in [Zeilbe85, §5] is fully so, constructing quite explicitly a sign-reversing involution.) □

As an application of these properties, let us reprove Proposition 6.4.7 and Proposition 6.4.9:

Second proof of Proposition 6.4.7. Define two $n \times n$-matrices

$$A := \begin{pmatrix} x_1 & 0 & 0 & \cdots & 0\\ x_2 & 0 & 0 & \cdots & 0\\ x_3 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ x_n & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad \text{and} \qquad B := \begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n\\ 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(Only the first column of A and the first row of B have any nonzero entries.)

Now,

$$\left(x_iy_j\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & x_2y_2 & \cdots & x_2y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_ny_1 & x_ny_2 & \cdots & x_ny_n \end{pmatrix}$$

$$= \underbrace{\begin{pmatrix} x_1 & 0 & 0 & \cdots & 0 \\ x_2 & 0 & 0 & \cdots & 0 \\ x_3 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & 0 & 0 & \cdots & 0 \end{pmatrix}}_{=A} \underbrace{\begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}}_{=B} = AB,$$

so that

$$\det\left(\left(x_iy_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \det\left(AB\right) = \det A \cdot \det B$$

(by Theorem 6.4.16). However, the matrix A has a zero column (since $n \geq 2$), and thus satisfies $\det A = 0$ (by Theorem 6.4.14 **(b)**[94]). Hence,

$$\det\left(\left(x_iy_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \underbrace{\det A}_{=0} \cdot \det B = 0.$$

Thus, Proposition 6.4.7 is proven again. □

Second proof of Proposition 6.4.9. Define two $n \times n$-matrices

$$A := \begin{pmatrix} x_1 & 1 & 0 & \cdots & 0 \\ x_2 & 1 & 0 & \cdots & 0 \\ x_3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & 1 & 0 & \cdots & 0 \end{pmatrix} \qquad \text{and} \qquad B := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ y_1 & y_2 & y_3 & \cdots & y_n \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(Only the first two columns of A and the first two rows of B have any nonzero entries.)

[94] Of course, by "Theorem 6.4.14 **(b)**", we mean "the analogue of Theorem 6.4.12 **(b)** for columns instead of rows".

Now,

$$\left(x_i+y_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}=\begin{pmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_n \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n+y_1 & x_n+y_2 & \cdots & x_n+y_n \end{pmatrix}$$
$$=\underbrace{\begin{pmatrix} x_1 & 1 & 0 & \cdots & 0 \\ x_2 & 1 & 0 & \cdots & 0 \\ x_3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & 1 & 0 & \cdots & 0 \end{pmatrix}}_{=A}\underbrace{\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ y_1 & y_2 & y_3 & \cdots & y_n \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}}_{=B}=AB,$$

so that

$$\det\left(\left(x_i+y_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\det\left(AB\right)=\det A\cdot\det B$$

(by Theorem 6.4.16). However, the matrix A has a zero column (since $n\geq 3$), and thus satisfies $\det A=0$ (by Theorem 6.4.14 **(b)**). Hence,

$$\det\left(\left(x_i+y_j\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\underbrace{\det A}_{=0}\cdot\det B=0.$$

Thus, Proposition 6.4.9 is proven again. □

The following fact follows equally easily from everything we know so far about determinants:

Corollary 6.4.17. Let $n\in\mathbb{N}$. Let $A\in K^{n\times n}$ and $d_1,d_2,\ldots,d_n\in K$. Then,

$$\det\left(\left(d_iA_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=d_1d_2\cdots d_n\cdot\det A \qquad (213)$$

and

$$\det\left(\left(d_jA_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=d_1d_2\cdots d_n\cdot\det A. \qquad (214)$$

First proof of Corollary 6.4.17 (sketched). The matrix $\left(d_iA_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ is obtained from the matrix A by multiplying the 1-st row by d_1, multiplying the 2-nd row by d_2, multiplying the 3-rd row by d_3, and so on. Theorem 6.4.12 **(d)** (applied repeatedly – once for each row) shows that these multiplications result in the determinant of A getting multiplied by $d_1,d_2,\ldots,d_n$ (in succession). Hence,

$$\det\left(\left(d_iA_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=d_1d_2\cdots d_n\cdot\det A.$$

Thus, (213) is proved. The proof of (214) is analogous (using columns instead of rows). Corollary 6.4.17 is proven. □

Second proof of Corollary 6.4.17 (sketched). Let D be the diagonal matrix

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \in K^{n\times n}.$$

Then, D is upper-triangular; hence, Theorem 6.4.11 shows that its determinant is $\det D = d_1 d_2 \cdots d_n$.

However, it is easy to see that $\left(d_i A_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = DA$. Hence,

$$\begin{aligned} \det\left(\left(d_i A_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) &= \det\left(DA\right) = \det D \cdot \det A \qquad \text{(by Theorem 6.4.16)} \\ &= d_1 d_2 \cdots d_n \cdot \det A \qquad \left(\text{since } \det D = d_1 d_2 \cdots d_n\right). \end{aligned}$$

This proves (213). A similar argument using $\left(d_j A_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = AD$ proves (214). Thus, Corollary 6.4.17 is proven again. □

Third proof of Corollary 6.4.17. Let us now proceed completely elementarily. The definition of a determinant yields

$$\det A = \sum_{\sigma\in S_n} (-1)^{\sigma} A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)} \qquad (215)$$

and

$$\begin{aligned} \det\left(\left(d_i A_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) &= \sum_{\sigma\in S_n} (-1)^{\sigma} \underbrace{\left(d_1 A_{1,\sigma(1)}\right)\left(d_2 A_{2,\sigma(2)}\right)\cdots\left(d_n A_{n,\sigma(n)}\right)}_{=(d_1 d_2\cdots d_n)\left(A_{1,\sigma(1)} A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}\right)} \\ &= \sum_{\sigma\in S_n} (-1)^{\sigma} \left(d_1 d_2 \cdots d_n\right)\left(A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}\right) \\ &= d_1 d_2 \cdots d_n \cdot \underbrace{\sum_{\sigma\in S_n} (-1)^{\sigma} A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}}_{\substack{=\det A \\ \text{(by (215))}}} \\ &= d_1 d_2 \cdots d_n \cdot \det A \end{aligned}$$

and

$$\begin{aligned}
&\det\left(\left(d_j A_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)\\
&=\sum_{\sigma\in S_n}(-1)^\sigma \underbrace{\left(d_{\sigma(1)}A_{1,\sigma(1)}\right)\left(d_{\sigma(2)}A_{2,\sigma(2)}\right)\cdots\left(d_{\sigma(n)}A_{n,\sigma(n)}\right)}_{=\left(d_{\sigma(1)}d_{\sigma(2)}\cdots d_{\sigma(n)}\right)\left(A_{1,\sigma(1)}A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}\right)}\\
&=\sum_{\sigma\in S_n}(-1)^\sigma \underbrace{\left(d_{\sigma(1)}d_{\sigma(2)}\cdots d_{\sigma(n)}\right)}_{\substack{=d_1d_2\cdots d_n\\ \text{(since }\sigma\text{ is a permutation of the set }[n])}}\left(A_{1,\sigma(1)}A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}\right)\\
&=\sum_{\sigma\in S_n}(-1)^\sigma\left(d_1d_2\cdots d_n\right)\left(A_{1,\sigma(1)}A_{2,\sigma(2)}\cdots A_{n,\sigma(n)}\right)\\
&=d_1d_2\cdots d_n\cdot\det A \qquad \text{(as we have seen above)}.
\end{aligned}$$

Once again, this proves Corollary 6.4.17. □

6.4.3. Cauchy–Binet

The multiplicativity of the determinant generalizes to non-square matrices A and B, but the general statement is subtler and less famous:

> **Theorem 6.4.18** (Cauchy–Binet formula)**.** Let $n, m \in \mathbb{N}$. Let $A \in K^{n\times m}$ be an $n \times m$-matrix, and let $B \in K^{m\times n}$ be an $m \times n$-matrix. Then,
>
> $$\det(AB) = \sum_{\substack{(g_1,g_2,\ldots,g_n)\in[m]^n;\\ g_1<g_2<\cdots<g_n}} \det\left(\operatorname{cols}_{g_1,g_2,\ldots,g_n} A\right)\cdot\det\left(\operatorname{rows}_{g_1,g_2,\ldots,g_n} B\right).$$
>
> Here, we are using the following notations:
>
> - We let $\operatorname{cols}_{g_1,g_2,\ldots,g_n} A$ be the $n\times n$-matrix obtained from A by removing all columns other than the g_1-st, the g_2-nd, the g_3-rd, etc.. In other words,
> $$\operatorname{cols}_{g_1,g_2,\ldots,g_n} A := \left(A_{i,g_j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}.$$
> - We let $\operatorname{rows}_{g_1,g_2,\ldots,g_n} B$ be the $n\times n$-matrix obtained from B by removing all rows other than the g_1-st, the g_2-nd, the g_3-rd, etc.. In other words,
> $$\operatorname{rows}_{g_1,g_2,\ldots,g_n} B := \left(B_{g_i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}.$$

Informally, we can rewrite the claim of Theorem 6.4.18 as follows:

$$\det(AB) = \sum \det(\text{some } n \text{ columns of } A)\cdot\det(\text{the corresponding } n \text{ rows of } B).$$

The sum runs over all ways to form an $n \times n$-matrix by picking n columns of A (in increasing order, with no repetitions). The corresponding n rows of B form an $n \times n$-matrix as well.

Example 6.4.19. Let $n = 2$ and $m = 3$, and let $A = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix}$ and $B = \begin{pmatrix} x & x' \\ y & y' \\ z & z' \end{pmatrix}$. Then, Theorem 6.4.18 yields

$$\begin{aligned}
\det(AB) &= \sum_{\substack{(g_1,g_2)\in[3]^2;\\ g_1<g_2}} \det\left(\operatorname{cols}_{g_1,g_2} A\right) \cdot \det\left(\operatorname{rows}_{g_1,g_2} B\right) \\
&= \det\left(\operatorname{cols}_{1,2} A\right) \cdot \det\left(\operatorname{rows}_{1,2} B\right) \\
&\qquad + \det\left(\operatorname{cols}_{1,3} A\right) \cdot \det\left(\operatorname{rows}_{1,3} B\right) \\
&\qquad + \det\left(\operatorname{cols}_{2,3} A\right) \cdot \det\left(\operatorname{rows}_{2,3} B\right) \\
&\qquad\qquad \left(\begin{array}{c} \text{since the only 2-tuples } (g_1,g_2) \in [3]^2 \\ \text{satisfying } g_1 < g_2 \text{ are } (1,2) \text{ and } (1,3) \text{ and } (2,3) \end{array}\right) \\
&= \det\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \cdot \det\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \\
&\qquad + \det\begin{pmatrix} a & c \\ a' & c' \end{pmatrix} \cdot \det\begin{pmatrix} x & x' \\ z & z' \end{pmatrix} \\
&\qquad + \det\begin{pmatrix} b & c \\ b' & c' \end{pmatrix} \cdot \det\begin{pmatrix} y & y' \\ z & z' \end{pmatrix} \\
&= \left(ab' - ba'\right)\left(xy' - yx'\right) + \left(ac' - ca'\right)\left(xz' - zx'\right) \\
&\qquad + \left(bc' - cb'\right)\left(yz' - zy'\right).
\end{aligned}$$

You can check this against the equality

$$\begin{aligned}
\det(AB) = (ax + by + cz)\left(a'x' + b'y' + c'z'\right) \\
- \left(ax' + by' + cz'\right)\left(a'x + b'y + c'z\right),
\end{aligned}$$

which is obtained by directly computing

$$AB = \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} x & x' \\ y & y' \\ z & z' \end{pmatrix} = \begin{pmatrix} ax + by + cz & ax' + by' + cz' \\ a'x + b'y + c'z & a'x' + b'y' + c'z' \end{pmatrix}.$$

Remark 6.4.20. If $m < n$, then the claim of Theorem 6.4.18 becomes

$$\begin{aligned}\det(AB) &= \sum_{\substack{(g_1,g_2,\ldots,g_n)\in[m]^n;\\ g_1<g_2<\cdots<g_n}} \det\left(\operatorname{cols}_{g_1,g_2,\ldots,g_n} A\right)\cdot\det\left(\operatorname{rows}_{g_1,g_2,\ldots,g_n} B\right)\\ &= (\text{empty sum})\\ &\qquad\qquad (\text{since the set } [m] \text{ has no } n \text{ distinct elements})\\ &= 0.\end{aligned}$$

When K is a field, this can also be seen trivially from rank considerations (to wit, the matrix A has rank $\leq m < n$, and thus the product AB has rank $< n$ as well). When K is not a field, the notion of a rank is not available, so we do need Theorem 6.4.18 to obtain this (although there are ways around this).

If $m = n$, then the claim of Theorem 6.4.18 becomes

$$\begin{aligned}\det(AB) &= \sum_{\substack{(g_1,g_2,\ldots,g_n)\in[n]^n;\\ g_1<g_2<\cdots<g_n}} \det\left(\operatorname{cols}_{g_1,g_2,\ldots,g_n} A\right)\cdot\det\left(\operatorname{rows}_{g_1,g_2,\ldots,g_n} B\right)\\ &= \det\underbrace{\left(\operatorname{cols}_{1,2,\ldots,n} A\right)}_{=A}\cdot\det\underbrace{\left(\operatorname{rows}_{1,2,\ldots,n} B\right)}_{=B}\\ &\qquad\qquad \left(\begin{array}{c}\text{since the only } n\text{-tuple } (g_1,g_2,\ldots,g_n)\in[n]^n\\ \text{satisfying } g_1<g_2<\cdots<g_n \text{ is } (1,2,\ldots,n)\end{array}\right)\\ &= \det A\cdot\det B,\end{aligned}$$

so that we recover the multiplicativity of the determinant (Theorem 6.4.16).

Proof of Theorem 6.4.18. See [Grinbe15, Theorem 6.32] or [Schwar16] or [Knuth1, §1.2.3, Exercise 46] or [Loehr11, Theorem 9.53] or [Stanle18, Theorem 9.4] or [Zeng93, §2] (a fully combinatorial proof) of `https://math.stackexchange.com/questions/3243063/` . □

6.4.4. $\det(A+B)$

So much for $\det(AB)$. What can we say about $\det(A+B)$? The answer is somewhat cumbersome, but still rather useful. We need some notation to state it:

Definition 6.4.21. Let $n, m \in \mathbb{N}$. Let A be an $n \times m$-matrix.

Let U be a subset of $[n]$. Let V be a subset of $[m]$.

Then, $\operatorname{sub}_U^V A$ is the $|U| \times |V|$-matrix defined as follows:

Writing the two sets U and V as

$$U = \{u_1, u_2, \ldots, u_p\} \qquad \text{and} \qquad V = \{v_1, v_2, \ldots, v_q\}$$

with

$$u_1 < u_2 < \cdots < u_p \qquad \text{and} \qquad v_1 < v_2 < \cdots < v_q,$$

we set

$$\operatorname{sub}_U^V A := \left(A_{u_i, v_j}\right)_{1 \leq i \leq p,\ 1 \leq j \leq q}.$$

Roughly speaking, $\operatorname{sub}_U^V A$ is the matrix obtained from A by focusing only on the i-th rows for $i \in U$ (that is, removing all the other rows) and only on the j-th columns for $j \in V$ (that is, removing all the other columns).

This matrix $\operatorname{sub}_U^V A$ is called the *submatrix of A obtained by restricting to the U-rows and the V-columns*. If this matrix is square (i.e., if $|U| = |V|$), then its determinant $\det\left(\operatorname{sub}_U^V A\right)$ is called a *minor* of A.

Example 6.4.22. We have

$$\operatorname{sub}_{\{1,2\}}^{\{1,3\}} \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = \begin{pmatrix} a & c \\ a' & c' \end{pmatrix}$$

and

$$\operatorname{sub}_{\{2\}}^{\{3\}} \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = \begin{pmatrix} c' \end{pmatrix}.$$

Theorem 6.4.23. Let $n \in \mathbb{N}$. For any subset I of $[n]$, we let $\widetilde{I}$ be the complement $[n] \setminus I$ of I. (For example, if $n = 4$ and $I = \{1, 4\}$, then $\widetilde{I} = \{2, 3\}$.)

For any finite set S of integers, define $\operatorname{sum} S := \sum\limits_{s \in S} s$.

Let A and B be two $n \times n$-matrices in $K^{n \times n}$. Then,

$$\det(A + B) = \sum_{P \subseteq [n]} \sum_{\substack{Q \subseteq [n]; \\ |P| = |Q|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \cdot \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right).$$

Example 6.4.24. For $n = 2$, this is saying that

$$\begin{aligned}
\det(A+B) &= \underbrace{(-1)^{\operatorname{sum}\varnothing + \operatorname{sum}\varnothing}}_{=(-1)^{0+0}=1} \underbrace{\det\left(\operatorname{sub}^{\varnothing}_{\varnothing} A\right)}_{=\det()=1} \cdot \underbrace{\det\left(\operatorname{sub}^{\{1,2\}}_{\{1,2\}} B\right)}_{=\det B} \\
&\quad + \underbrace{(-1)^{\operatorname{sum}\{1\} + \operatorname{sum}\{1\}}}_{=(-1)^{1+1}=1} \underbrace{\det\left(\operatorname{sub}^{\{1\}}_{\{1\}} A\right)}_{\substack{=A_{1,1} \\ \text{(since } \operatorname{sub}^{\{1\}}_{\{1\}} A \text{ is} \\ \text{the } 1\times 1\text{-matrix } \left(\begin{array}{c} A_{1,1} \end{array}\right))}} \cdot \underbrace{\det\left(\operatorname{sub}^{\{2\}}_{\{2\}} B\right)}_{=B_{2,2}} \\
&\quad + \underbrace{(-1)^{\operatorname{sum}\{1\} + \operatorname{sum}\{2\}}}_{=(-1)^{1+2}=-1} \underbrace{\det\left(\operatorname{sub}^{\{2\}}_{\{1\}} A\right)}_{=A_{1,2}} \cdot \underbrace{\det\left(\operatorname{sub}^{\{1\}}_{\{2\}} B\right)}_{=B_{2,1}} \\
&\quad + \underbrace{(-1)^{\operatorname{sum}\{2\} + \operatorname{sum}\{1\}}}_{=(-1)^{2+1}=-1} \underbrace{\det\left(\operatorname{sub}^{\{1\}}_{\{2\}} A\right)}_{=A_{2,1}} \cdot \underbrace{\det\left(\operatorname{sub}^{\{2\}}_{\{1\}} B\right)}_{=B_{1,2}} \\
&\quad + \underbrace{(-1)^{\operatorname{sum}\{2\} + \operatorname{sum}\{2\}}}_{=(-1)^{2+2}=1} \underbrace{\det\left(\operatorname{sub}^{\{2\}}_{\{2\}} A\right)}_{=A_{2,2}} \cdot \underbrace{\det\left(\operatorname{sub}^{\{1\}}_{\{1\}} B\right)}_{=B_{1,1}} \\
&\quad + \underbrace{(-1)^{\operatorname{sum}\{1,2\} + \operatorname{sum}\{1,2\}}}_{=(-1)^{3+3}=1} \underbrace{\det\left(\operatorname{sub}^{\{1,2\}}_{\{1,2\}} A\right)}_{=\det A} \cdot \underbrace{\det\left(\operatorname{sub}^{\varnothing}_{\varnothing} B\right)}_{=\det()=1} \\
&= \det B + A_{1,1}B_{2,2} - A_{1,2}B_{2,1} - A_{2,1}B_{1,2} + A_{2,2}B_{1,1} + \det A \\
&= \det A + \det B - A_{1,2}B_{2,1} - A_{2,1}B_{1,2} + A_{1,1}B_{2,2} + A_{2,2}B_{1,1}.
\end{aligned}$$

Theorem 6.4.23 can be thought of as a kind of "binomial theorem" for determinants: On its right hand side (for $n > 0$) is a sum that contains both $\det A$ and $\det B$ as addends (in fact, $\det A$ is the addend for $P = Q = [n]$, whereas $\det B$ is the addend for $P = Q = \varnothing$) as well as many "mixed" addends that contain both a part of A and a part of B.

Proof of Theorem 6.4.23. See [Grinbe15, Theorem 6.160]. (Note that $\operatorname{sub}^Q_P A$ is called $\operatorname{sub}^{w(Q)}_{w(P)} A$ in [Grinbe15].) The main difficulty of the proof is bookkeeping; the underlying idea is simple (expand everything and regroup).

Here is a rough outline of the argument. If $\sigma \in S_n$, and if P is a subset of $[n]$, then $\sigma(P) = \{\sigma(i) \mid i \in P\}$ is a subset of $[n]$ as well, and has the same size as P (since σ is a permutation and therefore injective); thus, it satisfies $|P| = |\sigma(P)|$.

The definition of $\det(A+B)$ yields

$$\det(A+B) = \sum_{\sigma\in S_n} (-1)^\sigma \underbrace{\left(A_{1,\sigma(1)} + B_{1,\sigma(1)}\right)\left(A_{2,\sigma(2)} + B_{2,\sigma(2)}\right)\cdots\left(A_{n,\sigma(n)} + B_{n,\sigma(n)}\right)}_{\substack{=\prod\limits_{i=1}^{n}\left(A_{i,\sigma(i)}+B_{i,\sigma(i)}\right)=\sum\limits_{P\subseteq[n]}\left(\prod\limits_{i\in P}A_{i,\sigma(i)}\right)\left(\prod\limits_{i\in\widetilde{P}}B_{i,\sigma(i)}\right) \\ \text{(by (150), applied to } a_i=A_{i,\sigma(i)} \text{ and } b_i=B_{i,\sigma(i)})}}$$

$$= \sum_{\sigma\in S_n} (-1)^\sigma \sum_{P\subseteq[n]} \left(\prod_{i\in P} A_{i,\sigma(i)}\right)\left(\prod_{i\in\widetilde{P}} B_{i,\sigma(i)}\right)$$

$$= \sum_{P\subseteq[n]} \sum_{\sigma\in S_n} (-1)^\sigma \left(\prod_{i\in P} A_{i,\sigma(i)}\right)\left(\prod_{i\in\widetilde{P}} B_{i,\sigma(i)}\right)$$

$$= \sum_{P\subseteq[n]} \sum_{\substack{Q\subseteq[n];\\ |P|=|Q|}} \sum_{\substack{\sigma\in S_n;\\ \sigma(P)=Q}} (-1)^\sigma \left(\prod_{i\in P} A_{i,\sigma(i)}\right)\left(\prod_{i\in\widetilde{P}} B_{i,\sigma(i)}\right)$$

(here, we have split the inner sum according to the value of the subset $\sigma(P) = \{\sigma(i) \mid i \in P\}$, recalling that it satisfies $|P| = |\sigma(P)|$).

Now, fix two subsets P and Q of $[n]$ satisfying $|P| = |Q|$. Thus, $\left|\widetilde{P}\right| = \left|\widetilde{Q}\right|$ as well. Write the sets P, Q, $\widetilde{P}$ and $\widetilde{Q}$ as

$$P = \{p_1 < p_2 < \cdots < p_k\} \qquad \text{and} \qquad Q = \{q_1 < q_2 < \cdots < q_k\} \qquad \text{and}$$
$$\widetilde{P} = \{p'_1 < p'_2 < \cdots < p'_\ell\} \qquad \text{and} \qquad \widetilde{Q} = \{q'_1 < q'_2 < \cdots < q'_\ell\},$$

where the notation "$U = \{u_1 < u_2 < \cdots < u_a\}$" is just a shorthand way to say "$U = \{u_1, u_2, \ldots, u_a\}$ and $u_1 < u_2 < \cdots < u_a$" (or, equivalently, "the elements of U in strictly increasing order are $u_1, u_2, \ldots, u_a$"). Now, for each permutation $\sigma \in S_n$ satisfying $\sigma(P) = Q$, we see that:

- The elements $\sigma(p_1), \sigma(p_2), \ldots, \sigma(p_k)$ are the elements $q_1, q_2, \ldots, q_k$ in some order (since $\sigma(P) = Q$), and thus there exists a unique permutation $\alpha \in S_k$ such that
$$\sigma(p_i) = q_{\alpha(i)} \qquad \text{for each } i \in [k].$$
We denote this α by α_σ.
- The elements $\sigma(p'_1), \sigma(p'_2), \ldots, \sigma(p'_\ell)$ are the elements $q'_1, q'_2, \ldots, q'_\ell$ in some order (since $\sigma(P) = Q$ entails $\sigma\left(\widetilde{P}\right) = \widetilde{Q}$, because σ is a permutation of $[n]$), and thus there exists a unique permutation $\beta \in S_\ell$ such that
$$\sigma(p'_i) = q'_{\beta(i)} \qquad \text{for each } i \in [\ell].$$
We denote this β by β_σ.

Thus, for each permutation $\sigma \in S_n$ satisfying $\sigma(P) = Q$, we have defined two permutations $\alpha_\sigma \in S_k$ and $\beta_\sigma \in S_\ell$ that (roughly speaking) describe the actions of σ on the subsets P and $\widetilde{P}$, respectively. It is not hard to see that the map

$$\{\text{permutations } \sigma \in S_n \text{ satisfying } \sigma(P) = Q\} \to S_k \times S_\ell,$$
$$\sigma \mapsto (\alpha_\sigma, \beta_\sigma)$$

is a bijection. Moreover, for any permutation $\sigma \in S_n$ satisfying $\sigma(P) = Q$, we have

$$(-1)^{\sigma} = (-1)^{\operatorname{sum} P + \operatorname{sum} Q} (-1)^{\alpha_\sigma} (-1)^{\beta_\sigma}. \tag{216}$$

(Proving this is perhaps the least pleasant part of this proof, but it is pure combinatorics. It is probably easiest to reduce this to the case when $P = [k]$ and $Q = [k]$ by a reduction procedure that involves multiplying σ by $\operatorname{sum} P + \operatorname{sum} Q - 2 \cdot (1 + 2 + \cdots + k)$ many transpositions[95]. Once we are in the case $P = [k]$ and $Q = [k]$, we can prove (216) by directly counting the inversions of σ (showing that $\ell(\sigma) = \ell(\alpha_\sigma) + \ell(\beta_\sigma)$). Note that the proof I give in [Grinbe15, Theorem 6.160] avoids proving (216), opting instead

[95] Specifically: Recall the simple transpositions s_i defined for all $i \in [n-1]$ in Definition 5.2.3. By replacing σ by σs_i (for some $i \in [n-1]$), we can swap two adjacent values of σ (namely, $\sigma(i)$ and $\sigma(i+1)$). Furthermore, $\sigma(P) = Q$ implies $(\sigma s_i)(s_i(P)) = Q$ (since $s_i s_i = s_i^2 = \mathrm{id}$). Thus, the equality $\sigma(P) = Q$ is preserved if we simultaneously replace σ by σs_i and replace P by $s_i(P)$. Such a simultaneous replacement will be called a *shift*. Furthermore, if i is chosen in such a way that $i \notin P$ and $i+1 \in P$, then this shift will be called a *left shift*.

Let us see what happens to σ, P, α_σ and β_σ when we perform a left shift. Indeed, consider a left shift which replaces σ by σs_i and replaces P by $s_i(P)$, where $i \in [n-1]$ is chosen in such a way that $i \notin P$ and $i+1 \in P$. The set $s_i(P)$ is the set P with the element $i+1$ replaced by i. Thus, $\operatorname{sum}(s_i(P)) = \operatorname{sum} P - 1$. In other words, our left shift has decremented $\operatorname{sum} P$ by 1. Thus, our left shift has flipped the sign of $(-1)^{\operatorname{sum} P + \operatorname{sum} Q}$ (since $\operatorname{sum} Q$ obviously stays unchanged). The permutation σ has been replaced by σs_i, which is the same permutation as σ but with the values $\sigma(i)$ and $\sigma(i+1)$ swapped. Since $i \notin P$ and $i+1 \in P$, this swap has not disturbed the relative order of the elements of P and $\widetilde{P}$ (but merely replaced $i+1$ by i in P and replaced i by $i+1$ in $\widetilde{P}$), so that the permutations α_σ and β_σ have not changed. Our left shift thus has left α_σ and β_σ unchanged. It has, however, flipped the sign of $(-1)^{\sigma}$ (because $(-1)^{\sigma s_i} = (-1)^{\sigma} \underbrace{(-1)^{s_i}}_{=-1} = -(-1)^{\sigma}$).

Let us summarize: Each left shift leaves α_σ and β_σ unchanged, while flipping the signs of $(-1)^{\operatorname{sum} P + \operatorname{sum} Q}$ and $(-1)^{\sigma}$. However, by performing left shifts, we can move the smallest element of P one step to the left, or (if the smallest element of P is already 1) we can move the second-smallest element of P one step to the left, or (if the two smallest elements of P are already 1 and 2) we can move the third-smallest element of P one step to the left, and so on. After sufficiently many such left shifts, the set P will have become $[k]$, whereas α_σ and β_σ will not have changed (because we have seen above that each left shift leaves α_σ and β_σ unchanged). The total number of left shifts we need for this is $(p_1 - 1) + (p_2 - 2) + \cdots + (p_k - k) = \operatorname{sum} P - (1 + 2 + \cdots + k)$.

Likewise, we can define *left co-shifts*, which are operations similar to left shifts but acting on the values rather than positions of σ and acting on Q rather than P. Explicitly, a left co-shift replaces σ by $s_i \sigma$ and replaces Q by $s_i(Q)$, where $i \in [n-1]$ is chosen such that $i \notin Q$ and $i+1 \in Q$. Again, we can see that each left co-shift leaves α_σ and β_σ unchanged, while flipping the signs of $(-1)^{\operatorname{sum} P + \operatorname{sum} Q}$ and $(-1)^{\sigma}$. After a sequence of $\operatorname{sum} Q - (1 + 2 + \cdots + k)$ left co-shifts, the set Q will have become $[k]$.

Each left shift and each left co-shift multiplies the permutation σ by a transposition. Hence, after our $\operatorname{sum} P - (1 + 2 + \cdots + k)$ left shifts and our $\operatorname{sum} Q - (1 + 2 + \cdots + k)$ left co-shifts, we will have multiplied σ by altogether

$$\begin{aligned} &(\operatorname{sum} P - (1 + 2 + \cdots + k)) + (\operatorname{sum} Q - (1 + 2 + \cdots + k)) \\ &= \operatorname{sum} P + \operatorname{sum} Q - 2 \cdot (1 + 2 + \cdots + k) \end{aligned}$$

many transpositions. At the end of this process, we have $P = [k]$ and $Q = [k]$.

for an argument using row permutations; see [Grinbe15, solution to Exercise 6.44] for the details.)

Now,

$$\begin{aligned}
&\sum_{\substack{\sigma\in S_n;\\ \sigma(P)=Q}} \underbrace{(-1)^{\sigma}}_{\substack{=(-1)^{\operatorname{sum}P+\operatorname{sum}Q}(-1)^{\alpha_\sigma}(-1)^{\beta_\sigma}\\ \text{(by (216))}}} \underbrace{\left(\prod_{i\in P} A_{i,\sigma(i)}\right)}_{\substack{=\prod_{i=1}^{k} A_{p_i,q_{\alpha_\sigma(i)}}\\ \text{(by the definition of } \alpha_\sigma)}} \underbrace{\left(\prod_{i\in \widetilde{P}} B_{i,\sigma(i)}\right)}_{\substack{=\prod_{i=1}^{\ell} B_{p'_i,q'_{\beta_\sigma(i)}}\\ \text{(by the definition of } \beta_\sigma)}} \\
&= \sum_{\substack{\sigma\in S_n;\\ \sigma(P)=Q}} (-1)^{\operatorname{sum}P+\operatorname{sum}Q}(-1)^{\alpha_\sigma}(-1)^{\beta_\sigma}\left(\prod_{i=1}^{k} A_{p_i,q_{\alpha_\sigma(i)}}\right)\left(\prod_{i=1}^{\ell} B_{p'_i,q'_{\beta_\sigma(i)}}\right) \\
&= \sum_{(\alpha,\beta)\in S_k\times S_\ell} (-1)^{\operatorname{sum}P+\operatorname{sum}Q}(-1)^{\alpha}(-1)^{\beta}\left(\prod_{i=1}^{k} A_{p_i,q_{\alpha(i)}}\right)\left(\prod_{i=1}^{\ell} B_{p'_i,q'_{\beta(i)}}\right) \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } (\alpha,\beta) \text{ for } (\alpha_\sigma,\beta_\sigma) \text{ in the sum,}\\ \text{since the map } \sigma\mapsto(\alpha_\sigma,\beta_\sigma) \text{ is a bijection}\end{array}\right) \\
&= (-1)^{\operatorname{sum}P+\operatorname{sum}Q} \underbrace{\left(\sum_{\alpha\in S_k}(-1)^{\alpha}\prod_{i=1}^{k} A_{p_i,q_{\alpha(i)}}\right)}_{\substack{=\det\left(\operatorname{sub}_P^Q A\right)\\ \text{(by the definition of } \operatorname{sub}_P^Q A\\ \text{and its determinant)}}} \underbrace{\left(\sum_{\beta\in S_\ell}(-1)^{\beta}\prod_{i=1}^{\ell} B_{p'_i,q'_{\beta(i)}}\right)}_{\substack{=\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right)\\ \text{(by the definition of } \operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\\ \text{and its determinant)}}} \\
&= (-1)^{\operatorname{sum}P+\operatorname{sum}Q}\det\left(\operatorname{sub}_P^Q A\right)\cdot\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right). \qquad (217)
\end{aligned}$$

Forget that we fixed P and Q. We thus have proved (217) for any two subsets P and Q of $[n]$ satisfying $|P|=|Q|$. Thus, our original computation of $\det(A+B)$ becomes

$$\begin{aligned}
\det(A+B) &= \sum_{P\subseteq[n]}\ \sum_{\substack{Q\subseteq[n];\\ |P|=|Q|}} \underbrace{\sum_{\substack{\sigma\in S_n;\\ \sigma(P)=Q}} (-1)^{\sigma}\left(\prod_{i\in P} A_{i,\sigma(i)}\right)\left(\prod_{i\in\widetilde{P}} B_{i,\sigma(i)}\right)}_{\substack{=(-1)^{\operatorname{sum}P+\operatorname{sum}Q}\det\left(\operatorname{sub}_P^Q A\right)\cdot\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right)\\ \text{(by (217))}}} \\
&= \sum_{P\subseteq[n]}\ \sum_{\substack{Q\subseteq[n];\\ |P|=|Q|}} (-1)^{\operatorname{sum}P+\operatorname{sum}Q}\det\left(\operatorname{sub}_P^Q A\right)\cdot\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right).
\end{aligned}$$

This proves Theorem 6.4.23. □

We shall soon see a few applications of Theorem 6.4.23. First, let us observe a simple property of diagonal matrices:[96]

[96] We are using the Iverson bracket notation (see Definition A.1.5) again.

Lemma 6.4.25. Let $n \in \mathbb{N}$. Let $d_1, d_2, \ldots, d_n \in K$. Let

$$D := (d_i [i = j])_{1 \leq i \leq n,\ 1 \leq j \leq n} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \in K^{n \times n}$$

be the diagonal $n \times n$-matrix with diagonal entries $d_1, d_2, \ldots, d_n$. Then:

(a) We have $\det\left(\operatorname{sub}_P^P D\right) = \prod\limits_{i \in P} d_i$ for any subset P of $[n]$.

(b) Let P and Q be two distinct subsets of $[n]$ satisfying $|P| = |Q|$. Then, $\det\left(\operatorname{sub}_P^Q D\right) = 0$.

Proof of Lemma 6.4.25. This is [Grinbe15, Lemma 6.163] (slightly rewritten); see [Grinbe15, Exercise 6.49] for a detailed proof. (That said, it is almost obvious: In part **(a)**, the submatrix $\operatorname{sub}_P^P D$ is itself diagonal, and its diagonal entries are precisely the d_i for $i \in P$. In part **(b)**, the submatrix $\operatorname{sub}_P^Q D$ has a zero row (indeed, from $|P| = |Q|$ and $P \neq Q$, we see that there exists some $i \in P \setminus Q$, and then the corresponding row of $\operatorname{sub}_P^Q D$ is zero) and thus has determinant 0.) □

Lemma 6.4.25 gives very simple formulas for minors of diagonal matrices. Thus, the formula of Theorem 6.4.23 becomes simpler when the matrix B is diagonal:

Theorem 6.4.26. Let $n \in \mathbb{N}$. Let A and D be two $n \times n$-matrices in $K^{n \times n}$ such that the matrix D is diagonal. Let $d_1, d_2, \ldots, d_n$ be the diagonal entries of the diagonal matrix D, so that

$$D = (d_i [i = j])_{1 \leq i \leq n,\ 1 \leq j \leq n} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \in K^{n \times n}.$$

Then,

$$\det(A + D) = \sum_{P \subseteq [n]} \det\left(\operatorname{sub}_P^P A\right) \cdot \prod_{i \in [n] \setminus P} d_i.$$

The minors $\det\left(\operatorname{sub}_P^P A\right)$ of an $n \times n$-matrix A are known as the *principal minors* of A.

Example 6.4.27. For $n = 3$, the claim of Theorem 6.4.26 is

$$\begin{aligned}
&\det(A+D)\\
&= \sum_{P\subseteq[3]} \det\left(\operatorname{sub}_P^P A\right)\cdot \prod_{i\in[3]\setminus P} d_i\\
&= \underbrace{\det\left(\operatorname{sub}_\varnothing^\varnothing A\right)}_{=1}\cdot \underbrace{\prod_{i\in[3]\setminus\varnothing} d_i}_{=d_1d_2d_3} + \underbrace{\det\left(\operatorname{sub}_{\{1\}}^{\{1\}} A\right)}_{=A_{1,1}}\cdot \underbrace{\prod_{i\in[3]\setminus\{1\}} d_i}_{=d_2d_3}\\
&\quad + \underbrace{\det\left(\operatorname{sub}_{\{2\}}^{\{2\}} A\right)}_{=A_{2,2}}\cdot \underbrace{\prod_{i\in[3]\setminus\{2\}} d_i}_{=d_1d_3} + \underbrace{\det\left(\operatorname{sub}_{\{3\}}^{\{3\}} A\right)}_{=A_{3,3}}\cdot \underbrace{\prod_{i\in[3]\setminus\{3\}} d_i}_{=d_1d_2}\\
&\quad + \underbrace{\det\left(\operatorname{sub}_{\{1,2\}}^{\{1,2\}} A\right)}_{=\det\begin{pmatrix} A_{1,1} & A_{1,2}\\ A_{2,1} & A_{2,2}\end{pmatrix}}\cdot \underbrace{\prod_{i\in[3]\setminus\{1,2\}} d_i}_{=d_3} + \underbrace{\det\left(\operatorname{sub}_{\{1,3\}}^{\{1,3\}} A\right)}_{=\det\begin{pmatrix} A_{1,1} & A_{1,3}\\ A_{3,1} & A_{3,3}\end{pmatrix}}\cdot \underbrace{\prod_{i\in[3]\setminus\{1,3\}} d_i}_{=d_2}\\
&\quad + \underbrace{\det\left(\operatorname{sub}_{\{2,3\}}^{\{2,3\}} A\right)}_{=\det\begin{pmatrix} A_{2,2} & A_{2,3}\\ A_{3,2} & A_{3,3}\end{pmatrix}}\cdot \underbrace{\prod_{i\in[3]\setminus\{2,3\}} d_i}_{=d_1} + \underbrace{\det\left(\operatorname{sub}_{\{1,2,3\}}^{\{1,2,3\}} A\right)}_{=\det A}\cdot \underbrace{\prod_{i\in[3]\setminus\{1,2,3\}} d_i}_{\substack{=(\text{empty product})\\ =1}}\\
&= d_1d_2d_3 + A_{1,1}d_2d_3 + A_{2,2}d_1d_3 + A_{3,3}d_1d_2\\
&\quad + \det\begin{pmatrix} A_{1,1} & A_{1,2}\\ A_{2,1} & A_{2,2}\end{pmatrix}\cdot d_3 + \det\begin{pmatrix} A_{1,1} & A_{1,3}\\ A_{3,1} & A_{3,3}\end{pmatrix}\cdot d_2\\
&\quad + \det\begin{pmatrix} A_{2,2} & A_{2,3}\\ A_{3,2} & A_{3,3}\end{pmatrix}\cdot d_1 + \det A.
\end{aligned}$$

Proof of Theorem 6.4.26 (sketched). (See [Grinbe15, Corollary 6.162] for details.) We shall use the notations $\widetilde{I}$ and $\operatorname{sum} S$ as defined in Theorem 6.4.23. If P and Q are two subsets of $[n]$ satisfying $|P| = |Q|$ but $P \neq Q$, then their complements $\widetilde{P}$ and $\widetilde{Q}$ are also distinct (since $P \neq Q$) and satisfy $\left|\widetilde{P}\right| = \left|\widetilde{Q}\right|$ (since $|P| = |Q|$), and therefore Lemma 6.4.25 **(b)** (applied to $\widetilde{P}$ and $\widetilde{Q}$ instead of P and Q) yields

$$\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} D\right) = 0. \qquad (218)$$

Now, Theorem 6.4.23 (applied to $B = D$) yields

$$\begin{aligned}
\det\left(A+D\right) &= \sum_{P\subseteq[n]} \sum_{\substack{Q\subseteq[n];\\ |P|=|Q|}} (-1)^{\operatorname{sum}P+\operatorname{sum}Q} \det\left(\operatorname{sub}_P^Q A\right) \cdot \underbrace{\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} D\right)}_{\substack{\text{This is 0 if } P\neq Q\\ \text{(by (218))}}} \\
&= \sum_{P\subseteq[n]} \underbrace{(-1)^{\operatorname{sum}P+\operatorname{sum}P}}_{=1} \det\left(\operatorname{sub}_P^P A\right) \cdot \underbrace{\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{P}} D\right)}_{\substack{=\prod_{i\in\widetilde{P}} d_i\\ \text{(by Lemma 6.4.25 } \textbf{(a)}\text{)}}} \\
&\qquad \left(\begin{array}{c}\text{here, we have removed all addends with } P\neq Q\\ \text{from the double sum, since these addends are 0}\end{array}\right) \\
&= \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot \prod_{i\in\widetilde{P}} d_i .
\end{aligned}$$

This proves Theorem 6.4.26 (since $\widetilde{P} = [n] \setminus P$). □

As a particular case of Theorem 6.4.26, we quickly obtain the following formula for a class of determinants that frequently appear in graph theory:

Proposition 6.4.28. Let $n \in \mathbb{N}$. Let $d_1, d_2, \ldots, d_n \in K$ and $x \in K$. Let F be the $n \times n$-matrix

$$\left(x + d_i\left[i=j\right]\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} x+d_1 & x & \cdots & x \\ x & x+d_2 & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x+d_n \end{pmatrix} \in K^{n\times n}.$$

Then,

$$\det F = d_1 d_2 \cdots d_n + x \sum_{i=1}^{n} d_1 d_2 \cdots \widehat{d_i} \cdots d_n ,$$

where the hat over the "d_i" means "omit the d_i factor" (that is, the expression "$d_1 d_2 \cdots \widehat{d_i} \cdots d_n$" is to be understood as "$d_1 d_2 \cdots d_{i-1} d_{i+1} d_{i+2} \cdots d_n$").

Proof of Proposition 6.4.28 (sketched). Define the two $n \times n$-matrices

$$A := (x)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} x & x & \cdots & x \\ x & x & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x \end{pmatrix} \in K^{n\times n} \qquad \text{and}$$

$$D := \left(d_i\left[i=j\right]\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \in K^{n\times n}.$$

Then, it is clear that $F = A + D$. Moreover, the matrix D is diagonal, and its diagonal entries are $d_1, d_2, \ldots, d_n$. Hence, Theorem 6.4.26 yields

$$\det(A + D) = \sum_{P \subseteq [n]} \det\left(\operatorname{sub}_P^P A\right) \cdot \prod_{i \in [n] \setminus P} d_i. \tag{219}$$

However, if P is a subset of $[n]$, then $\operatorname{sub}_P^P A$ is a submatrix of A and thus has the form $\begin{pmatrix} x & x & \cdots & x \\ x & x & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x \end{pmatrix}$ (since all entries of A equal x). If the subset P of $[n]$ has size ≥ 2, then this submatrix $\operatorname{sub}_P^P A = \begin{pmatrix} x & x & \cdots & x \\ x & x & \cdots & x \\ \vdots & \vdots & \ddots & \vdots \\ x & x & \cdots & x \end{pmatrix}$ has size $|P| \geq 2$ and therefore has determinant 0 (by (206), applied to $|P|$ instead of n). In other words, we have

$$\det\left(\operatorname{sub}_P^P A\right) = 0 \qquad \text{whenever } P \subseteq [n] \text{ satisfies } |P| \geq 2. \tag{220}$$

Now, (219) becomes

$$\begin{aligned}
\det\left(A+D\right) &= \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right)\cdot\prod_{i\in[n]\setminus P} d_i \\
&= \sum_{\substack{P\subseteq[n];\\ |P|\leq 1}} \det\left(\operatorname{sub}_P^P A\right)\cdot\prod_{i\in[n]\setminus P} d_i + \sum_{\substack{P\subseteq[n];\\ |P|\geq 2}} \underbrace{\det\left(\operatorname{sub}_P^P A\right)}_{\substack{=0\\ \text{(by (220))}}}\cdot\prod_{i\in[n]\setminus P} d_i \\
&\qquad\qquad \left(\text{since each } P\subseteq[n] \text{ satisfies either } |P|\leq 1 \text{ or } |P|\geq 2\right) \\
&= \sum_{\substack{P\subseteq[n];\\ |P|\leq 1}} \det\left(\operatorname{sub}_P^P A\right)\cdot\prod_{i\in[n]\setminus P} d_i \\
&= \underbrace{\det\left(\operatorname{sub}_\varnothing^\varnothing A\right)}_{\substack{=1\\ \text{(since } \operatorname{sub}_\varnothing^\varnothing A \text{ is}\\ \text{a } 0\times 0\text{-matrix)}}}\cdot\underbrace{\prod_{i\in[n]\setminus\varnothing} d_i}_{\substack{=\prod_{i\in[n]} d_i\\ =d_1d_2\cdots d_n}} + \sum_{p=1}^n \underbrace{\det\left(\operatorname{sub}_{\{p\}}^{\{p\}} A\right)}_{\substack{=x\\ \text{(since } \operatorname{sub}_{\{p\}}^{\{p\}} A=\left(\begin{array}{c} x \end{array}\right)\text{)}}}\cdot\underbrace{\prod_{i\in[n]\setminus\{p\}} d_i}_{=d_1d_2\cdots\widehat{d_p}\cdots d_n} \\
&\qquad\qquad \left(\begin{array}{c}\text{since the subsets } P \text{ of } [n] \text{ satisfying } |P|\leq 1\\ \text{are the } n+1 \text{ subsets } \varnothing,\ \{1\},\ \{2\},\ \ldots,\ \{n\}\end{array}\right) \\
&= d_1d_2\cdots d_n + \sum_{p=1}^n x\cdot d_1d_2\cdots\widehat{d_p}\cdots d_n \\
&= d_1d_2\cdots d_n + x\sum_{p=1}^n d_1d_2\cdots\widehat{d_p}\cdots d_n \\
&= d_1d_2\cdots d_n + x\sum_{i=1}^n d_1d_2\cdots\widehat{d_i}\cdots d_n
\end{aligned}$$

(here, we have renamed the summation index p as i). In view of $F = A + D$, this rewrites as

$$\det F = d_1d_2\cdots d_n + x\sum_{i=1}^n d_1d_2\cdots\widehat{d_i}\cdots d_n,$$

Thus, Proposition 6.4.28 is proven.

(See `https://math.stackexchange.com/questions/2110766/` for some different proofs of Proposition 6.4.28.) □

Another application of Theorem 6.4.26 is an explicit formula for the characteristic polynomial of a matrix. We recall that the characteristic polynomial of an $n\times n$-matrix $A\in K^{n\times n}$ is defined to be the polynomial[97] $\det\left(xI_n - A\right)\in K\left[x\right]$ (some authors define it to be $\det\left(A - xI_n\right)$ instead, but this is the same up to sign). This is a polynomial of degree n, whose leading term is x^n, whose

[97] Here, I_n denotes the $n\times n$ identity matrix.

next-highest term is $-\operatorname{Tr} A \cdot x^{n-1}$ where $\operatorname{Tr} A := \sum\limits_{i=1}^{n} A_{i,i}$ is the *trace* of A, and whose constant term is $(-1)^n \det A$. We shall extend this by explicitly computing all coefficients of this polynomial. For the sake of simplicity, we will compute $\det(A + xI_n)$ instead of $\det(xI_n - A)$ (this is tantamount to replacing x by $-x$), and we will take x to be an element of K rather than an indeterminate (but this setting is more general, since we can take K itself to be a polynomial ring and then choose x to be its indeterminate). Here is our formula:

Proposition 6.4.29. Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be an $n \times n$-matrix. Let $x \in K$. Let I_n denote the $n \times n$ identity matrix. Then,

$$\det(A + xI_n) = \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot x^{n-|P|} = \sum_{k=0}^{n} \left(\sum_{\substack{P\subseteq[n];\\ |P|=n-k}} \det\left(\operatorname{sub}_P^P A\right) \right) x^k.$$

Proof of Proposition 6.4.29 (sketched). (See [Grinbe15, Corollary 6.164] for details.) The matrix xI_n is diagonal, and its diagonal entries are $x, x, \ldots, x$; in fact,

$$xI_n = (x[i=j])_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & x \end{pmatrix}.$$

Hence, Theorem 6.4.26 (applied to $D = xI_n$ and $d_i = x$) yields

$$\begin{aligned}
&\det(A + xI_n) \\
&= \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot \underbrace{\prod_{i\in[n]\setminus P} x}_{\substack{=x^{|[n]\setminus P|}=x^{n-|P|} \\ (\text{since } |[n]\setminus P|=|[n]|-|P|=n-|P|)}} = \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot x^{n-|P|} \\
&= \sum_{k=0}^{n} \sum_{\substack{P\subseteq[n];\\ |P|=k}} \det\left(\operatorname{sub}_P^P A\right) x^{n-k} \qquad \left(\begin{array}{c}\text{here, we have split the sum} \\ \text{according to the value of } |P|\end{array}\right) \\
&= \sum_{k=0}^{n} \sum_{\substack{P\subseteq[n];\\ |P|=n-k}} \det\left(\operatorname{sub}_P^P A\right) x^{k} \qquad \left(\begin{array}{c}\text{here, we have substituted } n-k \\ \text{for } k \text{ in the sum}\end{array}\right) \\
&= \sum_{k=0}^{n} \left(\sum_{\substack{P\subseteq[n];\\ |P|=n-k}} \det\left(\operatorname{sub}_P^P A\right) \right) x^k.
\end{aligned}$$

Proposition 6.4.29 is proven. □

6.4.5. Factoring the matrix

Next, we will see some tricks for computing determinants.

Let us compute a determinant that recently went viral on the internet after Timothy Gowers livestreamed himself computing it[98] ([Grinbe15, Exercise 6.11], [EdeStr04]):

Proposition 6.4.30. Let $n \in \mathbb{N}$. Let A be the $n \times n$-matrix

$$\left(\binom{i+j-2}{i-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \begin{pmatrix} \binom{0}{0} & \binom{1}{0} & \cdots & \binom{n-1}{0} \\ \binom{1}{1} & \binom{2}{1} & \cdots & \binom{n}{1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{n-1}{n-1} & \binom{n}{n-1} & \cdots & \binom{2n-2}{n-1} \end{pmatrix}.$$

(For example, for $n = 4$, we have $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}$.)

Then, $\det A = 1$.

There are many ways to prove Proposition 6.4.30, but here is a particularly simple one:

Proof of Proposition 6.4.30 (sketched). (See [Grinbe15, Exercise 6.11] for details.)

[98] See `https://www.youtube.com/watch?v=byjhpzEoXFs` and `https://www.youtube.com/watch?v=frvBdaqLgLo` and `https://www.youtube.com/watch?v=m8R9rVbOM5o` .

For any $i, j \in [n]$, we have

$$\begin{aligned}
A_{i,j} &= \dbinom{i+j-2}{i-1} \qquad \text{(by the definition of } A\text{)} \\
&= \dbinom{(i-1)+(j-1)}{i-1} = \dbinom{(i-1)+(j-1)}{j-1} \qquad \text{(by Theorem 2.0.6)} \\
&= \sum_{k=0}^{i-1} \dbinom{i-1}{k} \underbrace{\dbinom{j-1}{j-1-k}}_{\substack{=\dbinom{j-1}{k} \\ \text{(by Theorem 2.0.6)}}} \\
&\qquad \left(\begin{array}{c}\text{by Proposition 3.2.19, applied to } i-1,\ j-1 \text{ and } j-1 \\ \text{instead of } a,\ b \text{ and } n\end{array}\right) \\
&= \sum_{k=0}^{i-1} \dbinom{i-1}{k} \dbinom{j-1}{k} = \sum_{k=0}^{n-1} \dbinom{i-1}{k} \dbinom{j-1}{k} \\
&\qquad \left(\begin{array}{c}\text{here, we extended the sum upwards to } k = n-1, \\ \text{but this has not changed the value of the sum,} \\ \text{since all newly introduced addends are } 0 \\ \text{(since } \dbinom{i-1}{k} = 0 \text{ whenever } k > i-1\text{)}\end{array}\right) \\
&= \sum_{k=1}^{n} \dbinom{i-1}{k-1} \dbinom{j-1}{k-1} \\
&\qquad \text{(here, we have substituted } k-1 \text{ for } k \text{ in the sum)}.
\end{aligned}$$

If we define two $n \times n$-matrices

$$L := \left(\dbinom{i-1}{k-1} \right)_{1 \leq i \leq n,\ 1 \leq k \leq n} \qquad \text{and} \qquad U := \left(\dbinom{j-1}{k-1} \right)_{1 \leq k \leq n,\ 1 \leq j \leq n},$$

then this rewrites as

$$A_{i,j} = \sum_{k=1}^{n} L_{i,k} U_{k,j} = (LU)_{i,j}$$

(by the definition of the matrix product LU). Since this equality holds for all $i, j \in [n]$, we thus conclude that $A = LU$.

Notice, however, that the matrix L is lower-triangular (because if $i < k$, then $i - 1 < k - 1$ and therefore $L_{i,k} = \dbinom{i-1}{k-1} = 0$), and thus (by Theorem 6.4.11) its determinant is the product of its diagonal entries. In other words,

$$\det L = \dbinom{1-1}{1-1} \dbinom{2-1}{2-1} \cdots \dbinom{n-1}{n-1} = \prod_{k=1}^{n} \underbrace{\dbinom{k-1}{k-1}}_{=1} = 1.$$

Similarly, the matrix U is upper-triangular, and its determinant is $\det U = 1$ as well.

Now, from $A = LU$, we obtain

$$\begin{aligned} \det A &= \det(LU) = \underbrace{\det L}_{=1} \cdot \underbrace{\det U}_{=1} \qquad \text{(by Theorem 6.4.16)} \\ &= 1; \end{aligned}$$

this proves Proposition 6.4.30. □

How can you discover such a proof? Our serendipitous factorization of A as LU might appear unmotivated, but from the viewpoint of linear algebra it is an instance of a well-known and well-understood kind of factorization, known as the *LU-decomposition* or the *LU-factorization*. Over a field, almost every square matrix[99] has an LU-decomposition (i.e., a factorization as a product of a lower-triangular matrix with an upper-triangular matrix). This LU-decomposition is unique if you require (e.g.) the diagonal entries of the lower-triangular factor to all equal 1. It can furthermore be algorithmically computed using Gaussian elimination (see, e.g., [OlvSha18, §1.3, Theorem 1.3]). Now, computing the LU-decomposition of the matrix A from Proposition 6.4.30 for $n = 4$, we find

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix}}_{\text{this is the lower-triangular factor}} \underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{\text{this is the upper-triangular factor}} .$$

The entries of both factors appear to be the binomial coefficients familiar from Pascal's triangle. This suggests that we might have

$$L = \left(\dbinom{i-1}{k-1} \right)_{1 \le i \le n,\ 1 \le k \le n} \qquad \text{and} \qquad U = \left(\dbinom{j-1}{k-1} \right)_{1 \le k \le n,\ 1 \le j \le n},$$

not just for $n = 4$ but also for arbitrary $n \in \mathbb{N}$. And once this guess has been made, it is easy to prove that $A = LU$ (our proof above is not the only one possible; four proofs appear in [EdeStr04]).

This is not the only example where LU-decomposition helps compute a determinant (see, e.g., [Kratte99, §2.6] for examples). Sometimes it is helpful to transpose a matrix, or to permute its rows or columns to obtain a matrix with a good LU-decomposition.

6.4.6. Factor hunting

The next trick – known as *factor hunting* – works not only for determinants; however, determinants provide some of the simplest examples.

[99] I will not go into details as to what "almost every" means here.

Theorem 6.4.31 (Vandermonde determinant)**.** Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be n elements of K. Then:

(a) We have

$$\det\left(\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n}\left(a_i - a_j\right).$$

(b) We have

$$\det\left(\left(a_j^{n-i}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n}\left(a_i - a_j\right).$$

(c) We have

$$\det\left(\left(a_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq j<i\leq n}\left(a_i - a_j\right).$$

(d) We have

$$\det\left(\left(a_j^{i-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq j<i\leq n}\left(a_i - a_j\right).$$

Example 6.4.32. Here is what the four parts of Theorem 6.4.31 say for $n = 3$:

(a) We have $\det\begin{pmatrix} a_1^2 & a_1 & 1 \\ a_2^2 & a_2 & 1 \\ a_3^2 & a_3 & 1 \end{pmatrix} = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$.

(b) We have $\det\begin{pmatrix} a_1^2 & a_2^2 & a_3^2 \\ a_1 & a_2 & a_3 \\ 1 & 1 & 1 \end{pmatrix} = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$.

(c) We have $\det\begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ 1 & a_3 & a_3^2 \end{pmatrix} = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)$.

(d) We have $\det\begin{pmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix} = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)$.

Theorem 6.4.31 is a classical and important result, known as the *Vandermonde determinant*. Many different proofs are known (see, e.g., [Grinbe15, Theorem 6.46] or [Aigner07, §5.3] or [Bourba74, Section III.8.6, Example (1)] or [Grinbe10, Theorem 1]; a combinatorial proof can also be found in Exercise A.5.3.6; two more proofs are obtained in Exercise A.5.3.8 and Exercise A.5.3.9). We will now sketch a proof using factor hunting and polynomials. We will first focus on proving part **(a)** of Theorem 6.4.31, and afterwards derive the other parts from it.

The first step of our proof is reducing Theorem 6.4.31 **(a)** to the "particular case" in which K is the polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ and the elements $a_1, a_2, \ldots, a_n$ are the indeterminates $x_1, x_2, \ldots, x_n$. This is merely a particular case (one possible choice of K and $a_1, a_2, \ldots, a_n$ among many); however, as we will soon see, proving Theorem 6.4.31 **(a)** in this particular case will quickly entail that Theorem 6.4.31 **(a)** holds in the general case. Let us elaborate on this argument. First, let us state Theorem 6.4.31 **(a)** in this particular case as a lemma:

> **Lemma 6.4.33.** Let $n \in \mathbb{N}$. Consider the polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ in n indeterminates $x_1, x_2, \ldots, x_n$ with integer coefficients. In this ring, we have
>
> $$\det\left(\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n} \left(x_i - x_j\right). \tag{221}$$

We can derive Theorem 6.4.31 **(a)** from Lemma 6.4.33 as follows:

*Proof of Theorem 6.4.31 **(a)** using Lemma 6.4.33.* The equality

$$\det\left(\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n} \left(a_i - a_j\right) \tag{222}$$

follows from the equality (221) by substituting $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$.

This is sufficiently clear to be considered a complete proof, but just in case, here are a few details.

We can substitute $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$ in any polynomial $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, since $a_1, a_2, \ldots, a_n$ are n elements of a commutative ring (namely, of K). It is obvious that $\prod\limits_{1\leq i<j\leq n} \left(x_i - x_j\right)$ becomes $\prod\limits_{1\leq i<j\leq n} \left(a_i - a_j\right)$ when we substitute $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$. It is perhaps a bit less obvious that $\det\left(\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)$ becomes $\det\left(\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)$ when we substitute $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$. To convince our skeptical selves of this, we expand both determinants: The definition of the determinant yields

$$\det\left(\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \sum_{\sigma\in S_n} (-1)^\sigma x_1^{n-\sigma(1)} x_2^{n-\sigma(2)} \cdots x_n^{n-\sigma(n)} \qquad \text{and}$$
$$\det\left(\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \sum_{\sigma\in S_n} (-1)^\sigma a_1^{n-\sigma(1)} a_2^{n-\sigma(2)} \cdots a_n^{n-\sigma(n)},$$

and it is clear that substituting $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$ transforms $\sum\limits_{\sigma\in S_n} (-1)^\sigma x_1^{n-\sigma(1)} x_2^{n-\sigma(2)} \cdots x_n^{n-\sigma(n)}$ into $\sum\limits_{\sigma\in S_n} (-1)^\sigma a_1^{n-\sigma(1)} a_2^{n-\sigma(2)} \cdots a_n^{n-\sigma(n)}$.

Thus, (222) follows from (221). In other words, Theorem 6.4.31 **(a)** follows from Lemma 6.4.33. □

Arguments like the one we just used are frequently applied in algebra; see [Conrad-UI] for some more examples.

It now remains to prove Lemma 6.4.33.

Proof of Lemma 6.4.33 (sketched). We set

$$f := \det\left(\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) \qquad \text{and} \qquad g := \prod_{1\leq i<j\leq n}\left(x_i - x_j\right).$$

Thus, we must prove that $f = g$.

We have

$$\begin{aligned} f &= \det\left(\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) \\ &= \sum_{\sigma\in S_n}(-1)^{\sigma}\, x_1^{n-\sigma(1)}x_2^{n-\sigma(2)}\cdots x_n^{n-\sigma(n)} \end{aligned} \tag{223}$$

(by the definition of a determinant). The right hand side of this equality is a homogeneous polynomial in $x_1, x_2, \ldots, x_n$ of degree $\dfrac{n(n-1)}{2}$ [100]. Thus, f is a homogeneous polynomial in $x_1, x_2, \ldots, x_n$ of degree $\dfrac{n(n-1)}{2}$. Furthermore, the monomial $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$ appears with coefficient 1 on the right hand side of (223) (indeed, all the $n!$ addends in the sum on this right hand side contain distinct monomials, and thus only the addend for $\sigma = \operatorname{id}$ makes any contribution to the coefficient of the monomial $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$). Hence,

$$\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right] f = 1. \tag{224}$$

Therefore, $f \neq 0$.

[100] because it is a $\mathbb{Z}$-linear combination of the monomials $x_1^{n-\sigma(1)}x_2^{n-\sigma(2)}\cdots x_n^{n-\sigma(n)}$, each of which has degree

$$\begin{aligned} (n-\sigma(1)) + (n-\sigma(2)) + \cdots + (n-\sigma(n)) &= n\cdot n - \underbrace{(\sigma(1)+\sigma(2)+\cdots+\sigma(n))}_{\substack{=1+2+\cdots+n \\ \text{(since } \sigma \text{ is a permutation of } [n])}} \\ &= n\cdot n - \underbrace{(1+2+\cdots+n)}_{=\frac{n(n+1)}{2}} = n\cdot n - \frac{n(n+1)}{2} \\ &= \frac{n(n-1)}{2} \end{aligned}$$

Now, let u and v be two elements of $[n]$ satisfying $u < v$. Then, the polynomial f becomes 0 when we set x_u equal to x_v (that is, when we substitute x_v for x_u). Indeed, when we set x_u equal to x_v, the matrix $\left(x_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ becomes a matrix that has two equal rows (namely, its u-th and its v-th row both become equal to $\left(x_v^{n-1}, x_v^{n-2}, \ldots, x_v^{n-n}\right)$), and thus its determinant becomes 0 (by Theorem 6.4.12 **(c)**); but this means precisely that $f = 0$ (since f is the determinant of this matrix).

Now, we recall the following well-known property of univariate polynomials:

> *Root factoring-off theorem:* Let R be a commutative ring. Let $p \in R[t]$ be a univariate polynomial that has a root $r \in R$. Then, this polynomial p is divisible by $t - r$ (in the ring $R[t]$).

Using this property, we can easily see that if a polynomial $p \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ becomes 0 when we set x_u equal to x_v, then this polynomial p is a multiple of $x_u - x_v$ (in the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$). (Indeed, viewing p as a polynomial in the single indeterminate x_u over the ring $\mathbb{Z}[x_1, x_2, \ldots, \widehat{x_u}, \ldots, x_n]$ [101], we see that x_v is a root of p, and therefore the root factoring-off theorem yields that p is divisible by $x_u - x_v$. [102])

Applying this observation to $p = f$, we conclude that f is a multiple of $x_u - x_v$ (in the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$), since we know that f becomes 0 when we set x_u equal to x_v.

Forget that we fixed u and v. We thus have shown that f is a multiple of $x_u - x_v$ (in the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$) whenever u and v are two elements of $[n]$ satisfying $u < v$. In other words, f is a multiple of each of the linear polynomials

$$\begin{array}{cccc} x_1 - x_2, & x_1 - x_3, & \ldots, & x_1 - x_n, \\ & x_2 - x_3, & \ldots, & x_2 - x_n, \\ & & \ddots & \vdots \\ & & & x_{n-1} - x_n \end{array}$$

(in the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$). However, these linear polynomials are irreducible[103]

[101] The meaning of the hat over the "x_u" is as in Proposition 6.4.28: It signifies that the entry x_u is omitted from the list (that is, "$x_1, x_2, \ldots, \widehat{x_u}, \ldots, x_n$" means "$x_1, x_2, \ldots, x_{u-1}, x_{u+1}, x_{u+2}, \ldots, x_n$").

[102] Here, we are tacitly using the canonical isomorphism between the polynomial rings

$$\mathbb{Z}[x_1, x_2, \ldots, x_n] \qquad \text{and} \qquad (\mathbb{Z}[x_1, x_2, \ldots, \widehat{x_u}, \ldots, x_n])[x_u].$$

This isomorphism allows us to treat multivariate polynomials in $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ as univariate polynomials in the indeterminate x_u over the ring $\mathbb{Z}[x_1, x_2, \ldots, \widehat{x_u}, \ldots, x_n]$, and vice versa (and ensures that the notion of divisibility does not change between the former and the latter).

[103] Check this! (Actually, any linear polynomial over $\mathbb{Z}$ is irreducible if the gcd of its coefficients is 1.)

and mutually non-associate (i.e., no two of them are associate[104])[105]. Since the ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ is a unique factorization domain[106], we thus conclude that any polynomial $p \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ that is a multiple of each of these linear polynomials must necessarily be a multiple of their product $\prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$. Hence, the polynomial f must be a multiple of this product $\prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$ (since f is a multiple of each of the linear polynomials above). In other words, the polynomial f must be a multiple of g (since $g = \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$). In other words, $f = gq$ for some $q \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$. Consider this q. Clearly, $gq = f \neq 0$ and thus $q \neq 0$ and $g \neq 0$.

The ring $\mathbb{Z}$ is an integral domain. Thus, any two nonzero polynomials a and b over $\mathbb{Z}$ satisfy $\deg(ab) = \deg a + \deg b$. Applying this to $a = g$ and $b = q$, we find $\deg(gq) = \deg g + \deg q$. In other words, $\deg f = \deg g + \deg q$ (since $gq = f$).

Now, $g = \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$ and thus

$$\deg g = \deg \left(\prod_{1 \leq i < j \leq n} (x_i - x_j) \right) = \sum_{1 \leq i < j \leq n} \underbrace{\deg (x_i - x_j)}_{=1} = \sum_{1 \leq i < j \leq n} 1$$
$$= \left(\text{\# of pairs } (i,j) \in [n]^2 \text{ satisfying } i < j \right) = \binom{n}{2} = \frac{n(n-1)}{2}.$$

However, we have $\deg f \leq \dfrac{n(n-1)}{2}$ (since f is a homogeneous polynomial of degree $\dfrac{n(n-1)}{2}$). In view of $\deg g = \dfrac{n(n-1)}{2}$, this rewrites as $\deg f \leq \deg g$. Hence,

$$\deg g \geq \deg f = \deg g + \deg q.$$

Therefore, $0 \geq \deg q$. This shows that the polynomial q is constant. In other words, $q \in \mathbb{Z}$.

It remains to show that this constant q is 1. However, this can be done by comparing some coefficients of f and g. Indeed, let us look at the coefficient of $x_1^{n-1} x_2^{n-2} \cdots x_n^{n-n}$ (as we already know this coefficient for f to be 1).

Expanding the product $\prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$, we obtain a sum of several (in fact, $2^{n(n-1)/2}$ many) monomials with + and − signs. I claim that among these

[104] Recall that two elements a and b of a principal ideal domain R are said to be *associate* if there exists some unit u of R such that $a = ub$. Being associate is known (and easily verified) to be an equivalence relation.

[105] Check this! (Recall that the only units of the polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ are 1 and -1.)

[106] This is a nontrivial, but rather well-known result in abstract algebra. Proofs can be found in [Ford21, Theorem 3.7.4], [Knapp16, Remark after Corollary 8.21], [MiRiRu87, Chapter IV, Theorems 4.8 and 4.9] and [Edward05, Essay 1.4, Corollary of Theorem 1 and Corollary 1 of Theorem 2].

monomials, the monomial $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$ will appear exactly once, and with a $+$ sign. Indeed, in order to obtain $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$ when expanding the product

$$\begin{array}{llllll}\prod\limits_{1\leq i<j\leq n}\left(x_i-x_j\right)= & (x_1-x_2) & (x_1-x_3) & \cdots & (x_1-x_n) & \\ & & (x_2-x_3) & \cdots & (x_2-x_n) & \\ & & & \ddots & \vdots & \\ & & & & (x_{n-1}-x_n), & \end{array}$$

it is necessary to pick the x_1 minuends from all $n-1$ factors in the first row (since none of the other factors contain any x_1), then to pick the x_2 minuends from all $n-2$ factors in the second row (since none of the remaining factors contain any x_2), and so on – i.e., to take the minuend (rather than the subtrahend) from each factor. Thus, only one of the monomials obtained by the expansion will be $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$, and it will appear with a $+$ sign. Hence, the coefficient of $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$ in the product $\prod\limits_{1\leq i<j\leq n}\left(x_i-x_j\right)$ is 1. In other words, the coefficient of $x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}$ in g is 1 (since $g=\prod\limits_{1\leq i<j\leq n}\left(x_i-x_j\right)$). In other words,

$$\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right]g=1.$$

Now, recall that $f=gq$. Hence,

$$\begin{aligned}\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right]f&=\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right](gq)\\&=q\cdot\underbrace{\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right]g}_{=1}\qquad\text{(since } q\in\mathbb{Z}\text{)}\\&=q,\end{aligned}$$

so that $q=\left[x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}\right]f=1$ (by (224)). Hence, $f=g\underbrace{q}_{=1}=g$. As we said, this completes the proof of Lemma 6.4.33. □

The technique used in the above proof of Lemma 6.4.33 may appear somewhat underhanded: Instead of computing our polynomial f upfront, we have kept lopping off linear factors from it until a constant polynomial remained (for degree reasons). This technique is called *identification of factors* or *factor hunting*, and is used in various different places, but particularly often in the computation of determinants (multiple examples are given in [Kratte99, §2.4 and further below]). While I consider it to be aesthetically inferior to sufficiently direct approaches, it has shown to be useful in situations in which no direct approaches are known to work.

Proof of Theorem 6.4.31 (sketched). **(a)** We have already given a proof of Theorem 6.4.31 **(a)** (and with Lemma 6.4.33 established, this proof is now complete).

(b) The matrix $\left(a_j^{n-i}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ is the transpose of the matrix $\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$. Thus, Theorem 6.4.31 **(b)** follows from Theorem 6.4.31 **(a)** using Theorem 6.4.10.

(c) Let A be the $n\times n$-matrix $\left(a_i^{n-j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$. Then, Theorem 6.4.31 **(a)** says that $\det A = \prod\limits_{1\leq i<j\leq n}\left(a_i - a_j\right)$.

Let $\tau\in S_n$ be the permutation of $[n]$ that sends each $j\in[n]$ to $n+1-j$. Then, each $i,j\in[n]$ satisfy $j-1 = n-\tau(j)$ and therefore

$$a_i^{j-1} = a_i^{n-\tau(j)} = A_{i,\tau(j)} \qquad \text{(by the definition of } A\text{)}.$$

Hence, $\left(a_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n} = \left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ and thus

$$\det\left(\left(a_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \det\left(\left(A_{i,\tau(j)}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = (-1)^\tau\cdot\det A$$

(by (209)).

However, the permutation τ has OLN $(n, n-1, n-2, \ldots, 1)$. Thus, each pair $(i,j)\in[n]^2$ satisfying $i<j$ is an inversion of τ. Therefore, the Coxeter length $\ell(\tau)$ of τ is the # of all pairs $(i,j)\in[n]^2$ satisfying $i<j$. Thus, the sign of τ is

$$\begin{aligned}(-1)^\tau &= (-1)^{\ell(\tau)} \qquad \text{(by the definition of the sign of a permutation)}\\ &= (-1)^{\left(\#\text{ of all pairs } (i,j)\in[n]^2 \text{ satisfying } i<j\right)}\\ &\qquad\qquad \left(\text{since } \ell(\tau) \text{ is the \# of all pairs } (i,j)\in[n]^2 \text{ satisfying } i<j\right)\\ &= \prod_{1\leq i<j\leq n}(-1).\end{aligned}$$

Now,

$$\begin{aligned}&\det\left(\left(a_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)\\ &= \underbrace{(-1)^\tau}_{=\prod\limits_{1\leq i<j\leq n}(-1)}\cdot\underbrace{\det A}_{=\prod\limits_{1\leq i<j\leq n}\left(a_i-a_j\right)} = \left(\prod_{1\leq i<j\leq n}(-1)\right)\cdot\left(\prod_{1\leq i<j\leq n}\left(a_i-a_j\right)\right)\\ &= \prod_{1\leq i<j\leq n}\underbrace{\left((-1)\left(a_i-a_j\right)\right)}_{=a_j-a_i} = \prod_{1\leq i<j\leq n}\left(a_j-a_i\right) = \prod_{1\leq j<i\leq n}\left(a_i-a_j\right)\end{aligned}$$

(here, we have renamed the index (i,j) as (j,i) in the product). This proves Theorem 6.4.31 **(c)**.

(d) The matrix $\left(a_j^{i-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ is the transpose of the matrix $\left(a_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$. Thus, Theorem 6.4.31 **(d)** follows from Theorem 6.4.31 **(c)** using Theorem 6.4.10. □

The Vandermonde determinant is itself a useful tool in the computation of various other determinants. Here is an example:

Proposition 6.4.34. Let $n \in \mathbb{N}$. Let $x_1, x_2, \ldots, x_n \in K$ and $y_1, y_2, \ldots, y_n \in K$. Then,

$$\begin{aligned}
&\det\left(\left(\left(x_i+y_j\right)^{n-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)\\
&= \det\begin{pmatrix} (x_1+y_1)^{n-1} & (x_1+y_2)^{n-1} & \cdots & (x_1+y_n)^{n-1} \\ (x_2+y_1)^{n-1} & (x_2+y_2)^{n-1} & \cdots & (x_2+y_n)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (x_n+y_1)^{n-1} & (x_n+y_2)^{n-1} & \cdots & (x_n+y_n)^{n-1} \end{pmatrix}\\
&= \left(\prod_{k=0}^{n-1}\binom{n-1}{k}\right)\left(\prod_{1\leq i<j\leq n}\left(x_i-x_j\right)\right)\left(\prod_{1\leq i<j\leq n}\left(y_j-y_i\right)\right).
\end{aligned}$$

First proof of Proposition 6.4.34 (sketched). Here is a rough outline of a proof that uses factor hunting (in the same way as in our above proofs of Theorem 6.4.31 **(a)** and Lemma 6.4.33). We WLOG assume that $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are distinct indeterminates in a polynomial ring over $\mathbb{Z}$. (This is again an assumption that we can make, because the argument that we used to derive Theorem 6.4.31 **(a)** from Lemma 6.4.33 can be applied here as well.) Then, we can easily see that

$$\det\left(\left(\left(x_i+y_j\right)^{n-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)$$

is a homogeneous polynomial of degree $n(n-1)$. This polynomial vanishes if we set any x_u equal to any x_v (for $u < v$), and also vanishes if we set any y_u equal to any y_v (for $u < v$). Thus we have identified $n(n-1)$ linear factors of this polynomial (namely, the differences $x_u - x_v$ and $y_v - y_u$ for $u < v$), and we can again conclude (since any polynomial ring over $\mathbb{Z}$ is a unique factorization domain) that

$$\det\left(\left(\left(x_i+y_j\right)^{n-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \left(\prod_{1\leq i<j\leq n}\left(x_i-x_j\right)\right)\left(\prod_{1\leq i<j\leq n}\left(y_j-y_i\right)\right)\cdot q$$

for a constant $q \in \mathbb{Z}$. It remains to prove that this constant q equals $\prod\limits_{k=0}^{n-1}\binom{n-1}{k}$. This can be done by studying the coefficients of the monomial

$$x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}y_1^0y_2^1\cdots y_n^{n-1}$$

in $\det\left(\left(\left(x_i+y_j\right)^{n-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)$ and in $\left(\prod_{1\leq i<j\leq n}\left(x_i-x_j\right)\right)\left(\prod_{1\leq i<j\leq n}\left(y_j-y_i\right)\right)$. We leave the details to the reader. □

Second proof of Proposition 6.4.34. (See [Grinbe15, Exercise 6.17 **(b)**] for details.) Let

$$C:=\left(\left(x_i+y_j\right)^{n-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\in K^{n\times n}.$$

For any $i,j\in[n]$, we have

$$\begin{aligned}C_{i,j}&=\left(x_i+y_j\right)^{n-1}=\sum_{k=0}^{n-1}\binom{n-1}{k}x_i^k y_j^{n-1-k}\qquad\text{(by the binomial formula)}\\&=\sum_{k=1}^{n}\binom{n-1}{k-1}x_i^{k-1}y_j^{n-k}\end{aligned}$$

(here, we have substituted $k-1$ for k in the sum). If we define two $n\times n$-matrices P and Q by

$$P:=\left(\binom{n-1}{k-1}x_i^{k-1}\right)_{1\leq i\leq n,\ 1\leq k\leq n}\qquad\text{and}\qquad Q:=\left(y_j^{n-k}\right)_{1\leq k\leq n,\ 1\leq j\leq n},$$

then we can rewrite this as

$$C_{i,j}=\sum_{k=1}^{n}P_{i,k}Q_{k,j}=\left(PQ\right)_{i,j}$$

(by the definition of the matrix product). Since this holds for all $i,j\in[n]$, we thus obtain $C=PQ$. Hence,

$$\det C=\det\left(PQ\right)=\det P\cdot\det Q\tag{225}$$

(by Theorem 6.4.16). It now remains to compute $\det P$ and $\det Q$.

From $Q=\left(y_j^{n-k}\right)_{1\leq k\leq n,\ 1\leq j\leq n}=\left(y_j^{n-i}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$, we obtain

$$\det Q=\det\left(\left(y_j^{n-i}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\prod_{1\leq i<j\leq n}\left(y_i-y_j\right)\tag{226}$$

(by Theorem 6.4.31 **(b)**, applied to $a_i=y_i$).

From $P=\left(\binom{n-1}{k-1}x_i^{k-1}\right)_{1\leq i\leq n,\ 1\leq k\leq n}=\left(\binom{n-1}{j-1}x_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$, we obtain

$$\begin{aligned}
\det P &= \det \left(\left(\binom{n-1}{j-1} x_i^{j-1} \right)_{1\leq i\leq n,\ 1\leq j\leq n} \right) \\
&= \underbrace{\binom{n-1}{1-1}\binom{n-1}{2-1}\cdots\binom{n-1}{n-1}}_{=\prod\limits_{k=0}^{n-1}\binom{n-1}{k}} \cdot \underbrace{\det\left(\left(x_i^{j-1} \right)_{1\leq i\leq n,\ 1\leq j\leq n} \right)}_{\substack{=\prod\limits_{1\leq j<i\leq n}(x_i-x_j) \\ \text{(by Theorem 6.4.31 \textbf{(c)},} \\ \text{applied to } a_i=x_i)}} \\
&\qquad \left(\begin{array}{c} \text{by (214), applied to } A = \left(x_i^{j-1} \right)_{1\leq i\leq n,\ 1\leq j\leq n} \\ \text{and } d_i = \dbinom{n-1}{i-1} \end{array} \right) \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \cdot \prod_{1\leq j<i\leq n} (x_i - x_j) \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \cdot \prod_{1\leq i<j\leq n} (x_j - x_i) \qquad (227)
\end{aligned}$$

(here, we have renamed the index (j,i) as (i,j) in the second product).

Now, (225) becomes

$$\begin{aligned}
\det C &= \det P \cdot \det Q \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \cdot \left(\prod_{1\leq i<j\leq n} (x_j - x_i) \right) \cdot \prod_{1\leq i<j\leq n} (y_i - y_j) \\
&\qquad \text{(by (227) and (226))} \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \cdot \prod_{1\leq i<j\leq n} \underbrace{\left((x_j - x_i)(y_i - y_j) \right)}_{=(x_i-x_j)(y_j-y_i)} \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \cdot \prod_{1\leq i<j\leq n} \left((x_i - x_j)(y_j - y_i) \right) \\
&= \left(\prod_{k=0}^{n-1} \binom{n-1}{k} \right) \left(\prod_{1\leq i<j\leq n} (x_i - x_j) \right) \left(\prod_{1\leq i<j\leq n} (y_j - y_i) \right).
\end{aligned}$$

This proves Proposition 6.4.34 (since $C = \left((x_i + y_j)^{n-1} \right)_{1\leq i\leq n,\ 1\leq j\leq n}$). □

6.4.7. Laplace expansion

Let us next recall another fundamental property of determinants: *Laplace expansion*. We will use the following notation:

Convention 6.4.35. Let $n \in \mathbb{N}$. Let A be an $n \times n$-matrix. Let $i, j \in [n]$. Then, we set

$$A_{\sim i, \sim j} := \operatorname{sub}_{[n] \setminus \{i\}}^{[n] \setminus \{j\}} A \qquad \text{(using the notation from Definition 6.4.21)}.$$

This is the $(n-1) \times (n-1)$-matrix obtained from A by removing its i-th row and its j-th column.

Example 6.4.36. If $A = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$, then $A_{\sim 1, \sim 2} = \begin{pmatrix} a' & c' \\ a'' & c'' \end{pmatrix}$.

Now, we can state the theorem underlying Laplace expansion:

Theorem 6.4.37. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix.

(a) For every $p \in [n]$, we have

$$\det A = \sum_{q=1}^{n} (-1)^{p+q} A_{p,q} \det \left(A_{\sim p, \sim q} \right).$$

(b) For every $q \in [n]$, we have

$$\det A = \sum_{p=1}^{n} (-1)^{p+q} A_{p,q} \det \left(A_{\sim p, \sim q} \right).$$

Note that some authors denote the minors $\det \left(A_{\sim p, \sim q} \right)$ in Theorem 6.4.37 by $A_{p,q}$. This is, of course, totally incompatible with our notations.

Proof of Theorem 6.4.37. See [Grinbe15, Theorem 6.82] or [Ford21, Lemma 4.5.7] or [Laue15, 5.8 and 5.8′] or [Strick13, Proposition B.24 and Proposition B.25] or [Loehr11, Theorem 9.48]. □

Theorem 6.4.37 yields several ways to compute the determinant of a matrix[107]. When we compute a determinant $\det A$ using Theorem 6.4.37 **(a)**, we say that we *expand this determinant along the p-th row*. When we compute a determinant $\det A$ using Theorem 6.4.37 **(b)**, we say that we *expand this determinant along the q-th column*.

Theorem 6.4.37 has many applications, some of which you have probably seen in your course on linear algebra. (A few might appear on the homework.) The main theoretical application of Theorem 6.4.37 is the concept of the *adjugate* (or *classical adjoint*) of a matrix, which we shall introduce in a few moments.

[107] In fact, some authors use Theorem 6.4.37 as a **definition** of the determinant. (However, this is somewhat tricky, as it requires proving that all the values obtained for $\det A$ by applying Theorem 6.4.37 are actually equal.)

First, let us see what happens if we replace the $A_{p,q}$ in Theorem 6.4.37 by entries from another row or another column. In fact, the respective sums become 0 (instead of $\det A$), as the following proposition shows:

Proposition 6.4.38. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Let $r \in [n]$.

(a) For every $p \in [n]$ satisfying $p \neq r$, we have

$$0 = \sum_{q=1}^{n} (-1)^{p+q} A_{r,q} \det \left(A_{\sim p, \sim q} \right).$$

(b) For every $q \in [n]$ satisfying $q \neq r$, we have

$$0 = \sum_{p=1}^{n} (-1)^{p+q} A_{p,r} \det \left(A_{\sim p, \sim q} \right).$$

Proof. See [Grinbe15, Proposition 6.96]. This is also implicit in [Strick13, proof of Proposition B.28] and [Loehr11, proof of Theorem 9.50].

Here is a sketch of the proof:

(a) Let $p \in [n]$ satisfy $p \neq r$. Let C be the matrix A with its p-th row replaced by its r-th row. Then, the matrix C has two equal rows, so that $\det C = 0$ (by Theorem 6.4.12 **(c)**). On the other hand, expanding $\det C$ along the p-th row (i.e., applying Theorem 6.4.37 **(a)** to C instead of A) yields

$$\det C = \sum_{q=1}^{n} (-1)^{p+q} \underbrace{C_{p,q}}_{=A_{r,q}} \det \underbrace{\left(C_{\sim p, \sim q} \right)}_{=A_{\sim p, \sim q}} = \sum_{q=1}^{n} (-1)^{p+q} A_{r,q} \det \left(A_{\sim p, \sim q} \right).$$

Comparing these two equalities, we obtain the claim of Proposition 6.4.38 **(a)**. A similar argument proves Proposition 6.4.38 **(b)**. □

We can now define the adjugate of a matrix:

Definition 6.4.39. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. We define a new $n \times n$-matrix $\operatorname{adj} A \in K^{n \times n}$ by

$$\operatorname{adj} A = \left((-1)^{i+j} \det \left(A_{\sim j, \sim i} \right) \right)_{1 \leq i \leq n,\ 1 \leq j \leq n}.$$

This matrix $\operatorname{adj} A$ is called the *adjugate* of the matrix A. (Some older texts call it the *adjoint*, but this name has since been conquered by a different notion. As a compromise, some still call $\operatorname{adj} A$ the *classical adjoint* of A.)

Example 6.4.40. The adjugate of the 0×0-matrix is the 0×0-matrix.

The adjugate of a 1×1-matrix $\begin{pmatrix} a \end{pmatrix}$ is $\operatorname{adj} \begin{pmatrix} a \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}$.

The adjugate of a 2×2-matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is

$$\operatorname{adj}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

The adjugate of a 3×3-matrix $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ is

$$\operatorname{adj}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} ei - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - ge & bg - ah & ae - bd \end{pmatrix}.$$

The main property of the adjugate $\operatorname{adj} A$ is its connection to the inverse A^{-1} of a matrix A. Indeed, if an $n \times n$-matrix A is invertible, then its inverse A^{-1} is $\dfrac{1}{\det A} \cdot \operatorname{adj} A$. More generally, even if A is not invertible, the product of $\operatorname{adj} A$ with A (in either order) equals $(\det A) \cdot I_n$ (where I_n is the $n \times n$ identity matrix). Let us state this as a theorem:

Theorem 6.4.41. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Let I_n denote the $n \times n$ identity matrix. Then,

$$A \cdot (\operatorname{adj} A) = (\operatorname{adj} A) \cdot A = (\det A) \cdot I_n.$$

Proof. See [Grinbe15, Theorem 6.100] or [Ford21, Lemma 4.5.9] or [Loehr11, Theorem 9.50] or [Strick13, Proposition B.28].

Here is a sketch of the argument: In order to show that $A \cdot (\operatorname{adj} A) = (\det A) \cdot I_n$, it suffices to check that the (i, j)-th entry of $A \cdot (\operatorname{adj} A)$ equals $\det A$ whenever $i = j$ and equals 0 otherwise. However, this follows from Theorem 6.4.37 **(a)** (in the case $i = j$) and Proposition 6.4.38 **(a)** (in the case $i \neq j$). Thus, $A \cdot (\operatorname{adj} A) = (\det A) \cdot I_n$ is proved. Similarly, $(\operatorname{adj} A) \cdot A = (\det A) \cdot I_n$ can be shown. □

More about the adjugate matrix can be found in [Grinbe15, §6.15] and [Grinbe19, §5.4–§5.6]; see also [Robins05] for some applications.

There is also a generalization of Theorem 6.4.37, called *Laplace expansion along multiple rows (or columns)*:

Theorem 6.4.42. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. We shall use the notations $\widetilde{I}$ and $\operatorname{sum} S$ as defined in Theorem 6.4.23.

(a) For every subset P of $[n]$, we have

$$\det A = \sum_{\substack{Q \subseteq [n]; \\ |Q| = |P|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} A\right).$$

(b) For every subset Q of $[n]$, we have

$$\det A = \sum_{\substack{P \subseteq [n];\\ |P|=|Q|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} A\right).$$

Example 6.4.43. Let $n = 4$ and $A = \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \\ a''' & b''' & c''' & d''' \end{pmatrix}$ and $P = \{3,4\}$. Then, Theorem 6.4.42 **(a)** says that

$$\begin{aligned}
&\det A \\
&= \sum_{\substack{Q \subseteq [n];\\ |Q|=|P|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} A\right) \\
&= (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{1,2\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{1,2\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{1,2\}}} A\right) \\
&\qquad + (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{1,3\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{1,3\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{1,3\}}} A\right) \\
&\qquad + (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{1,4\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{1,4\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{1,4\}}} A\right) \\
&\qquad + (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{2,3\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{2,3\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{2,3\}}} A\right) \\
&\qquad + (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{2,4\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{2,4\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{2,4\}}} A\right) \\
&\qquad + (-1)^{\operatorname{sum}\{3,4\} + \operatorname{sum}\{3,4\}} \det\left(\operatorname{sub}_{\{3,4\}}^{\{3,4\}} A\right) \det\left(\operatorname{sub}_{\widetilde{\{3,4\}}}^{\widetilde{\{3,4\}}} A\right) \\
&= \det\begin{pmatrix} a'' & b'' \\ a''' & b''' \end{pmatrix} \det\begin{pmatrix} c & d \\ c' & d' \end{pmatrix} - \det\begin{pmatrix} a'' & c'' \\ a''' & c''' \end{pmatrix} \det\begin{pmatrix} b & d \\ b' & d' \end{pmatrix} \\
&\qquad + \det\begin{pmatrix} a'' & d'' \\ a''' & d''' \end{pmatrix} \det\begin{pmatrix} b & c \\ b' & c' \end{pmatrix} + \det\begin{pmatrix} b'' & c'' \\ b''' & c''' \end{pmatrix} \det\begin{pmatrix} a & d \\ a' & d' \end{pmatrix} \\
&\qquad - \det\begin{pmatrix} b'' & d'' \\ b''' & d''' \end{pmatrix} \det\begin{pmatrix} a & c \\ a' & c' \end{pmatrix} + \det\begin{pmatrix} c'' & d'' \\ c''' & d''' \end{pmatrix} \det\begin{pmatrix} a & b \\ a' & b' \end{pmatrix}.
\end{aligned}$$

Proof of Theorem 6.4.42. See [Grinbe15, Theorem 6.156]. □

6.4.8. Desnanot–Jacobi and Dodgson condensation

We come to more exotic results. The following theorem is one of several versions of the *Desnanot–Jacobi formula*:

Theorem 6.4.44 (Desnanot–Jacobi formula, take 1)**.** Let $n \in \mathbb{N}$ be such that $n \geq 2$. Let $A \in K^{n\times n}$ be an $n \times n$-matrix.

Let A' be the $(n-2) \times (n-2)$-matrix

$$\operatorname{sub}_{\{2,3,\ldots,n-1\}}^{\{2,3,\ldots,n-1\}} A = \left(A_{i+1,j+1}\right)_{1\leq i\leq n-2,\ 1\leq j\leq n-2}.$$

(This is precisely what remains of the matrix A when we remove the first row, the last row, the first column and the last column.) Then,

$$\begin{aligned}\det A \cdot \det\left(A'\right) &= \det\left(A_{\sim 1,\sim 1}\right) \cdot \det\left(A_{\sim n,\sim n}\right) - \det\left(A_{\sim 1,\sim n}\right) \cdot \det\left(A_{\sim n,\sim 1}\right) \\ &= \det \begin{pmatrix} \det\left(A_{\sim 1,\sim 1}\right) & \det\left(A_{\sim 1,\sim n}\right) \\ \det\left(A_{\sim n,\sim 1}\right) & \det\left(A_{\sim n,\sim n}\right) \end{pmatrix}.\end{aligned}$$

Example 6.4.45. For $n = 3$, this is saying that

$$\begin{aligned}&\det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \cdot \det \begin{pmatrix} b' \end{pmatrix} \\ &= \det \begin{pmatrix} b' & c' \\ b'' & c'' \end{pmatrix} \cdot \det \begin{pmatrix} a & b \\ a' & b' \end{pmatrix} - \det \begin{pmatrix} a' & b' \\ a'' & b'' \end{pmatrix} \cdot \det \begin{pmatrix} b & c \\ b' & c' \end{pmatrix}.\end{aligned}$$

Proof of Theorem 6.4.44. See [Grinbe15, Proposition 6.122] or [Bresso99, §3.5, proof of Theorem 3.12] or [Zeilbe98]. □

Theorem 6.4.44 provides a recursive way of computing determinants: Indeed, in the setting of Theorem 6.4.44, if $\det(A')$ is invertible (which, when K is a field, simply means that $\det(A') \neq 0$), then Theorem 6.4.44) yields

$$\det A = \frac{\det\left(A_{\sim 1,\sim 1}\right) \cdot \det\left(A_{\sim n,\sim n}\right) - \det\left(A_{\sim 1,\sim n}\right) \cdot \det\left(A_{\sim n,\sim 1}\right)}{\det\left(A'\right)}. \qquad (228)$$

The five matrices appearing on the right hand side of this are smaller than A, so their determinants are often easier to compute than $\det A$. In particular, if you are proving something by strong induction on n, you will occasionally be able to use the induction hypothesis to compute these determinants. This method of recursively simplifying determinants is often known as *Dodgson condensation*, as it was popularized (perhaps even discovered) by Charles Lutwidge Dodgson (aka Lewis Carroll) in [Dodgso67, Appendix II]. We outline a sample application:

Theorem 6.4.46 (Cauchy determinant)**.** Let $n \in \mathbb{N}$. Let $x_1, x_2, \ldots, x_n$ be n elements of K. Let $y_1, y_2, \ldots, y_n$ be n elements of K. Assume that $x_i + y_j$ is invertible in K for each $(i,j) \in [n]^2$. Then,

$$\det\left(\left(\frac{1}{x_i + y_j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \frac{\prod\limits_{1\leq i<j\leq n}\left(\left(x_i - x_j\right)\left(y_i - y_j\right)\right)}{\prod\limits_{(i,j)\in[n]^2}\left(x_i + y_j\right)}.$$

Once again, there are many ways to prove this (see, e.g., [Grinbe15, Exercise 6.18], [Prasol94, §1.3], [Grinbe09, Theorem 2], or `https://proofwiki.org/wiki/Value_of_Cauchy_Determinant`). But using the Desnanot–Jacobi identity, there is a rather straightforward proof of Theorem 6.4.46. Indeed, if A is a *Cauchy matrix* (i.e., a matrix of the form $\left(\frac{1}{x_i + y_j}\right)_{1\leq i\leq n,\ 1\leq j\leq n}$), then so is each submatrix of A. Thus, if we proceed by strong induction on n, we can use the induction hypothesis to compute all five determinants on the right hand side of (228). The only difficulty is making sure that $\det\left(A'\right)$ is invertible. To achieve this, we again have to WLOG assume that our x's and y's are indeterminates in a polynomial ring, and we have to rewrite the claim of Theorem 6.4.46 in the form

$$\det\left(\left(\prod_{k\neq j}\left(x_i + y_k\right)\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n}\left(\left(x_i - x_j\right)\left(y_i - y_j\right)\right)$$

in order for both sides to actually be polynomials in $\mathbb{Z}\left[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n\right]$. The details are left to the reader.

Theorem 6.4.44 can be generalized significantly. Here is the simplest generalization, in which the special role played by the first and last rows and the first and last columns is instead given to any two rows and any two columns:

Theorem 6.4.47. Let $n \in \mathbb{N}$ be such that $n \geq 2$. Let p, q, u and v be four elements of $[n]$ such that $p < q$ and $u < v$. Let A be an $n \times n$-matrix. Then,

$$\begin{aligned}&\det A \cdot \det\left(\operatorname{sub}_{[n]\setminus\{p,q\}}^{[n]\setminus\{u,v\}} A\right)\\ &= \det\left(A_{\sim p,\sim u}\right) \cdot \det\left(A_{\sim q,\sim v}\right) - \det\left(A_{\sim p,\sim v}\right) \cdot \det\left(A_{\sim q,\sim u}\right).\end{aligned}$$

Proof. See [Grinbe15, Theorem 6.126]. □

Even more generally, *Jacobi's complementary minor theorem for adjugates* (appearing, e.g., in [Grinbe19, Theorem 5.22], or in equivalent forms in [Prasol94, Theorem 2.5.2] and [BruSch83, (13)]) says the following:

Theorem 6.4.48 (Jacobi's complementary minor theorem for adjugates)**.** Let $n \in \mathbb{N}$. For any subset I of $[n]$, we let $\widetilde{I}$ denote the complement $[n] \setminus I$ of I. Set $\operatorname{sum} S = \sum\limits_{s \in S} s$ for any finite set S of integers. (For example, $\operatorname{sum}\{2,4,5\} = 2+4+5 = 11$.)

Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Let P and Q be two subsets of $[n]$ such that $|P| = |Q| \geq 1$. Then,

$$\det\left(\operatorname{sub}_P^Q (\operatorname{adj} A)\right) = (-1)^{\operatorname{sum} P + \operatorname{sum} Q} (\det A)^{|Q|-1} \det\left(\operatorname{sub}_{\widetilde{Q}}^{\widetilde{P}} A\right).$$

Theorem 6.4.47 is the particular case of Theorem 6.4.48 for $P = \{u, v\}$ and $Q = \{p, q\}$. [108] Theorem 6.4.44 is, of course, the particular case of Theorem 6.4.47 for $p = 1$ and $q = n$ and $u = 1$ and $v = n$.

6.5. Determinants in combinatorics

We have so far mostly been discussing algebraic properties of determinants, if often from a combinatorial point of view. We shall now see some situations in which determinants naturally appear in combinatorics.

6.5.1. Lindström–Gessel–Viennot

We begin with an application to lattice path enumeration – i.e., to the counting of paths on a certain infinite digraph called the *integer lattice*. A survey of this subject can be found in [Kratte17]; we will restrict ourselves to one of the most accessible highlights: the *Lindström–Gessel–Viennot theorem*. (Alternate treatments of this theorem can be found in [Sagan19, §2.5], in [Stanle11, §2.7] and in [GesVie89, §2]. Some applications predating the general statement of the theorem can be found in [GesVie85].)

We have already seen lattice paths (and even counted them in Subsection 4.4.1). We shall now introduce them formally and study them in greater depth.

Convention 6.5.1. (a) Recall that "*digraph*" means "directed graph", i.e., a graph whose edges are directed (and are called *arcs*). Against a widespread

[108] Indeed, if we set $P = \{u, v\}$ and $Q = \{p, q\}$ in the situation of Theorem 6.4.47, then

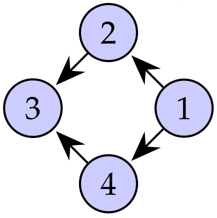
$$\operatorname{sub}_P^Q (\operatorname{adj} A) = \begin{pmatrix} (-1)^{u+p} \det\left(A_{\sim p, \sim u}\right) & (-1)^{u+q} \det\left(A_{\sim q, \sim u}\right) \\ (-1)^{v+p} \det\left(A_{\sim p, \sim v}\right) & (-1)^{v+q} \det\left(A_{\sim q, \sim v}\right) \end{pmatrix} \qquad \text{and}$$

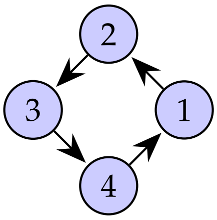
$$\operatorname{sub}_{\widetilde{Q}}^{\widetilde{P}} A = \operatorname{sub}_{[n] \setminus \{p,q\}}^{[n] \setminus \{u,v\}} A;$$

thus, Theorem 6.4.48 is easily seen to boil down to Theorem 6.4.47 in this case (the powers of -1 all cancel).

convention, we will allow our digraphs to be infinite (i.e., to have infinitely many vertices and arcs).

(b) A digraph D will be called *path-finite* if it has the property that for any two vertices u and v, there are only finitely many paths from u to v. (Thus, in particular, such paths can be counted.)

(c) A digraph D will be called *acyclic* if it has no directed cycles. For example, the digraph  is acyclic, whereas the digraph



is not.

(d) A *simple digraph D* means a digraph whose arcs are merely pairs of distinct vertices (i.e., each arc is a pair (u, v) of two vertices u and v with $u \neq v$).

We note that a path may contain 0 arcs (in which case its starting and ending point are identical).

Definition 6.5.2. We consider the infinite simple digraph with vertex set $\mathbb{Z}^2$ (so the vertices are pairs of integers) and arcs

$$(i, j) \to (i+1, j) \qquad \text{for all } (i, j) \in \mathbb{Z}^2 \tag{229}$$

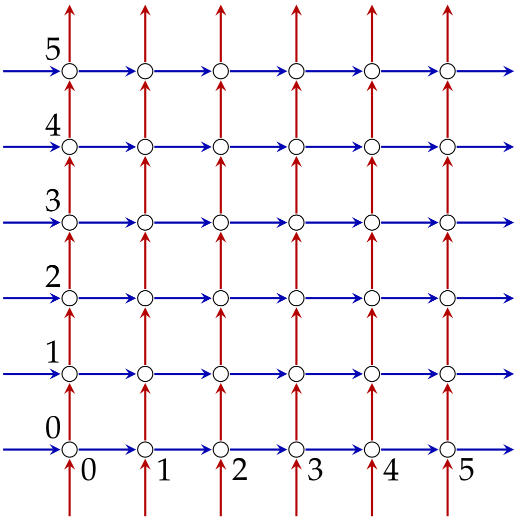
and

$$(i, j) \to (i, j+1) \qquad \text{for all } (i, j) \in \mathbb{Z}^2. \tag{230}$$

The arcs of the form (229) are called "*east-steps*" or "*right-steps*"; the arcs of the form (230) are called "*north-steps*" or "*up-steps*".

The vertices of this digraph will be called *lattice points* or *grid points* or simply *points*. They will be represented as points in the Cartesian plane (in the usual way: the vertex $(i, j) \in \mathbb{Z}^2$ is represented as the point with x-coordinate i and y-coordinate j).

The entire digraph will be denoted by $\mathbb{Z}^2$ and called the *integer lattice* or *integer grid* (or, to be short, just *lattice* or *grid*). Here is a picture of a small part of this digraph $\mathbb{Z}^2$:



(with east-steps colored blue and north-steps colored dark-red). Of course, the digraph continues indefinitely in all directions. In the following, we will not draw the vertices as circles, nor will we draw the arcs as arrows; we will simply draw the grid lines in order to avoid crowding our pictures.

However, $\mathbb{Z}^2$ is also an abelian group under addition. Thus, points can be added and subtracted entrywise; e.g., for any $(a, b) \in \mathbb{Z}^2$ and $(c, d) \in \mathbb{Z}^2$, we have

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{and}$$
$$(a, b) - (c, d) = (a - c, b - d) .$$

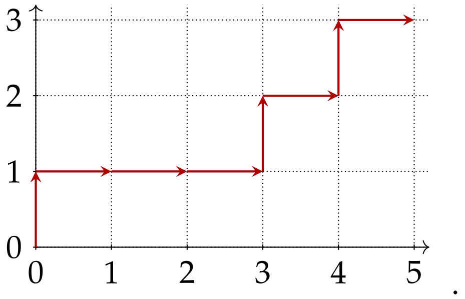
Thus, the digraph $\mathbb{Z}^2$ has an arc from a vertex u to a vertex v if and only if $v - u \in \{(0, 1), (1, 0)\}$.

The digraph $\mathbb{Z}^2$ is acyclic (i.e., it has no directed cycles). Thus, its paths are the same as its walks. We call these paths the *lattice paths* (or just *paths*). Thus, a lattice path is a finite tuple $(v_0, v_1, \ldots, v_n)$ of points $v_i \in \mathbb{Z}^2$ with the property that

$$v_i - v_{i-1} \in \{(0, 1), (1, 0)\} \qquad \text{for each } i \in [n] . \tag{231}$$

The *step sequence* of a path $(v_0, v_1, \ldots, v_n)$ is defined to be the n-tuple $(v_1 - v_0, v_2 - v_1, \ldots, v_n - v_{n-1})$. Each entry of this n-tuple is either $(0, 1)$ or $(1, 0)$ (because of (231)). We will often write U and R for the pairs $(0, 1)$ and $(1, 0)$, respectively (as they correspond to an **u**p-step and a **r**ight-step). Informally speaking, the step sequence of a path records the directions (i.e., east or north) of all steps of the path.

Example 6.5.3. Here is a path from $(0,0)$ to $(5,3)$:



Formally speaking, this path is the 9-tuple

$$((0,0),(0,1),(1,1),(2,1),(3,1),(3,2),(4,2),(4,3),(5,3)).$$

Its step sequence (i.e., the sequence of the directions of its steps) is $URRRURUR$ (meaning that its first step is an up-step, its second step is a right-step, its third step is a right-step, and so on).

Clearly, any path is uniquely determined by its starting point and its step sequence.

Note that we are considering one of the simplest possible notions of a lattice path here. In more advanced texts, the word "lattice path" is often used for paths in digraphs more complicated than $\mathbb{Z}^2$ (for instance, a digraph with the same vertex set $\mathbb{Z}^2$ but allowing steps in all four directions). However, the digraph we are considering is perhaps the most useful for algebraic combinatorics.

In Subsection 4.4.1, we have counted the lattice paths from $(0,0)$ to $(6,4)$ that begin with an east-step and end with a north-step. These are, of course, in bijection with the paths from $(1,0)$ to $(6,3)$ (since the first and last step are predetermined and thus can be ignored). Let us now generalize this by counting paths between any two lattice points:

Proposition 6.5.4. Let $(a,b) \in \mathbb{Z}^2$ and $(c,d) \in \mathbb{Z}^2$ be two points. Then,

$$(\text{\# of paths from } (a,b) \text{ to } (c,d)) = \begin{cases} \dbinom{c+d-a-b}{c-a}, & \text{if } c+d \geq a+b; \\ 0, & \text{if } c+d < a+b. \end{cases}$$

Proof of Proposition 6.5.4. This is just a formalization (and generalization) of the reasoning we used in Subsection 4.4.1.

We shall first show the following two observations:

> *Observation 1:* Each path from (a,b) to (c,d) has exactly $c+d-a-b$ steps[109].

> *Observation 2:* Each path from (a,b) to (c,d) has exactly $c-a$ east-steps.

[*Proof of Observation 1:* We define the *coordinate sum* of a point $(x,y) \in \mathbb{Z}^2$ to be $x+y$. We shall denote this coordinate sum by $\operatorname{cs}(x,y)$. We observe that the coordinate sum of a point increases by exactly 1 along each arc of $\mathbb{Z}^2$: That is, if $u \to v$ is an arc of $\mathbb{Z}^2$, then

$$\operatorname{cs}(v) - \operatorname{cs}(u) = 1. \tag{232}$$

(This is because we can write u in the form $u = (i,j)$ and then must have either $v = (i+1,j)$ or $v = (i,j+1)$; but this entails $\operatorname{cs}(v) = \underbrace{i+j}_{=\operatorname{cs}(u)} + 1 = \operatorname{cs}(u) + 1$ in either case.)

Let $(v_0, v_1, \ldots, v_n)$ be a path from (a,b) to (c,d). Thus, $v_0 = (a,b)$ and $v_n = (c,d)$. Moreover, for each $i \in [n]$, we know that $v_{i-1} \to v_i$ is an arc of $\mathbb{Z}^2$, and thus we have

$$\operatorname{cs}(v_i) - \operatorname{cs}(v_{i-1}) = 1$$

(by (232), applied to $u = v_{i-1}$ and $v = v_i$). Summing these equalities over all $i \in [n]$, we obtain

$$\sum_{i=1}^{n} (\operatorname{cs}(v_i) - \operatorname{cs}(v_{i-1})) = \sum_{i=1}^{n} 1 = n.$$

Hence,

$$\begin{aligned} n &= \sum_{i=1}^{n} (\operatorname{cs}(v_i) - \operatorname{cs}(v_{i-1})) = \operatorname{cs}\underbrace{(v_n)}_{=(c,d)} - \operatorname{cs}\underbrace{(v_0)}_{=(a,b)} \qquad \text{(by the telescope principle)} \\ &= \underbrace{\operatorname{cs}(c,d)}_{=c+d} - \underbrace{\operatorname{cs}(a,b)}_{=a+b} = c+d-(a+b) = c+d-a-b. \end{aligned}$$

In other words, the path $(v_0, v_1, \ldots, v_n)$ has exactly $c+d-a-b$ steps (since this path clearly has n steps).

Forget that we fixed $(v_0, v_1, \ldots, v_n)$. We thus have shown that each path $(v_0, v_1, \ldots, v_n)$ from (a,b) to (c,d) has exactly $c+d-a-b$ steps. This proves Observation 1.]

[*Proof of Observation 2:* For any point $v \in \mathbb{Z}^2$, we define $\operatorname{x}(v)$ to be the x-coordinate of v. (Thus, $\operatorname{x}(x,y) = x$ for each $(x,y) \in \mathbb{Z}^2$.)

Obviously, the x-coordinate of a point increases by exactly 1 along each east-step and stays unchanged along each north-step: That is, if $u \to v$ is an arc of $\mathbb{Z}^2$, then

$$\operatorname{x}(v) - \operatorname{x}(u) = \begin{cases} 1, & \text{if } u \to v \text{ is an east-step;} \\ 0, & \text{if } u \to v \text{ is a north-step.} \end{cases} \tag{233}$$

[109] A "step" of a path means an arc of this path.

Let $(v_0, v_1, \ldots, v_n)$ be a path from (a,b) to (c,d). Thus, $v_0 = (a,b)$ and $v_n = (c,d)$. Moreover, for each $i \in [n]$, we know that $v_{i-1} \rightarrow v_i$ is an arc of $\mathbb{Z}^2$, and thus we have

$$\mathrm{x}(v_i) - \mathrm{x}(v_{i-1}) = \begin{cases} 1, & \text{if } v_{i-1} \rightarrow v_i \text{ is an east-step;} \\ 0, & \text{if } v_{i-1} \rightarrow v_i \text{ is a north-step} \end{cases}$$

(by (233), applied to $u = v_{i-1}$ and $v = v_i$). Summing these equalities over all $i \in [n]$, we obtain

$$\begin{aligned} \sum_{i=1}^{n} (\mathrm{x}(v_i) - \mathrm{x}(v_{i-1})) &= \sum_{i=1}^{n} \begin{cases} 1, & \text{if } v_{i-1} \rightarrow v_i \text{ is an east-step;} \\ 0, & \text{if } v_{i-1} \rightarrow v_i \text{ is a north-step} \end{cases} \\ &= (\text{\# of } i \in [n] \text{ such that } v_{i-1} \rightarrow v_i \text{ is an east-step}) \\ &= (\text{\# of east-steps in the path } (v_0, v_1, \ldots, v_n)). \end{aligned}$$

Hence,

$$\begin{aligned} &(\text{\# of east-steps in the path } (v_0, v_1, \ldots, v_n)) \\ &= \sum_{i=1}^{n} (\mathrm{x}(v_i) - \mathrm{x}(v_{i-1})) = \mathrm{x}\underbrace{(v_n)}_{=(c,d)} - \mathrm{x}\underbrace{(v_0)}_{=(a,b)} \qquad \text{(by the telescope principle)} \\ &= \underbrace{\mathrm{x}(c,d)}_{=c} - \underbrace{\mathrm{x}(a,b)}_{=a} = c - a. \end{aligned}$$

In other words, the path $(v_0, v_1, \ldots, v_n)$ has exactly $c - a$ east-steps.

Forget that we fixed $(v_0, v_1, \ldots, v_n)$. We thus have shown that each path $(v_0, v_1, \ldots, v_n)$ from (a,b) to (c,d) has exactly $c - a$ east-steps. This proves Observation 2.]

Observation 1 immediately shows that no path from (a,b) to (c,d) exists when $c + d - a - b < 0$. In other words, no path from (a,b) to (c,d) exists when $c + d < a + b$. In other words, (# of paths from (a,b) to (c,d)) $= 0$ when $c + d < a + b$. This proves Proposition 6.5.4 in the case when $c + d < a + b$. Hence, for the rest of this proof of Proposition 6.5.4, we WLOG assume that $c + d \geq a + b$. Thus, $c + d - a - b \geq 0$.

Observations 1 and 2 have a sort of (common) converse:

> *Observation 3:* Let p be a path that starts at the point (a,b) and has exactly $c + d - a - b$ steps. Assume that exactly $c - a$ of these steps are east-steps. Then, this path p ends at (c,d).

[*Proof of Observation 3:* Let (c', d') be the point at which this path p ends. Then, we can apply Observation 1 to (c', d') instead of (c,d), and hence conclude that this path has exactly $c' + d' - a - b$ steps. Since we already know that this path has exactly $c + d - a - b$ steps, we therefore conclude that $c' + d' - a - b = c + d - a - b$. In other words, $c' + d' = c + d$. Similarly, using Observation 2, we can find that $c' = c$. Subtracting this equality from $c' + d' = c + d$, we obtain $d' = d$. Combining $c' = c$ with $d' = d$, we find $(c', d') = (c, d)$. Thus, our path p ends at (c, d) (since we know that it ends at (c', d')). This proves Observation 3.]

Now, combining Observations 1, 2 and 3, we see that the paths from (a, b) to (c, d) are precisely the paths that start at (a, b) and have exactly $c + d - a - b$ steps and exactly $c - a$ east-steps (among these $c + d - a - b$ steps). Such a path is therefore uniquely determined if we know **which** $c - a$ of its $c + d - a - b$ steps are east-steps. Thus, specifying such a path is equivalent to specifying a $(c - a)$-element subset of the $(c + d - a - b)$-element set[110] $[c + d - a - b]$. The bijection principle thus yields[111]

$$\begin{aligned}
&(\text{\# of paths from } (a,b) \text{ to } (c,d)) \\
&= (\text{\# of } (c-a)\text{-element subsets of } [c+d-a-b]) \\
&= \binom{c+d-a-b}{c-a}.
\end{aligned}$$

This proves Proposition 6.5.4 (since we have assumed that $c + d \geq a + b$). □

Now, let us try to count something more interesting: tuples of non-intersecting paths.

Definition 6.5.5. Let $k \in \mathbb{N}$.

(a) A *k-vertex* means a k-tuple of lattice points. For example, $((1,2), (4,5), (7,4))$ is a 3-vertex.

(b) If $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ is a k-vertex, and if $\sigma \in S_k$ is a permutation, then $\sigma(\mathbf{A})$ shall denote the k-vertex $\left(A_{\sigma(1)}, A_{\sigma(2)}, \ldots, A_{\sigma(k)}\right)$. For instance, for the simple transposition $s_1 \in S_3$, we have $s_1(A, B, C) = (B, A, C)$ for any 3-vertex (A, B, C).

(c) If $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ are two k-vertices, then a *path tuple* from $\mathbf{A}$ to $\mathbf{B}$ means a k-tuple $(p_1, p_2, \ldots, p_k)$, where each p_i is a path from A_i to B_i.

(d) A path tuple $(p_1, p_2, \ldots, p_k)$ is said to be *non-intersecting* if no two of the paths $p_1, p_2, \ldots, p_k$ have any vertex in common. (Visually speaking, this not only forbids them from crossing each other, but also forbids them from touching or bouncing off each other, or starting or ending at the same point.)

[110] Here we are tacitly using $c + d - a - b \geq 0$.

[111] To make this more formal: We are saying that the map

$$\begin{aligned}
\{\text{paths from } (a,b) \text{ to } (c,d)\} &\to \{(c-a)\text{-element subsets of } [c+d-a-b]\}, \\
(v_0, v_1, \ldots, v_{c+d-a-b}) &\mapsto \{i \in [c+d-a-b] \mid \text{the arc } v_{i-1} \to v_i \text{ is an east-step}\}
\end{aligned}$$

is a bijection, and we are applying the bijection principle to this bijection.

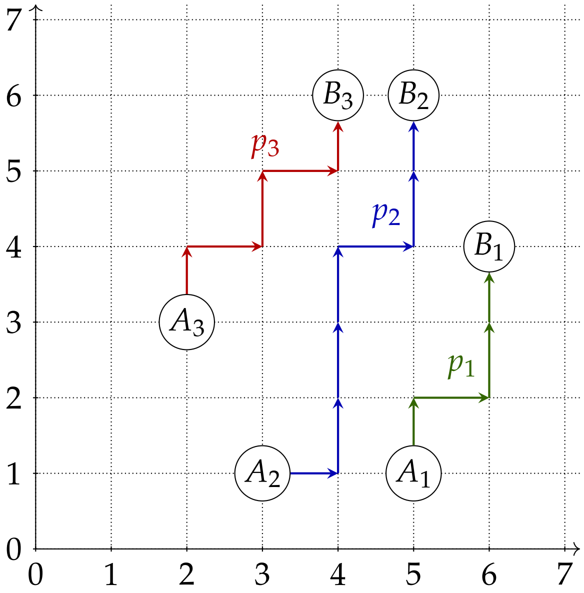
We shall abbreviate "non-intersecting path tuple" as "*nipat*". (Historically, the more common abbreviation is "*NILP*", for "non-intersecting lattice paths", but I prefer "nipat" as it stresses the tupleness.)

(e) A path tuple $(p_1, p_2, \ldots, p_k)$ is said to be *intersecting* if it is not non-intersecting (i.e., if two of its paths have a vertex in common).

We shall abbreviate "intersecting path tuple" as "*ipat*".

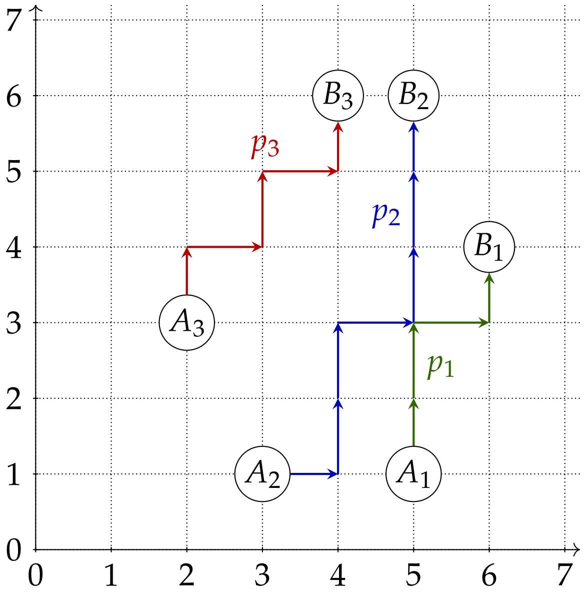
Example 6.5.6. Here are some path tuples for $k = 3$:

(a) The following path tuple is a nipat:



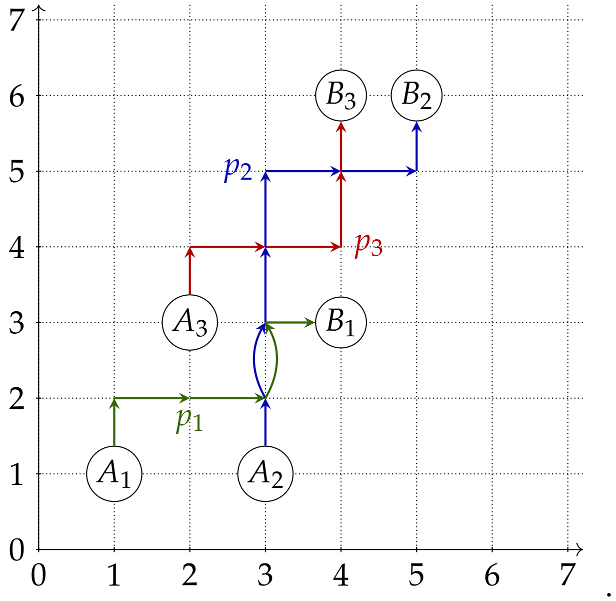
.

(b) The following path tuple is an ipat:



.

(c) The following path tuple is an ipat, too (for several reasons):



(In this tuple, the paths p_1 and p_2 even have an arc in common. Don't let the picture confuse you: The two curved arcs are actually one and the same arc of $\mathbb{Z}^2$ appearing in two paths, not two different arcs.)

Here is a first result on the case $k = 2$:

Proposition 6.5.7 (LGV lemma for two paths)**.** Let (A, A') and (B, B') be two 2-vertices (i.e., let A, A', B, B' be four lattice points). Then,

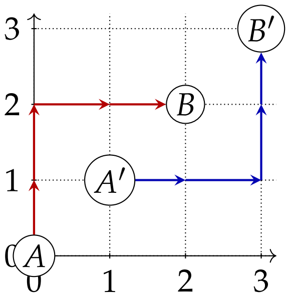
$$\begin{aligned}
&\det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\
&= (\text{\# of nipats from } (A, A') \text{ to } (B, B')) \\
&\qquad - (\text{\# of nipats from } (A, A') \text{ to } (B', B)) .
\end{aligned}$$

Example 6.5.8. Let $A = (0, 0)$ and $A' = (1, 1)$ and $B = (2, 2)$ and $B' = (3, 3)$. Then, Proposition 6.5.7 says that

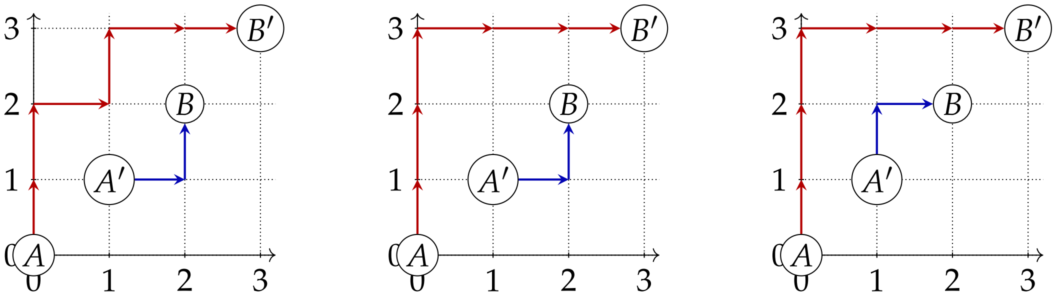
$$\begin{aligned}
\det \begin{pmatrix} \dbinom{4}{2} & \dbinom{6}{3} \\ \dbinom{2}{1} & \dbinom{4}{2} \end{pmatrix} &= (\text{\# of nipats from } (A, A') \text{ to } (B, B')) \\
&\qquad - (\text{\# of nipats from } (A, A') \text{ to } (B', B)) .
\end{aligned}$$

(The matrix entries on the left hand side have been computed using Proposition 6.5.4.)

And indeed, this equality is easily verified. There are 2 nipats from (A, A') to (B, B'), one of which is

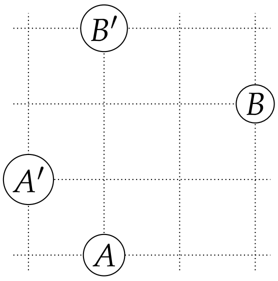


while the other is its reflection in the $x = y$ diagonal. There are 6 nipats from (A, A') to (B', B), three of which are



while the other three are their reflections in the $x = y$ diagonal. The right hand side of the above equality is thus $2 - 6 = -4$, which is also the left hand side.

Example 6.5.9. Let $A = (0,0)$ and $A' = (-1,1)$ and $B = (2,2)$ and $B' = (0,3)$. Then, the claim of Proposition 6.5.7 simplifies, since $(\text{\# of nipats from } (A, A') \text{ to } (B', B)) = 0$ in this case. Here is a picture of the four points that should make this visually clear:

 .

Proof of Proposition 6.5.7. We have

$$\begin{aligned}
&\det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\
&= \underbrace{(\text{\# of paths from } A \text{ to } B) \cdot (\text{\# of paths from } A' \text{ to } B')}_{\substack{=(\text{\# of path tuples from } (A,A') \text{ to } (B,B')) \\ (\text{by the product rule, since a path tuple from } (A,A') \text{ to } (B,B') \text{ is just} \\ \text{a pair consisting of a path from } A \text{ to } B \text{ and a path from } A' \text{ to } B')}} \\
&\qquad - \underbrace{(\text{\# of paths from } A \text{ to } B') \cdot (\text{\# of paths from } A' \text{ to } B)}_{\substack{=(\text{\# of path tuples from } (A,A') \text{ to } (B',B)) \\ (\text{by the product rule, since a path tuple from } (A,A') \text{ to } (B',B) \text{ is just} \\ \text{a pair consisting of a path from } A \text{ to } B' \text{ and a path from } A' \text{ to } B)}} \\
&= \left(\text{\# of path tuples from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right) \\
&\qquad - \left(\text{\# of path tuples from } \left(A, A'\right) \text{ to } \left(B', B\right)\right). \qquad (234)
\end{aligned}$$

We need to show that on the right hand side, all the intersecting path tuples cancel each other out (so that only the nipats remain).

Our k-vertices are 2-vertices; thus, our path tuples are pairs. Hence, such a path tuple (p, p') is intersecting if and only if p and p' have a vertex in common. We shall use these common vertices to define a sign-reversing involution on the intersecting path tuples. Specifically, we do the following:

Define the set

$$\begin{aligned}
\mathcal{A} := &\left\{\text{path tuples from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right\} \\
&\qquad \sqcup \left\{\text{path tuples from } \left(A, A'\right) \text{ to } \left(B', B\right)\right\}.
\end{aligned}$$

Here, the symbol "$\sqcup$" means "disjoint union (of sets)", which is a way of uniting two sets without removing duplicates (i.e., even if the sets are not disjoint, we treat them as disjoint for the purpose of the union, and therefore include two copies of each common element). As a consequence of us taking the disjoint union, each path tuple in $\mathcal{A}$ "remembers" whether it comes from the set $\{\text{path tuples from } (A, A') \text{ to } (B, B')\}$ or from the set $\{\text{path tuples from } (A, A') \text{ to } (B', B)\}$ (and if these two sets have a path tuple in common, then $\mathcal{A}$ has two copies of it, each of which remembers from which set it comes). However, in practice, this is barely relevant: Indeed, the only case in which the sets $\{\text{path tuples from } (A, A') \text{ to } (B, B')\}$ and $\{\text{path tuples from } (A, A') \text{ to } (B', B)\}$ can fail to be disjoint is the case when $B = B'$; however, in this case, the claim we are proving is trivial anyway, since there are no nipats[112], and our matrix has determinant 0 (since it has two equal columns).

Define a subset $\mathcal{X}$ of $\mathcal{A}$ by

$$\mathcal{X} := \{\text{ipats in } \mathcal{A}\} = \left\{\left(p, p'\right) \in \mathcal{A} \ \mid \ p \text{ and } p' \text{ have a vertex in common}\right\}.$$

[112] Indeed, if p and p' are two paths with the same destination, then p and p' automatically have a vertex in common.

Hence, $\mathcal{A} \setminus \mathcal{X} = \{\text{nipats in } \mathcal{A}\}$.

For each $(p, p') \in \mathcal{A}$, we set

$$\operatorname{sign}(p, p') := \begin{cases} 1, & \text{if } (p, p') \text{ is a path tuple from } (A, A') \text{ to } (B, B'); \\ -1, & \text{if } (p, p') \text{ is a path tuple from } (A, A') \text{ to } (B', B). \end{cases}$$

(This is well-defined, because each $(p, p') \in \mathcal{A}$ is either a path tuple from (A, A') to (B, B') or a path tuple from (A, A') to (B', B) but never both at the same time[113].) Thus,

$$\begin{aligned} &(\text{\# of path tuples from } (A, A') \text{ to } (B, B')) \\ &\qquad - (\text{\# of path tuples from } (A, A') \text{ to } (B', B)) \\ &= \sum_{(p,p') \in \mathcal{A}} \operatorname{sign}(p, p') \end{aligned}$$

and

$$\begin{aligned} &(\text{\# of nipats from } (A, A') \text{ to } (B, B')) \\ &\qquad - (\text{\# of nipats from } (A, A') \text{ to } (B', B)) \\ &= \sum_{(p,p') \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign}(p, p') \qquad (\text{since } \mathcal{A} \setminus \mathcal{X} = \{\text{nipats in } \mathcal{A}\}). \end{aligned}$$

We want to prove that the left hand sides of these two equalities are equal. Thus, it clearly suffices to show that the right hand sides are equal. By Lemma 6.1.3, it suffices to find a sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$ that has no fixed points.

So let us define our sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$. For each path tuple $(p, p') \in \mathcal{X}$, we define $f(p, p')$ as follows:

- Since $(p, p') \in \mathcal{X}$, the paths p and p' have a vertex in common. There might be several; let v be the first one. (The first one on p or the first one on p' ? Doesn't matter, because these are the same thing. Indeed, if the first vertex on p that is contained in p' was different from the first vertex on p' that is contained in p, then we could obtain a nontrivial circuit of our digraph by walking from the former vertex to the latter vertex along p and then back along p'; but this is impossible, since our digraph is acyclic.)

  We call this vertex v the *first intersection* of (p, p').

- Call the part of p that comes after v the *tail* of p, and the part of p that comes before v the *head* of p.

  Call the part of p' that comes after v the *tail* of p', and the part of p' that comes before v the *head* of p'.

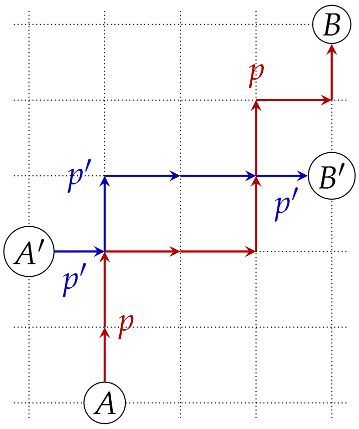
[113] because we took the **disjoint** union of $\{\text{path tuples from } (A, A') \text{ to } (B, B')\}$ and $\{\text{path tuples from } (A, A') \text{ to } (B', B)\}$

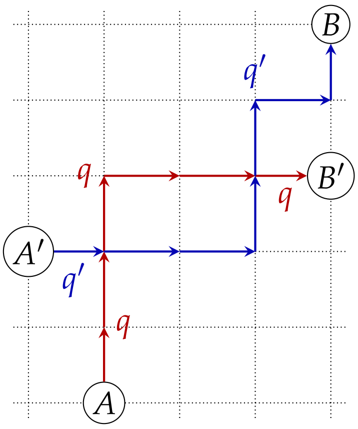
- Now, we exchange the tails of the paths p and p'. That is, we set

$$q := \left(\text{head of } p\right) \cup \left(\text{tail of } p'\right) \qquad \text{and}$$
$$q' := \left(\text{head of } p'\right) \cup \left(\text{tail of } p\right)$$

  (where the symbol "$\cup$" means combining a path ending at v with a path starting at v in the obvious way), and set $f\left(p, p'\right) := \left(q, q'\right)$.

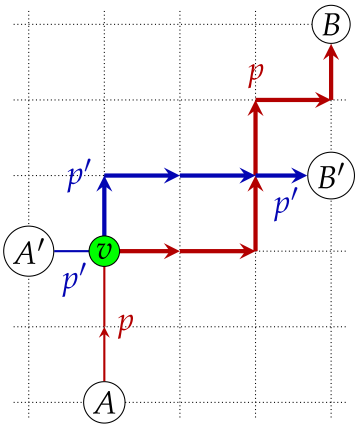
Thus, we have defined a map $f : \mathcal{X} \to \mathcal{X}$ (in a moment, we will explain why it is well-defined). Here is an example:

If $\left(p, p'\right) =$ 

, then $\left(q, q'\right) =$ 

.

Here is the same configuration, with the point v marked and with the tails of the two paths drawn extra-thick:



.

We note that if $\left(p, p'\right) \in \mathcal{X}$ is an ipat from $\left(A, A'\right)$ to $\left(B, B'\right)$, then $f\left(p, p'\right) = \left(q, q'\right)$ is an ipat from $\left(A, A'\right)$ to $\left(B', B\right)$ (because by exchanging the tails of p and p', we have caused the two paths to exchange their destinations as well), and vice versa. Thus, $f\left(p, p'\right) \in \mathcal{X}$ whenever $\left(p, p'\right) \in \mathcal{X}$. This shows that the map $f : \mathcal{X} \to \mathcal{X}$ is well-defined.

Furthermore, let $\left(p, p'\right) \in \mathcal{X}$ be any ipat, and let $\left(q, q'\right) = f\left(p, p'\right)$. Then, the vertex v chosen in the definition of $f\left(p, p'\right)$ (that is, the first intersection of $\left(p, p'\right)$) is still the first intersection of $\left(q, q'\right)$ (because when we exchange the tails of p and p', we do not change their heads, and thus the resulting paths q and q' still do not intersect until v), and therefore this vertex gets chosen again if we apply our map f to (q,q'). As a consequence, $f(q,q')$ is again (p,p') (since exchanging the tails of q and q' simply undoes the changes incurred when we exchanged the tails of p and p'). Thus,

$$(f\circ f)(p,p') = f\left(\underbrace{f(p,p')}_{=(q,q')}\right) = f(q,q') = (p,p').$$

Forget that we fixed (p,p'). We thus have shown that $(f\circ f)(p,p') = (p,p')$ for each $(p,p')\in\mathcal{X}$. Hence, $f\circ f = \operatorname{id}$. In other words, f is an involution on $\mathcal{X}$. Moreover, this involution f is sign-reversing (i.e., satisfies $\operatorname{sign}(f(p,p')) = -\operatorname{sign}(p,p')$ for any $(p,p')\in\mathcal{X}$) [114]. As a consequence of the latter fact, we see that f has no fixed points (i.e., that we have $f(p,p')\neq(p,p')$ for any $(p,p')\in\mathcal{X}$). Hence, Lemma 6.1.3 yields

$$\sum_{(p,p')\in\mathcal{A}} \operatorname{sign}(p,p') = \sum_{(p,p')\in\mathcal{A}\setminus\mathcal{X}} \operatorname{sign}(p,p'). \tag{235}$$

As we have explained above, the left hand side of this equality is

$$\begin{aligned}&(\#\text{ of path tuples from }(A,A')\text{ to }(B,B'))\\&\qquad-(\#\text{ of path tuples from }(A,A')\text{ to }(B',B)),\end{aligned}$$

whereas its right hand side is

$$\begin{aligned}&(\#\text{ of nipats from }(A,A')\text{ to }(B,B'))\\&\qquad-(\#\text{ of nipats from }(A,A')\text{ to }(B',B))\end{aligned}$$

(since $\mathcal{A}\setminus\mathcal{X} = \{\text{nipats in }\mathcal{A}\}$). Hence, (235) rewrites as

$$\begin{aligned}&(\#\text{ of path tuples from }(A,A')\text{ to }(B,B'))\\&\qquad-(\#\text{ of path tuples from }(A,A')\text{ to }(B',B))\\&=(\#\text{ of nipats from }(A,A')\text{ to }(B,B'))\\&\qquad-(\#\text{ of nipats from }(A,A')\text{ to }(B',B)).\end{aligned}$$

In view of (234), this rewrites as

$$\begin{aligned}&\det\begin{pmatrix}(\#\text{ of paths from }A\text{ to }B) & (\#\text{ of paths from }A\text{ to }B')\\(\#\text{ of paths from }A'\text{ to }B) & (\#\text{ of paths from }A'\text{ to }B')\end{pmatrix}\\&=(\#\text{ of nipats from }(A,A')\text{ to }(B,B'))\\&\qquad-(\#\text{ of nipats from }(A,A')\text{ to }(B',B)).\end{aligned}$$

This completes our proof of Proposition 6.5.7. □

[114] This is because we have observed above that if $(p,p')\in\mathcal{X}$ is an ipat from (A,A') to (B,B'), then $f(p,p') = (q,q')$ is an ipat from (A,A') to (B',B), and vice versa.

As in Example 6.5.9, the proposition becomes particularly nice when we have $(\text{\# of nipats from } (A, A') \text{ to } (B', B)) = 0$. Here is a sufficient criterion for when this happens:

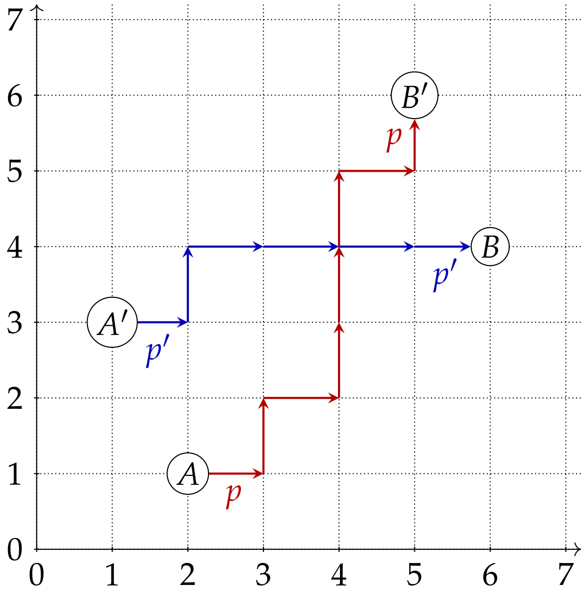
Proposition 6.5.10 (baby Jordan curve theorem)**.** Let A, B, A' and B' be four lattice points satisfying

$$\mathrm{x}(A') \leq \mathrm{x}(A), \qquad \mathrm{y}(A') \geq \mathrm{y}(A), \tag{236}$$
$$\mathrm{x}(B') \leq \mathrm{x}(B), \qquad \mathrm{y}(B') \geq \mathrm{y}(B). \tag{237}$$

Here, $\mathrm{x}(P)$ and $\mathrm{y}(P)$ denote the two coordinates of any point $P \in \mathbb{Z}^2$.

Let p be any path from A to B'. Let p' be any path from A' to B. Then, p and p' have a vertex in common.

Note that the condition (236) can be restated as "the point A' lies weakly northwest of A", where "weakly northwest of A" allows for the options "due north of A", "due west of A" and "at A". Likewise, (237) can be restated as "the point B' lies weakly northwest of B". The following picture illustrates the situation of Proposition 6.5.10:



Proposition 6.5.10 has an intuitive plausibility to it (one can think of the path p as creating a "river" that the path p' must necessarily cross somewhere), but it is not obvious from a mathematical perspective. We give a rigorous proof in Section B.4.

Proposition 6.5.7 is just the $k = 2$ case of a more general theorem that we will soon derive; however, it already has a nice application:

Corollary 6.5.11. Let $n, k \in \mathbb{N}$. Then, $\dbinom{n}{k}^2 \geq \dbinom{n}{k-1} \cdot \dbinom{n}{k+1}$.

Proof of Corollary 6.5.11 (sketched). This is easy to see algebraically, but here is a combinatorial proof: Define four lattice points $A = (1,0)$ and $A' = (0,1)$ and $B = (k+1, n-k)$ and $B' = (k, n-k+1)$. Then, Proposition 6.5.7 yields

$$\det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix}$$
$$= (\text{\# of nipats from } (A, A') \text{ to } (B, B')) - \underbrace{(\text{\# of nipats from } (A, A') \text{ to } (B', B))}_{\substack{=0 \\ \text{(since Proposition 6.5.10 yields that any path} \\ \text{from } A \text{ to } B' \text{ and any path from } A' \text{ to } B \text{ have a} \\ \text{vertex in common)}}}$$
$$= (\text{\# of nipats from } (A, A') \text{ to } (B, B')) \geq 0.$$

However, Proposition 6.5.4 yields

$$\begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix}$$
$$= \begin{pmatrix} \dbinom{n}{k} & \dbinom{n}{k-1} \\ \dbinom{n}{k+1} & \dbinom{n}{k} \end{pmatrix},$$

so the determinant on the left hand side is $\dbinom{n}{k}^2 - \dbinom{n}{k-1} \cdot \dbinom{n}{k+1}$. Thus, we have obtained

$$\binom{n}{k}^2 - \binom{n}{k-1} \cdot \binom{n}{k+1} \geq 0,$$

and this proves Corollary 6.5.11. □

Corollary 6.5.11 is often stated as "the sequence $\dbinom{n}{0}, \dbinom{n}{1}, \ldots, \dbinom{n}{n}$ is log-concave". There are many more log-concave sequences in combinatorics (see, e.g., [Sagan19], [Stanle89] and [Brande14] for more).

The following proposition – which is one of the weakest forms of the *LGV lemma* (short for *Lindström–Gessel–Viennot lemma*) – extends the logic of Proposition 6.5.7 to nipats between k-vertices for general k).

Proposition 6.5.12 (LGV lemma, lattice counting version)**.** Let $k \in \mathbb{N}$. Let $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ be two k-vertices. Then,

$$\begin{aligned} & \det\left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{1 \le i \le k,\ 1 \le j \le k}\right) \\ & = \sum_{\sigma \in S_k} (-1)^{\sigma} \left(\text{\# of nipats from } \mathbf{A} \text{ to } \sigma(\mathbf{B})\right). \end{aligned}$$

The right hand side of this equality can be viewed as a signed count of all k-tuples of paths that start at the points $A_1, A_2, \ldots, A_k$ in **this** order, but end at the points $B_1, B_2, \ldots, B_k$ in **some** order. For example, for $k = 3$, the claim of Proposition 6.5.12 takes the form

$$\begin{aligned} & \det\left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{1 \le i \le 3,\ 1 \le j \le 3}\right) \\ & = \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_1, B_2, B_3)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_1, B_3, B_2)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_2, B_1, B_3)\right) \\ & \qquad + \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_2, B_3, B_1)\right) \\ & \qquad + \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_3, B_1, B_2)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_3, B_2, B_1)\right). \end{aligned}$$

Proof of Proposition 6.5.12 (sketched). We adapt the idea of our proof of Proposition 6.5.7, but we have to be more systematic now. Define a set

$$\mathcal{A} := \{(\sigma, \mathbf{p}) \mid \sigma \in S_k, \text{ and } \mathbf{p} \text{ is a path tuple from } \mathbf{A} \text{ to } \sigma(\mathbf{B})\}$$

[115]. Define a subset $\mathcal{X}$ of $\mathcal{A}$ by[116]

$$\mathcal{X} := \{\text{ipats in } \mathcal{A}\} = \{(\sigma, \mathbf{p}) \in \mathcal{A} \mid \mathbf{p} \text{ is intersecting}\}.$$

Set

$$\operatorname{sign}(\sigma, \mathbf{p}) := (-1)^{\sigma} \qquad \text{for each } (\sigma, \mathbf{p}) \in \mathcal{A}.$$

[115] This set $\mathcal{A}$ is meant to generalize the set $\mathcal{A}$ that was used in the proof of Proposition 6.5.7. The reason why we are defining it to be

$$\begin{aligned} & \{(\sigma, \mathbf{p}) \mid \sigma \in S_k, \text{ and } \mathbf{p} \text{ is a path tuple from } \mathbf{A} \text{ to } \sigma(\mathbf{B})\} \\ & \text{instead of } \{\mathbf{p} \mid \mathbf{p} \text{ is a path tuple from } \mathbf{A} \text{ to } \sigma(\mathbf{B}) \text{ for some } \sigma \in S_k\} \end{aligned}$$

is to make sure that each path tuple in $\mathcal{A}$ "remembers" which permutation $\sigma \in S_k$ it comes from. (This is the same rationale that caused us to take the disjoint union in the proof of Proposition 6.5.7; but now we are explicitly inserting the σ into the elements of $\mathcal{A}$ rather than handwaving about disjoint unions.)

[116] Here we are saying that a pair $(\sigma, \mathbf{p}) \in \mathcal{A}$ is an *ipat* if the path tuple $\mathbf{p}$ is an ipat, and we are saying that a pair $(\sigma, \mathbf{p}) \in \mathcal{A}$ is a *nipat* if the path tuple $\mathbf{p}$ is a nipat. This is a bit sloppy (σ has nothing to do with whether $\mathbf{p}$ is an ipat or a nipat), but we hope that no confusion will ensue.

Again, we need to find a sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$ that has no fixed points.

Again, we construct this involution by exchanging the tails of two intersecting paths[117] in our path tuple. There is a complication now, due to the fact that there might be several pairs of intersecting paths. We have to come up with a rule for picking one such pair so that when we apply f again to the result of the exchange, then we again pick the same pair. Otherwise, f won't be an involution!

There are different ways to do this. Here is one: If $(\sigma, (p_1, p_2, \ldots, p_k)) \in \mathcal{X}$, then we construct $f(\sigma, (p_1, p_2, \ldots, p_k)) \in \mathcal{X}$ as follows:

- We say that a point u is *crowded* if it is contained in at least two of our paths $p_1, p_2, \ldots, p_k$. Since $(p_1, p_2, \ldots, p_k)$ is intersecting, there exists at least one crowded point.

- We pick the smallest $i \in [k]$ such that p_i contains a crowded point.

- Then, we pick the first crowded point v on p_i.

- Then, we pick the largest $j \in [k]$ such that v belongs to p_j. (Note that $j > i$, since v is crowded.)

- Then, we exchange the tails of the paths p_i and p_j (while leaving all other paths unchanged).

- We let $(q_1, q_2, \ldots, q_k)$ be the resulting path tuple[118].

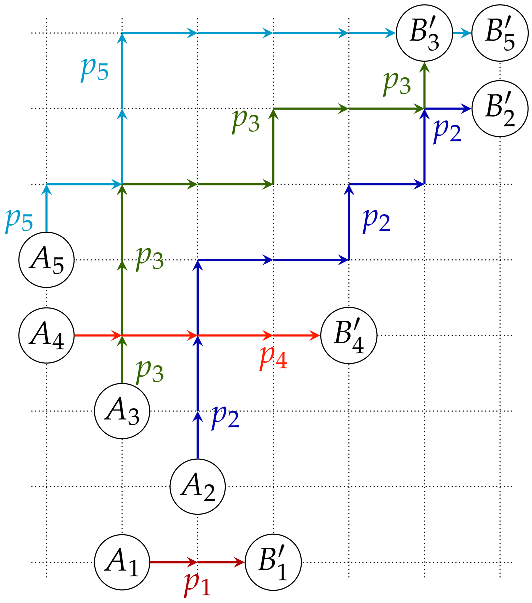
- We set $\sigma' := \sigma t_{i,j}$, where $t_{i,j}$ is the transposition in S_k that swaps i with j. Thus, $(q_1, q_2, \ldots, q_k)$ is a path tuple from $\mathbf{A}$ to $\sigma'(\mathbf{B})$ (because exchanging the tails of the paths p_i and p_j has switched their ending points $B_{\sigma(i)}$ and $B_{\sigma(j)}$ to $B_{\sigma(j)} = B_{\sigma'(i)}$ and $B_{\sigma(i)} = B_{\sigma'(j)}$, respectively).

- Finally, we set
$$f(\sigma, (p_1, p_2, \ldots, p_k)) := (\sigma', (q_1, q_2, \ldots, q_k)).$$

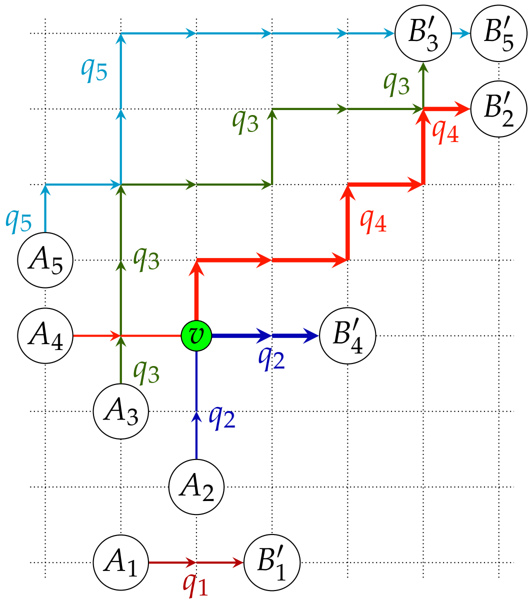
[117] This is probably obvious, but just in case: We say that two paths *intersect* if they have a vertex in common.

[118] Thus,
$$q_i = (\text{head of } p_i) \cup (\text{tail of } q_j) \qquad \text{and} \qquad q_j = (\text{head of } p_j) \cup (\text{tail of } q_i)$$
(where "head" means "part until v", and "tail" means "part after v"). Furthermore, we have $q_m = p_m$ for any $m \in [k] \setminus \{i, j\}$, since we have left all paths other than p_i and p_j unchanged.

This defines a map $f : \mathcal{X} \to \mathcal{X}$ (again, it is not hard to see that it is well-defined). Here is an example: If $k = 5$ and if $(p_1, p_2, \ldots, p_k)$ is



(where B_m' is shorthand for $B_{\sigma(m)}$), then v is the point where paths p_2 and p_4 intersect, and we have $i = 2$ and $j = 4$, and therefore $(q_1, q_2, \ldots, q_k)$ is



(where we again have drawn the exchanged tails extra-thick).

Convince yourself that the map f defined above really is a sign-reversing involution from $\mathcal{X}$ to $\mathcal{X}$. (This means showing that applying f twice in succession to any given $(\sigma, \mathbf{p}) \in \mathcal{X}$ returns $(\sigma, \mathbf{p})$, and that $\operatorname{sign}(f(\sigma, \mathbf{p})) = -\operatorname{sign}(\sigma, \mathbf{p})$ for any $(\sigma, \mathbf{p}) \in \mathcal{X}$. The proof of the second claim, of course, relies on parts **(b)** and **(d)** of Proposition 5.4.2.)

Thus, we have defined a sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$. This involution f has no fixed points (since it is sign-reversing). It is now easy to complete the proof: Lemma 6.1.3 yields

$$\sum_{(\sigma,\mathbf{p})\in\mathcal{A}} \operatorname{sign}(\sigma,\mathbf{p}) = \sum_{(\sigma,\mathbf{p})\in\mathcal{A}\setminus\mathcal{X}} \operatorname{sign}(\sigma,\mathbf{p}).$$

In view of our definition of $\operatorname{sign}(\sigma,\mathbf{p})$, this rewrites as

$$\sum_{(\sigma,\mathbf{p})\in\mathcal{A}} (-1)^{\sigma} = \sum_{(\sigma,\mathbf{p})\in\mathcal{A}\setminus\mathcal{X}} (-1)^{\sigma}. \tag{238}$$

The left hand side of this equality is

$$\begin{aligned}\sum_{(\sigma,\mathbf{p})\in\mathcal{A}} (-1)^{\sigma} = \sum_{\sigma\in S_k} (-1)^{\sigma} & \underbrace{(\text{\# of path tuples from } \mathbf{A} \text{ to } \sigma(\mathbf{B}))}_{\substack{=\prod_{i=1}^{k}\left(\text{\# of paths from } A_i \text{ to } B_{\sigma(i)}\right) \\ \text{(by the product rule, since a path tuple from } \mathbf{A} \text{ to } \sigma(\mathbf{B}) \text{ is just} \\ \text{a tuple } (p_1,p_2,\ldots,p_k)\text{, where each } p_i \text{ is a path from } A_i \text{ to } B_{\sigma(i)})}} \\ & \qquad (\text{by the definition of } \mathcal{A}) \\ = \sum_{\sigma\in S_k} (-1)^{\sigma} \prod_{i=1}^{k} & \left(\text{\# of paths from } A_i \text{ to } B_{\sigma(i)}\right) \\ = \det & \left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{1\le i\le k,\ 1\le j\le k}\right)\end{aligned}$$

(by the definition of the determinant), whereas the right hand side is

$$\begin{aligned}\sum_{(\sigma,\mathbf{p})\in\mathcal{A}\setminus\mathcal{X}} (-1)^{\sigma} &= \sum_{(\sigma,\mathbf{p})\in\mathcal{A} \text{ is a nipat}} (-1)^{\sigma} \qquad \left(\begin{array}{c}\text{since } \mathcal{X} = \{\text{ipats in } \mathcal{A}\} \\ \text{entails } \mathcal{A}\setminus\mathcal{X} = \{\text{nipats in } \mathcal{A}\}\end{array}\right) \\ &= \sum_{\sigma\in S_k} (-1)^{\sigma} (\text{\# of nipats from } \mathbf{A} \text{ to } \sigma(\mathbf{B}))\end{aligned}$$

(by the definition of $\mathcal{A}$). Thus, (238) rewrites as

$$\begin{aligned}&\det\left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{1\le i\le k,\ 1\le j\le k}\right) \\ &= \sum_{\sigma\in S_k} (-1)^{\sigma} (\text{\# of nipats from } \mathbf{A} \text{ to } \sigma(\mathbf{B})).\end{aligned}$$

This proves Proposition 6.5.12. □

So far we have just been counting paths; but we can easily introduce weights to obtain a more general result:

Theorem 6.5.13 (LGV lemma, lattice weight version)**.** Let K be a commutative ring.

For each arc a of the digraph $\mathbb{Z}^2$, let $w(a)$ be an element of K. We call this element $w(a)$ the *weight* of a.

For each path p of $\mathbb{Z}^2$, define the *weight* $w(p)$ of p by

$$w(p) := \prod_{a \text{ is an arc of } p} w(a).$$

For each path tuple $\mathbf{p} = (p_1, p_2, \ldots, p_k)$, define the *weight* $w(\mathbf{p})$ of $\mathbf{p}$ by

$$w(\mathbf{p}) := w(p_1)\, w(p_2) \cdots w(p_k).$$

Let $k \in \mathbb{N}$. Let $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ be two k-vertices. Then,

$$\det\left(\left(\sum_{p:A_i\to B_j} w(p)\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right) = \sum_{\sigma\in S_k} (-1)^{\sigma} \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \sigma(\mathbf{B})}} w(\mathbf{p}).$$

Here, "$p : A_i \to B_j$" means "p is a path from A_i to B_j".

Clearly, Proposition 6.5.12 is the particular case of Theorem 6.5.13 when $K = \mathbb{Z}$ and $w(a) = 1$ for all arcs a (because in this case, all the weights $w(p)$ and $w(\mathbf{p})$ of paths and path tuples equal 1, and therefore the sums over paths or nipats become the #s of paths or nipats).

Proof of Theorem 6.5.13. The same argument as for Proposition 6.5.12 can be used here; just replace $\operatorname{sign}(\sigma, \mathbf{p}) := (-1)^{\sigma}$ by $\operatorname{sign}(\sigma, \mathbf{p}) = (-1)^{\sigma} \cdot w(\mathbf{p})$. (The only new observation required is that when we exchange the tails of two paths in our path tuple, the weight of the path tuple does not change. This is rather clear: The weight of a path tuple is the product of the weights of all arcs in all paths of the tuple[119]. When we exchange the tails of two paths, some arcs get moved from one path to the other, but the total product stays unchanged.) □

We can generalize Theorem 6.5.13 further. Indeed, we have barely used anything specific to $\mathbb{Z}^2$ in our proofs; all we used is that $\mathbb{Z}^2$ is a path-finite acyclic digraph. Thus, Theorem 6.5.13 remains true if we replace $\mathbb{Z}^2$ by an arbitrary such digraph. We thus obtain the following more general result:

Theorem 6.5.14 (LGV lemma, digraph weight version)**.** Let K be a commutative ring.

[119] An arc will appear multiple times in the product if it appears in multiple paths.

Let D be a path-finite (but possibly infinite) acyclic digraph. We extend Definition 6.5.5 to D instead of $\mathbb{Z}^2$ (with the obvious changes: "lattice points" becomes "vertices of D").

For each arc a of the digraph D, let $w(a)$ be an element of K. We call this element $w(a)$ the *weight* of a.

For each path p of D, define the *weight* $w(p)$ of p by

$$w(p) := \prod_{a \text{ is an arc of } p} w(a).$$

For each path tuple $\mathbf{p} = (p_1, p_2, \ldots, p_k)$, define the *weight* $w(\mathbf{p})$ of $\mathbf{p}$ by

$$w(\mathbf{p}) := w(p_1)\, w(p_2) \cdots w(p_k).$$

Let $k \in \mathbb{N}$. Let $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ be two k-vertices (i.e., two k-tuples of vertices of D). Then,

$$\det\left(\left(\sum_{p:A_i\to B_j} w(p)\right)_{1\le i\le k,\ 1\le j\le k}\right) = \sum_{\sigma\in S_k} (-1)^{\sigma} \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \sigma(\mathbf{B})}} w(\mathbf{p}).$$

Here, "$p : A_i \to B_j$" means "p is a path from A_i to B_j".

Proof. Completely analogous to the proof of Theorem 6.5.13. □

One nice thing about the digraph $\mathbb{Z}^2$, however, is that in many cases, the sum

$$\sum_{\sigma\in S_k} (-1)^{\sigma} \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \sigma(\mathbf{B})}} w(\mathbf{p})$$

has only one nonzero addend. We have already seen this happen often in the $k = 2$ case (thanks to Proposition 6.5.10). Here is the analogous statement for general k:

Corollary 6.5.15 (LGV lemma, nonpermutable lattice weight version)**.** Consider the setting of Theorem 6.5.13, but additionally assume that

$$\mathrm{x}(A_1) \ge \mathrm{x}(A_2) \ge \cdots \ge \mathrm{x}(A_k); \tag{239}$$

$$\mathrm{y}(A_1) \le \mathrm{y}(A_2) \le \cdots \le \mathrm{y}(A_k); \tag{240}$$

$$\mathrm{x}(B_1) \ge \mathrm{x}(B_2) \ge \cdots \ge \mathrm{x}(B_k); \tag{241}$$

$$\mathrm{y}(B_1) \le \mathrm{y}(B_2) \le \cdots \le \mathrm{y}(B_k). \tag{242}$$

Here, $\mathrm{x}(P)$ and $\mathrm{y}(P)$ denote the two coordinates of any point $P \in \mathbb{Z}^2$.

Then, there are no nipats from $\mathbf{A}$ to $\sigma(\mathbf{B})$ when $\sigma \in S_k$ is not the identity permutation $\operatorname{id} \in S_k$. Therefore, the claim of Theorem 6.5.13 simplifies to

$$\det\left(\left(\sum_{p:A_i\to B_j} w(p)\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right) = \sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\mathbf{B}}} w(\mathbf{p}). \tag{243}$$

Proof of Corollary 6.5.15 (sketched). This is easy using Proposition 6.5.10. Here are the details:

Let $\sigma \in S_k$ be a permutation that is not the identity permutation $\operatorname{id} \in S_k$. Then, we don't have $\sigma(1) \leq \sigma(2) \leq \cdots \leq \sigma(k)$ (since σ is not id). In other words, there exists some $i \in [k-1]$ such that $\sigma(i) > \sigma(i+1)$. Consider this i.

Now, let $\mathbf{p}$ be a nipat from $\mathbf{A}$ to $\sigma(\mathbf{B})$. Write $\mathbf{p}$ in the form $\mathbf{p} = (p_1, p_2, \ldots, p_k)$. Thus, p_i is a path from A_i to $B_{\sigma(i)}$, whereas p_{i+1} is a path from A_{i+1} to $B_{\sigma(i+1)}$. Moreover, p_i and p_{i+1} have no vertex in common (since $\mathbf{p}$ is a nipat).

The sequence $(\mathrm{x}(B_1), \mathrm{x}(B_2), \ldots, \mathrm{x}(B_k))$ is weakly decreasing (by (241)). In other words, if m and n are two elements of $[k]$ satisfying $m > n$, then $\mathrm{x}(B_m) \leq \mathrm{x}(B_n)$. Applying this to $m = \sigma(i)$ and $n = \sigma(i+1)$, we obtain $\mathrm{x}\left(B_{\sigma(i)}\right) \leq \mathrm{x}\left(B_{\sigma(i+1)}\right)$ (since $\sigma(i) > \sigma(i+1)$). Likewise, using (242), we can obtain $\mathrm{y}\left(B_{\sigma(i)}\right) \geq \mathrm{y}\left(B_{\sigma(i+1)}\right)$. However, (239) shows that $\mathrm{x}(A_i) \geq \mathrm{x}(A_{i+1})$. In other words, $\mathrm{x}(A_{i+1}) \leq \mathrm{x}(A_i)$. Furthermore, (240) shows that $\mathrm{y}(A_i) \leq \mathrm{y}(A_{i+1})$. In other words, $\mathrm{y}(A_{i+1}) \geq \mathrm{y}(A_i)$.

Hence, Proposition 6.5.10 (applied to $A = A_i$, $B = B_{\sigma(i+1)}$, $A' = A_{i+1}$, $B' = B_{\sigma(i)}$, $p = p_i$ and $p' = p_{i+1}$) yields that p_i and p_{i+1} have a vertex in common. This contradicts the fact that p_i and p_{i+1} have no vertex in common.

Forget that we fixed $\mathbf{p}$. We thus have found a contradiction for each nipat $\mathbf{p}$ from $\mathbf{A}$ to $\sigma(\mathbf{B})$. Hence, there are no nipats from $\mathbf{A}$ to $\sigma(\mathbf{B})$.

Forget that we fixed σ. We thus have proved that there are no nipats from $\mathbf{A}$ to $\sigma(\mathbf{B})$ when $\sigma \in S_k$ is not the identity permutation $\operatorname{id} \in S_k$. Hence, if $\sigma \in S_k$ is not the identity permutation $\operatorname{id} \in S_k$, then

$$\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\sigma(\mathbf{B})}} w(\mathbf{p}) = (\text{empty sum}) = 0. \tag{244}$$

Now, Theorem 6.5.13 yields

$$\begin{aligned}
&\det\left(\left(\sum_{p:A_i\to B_j} w\left(p\right)\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right)\\
&=\sum_{\sigma\in S_k}\left(-1\right)^{\sigma}\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\sigma(\mathbf{B})}} w\left(\mathbf{p}\right)\\
&=\underbrace{\left(-1\right)^{\operatorname{id}}}_{=1}\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\operatorname{id}(\mathbf{B})}} w\left(\mathbf{p}\right)+\sum_{\substack{\sigma\in S_k;\\ \sigma\neq\operatorname{id}}}\left(-1\right)^{\sigma}\underbrace{\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\sigma(\mathbf{B})}} w\left(\mathbf{p}\right)}_{\substack{=0\\ \text{(by (244))}}}\\
&\qquad\qquad\left(\text{here, we have split off the addend for }\sigma=\operatorname{id}\text{ from the sum}\right)\\
&=\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\operatorname{id}(\mathbf{B})}} w\left(\mathbf{p}\right)+\underbrace{\sum_{\substack{\sigma\in S_k;\\ \sigma\neq\operatorname{id}}}\left(-1\right)^{\sigma}0}_{=0}=\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\operatorname{id}(\mathbf{B})}} w\left(\mathbf{p}\right)=\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\mathbf{B}}} w\left(\mathbf{p}\right)
\end{aligned}$$

(since $\operatorname{id}\left(\mathbf{B}\right)=\mathbf{B}$). The proof of Corollary 6.5.15 is now complete. □

Corollary 6.5.16. Let $k\in\mathbb{N}$. Let $a_1,a_2,\ldots,a_k$ and $b_1,b_2,\ldots,b_k$ be nonnegative integers such that

$$a_1\geq a_2\geq\cdots\geq a_k \qquad\text{and}\qquad b_1\geq b_2\geq\cdots\geq b_k.$$

Then,

$$\det\left(\left(\binom{a_i}{b_j}\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right)\geq 0.$$

For example, if $a_1\geq a_2\geq a_3\geq 0$ and $b_1\geq b_2\geq b_3\geq 0$, then

$$\det\begin{pmatrix}\binom{a_1}{b_1} & \binom{a_1}{b_2} & \binom{a_1}{b_3}\\ \binom{a_2}{b_1} & \binom{a_2}{b_2} & \binom{a_2}{b_3}\\ \binom{a_3}{b_1} & \binom{a_3}{b_2} & \binom{a_3}{b_3}\end{pmatrix}\geq 0.$$

Proof of Corollary 6.5.16 (sketched). Set $K=\mathbb{Z}$, and set $w\left(a\right):=1$ for each arc a of $\mathbb{Z}^2$. Define the lattice points

$$A_i:=\left(0,-a_i\right) \qquad\text{and}\qquad B_i:=\left(b_i,-b_i\right)$$

for all $i \in [k]$. These lattice points satisfy the assumptions of Corollary 6.5.15. Hence, (243) entails

$$\det\left(\left(\sum_{p:A_i\to B_j} w(p)\right)_{1\le i\le k,\ 1\le j\le k}\right) = \sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\mathbf{B}}} w(\mathbf{p}).$$

Since all the weights $w(p)$ and $w(\mathbf{p})$ are 1 in our situation, we can rewrite this as

$$\det\left((\#\text{ of paths from } A_i \text{ to } B_j)_{1\le i\le k,\ 1\le j\le k}\right) = (\#\text{ of nipats from } \mathbf{A} \text{ to } \mathbf{B}).$$

Using Proposition 6.5.4, we can easily see that the matrix on the left hand side of this equality is $\left(\dbinom{a_i}{b_j}\right)_{1\le i\le k,\ 1\le j\le k}$. Thus, this equality rewrites as

$$\det\left(\left(\dbinom{a_i}{b_j}\right)_{1\le i\le k,\ 1\le j\le k}\right) = (\#\text{ of nipats from } \mathbf{A} \text{ to } \mathbf{B}).$$

Its left hand side is therefore ≥ 0 (since its right hand side is ≥ 0). This proves Corollary 6.5.16. □

Corollary 6.5.17. Let $k \in \mathbb{N}$. Recall the Catalan numbers $c_n = \dfrac{1}{n+1}\dbinom{2n}{n}$ for all $n \in \mathbb{N}$. Then,

$$\det\left((c_{i+j-2})_{1\le i\le k,\ 1\le j\le k}\right) = \det\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-1} \\ c_1 & c_2 & \cdots & c_k \\ \vdots & \vdots & \ddots & \vdots \\ c_{k-1} & c_k & \cdots & c_{2k-2} \end{pmatrix} = 1.$$

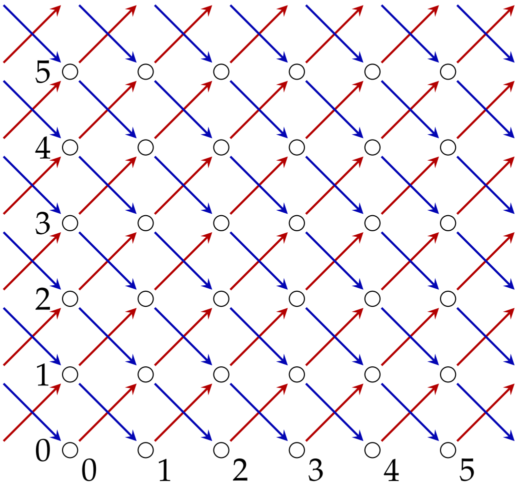
Proof of Corollary 6.5.17 (sketched). We will use not the lattice $\mathbb{Z}^2$, but a different digraph. Namely, we use the simple digraph with vertex set $\mathbb{Z} \times \mathbb{N}$ (that is, the vertices are the lattice points that lie on the x-axis or above it) and arcs

$$(i,j) \to (i+1,\ j+1) \qquad \text{for all } (i,j) \in \mathbb{Z}\times\mathbb{N}$$

and

$$(i,j) \to (i+1,\ j-1) \qquad \text{for all } (i,j) \in \mathbb{Z}\times\mathbb{P},$$

where $\mathbb{P} := \{1, 2, 3, \ldots\}$. Here is a picture of a small part of this digraph:



.

As we know, the Catalan number c_n counts the paths from $(0, 0)$ to $(2n, 0)$ on this digraph (indeed, these are just the Dyck paths[120]). Hence, c_n also counts the paths from $(i, 0)$ to $(2n + i, 0)$ whenever $i \in \mathbb{N}$ (because these are just the Dyck paths shifted by i in the x-direction). It is easy to see that this digraph is acyclic and path-finite.

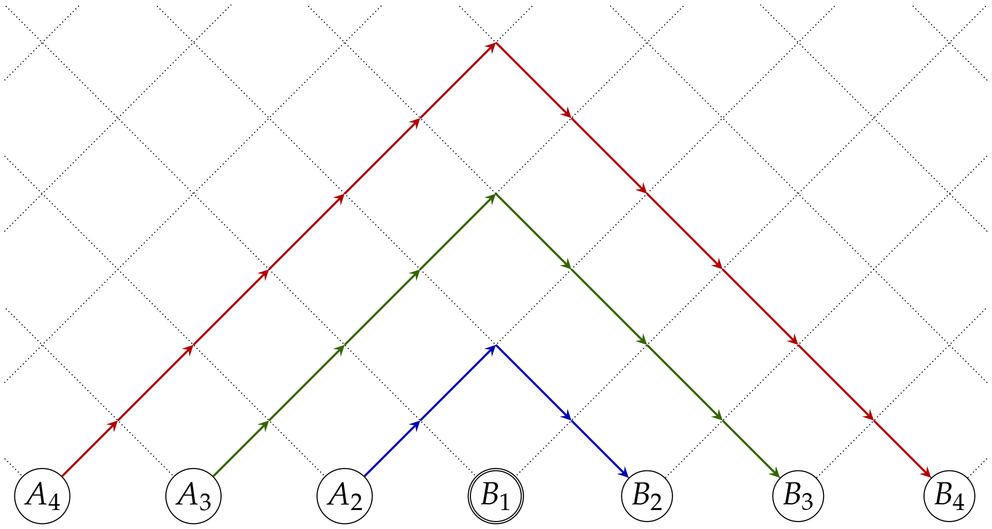
Now, define two k-vertices $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ by setting

$$A_i := (-2(i-1), 0) \qquad \text{and} \qquad B_i := (2(i-1), 0)$$

for all $i \in [k]$. It is not hard to show (see Exercise A.5.4.2 **(a)**) that there is only one nipat from $\mathbf{A}$ to $\mathbf{B}$, which is shown in the case $k = 4$ on the following

[120] See Example 2 in Section 3.1 for the definition of a Dyck path.

picture:[121]



(the point A_1 coincides with B_1, and the path from A_1 to B_1 is invisible, since it has no arcs). Moreover, it can be shown (see Exercise A.5.4.2 **(b)**) that there are no nipats from $\mathbf{A}$ to $\sigma(\mathbf{B})$ when $\sigma \in S_k$ is not the identity permutation id $\in S_k$. (This is analogous to Corollary 6.5.15.) Hence, if we set $K = \mathbb{Z}$ and $w(a) = 1$ for each arc a of our digraph, then (243) entails

$$\det\left(\left(\sum_{p:A_i\to B_j} w(p)\right)_{1\le i\le k,\ 1\le j\le k}\right) = \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \mathbf{B}}} w(\mathbf{p})$$

(by the same reasoning as in the proof of Corollary 6.5.15). The right hand side of this equality is 1 (since there is only one nipat from $\mathbf{A}$ to $\mathbf{B}$), while the matrix on the left hand side is easily seen to be $(c_{i+j-2})_{1\le i\le k,\ 1\le j\le k}$ (since the # of paths from A_i to B_j is the Catalan number c_{i+j-2}). This yields the claim of Corollary 6.5.17. The details are LTTR. □

The LGV lemma in all its variants is one major place in which combinatorial questions reduce to the computation of determinants. Other such places are the *matrix-tree theorem* (see, e.g., [Zeilbe85, §4], [Loehr11, §3.17], [Stanle18, Theorems 9.8 and 10.4]) and the enumeration of perfect matchings or domino tilings (see, e.g., [Stucky15], [Loehr11, §12.12–§12.13], [Aigner07, §10.1]). Soon, we will also encounter determinants in the study of symmetric functions.

[121] In this picture, we are drawing only "half" of the grid. Indeed, the vertices (i,j) of our digraph $\mathbb{Z}\times\mathbb{N}$ can be classified into *even vertices* (i.e., the ones for which $i+j$ is even) and *odd vertices* (i.e., the ones for which $i+j$ is odd). Any arc either connects two even vertices or connects two odd vertices. Hence, a path starting at an even vertex cannot contain any odd vertex (and vice versa). Since all our vertices $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_k$ are even, we thus don't have to bother even drawing the odd vertices (as they have no chance to appear in any paths between our vertices). As a consequence, we are drawing only the grid lines containing the even vertices.

7. Symmetric functions

The topic of the rest of this course is the theory of *symmetric functions*. Specifically, we will restrict ourselves to *symmetric polynomials* (the "functions" part is a technical tweak that makes the theory neater but we won't have time to introduce). Serious treatments of the subject can be found in [Wildon20], [Loehr11, Chapters 10–11], [Egge19], [Macdon95], [Aigner07, Chapter 8], [Stanle01, Chapter 7], [Sagan19, Chapter 7], [Sagan01, Chapter 4], [Krishn86], [FoaHan04, Chapters 14–19], [Savage22], [GriRei20, Chapter 2] and [LLPT95].

We begin with some oversimplified historical motivation.

Symmetric polynomials first(?) appeared in the study of roots of polynomials. Consider a monic univariate polynomial

$$f = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n x^0 \in \mathbb{C}[x]$$

(note the nonstandard labeling of coefficients). Let $r_1, r_2, \ldots, r_n \in \mathbb{C}$ be the roots of this polynomial (listed with multiplicities). Then, François Viète (aka Franciscus Vieta) noticed that

$$f = (x - r_1)(x - r_2) \cdots (x - r_n),$$

so that (by comparing coefficients) we see that

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -a_1; \\ \sum_{i<j} r_i r_j &= a_2; \\ \sum_{i<j<k} r_i r_j r_k &= -a_3; \\ &\ldots; \\ r_1 r_2 \cdots r_n &= (-1)^n a_n. \end{aligned}$$

These equalities are now known as *Viete's formulas*. They allow computing certain expressions in the r_i's without having to compute the r_i's themselves. For instance, we can compute $r_1^2 + r_2^2 + \cdots + r_n^2$ (that is, the sum of the squares of all roots of f) by observing that

$$(r_1 + r_2 + \cdots + r_n)^2 = \left(r_1^2 + r_2^2 + \cdots + r_n^2\right) + 2\sum_{i<j} r_i r_j,$$

so that

$$r_1^2 + r_2^2 + \cdots + r_n^2 = \left(\underbrace{r_1 + r_2 + \cdots + r_n}_{=-a_1}\right)^2 - 2\underbrace{\sum_{i<j} r_i r_j}_{=a_2} = a_1^2 - 2a_2.$$

This shows, among other things, that $r_1^2 + r_2^2 + \cdots + r_n^2$ is an integer if the coefficients of f are integers. Newton and others found similar formulas for $r_1^3 + r_2^3 + \cdots + r_n^3$ and other such polynomials. (These formulas are now known as the *Newton–Girard identities* – see Theorem 7.1.12 below.) Gauss extended this to arbitrary symmetric polynomials in $r_1, r_2, \ldots, r_n$ (by algorithmically expressing them as polynomials in $a_1, a_2, \ldots, a_n$), and used it in one of his proofs of the Fundamental Theorem of Algebra [Gauss16]; Galois used this to build what is now known as Galois theory (even though modern treatments of Galois theory often avoid symmetric polynomials); some harbingers of this can be seen in Cardano's solution of the cubic equation. See [Tignol16] and [Armstr19] for the real history.

Here is a simple modern application of the same ideas: Let $A \in \mathbb{C}^{n \times n}$ be a matrix with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$ (listed with algebraic multiplicities). Let $f \in \mathbb{C}[x]$ be a univariate polynomial. The *spectral mapping theorem* says that the eigenvalues of the matrix $f[A]$ are $f[\lambda_1], f[\lambda_2], \ldots, f[\lambda_n]$ (here, I am using the notation $f[a]$ for the value of f at some element a; this is usually written $f(a)$). Thus, the characteristic polynomial of $f[A]$ is

$$\begin{aligned}\chi_{f[A]} &= (x - f[\lambda_1])(x - f[\lambda_2]) \cdots (x - f[\lambda_n]) \\ &= x^n - (f[\lambda_1] + f[\lambda_2] + \cdots + f[\lambda_n])\, x^{n-1} + \left(\sum_{i<j} f[\lambda_i] f[\lambda_j] \right) x^{n-2} \pm \cdots .\end{aligned}$$

Hence, all coefficients of $\chi_{f[A]}$ are symmetric polynomials in the λ_is that depend only on f (not on A). In particular, this shows that $\chi_{f[A]}$ is uniquely determined by f and χ_A. But can you compute $\chi_{f[A]}$ exactly in terms of f and χ_A without computing the roots $\lambda_1, \lambda_2, \ldots, \lambda_n$? Yes, if you know how to express **any** symmetric polynomial in the λ_is in terms of the coefficients of χ_A. This is the same problem that Gauss solved with his algorithm for expressing an arbitrary symmetric polynomial in the roots of a polynomial in terms of the coefficients of the polynomial. Incidentally, this algorithm also becomes helpful when one tries to generalize the spectral mapping theorem to matrices over arbitrary commutative rings. Here, eigenvalues don't always exist (let alone n of them), so it becomes necessary to restate the theorem in a language that does not rely on them. Again, symmetric polynomials provide the way to do this.

7.1. Definitions and examples of symmetric polynomials

Convention 7.1.1. Fix a commutative ring K. Fix an $N \in \mathbb{N}$. (Perhaps n would be more conventional, but lowercase letters are chronically in short supply in this subject.)

Throughout this chapter, we will keep K and N fixed. We will use Definition 5.1.2.

Recall that S_N denotes the N-th symmetric group, i.e., the group of all permutations of the set $[N] := \{1, 2, \ldots, N\}$.

Definition 7.1.2. **(a)** Let $\mathcal{P}$ be the polynomial ring $K[x_1, x_2, \ldots, x_N]$ in N variables over K. This is not just a ring; it is a commutative K-algebra.

(b) The symmetric group S_N acts on the set $\mathcal{P}$ according to the formula

$$\sigma \cdot f = f\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right] \qquad \text{for any } \sigma \in S_N \text{ and any } f \in \mathcal{P}.$$

Here, $f[a_1, a_2, \ldots, a_N]$ means the result of substituting $a_1, a_2, \ldots, a_N$ for the indeterminates $x_1, x_2, \ldots, x_N$ in a polynomial $f \in \mathcal{P}$.

(For example, if $N = 4$ and $\sigma = \operatorname{cyc}_{1,2,3} \in S_4$, then $\sigma \cdot f = f\left[x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}\right] = f[x_2, x_3, x_1, x_4]$ for any $f \in \mathcal{P}$, so that, for example,

$$\sigma \cdot \left(2x_1 + 3x_2^2 + 4x_3 - x_4^{15}\right) = 2x_2 + 3x_3^2 + 4x_1 - x_4^{15}$$

and $\sigma \cdot (x_1 - x_3x_4) = x_2 - x_1x_4$.)

Roughly speaking, the group S_N is thus acting on $\mathcal{P}$ by permuting variables: A permutation $\sigma \in S_N$ transforms a polynomial f by substituting $x_{\sigma(i)}$ for each x_i.

Note that this action of S_N on $\mathcal{P}$ is a well-defined group action (as we will see in Proposition 7.1.4 below).

(c) A polynomial $f \in \mathcal{P}$ is said to be *symmetric* if it satisfies

$$\sigma \cdot f = f \qquad \text{for all } \sigma \in S_N.$$

(d) We let $\mathcal{S}$ be the set of all symmetric polynomials $f \in \mathcal{P}$.

Example 7.1.3. Let $N = 3$ and $K = \mathbb{Q}$, and let us rename the indeterminates x_1, x_2, x_3 as x, y, z. Then:

(a) We have $x + y + z \in \mathcal{S}$ (since, for example, the simple transposition $s_1 \in S_3$ satisfies $s_1 \cdot (x + y + z) = y + x + z = x + y + z$, and similarly any other $\sigma \in S_3$ also satisfies $\sigma \cdot (x + y + z) = x + y + z$).

(b) We have $x + y \notin \mathcal{S}$ (since the transposition $t_{1,3} \in S_3$ satisfies $t_{1,3} \cdot (x + y) = z + y \neq x + y$).

(c) We have $(x - y)(y - z)(z - x) \notin \mathcal{S}$ (since the simple transposition $s_1 \in S_3$ transforms $(x - y)(y - z)(z - x)$ into

$$\begin{aligned} s_1 \cdot ((x - y)(y - z)(z - x)) &= (y - x)(x - z)(z - y) \\ &= -(x - y)(y - z)(z - x) \\ &\neq (x - y)(y - z)(z - x), \end{aligned}$$

because $-1 \neq 1$ in $\mathbb{Q}$). Actually, the polynomial $(x - y)(y - z)(z - x)$ is an example of an *antisymmetric* polynomial – i.e., a polynomial $f \in \mathcal{P}$ such that $\sigma \cdot f = (-1)^{\sigma} f$ for all $\sigma \in S_N$. However, if $K = \mathbb{Z}/2$ (or if K is a $\mathbb{Z}/2$-algebra), then antisymmetric polynomials and symmetric polynomials are the same thing.

(d) We have $((x-y)(y-z)(z-x))^2 \in \mathcal{S}$. More generally, if $f \in \mathcal{P}$ is antisymmetric, then f^2 is symmetric, so that $f^2 \in \mathcal{S}$.

(e) We have $37 \in \mathcal{S}$. More generally, any constant polynomial $f \in \mathcal{P}$ is symmetric.

(f) We have $(1-x)(1-y)(1-z) \in \mathcal{S}$.

(g) We have $\dfrac{1}{(1-x)(1-y)(1-z)} \notin \mathcal{S}$, because this is not a polynomial. It is an example of a *symmetric power series*.

Some basic properties of our current setup are worth mentioning:

Proposition 7.1.4. The action of S_N on $\mathcal{P}$ is a well-defined group action. In other words, the following holds:

(a) We have $\operatorname{id}_{[N]} \cdot f = f$ for every $f \in \mathcal{P}$.

(b) We have $(\sigma\tau) \cdot f = \sigma \cdot (\tau \cdot f)$ for every $\sigma, \tau \in S_N$ and $f \in \mathcal{P}$.

The proof of this proposition is straightforward, but due to its somewhat slippery nature (the two substitutions in part **(b)** are a particularly frequent source of confusion), we present it in full:

Proof of Proposition 7.1.4. **(a)** If $f \in \mathcal{P}$, then the definition of $\operatorname{id}_{[N]} \cdot f$ yields

$$\operatorname{id}_{[N]} \cdot f = f\left[x_{\operatorname{id}(1)}, x_{\operatorname{id}(2)}, \ldots, x_{\operatorname{id}(N)}\right] = f\left[x_1, x_2, \ldots, x_N\right] = f.$$

This proves Proposition 7.1.4 **(a)**.

(b) Let $\sigma, \tau \in S_N$ and $f \in \mathcal{P}$. The definition of $\sigma \cdot (\tau \cdot f)$ yields

$$\sigma \cdot (\tau \cdot f) = (\tau \cdot f)\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right]. \tag{245}$$

Write the polynomial f in the form

$$f = \sum_{(a_1,a_2,\ldots,a_N) \in \mathbb{N}^N} f_{(a_1,a_2,\ldots,a_N)} x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}, \tag{246}$$

where $f_{(a_1,a_2,\ldots,a_N)} \in K$ are its coefficients. The definition of $\tau \cdot f$ yields

$$\tau \cdot f = f\left[x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(N)}\right] = \sum_{(a_1,a_2,\ldots,a_N) \in \mathbb{N}^N} f_{(a_1,a_2,\ldots,a_N)} x_{\tau(1)}^{a_1} x_{\tau(2)}^{a_2} \cdots x_{\tau(N)}^{a_N}$$

(here, we have substituted $x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(N)}$ for $x_1, x_2, \ldots, x_N$ on both sides of (246)). Substituting $x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}$ for $x_1, x_2, \ldots, x_N$ on both sides of this equality, we obtain

$$\begin{aligned}
&(\tau \cdot f)\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right] \\
&= \sum_{(a_1,a_2,\ldots,a_N) \in \mathbb{N}^N} f_{(a_1,a_2,\ldots,a_N)} \underbrace{x_{\sigma(\tau(1))}^{a_1} x_{\sigma(\tau(2))}^{a_2} \cdots x_{\sigma(\tau(N))}^{a_N}}_{\substack{= x_{(\sigma\tau)(1)}^{a_1} x_{(\sigma\tau)(2)}^{a_2} \cdots x_{(\sigma\tau)(N)}^{a_N} \\ \text{(since } \sigma(\tau(i)) = (\sigma\tau)(i) \text{ for all } i \in [N])}} \\
&\qquad \left(\text{since our substitution replaces each } x_i \text{ by } x_{\sigma(i)}\right) \\
&= \sum_{(a_1,a_2,\ldots,a_N) \in \mathbb{N}^N} f_{(a_1,a_2,\ldots,a_N)} x_{(\sigma\tau)(1)}^{a_1} x_{(\sigma\tau)(2)}^{a_2} \cdots x_{(\sigma\tau)(N)}^{a_N}.
\end{aligned}$$

On the other hand, the definition of the action of S_N on $\mathcal{P}$ yields

$$\begin{aligned}(\sigma\tau)\cdot f &= f\left[x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \ldots, x_{(\sigma\tau)(N)}\right] \\ &= \sum_{(a_1,a_2,\ldots,a_N)\in\mathbb{N}^N} f_{(a_1,a_2,\ldots,a_N)} x_{(\sigma\tau)(1)}^{a_1} x_{(\sigma\tau)(2)}^{a_2} \cdots x_{(\sigma\tau)(N)}^{a_N}\end{aligned}$$

(here, we have substituted $x_{(\sigma\tau)(1)}, x_{(\sigma\tau)(2)}, \ldots, x_{(\sigma\tau)(N)}$ for $x_1, x_2, \ldots, x_N$ on both sides of (246)). Comparing these two equalities, we obtain

$$(\sigma\tau)\cdot f = (\tau\cdot f)\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right] = \sigma\cdot(\tau\cdot f)$$

(by (245)). This proves Proposition 7.1.4 **(b)**. □

We recall the following notions from abstract algebra:

- A *K-algebra isomorphism* from a K-algebra A to a K-algebra B means an invertible K-algebra morphism $f : A \to B$ such that its inverse $f^{-1} : B \to A$ is a K-algebra morphism from B to A. (Actually, any invertible K-algebra morphism is an isomorphism.)
- A *K-algebra automorphism* of a K-algebra A means a K-algebra isomorphism from A to A.

Proposition 7.1.5. The group S_N acts on $\mathcal{P}$ by K-algebra automorphisms. In other words, for each $\sigma \in S_N$, the map

$$\begin{aligned}\mathcal{P} &\to \mathcal{P}, \\ f &\mapsto \sigma\cdot f\end{aligned}$$

is a K-algebra automorphism of $\mathcal{P}$ (that is, a K-algebra isomorphism from $\mathcal{P}$ to $\mathcal{P}$).

Proof of Proposition 7.1.5 (sketched). Fix $\sigma \in S_N$. For any $f, g \in \mathcal{P}$, we have

$$\begin{aligned}\sigma\cdot(fg) &= (fg)\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right] \qquad \text{(by the definition of the action of } S_N \text{ on } \mathcal{P}\text{)} \\ &= \underbrace{f\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right]}_{\substack{=\sigma\cdot f \\ \text{(by the definition of the action of } S_N \text{ on } \mathcal{P}\text{)}}} \cdot \underbrace{g\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right]}_{\substack{=\sigma\cdot g \\ \text{(by the definition of the action of } S_N \text{ on } \mathcal{P}\text{)}}} \\ &= (\sigma\cdot f)\cdot(\sigma\cdot g)\,.\end{aligned}$$

Thus, the map

$$\begin{aligned}\mathcal{P} &\to \mathcal{P}, \\ f &\mapsto \sigma\cdot f\end{aligned}$$

respects multiplication. Similarly, this map respects addition, respects scaling, respects the zero and respects the unity. Hence, this map is a K-algebra morphism from $\mathcal{P}$ to $\mathcal{P}$. Furthermore, this map is invertible, since its inverse is the map

$$\begin{aligned} \mathcal{P} &\to \mathcal{P}, \\ f &\mapsto \sigma^{-1} \cdot f. \end{aligned}$$

Thus, this map is an invertible K-algebra morphism from $\mathcal{P}$ to $\mathcal{P}$, and therefore a K-algebra isomorphism from $\mathcal{P}$ to $\mathcal{P}$. In other words, this map is a K-algebra automorphism of $\mathcal{P}$. This proves Proposition 7.1.5. □

Theorem 7.1.6. The subset $\mathcal{S}$ is a K-subalgebra of $\mathcal{P}$.

Proof of Theorem 7.1.6 (sketched). We need to show that $\mathcal{S}$ is closed under addition, multiplication and scaling, and that $\mathcal{S}$ contains the zero and the unity of $\mathcal{P}$. Let me just show that $\mathcal{S}$ is closed under multiplication (since all the other claims are equally easy): Let $f, g \in \mathcal{S}$. We must show that $fg \in \mathcal{S}$.

The polynomial f is symmetric (since $f \in \mathcal{S}$); in other words, $\sigma \cdot f = f$ for each $\sigma \in S_N$. Similarly, $\sigma \cdot g = g$ for each $\sigma \in S_N$. Now, for each $\sigma \in S_N$, we have

$$\sigma \cdot (fg) = \underbrace{(\sigma \cdot f)}_{\substack{=f \\ \text{(as we have seen)}}} \cdot \underbrace{(\sigma \cdot g)}_{\substack{=g \\ \text{(as we have seen)}}} = fg.$$

This shows that fg is symmetric, i.e., we have $fg \in \mathcal{S}$.

Forget that we fixed f, g. We thus have shown that $fg \in \mathcal{S}$ for any $f, g \in \mathcal{S}$. This shows that $\mathcal{S}$ is closed under multiplication. As explained above, this concludes our proof of Theorem 7.1.6. □

Definition 7.1.7. The K-subalgebra $\mathcal{S}$ of $\mathcal{P}$ is called the *ring of symmetric polynomials in N variables over K*.

Some more terminology is worth defining:

Definition 7.1.8. (a) A *monomial* is an expression of the form $x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ with $a_1, a_2, \ldots, a_N \in \mathbb{N}$.

(b) The *degree* $\deg \mathfrak{m}$ of a monomial $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ is defined to be $a_1 + a_2 + \cdots + a_N \in \mathbb{N}$.

(c) A monomial $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ is said to be *squarefree* if $a_1, a_2, \ldots, a_N \in \{0, 1\}$. (This is saying that no square or higher power of an indeterminate appears in $\mathfrak{m}$; thus the name "squarefree".)

(d) A monomial $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ is said to be *primal* if there is at most one $i \in [N]$ satisfying $a_i > 0$. (This is saying that the monomial $\mathfrak{m}$ contains no two distinct indeterminates. Thus, a primal monomial is just 1 or a power of an indeterminate.)

Now we can define some specific symmetric polynomials:

Definition 7.1.9. **(a)** For each $n \in \mathbb{Z}$, define a symmetric polynomial $e_n \in \mathcal{S}$ by

$$e_n = \sum_{\substack{(i_1,i_2,\ldots,i_n)\in[N]^n;\\ i_1<i_2<\cdots<i_n}} x_{i_1}x_{i_2}\cdots x_{i_n} = (\text{sum of all squarefree monomials of degree } n).$$

This e_n is called the *n-th elementary symmetric polynomial* in $x_1, x_2, \ldots, x_N$.

(b) For each $n \in \mathbb{Z}$, define a symmetric polynomial $h_n \in \mathcal{S}$ by

$$h_n = \sum_{\substack{(i_1,i_2,\ldots,i_n)\in[N]^n;\\ i_1\leq i_2\leq\cdots\leq i_n}} x_{i_1}x_{i_2}\cdots x_{i_n} = (\text{sum of all monomials of degree } n).$$

This h_n is called the *n-th complete homogeneous symmetric polynomial* in $x_1, x_2, \ldots, x_N$.

(c) For each $n \in \mathbb{Z}$, define a symmetric polynomial $p_n \in \mathcal{S}$ by

$$\begin{aligned} p_n &= \begin{cases} x_1^n + x_2^n + \cdots + x_N^n, & \text{if } n > 0; \\ 1, & \text{if } n = 0; \\ 0, & \text{if } n < 0 \end{cases} \\ &= (\text{sum of all primal monomials of degree } n). \end{aligned}$$

This p_n is called the *n-th power sum* in $x_1, x_2, \ldots, x_N$.

Example 7.1.10. **(a)** The 2-nd elementary symmetric polynomial is

$$\begin{aligned} e_2 &= \sum_{\substack{(i_1,i_2)\in[N]^2;\\ i_1<i_2}} x_{i_1}x_{i_2} = \sum_{\substack{(i,j)\in[N]^2;\\ i<j}} x_i x_j \\ &= \begin{array}{ccccccccc} x_1x_2 & + & x_1x_3 & + & \cdots & + & x_1x_N \\ & + & x_2x_3 & + & \cdots & + & x_2x_N \\ & & & \ddots & \cdots & \cdots & \cdots \\ & & & & & + & x_{N-1}x_N. \end{array} \end{aligned}$$

(b) The 2-nd complete homogeneous symmetric polynomial is

$$\begin{aligned} h_2 &= \sum_{\substack{(i_1,i_2)\in[N]^2;\\ i_1\leq i_2}} x_{i_1}x_{i_2} = \sum_{\substack{(i,j)\in[N]^2;\\ i\leq j}} x_i x_j \\ &= \begin{array}{ccccccccc} x_1^2 & + & x_1x_2 & + & x_1x_3 & + & \cdots & + & x_1x_N \\ & + & x_2^2 & + & x_2x_3 & + & \cdots & + & x_2x_N \\ & & & & & \ddots & \cdots & \cdots & \cdots \\ & & & & & + & x_{N-1}^2 & + & x_{N-1}x_N \\ & & & & & & & + & x_N^2. \end{array} \end{aligned}$$

(c) The 2-nd power sum is

$$p_2 = x_1^2 + x_2^2 + \cdots + x_N^2.$$

In light of the above two formulas for e_2 and h_2, we thus have $h_2 = p_2 + e_2$.

(d) We have

$$e_1 = h_1 = p_1 = x_1 + x_2 + \cdots + x_N.$$

(e) We have

$$e_0 = h_0 = p_0 = 1.$$

(f) If $n < 0$, then $e_n = h_n = p_n = 0$.

(g) If $N = 0$ (that is, if $\mathcal{P}$ is a polynomial ring in 0 variables), then $e_n = h_n = p_n = 0$ for all $n > 0$ (because there are no monomials of positive degree in this case), but $e_0 = h_0 = p_0 = 1$ still holds. This is a boring border case which, however, is important to get right.

Proposition 7.1.11. For each integer $n > N$, we have $e_n = 0$.

Proof. Let $n > N$ be an integer. Then, the set $[N]$ has no n distinct elements. Thus, there exists no n-tuple $(i_1, i_2, \ldots, i_n) \in [N]^n$ satisfying $i_1 < i_2 < \cdots < i_n$ (because if $(i_1, i_2, \ldots, i_n)$ was such an n-tuple, then its n entries $i_1, i_2, \ldots, i_n$ would be n distinct elements of $[N]$).

Now, the definition of e_n yields

$$\begin{aligned} e_n &= \sum_{\substack{(i_1,i_2,\ldots,i_n)\in[N]^n;\\ i_1<i_2<\cdots<i_n}} x_{i_1} x_{i_2} \cdots x_{i_n} = (\text{empty sum}) \\ &\qquad \left(\begin{array}{c}\text{since there exists no } n\text{-tuple } (i_1, i_2, \ldots, i_n) \in [N]^n \\ \text{satisfying } i_1 < i_2 < \cdots < i_n\end{array}\right) \\ &= 0. \end{aligned}$$

This proves Proposition 7.1.11. □

Thus, there are only N "interesting" elementary symmetric polynomials: namely, $e_1, e_2, \ldots, e_N$. All other e_n's are either 1 or 0.

In contrast, there are infinitely many "interesting" complete homogeneous symmetric polynomials and power sums (provided that $N > 0$). For example, for $N = 2$, we have $h_5 = x_1^5 + x_1^4 x_2 + x_1^3 x_2^2 + x_1^2 x_2^3 + x_1 x_2^4 + x_2^5$ and $p_5 = x_1^5 + x_2^5$.

We have so far defined three sequences $(e_0, e_1, e_2, \ldots)$, $(h_0, h_1, h_2, \ldots)$ and $(p_0, p_1, p_2, \ldots)$ of symmetric polynomials. The following theorem (known as the *Newton–Girard formulas* or the *Newton–Girard identities*) relates these three sequences:

Theorem 7.1.12 (Newton–Girard formulas)**.** For any positive integer n, we have

$$\sum_{j=0}^{n} (-1)^j e_j h_{n-j} = 0; \tag{247}$$

$$\sum_{j=1}^{n} (-1)^{j-1} e_{n-j} p_j = n e_n; \tag{248}$$

$$\sum_{j=1}^{n} h_{n-j} p_j = n h_n. \tag{249}$$

Example 7.1.13. The formula (248), applied to $n = 2$, says that $e_1 p_1 - p_2 = 2e_2$. Therefore,

$$p_2 = e_1 p_1 - 2e_2 = (x_1 + x_2 + \cdots + x_N)(x_1 + x_2 + \cdots + x_N) - 2\sum_{i<j} x_i x_j.$$

Before we prove (part of) Theorem 7.1.12, we establish some equalities in the polynomial rings $\mathcal{P}[t]$ and $\mathcal{P}[u,v]$ (here, t, u, v are three new indeterminates) and in the FPS ring $\mathcal{P}[[t]]$:

Proposition 7.1.14. (a) In the polynomial ring $\mathcal{P}[t]$, we have

$$\prod_{i=1}^{N} (1 - tx_i) = \sum_{n \in \mathbb{N}} (-1)^n t^n e_n.$$

(b) In the polynomial ring $\mathcal{P}[u,v]$, we have

$$\prod_{i=1}^{N} (u - vx_i) = \sum_{n=0}^{N} (-1)^n u^{N-n} v^n e_n.$$

(c) In the FPS ring $\mathcal{P}[[t]]$, we have

$$\prod_{i=1}^{N} \frac{1}{1 - tx_i} = \sum_{n \in \mathbb{N}} t^n h_n.$$

Proof of Proposition 7.1.14 (sketched). **(a)** For each $i \in \{1, 2, \ldots, N\}$, we have

$$1 + tx_i = \sum_{a \in \{0,1\}} (tx_i)^a.$$

Multiplying these equalities over all $i \in \{1, 2, \ldots, N\}$, we obtain

$$\begin{aligned}
\prod_{i=1}^{N} (1 + tx_i) &= \prod_{i=1}^{N} \sum_{a \in \{0,1\}} (tx_i)^a = \sum_{(a_1, a_2, \ldots, a_N) \in \{0,1\}^N} \underbrace{(tx_1)^{a_1} (tx_2)^{a_2} \cdots (tx_N)^{a_N}}_{= t^{a_1 + a_2 + \cdots + a_N} x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}} \\
&\qquad \text{(by Proposition 3.11.22)} \\
&= \sum_{(a_1, a_2, \ldots, a_N) \in \{0,1\}^N} t^{a_1 + a_2 + \cdots + a_N} x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N} = \sum_{\substack{\mathfrak{m} \text{ is a squarefree} \\ \text{monomial}}} t^{\deg \mathfrak{m}} \mathfrak{m} \\
&\qquad \left(\begin{array}{c} \text{since the squarefree monomials are precisely} \\ \text{the } x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N} \text{ with } (a_1, a_2, \ldots, a_N) \in \{0,1\}^N, \\ \text{and since the degree of such a monomial} \\ \text{is precisely } a_1 + a_2 + \cdots + a_N \end{array} \right) \\
&= \sum_{n \in \mathbb{N}} \sum_{\substack{\mathfrak{m} \text{ is a squarefree} \\ \text{monomial of degree } n}} t^n \mathfrak{m} \qquad \left(\begin{array}{c} \text{here, we have split the sum} \\ \text{according to the value of } \deg \mathfrak{m} \end{array} \right) \\
&= \sum_{n \in \mathbb{N}} t^n \underbrace{\sum_{\substack{\mathfrak{m} \text{ is a squarefree} \\ \text{monomial of degree } n}} \mathfrak{m}}_{\substack{= (\text{sum of all squarefree monomials of degree } n) \\ = e_n \\ \text{(by the definition of } e_n)}} \\
&= \sum_{n \in \mathbb{N}} t^n e_n.
\end{aligned}$$

Substituting $-t$ for t on both sides of this equality, we obtain

$$\prod_{i=1}^{N} (1 - tx_i) = \sum_{n \in \mathbb{N}} \underbrace{(-t)^n}_{= (-1)^n t^n} e_n = \sum_{n \in \mathbb{N}} (-1)^n t^n e_n.$$

This proves Proposition 7.1.14 **(a)**.

(b) This is similar to part **(a)**. (See Exercise A.6.1.1 for details.)

(c) For each $i \in \{1, 2, \ldots, N\}$, we have

$$\begin{aligned}
\frac{1}{1 - tx_i} &= 1 + tx_i + (tx_i)^2 + (tx_i)^3 + \cdots \\
&\qquad \left(\begin{array}{c} \text{by substituting } tx_i \text{ for } x \text{ in the} \\ \text{geometric series formula (5)} \end{array} \right) \\
&= \sum_{a \in \mathbb{N}} (tx_i)^a.
\end{aligned}$$

Multiplying these equalities over all $i \in \{1, 2, \ldots, N\}$, we obtain

$$\begin{aligned}
\prod_{i=1}^{N} \frac{1}{1 - tx_i} &= \prod_{i=1}^{N} \sum_{a \in \mathbb{N}} (tx_i)^a \\
&= \sum_{(a_1, a_2, \ldots, a_N) \in \mathbb{N}^N} \underbrace{(tx_1)^{a_1} (tx_2)^{a_2} \cdots (tx_N)^{a_N}}_{= t^{a_1 + a_2 + \cdots + a_N} x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}} \\
&\qquad \text{(by Proposition 3.11.23)} \\
&= \sum_{(a_1, a_2, \ldots, a_N) \in \mathbb{N}^N} t^{a_1 + a_2 + \cdots + a_N} x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N} = \sum_{\mathfrak{m} \text{ is a monomial}} t^{\deg \mathfrak{m}} \mathfrak{m} \\
&\qquad \left(\begin{array}{c} \text{since the monomials are precisely} \\ \text{the } x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N} \text{ with } (a_1, a_2, \ldots, a_N) \in \mathbb{N}^N, \\ \text{and since the degree of such a monomial} \\ \text{is precisely } a_1 + a_2 + \cdots + a_N \end{array}\right) \\
&= \sum_{n \in \mathbb{N}} \sum_{\substack{\mathfrak{m} \text{ is a monomial} \\ \text{of degree } n}} t^n \mathfrak{m} \qquad \left(\begin{array}{c} \text{here, we have split the sum} \\ \text{according to the value of } \deg \mathfrak{m} \end{array}\right) \\
&= \sum_{n \in \mathbb{N}} t^n \underbrace{\sum_{\substack{\mathfrak{m} \text{ is a monomial} \\ \text{of degree } n}} \mathfrak{m}}_{\substack{= (\text{sum of all monomials of degree } n) = h_n \\ (\text{by the definition of } h_n)}} = \sum_{n \in \mathbb{N}} t^n h_n .
\end{aligned}$$

This proves Proposition 7.1.14 **(c)**. □

Let us now prove the first Newton–Girard formula (247):

Proof of the 1st Newton–Girard formula (247). In the FPS ring $\mathcal{P}[[t]]$, we have

$$\prod_{i=1}^{N} (1 - tx_i) = \sum_{n \in \mathbb{N}} (-1)^n t^n e_n \qquad \text{(by Proposition 7.1.14 } \textbf{(a)}\text{)}$$

and

$$\prod_{i=1}^{N} \frac{1}{1 - tx_i} = \sum_{n \in \mathbb{N}} t^n h_n \qquad \text{(by Proposition 7.1.14 } \textbf{(c)}\text{)} .$$

Multiplying these two equalities, we obtain

$$\begin{aligned}
&\left(\prod_{i=1}^{N}(1-tx_i)\right)\left(\prod_{i=1}^{N}\frac{1}{1-tx_i}\right)\\
&=\left(\sum_{n\in\mathbb{N}}(-1)^n t^n e_n\right)\left(\sum_{n\in\mathbb{N}} t^n h_n\right)=\left(\sum_{j\in\mathbb{N}}(-1)^j t^j e_j\right)\left(\sum_{k\in\mathbb{N}} t^k h_k\right)\\
&\qquad\qquad\left(\begin{array}{c}\text{here, we have renamed the summation}\\ \text{indices } n \text{ and } n \text{ (in the two sums) as } j \text{ and } k\end{array}\right)\\
&=\underbrace{\sum_{j\in\mathbb{N}}\sum_{k\in\mathbb{N}}}_{=\sum\limits_{(j,k)\in\mathbb{N}^2}}(-1)^j\underbrace{t^je_jt^kh_k}_{=e_jh_kt^{j+k}}=\sum_{(j,k)\in\mathbb{N}^2}(-1)^j e_jh_kt^{j+k}\\
&=\sum_{n\in\mathbb{N}}\left(\sum_{\substack{(j,k)\in\mathbb{N}^2;\\ j+k=n}}(-1)^j e_jh_k\right)t^n
\end{aligned}$$

(here, we have split the sum according to the value of $j+k$). Comparing this with

$$\left(\prod_{i=1}^{N}(1-tx_i)\right)\left(\prod_{i=1}^{N}\frac{1}{1-tx_i}\right)=\prod_{i=1}^{N}\underbrace{\left((1-tx_i)\cdot\frac{1}{1-tx_i}\right)}_{=1}=\prod_{i=1}^{N}1=1,$$

we obtain

$$1=\sum_{n\in\mathbb{N}}\left(\sum_{\substack{(j,k)\in\mathbb{N}^2;\\ j+k=n}}(-1)^j e_jh_k\right)t^n.$$

This is an equality between two FPSs in $\mathcal{P}[[t]]$. Comparing coefficients in front of t^n, we conclude that each positive integer n satisfies

$$0=\sum_{\substack{(j,k)\in\mathbb{N}^2;\\ j+k=n}}(-1)^j e_jh_k=\sum_{j=0}^{n}(-1)^j e_jh_{n-j}$$

(here, we have substituted $(j,n-j)$ for (j,k) in the sum, since the map $\{0,1,\ldots,n\}\to\left\{(j,k)\in\mathbb{N}^2 \mid j+k=n\right\}$ that sends each $j\in\{0,1,\ldots,n\}$ to the pair $(j,n-j)$ is a bijection). This proves the 1st Newton–Girard formula (247). □

Proving the other two formulas in Theorem 7.1.12 is a homework problem (Exercise A.6.1.3). Note that there exist proofs of different kinds: FPS manipulations; induction; sign-reversing involutions.

Note that our above proof of Theorem 7.1.12 attests to the usefulness of generating functions: Even though the polynomials $f \in \mathcal{P}$ already involve N variables $x_1, x_2, \ldots, x_N$, the proof proceeds by adjoining yet another variable t (to form the ring $\mathcal{P}[[t]]$).

The Newton–Girard formulas can be used to express the e_i's and the h_i's in terms of each other, and the p_i's in terms of the e_i's and the h_i's, and finally the e_i's and the h_i's in terms of the p_i's when K is a commutative $\mathbb{Q}$-algebra (i.e., when the numbers $1, 2, 3, \ldots$ have inverses in K). More generally, it turns out that we can express any symmetric polynomial in terms of e_i's or of h_i's or (if K is a commutative $\mathbb{Q}$-algebra) of p_i's:

Theorem 7.1.15 (Fundamental Theorem of Symmetric Polynomials, due to Gauss et al.)**.** **(a)** The elementary symmetric polynomials $e_1, e_2, \ldots, e_N$ are algebraically independent (over K) and generate the K-algebra $\mathcal{S}$.

In other words, each $f \in \mathcal{S}$ can be uniquely written as a polynomial in $e_1, e_2, \ldots, e_N$.

In yet other words, the map

$$\underbrace{K[y_1, y_2, \ldots, y_N]}_{\substack{\text{a polynomial ring} \\ \text{in } N \text{ variables}}} \to \mathcal{S},$$
$$g \mapsto g[e_1, e_2, \ldots, e_N]$$

is a K-algebra isomorphism.

(b) The complete homogeneous symmetric polynomials $h_1, h_2, \ldots, h_N$ are algebraically independent (over K) and generate the K-algebra $\mathcal{S}$.

In other words, each $f \in \mathcal{S}$ can be uniquely written as a polynomial in $h_1, h_2, \ldots, h_N$.

In yet other words, the map

$$\underbrace{K[y_1, y_2, \ldots, y_N]}_{\substack{\text{a polynomial ring} \\ \text{in } N \text{ variables}}} \to \mathcal{S},$$
$$g \mapsto g[h_1, h_2, \ldots, h_N]$$

is a K-algebra isomorphism.

(c) Now assume that K is a commutative $\mathbb{Q}$-algebra (e.g., a field of characteristic 0). Then, the power sums $p_1, p_2, \ldots, p_N$ are algebraically independent (over K) and generate the K-algebra $\mathcal{S}$.

In other words, each $f \in \mathcal{S}$ can be uniquely written as a polynomial in $p_1, p_2, \ldots, p_N$.

In yet other words, the map

$$\underbrace{K[y_1, y_2, \ldots, y_N]}_{\substack{\text{a polynomial ring} \\ \text{in } N \text{ variables}}} \to \mathcal{S},$$
$$g \mapsto g[p_1, p_2, \ldots, p_N]$$

is a K-algebra isomorphism.

Example 7.1.16. **(a)** Theorem 7.1.15 **(a)** yields that p_3 can be uniquely written as a polynomial in $e_1, e_2, \ldots, e_N$. How to write it this way?

Here is a method that (more generally) can be used to express p_n (for any given $n > 0$) as a polynomial in $e_1, e_2, \ldots, e_n$. This method is recursive, so we assume that all the "smaller" power sums $p_1, p_2, \ldots, p_{n-1}$ have already been expressed in this way. Now, the 2nd Newton–Girard formula (248) yields

$$\begin{aligned} ne_n &= \sum_{j=1}^{n} (-1)^{j-1} e_{n-j} p_j = \sum_{j=1}^{n-1} (-1)^{j-1} e_{n-j} p_j + (-1)^{n-1} \underbrace{e_{n-n}}_{=e_0=1} p_n \\ &\qquad \left(\begin{array}{c} \text{here, we have split off the addend} \\ \text{for } j = n \text{ from the sum} \end{array} \right) \\ &= \sum_{j=1}^{n-1} (-1)^{j-1} e_{n-j} p_j + (-1)^{n-1} p_n. \end{aligned}$$

Solving this equality for p_n, we obtain

$$p_n = (-1)^{n-1} \left(ne_n - \sum_{j=1}^{n-1} (-1)^{j-1} e_{n-j} p_j \right).$$

The right hand side can now be expressed in terms of $e_1, e_2, \ldots, e_n$ (since the only power sums appearing in it are $p_1, p_2, \ldots, p_{n-1}$, which we already know how to express in these terms); therefore, we obtain an expression of p_n as a polynomial in $e_1, e_2, \ldots, e_n$.

For example, here is what we obtain for $n \in [4]$ by following this method:

$$\begin{aligned} p_1 &= e_1; \\ p_2 &= e_1^2 - 2e_2; \\ p_3 &= e_1^3 - 3e_2e_1 + 3e_3; \\ p_4 &= e_1^4 - 4e_2e_1^2 + 2e_2^2 + 4e_3e_1 - 4e_4. \end{aligned}$$

If $N < n$, then this expression of p_n as a polynomial in $e_1, e_2, \ldots, e_n$ becomes an expression as a polynomial in $e_1, e_2, \ldots, e_N$ if we throw away all addends that contain one of $e_{N+1}, e_{N+2}, \ldots, e_n$ as factor (we are allowed to do this, because Proposition 7.1.11 shows that all these addends are 0). For example, if $N = 2$, then the expression $p_4 = e_1^4 - 4e_2e_1^2 + 2e_2^2 + 4e_3e_1 - 4e_4$ becomes $p_4 = e_1^4 - 4e_2e_1^2 + 2e_2^2$ this way.

(b) Theorem 7.1.15 **(b)** yields that p_3 can be uniquely written as a polynomial in $h_1, h_2, \ldots, h_N$. How to write it this way?

In part **(a)**, we have given a method to express p_n (for any given $n > 0$) as a polynomial in $e_1, e_2, \ldots, e_n$. A similar method (but using (249) instead of (248)) can be used to express p_n (for any given $n > 0$) as a polynomial in $h_1, h_2, \ldots, h_n$. For example, for $n \in [4]$, this method produces

$$\begin{aligned}
p_1 &= h_1; \\
p_2 &= -h_1^2 + 2h_2; \\
p_3 &= h_1^3 - 3h_2h_1 + 3h_3; \\
p_4 &= -h_1^4 + 4h_2h_1^2 - 2h_2^2 - 4h_3h_1 + 4h_4.
\end{aligned}$$

(The similarity with the analogous formulas expressing p_n in terms of $e_1, e_2, \ldots, e_n$ is not accidental – the formulas are indeed identical when n is odd and differ in all signs when n is even. Proving this is Exercise A.6.1.7 **(b)**.)

So we can express p_n as a polynomial in $h_1, h_2, \ldots, h_n$. However, expressing p_n as a polynomial in $h_1, h_2, \ldots, h_N$ is harder when $N < n$. For example, if $N = 2$, then the former expression is $p_4 = -h_1^4 + 4h_2h_1^2 - 2h_2^2 - 4h_3h_1 + 4h_4$, while the latter is $p_4 = -h_1^4 + 2h_2^2$; there is no easy way to get the latter from the former.

(c) Assume that K is a $\mathbb{Q}$-algebra. Theorem 7.1.15 **(c)** yields that e_3 can be uniquely written as a polynomial in $p_1, p_2, \ldots, p_N$. How to write it this way?

In part **(a)**, we have given a method to express p_n (for any given $n > 0$) as a polynomial in $e_1, e_2, \ldots, e_n$. The crux of this method was to solve the equation (248) for p_n. If we instead solve it for e_n (which is almost immediate: it gives $e_n = \dfrac{1}{n} \sum\limits_{j=1}^{n} (-1)^{j-1} e_{n-j} p_j$), then we obtain a method for expressing e_n (for any given $n > 0$) as a polynomial in $p_1, p_2, \ldots, p_n$. Applied to all $n \in [4]$, this method produces

$$\begin{aligned}
e_1 &= p_1; \\
e_2 &= \frac{1}{2}p_1^2 - \frac{1}{2}p_2; \\
e_3 &= \frac{1}{6}p_1^3 - \frac{1}{2}p_2p_1 + \frac{1}{3}p_3; \\
e_4 &= \frac{1}{24}p_1^4 - \frac{1}{4}p_2p_1^2 + \frac{1}{8}p_2^2 + \frac{1}{3}p_3p_1 - \frac{1}{4}p_4.
\end{aligned}$$

Note the fractions on the right hand sides! This is why we required K to be a $\mathbb{Q}$-algebra in Theorem 7.1.15 **(c)**. In general, we cannot express e_n in terms of $p_1, p_2, \ldots, p_n$ if the integer n is not invertible in K.

The question of expressing e_n as a polynomial in $p_1, p_2, \ldots, p_N$ (as opposed to $p_1, p_2, \ldots, p_n$) is easily reduced to what we just have done: If $n \leq N$, then we have answered it already; if $n > N$, then the answer is $e_n = 0$ (by Proposition 7.1.11).

(d) Not even algebraic independence of $p_1, p_2, \ldots, p_N$ is true in general (if we don't assume that K is a $\mathbb{Q}$-algebra)! Indeed, if $K = \mathbb{Z}/2$, then

$$p_1^2 = (x_1 + x_2 + \cdots + x_N)^2 = \underbrace{x_1^2 + x_2^2 + \cdots + x_N^2}_{=p_2} + 2 \underbrace{\sum_{i<j} x_i x_j}_{\substack{=0 \\ \text{if } K=\mathbb{Z}/2}} = p_2.$$

More generally, if $K = \mathbb{Z}/p$ for some prime p, then the Idiot's Binomial Formula (i.e., the formula $(x+y)^p = x^p + y^p$ that holds in any commutative $\mathbb{Z}/p$-algebra) yields $p_1^p = p_p$. (Did I mention that lowercase letters are in short supply in the theory of symmetric polynomials?)

(e) If $N = 3$, then Theorem 7.1.15 **(b)** yields that h_4 can be written as a polynomial in h_1, h_2, h_3. Here is how this looks like:

$$h_4 = h_1^4 - 3h_2h_1^2 + h_2^2 + 2h_3h_1.$$

(f) If $N = 3$, then

$$((x-y)(y-z)(z-x))^2 = e_2^2e_1^2 - 4e_2^3 - 4e_3e_1^3 + 18e_3e_2e_1 - 27e_3^2$$

(where we are again denoting x_1, x_2, x_3 by x, y, z).

We omit the proof of Theorem 7.1.15 for now.

Let us record a useful criterion for showing that a polynomial is symmetric:

Lemma 7.1.17. For each $i \in [N-1]$, we consider the simple transposition $s_i \in S_N$ defined in Definition 5.2.3 (applied to $n = N$).

Let $f \in \mathcal{P}$. Assume that

$$s_k \cdot f = f \qquad \text{for each } k \in [N-1]. \tag{250}$$

Then, the polynomial f is symmetric.

In plainer terms, Lemma 7.1.17 says that if a polynomial $f \in \mathcal{P}$ remains unchanged whenever we swap two adjacent indeterminates (i.e., it remains unchanged if we swap x_1 with x_2; it remains unchanged if we swap x_2 with x_3; it remains unchanged if we swap x_3 with x_4; etc.), then this polynomial f is symmetric. For example, for $N = 3$, it says that if a polynomial $f \in K[x_1, x_2, x_3]$ satisfies $f[x_2, x_1, x_3] = f$ and $f[x_1, x_3, x_2] = f$, then f is symmetric.

Proof of Lemma 7.1.17. This follows from Corollary 5.3.22 or from Theorem 5.3.17 **(a)**. See Section B.5 for the details of this proof. □

7.2. N-partitions and monomial symmetric polynomials

Recall that an *(integer) partition* means a weakly decreasing finite tuple of positive integers – such as $(5,3,3,2,1)$.

Let us define a variant of this notion:

Definition 7.2.1. An *N-partition* will mean a weakly decreasing N-tuple of nonnegative integers. In other words, an N-partition means an N-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_N) \in \mathbb{N}^N$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$.

For example, $(5,3,3,2,1,0,0)$ is a 7-partition.

Per se, an N-partition can contain zeroes and thus is not always a partition. However, the N-partitions are "more or less the same" as the partitions of length $\leq N$. Indeed:

Proposition 7.2.2. There is a bijection

$$\{\text{partitions of length } \leq N\} \to \{N\text{-partitions}\},$$
$$(\lambda_1, \lambda_2, \ldots, \lambda_\ell) \mapsto \left(\lambda_1, \lambda_2, \ldots, \lambda_\ell, \underbrace{0, 0, \ldots, 0}_{N-\ell \text{ zeroes}}\right).$$

Proof. Straightforward. (We essentially did this back in our proof of Proposition 4.4.7 **(a)**, although we used the letter k instead of N back then.) □

The N-partitions turn out to be closely connected to the ring $\mathcal{S}$. Indeed, we will soon see various bases of the K-module $\mathcal{S}$, all of which are indexed by the N-partitions. We shall construct the simplest one in a moment. First, we define some auxiliary notations:

Definition 7.2.3. Let $a = (a_1, a_2, \ldots, a_N) \in \mathbb{N}^N$. Then:

(a) We let x^a denote the monomial $x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$.

(b) We let $\operatorname{sort} a$ mean the N-partition obtained from a by sorting the entries of a in weakly decreasing order.

For example, if $N = 5$, then $x^{(1,5,0,4,4)} = x_1^1 x_2^5 x_3^0 x_4^4 x_5^4 = x_1 x_2^5 x_4^4 x_5^4$ and $\operatorname{sort}(1,5,0,4,4) = (5,4,4,1,0)$.

Definition 7.2.4. Let λ be any N-partition. Then, we define a symmetric polynomial $m_\lambda \in \mathcal{S}$ by

$$m_\lambda := \sum_{\substack{a \in \mathbb{N}^N; \\ \operatorname{sort} a = \lambda}} x^a.$$

This is called the *monomial symmetric polynomial corresponding to λ*.

Example 7.2.5. Let $N = 3$. Then,

$$\begin{aligned} m_{(2,1,0)} &= \sum_{\substack{a \in \mathbb{N}^3; \\ \operatorname{sort} a = (2,1,0)}} x^a = x^{(2,1,0)} + x^{(2,0,1)} + x^{(1,2,0)} + x^{(1,0,2)} + x^{(0,2,1)} + x^{(0,1,2)} \\ &= x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2 \end{aligned}$$

and

$$\begin{aligned} m_{(3,2,1)} &= \sum_{\substack{a \in \mathbb{N}^3; \\ \operatorname{sort} a = (3,2,1)}} x^a = x^{(3,2,1)} + x^{(3,1,2)} + x^{(2,3,1)} + x^{(2,1,3)} + x^{(1,3,2)} + x^{(1,2,3)} \\ &= x_1^3 x_2^2 x_3 + x_1^3 x_2 x_3^2 + x_1^2 x_2^3 x_3 + x_1^2 x_2 x_3^3 + x_1 x_2^3 x_3^2 + x_1 x_2^2 x_3^3 \\ &= x_1^3 x_2^2 x_3 + (\text{all other 5 permutations of this monomial}) \end{aligned}$$

and

$$\begin{aligned} m_{(2,2,1)} &= \sum_{\substack{a \in \mathbb{N}^3; \\ \operatorname{sort} a = (2,2,1)}} x^a = x^{(2,2,1)} + x^{(2,1,2)} + x^{(1,2,2)} \\ &= x_1^2 x_2^2 x_3 + x_1^2 x_2 x_3^2 + x_1 x_2^2 x_3^2 \end{aligned}$$

and

$$m_{(2,2,2)} = \sum_{\substack{a \in \mathbb{N}^3; \\ \operatorname{sort} a = (2,2,2)}} x^a = x_1^2 x_2^2 x_3^2.$$

Our symmetric polynomials e_n, h_n and p_n so far can be easily expressed in terms of monomial symmetric polynomials:

Proposition 7.2.6. (a) For each $n \in \{0, 1, \ldots, N\}$, we have

$$e_n = m_{(1,1,\ldots,1,0,0,\ldots,0)},$$

where $(1, 1, \ldots, 1, 0, 0, \ldots, 0)$ is the N-tuple that begins with n many 1's and ends with $N - n$ many 0's.

(b) For each $n \in \mathbb{N}$, we have

$$h_n = \sum_{\substack{\lambda \text{ is an } N\text{-partition}; \\ |\lambda| = n}} m_\lambda,$$

where the *size* $|\lambda|$ of an N-partition λ is defined to be the sum of its entries (i.e., if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$, then $|\lambda| := \lambda_1 + \lambda_2 + \cdots + \lambda_N$).

(c) Assume that $N > 0$. For each $n \in \mathbb{N}$, we have

$$p_n = m_{(n,0,0,\ldots,0)},$$

where $(n, 0, 0, \ldots, 0)$ is the N-tuple that begins with an n and ends with $N-1$ zeroes.

Proof. Easy and LTTR. □

The monomial symmetric polynomials m_λ are the "building blocks" of symmetric polynomials, in the same way as the monomials are the "building blocks" of polynomials. Here is a way to make this precise:

Theorem 7.2.7. (a) The family $(m_\lambda)_{\lambda \text{ is an } N\text{-partition}}$ is a basis of the K-module $\mathcal{S}$.

(b) Each symmetric polynomial $f \in \mathcal{S}$ satisfies

$$f = \sum_{\substack{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N) \\ \text{is an } N\text{-partition}}} \left(\left[x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_N^{\lambda_N} \right] f \right) m_\lambda .$$

(c) Let $n \in \mathbb{N}$. Let

$$\mathcal{S}_n := \{\text{homogeneous symmetric polynomials } f \in \mathcal{P} \text{ of degree } n\}$$

(where we understand the zero polynomial $0 \in \mathcal{P}$ to be homogeneous of every degree). Then, $\mathcal{S}_n$ is a K-submodule of $\mathcal{S}$.

(d) Define the *size* of any N-partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ to be the number $\lambda_1 + \lambda_2 + \cdots + \lambda_N \in \mathbb{N}$. Then, the family $(m_\lambda)_{\lambda \text{ is an } N\text{-partition of size } n}$ is a basis of the K-module $\mathcal{S}_n$.

Example 7.2.8. Let $N = 3$, and let us rename the indeterminates x_1, x_2, x_3 as x, y, z. The polynomial $(x+y)(y+z)(z+x)$ is symmetric, thus belongs to $\mathcal{S}$. Expanding it, we find

$$\begin{aligned}(x+y)(y+z)(z+x) &= \underbrace{x^2y + x^2z + y^2x + y^2z + z^2x + z^2y}_{=m_{(2,1,0)}} + 2 \underbrace{xyz}_{=m_{(1,1,1)}} \\ &= m_{(2,1,0)} + 2m_{(1,1,1)}.\end{aligned}$$

Thus, we have written $(x+y)(y+z)(z+x)$ as a K-linear combination of m_λ's for various N-partitions λ. The same procedure (i.e., expanding, and then collecting monomials that differ only in the order of their exponents, such as the monomials $x^2y, x^2z, y^2x, y^2z, z^2x, z^2y$ in our example) can be applied to any symmetric polynomial $f \in \mathcal{S}$, and always results in a representation of f as a K-linear combination of m_λ's (because the symmetry of f ensures that monomials that differ only in the order of their exponents appear in f with equal coefficients).

The proof of Theorem 7.2.7 will rely on a simple proposition that expresses how a permutation $\sigma \in S_N$ transforms the coefficients of a polynomial $f \in \mathcal{P}$ (guess what: it permutes these coefficients):

Proposition 7.2.9. Let $\sigma \in S_N$ and $f \in \mathcal{P}$. Then,

$$\left[x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}\right] (\sigma \cdot f) = \left[x_1^{a_{\sigma(1)}} x_2^{a_{\sigma(2)}} \cdots x_N^{a_{\sigma(N)}}\right] f$$

for any $(a_1, a_2, \ldots, a_N) \in \mathbb{N}^N$.

Here, as in Section 3.15, we are using the notation $\left[x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}\right] g$ for the coefficient of a monomial $x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ in a polynomial $g \in \mathcal{P}$.

The proof of Proposition 7.2.9 is quite easy and can be found in Section B.6.

Proof of Theorem 7.2.7 (sketched). Here is a rough outline of the proof; we leave the details to the reader.

(a) The method shown in Example 7.2.8 shows that each $f \in \mathcal{S}$ is a K-linear combination of the family $(m_\lambda)_{\lambda \text{ is an } N\text{-partition}}$. Thus, this family spans $\mathcal{S}$. It remains to show that this family is K-linearly independent.

To show this, we observe that if you expand a linear combination $\sum\limits_{\lambda \text{ is an } N\text{-partition}} a_\lambda m_\lambda$ (where $a_\lambda \in K$), then none of the addends can cancel (since no two m_λ's have any monomial in common[122]); thus, the linear combination cannot be 0 unless all the a_λ's are 0. This proves the K-linear independence of the family $(m_\lambda)_{\lambda \text{ is an } N\text{-partition}}$. Thus, the proof of Theorem 7.2.7 **(a)** is complete.

(b) This should be clear from Example 7.2.8 as well.

(c) This is rather obvious: Any K-linear combination of homogeneous polynomials of degree n is again homogeneous of degree n.

(d) This follows by the same argument as part **(a)**, except that we now need to observe that homogeneous polynomials of degree n are K-linear combinations of degree-n monomials (rather than arbitrary monomials). □

7.3. Schur polynomials

7.3.1. Alternants

Here is one way to generate symmetric polynomials:

Example 7.3.1. Let $N = 3$, and let us again abbreviate the indeterminates x_1, x_2, x_3 as x, y, z. For simplicity, we assume that K is a field. As we know (from the Vandermonde determinant – specifically, Theorem 6.4.31 **(a)**), we have

$$\det \begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix} = \prod_{i<j} (x_i - x_j) = (x-y)(x-z)(y-z).$$

[122] and since each m_λ contains at least one monomial (trivial observation, but should not be forgotten)

What about similar determinants, such as $\det\begin{pmatrix} x^5 & x^3 & 1 \\ y^5 & y^3 & 1 \\ z^5 & z^3 & 1 \end{pmatrix}$? Just as in the proof of Lemma 6.4.33 (in which we computed the original Vandermonde determinant), we can argue that this is a polynomial in x, y, z that is divisible by each of $x - y$ and $x - z$ and $y - z$ (since it becomes 0 if we set one of x, y, z equal to another). Hence,

$$\det\begin{pmatrix} x^5 & x^3 & 1 \\ y^5 & y^3 & 1 \\ z^5 & z^3 & 1 \end{pmatrix} = (x-y)(x-z)(y-z) \cdot q$$

for some $q \in K[x, y, z]$. However, this time, degree considerations yield $\deg q = 8 - 3 = 5$, so q is no longer just a constant. What is q ? Using computer algebra, we see that

$$\begin{aligned} q &= \frac{\det\begin{pmatrix} x^5 & x^3 & 1 \\ y^5 & y^3 & 1 \\ z^5 & z^3 & 1 \end{pmatrix}}{(x-y)(x-z)(y-z)} = \frac{-x^5y^3 + x^5z^3 + x^3y^5 - x^3z^5 - y^5z^3 + y^3z^5}{-x^2y + x^2z + xy^2 - xz^2 - y^2z + yz^2} \\ &= x^2y^3 + x^3y^2 + x^2z^3 + x^3z^2 + y^2z^3 + y^3z^2 + xyz^3 \\ &\qquad + xy^3z + x^3yz + 2xy^2z^2 + 2x^2yz^2 + 2x^2y^2z \\ &= m_{(3,2,0)} + m_{(3,1,1)} + 2m_{(2,2,1)} \in \mathcal{S}. \end{aligned}$$

Note that $q \in \mathcal{S}$ can be easily seen without computing q. Indeed, if we swap two of our variables x, y, z, then both $\det\begin{pmatrix} x^5 & x^3 & 1 \\ y^5 & y^3 & 1 \\ z^5 & z^3 & 1 \end{pmatrix}$ and $(x-y)(x-z)(y-z)$ get multiplied by -1, so their ratio q stays unchanged. This shows that $\sigma \cdot q = q$ whenever $\sigma \in S_3$ is a transposition. Since the transpositions generate the group S_3 (indeed, Corollary 5.3.22 yields that the simple transpositions s_1, s_2 generate S_3), this entails that $\sigma \cdot q = q$ for any $\sigma \in S_3$ (not just for transpositions). This means that q is symmetric.

There is nothing special about the exponents 5 and 3 and 0 in the above determinant. More generally, for any $a, b, c \in \mathbb{N}$, we can define the so-called *alternant*

$$\det\begin{pmatrix} x^a & x^b & x^c \\ y^a & y^b & y^c \\ z^a & z^b & z^c \end{pmatrix} \in \mathcal{P}.$$

When studying this alternant, we can WLOG assume that a, b, c are distinct (since otherwise, the alternant is just 0) and furthermore assume that $a >$

$b > c$ (since the general case is reduced to this one by swapping the columns around). The alternant is then a polynomial divisible by $x - y$ and $x - z$ and $y - z$ (since it becomes 0 if we set one of x, y, z equal to another), and thus divisible by $(x - y)(x - z)(y - z) = \det \begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix}$ (the simplest nonzero alternant). Moreover, the ratio

$$\frac{\det \begin{pmatrix} x^a & x^b & x^c \\ y^a & y^b & y^c \\ z^a & z^b & z^c \end{pmatrix}}{(x-y)(x-z)(y-z)} = \frac{\det \begin{pmatrix} x^a & x^b & x^c \\ y^a & y^b & y^c \\ z^a & z^b & z^c \end{pmatrix}}{\det \begin{pmatrix} x^2 & x & 1 \\ y^2 & y & 1 \\ z^2 & z & 1 \end{pmatrix}}$$

is a symmetric polynomial in x, y, z (by the same argument that we used before). Some experimentation suggests that all coefficients of this polynomial are positive integers (to be rigorous, nonnegative integers). There is probably no way of showing this without explicitly finding this polynomial – and the best way to do so is by defining this polynomial combinatorially.

Let us prepare for doing this.

Definition 7.3.2. (a) We let ρ be the N-tuple $(N-1, N-2, \ldots, N-N) \in \mathbb{N}^N$.

(b) For any N-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{N}^N$, we define

$$a_\alpha := \det \left(\underbrace{\left(x_i^{\alpha_j} \right)_{1 \leq i \leq N,\ 1 \leq j \leq N}}_{\in \mathcal{P}^{N \times N}} \right) \in \mathcal{P}.$$

This is called the *α-alternant* (of $x_1, x_2, \ldots, x_N$).

For example, for $N = 3$, we have

$$a_{(5,3,0)} = \det \begin{pmatrix} x^5 & x^3 & 1 \\ y^5 & y^3 & 1 \\ z^5 & z^3 & 1 \end{pmatrix} \qquad \text{(where } (x, y, z) = (x_1, x_2, x_3)\text{)}.$$

Note that the definition of a_ρ yields

$$\begin{aligned} a_\rho &= \det\left(\left(x_i^{\rho_j}\right)_{1\leq i\leq N,\ 1\leq j\leq N}\right) = \det\left(\left(x_i^{N-j}\right)_{1\leq i\leq N,\ 1\leq j\leq N}\right) \\ &\qquad\qquad (\text{since } \rho_j = N-j \text{ for each } j\in[N]) \\ &= \prod_{1\leq i<j\leq N} (x_i - x_j) \end{aligned} \tag{251}$$

(by Theorem 6.4.31 **(a)**, applied to N, $\mathcal{P}$ and x_i instead of n, K and a_i).

Thus, we suspect:

> **Conjecture 7.3.3.** For every $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{N}^N$, the alternant a_α is a multiple of a_ρ in the polynomial ring $\mathcal{P}$. Furthermore, if $\alpha_1 > \alpha_2 > \cdots > \alpha_N$, then the polynomial a_α / a_ρ has positive (more precisely, nonnegative) integer coefficients.

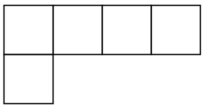
We will prove this by explicitly constructing a_α / a_ρ combinatorially.

7.3.2. Young diagrams and Schur polynomials

Let us first define the *Young diagram* of an N-partition. This is analogous to the definition of the Young diagram of a partition (which we did back in the proof of Proposition 4.1.14):

> **Definition 7.3.4.** Let λ be an N-partition.
>
> The *Young diagram* of λ is defined to be a table of N left-aligned rows, with the i-th row (counted from the top, as always) having λ_i boxes. Formally, the Young diagram of λ is defined as the set
>
> $$\{(i,j) \mid i \in [N] \text{ and } j \in [\lambda_i]\} \subseteq \{1,2,3,\ldots\}^2 .$$
>
> We visually represent each element (i,j) of this Young diagram as a box in row i and column j; thus we obtain a table with N left-aligned rows (some of which might be empty).
>
> We denote the Young diagram of λ by $Y(\lambda)$.

For example, the 3-partition $(4,1,0)$ has Young diagram



.

(The 3-rd row is invisible since it has length 0.) The four boxes in the 1-st (i.e., topmost) row of this diagram are $(1,1)$, $(1,2)$, $(1,3)$ and $(1,4)$ (from left to right), while the single box in its 2-nd row is $(2,1)$.

Now, we are going to fill our Young diagrams – i.e., to put numbers in the boxes:

Definition 7.3.5. Let λ be an N-partition.

A *Young tableau* of shape λ means a way of filling the boxes of $Y(\lambda)$ with elements of $[N]$ (one element per box). Formally speaking, it is defined as a map $T : Y(\lambda) \to [N]$. We visually represent such a map by filling in the number $T(i,j)$ into each box (i,j).

We often abbreviate "Young tableau" as "*tableau*". The plural of "tableau" is "tableaux".

For instance, here is a Young tableau of shape $(4,3,3,0,0,0,0,\ldots,0)$ (defined for any $N \geq 7$):

$$\begin{array}{|c|c|c|c|}\hline 1 & 7 & 2 & 4 \\ \hline 3 & 3 & 6 \\ \cline{1-3} 2 & 6 & 1 \\ \cline{1-3} \end{array}\ .$$

Formally speaking, this is a map $T : Y(4,3,3,0,0,0,0,\ldots,0) \to [N]$ that sends the pairs $(1,1), (1,2), (1,3), (1,4), (2,1), \ldots$ to $1,7,2,4,3,\ldots$, respectively.

We will use some visually inspired language when talking about Young diagrams and tableaux:

- For instance, the *entry* of a tableau T in box (i,j) will mean the value $T(i,j)$.

- Also, the *u-th row* of a tableau T (for a given $u \geq 1$) will mean the sequence of all entries of T in the boxes (i,j) with $i = u$.

- Likewise, the *v-th column* of a tableau T (for a given $v \geq 1$) will mean the sequence of all entries of T in the boxes (i,j) with $j = v$.

- If T is a Young tableau of shape λ, then the boxes of $Y(\lambda)$ will also be called the boxes of T.

- Two boxes of a Young diagram (or of a tableau) are said to be *adjacent* if they have an edge in common when drawn on the picture (i.e., when one of them has the form (i,j), while the other has the form $(i,j+1)$ or $(i+1,j)$).

- The words "north", "west", "south" and "east" are to be understood according to the picture of a Young diagram: e.g., the box $(2,4)$ lies one step north and three steps west of the box $(3,7)$.

Some tableaux are better than others:

Definition 7.3.6. Let λ be an N-partition.

A Young tableau T of shape λ is said to be *semistandard* if its entries

- increase weakly along each row (from left to right);

- increase strictly down each column (from top to bottom).

Formally speaking, this means that a Young tableau $T : Y(\lambda) \to [N]$ is semistandard if and only if

- we have $T(i,j) \leq T(i,j+1)$ for any $(i,j) \in Y(\lambda)$ satisfying $(i,j+1) \in Y(\lambda)$;
- we have $T(i,j) < T(i+1,j)$ for any $(i,j) \in Y(\lambda)$ satisfying $(i+1,j) \in Y(\lambda)$.

We let $\operatorname{SSYT}(\lambda)$ denote the set of all semistandard Young tableaux of shape λ. (This depends on N as well, but N is fixed, so we omit it from our notation.) We will usually say "*semistandard tableau*" instead of "semistandard Young tableau".

Example 7.3.7. Consider the following 6 Young tableaux of shape $(4,2,1,0,0,0,\ldots,0)$:

$$\begin{ytableau} 1 & 3 & 3 & 4 \\ 2 & 3 & 5 \\ 4 \end{ytableau} \qquad \begin{ytableau} 2 & 1 & 3 & 4 \\ 3 & 4 & 5 \\ 6 \end{ytableau} \qquad \begin{ytableau} 1 & 1 & 2 & 3 \\ 2 & 4 & 5 \\ 6 \end{ytableau}$$
$$\begin{ytableau} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 \\ 8 \end{ytableau} \qquad \begin{ytableau} 1 & 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 \end{ytableau} \qquad \begin{ytableau} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 \\ 1 \end{ytableau} \tag{252}$$

Which of these 6 tableaux are semistandard? The first one is not semistandard, since the entries in its second column do not strictly increase down the column. The second one is not semistandard, since the entries in its first row do not weakly increase along the row. The third one is semistandard. The fourth one is semistandard, too. The fifth one is semistandard, too (actually it has a special property: each of its entries is the smallest possible value that an entry of a semistandard tableau could have in its box). The sixth one is not semistandard, again because of the columns.

Definition 7.3.8. Let λ be an N-partition. If T is any Young tableau of shape λ, then we define the corresponding monomial

$$x_T := \prod_{c \text{ is a box of } Y(\lambda)} x_{T(c)} = \prod_{(i,j) \in Y(\lambda)} x_{T(i,j)} = \prod_{k=1}^{N} x_k^{(\# \text{ of times } k \text{ appears in } T)}.$$

For example, the three Young tableaux in (252) have corresponding monomials

$$\begin{aligned}
&x_1x_3x_3x_4x_2x_3x_5x_4 = x_1x_2x_3^3x_4^2x_5,\\
&x_2x_1x_3x_4x_3x_4x_5x_6,\\
&x_1x_1x_2x_3x_2x_4x_5x_6.
\end{aligned}$$

Definition 7.3.9. Let λ be an N-partition. We define the *Schur polynomial* $s_\lambda \in \mathcal{P}$ by

$$s_\lambda := \sum_{T \in \operatorname{SSYT}(\lambda)} x_T.$$

Example 7.3.10. (a) Let $n \in \mathbb{N}$. Consider the N-partition $(n, 0, 0, \ldots, 0)$. The semistandard tableaux T of shape $(n, 0, 0, \ldots, 0)$ are simply the fillings of a single row with n elements of $[N]$ that weakly increase from left to right:

$$T = \begin{array}{|c|c|c|c|}\hline i_1 & i_2 & \cdots & i_n \\ \hline\end{array} \qquad \text{with } i_1 \leq i_2 \leq \cdots \leq i_n.$$

Thus,

$$s_{(n,0,0,\ldots,0)} = \sum_{i_1 \leq i_2 \leq \cdots \leq i_n} x_{i_1} x_{i_2} \cdots x_{i_n} = h_n.$$

(b) Let $n \in \{0, 1, \ldots, N\}$. Consider the N-partition $(1, 1, \ldots, 1, 0, 0, \ldots, 0)$ (with n ones and $N - n$ zeroes). The semistandard tableaux T of shape $(1, 1, \ldots, 1, 0, 0, \ldots, 0)$ are simply the fillings of a single column with n elements of $[N]$ that strictly increase from top to bottom:

$$T = \begin{array}{|c|}\hline i_1 \\ \hline i_2 \\ \hline \vdots \\ \hline i_n \\ \hline\end{array} \qquad \text{with } i_1 < i_2 < \cdots < i_n.$$

Hence,

$$s_{(1,1,\ldots,1,0,0,\ldots,0) \text{ (with } n \text{ ones and } N-n \text{ zeroes)}} = \sum_{i_1 < i_2 < \cdots < i_n} x_{i_1} x_{i_2} \cdots x_{i_n} = e_n.$$

(c) Assume that $N \geq 2$. Consider the N-partition $(2, 1, 0, 0, 0, \ldots, 0)$ (with all entries from the third on being 0). The semistandard tableaux T of shape $(2, 1, 0, 0, 0, \ldots, 0)$ all have the form

$$T = \begin{array}{|c|c|}\hline i & j \\ \hline k \\ \cline{1-1}\end{array} \qquad \text{with } i \leq j \text{ and } i < k.$$

Hence,

$$\begin{aligned}
s_{(2,1,0,0,0,\ldots,0)} &= \sum_{\substack{i\leq j;\\ i<k}} x_i x_j x_k = \underbrace{\sum_{\substack{i<k;\\ j=i}} x_i x_j x_k}_{=\sum_{i<k} x_i x_i x_k} + \underbrace{\sum_{i<j<k} x_i x_j x_k}_{=e_3} + \underbrace{\sum_{\substack{i<k;\\ j=k}} x_i x_j x_k}_{=\sum_{i<k} x_i x_k x_k} + \underbrace{\sum_{i<k<j} x_i x_j x_k}_{=e_3} \\
&\qquad \left(\begin{array}{c}\text{since each triple } (i,j,k) \text{ of elements of } [N] \\ \text{that satisfies } i \leq j \text{ and } i<k \text{ must satisfy} \\ \textbf{exactly one} \text{ of the four} \\ \text{conditions } (i<k \text{ and } j=i) \text{ and } i<j<k \\ \text{and } (i<k \text{ and } j=k) \text{ and } i<k<j, \\ \text{and conversely, each triple satisfying one} \\ \text{of the latter four conditions must} \\ \text{satisfy } i\leq j \text{ and } i<k \end{array}\right) \\
&= \sum_{i<k} x_i x_i x_k + e_3 + \sum_{i<k} x_i x_k x_k + e_3 = 2e_3 + \sum_{i<k} \underbrace{x_i x_i}_{=x_i^2} x_k + \sum_{i<k} x_i \underbrace{x_k x_k}_{=x_k^2} \\
&= 2e_3 + \underbrace{\sum_{i<k} x_i^2 x_k + \sum_{i<k} x_i x_k^2}_{=m_{(2,1,0,0,\ldots,0)}} = 2e_3 + \underbrace{m_{(2,1,0,0,\ldots,0)}}_{\substack{=e_2e_1-3e_3\\ \text{(check this!)}}} \\
&= 2e_3 + e_2e_1 - 3e_3 = e_2e_1 - e_3.
\end{aligned}$$

Theorem 7.3.11. Let λ be an N-partition.

(a) The polynomial s_λ is symmetric.

(b) We have

$$a_{\lambda+\rho} = a_\rho \cdot s_\lambda.$$

Here, the addition on $\mathbb{N}^N$ is defined entrywise: that is, if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_N)$ are two N-tuples in $\mathbb{N}^N$, then we set

$$\alpha + \beta := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_N + \beta_N).$$

This theorem (once it will be proved) will yield Conjecture 7.3.3 in the case when $\alpha_1 > \alpha_2 > \cdots > \alpha_N$. Indeed, if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{N}^N$ is an N-tuple satisfying $\alpha_1 > \alpha_2 > \cdots > \alpha_N$, then we can write α as $\alpha = \lambda + \rho$ for some N-partition λ (namely, for $\lambda = \alpha - \rho = (\alpha_1 - (N-1), \alpha_2 - (N-2), \ldots, \alpha_N - (N-N))$), and then Theorem 7.3.11 **(b)** will yield $a_\alpha = a_\rho \cdot s_\lambda$, so that $a_\alpha / a_\rho = s_\lambda$, which is a symmetric polynomial (by Theorem 7.3.11 **(a)**) and furthermore has positive coefficients (by its combinatorial definition). Once Conjecture 7.3.3 is proved in the case when $\alpha_1 > \alpha_2 > \cdots > \alpha_N$, the validity of its first claim in the general case easily follows (because the alternant a_α is 0 when two of $\alpha_1, \alpha_2, \ldots, \alpha_N$ are equal, and otherwise can be reduced to the case $\alpha_1 > \alpha_2 > \cdots > \alpha_N$ by swapping the columns around).

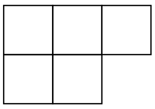
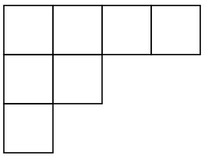
We will prove Theorem 7.3.11 **(a)** soon and Theorem 7.3.11 **(b)** later.

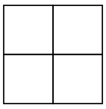
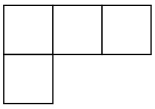
7.3.3. Skew Young diagrams and skew Schur polynomials

Before we get to the proof, let us generalize the situation a bit:

> **Definition 7.3.12.** Let λ and μ be two N-partitions.
>
> We say that $\mu \subseteq \lambda$ if and only if $Y(\mu) \subseteq Y(\lambda)$. Equivalently, $\mu \subseteq \lambda$ if and only if
> $$\text{each } i \in [N] \text{ satisfies } \mu_i \leq \lambda_i$$
> (where we write μ and λ as $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$ and $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$). Thus we have defined a partial order $\subseteq$ on the set of all N-partitions.

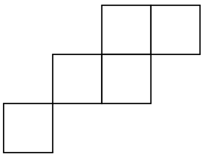
For example, we have $(3,2,0) \subseteq (4,2,1)$ (since $3 \leq 4$ and $2 \leq 2$ and $0 \leq 1$), but we don't have $(2,2,0) \subseteq (3,1,0)$ (since $2 > 1$). We can see this on the Young diagrams:

we have  $\subseteq$  ,

but we don't have  $\subseteq$  .

> **Definition 7.3.13.** Let λ and μ be two N-partitions such that $\mu \subseteq \lambda$. Then, we define the *skew Young diagram* $Y(\lambda/\mu)$ to be the set difference
> $$\begin{aligned} Y(\lambda) \setminus Y(\mu) &= \{(i,j) \ \mid \ i \in [N] \text{ and } j \in [\lambda_i] \setminus [\mu_i]\} \\ &= \{(i,j) \ \mid \ i \in [N] \text{ and } j \in \mathbb{Z} \text{ and } \mu_i < j \leq \lambda_i\}. \end{aligned}$$

For example,

$Y((4,3,1) \,/\, (2,1,0)) =$  .

We note that any row or column of a skew Young diagram $Y(\lambda/\mu)$ is contiguous, i.e., has no holes between boxes. Better yet, if (a,b) and (e,f) are two boxes of $Y(\lambda/\mu)$, then any box (c,d) that lies "between" them (i.e., that satisfies $a \leq c \leq e$ and $b \leq d \leq f$) must also belong to $Y(\lambda/\mu)$. Let us state this as a lemma:

Lemma 7.3.14 (Convexity of skew Young diagrams)**.** Let λ and μ be two N-partitions such that $\mu \subseteq \lambda$. Let (a, b) and (e, f) be two elements of $Y(\lambda/\mu)$. Let $(c, d) \in \mathbb{Z}^2$ satisfy $a \leq c \leq e$ and $b \leq d \leq f$. Then, $(c, d) \in Y(\lambda/\mu)$.

Hints to the proof of Lemma 7.3.14. This follows easily from the definition of $Y(\lambda/\mu)$ using the fact that λ and μ are weakly decreasing N-tuples. A detailed proof can be found in Section B.7. □

Lemma 7.3.14 is known as the *convexity* of $Y(\lambda/\mu)$ (albeit in a very specific sense of the word "convexity").

Next, we can define Young tableaux of shape λ/μ whenever λ and μ are two N-partitions satisfying $\mu \subseteq \lambda$. The definition is analogous to Definition 7.3.5, except that we are only filling the boxes of $Y(\lambda/\mu)$ (rather than all boxes of $Y(\lambda)$) this time:

Definition 7.3.15. Let λ and μ be two N-partitions such that $\mu \subseteq \lambda$. A *Young tableau* of shape λ/μ means a way of filling the boxes of $Y(\lambda/\mu)$ with elements of $[N]$ (one element per box). Formally speaking, it is defined as a map $T : Y(\lambda/\mu) \to [N]$. We visually represent such a map by filling in the number $T(i, j)$ into each box (i, j).

Young tableaux of shape λ/μ are often called *skew Young tableaux*.

If we don't have $\mu \subseteq \lambda$, then we agree that there are no Young tableaux of shape λ/μ.

The notion of a semistandard tableau of shape λ/μ is, again, defined in the same way as for shape λ:

Definition 7.3.16. Let λ and μ be two N-partitions.

A Young tableau T of shape λ/μ is said to be *semistandard* if its entries

- increase weakly along each row (from left to right);
- increase strictly down each column (from top to bottom).

Formally speaking, this means that a Young tableau $T : Y(\lambda/\mu) \to [N]$ is semistandard if and only if

- we have $T(i, j) \leq T(i, j+1)$ for any $(i, j) \in Y(\lambda/\mu)$ satisfying $(i, j+1) \in Y(\lambda/\mu)$;
- we have $T(i, j) < T(i+1, j)$ for any $(i, j) \in Y(\lambda/\mu)$ satisfying $(i+1, j) \in Y(\lambda/\mu)$.

We let $\operatorname{SSYT}(\lambda/\mu)$ denote the set of all semistandard Young tableaux of shape λ/μ. We will usually say "*semistandard tableau*" instead of "semistandard Young tableau".

For example, here is a semistandard Young tableau of shape $(4,3,1) / (2,1,0)$:

$$\begin{array}{cccc} & & \boxed{1} & \boxed{3} \\ & \boxed{2} & \boxed{2} & \\ \boxed{1} & & & \end{array} .$$

Meanwhile, there are no Young tableaux of shape $(3,2,1) / (2,2,2)$ (since we don't have $(2,2,2) \subseteq (3,2,1)$), and thus the set $\operatorname{SSYT}((3,2,1) / (2,2,2))$ is empty.

The phrases "increase weakly along each row" and "increase strictly down each column" in Definition 7.3.13 have been formalized in terms of adjacent entries: e.g., we have declared "increase weakly along each row" to mean "$T(i,j) \leq T(i,j+1)$" rather than "$T(i,j_1) \leq T(i,j_2)$ whenever $j_1 \leq j_2$". However, since any row or column of $Y(\lambda / \mu)$ is contiguous, the latter stronger meaning actually follows from the former. To wit:

Lemma 7.3.17. Let λ and μ be two N-partitions. Let T be a semistandard Young tableau of shape λ / μ. Then:

(a) If (i,j_1) and (i,j_2) are two elements of $Y(\lambda / \mu)$ satisfying $j_1 \leq j_2$, then $T(i,j_1) \leq T(i,j_2)$.

(b) If (i_1,j) and (i_2,j) are two elements of $Y(\lambda / \mu)$ satisfying $i_1 \leq i_2$, then $T(i_1,j) \leq T(i_2,j)$.

(c) If (i_1,j) and (i_2,j) are two elements of $Y(\lambda / \mu)$ satisfying $i_1 < i_2$, then $T(i_1,j) < T(i_2,j)$.

(d) If (i_1,j_1) and (i_2,j_2) are two elements of $Y(\lambda / \mu)$ satisfying $i_1 \leq i_2$ and $j_1 \leq j_2$, then $T(i_1,j_1) \leq T(i_2,j_2)$.

(e) If (i_1,j_1) and (i_2,j_2) are two elements of $Y(\lambda / \mu)$ satisfying $i_1 < i_2$ and $j_1 \leq j_2$, then $T(i_1,j_1) < T(i_2,j_2)$.

Hints to the proof of Lemma 7.3.17. This is easy using Lemma 7.3.14. A detailed proof can be found in Section B.7. □

We extend Definition 7.3.8 to skew tableaux:

Definition 7.3.18. Let λ and μ be two N-partitions. If T is any Young tableau of shape λ / μ, then we define the corresponding monomial

$$x_T := \prod_{c \text{ is a box of } Y(\lambda/\mu)} x_{T(c)} = \prod_{(i,j) \in Y(\lambda/\mu)} x_{T(i,j)} = \prod_{k=1}^{N} x_k^{(\#\text{ of times } k \text{ appears in } T)}.$$

For example,

$$\text{if } T = \begin{array}{cccc} & & \boxed{1} & \boxed{3} \\ & \boxed{2} & \boxed{2} & \\ \boxed{3} & \boxed{4} & \boxed{4} & \end{array}, \text{ then } x_T = x_1 x_3 x_2 x_2 x_3 x_4 x_4 = x_1 x_2^2 x_3^2 x_4^2.$$

Finally, we generalize Definition 7.3.9 to λ / μ:

Definition 7.3.19. Let λ and μ be two N-partitions. We define the *skew Schur polynomial* $s_{\lambda/\mu} \in \mathcal{P}$ by

$$s_{\lambda/\mu} := \sum_{T \in \operatorname{SSYT}(\lambda/\mu)} x_T.$$

Example 7.3.20. **(a)** We have

$$s_{(3,3,2,0,0,0,\ldots,0)/(2,1,0,0,0,\ldots,0)} = \sum_{i<j\geq k<\ell\geq m} x_i x_j x_k x_\ell x_m,$$

since the semistandard tableaux of shape $(3,3,2,0,0,0,\ldots,0) / (2,1,0,0,0,\ldots,0)$ have the form

$$\begin{array}{ccc} & & \boxed{i} \\ & \boxed{k} & \boxed{j} \\ \boxed{m} & \boxed{\ell} & \end{array}$$

for $i,j,k,\ell,m \in [N]$ satisfying $i < j \geq k < \ell \geq m$.

(b) We have

$$s_{(3,2,1,0,0,0,\ldots,0)/(2,1,0,0,0,\ldots,0)} = \sum_{i,j,k} x_i x_j x_k,$$

since the semistandard tableaux of shape $(3,2,1,0,0,0,\ldots,0) / (2,1,0,0,0,\ldots,0)$ have the form

$$\begin{array}{ccc} & & \boxed{i} \\ & \boxed{j} & \\ \boxed{k} & & \end{array}$$

for $i,j,k \in [N]$ satisfying no special requirements (as there are never two entries in the same row or in the same column of the tableau). Thus,

$$s_{(3,2,1,0,0,0,\ldots,0)/(2,1,0,0,0,\ldots,0)} = \sum_{i,j,k} x_i x_j x_k = \left(\sum_i x_i\right)^3 = (x_1 + x_2 + \cdots + x_N)^3.$$

Theorem 7.3.21. Let λ and μ be any two N-partitions. Then, the polynomial $s_{\lambda/\mu}$ is symmetric.

Remark 7.3.22. If we set $\mathbf{0} = (0, 0, \ldots, 0) \in \mathbb{N}^N$, then $s_{\lambda/\mathbf{0}} = s_\lambda$ (since the semistandard tableaux of shape $\lambda/\mathbf{0}$ are precisely the semistandard tableaux of shape λ). Hence, Theorem 7.3.21 generalizes Theorem 7.3.11 **(a)**.

We will now prove Theorem 7.3.21 bijectively, using a beautiful set of combinatorial bijections known as the *Bender–Knuth involutions*.

7.3.4. The Bender–Knuth involutions

Proof of Theorem 7.3.21. For each $i \in [N-1]$, we consider the simple transposition $s_i \in S_N$ defined in Definition 5.2.3 (applied to $n = N$). As we recall, this is the transposition that swaps i with $i+1$. (The notation s_i for this transposition is unfortunately similar to the notation s_λ for Schur polynomials; however, this should not cause any confusion, since the only Schur polynomial that will appear in this proof is $s_{\lambda/\mu}$, which cannot be mistaken for a transposition.)

We must show that the polynomial $s_{\lambda/\mu}$ is symmetric. According to Lemma 7.1.17, it will suffice to show that $s_k \cdot s_{\lambda/\mu} = s_{\lambda/\mu}$ for each $k \in [N-1]$.

So let us fix some $k \in [N-1]$. In order to prove $s_k \cdot s_{\lambda/\mu} = s_{\lambda/\mu}$, we will construct a bijection

$$\beta_k : \operatorname{SSYT}(\lambda/\mu) \to \operatorname{SSYT}(\lambda/\mu)$$

(called the k-th *Bender–Knuth involution*) that

- interchanges the # of k's with the # of $(k+1)$'s in a tableau (that is, if a tableau T has a many k's and b many $(k+1)$'s, then $\beta_k(T)$ will have b many k's and a many $(k+1)$'s);
- leaves all the other entries of the tableau unchanged.

Indeed, once such a bijection β_k is constructed, we can easily see that

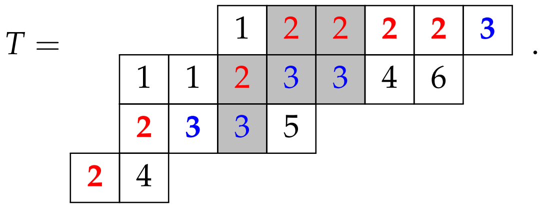
$$x_{\beta_k(T)} = s_k \cdot x_T \qquad \text{for each } T \in \operatorname{SSYT}(\lambda/\mu),$$

so that applying s_k to $s_{\lambda/\mu} = \sum\limits_{T \in \operatorname{SSYT}(\lambda/\mu)} x_T$ will amount to permuting the addends in the sum.[123]

We construct the map β_k as follows: Let $T \in \operatorname{SSYT}(\lambda/\mu)$. We focus on the k's and the $(k+1)$'s in T (that is, on the entries of T that are equal to k or to $k+1$). An entry k in T will be called *matched* if there is a $k+1$ directly underneath it (in the same column). An entry $k+1$ in T will be called *matched* if there is a k directly above it (in the same column). All other k's and $(k+1)$'s in T will be called *free*. Let us see an example of this first:

[123] We will explain this argument in more detail at the end of this proof.

Example 7.3.23. For this example, let $k = 2$. Here is a semistandard tableau $T \in \operatorname{SSYT}\left((9,8,5,2,0,0) \ / \ (3,1,1,0,0,0)\right)$ with the free entries printed in boldface and the matched entries printed on a grey background:



$$T = \begin{array}{ccccccccc} & & & 1 & \colorbox{lightgray}{2} & \colorbox{lightgray}{2} & \mathbf{2} & \mathbf{2} & \mathbf{3} \\ & 1 & 1 & \colorbox{lightgray}{2} & \colorbox{lightgray}{3} & \colorbox{lightgray}{3} & 4 & 6 & \\ & \mathbf{2} & \mathbf{3} & \colorbox{lightgray}{3} & 5 & & & & \\ \mathbf{2} & 4 & & & & & & & \end{array} .$$

(We have color-coded the entries so that 2's are red, 3's are blue, and all other entries are black. You can mostly forget about the black entries, since our construction of $\beta_k(T)$ will neither change them nor depend on them.)

We note that the entries of T increase weakly along each row (since T is semistandard), and increase strictly down each column (for the same reason). Now, an entry k in T is matched if and only if there is a $k+1$ anywhere in its column (because if there is a $k+1$ anywhere in its column, then this $k+1$ must be directly underneath the k [124], and therefore the k is matched). Likewise, an entry $k+1$ in T is matched if and only if there is a k anywhere in its column. Thus, matched entries come in pairs: If a k in T is matched, then the $k+1$ directly underneath it is also matched, and conversely, if a $k+1$ in T is matched, then the k directly above it is also matched. Hence, there is an obvious bijection between the sets $\{\text{matched } k\text{'s in } T\}$ and $\{\text{matched } (k+1)\text{'s in } T\}$ [125]. Thus, by the bijection principle, we have

$$\begin{aligned} &(\text{\# of matched } k\text{'s in } T) \\ &= (\text{\# of matched } (k+1)\text{'s in } T) . \end{aligned} \tag{253}$$

Each column of T that contains a matched entry must contain exactly two matched entries (one k and one $k+1$); we shall refer to these two entries as each other's "*partners*".

Our goal is to modify some of the entries k and $k+1$ in such a way that we obtain a new semistandard tableau that has as many k's as our original tableau T had $(k+1)$'s, and has as many $(k+1)$'s as our original tableau T had k's. We do not want to change any entries other than k's and $(k+1)$'s; nor do we want to replace any k's or $(k+1)$'s by entries other than k and $k+1$.

These requirements force us to leave all matched entries (both k's and $(k+1)$'s) unchanged. Indeed, if an entry is matched, then its column contains both a k and a $k+1$, and thus neither of these two entries can be changed without breaking the "entries increase strictly down each column" condition in Definition 7.3.16. Thus, the matched entries will have to stay unchanged.

[124] since the entries of each column of T increase down this column

[125] Strictly speaking, these sets should consist not of the entries, but rather of the boxes in which they are located.

On the other hand, we can arbitrarily replace the free entries by k's or $(k+1)$'s, as long as we make sure to keep the rows weakly increasing; the columns will stay strictly increasing no matter what we do (because a column containing a free k does not contain any $k+1$, and a column containing a free $k+1$ does not contain any k), so our tableau will remain semistandard.

In view of these observations, let us perform the following procedure:

- For each row of T, if there are a free k's and b free $(k+1)$'s in this row, we replace them by b free k's and a free $(k+1)$'s (placed in this order, from left to right).

We define $\beta_k(T)$ to be the result of this procedure.

Example 7.3.24. If k and T are as in Example 7.3.23, then

$$\beta_k(T) = \begin{array}{ccccccccc} & & & 1 & {\color{red}2} & {\color{red}2} & {\color{red}\mathbf{2}} & {\color{blue}\mathbf{3}} & {\color{blue}\mathbf{3}} \\ & 1 & 1 & {\color{red}2} & {\color{blue}3} & {\color{blue}3} & 4 & 6 & \\ & {\color{red}\mathbf{2}} & {\color{blue}\mathbf{3}} & {\color{blue}3} & 5 & & & & \\ {\color{blue}\mathbf{3}} & 4 & & & & & & & \end{array} .$$

Indeed:

- The 1-st row of T had 2 free 2's and 1 free 3, so we replaced them by 1 free 2 and 2 free 3's.

- The 2-nd row had 0 free 2's and 0 free 3's, so we replaced them by 0 free 2's and 0 free 3's. (Of course, this did not change anything.)

- The 3-rd row had 1 free 2 and 1 free 3, so we replaced them by 1 free 2 and 1 free 3. (Of course, this did not change anything.)

- The 4-th row had 1 free 2 and 0 free 3's, so we replaced them by 0 free 2's and 1 free 3.

Thus, $\beta_k(T)$ is obtained from T by "flipping the imbalance between free k's and free $(k+1)$'s" in each row of T (so that a row that was heavy on free k's becomes equally heavy on free $(k+1)$'s, and vice versa). Rows that have equally many free k's and free $(k+1)$'s stay unchanged.

In order to make sure that β_k is a well-defined map from $\operatorname{SSYT}(\lambda/\mu)$ to $\operatorname{SSYT}(\lambda/\mu)$, we need to show that the tableau $\beta_k(T)$ is semistandard. As we have already explained, the columns are not at issue (we have only changed free entries, so the columns remain strictly increasing), but we need to convince ourselves that the rows are still weakly increasing. It is clear that the **free** entries in each row are in the right order (i.e., any free k stands further left than any free $k+1$), and it is also clear that the **matched** entries in each row are in the right order (since they are unchanged from T); however, it is imaginable that the order between free and matched entries has gotten messed up (e.g., a larger free entry stands further left than a smaller matched entry in $\beta_k(T)$). We need to prove that this does not happen.

To prove this, we make the following observation:

> *Observation 1:* Each row of T can be subdivided into the following six blocks:

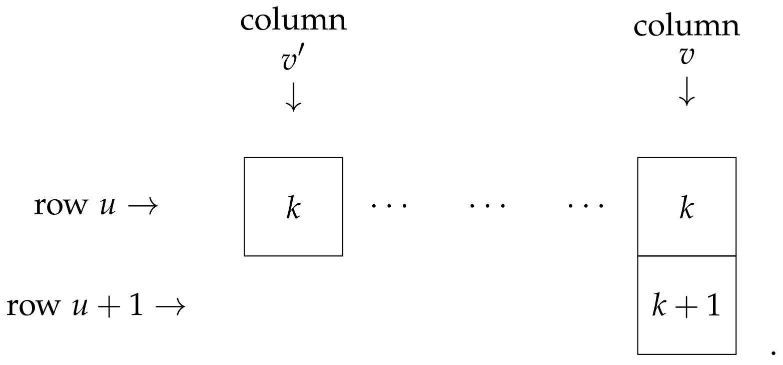
entries $< k$	matched k's	free k's	free $(k+1)$'s	matched $(k+1)$'s	entries $> k+1$

,

> which appear in this order from left to right. (Each of these blocks can be empty.)

[*Proof of Observation 1:* Consider some row of T. The entries in this row increase weakly from left to right (since T is semistandard), so it is clear that all entries $< k$ stand further left than all k's, which in turn stand further left than all $(k+1)$'s, which in turn stand further left than all entries $> k+1$. It therefore remains to show that all matched k's stand further left than all free k's, and that all free $(k+1)$'s stand further left than all matched $(k+1)$'s. We will prove the first of these two statements only (since the proof of the second is largely analogous).

So we need to show that all matched k's in our row stand further left than all free k's. Assume the contrary. Thus, there is some matched k that stands further right than some free k. Let the former matched k stand in box (u,v), and let the latter free k stand in box (u,v'); thus, $v > v'$ (since the matched k stands further right than the free k) and $T(u,v') = k$ (since there is a k in box (u,v')). Since the k in box (u,v) is matched, there is a $k+1$ directly underneath it; in other words, the box $(u+1,v)$ belongs to $Y(\lambda/\mu)$ and we have $T(u+1,v) = k+1$. Here is an illustration of this situation:



.

Now, the Young diagram of λ/μ contains the box (u,v'), but also contains the box $(u+1,v)$, which lies one row south and some number of columns east of the former box (since $v > v'$). Hence, the Young diagram of λ/μ must have a box $(u+1, v')$ directly underneath the box (u, v') (that is, the box $(u+1, v')$ must belong to $Y(\lambda/\mu)$ [126]). Here is an illustration of this:

$$\begin{array}{rccccc} & \text{column} & & & & \text{column} \\ & v' & & & & v \\ & \downarrow & & & & \downarrow \\ \text{row } u \rightarrow & \boxed{k} & \cdots & \cdots & \cdots & \boxed{k} \\ \text{row } u+1 \rightarrow & \boxed{?} & \cdots & \cdots & \cdots & \boxed{k+1} \end{array}.$$

Thus, we know that there is a box $(u+1, v')$ in the Young diagram of λ/μ. The entry of the tableau T in this box $(u+1, v')$ must satisfy $T(u+1, v') > T(u, v')$ (because the entries of T increase strictly down each column) and $T(u+1, v') \leq T(u+1, v)$ (because the entries of T increase weakly along each row, and because $v > v'$ shows that the entry $T(u+1, v')$ lies further left than $T(u+1, v)$ [127]). These two inequalities rewrite as $T(u+1, v') > k$ and $T(u+1, v') \leq k+1$ (since $T(u, v') = k$ and $T(u+1, v) = k+1$). Thus, the number $T(u+1, v')$ lies in the half-open interval $(k, k+1]$. Since $T(u+1, v')$ is an integer, we must thus have $T(u+1, v') = k+1$. In other words, the entry k in box (u, v') of our tableau T has a $k+1$ directly underneath it. Therefore, this entry k is matched. This contradicts our assumption that this k is free. This contradiction shows that our assumption was false. Thus, we have shown that all matched k's in our row stand further left than all free k's. Similarly, we can show that all free $(k+1)$'s stand further left than all matched $(k+1)$'s (the argument is analogous, but it uses the $(u-1)$-st row of T rather than the $(u+1)$-st one). As explained above, this completes the proof of Observation 1.]

Observation 1 entails that the free entries in each row of T are stuck together between the rightmost matched k and the leftmost matched $k+1$. Hence, replacing these free entries as in our above definition of $\beta_k(T)$ does not mess up the weakly increasing order of the entries in this row. This completes our proof that $\beta_k(T)$ is a semistandard tableau.

Hence, the map $\beta_k : \operatorname{SSYT}(\lambda/\mu) \to \operatorname{SSYT}(\lambda/\mu)$ is well-defined. This map β_k is called the k-th *Bender–Knuth involution*.

We shall now show that this map β_k is a bijection. Better yet, we will show that it is an involution (i.e., that $\beta_k \circ \beta_k = \operatorname{id}$):

[126] Here is a rigorous *proof:* We know that (u, v') and $(u+1, v)$ are two elements of $Y(\lambda/\mu)$. Moreover, $(u+1, v') \in \mathbb{Z}^2$ satisfies $u \leq u+1 \leq u+1$ and $v' \leq v' \leq v$ (since $v > v'$). Thus, Lemma 7.3.14 (applied to (u, v'), $(u+1, v)$ and $(u+1, v')$ instead of (a, b), (e, f) and (c, d)) yields $(u+1, v') \in Y(\lambda/\mu)$. Qed.

[127] Strictly speaking, we are using Lemma 7.3.17 **(a)** here (applying it to $(u+1, v')$ and $(u+1, v)$ instead of (i, j_1) and (i, j_2)).

Observation 2: We have $\beta_k \circ \beta_k = \operatorname{id}$.

[*Proof of Observation 2:* We need to check that $\beta_k(\beta_k(T)) = T$ for each $T \in \operatorname{SSYT}(\lambda/\mu)$. So let $T \in \operatorname{SSYT}(\lambda/\mu)$ be arbitrary. Recall our above definition of free and matched k's and $(k+1)$'s in T. The construction of $\beta_k(T)$ replaced some free entries while leaving the matched ones unchanged.

Now, we claim that the matched entries of $\beta_k(T)$ stand in the exact same boxes as the matched entries of T, whereas the free entries of $\beta_k(T)$ stand in the exact same boxes as the free entries of T. Indeed, the matched entries of T remain matched in $\beta_k(T)$ (since neither these entries themselves, nor their "partners" have changed in the construction of $\beta_k(T)$), whereas the free entries of T remain free in $\beta_k(T)$ (since the construction of $\beta_k(T)$ cannot have produced any "partners" for them[128]).

This has the consequence that if we apply our definition of β_k to the semistandard tableau $\beta_k(T)$ (to construct $\beta_k(\beta_k(T))$), then we end up undoing the very changes that transformed T into $\beta_k(T)$ (indeed, in each row, the original imbalance between free k's and free $(k+1)$'s that was flipped in the construction of $\beta_k(T)$ gets flipped again, and thus gets restored to its original state[129]). Hence, $\beta_k(\beta_k(T)) = T$.

Forget that we fixed T. We thus have shown that $\beta_k(\beta_k(T)) = T$ for each $T \in \operatorname{SSYT}(\lambda/\mu)$. In other words, $\beta_k \circ \beta_k = \operatorname{id}$. This proves Observation 2.]

Observation 2 shows that β_k is an involution. Hence, β_k is a bijection.

The map β_k leaves all entries of the tableau other than k's and $(k+1)$'s unchanged (because of how we defined β_k). Let us now show that β_k interchanges the # of k's with the # of $(k+1)$'s in a tableau (that is, if a tableau T has a many k's and b many $(k+1)$'s, then $\beta_k(T)$ will have b many k's and a many $(k+1)$'s). More precisely, we shall show the following:

Observation 3: Let $T \in \operatorname{SSYT}(\lambda/\mu)$. Then,

$$(\text{\# of } k\text{'s in } \beta_k(T)) = (\text{\# of } (k+1)\text{'s in } T) \tag{254}$$

and

$$(\text{\# of } (k+1)\text{'s in } \beta_k(T)) = (\text{\# of } k\text{'s in } T). \tag{255}$$

Moreover, if $i \in [N]$ satisfies $i \neq k$ and $i \neq k+1$, then

$$(\text{\# of } i\text{'s in } \beta_k(T)) = (\text{\# of } i\text{'s in } T). \tag{256}$$

[128] Why not? Let's take, for example, a free k. This free k is the only k in its column (since the entries of T increase strictly down each column), and there is no $k+1$ in its column (since otherwise, the k would be matched, not free). Thus, there is no entry in its column that could become a "partner" for it in $\beta_k(T)$. An analogous argument applies to a free $k+1$.

[129] In more detail: If some row of T had a free k's and b free $(k+1)$'s, then the same row of $\beta_k(T)$ has b free k's and a free $(k+1)$'s, and therefore the same row of $\beta_k(\beta_k(T))$ will, in turn, have a free k's and b free $(k+1)$'s again; but this means that its free entries are the same as in T.

[*Proof of Observation 3:* We recall a simple fact we noticed during our proof of Observation 2 above: The matched entries of $\beta_k(T)$ stand in the exact same boxes as the matched entries of T, whereas the free entries of $\beta_k(T)$ stand in the exact same boxes as the free entries of T. Thus, the matched entries of T remain matched in $\beta_k(T)$, whereas the free entries of T remain free in $\beta_k(T)$ (even if some of them change their values).

Since the matched entries of T remain unchanged under the map β_k, we therefore have

$$\begin{aligned}&(\text{\# of matched } k\text{'s in } \beta_k(T))\\&=(\text{\# of matched } k\text{'s in } T)\end{aligned}\tag{257}$$

and

$$\begin{aligned}&(\text{\# of matched } (k+1)\text{'s in } \beta_k(T))\\&=(\text{\# of matched } (k+1)\text{'s in } T).\end{aligned}\tag{258}$$

On the other hand, the map β_k flips the imbalance between free k's and free $(k+1)$'s in each row (but all these free entries remain free, whereas the matched entries of T remain matched in $\beta_k(T)$); therefore, it also flips the total imbalance between free k's and free $(k+1)$'s in the entire tableau[130]. Thus,

$$\begin{aligned}&(\text{\# of free } k\text{'s in } \beta_k(T))\\&=(\text{\# of free } (k+1)\text{'s in } T)\end{aligned}\tag{259}$$

and

$$\begin{aligned}&(\text{\# of free } (k+1)\text{'s in } \beta_k(T))\\&=(\text{\# of free } k\text{'s in } T).\end{aligned}\tag{260}$$

Now, each k in $\beta_k(T)$ is either free or matched (but not both at the same time). Hence,

$$\begin{aligned}&(\text{\# of } k\text{'s in } \beta_k(T))\\&=\underbrace{(\text{\# of free } k\text{'s in } \beta_k(T))}_{\substack{=(\text{\# of free } (k+1)\text{'s in } T)\\ (\text{by (259)})}}+\underbrace{(\text{\# of matched } k\text{'s in } \beta_k(T))}_{\substack{=(\text{\# of matched } k\text{'s in } T)\\ (\text{by (257)})}}\\&=(\text{\# of free } (k+1)\text{'s in } T)+\underbrace{(\text{\# of matched } k\text{'s in } T)}_{\substack{=(\text{\# of matched } (k+1)\text{'s in } T)\\ (\text{by (253)})}}\\&=(\text{\# of free } (k+1)\text{'s in } T)+(\text{\# of matched } (k+1)\text{'s in } T)\\&=(\text{\# of } (k+1)\text{'s in } T)\end{aligned}$$

[130] since the total # of free k's in a tableau equals the sum of the #s of free k's in all rows (and the same holds for free $(k+1)$'s)

(since each $k+1$ in T is either free or matched, but not both at the same time).

Also, each $k+1$ in $\beta_k(T)$ is either free or matched (but not both at the same time). Hence,

$$\begin{aligned}
&(\text{\# of } (k+1)\text{'s in } \beta_k(T)) \\
&= \underbrace{(\text{\# of free } (k+1)\text{'s in } \beta_k(T))}_{\substack{=(\text{\# of free } k\text{'s in } T) \\ (\text{by (260)})}} + \underbrace{(\text{\# of matched } (k+1)\text{'s in } \beta_k(T))}_{\substack{=(\text{\# of matched } (k+1)\text{'s in } T) \\ (\text{by (258)})}} \\
&= (\text{\# of free } k\text{'s in } T) + \underbrace{(\text{\# of matched } (k+1)\text{'s in } T)}_{\substack{=(\text{\# of matched } k\text{'s in } T) \\ (\text{by (253)})}} \\
&= (\text{\# of free } k\text{'s in } T) + (\text{\# of matched } k\text{'s in } T) \\
&= (\text{\# of } k\text{'s in } T)
\end{aligned}$$

(since each k in T is either free or matched, but not both at the same time).

Moreover, if $i \in [N]$ satisfies $i \neq k$ and $i \neq k+1$, then

$$(\text{\# of } i\text{'s in } \beta_k(T)) = (\text{\# of } i\text{'s in } T)$$

(since the map β_k leaves all i's in T unchanged[131], and does not replace any other entries by i's). Thus, Observation 3 is proved.]

From Observation 3, we can easily conclude the following:

Observation 4: We have $x_{\beta_k(T)} = s_k \cdot x_T$ for each $T \in \operatorname{SSYT}(\lambda/\mu)$.

[*Proof of Observation 4:* For the sake of completeness, here is a detailed proof. Let $T \in \operatorname{SSYT}(\lambda/\mu)$. Then,

$$\begin{aligned}
x_T &= \prod_{i=1}^{N} x_i^{(\text{\# of times } i \text{ appears in } T)} \qquad (\text{by Definition 7.3.18}) \\
&= \prod_{i=1}^{N} x_i^{(\text{\# of } i\text{'s in } T)} \\
&\qquad\qquad (\text{since } (\text{\# of times } i \text{ appears in } T) = (\text{\# of } i\text{'s in } T) \text{ for each } i \in [N]) \\
&= x_k^{(\text{\# of } k\text{'s in } T)} \cdot x_{k+1}^{(\text{\# of } (k+1)\text{'s in } T)} \cdot \prod_{\substack{i \in [N]; \\ i \neq k \text{ and } i \neq k+1}} x_i^{(\text{\# of } i\text{'s in } T)} \qquad (261)
\end{aligned}$$

(here, we have split off the factors for $i = k$ and for $i = k+1$ from the product). The

[131] because $i \neq k$ and $i \neq k+1$

same argument (applied to $\beta_k(T)$ instead of T) yields

$$\begin{aligned}
x_{\beta_k(T)} &= \underbrace{x_k^{(\text{\# of } k\text{'s in } \beta_k(T))}}_{\substack{=x_k^{(\text{\# of } (k+1)\text{'s in } T)} \\ \text{(by (254))}}} \cdot \underbrace{x_{k+1}^{(\text{\# of } (k+1)\text{'s in } \beta_k(T))}}_{\substack{=x_{k+1}^{(\text{\# of } k\text{'s in } T)} \\ \text{(by (255))}}} \cdot \prod_{\substack{i\in[N];\\ i\neq k \text{ and } i\neq k+1}} \underbrace{x_i^{(\text{\# of } i\text{'s in } \beta_k(T))}}_{\substack{=x_i^{(\text{\# of } i\text{'s in } T)} \\ \text{(by (256))}}} \\
&= x_k^{(\text{\# of } (k+1)\text{'s in } T)} \cdot x_{k+1}^{(\text{\# of } k\text{'s in } T)} \cdot \prod_{\substack{i\in[N];\\ i\neq k \text{ and } i\neq k+1}} x_i^{(\text{\# of } i\text{'s in } T)} \\
&= x_{k+1}^{(\text{\# of } k\text{'s in } T)} \cdot x_k^{(\text{\# of } (k+1)\text{'s in } T)} \cdot \prod_{\substack{i\in[N];\\ i\neq k \text{ and } i\neq k+1}} x_i^{(\text{\# of } i\text{'s in } T)}.
\end{aligned}$$

On the other hand, applying the transposition s_k (or, more precisely, the action of this transposition $s_k \in S_N$ on the ring $\mathcal{P}$) to both sides of the equality (261), we obtain

$$\begin{aligned}
s_k \cdot x_T &= s_k \cdot \left(x_k^{(\text{\# of } k\text{'s in } T)} \cdot x_{k+1}^{(\text{\# of } (k+1)\text{'s in } T)} \cdot \prod_{\substack{i\in[N];\\ i\neq k \text{ and } i\neq k+1}} x_i^{(\text{\# of } i\text{'s in } T)} \right) \\
&= x_{k+1}^{(\text{\# of } k\text{'s in } T)} \cdot x_k^{(\text{\# of } (k+1)\text{'s in } T)} \cdot \prod_{\substack{i\in[N];\\ i\neq k \text{ and } i\neq k+1}} x_i^{(\text{\# of } i\text{'s in } T)}
\end{aligned}$$

(since the action of s_k on $\mathcal{P}$ swaps the indeterminates x_k and x_{k+1} while leaving all other indeterminates x_i unchanged). Comparing the last two equalities, we obtain $x_{\beta_k(T)} = s_k \cdot x_T$. This proves Observation 4.]

Now, the definition of $s_{\lambda/\mu}$ yields

$$s_{\lambda/\mu} = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)} x_T. \tag{262}$$

Applying the permutation $s_k \in S_N$ (or, rather, the action of this permutation on the ring $\mathcal{P}$) to both sides of this equality, we obtain

$$\begin{aligned}
s_k \cdot s_{\lambda/\mu} &= s_k \cdot \sum_{T\in\operatorname{SSYT}(\lambda/\mu)} x_T = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)} \underbrace{s_k \cdot x_T}_{\substack{=x_{\beta_k(T)} \\ \text{(by Observation 4)}}} \\
&\qquad \left(\begin{array}{c}\text{since the group } \mathcal{S}_N \text{ acts on the ring } \mathcal{P} \\ \text{by } K\text{-algebra automorphisms, and thus} \\ \text{the action of } s_k \text{ on } \mathcal{P} \text{ is } K\text{-linear}\end{array}\right) \\
&= \sum_{T\in\operatorname{SSYT}(\lambda/\mu)} x_{\beta_k(T)} = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)} x_T \\
&\qquad \left(\begin{array}{c}\text{here, we have substituted } T \text{ for } \beta_k(T) \text{ in the sum,} \\ \text{since the map } \beta_k : \operatorname{SSYT}(\lambda/\mu) \to \operatorname{SSYT}(\lambda/\mu) \\ \text{is a bijection}\end{array}\right) \\
&= s_{\lambda/\mu} \qquad \text{(by (262))}.
\end{aligned}$$

Now, forget that we fixed k. We thus have shown that

$$s_k \cdot s_{\lambda/\mu} = s_{\lambda/\mu} \qquad \text{for each } k \in [N-1] . \tag{263}$$

Hence, Lemma 7.1.17 (applied to $f = s_{\lambda/\mu}$) shows that the polynomial $s_{\lambda/\mu}$ is symmetric. This proves Theorem 7.3.21. □

As we already mentioned, Theorem 7.3.11 **(a)** is a particular case of Theorem 7.3.21 (namely, the one obtained when we set $\mu = \mathbf{0} = (0, 0, \ldots, 0)$), because $s_{\lambda/\mathbf{0}} = s_\lambda$.

7.3.5. The Littlewood–Richardson rule

The Bender–Knuth involutions have served us well in the above proof of Theorem 7.3.21, but they have much more to offer. We will soon see them prove one of the most famous results in the theory of symmetric polynomials, namely the Littlewood–Richardson rule. In the process, we will also (finally) prove Theorem 7.3.11 **(b)**.

The Littlewood–Richardson rule has its roots in the representation theory of the classical groups (specifically, $\mathrm{GL}_N(\mathbb{C})$). We shall say a few words about this motivation before we move on to stating the rule itself (which is purely combinatorial, as is its proof). At the simplest level, the Littlewood–Richardson rule is about expanding the product $s_\nu s_\lambda$ of two Schur polynomials as a sum of other Schur polynomials. For instance, for $N = 4$, we have

$$s_{2100} s_{1100} = s_{2111} + s_{2210} + s_{3110} + s_{3200},$$

where we are omitting commas and parentheses for brevity (i.e., we are writing 2100 for the N-partition $(2, 1, 0, 0)$, and likewise for the other N-partitions). Likewise, for $N = 3$, we have

$$s_{210} s_{210} = s_{222} + 2 s_{321} + s_{330} + s_{411} + s_{420}.$$

I think it was Hermann Weyl who originally proved the existence of such an expansion (i.e., that any product $s_\nu s_\lambda$ of two Schur polynomials is a sum of Schur polynomials). The original proof used Lie group representations. The idea of the proof, in a nutshell, is the following (skip this paragraph if you are unfamiliar with representation theory): The irreducible polynomial representations of the classical group $\mathrm{GL}_N(\mathbb{C})$ are (more or less) in bijection with the N-partitions, meaning that there is an irreducible polynomial representation V_λ for each N-partition λ, and all irreps (= irreducible polynomial representations) of $\mathrm{GL}_N(\mathbb{C})$ have this form[132]. These V_λ's are known as the *Weyl modules*, or in a slightly more general form as the *Schur functors*. The tensor product of

[132] At least if one uses the "right" definition of a polynomial representation. See [KraPro10, §5 and §6] or [Prasad15, §6.1] for details.

two such irreps can be decomposed as a direct sum of irreps (since polynomial representations of $\operatorname{GL}_N(\mathbb{C})$ are completely reducible):

$$V_\nu \otimes V_\lambda \cong \bigoplus_{\omega \text{ is an } N\text{-partition}} \underbrace{V_\omega^{c(\nu,\lambda,\omega)}}_{\substack{\text{a direct sum of } c(\nu,\lambda,\omega) \\ \text{many } V_\omega\text{'s}}}.$$

The multiplicities $c(\nu,\lambda,\omega)$ in this decomposition are precisely the coefficients that you get when you decompose the product of the Schur polynomial s_ν and s_λ as a sum of Schur polynomials:

$$s_\nu s_\lambda = \sum_{\omega \text{ is an } N\text{-partition}} c(\nu,\lambda,\omega)\, s_\omega.$$

In fact, the Schur polynomials s_λ are the so-called *characters* of the irreps V_λ, and it is known that tensor products of representations correspond to products of their characters.

All of this, in the detail it deserves, is commonly taught in a 1st or 2nd course on representation theory (e.g., [Proces07] or [EGHetc11] or [Prasad15, Chapter 6]). But we are here for something else: we want to know these $c(\nu,\lambda,\omega)$'s. In other words, we want a formula that expands a product $s_\nu s_\lambda$ as a finite sum of Schur polynomials.

Such a formula was first conjectured by Dudley Ernest Littlewood and Archibald Read Richardson in 1934. It remained unproven for 40 years, not least because the statement was not very clear. In the 1970s, proofs were found independently by Marcel-Paul Schützenberger and Glanffrwd Thomas. Since then, at least a dozen different proofs have appeared. The proof that I will show was published by Stembridge in 1997 (in [Stembr02], perhaps one of the most readable papers in all of mathematics), and crystallizes decades of work by many authors (Gasharov's somewhat similar proof [Gashar98] probably being the main harbinger). It will prove not just an expansion for $s_\nu s_\lambda$, but also a generalization (replacing s_λ by a skew Schur polynomial $s_{\lambda/\mu}$) found by Zelevinsky in 1981 ([Zelevi81]), as well as Theorem 7.3.11 **(b)**. My presentation of this proof will follow [GriRei20, §2.6] (which, in turn, elaborates on [Stembr02]).

To state the Littlewood–Richardson rule, we need some notions and notations. We begin with the notations:

Definition 7.3.25. **(a)** We let $\mathbf{0}$ denote the N-tuple $(0,0,\ldots,0) \in \mathbb{N}^N$.

(b) Let $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_N)$ and $\beta = (\beta_1,\beta_2,\ldots,\beta_N)$ be two N-tuples in $\mathbb{N}^N$. Then, we set

$$\alpha + \beta := (\alpha_1+\beta_1, \alpha_2+\beta_2, \ldots, \alpha_N+\beta_N) \qquad \text{and}$$
$$\alpha - \beta := (\alpha_1-\beta_1, \alpha_2-\beta_2, \ldots, \alpha_N-\beta_N).$$

Note that $\alpha + \beta \in \mathbb{N}^N$, whereas $\alpha - \beta \in \mathbb{Z}^N$.

Of course, the addition operation $+$ that we just defined on the set $\mathbb{N}^N$ is associative and commutative, and the N-tuple $\mathbf{0}$ is its neutral element. The subtraction operation $-$ undoes $+$. Note that the operation $+$ defined in Definition 7.3.25 is precisely the one that we used in Theorem 7.3.11 **(b)**. We notice that (using the notation of Definition 7.2.3 **(a)**) we have

$$x^\alpha x^\beta = x^{\alpha+\beta} \tag{264}$$

for any two N-tuples $\alpha, \beta \in \mathbb{N}^N$ (check this!).

Our next piece of notation is mostly a bookkeeping device:

Definition 7.3.26. Let λ and μ be two N-partitions. Let T be a tableau of shape λ/μ. We define the *content* of T to be the N-tuple $(a_1, a_2, \ldots, a_N)$, where

$$a_i := (\text{\# of } i\text{'s in } T) = (\text{\# of boxes } c \text{ of } T \text{ such that } T(c) = i).$$

We denote this N-tuple by $\operatorname{cont} T$.

For instance, if $N = 5$, then $\operatorname{cont} \begin{ytableau} 1 & 1 & 2 \\ 4 \end{ytableau} = (2, 1, 0, 1, 0)$.

Note that

$$x_T = x^{\operatorname{cont} T} \qquad \text{for any tableau } T. \tag{265}$$

(Indeed, both sides of this equality equal $\prod\limits_{i=1}^{N} x_i^{(\text{\# of } i\text{'s in } T)}$.)

Another notation lets us cut certain columns out of a tableau:

Definition 7.3.27. Let λ and μ be two N-partitions. Let T be a tableau of shape λ/μ. Let j be a positive integer. Then, $\operatorname{col}_{\geq j} T$ means the restriction of T to columns $j, j+1, j+2, \ldots$ (that is, the result of removing the first $j-1$ columns from T). Formally speaking, this means the restriction of the map T to the set $\{(u, v) \in Y(\lambda/\mu) \mid v \geq j\}$.

For example,

$$\operatorname{col}_{\geq 3} \begin{ytableau} \none & 1 & 1 & 2 \\ \none & 2 & 3 \\ 1 & 3 & 5 \\ 2 & 2 \end{ytableau} = \begin{ytableau} 1 & 2 \\ 3 \\ 5 \end{ytableau} \qquad \text{and}$$

$$\operatorname{col}_{\geq 5} \begin{ytableau} \none & 1 & 1 & 2 \\ \none & 2 & 3 \\ 1 & 3 & 5 \\ 2 & 2 \end{ytableau} = (\text{empty tableau}).$$

Remark 7.3.28. What shape does the tableau $\operatorname{col}_{\geq j} T$ in Definition 7.3.27 have?

We don't care, since we will only need this tableau for its content $\operatorname{col}_{\geq j} T$ (which is defined independently of the shape). However, the answer is not hard to give: If $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$, then $\operatorname{col}_{\geq j} T$ is a skew Young tableau of shape λ' / μ', where

$$\lambda' = (\min\{j-1, \lambda_1\}, \min\{j-1, \lambda_2\}, \ldots, \min\{j-1, \lambda_N\}) \qquad \text{and}$$
$$\mu' = (\min\{j-1, \mu_1\}, \min\{j-1, \mu_2\}, \ldots, \min\{j-1, \mu_N\}).$$

(Thus, the first $j-1$ columns of $\operatorname{col}_{\geq j} T$ are empty, i.e., have no boxes.)

Now we are ready to define a nontrivial notion:

Definition 7.3.29. Let λ, μ, ν be three N-partitions. A semistandard tableau T of shape λ / μ is said to be *ν-Yamanouchi* (this is an adjective) if for each positive integer j, the N-tuple $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) \in \mathbb{N}^N$ is an N-partition (i.e., weakly decreasing).

This is a complex and somewhat confusing notion; before we move on, let us thus give a metaphor that might help clarify it, and several examples.

Remark 7.3.30. Definition 7.3.29 becomes somewhat easier to conceptualize (and memorize) through a voting metaphor (which, incidentally, is the reason why $\mathbf{0}$-Yamanouchi tableaux are sometimes called "ballot tableaux"):

Let λ, μ, ν and T be as in Definition 7.3.29. Consider an election between N candidates numbered $1, 2, \ldots, N$. Regard each entry i of T as a single vote for candidate i. Thus, for example, the tableau $\begin{ytableau} \none & 1 & 2 \\ 2 & 5 \end{ytableau}$ has one vote for candidate 1, two votes for candidate 2, and one for candidate 5. Now, we count the votes by keeping an "tally board", i.e., an N-tuple $(a_1, a_2, \ldots, a_N) \in \mathbb{N}^N$ that records how many votes each candidate has received (namely, candidate i has received a_i votes). Assume that, at the beginning of our counting process, the tally board is ν (as a consequence of ballot stuffing, or because some votes have already been counted on the previous day). Now, we process the votes from the tableau T, column by column, starting with the rightmost column and moving left. Each time a column is processed, all the votes from this column are simultaneously added to our tally board. Thus, after the rightmost column is processed, our tally board is $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$, where j is the index of the rightmost column (i.e., the rightmost column is the j-th column). Then, the second-to-rightmost column gets processed, and the tally board becomes $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j-1} T\right)$. And so on, until all columns have been processed.

Now, the tableau T is ν-Yamanouchi if and only if the tally board has stayed weakly decreasing (i.e., candidate 1 has at least as many votes as candidate 2, who in turn has at least as many votes as candidate 3, who in turn has at least as many votes as candidate 4, and so on) throughout the vote counting process. This is just a trivial restatement of the definition of "ν-Yamanouchi", but in my impression it is conducive to understanding.

One takeaway from this interpretation is the following useful feature of the vote counting process: No candidate gains more than one vote at a single time (because no column of T has two equal entries). Thus, the number of votes for any given candidate increases only in small steps (viz., not at all or by only 1 vote).

Example 7.3.31. (a) Let $N = 3$ and $\nu = \mathbf{0} = (0,0,0)$. Which of the following six tableaux are $\mathbf{0}$-Yamanouchi?

$$T_1 = \begin{ytableau} \none & 1 & 1 \\ 2 & 2 \end{ytableau}\,, \qquad T_2 = \begin{ytableau} \none & 1 & 1 \\ 2 & 3 \end{ytableau}\,, \qquad T_3 = \begin{ytableau} \none & 1 & 2 \\ 2 & 2 \end{ytableau}\,,$$

$$T_4 = \begin{ytableau} \none & 1 \\ 1 \\ 2 \end{ytableau}\,, \qquad T_5 = \begin{ytableau} \none & 1 \\ 1 \\ 3 \end{ytableau}\,, \qquad T_6 = \begin{ytableau} \none & \none & 1 & 1 \\ \none & 1 & 2 & 2 \\ 2 & 3 \end{ytableau}\,.$$

Note that all six of these tableaux are semistandard.

Let us check whether T_1 is $\mathbf{0}$-Yamanouchi. Indeed, we compute the N-tuple $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) \in \mathbb{N}^N$ for each positive integer j, obtaining

$$\begin{aligned} \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 1} T_1\right) &= \mathbf{0} + (2,2,0) = (2,2,0)\,; \\ \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 2} T_1\right) &= \mathbf{0} + (2,1,0) = (2,1,0)\,; \\ \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 3} T_1\right) &= \mathbf{0} + (1,0,0) = (1,0,0)\,; \\ \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T_1\right) &= \mathbf{0} + (0,0,0) = (0,0,0) \quad \text{for each } j \geq 4. \end{aligned}$$

All of the results $(2,2,0)$, $(2,1,0)$, $(1,0,0)$ and $(0,0,0)$ are N-partitions. Thus, T_1 is $\mathbf{0}$-Yamanouchi.

Let us check whether T_2 is $\mathbf{0}$-Yamanouchi. Indeed,

$$\begin{aligned} \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 1} T_2\right) &= \mathbf{0} + (2,1,1) = (2,1,1) \quad \text{is an } N\text{-partition;} \\ \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 2} T_2\right) &= \mathbf{0} + (2,0,1) = (2,0,1) \quad \text{is } \textbf{not} \text{ an } N\text{-partition.} \end{aligned}$$

Thus, T_2 is **not** $\mathbf{0}$-Yamanouchi.

The tableau T_3 is **not** $\mathbf{0}$-Yamanouchi, since $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq 1} T_3\right) = (1,3,0)$ is not an N-partition.

The tableau T_4 is $\mathbf{0}$-Yamanouchi.

The tableau T_5 is **not** $\mathbf{0}$-Yamanouchi, since $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq 1} T_5\right) = (2,0,1)$ is not an N-partition.

The tableau T_6 is $\mathbf{0}$-Yamanouchi.

(b) So we know that T_2, T_3, T_5 are not $\mathbf{0}$-Yamanouchi. However, they are ν-Yamanouchi for some other N-partitions ν. For example:

- The tableau T_2 becomes ν-Yamanouchi for $\nu = (1,1,0)$.
- The tableau T_3 becomes ν-Yamanouchi for $\nu = (2,0,0)$.
- The tableau T_5 becomes ν-Yamanouchi for $\nu = (1,1,0)$.

These are, in a sense, the "minimal" choices of ν for this to happen, but of course there are many other choices of ν that work.

We can now state the Littlewood–Richardson rule:

Theorem 7.3.32 (Zelevinsky's generalized Littlewood–Richardson rule, in Yamanouchi form)**.** Let λ, μ, ν be three N-partitions. Then,

$$s_\nu \cdot s_{\lambda/\mu} = \sum_{\substack{T \text{ is a } \nu\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } \lambda/\mu}} s_{\nu + \operatorname{cont} T}. \qquad (266)$$

Some comments are in order:

- In the sum on the right hand side of (266), the Schur polynomial $s_{\nu+\operatorname{cont} T}$ is always well-defined. Indeed, if T is a ν-Yamanouchi semistandard tableau of shape λ/μ, then $\nu + \operatorname{cont} \underbrace{T}_{=\operatorname{col}_{\geq 1} T} = \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 1} T\right)$ is an N-partition (by the definition of "ν-Yamanouchi"), so that $s_{\nu+\operatorname{cont} T}$ is a well-defined Schur polynomial.
- Theorem 7.3.32 expresses a product of a regular Schur polynomial s_ν with a skew Schur polynomial $s_{\lambda/\mu}$ as a sum of Schur polynomials. You can get a similar formula for the product of two regular Schur polynomials by setting $\mu = \mathbf{0} = (0,0,\ldots,0)$ in Theorem 7.3.32, so that $s_{\lambda/\mu}$ becomes $s_{\lambda/\mathbf{0}} = s_\lambda$.

Example 7.3.33. Let us apply Theorem 7.3.32 to $N = 3$ and $\nu = (1,0,0)$ and $\lambda = (2,1,0)$ and $\mu = \mathbf{0} = (0,0,0)$. Thus we get

$$s_{(1,0,0)} \cdot s_{(2,1,0)} = \sum_{\substack{T \text{ is a } (1,0,0)\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } (2,1,0)/\mathbf{0}}} s_{(1,0,0)+\operatorname{cont} T}. \qquad (267)$$

What are the T's in the sum? The $(1,0,0)$-Yamanouchi semistandard tableaux of shape $(2,1,0)/\mathbf{0}$ are

$$\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 2 \\ \cline{1-1}\end{array}\ , \qquad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 \\ \cline{1-1}\end{array}\ , \qquad \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\ ,$$

and the corresponding addends of our sum are

$$\begin{aligned} s_{(1,0,0)+(2,1,0)} &= s_{(3,1,0)}, \\ s_{(1,0,0)+(1,2,0)} &= s_{(2,2,0)}, \\ s_{(1,0,0)+(1,1,1)} &= s_{(2,1,1)}. \end{aligned}$$

Thus, the equality (267) rewrites as

$$s_{(1,0,0)} \cdot s_{(2,1,0)} = s_{(3,1,0)} + s_{(2,2,0)} + s_{(2,1,1)}.$$

Note that $s_{(1,0,0)} = x_1 + x_2 + x_3$ and $s_{(2,1,0)} = \sum\limits_{i \leq j \text{ and } i < k} x_i x_j x_k$.

We will prove the Littlewood–Richardson rule as a consequence of the following lemma:

Lemma 7.3.34 (Stembridge's Lemma)**.** Let λ, μ, ν be three N-partitions. Then,

$$a_{\nu+\rho} \cdot s_{\lambda/\mu} = \sum_{\substack{T \text{ is a } \nu\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } \lambda/\mu}} a_{\nu+\operatorname{cont} T+\rho}.$$

Before we prove this lemma, let us explore its consequences. One of them is the Littlewood–Richardson rule; another is Theorem 7.3.11 **(b)**. Let us first see how the latter can be derived from the lemma. This derivation, in turn, relies on another (simple) lemma:

Lemma 7.3.35. Let λ be any N-partition. Let T be a semistandard tableau of shape λ. Then, $T(i,j) \geq i$ for each $(i,j) \in Y(\lambda)$.

Proof of Lemma 7.3.35. This lemma is an easy consequence of the fact that the entries of a semistandard tableau increase strictly down each column. A detailed proof is given in Section B.7. □

*Proof of Theorem 7.3.11 **(b)** using Lemma 7.3.34.* Recall that $\mathbf{0} = (0, 0, \ldots, 0) \in \mathbb{N}^N$. Applying Lemma 7.3.34 to $\mu = \mathbf{0}$ and $\nu = \mathbf{0}$, we obtain

$$a_{\mathbf{0}+\rho} \cdot s_{\lambda/\mathbf{0}} = \sum_{\substack{T \text{ is a } \mathbf{0}\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } \lambda/\mathbf{0}}} a_{\mathbf{0}+\operatorname{cont} T+\rho}.$$

This rewrites as

$$a_\rho \cdot s_\lambda = \sum_{\substack{T \text{ is a } \mathbf{0}\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } \lambda/\mathbf{0}}} a_{\operatorname{cont} T+\rho} \qquad (268)$$

(since $\mathbf{0}+\rho=\rho$ and $s_{\lambda/\mathbf{0}}=s_\lambda$ and $\mathbf{0}+\operatorname{cont}T=\operatorname{cont}T$).

Now, we shall analyze the sum on the right hand side. What are the $\mathbf{0}$-Yamanouchi semistandard tableaux of shape $\lambda/\mathbf{0}$? One such tableau is easy to construct: namely, the one tableau (of shape $\lambda/\mathbf{0}$) whose all entries in the 1-st row are 1's, all entries in the 2-nd row are 2's, all entries in the 3-rd row are 3's, and so on. Let us call this tableau *minimalistic*, and denote it by T_0. Formally speaking, this minimalistic tableau T_0 is defined to be the map $Y(\lambda/0)\to[N]$ that sends each $(i,j)\in Y(\lambda/0)$ to i. Here is how this minimalistic tableau looks like for $N=4$ and $\lambda=(4,2,2,1)$:

$$T_0=\begin{array}{|c|c|c|c|}\hline 1&1&1&1\\ \hline 2&2 \\ \cline{1-2} 3&3 \\ \cline{1-2} 4 \\ \cline{1-1}\end{array}\ .$$

It turns out that this minimalistic tableau is the only T on the right hand side of (268). This will follow from the following two observations:

> *Observation 1:* The minimalistic tableau T_0 is a $\mathbf{0}$-Yamanouchi semistandard tableau of shape $\lambda/\mathbf{0}$.
>
> *Observation 2:* If T is a $\mathbf{0}$-Yamanouchi semistandard tableau of shape $\lambda/\mathbf{0}$, then $T=T_0$.

[*Proof of Observation 1:* It is clear that T_0 is a semistandard tableau of shape $\lambda/\mathbf{0}$. Thus, we only need to show that it is $\mathbf{0}$-Yamanouchi. In other words, we need to show that for each positive integer j, the N-tuple $\mathbf{0}+\operatorname{cont}\left(\operatorname{col}_{\geq j}T_0\right)\in\mathbb{N}^N$ is an N-partition (i.e., weakly decreasing).

This can be done directly: Write λ in the form $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_N)$. Thus, $\lambda_1\geq\lambda_2\geq\cdots\geq\lambda_N$ (since λ is an N-partition). Let j be a positive integer. Recall that the tableau T_0 is minimalistic; hence, the restricted tableau $\operatorname{col}_{\geq j}T_0$ is itself minimalistic (meaning that all its entries in the 1-st row are 1's, all entries in the 2-nd row are 2's, all entries in the 3-rd row are 3's, and so on). Therefore, for each $i\in[N]$, we have

$$\begin{aligned}&\left(\#\text{ of }i\text{'s in }\operatorname{col}_{\geq j}T_0\right)\\ &=\left(\#\text{ of boxes in the }i\text{-th row of }\operatorname{col}_{\geq j}T_0\right)\\ &=\max\{\lambda_i-(j-1),0\}\end{aligned}\tag{269}$$

(since the i-th row of T_0 has λ_i many boxes, and thus the i-th row of $\operatorname{col}_{\geq j}T_0$ has $\max\{\lambda_i-(j-1),0\}$ many boxes). Now, the N-tuple

$$\begin{aligned}&\mathbf{0}+\operatorname{cont}\left(\operatorname{col}_{\geq j}T_0\right)\\ &=\operatorname{cont}\left(\operatorname{col}_{\geq j}T_0\right)\\ &=\left(\#\text{ of 1's in }\operatorname{col}_{\geq j}T_0,\ \ \#\text{ of 2's in }\operatorname{col}_{\geq j}T_0,\ \ \ldots,\ \ \#\text{ of }N\text{'s in }\operatorname{col}_{\geq j}T_0\right)\\ &=\left(\max\{\lambda_1-(j-1),0\},\ \max\{\lambda_2-(j-1),0\},\ \ldots,\ \max\{\lambda_N-(j-1),0\}\right)\\ &\qquad\qquad(\text{by (269)})\end{aligned}$$

is weakly decreasing (since $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ quickly yields $\max\{\lambda_1 - (j-1), 0\} \geq \max\{\lambda_2 - (j-1), 0\} \geq \cdots \geq \max\{\lambda_N - (j-1), 0\}$), and thus is an N-partition. Forget that we fixed j. Thus, we have shown that for each positive integer j, the N-tuple $\mathbf{0} + \operatorname{cont}(\operatorname{col}_{\geq j} T_0) \in \mathbb{N}^N$ is an N-partition. This proves that the tableau T_0 is $\mathbf{0}$-Yamanouchi. This completes the proof of Observation 1.]

[*Proof of Observation 2:* Let T be a $\mathbf{0}$-Yamanouchi semistandard tableau of shape $\lambda/\mathbf{0}$. We must prove that $T = T_0$.

Let us assume the contrary. Thus, $T \neq T_0$. Hence, there exists some $(i,j) \in Y(\lambda/\mathbf{0})$ satisfying $T(i,j) \neq T_0(i,j)$. Choose such an (i,j) with maximum possible j. More precisely, among all such pairs (i,j) with maximum possible j, we choose one with the minimum possible i.

Thus, for each $(i',j') \in Y(\lambda/\mathbf{0})$ satisfying $j' > j$, we have

$$T(i',j') = T_0(i',j') \tag{270}$$

(since we have chosen (i,j) to have maximum possible j among the pairs satisfying $T(i,j) \neq T_0(i,j)$). Furthermore, for each $(i',j') \in Y(\lambda/\mathbf{0})$ satisfying $i' < i$ and $j' = j$, we have

$$T(i',j') = T_0(i',j') \tag{271}$$

(since we have chosen (i,j) to have minimum possible i among the maximum-j pairs satisfying $T(i,j) \neq T_0(i,j)$).

The definition of the minimalistic tableau T_0 yields $T_0(i,j) = i$. Set $p := T(i,j)$. Hence, $p = T(i,j) \neq T_0(i,j) = i$. [133]

The number p appears at least once in the j-th column of T (since $p = T(i,j)$), and thus appears at least once in the restricted tableau $\operatorname{col}_{\geq j} T$ (since this restricted tableau contains the j-th column of T).

The definition of $Y(\lambda/\mathbf{0})$ yields $Y(\lambda/\mathbf{0}) = Y(\lambda) \setminus \underbrace{Y(\mathbf{0})}_{=\varnothing} = Y(\lambda)$. Hence, a tableau of shape $\lambda/\mathbf{0}$ is the same as a tableau of shape λ. Thus, T is a tableau of shape λ (since T is a tableau of shape $\lambda/\mathbf{0}$). Since T is semistandard, we can thus apply Lemma 7.3.35, and conclude that $T(i,j) \geq i$. Hence, $p = T(i,j) \geq i$. Combining this with $p \neq i$, we obtain $p > i$. In other words, $i < p$.

Now, recall that T is $\mathbf{0}$-Yamanouchi; hence, $\mathbf{0} + \operatorname{cont}(\operatorname{col}_{\geq j} T)$ is an N-partition (by the definition of "$\mathbf{0}$-Yamanouchi"). In other words, $\operatorname{cont}(\operatorname{col}_{\geq j} T)$ is an N-partition

[133] Here is an example of how our tableau T can look like at this point (for $N = 6$ and $\lambda = (6,5,5,2,2,1)$ and $(i,j) = (3,2)$):

?	1	1	1	1	1
?	2	2	2	2	
?	p	3	3	3	
?	?				
?	?				
?					

.

Here, the known entries come from (270) and (271) (since the definition of the minimalistic tableau T_0 shows that $T_0(i',j') = i'$ for each $(i',j') \in Y(\lambda/\mathbf{0})$).

(since $\mathbf{0} + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) = \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$). Write this N-partition $\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ as $(a_1, a_2, \ldots, a_N)$. For each $k \in [N]$, its entry a_k is the # of k's in $\operatorname{col}_{\geq j} T$ (by the definition of $\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$). Applying this to $k = i$, we see that a_i is the # of i's in $\operatorname{col}_{\geq j} T$.

Similarly, a_p is the # of p's in $\operatorname{col}_{\geq j} T$. Hence, $a_p \geq 1$ (since we know that the number p appears at least once in the restricted tableau $\operatorname{col}_{\geq j} T$). However, $a_1 \geq a_2 \geq \cdots \geq a_N$ (since $(a_1, a_2, \ldots, a_N)$ is an N-partition), and thus $a_i \geq a_p$ (since $i < p$). Hence, $a_i \geq a_p \geq 1$. In other words, the number i appears at least once in the restricted tableau $\operatorname{col}_{\geq j} T$ (since a_i is the # of i's in $\operatorname{col}_{\geq j} T$). In other words, the number i appears at least once in one of the columns $j, j+1, j+2, \ldots$ of the tableau T. In other words, there exists some $(i', j') \in Y(\lambda / \mathbf{0})$ satisfying $j' \geq j$ and $T(i', j') = i$. Consider this (i', j').

Let us first assume (for the sake of contradiction) that $j' > j$. Thus, (270) yields $T(i', j') = T_0(i', j') = i'$ (by the definition of the minimalistic tableau T_0). Therefore, $i' = T(i', j') = i$. Hence, we can rewrite $(i', j') \in Y(\lambda / \mathbf{0})$ and $T(i', j') = i$ as $(i, j') \in Y(\lambda / \mathbf{0})$ and $T(i, j') = i$. Also, $j < j'$ (since $j' > j$). However, the tableau T is semistandard; thus, its entries increase weakly along each row. Therefore, from $j < j'$, we obtain $T(i, j) \leq T(i, j')$ [134]. Thus, $p = T(i, j) \leq T(i, j') = i$. But this contradicts $p > i$.

This contradiction shows that our assumption (that $j' > j$) was false. Hence, we must have $j' \leq j$. Combined with $j' \geq j$, this yields $j' = j$. Thus, we can rewrite $(i', j') \in Y(\lambda / \mathbf{0})$ and $T(i', j') = i$ as $(i', j) \in Y(\lambda / \mathbf{0})$ and $T(i', j) = i$.

We assume (for the sake of contradiction) that $i' < i$. Hence, (271) yields $T(i', j') = T_0(i', j') = i'$ (by the definition of the minimalistic tableau T_0), so that $i' = T(i', j') = i$; but this contradicts $i' < i$.

This contradiction shows that our assumption (that $i' < i$) was false. Hence, we must have $i' \geq i$. In other words, $i \leq i'$. However, the tableau T is semistandard; thus, its entries increase strictly down each column. Therefore, from $i \leq i'$, we obtain $T(i, j) \leq T(i', j)$ [135]. Thus, $T(i', j) \geq T(i, j) = p > i$, so that $i < T(i', j) = i$. Thus we have obtained a contradiction again. This contradiction shows that our assumption was false; hence, $T = T_0$. This proves Observation 2.]

Combining Observation 1 with Observation 2, we see that the minimalistic tableau T_0 is the **only** $\mathbf{0}$-Yamanouchi semistandard tableau of shape $\lambda / \mathbf{0}$. Hence, the sum on the right hand side of (268) has only one addend, namely the addend for $T = T_0$. Thus, (268) simplifies to

$$a_\rho \cdot s_\lambda = a_{\operatorname{cont}(T_0) + \rho} = a_{\lambda + \rho},$$

since it is easy to see that $\operatorname{cont}(T_0) = \lambda$. This proves Theorem 7.3.11 **(b)** (using Lemma 7.3.34). □

Let us furthermore derive Theorem 7.3.32 from Lemma 7.3.34. This relies on some elementary properties of certain polynomials. The underlying notion is defined in an arbitrary commutative ring:

[134] Strictly speaking, this follows by applying Lemma 7.3.17 **(a)** to (i, j) and (i, j') instead of (i, j_1) and (i, j_2).

[135] Strictly speaking, this follows by applying Lemma 7.3.17 **(b)** to (i, j) and (i', j) instead of (i_1, j) and (i_2, j).

Definition 7.3.36. Let L be a commutative ring. Let $a \in L$. The element a of L is said to be *regular* if and only if every $x \in L$ satisfying $ax = 0$ satisfies $x = 0$.

Regular elements of a commutative ring are often called *"non-zero-divisors"*[136] or *cancellable* elements. The latter word is explained by the following simple fact:

Lemma 7.3.37. Let L be a commutative ring. Let $a, u, v \in L$ be such that a is regular. Assume that $au = av$. Then, $u = v$.

Proof of Lemma 7.3.37. We have $a(u - v) = au - av = 0$ (since $au = av$). However, a is regular; in other words, every $x \in L$ satisfying $ax = 0$ satisfies $x = 0$ (by the definition of "regular"). Applying this to $x = u - v$, we obtain $u - v = 0$ (since $a(u - v) = 0$). Thus, $u = v$. This proves Lemma 7.3.37. □

Lemma 7.3.37 shows that regular elements of a commutative ring can be cancelled when they appear as factors on both sides of an equality. To make use of this, we need to actually find nontrivial regular elements. Here is one:

Lemma 7.3.38. The element a_ρ of the polynomial ring $\mathcal{P}$ is regular.

Proof of Lemma 7.3.38 (sketched). There are different ways to prove this. One is to define a lexicographic order on the monomials in $\mathcal{P}$, and to argue that the leading coefficient of a_ρ with respect to this order is 1 (which is a regular element of R); this uses a bit of multivariate polynomial theory (see [21w, Lecture 16, Proposition 1.2.9] for the properties of polynomials that are used here).[137]

Here is a more elementary proof. First, we observe that each of the indeterminates $x_1, x_2, \ldots, x_N$ is regular (as an element of $\mathcal{P}$). Indeed, multiplying a polynomial f by an indeterminate x_i merely shifts the coefficients of f to different monomials; thus, if $x_i f = 0$, then $f = 0$. Next, we conclude that the polynomial $x_i - x_j \in \mathcal{P}$ is regular whenever $1 \leq i < j \leq N$. Indeed, this polynomial $x_i - x_j$ is the image of the indeterminate x_i under a certain K-algebra automorphism of $\mathcal{P}$ (namely, under the automorphism that sends x_i to $x_i - x_j$ while leaving all other indeterminates unchanged[138]), and therefore is regular because x_i is

[136] This name is somewhat murky in the literature (and is best avoided). In fact, many authors prefer to consider 0 to be a non-zero-divisor as well (so that they can say that an integral domain has no zero-divisors, rather than saying that the only zero-divisor in an integral domain is 0), even though 0 is not a regular element (unless the ring L is trivial). This exception tends to make the notion of a non-zero-divisor fickle and unreliable.

[137] This argument can in fact be used to show a more general statement: Namely, for any N-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N) \in \mathbb{N}^N$ satisfying $\alpha_1 > \alpha_2 > \cdots > \alpha_N$, the alternant a_α is regular in $\mathcal{P}$. (But we won't need this statement.)

[138] This is an automorphism, because its inverse is easily constructed (namely, it sends x_i to $x_i + x_j$ while leaving all other indeterminates unchanged).

regular (and because any ring automorphism sends regular elements to regular elements). However, it is easy to see (see [Grinbe21, Proposition 2.3] for a proof) that any finite product of regular elements is again regular. Thus, the element $\prod\limits_{1\leq i<j\leq N}\left(x_i-x_j\right)\in\mathcal{P}$ is regular (since it is the product of the regular elements x_i-x_j for $1\leq i<j\leq N$). In view of (251), this rewrites as follows: The element $a_\rho\in\mathcal{P}$ is regular. This proves Lemma 7.3.38. □

We can now derive Theorem 7.3.32 from Lemma 7.3.34:

Proof of Theorem 7.3.32 using Lemma 7.3.34. Theorem 7.3.11 **(b)** (applied to ν instead of λ) tells us that $a_{\nu+\rho}=a_\rho\cdot s_\nu$. However, Lemma 7.3.34 says that

$$\begin{aligned}a_{\nu+\rho}\cdot s_{\lambda/\mu}&=\sum_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}\underbrace{a_{\nu+\operatorname{cont}T+\rho}}_{\substack{=a_\rho\cdot s_{\nu+\operatorname{cont}T}\\\text{(by Theorem 7.3.11 (b)}\\\text{(applied to }\nu+\operatorname{cont}T\text{ instead of }\lambda\text{),}\\\text{since }\nu+\operatorname{cont}T\text{ is an }N\text{-partition}\\\text{(as we have shown in a comment}\\\text{after Theorem 7.3.32))}}}\\&=\sum_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}a_\rho\cdot s_{\nu+\operatorname{cont}T}=a_\rho\cdot\sum_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}s_{\nu+\operatorname{cont}T}.\end{aligned}$$

In view of $a_{\nu+\rho}=a_\rho\cdot s_\nu$, this equality rewrites as

$$a_\rho\cdot s_\nu\cdot s_{\lambda/\mu}=a_\rho\cdot\sum_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}s_{\nu+\operatorname{cont}T}.$$

Since the element $a_\rho\in\mathcal{P}$ is regular (by Lemma 7.3.38), we can cancel a_ρ from this equality (i.e., we can apply Lemma 7.3.37 to $L=\mathcal{P}$ and $a=a_\rho$ and $u=s_\nu\cdot s_{\lambda/\mu}$ and $v=\sum\limits_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}s_{\nu+\operatorname{cont}T}$). As a result, we obtain

$$s_\nu\cdot s_{\lambda/\mu}=\sum_{\substack{T\text{ is a }\nu\text{-Yamanouchi}\\\text{semistandard tableau}\\\text{of shape }\lambda/\mu}}s_{\nu+\operatorname{cont}T}.$$

Thus, Theorem 7.3.32 is proven. □

Thus it remains to prove Stembridge's lemma. Before we do so, let us spell out two simple properties of alternants that will be used in the proof:

> **Lemma 7.3.39.** Let $\alpha\in\mathbb{N}^N$.
>
> **(a)** If the N-tuple α has two equal entries, then $a_\alpha=0$.
>
> **(b)** Let $\beta\in\mathbb{N}^N$ be an N-tuple obtained from α by swapping two entries. Then, $a_\beta=-a_\alpha$.

Proof of Lemma 7.3.39. This is an easy consequence of Definition 7.3.2 **(b)**. See Section B.7 for a detailed proof. □

Proof of Lemma 7.3.34. For any $\beta \in \mathbb{N}^N$ and any $i \in [N]$, we let β_i denote the i-th entry of β. Thus, for example, $\rho_k = N - k$ for each $k \in [N]$ (since $\rho = (N-1, N-2, \ldots, N-N)$).

Since addition on $\mathbb{N}^N$ is defined entrywise, we have $(\beta + \gamma)_i = \beta_i + \gamma_i$ for any $\beta, \gamma \in \mathbb{N}^N$ and $i \in [N]$.

The group S_N acts on $\mathcal{P}$ by K-algebra automorphisms. Hence, in particular, we have

$$\sigma \cdot (fg) = (\sigma \cdot f) \cdot (\sigma \cdot g)$$

for any $\sigma \in S_N$ and any $f, g \in \mathcal{P}$. In other words, we have

$$(\sigma \cdot f) \cdot (\sigma \cdot g) = \sigma \cdot (fg) \qquad (272)$$

for any $\sigma \in S_N$ and any $f, g \in \mathcal{P}$.

The polynomial $s_{\lambda/\mu}$ is symmetric (by Theorem 7.3.21). The definition of $s_{\lambda/\mu}$ yields

$$s_{\lambda/\mu} = \sum_{T \in \operatorname{SSYT}(\lambda/\mu)} \underbrace{x_T}_{\substack{= x^{\operatorname{cont} T} \\ \text{(by (265))}}} = \sum_{T \in \operatorname{SSYT}(\lambda/\mu)} x^{\operatorname{cont} T}. \qquad (273)$$

For any $\beta \in \mathbb{N}^N$, we have

$$\begin{aligned}
a_\beta &= \det\left(\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}\right) \qquad \text{(by the definition of the alternant } a_\beta\text{)} \\
&= \det\left(\left(x_j^{\beta_i}\right)_{1\le i\le N,\ 1\le j\le N}\right) \\
&\qquad \left(\begin{array}{c}\text{by Theorem 6.4.10,} \\ \text{since } \left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N} = \left(\left(x_j^{\beta_i}\right)_{1\le i\le N,\ 1\le j\le N}\right)^T\end{array}\right) \\
&= \sum_{\sigma \in S_N} (-1)^\sigma \underbrace{x_{\sigma(1)}^{\beta_1} x_{\sigma(2)}^{\beta_2} \cdots x_{\sigma(N)}^{\beta_N}}_{\substack{= \sigma \cdot \left(x_1^{\beta_1} x_2^{\beta_2} \cdots x_N^{\beta_N}\right) \\ \text{(because the action of } \sigma \in S_N \\ \text{on } \mathcal{P} \text{ substitutes } x_{\sigma(i)} \text{ for each } x_i\text{)}}} \\
&\qquad \text{(by the definition of a determinant)} \\
&= \sum_{\sigma \in S_N} (-1)^\sigma \sigma \cdot \underbrace{\left(x_1^{\beta_1} x_2^{\beta_2} \cdots x_N^{\beta_N}\right)}_{= x^\beta} = \sum_{\sigma \in S_N} (-1)^\sigma \sigma \cdot x^\beta. \qquad (274)
\end{aligned}$$

Applying this to $\beta = \nu + \rho$, we obtain

$$a_{\nu+\rho} = \sum_{\sigma \in S_N} (-1)^\sigma \sigma \cdot x^{\nu+\rho}.$$

Multiplying both sides of this equality by $s_{\lambda/\mu}$, we find

$$\begin{aligned}
a_{\nu+\rho}\cdot s_{\lambda/\mu} &= \left(\sum_{\sigma\in S_N}(-1)^\sigma\,\sigma\cdot x^{\nu+\rho}\right)\cdot s_{\lambda/\mu} \\
&= \sum_{\sigma\in S_N}(-1)^\sigma\left(\sigma\cdot x^{\nu+\rho}\right)\cdot \underbrace{s_{\lambda/\mu}}_{\substack{=\sigma\cdot s_{\lambda/\mu} \\ \text{(since } s_{\lambda/\mu} \text{ is symmetric,} \\ \text{so that } \sigma\cdot s_{\lambda/\mu}=s_{\lambda/\mu})}} \\
&= \sum_{\sigma\in S_N}(-1)^\sigma\underbrace{\left(\sigma\cdot x^{\nu+\rho}\right)\cdot\left(\sigma\cdot s_{\lambda/\mu}\right)}_{\substack{=\sigma\cdot\left(x^{\nu+\rho}s_{\lambda/\mu}\right) \\ \text{(by (272))}}} \\
&= \sum_{\sigma\in S_N}(-1)^\sigma\,\sigma\cdot\left(x^{\nu+\rho}s_{\lambda/\mu}\right). \qquad (275)
\end{aligned}$$

However, multiplying both sides of (273) by $x^{\nu+\rho}$, we find

$$\begin{aligned}
x^{\nu+\rho}s_{\lambda/\mu} &= x^{\nu+\rho}\sum_{T\in\operatorname{SSYT}(\lambda/\mu)}x^{\operatorname{cont}T} = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\underbrace{x^{\nu+\rho}x^{\operatorname{cont}T}}_{\substack{=x^{\nu+\rho+\operatorname{cont}T} \\ \text{(by (264))}}} \\
&= \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\underbrace{x^{\nu+\rho+\operatorname{cont}T}}_{=x^{\nu+\operatorname{cont}T+\rho}} = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}x^{\nu+\operatorname{cont}T+\rho}.
\end{aligned}$$

Thus, any $\sigma\in S_N$ satisfies

$$\sigma\cdot\left(x^{\nu+\rho}s_{\lambda/\mu}\right) = \sigma\cdot\left(\sum_{T\in\operatorname{SSYT}(\lambda/\mu)}x^{\nu+\operatorname{cont}T+\rho}\right) = \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\sigma\cdot x^{\nu+\operatorname{cont}T+\rho}$$

(since the action of σ on $\mathcal{P}$ is a K-algebra automorphism of $\mathcal{P}$, and thus in particular is K-linear). Therefore, (275) becomes

$$\begin{aligned}
a_{\nu+\rho}\cdot s_{\lambda/\mu} &= \sum_{\sigma\in S_N}(-1)^\sigma\underbrace{\sigma\cdot\left(x^{\nu+\rho}s_{\lambda/\mu}\right)}_{=\sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\sigma\cdot x^{\nu+\operatorname{cont}T+\rho}} \\
&= \sum_{\sigma\in S_N}(-1)^\sigma\sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\sigma\cdot x^{\nu+\operatorname{cont}T+\rho} \\
&= \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}\underbrace{\sum_{\sigma\in S_N}(-1)^\sigma\,\sigma\cdot x^{\nu+\operatorname{cont}T+\rho}}_{\substack{=a_{\nu+\operatorname{cont}T+\rho} \\ \text{(by (274), applied to } \beta=\nu+\operatorname{cont}T+\rho)}} \\
&= \sum_{T\in\operatorname{SSYT}(\lambda/\mu)}a_{\nu+\operatorname{cont}T+\rho}. \qquad (276)
\end{aligned}$$

This almost looks like the claim we want to prove, but the sum on the right hand side is too big: It runs over all semistandard tableaux of shape λ/μ, while we only want it to run over the ones that are ν-Yamanouchi. Thus, we will now try to cancel the extraneous addends (i.e., the addends corresponding to the T's that are not ν-Yamanouchi).

Let us first make this a bit more precise. We define two sets

$$\mathcal{A} := \operatorname{SSYT}(\lambda/\mu) \qquad \text{and}$$
$$\mathcal{X} := \{T \in \operatorname{SSYT}(\lambda/\mu) \mid T \text{ is not } \nu\text{-Yamanouchi}\}.$$

For each $T \in \mathcal{A}$, we define an element $\operatorname{sign} T \in \mathcal{P}$ by

$$\operatorname{sign} T := a_{\nu+\operatorname{cont} T+\rho}.$$

Thus, (276) rewrites as

$$a_{\nu+\rho} \cdot s_{\lambda/\mu} = \sum_{T\in\mathcal{A}} \operatorname{sign} T. \tag{277}$$

We shall now construct a sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$.

Indeed, let $T \in \mathcal{X}$. Thus, T is a semistandard tableau of shape λ/μ that is not ν-Yamanouchi (by the definition of $\mathcal{X}$). Hence, there exists at least one $j \geq 1$ such that the N-tuple $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ is **not** an N-partition (by the definition of "ν-Yamanouchi"). Any such j will be called a *violator* of T. Thus, there exists at least one violator of T. In other words, the set of all violators of T is nonempty. On the other hand, this set is finite[139]. Hence, this set has a maximum element. In other words, the largest violator of T exists.[140]

Let j be the **largest** violator of T. Then, $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ is not an N-partition, but $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right)$ is an N-partition (since j is the **largest** violator of T).

Define two N-tuples $b \in \mathbb{N}^N$ and $c \in \mathbb{N}^N$ by $b := \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ and $c := \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right)$. Thus, b is not an N-partition[141], but c is an N-partition[142].

[139] *Proof.* Let $j \geq 1$ be larger than each entry of λ. Then, the restricted tableau $\operatorname{col}_{\geq j} T$ is empty and thus satisfies $\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) = \mathbf{0}$. Hence, $\nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)}_{=\mathbf{0}} = \nu + \mathbf{0} = \nu$, which is an N-partition by assumption. Thus, j is not a violator of T (by the definition of a "violator").

Forget that we fixed j. We thus have shown that if $j \geq 1$ is larger than each entry of λ, then j is not a violator of T. Hence, if $j \geq 1$ is sufficiently high, then j is not a violator of T. Thus, the set of violators of T is bounded from above, and therefore finite (since it is a set of positive integers).

[140] For example, if $\nu = \mathbf{0}$, then the tableaux

$$T_2 = \begin{array}{ccc} & \boxed{1} & \boxed{1} \\ \boxed{2} & \boxed{3} & \end{array}, \qquad T_3 = \begin{array}{ccc} & \boxed{1} & \boxed{2} \\ \boxed{2} & \boxed{2} & \end{array}, \qquad T_5 = \begin{array}{cc} & \boxed{1} \\ \boxed{1} & \\ \boxed{3} & \end{array}$$

from Example 7.3.31 have largest violators $2, 3, 1$, respectively.

[141] since $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ is not an N-partition

[142] since $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right)$ is an N-partition

Since b is not an N-partition, there exists some $k \in [N-1]$ such that $b_k < b_{k+1}$. Such a k will be called a *misstep* of T. Thus, there exists a misstep of T. Let k be the **smallest** misstep of T. Then, $b_k < b_{k+1}$ (since k is a misstep of T). Furthermore, $c_k \geq c_{k+1}$ (since c is an N-partition).

Example 7.3.40. For this example, let $N = 7$ and $\nu = (4, 2, 2, 0, 0, 0, 0)$ and $\lambda = (7, 7, 6, 5, 4, 0, 0)$ and $\mu = (6, 2, 2, 0, 0, 0, 0)$. Let T be the following semistandard tableau of shape λ / μ:

$$T = \begin{array}{ccccccc} & & & & & & 2 \\ & & 1 & 1 & 2 & 2 & 3 \\ & & 2 & 2 & 3 & 4 & \\ 1 & 3 & 3 & 5 & 6 & & \\ 2 & 4 & 5 & 6 & & & \end{array} .$$

We have

$$\begin{aligned} \nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)}_{=\mathbf{0}} &= \nu = (4, 2, 2, 0, 0, 0, 0) \qquad \text{for each } j \geq 8; \\ \nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq 7} T\right)}_{=(0,1,1,0,0,0,0)} &= \nu + (0, 1, 1, 0, 0, 0, 0) = (4, 3, 3, 0, 0, 0, 0); \\ \nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq 6} T\right)}_{=(0,2,1,1,0,0,0)} &= \nu + (0, 2, 1, 1, 0, 0, 0) = (4, 4, 3, 1, 0, 0, 0); \\ \nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq 5} T\right)}_{=(0,3,2,1,0,1,0)} &= \nu + (0, 3, 2, 1, 0, 1, 0) = (4, 5, 4, 1, 0, 1, 0). \end{aligned}$$

Thus, $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq 5} T\right)$ is not an N-partition. This shows that T is not ν-Yamanouchi (so that $T \in \mathcal{X}$), and in fact 5 is the smallest violator of T. Thus, according to our above instructions, we set

$$\begin{aligned} & j := 5 \qquad \text{and} \\ & b := \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) = \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 5} T\right) = (4, 5, 4, 1, 0, 1, 0) \qquad \text{and} \\ & c := \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right) = \nu + \operatorname{cont}\left(\operatorname{col}_{\geq 6} T\right) = (4, 4, 3, 1, 0, 0, 0). \end{aligned}$$

The missteps of T are the numbers $k \in [N-1]$ such that $b_k < b_{k+1}$; these numbers are 2 and 5 (since $b_2 < b_3$ and $b_5 < b_6$). Thus, the smallest misstep of T is 2. Hence, we set $k := 2$.

Let us next make a few general observations about b and c.

The restrictions $\operatorname{col}_{\geq j} T$ and $\operatorname{col}_{\geq j+1} T$ of T are "almost the same": The only difference between them is that the j-th column of T is included in $\operatorname{col}_{\geq j} T$ but not in $\operatorname{col}_{\geq j+1} T$. Hence,

$$\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right) = \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right) + \operatorname{cont}\left(\operatorname{col}_j T\right),$$

where $\operatorname{col}_j T$ denotes the j-th column of T (or, to be more precise, the restriction of T to the j-th column). Now,

$$\begin{aligned} b &= \nu + \underbrace{\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)}_{=\operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right)+\operatorname{cont}\left(\operatorname{col}_j T\right)} = \underbrace{\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j+1} T\right)}_{=c} + \operatorname{cont}\left(\operatorname{col}_j T\right) \\ &= c + \operatorname{cont}\left(\operatorname{col}_j T\right). \end{aligned} \tag{278}$$

Now, recall that the tableau T is semistandard; thus, its entries increase strictly down each column. Hence, in particular, the entries of the j-th column of T increase strictly down this column. Therefore, any given number $i \in [N]$ appears at most once in this column. In other words, any given number $i \in [N]$ appears at most once in $\operatorname{col}_j T$. In other words, $\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_i \leq 1$ for each $i \in [N]$ (because $\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_i$ counts how often i appears in $\operatorname{col}_j T$). Applying this inequality to $i = k+1$, we obtain $\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_{k+1} \leq 1$. Now, from (278), we obtain

$$b_{k+1} = \left(c + \operatorname{cont}\left(\operatorname{col}_j T\right)\right)_{k+1} = c_{k+1} + \underbrace{\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_{k+1}}_{\leq 1} \leq c_{k+1} + 1,$$

so that $b_k < b_{k+1} \leq c_{k+1} + 1$. Since b_k and $c_{k+1} + 1$ are integers, this entails $b_k \leq (c_{k+1} + 1) - 1 = c_{k+1}$. However, (278) also yields

$$b_k = \left(c + \operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k = c_k + \underbrace{\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k}_{\substack{\geq 0 \\ \text{(since } \left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k \text{ counts} \\ \text{how often } k \text{ appears in } \operatorname{col}_j T\text{)}}} \geq c_k,$$

so that $c_k \leq b_k \leq c_{k+1}$. Combining this with $c_k \geq c_{k+1}$, we obtain $c_k = c_{k+1}$. Hence, $c_{k+1} = c_k$. Now, combining $b_k \leq c_{k+1} = c_k$ with $c_k \leq b_k$, we obtain $b_k = c_k$. Comparing this with $b_k = c_k + \left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k$, we obtain $c_k + \left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k = c_k$, so that $\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k = 0$. In other words, the number k appears 0 times in $\operatorname{col}_j T$ (since $\left(\operatorname{cont}\left(\operatorname{col}_j T\right)\right)_k$ counts how often k appears in $\operatorname{col}_j T$). In other words, the number k does not appear in $\operatorname{col}_j T$. In other words, the number k does not appear in the j-th column of T.

Let us make one more simple observation, which we will not use until later: We have $b_k < b_{k+1}$, so that $b_k \leq b_{k+1} - 1$ (since b_k and b_{k+1} are integers). Thus, $b_k + 1 \leq b_{k+1}$. Combining this with $b_{k+1} \leq \underbrace{c_{k+1}}_{=c_k \leq b_k} + 1 \leq b_k + 1$, we obtain

$$b_k + 1 = b_{k+1}. \tag{279}$$

Now, let $\operatorname{col}_{<j} T$ be the restriction of T to columns $1, 2, \ldots, j-1$ (that is, the result of removing all but the first $j-1$ columns from T). Formally speaking, this means the restriction of the map T to the set $\{(u,v) \in Y(\lambda/\mu) \mid v < j\}$. This restriction $\operatorname{col}_{<j} T$ is a semistandard skew tableau of a certain (skew) shape; thus, we can apply the Bender–Knuth involution β_k (from our above proof of Theorem 7.3.21) to this tableau $\operatorname{col}_{<j} T$ instead of T. Let T^* be the tableau obtained from T by applying β_k **only to the columns** $1, 2, \ldots, j-1$ of T (that is, replacing $\operatorname{col}_{<j} T$ by $\beta_k(\operatorname{col}_{<j} T)$), while leaving the columns $j, j+1, j+2, \ldots$ unchanged. Thus, formally, T^* is the tableau of shape $Y(\lambda/\mu)$ defined by

$$\operatorname{col}_{<j}(T^*) = \beta_k(\operatorname{col}_{<j} T) \qquad \text{and} \tag{280}$$

$$\operatorname{col}_{\geq j}(T^*) = \operatorname{col}_{\geq j} T \tag{281}$$

(where $\operatorname{col}_{<j}(T^*)$ is defined just as $\operatorname{col}_{<j} T$ was defined, except that we are using T^* instead of T).

Example 7.3.41. Let N, v, λ, μ and T be as in Example 7.3.40. Let us now compute T^*. As we know, $j = 5$ and $k = 2$. Thus, in order to obtain T^*, we need to apply the Bender–Knuth involution $\beta_k = \beta_2$ **only to the columns** $1, 2, \ldots, j-1$ of T (that is, only to the first $j-1 = 4$ columns of T), while leaving the columns $5, 6, 7, \ldots$ unchanged. Here is how this looks like:

$$T = \begin{array}{ccccccc} & & & & & & 2 \\ & & 1 & 1 & 2 & 2 & 3 \\ & & 2 & 2 & 3 & 4 & \\ 1 & 3 & 3 & 5 & 6 & & \\ 2 & 4 & 5 & 6 & & & \end{array} \qquad \Longrightarrow \qquad T^* = \begin{array}{ccccccc} & & & & & & 2 \\ & & 1 & 1 & 2 & 2 & 3 \\ & & 2 & 3 & 3 & 4 & \\ 1 & 2 & 3 & 5 & 6 & & \\ 3 & 4 & 5 & 6 & & & \end{array}$$

(where we have grayed out all boxes in columns $5, 6, 7, \ldots$, because the entries in these boxes stay unchanged and are ignored by the Bender–Knuth involution).

We shall now show that $T^* \in \mathcal{X}$. Indeed, let us first check that the tableau T^* is semistandard. We know that the tableau T is semistandard, so that its restrictions $\operatorname{col}_{<j} T$ and $\operatorname{col}_{\geq j} T$ are semistandard; thus, $\beta_k(\operatorname{col}_{<j} T)$ is semistandard as well (since the Bender–Knuth involution β_k sends semistandard tableaux to semistandard tableaux). Now, recall that the tableau T^* is obtained from T by applying β_k to columns $1, 2, \ldots, j-1$ only; thus, T^* is obtained by glueing the tableaux $\beta_k(\operatorname{col}_{<j} T)$ and $\operatorname{col}_{\geq j} T$ together (along a vertical line). Hence:

- Each column of T^* is either a column of $\beta_k(\operatorname{col}_{<j} T)$ or a column of $\operatorname{col}_{\geq j} T$ (depending on whether it is one of columns $1, 2, \ldots, j-1$ or one of columns $j, j+1, j+2, \ldots$). In either case, the entries of this column increase strictly down this column (because the tableaux $\beta_k(\operatorname{col}_{<j} T)$ and

$\operatorname{col}_{\geq j} T$ are semistandard). Thus, we have shown that the entries of T^* increase strictly down each column.

- It is not hard to see that the entries of T^* increase weakly along each row[143].

[143] *Proof.* Let $i \in [N]$. We must prove that the entries of T^* increase weakly along the i-th row of T^*. Assume the contrary. Thus, there exist two adjacent entries in the i-th row of T^* that are out of order (in the sense that the one lying further left is larger than the one lying further right). In other words, there exists some positive integer u such that $(i, u) \in Y(\lambda / \mu)$ and $(i, u+1) \in Y(\lambda / \mu)$ and $T^*(i, u) > T^*(i, u+1)$. Consider this u.

Recall that T^* is obtained by glueing the tableaux $\beta_k\left(\operatorname{col}_{<j} T\right)$ and $\operatorname{col}_{\geq j} T$ together (along a vertical line). Thus, the i-th row of T^* is obtained by glueing the i-th row of $\beta_k\left(\operatorname{col}_{<j} T\right)$ together with the i-th row of $\operatorname{col}_{\geq j} T$. In other words, this row consists of two blocks, looking as follows:

i-th row of $\beta_k\left(\operatorname{col}_{<j} T\right)$	i-th row of $\operatorname{col}_{\geq j} T$

.

We shall refer to these two blocks as the *left block* and the *right block* (so the left block is the i-th row of $\beta_k\left(\operatorname{col}_{<j} T\right)$, whereas the right block is the i-th row of $\operatorname{col}_{\geq j} T$). The boundary between the two blocks falls between the $(j-1)$-st and j-th columns; the left block covers columns $1, 2, \ldots, j-1$, while the right block covers columns $j, j+1, j+2, \ldots$.

The entries of the left block increase weakly from left to right (since this left block is a row of the tableau $\beta_k\left(\operatorname{col}_{<j} T\right)$, which is semistandard). Thus, if both boxes (i, u) and $(i, u+1)$ belonged to the left block, then we would have $T^*(i, u) \leq T^*(i, u+1)$, which would contradict $T^*(i, u) > T^*(i, u+1)$. Hence, it is impossible for both boxes (i, u) and $(i, u+1)$ to belong to the left block; thus, at least one of these boxes must belong to the right block. Therefore, $(i, u+1)$ belongs to the right block (since the right block is further right than the left block).

The entries of the right block also increase weakly from left to right (since this right block is a row of the tableau $\operatorname{col}_{\geq j} T$, which is semistandard). Thus, if both boxes (i, u) and $(i, u+1)$ belonged to the right block, then we would have $T^*(i, u) \leq T^*(i, u+1)$, which would contradict $T^*(i, u) > T^*(i, u+1)$. Hence, it is impossible for both boxes (i, u) and $(i, u+1)$ to belong to the right block; thus, at least one of these boxes must belong to the left block. Therefore, (i, u) belongs to the left block (since $(i, u+1)$ belongs to the right block).

Thus, the boxes (i, u) and $(i, u+1)$ straddle the boundary between the left block and the right block. Since this boundary falls between the $(j-1)$-st and j-th columns, this entails that the box (i, u) lies on the $(j-1)$-st column, while the box $(i, u+1)$ lies on the j-th column. In other words, $u = j-1$ and $u+1 = j$. Thus, the inequality $T^*(i, u) > T^*(i, u+1)$ can be rewritten as $T^*(i, j-1) > T^*(i, j)$. Moreover, from $u = j-1$, we obtain $j-1 = u$ and thus $(i, j-1) = (i, u) \in Y(\lambda / \mu)$. Furthermore, from $u+1 = j$, we obtain $j = u+1$ and thus $(i, j) = (i, u+1) \in Y(\lambda / \mu)$.

The equality (281) shows that the entries of T^* in columns $j, j+1, j+2, \ldots$ equal the corresponding entries of T. Thus, in particular, we have $T^*(i, j) = T(i, j)$ (since the box (i, j) lies in column j). Thus, $T^*(i, j-1) > T^*(i, j) = T(i, j)$.

On the other hand, the tableau T is semistandard, so that its entries increase weakly along each row. Hence, $T(i, j-1) \leq T(i, j)$. Therefore, $T(i, j) \geq T(i, j-1)$, so that $T^*(i, j-1) > T(i, j) \geq T(i, j-1)$.

We know that the number k does not appear in the j-th column of T; thus, $T(i, j) \neq k$ (since $T(i, j)$ is an entry in the j-th column of T).

We recall a simple property of the Bender-Knuth involution β_k (which follows directly from the construction of β_k): When we apply β_k to a semistandard tableau, Combining these two conclusions, we conclude that T^* is a semistandard tableau. In other words, $T^* \in \operatorname{SSYT}(\lambda / \mu)$.

Recall that $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ is not an N-partition. In view of (281), this rewrites as follows: $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j}(T^*)\right)$ is not an N-partition. Hence, the tableau T^* is not ν-Yamanouchi. Thus, $T^* \in \mathcal{X}$ (by the definition of $\mathcal{X}$, since $T^* \in \operatorname{SSYT}(\lambda / \mu)$).

Forget that we fixed T. Thus, for each tableau $T \in \mathcal{X}$, we have constructed a tableau $T^* \in \mathcal{X}$. Let $f : \mathcal{X} \to \mathcal{X}$ be the map that sends each $T \in \mathcal{X}$ to T^*. We shall now show that f is a sign-reversing involution. First, we shall show the following:

> *Observation 1:* The map f is an involution.

[*Proof of Observation 1:* We must show that $f \circ f = \operatorname{id}$. In other words, we must prove that $f(f(T)) = T$ for each $T \in \mathcal{X}$.

Let $T \in \mathcal{X}$. Then, the definition of f yields $f(T) = T^*$ and $f(T^*) = (T^*)^*$. Recall how T^* is constructed from T:

- We let j be the **largest** violator of T. This is the largest $j \geq 1$ such that $\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$ is not an N-partition.
- We let k be the **smallest** misstep of T. This is the smallest $k \in [N-1]$ such that $\left(\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)\right)_k < \left(\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)\right)_{k+1}$. [144]

- some k's get replaced by $(k+1)$'s,
- some $(k+1)$'s get replaced by k's, and
- all other entries remain unchanged.

Thus, in particular, when we apply β_k to a semistandard tableau, the only entries that can get replaced by larger entries are k's, and in that case they can only be replaced by $(k+1)$'s. In other words, if some entry of a semistandard tableau gets replaced by a larger entry when we apply β_k to the tableau, then this entry must have been k before applying β_k, and must get replaced by $k+1$ when β_k is applied.

Since T^* is obtained from T by applying β_k to columns $1, 2, \ldots, j-1$ (while all other columns remain unchanged), we thus conclude that if some entry of T gets replaced by a larger entry when we pass from T to T^*, then this entry must have been k in T, and must get replaced by $k+1$ in T^*. Let us restate this in a more formal language: If $(p,q) \in Y(\lambda/\mu)$ satisfies $T^*(p,q) > T(p,q)$, then

$$T(p,q) = k \qquad \text{and} \qquad T^*(p,q) = k+1.$$

We can apply this to $(p,q) = (i, j-1)$ (since $T^*(i,j-1) > T(i,j-1)$), and thus conclude that $T(i,j-1) = k$ and $T^*(i,j-1) = k+1$.

Now, from $T(i,j-1) = k$, we obtain $k = T(i,j-1) \leq T(i,j)$. On the other hand, $T^*(i,j-1) > T(i,j)$, so that $T(i,j) < T^*(i,j-1) = k+1$. Since $T(i,j)$ and $k+1$ are integers, this entails $T(i,j) \leq (k+1) - 1 = k$. Combining this with $k \leq T(i,j)$, we obtain $T(i,j) = k$. This contradicts $T(i,j) \neq k$. This contradiction shows that our assumption was wrong. Hence, we have shown that the entries of T^* increase weakly along the i-th row of T^*. Qed.

[144] Indeed, a misstep of T was defined to be a $k \in [N-1]$ such that $b_k < b_{k+1}$, where

- We apply the Bender–Knuth involution β_k **only to the columns** $1, 2, \ldots, j-1$ of T, while leaving the columns $j, j+1, j+2, \ldots$ unchanged. The result is T^*.

The construction of $(T^*)^*$ from T^* proceeds similarly:

- We let j' be the **largest** violator of T^*.
- We let k' be the **smallest** misstep of T^*.
- We apply the Bender–Knuth involution β_k **only to the columns** $1, 2, \ldots, j'-1$ of T^*, while leaving the columns $j', j'+1, j'+2, \ldots$ unchanged. The result is $(T^*)^*$.

We claim that this construction undoes the previous construction and recovers T (so that $(T^*)^* = T$). To see this, we argue as follows:

- We know that $\operatorname{col}_{\geq j}(T^*) = \operatorname{col}_{\geq j} T$, so that j is the largest violator of T^* (since j is the largest violator of T) [145]. Therefore, $j' = j$.
- Knowing that $j' = j$ and $\operatorname{col}_{\geq j}(T^*) = \operatorname{col}_{\geq j} T$, we now conclude that k is the smallest misstep of T^* (since k is the smallest misstep of T). Therefore, $k' = k$.
- Knowing that $j' = j$ and $k' = k$, we conclude that $(T^*)^*$ is obtained from T^* by the exact same operation that we used to obtain T^* from T: namely, by applying the Bender–Knuth involution β_k only to the columns $1, 2, \ldots, j-1$ (while leaving the columns $j, j+1, j+2, \ldots$ unchanged). However, this operation undoes itself when applied a second time, because the Bender–Knuth involution β_k is an involution[146]. Thus, we conclude that $(T^*)^* = T$.

$b = \nu + \operatorname{cont}(\operatorname{col}_{\geq j} T)$. In other words, a misstep of T means a $k \in [N-1]$ such that $(\nu + \operatorname{cont}(\operatorname{col}_{\geq j} T))_k < (\nu + \operatorname{cont}(\operatorname{col}_{\geq j} T))_{k+1}$.

[145] Here is the argument in some more detail:

We have

$$\operatorname{col}_{\geq j}(T^*) = \operatorname{col}_{\geq j} T, \tag{282}$$

and therefore we also have

$$\operatorname{col}_{\geq p}(T^*) = \operatorname{col}_{\geq p} T \qquad \text{for any integer } p > j \tag{283}$$

(since the tableau $\operatorname{col}_{\geq p} T$ is obtained by removing some columns from $\operatorname{col}_{\geq j} T$, whereas the tableau $\operatorname{col}_{\geq p}(T^*)$ is obtained in the same fashion from $\operatorname{col}_{\geq j}(T^*)$).

We know that j is the largest violator of T. In other words, the N-tuple $\nu + \operatorname{cont}(\operatorname{col}_{\geq j} T)$ is not an N-partition, but $\nu + \operatorname{cont}(\operatorname{col}_{\geq p} T)$ is an N-partition for any integer $p > j$. In view of (282) and (283), we can rewrite this as follows: The N-tuple $\nu + \operatorname{cont}(\operatorname{col}_{\geq j}(T^*))$ is not an N-partition, but $\nu + \operatorname{cont}(\operatorname{col}_{\geq p}(T^*))$ is an N-partition for any integer $p > j$. In other words, j is the largest violator of T^*.

[146] This has been shown during our proof of Theorem 7.3.21.

Thus, $f\left(\underbrace{f\left(T\right)}_{=T^*}\right) = f\left(T^*\right) = \left(T^*\right)^* = T$.

Forget that we fixed T. We thus have proved that $f\left(f\left(T\right)\right) = T$ for each $T \in \mathcal{X}$. As explained, this completes the proof of Observation 1.]

Next, we shall show two observations about the effect of the map f on the sign of a tableau:

Observation 2: We have $\operatorname{sign}\left(f\left(T\right)\right) = -\operatorname{sign} T$ for all $T \in \mathcal{X}$.

[*Proof of Observation 2:* Let $T \in \mathcal{X}$. We must show that $\operatorname{sign}\left(f\left(T\right)\right) = -\operatorname{sign} T$.

Define two N-tuples $\alpha \in \mathbb{N}^N$ and $\gamma \in \mathbb{N}^N$ by $\alpha := \nu + \operatorname{cont} T + \rho$ and $\gamma := \nu + \operatorname{cont}\left(T^*\right) + \rho$. Then, $f\left(T\right) = T^*$ (by the definition of f), and thus

$$\begin{aligned}\operatorname{sign}\left(f\left(T\right)\right) = \operatorname{sign}\left(T^*\right) &= a_{\nu+\operatorname{cont}(T^*)+\rho} && \left(\text{by the definition of } \operatorname{sign}\left(T^*\right)\right)\\ &= a_\gamma && \left(\text{since } \nu + \operatorname{cont}\left(T^*\right) + \rho = \gamma\right).\end{aligned}$$

Also, the definition of $\operatorname{sign} T$ yields

$$\operatorname{sign} T = a_{\nu+\operatorname{cont} T+\rho} = a_\alpha \qquad \left(\text{since } \nu + \operatorname{cont} T + \rho = \alpha\right).$$

Now, we are going to show that the N-tuple γ is obtained from α by swapping two entries. Once this is shown, we will easily conclude $\operatorname{sign}\left(f\left(T\right)\right) = -\operatorname{sign} T$ by applying Lemma 7.3.39 **(b)**.

We recall the notations from the construction of T^*: Let j be the largest violator of T. Let k be the smallest misstep of T. Define an N-tuple $b \in \mathbb{N}^N$ by $b := \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)$. Then, $b_k + 1 = b_{k+1}$ (as we have proved in (279)). However,

$$\begin{aligned}b_k &= \left(\nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)\right)_k && \left(\text{since } b = \nu + \operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)\right)\\ &= \nu_k + \underbrace{\left(\operatorname{cont}\left(\operatorname{col}_{\geq j} T\right)\right)_k}_{\substack{=\left(\#\text{ of } k\text{'s in } \operatorname{col}_{\geq j} T\right)\\ \text{(by Definition 7.3.26)}}}\\ &= \nu_k + \left(\#\text{ of } k\text{'s in } \operatorname{col}_{\geq j} T\right). && (284)\end{aligned}$$

The same argument (applied to $k+1$ instead of k) yields

$$b_{k+1} = \nu_{k+1} + \left(\#\text{ of } \left(k+1\right)\text{'s in } \operatorname{col}_{\geq j} T\right). \qquad (285)$$

We shall now show that $\gamma_k = \alpha_{k+1}$. Indeed, the vertical line that separates the $(j-1)$-st and j-th columns cuts the tableau T into its two parts $\operatorname{col}_{<j} T$ and $\operatorname{col}_{\geq j} T$. Thus, every $i \in [N]$ satisfies

$$\begin{aligned}&\left(\#\text{ of } i\text{'s in } T\right)\\ &= \left(\#\text{ of } i\text{'s in } \operatorname{col}_{<j} T\right) + \left(\#\text{ of } i\text{'s in } \operatorname{col}_{\geq j} T\right). && (286)\end{aligned}$$

The same argument (applied to T^* instead of T) shows that every $i \in [N]$ satisfies

$$\begin{aligned}&(\text{# of } i\text{'s in } T^*)\\ &= (\text{# of } i\text{'s in } \operatorname{col}_{<j}(T^*)) + (\text{# of } i\text{'s in } \operatorname{col}_{\geq j}(T^*)).\end{aligned} \tag{287}$$

Now, the definition of $\operatorname{cont}(T^*)$ yields

$$\begin{aligned}(\operatorname{cont}(T^*))_k &= (\text{# of } k\text{'s in } T^*)\\ &= \left(\text{# of } k\text{'s in } \underbrace{\operatorname{col}_{<j}(T^*)}_{\substack{=\beta_k(\operatorname{col}_{<j} T)\\ \text{(by (280))}}}\right) + \left(\text{# of } k\text{'s in } \underbrace{\operatorname{col}_{\geq j}(T^*)}_{\substack{=\operatorname{col}_{\geq j} T\\ \text{(by (281))}}}\right)\\ &\qquad \text{(by (287), applied to } i = k)\\ &= \underbrace{(\text{# of } k\text{'s in } \beta_k(\operatorname{col}_{<j} T))}_{\substack{=(\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T)\\ \text{(by (254),}\\ \text{applied to } \operatorname{col}_{<j} T \text{ instead of } T)}} + \underbrace{(\text{# of } k\text{'s in } \operatorname{col}_{\geq j} T)}_{\substack{=b_k-\nu_k\\ \text{(by (284))}}}\\ &= (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + \underbrace{b_k}_{\substack{=b_{k+1}-1\\ \text{(since } b_k+1=b_{k+1})}} - \nu_k\\ &= (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - 1 - \nu_k.\end{aligned}$$

However, $\gamma = \nu + \operatorname{cont}(T^*) + \rho$, so that

$$\begin{aligned}\gamma_k &= (\nu + \operatorname{cont}(T^*) + \rho)_k\\ &= \nu_k + \underbrace{(\operatorname{cont}(T^*))_k}_{=(\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T)+b_{k+1}-1-\nu_k} + \underbrace{\rho_k}_{\substack{=N-k\\ \text{(by the definition of } \rho)}}\\ &= \nu_k + (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - 1 - \nu_k + N - k\\ &= (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - 1 + N - k.\end{aligned} \tag{288}$$

On the other hand, the definition of $\operatorname{cont} T$ yields

$$\begin{aligned}(\operatorname{cont} T)_{k+1} &= (\text{# of } (k+1)\text{'s in } T)\\ &= (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + \underbrace{(\text{# of } (k+1)\text{'s in } \operatorname{col}_{\geq j} T)}_{\substack{=b_{k+1}-\nu_{k+1}\\ \text{(by (285))}}}\\ &\qquad \text{(by (286), applied to } i = k+1)\\ &= (\text{# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - \nu_{k+1}.\end{aligned}$$

However, $\alpha = \nu + \operatorname{cont} T + \rho$, so that

$$\begin{aligned}\alpha_{k+1} &= (\nu + \operatorname{cont} T + \rho)_{k+1} \\ &= \nu_{k+1} + \underbrace{(\operatorname{cont} T)_{k+1}}_{=(\text{\# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - \nu_{k+1}} + \underbrace{\rho_{k+1}}_{\substack{=N-(k+1) \\ \text{(by the definition of } \rho\text{)}}} \\ &= \nu_{k+1} + (\text{\# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - \nu_{k+1} + N - (k+1) \\ &= (\text{\# of } (k+1)\text{'s in } \operatorname{col}_{<j} T) + b_{k+1} - 1 + N - k.\end{aligned}$$

Comparing this with (288), we obtain

$$\gamma_k = \alpha_{k+1}. \qquad (289)$$

A similar argument (using (255) instead of (254)) can be used to show that

$$\gamma_{k+1} = \alpha_k. \qquad (290)$$

(See Section B.7 for the details of this argument.)

A further argument of this form (using (256) instead of (254)) can be used to show that

$$\gamma_i = \alpha_i \qquad \text{for each } i \in [N] \text{ satisfying } i \neq k \text{ and } i \neq k+1. \qquad (291)$$

(See Section B.7 for the details of this argument.)

Combining the three equalities (289), (290) and (291), we see that the N-tuple γ is obtained from α by swapping two entries (namely, the k-th and the $(k+1)$-st entry). Thus, Lemma 7.3.39 **(b)** (applied to γ instead of β) yields that $a_\gamma = -a_\alpha$. This rewrites as $\operatorname{sign}(f(T)) = -\operatorname{sign} T$ (since $\operatorname{sign}(f(T)) = a_\gamma$ and $\operatorname{sign} T = a_\alpha$). This proves Observation 2.]

Observation 3: We have $\operatorname{sign} T = 0$ for all $T \in \mathcal{X}$ satisfying $f(T) = T$.

[*Proof of Observation 3:* Let $T \in \mathcal{X}$ be such that $f(T) = T$.

We shall use all the notations that we have introduced in the proof of Observation 2 above. In particular, we define two N-tuples $\alpha \in \mathbb{N}^N$ and $\gamma \in \mathbb{N}^N$ by $\alpha := \nu + \operatorname{cont} T + \rho$ and $\gamma := \nu + \operatorname{cont}(T^*) + \rho$, and we let k be the smallest misstep of T.

The definition of f yields $f(T) = T^*$, so that $T^* = f(T) = T$. Thus,

$$\gamma = \nu + \underbrace{\operatorname{cont}(T^*)}_{=\operatorname{cont} T} + \rho = \nu + \operatorname{cont} T + \rho = \alpha.$$

Hence, $\gamma_k = \alpha_k$. However, the equality (289) (which we have shown in the proof of Observation 2) yields $\gamma_k = \alpha_{k+1}$. Comparing these two equalities, we obtain $\alpha_k = \alpha_{k+1}$. Therefore, the N-tuple $\alpha \in \mathbb{N}^N$ has two equal entries (namely, its k-th and its $(k+1)$-st entry). Thus, Lemma 7.3.39 **(a)** yields $a_\alpha = 0$.

However, the definition of $\operatorname{sign} T$ yields

$$\begin{aligned} \operatorname{sign} T &= a_{\nu+\operatorname{cont} T+\rho} = a_\alpha \qquad (\text{since } \nu + \operatorname{cont} T + \rho = \alpha) \\ &= 0. \end{aligned}$$

This proves Observation 3.]

Now, let us combine what we have shown. We know that the map $f : \mathcal{X} \to \mathcal{X}$ is an involution (by Observation 1). Moreover, we have

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I \qquad \text{for all } I \in \mathcal{X}$$

(by Observation 2, applied to $T = I$). Furthermore,

$$\operatorname{sign} I = 0 \qquad \text{for all } I \in \mathcal{X} \text{ satisfying } f(I) = I$$

(by Observation 3, applied to $T = I$). Therefore, Lemma 6.1.4 (applied to the additive abelian group $\mathcal{P}$) yields

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

Renaming the summation index I as T on both sides of this equality, we obtain

$$\sum_{T \in \mathcal{A}} \operatorname{sign} T = \sum_{T \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} T.$$

Hence, (277) rewrites as

$$\begin{aligned} a_{\nu+\rho} \cdot s_{\lambda/\mu} &= \sum_{T \in \mathcal{A} \setminus \mathcal{X}} \underbrace{\operatorname{sign} T}_{\substack{= a_{\nu+\operatorname{cont} T+\rho} \\ \text{(by the definition of } \operatorname{sign} T)}} = \sum_{T \in \mathcal{A} \setminus \mathcal{X}} a_{\nu+\operatorname{cont} T+\rho} \\ &= \sum_{\substack{T \text{ is a } \nu\text{-Yamanouchi} \\ \text{semistandard tableau} \\ \text{of shape } \lambda/\mu}} a_{\nu+\operatorname{cont} T+\rho} \end{aligned}$$

(since $\mathcal{A} \setminus \mathcal{X}$ is the set of all ν-Yamanouchi semistandard tableaux of shape λ/μ [147]). This proves Lemma 7.3.34. □

Remark 7.3.42. All the above properties of skew Schur polynomials $s_{\lambda/\mu}$ can be generalized further by taking an arbitrary $M \in \mathbb{N}$ and allowing λ and μ to be M-partitions (rather than N-partitions). Thus, the Young diagram $Y(\lambda/\mu)$ is now defined to be the set $\{(i,j) \mid i \in [M] \text{ and } j \in [\lambda_i] \setminus [\mu_i]\}$; in

[147] because

$$\mathcal{A} = \operatorname{SSYT}(\lambda/\mu) \qquad \text{and} \qquad \mathcal{X} = \{T \in \operatorname{SSYT}(\lambda/\mu) \mid T \text{ is not } \nu\text{-Yamanouchi}\}$$

particular, it may have more than N rows (if $M > N$). In this generalized setup, the tableaux of shape λ/μ are defined just as they were in Definition 7.3.15 (in particular, they may have more than N rows, but their entries still have to be elements of $[N]$); the same applies to the notions of semistandard tableaux and the skew Schur polynomials (which are still polynomials in $\mathcal{P} = K[x_1, x_2, \ldots, x_N]$). All of our above results (particularly, Theorem 7.3.21 and Theorem 7.3.32) still hold in this generalized setup (note that the ν in Theorem 7.3.32 must still be an N-partition, not an M-partition), and the proofs given above still work.

7.3.6. The Pieri rules

Having proved the Littlewood–Richardson rule, let us discuss a few more of its consequences. As we know from Example 7.3.10, the complete homogeneous symmetric polynomials h_n and the elementary symmetric polynomials e_n (for $n \in \{0, 1, \ldots, N\}$) are instances of Schur polynomials. Thus, by appropriately specializing Theorem 7.3.32, we can obtain rules for expressing products of the form $h_n s_\mu$ and $e_n s_\mu$ as sums of Schur polynomials. These rules are known as the *Pieri rules*. To formulate them, we need some more notations:

Definition 7.3.43. Let λ and μ be two N-partitions.

(a) We write λ/μ for the pair (μ, λ). Such a pair is called a *skew partition*.

(b) We say that λ/μ is a *horizontal strip* if we have $\mu \subseteq \lambda$ and the Young diagram $Y(\lambda/\mu)$ has no two boxes lying in the same column.

(c) We say that λ/μ is a *vertical strip* if we have $\mu \subseteq \lambda$ and the Young diagram $Y(\lambda/\mu)$ has no two boxes lying in the same row.

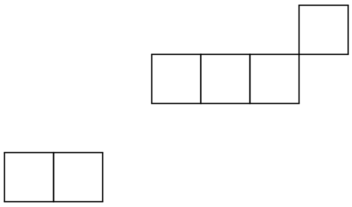
Now, let $n \in \mathbb{N}$.

(d) We say that λ/μ is a *horizontal n-strip* if λ/μ is a horizontal strip and satisfies $|Y(\lambda/\mu)| = n$.

(e) We say that λ/μ is a *vertical n-strip* if λ/μ is a vertical strip and satisfies $|Y(\lambda/\mu)| = n$.

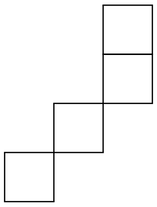
Example 7.3.44. Let $N = 4$.

(a) If $\lambda = (8,7,4,3)$ and $\mu = (7,4,4,1)$, then we have $\mu \subseteq \lambda$, and the Young diagram $Y(\lambda/\mu)$ looks as follows:

$Y(\lambda/\mu) =$  .

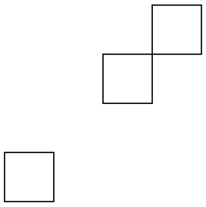
From this picture, it is clear that this skew partition λ/μ is a horizontal strip (and, in fact, a horizontal 6-strip, since $|Y(\lambda/\mu)| = 6$), but not a vertical strip (since, e.g., there are 3 boxes in the second row of $Y(\lambda/\mu)$).

(b) If $\lambda = (3,3,2,1)$ and $\mu = (2,2,1,0)$, then we have $\mu \subseteq \lambda$, and the Young diagram $Y(\lambda/\mu)$ looks as follows:

$Y(\lambda/\mu) =$  .

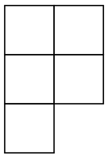
From this picture, it is clear that this skew partition λ/μ is a vertical strip (and, in fact, a vertical 4-strip, since $|Y(\lambda/\mu)| = 4$), but not a horizontal strip (since there are 2 boxes in the third column of $Y(\lambda/\mu)$).

(c) If $\lambda = (4,3,1,1)$ and $\mu = (3,2,1,0)$, then we have $\mu \subseteq \lambda$, and the Young diagram $Y(\lambda/\mu)$ looks as follows:

$Y(\lambda/\mu) =$  .

From this picture, it is clear that this skew partition λ/μ is both a horizontal strip (and, in fact, a horizontal 3-strip) and a vertical strip (and, in fact, a vertical 3-strip).

(d) If $\lambda = (3,3,2,1)$ and $\mu = (1,1,1,1)$, then we have $\mu \subseteq \lambda$, and the Young diagram $Y(\lambda/\mu)$ looks as follows:

$Y(\lambda/\mu) =$  .

From this picture, it is clear that this skew partition λ/μ is neither a horizontal strip nor a vertical strip.

Horizontal and vertical strips can also be characterized in terms of the entries of the partitions:

Proposition 7.3.45. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$ be two N-partitions.

(a) The skew partition λ / μ is a horizontal strip if and only if we have

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \mu_2 \geq \cdots \geq \lambda_N \geq \mu_N.$$

(b) The skew partition λ / μ is a vertical strip if and only if we have

$$\mu_i \leq \lambda_i \leq \mu_i + 1 \qquad \text{for each } i \in [N].$$

Proof. See Exercise A.6.3.7. □

We can now state the *Pieri rules*:

Theorem 7.3.46 (Pieri rules)**.** Let $n \in \mathbb{N}$. Let μ be an N-partition. Then:

(a) We have

$$h_n s_\mu = \sum_{\substack{\lambda \text{ is an } N\text{-partition;} \\ \lambda/\mu \text{ is a horizontal } n\text{-strip}}} s_\lambda.$$

(b) We have

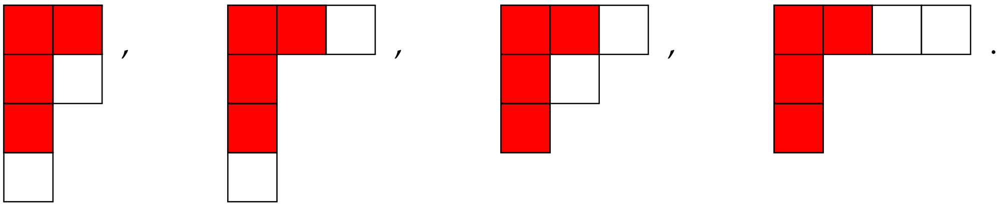
$$e_n s_\mu = \sum_{\substack{\lambda \text{ is an } N\text{-partition;} \\ \lambda/\mu \text{ is a vertical } n\text{-strip}}} s_\lambda.$$

Example 7.3.47. Let $N = 4$ and $\mu = (2, 1, 1, 0)$. Then:

(a) Theorem 7.3.46 **(a)** (applied to $n = 2$) yields

$$h_2 s_\mu = \sum_{\substack{\lambda \text{ is an } N\text{-partition;} \\ \lambda/\mu \text{ is a horizontal 2-strip}}} s_\lambda = s_{(2,2,1,1)} + s_{(3,1,1,1)} + s_{(3,2,1,0)} + s_{(4,1,1,0)},$$

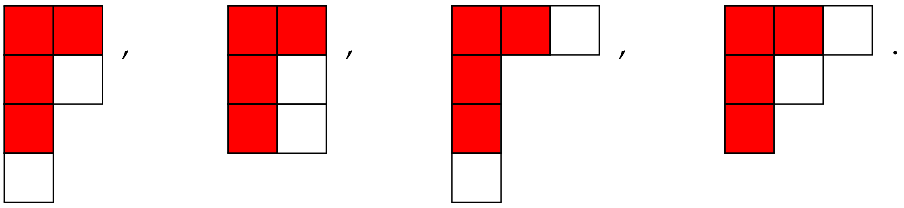
since the N-partitions λ for which λ / μ is a horizontal 2-strip are precisely the four N-partitions $(2, 2, 1, 1)$, $(3, 1, 1, 1)$, $(3, 2, 1, 0)$ and $(4, 1, 1, 0)$. Here are the Young diagrams $Y(\lambda)$ of these four N-partitions λ (with the $Y(\mu)$ subdiagram colored red each time):



(b) Theorem 7.3.46 **(b)** (applied to $n = 2$) yields

$$e_2 s_\mu = \sum_{\substack{\lambda \text{ is an } N\text{-partition;} \\ \lambda/\mu \text{ is a vertical 2-strip}}} s_\lambda = s_{(2,2,1,1)} + s_{(2,2,2,0)} + s_{(3,1,1,1)} + s_{(3,2,1,0)},$$

since the N-partitions λ for which λ/μ is a vertical 2-strip are precisely the four N-partitions $(2,2,1,1)$, $(2,2,2,0)$, $(3,1,1,1)$ and $(3,2,1,0)$. Here are the Young diagrams $Y(\lambda)$ of these four N-partitions λ (with the $Y(\mu)$ subdiagram colored red each time):



Proof of Theorem 7.3.46. See Exercise A.6.3.8. □

7.3.7. The Jacobi–Trudi identities

The *Jacobi–Trudi identities* are determinantal formulas expressing a skew Schur polynomial $s_{\lambda/\mu}$ in terms of complete homogeneous symmetric polynomials h_n or elementary symmetric polynomials e_n. We begin with the former:

Theorem 7.3.48 (First Jacobi–Trudi formula)**.** Let $M \in \mathbb{N}$. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_M)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_M)$ be two M-partitions (i.e., weakly decreasing M-tuples of nonnegative integers). Then,

$$s_{\lambda/\mu} = \det\left(\left(h_{\lambda_i-\mu_j-i+j}\right)_{1\leq i\leq M,\ 1\leq j\leq M}\right).$$

(Here, $s_{\lambda/\mu}$ is defined as in Definition 7.3.19, where the semistandard tableaux of shape λ/μ are defined as certain fillings of $Y(\lambda/\mu) := \{(i,j) \mid i \in [M] \text{ and } j \in [\lambda_i] \setminus [\mu_i]\}$, but their entries are still supposed to be elements of $[N]$. Compare with Remark 7.3.42.)

Example 7.3.49. If $M = 3$, then Theorem 7.3.48 says that

$$s_{\lambda/\mu} = \det\left(\left(h_{\lambda_i-\mu_j-i+j}\right)_{1\leq i\leq 3,\ 1\leq j\leq 3}\right) = \det\begin{pmatrix} h_{\lambda_1-\mu_1} & h_{\lambda_1-\mu_2+1} & h_{\lambda_1-\mu_3+2} \\ h_{\lambda_2-\mu_1-1} & h_{\lambda_2-\mu_2} & h_{\lambda_2-\mu_3+1} \\ h_{\lambda_3-\mu_1-2} & h_{\lambda_3-\mu_2-1} & h_{\lambda_3-\mu_3} \end{pmatrix}.$$

For instance, if $\lambda = (4,2,1)$ and $\mu = (1,0,0)$, then

$$\begin{aligned} s_{\lambda/\mu} &= \det\begin{pmatrix} h_{4-1} & h_{4-0+1} & h_{4-0+2} \\ h_{2-1-1} & h_{2-0} & h_{2-0+1} \\ h_{1-1-2} & h_{1-0-1} & h_{1-0} \end{pmatrix} = \det\begin{pmatrix} h_3 & h_5 & h_6 \\ h_0 & h_2 & h_3 \\ h_{-2} & h_0 & h_1 \end{pmatrix} \\ &= \det\begin{pmatrix} h_3 & h_5 & h_6 \\ 1 & h_2 & h_3 \\ 0 & 1 & h_1 \end{pmatrix} \qquad (\text{since } h_0 = 1 \text{ and } h_{-2} = 0). \end{aligned}$$

The proof of Theorem 7.3.48 is not too hard using what we have learnt about lattice paths in Subsection 6.5.1. Here is an outline (with some details left to exercises):

Proof of Theorem 7.3.48 (sketched). Let us follow Convention 6.5.1, Definition 6.5.2 and Definition 6.5.5. We will work with the digraph $\mathbb{Z}^2$. For each arc a of the digraph $\mathbb{Z}^2$, we define an element $w(a) \in \mathcal{P}$ (called the *weight* of a) as follows:

- If a is an east-step $(i, j) \rightarrow (i+1, j)$ with $j \in [N]$, then we set $w(a) := x_j$.
- If a is any other arc, then we set $w(a) := 1$.

For each path p of $\mathbb{Z}^2$, define the *weight* $w(p)$ of p by

$$w(p) := \prod_{a \text{ is an arc of } p} w(a).$$

Now, it is not hard to see the following (compare with Proposition 6.5.4):

Observation 1: Let a and c be two integers. Then,

$$\sum_{\substack{p \text{ is a path} \\ \text{from } (a,1) \text{ to } (c,N)}} w(p) = h_{c-a}.$$

See Exercise A.6.3.9 **(a)** for a proof of Observation 1.

Next, for each path tuple $\mathbf{p} = (p_1, p_2, \ldots, p_k)$, let us define the *weight* $w(\mathbf{p})$ of $\mathbf{p}$ by

$$w(\mathbf{p}) := w(p_1) w(p_2) \cdots w(p_k).$$

Set $k := M$ (for the sake of convenience). Thus, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_k)$.

Define two k-vertices $\mathbf{A} = (A_1, A_2, \ldots, A_k)$ and $\mathbf{B} = (B_1, B_2, \ldots, B_k)$ by setting

$$A_i := (\mu_i - i,\ 1) \qquad \text{and} \qquad B_i := (\lambda_i - i,\ N) \qquad \text{for each } i \in [k].$$

It is easy to see that the conditions (239), (240), (241) and (242) of Corollary 6.5.15 are satisfied. Hence, (243) yields

$$\begin{aligned} &\det\left(\left(\sum_{p: A_i \rightarrow B_j} w(p)\right)_{1 \leq i \leq k,\ 1 \leq j \leq k}\right) \\ &= \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \mathbf{B}}} w(\mathbf{p}), \end{aligned} \tag{292}$$

where "$p : A_i \to B_j$" means "p is a path from A_i to B_j". The left hand side of this equality is

$$\begin{aligned}
&\det\left(\left(\sum_{p:A_i\to B_j} w\left(p\right)\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right)\\
&=\det\left(\left(h_{(\lambda_j-j)-(\mu_i-i)}\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right) \qquad \text{(by Observation 1)}\\
&=\det\left(\left(h_{(\lambda_i-i)-(\mu_j-j)}\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right) \qquad \text{(by Theorem 6.4.10)}\\
&=\det\left(\left(h_{\lambda_i-\mu_j-i+j}\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right)\\
&=\det\left(\left(h_{\lambda_i-\mu_j-i+j}\right)_{1\leq i\leq M,\ 1\leq j\leq M}\right) \qquad (293)
\end{aligned}$$

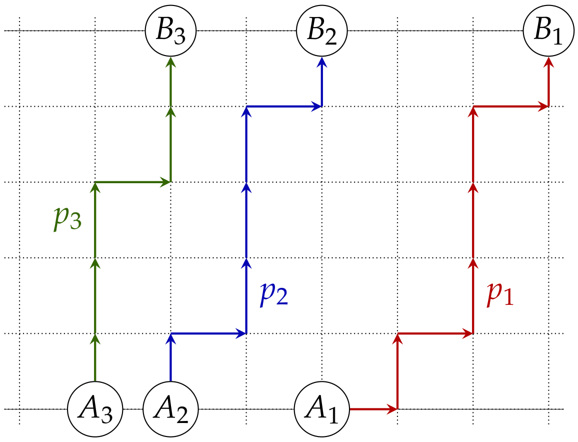
(since $k = M$). We shall now analyze the right hand side of (292). To that purpose, we need to understand the nipats from **A** to **B**.

We define the *height* of an east-step $(i, j) \to (i+1, j)$ to be the number j. We define the *height sequence* of a path p to be the sequence of the heights of the east-steps of p (going from the starting point to the ending point of p). For example, the path shown in Example 6.5.3 has height sequence $(1, 1, 1, 2, 3)$. It is clear that the height sequence of a path is always weakly increasing.

If $\mathbf{p} = (p_1, p_2, \ldots, p_k)$ is a nipat from **A** to **B**, we let $T(\mathbf{p})$ be the tableau of shape $Y(\lambda/\mu)$ such that the entries in the i-th row of $T(\mathbf{p})$ (for each $i \in [k]$) are the entries of the height sequence of p_i.

Example 7.3.50. Let $N = 6$ and $M = 3$ (so that $k = M = 3$) and $\lambda = (4, 2, 1)$ and $\mu = (1, 0, 0)$. Here is a nipat $\mathbf{p}$ from **A** to **B**, and the corresponding tableau $T(\mathbf{p})$:

$\mathbf{p} =$



$$\Longrightarrow \quad T(\mathbf{p}) = \begin{ytableau} \none & 1 & 2 & 5 \\ 2 & 5 \\ 4 \end{ytableau} .$$

We could have defined the tableau $T(\mathbf{p})$ just as easily for any path tuple $\mathbf{p}$

from $\mathbf{A}$ to $\mathbf{B}$ (not just for a nipat); however, the case of a nipat is particularly useful, because it turns out that the tableau $T(\mathbf{p})$ is semistandard if and only if $\mathbf{p}$ is a nipat. Moreover, the following stronger statement holds:

Observation 2: There is a bijection

$$\begin{aligned}\{\text{nipats from } \mathbf{A} \text{ to } \mathbf{B}\} &\to \operatorname{SSYT}(\lambda/\mu), \\ \mathbf{p} &\mapsto T(\mathbf{p}).\end{aligned}$$

See Exercise A.6.3.9 **(b)** for a proof of Observation 2.

It is easy to see that $w(\mathbf{p}) = x_{T(\mathbf{p})}$ for any nipat $\mathbf{p}$ from $\mathbf{A}$ to $\mathbf{B}$. Hence,

$$\begin{aligned}\sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \mathbf{B}}} \underbrace{w(\mathbf{p})}_{=x_{T(\mathbf{p})}} &= \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \mathbf{B}}} x_{T(\mathbf{p})} = \sum_{T \in \operatorname{SSYT}(\lambda/\mu)} x_T \\ &\qquad \left(\begin{array}{c}\text{here, we have substituted } T \text{ for } T(\mathbf{p}) \\ \text{in the sum, since the map in} \\ \text{Observation 2 is a bijection}\end{array}\right) \\ &= s_{\lambda/\mu} \qquad \left(\text{since } s_{\lambda/\mu} \text{ is defined to be } \sum_{T \in \operatorname{SSYT}(\lambda/\mu)} x_T\right).\end{aligned}$$

Thus,

$$\begin{aligned}s_{\lambda/\mu} &= \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \mathbf{B}}} w(\mathbf{p}) = \det\left(\left(\sum_{p: A_i \to B_j} w(p)\right)_{1 \le i \le k,\ 1 \le j \le k}\right) \qquad (\text{by } (292)) \\ &= \det\left(\left(h_{\lambda_i - \mu_j - i + j}\right)_{1 \le i \le M,\ 1 \le j \le M}\right) \qquad (\text{by } (293)).\end{aligned}$$

This proves Theorem 7.3.48. □

Our above proof of Theorem 7.3.48 is essentially taken from [Stanle01, First proof of Theorem 7.16.1]; other proofs can be found in [GriRei20, Exercise 2.7.13] (see also [GriRei20, paragraph after Theorem 2.4.6] for several references).

The *second Jacobi–Trudi formula* involves elementary symmetric polynomials e_n (instead of h_n) and transpose partitions (as in Exercise A.3.1.1):

Theorem 7.3.51 (Second Jacobi–Trudi formula)**.** Let λ and μ be two partitions. Let λ^t and μ^t be the transposes of λ and μ. Let $M \in \mathbb{N}$ be such that both λ^t and μ^t have length $\le M$. We extend the partitions λ^t and μ^t to M-tuples (by inserting zeroes at the end). Write these M-tuples λ^t and μ^t as $\lambda^t = \left(\lambda_1^t, \lambda_2^t, \ldots, \lambda_M^t\right)$ and $\mu = \left(\mu_1^t, \mu_2^t, \ldots, \mu_M^t\right)$. Then,

$$s_{\lambda/\mu} = \det\left(\left(e_{\lambda_i^t - \mu_j^t - i + j}\right)_{1 \le i \le M,\ 1 \le j \le M}\right).$$

Example 7.3.52. If $M = 3$, then Theorem 7.3.51 says that

$$s_{\lambda/\mu} = \det\left(\left(e_{\lambda_i^t - \mu_j^t - i + j}\right)_{1 \leq i \leq M,\ 1 \leq j \leq M}\right) = \det\begin{pmatrix} e_{\lambda_1^t - \mu_1^t} & e_{\lambda_1^t - \mu_2^t + 1} & e_{\lambda_1^t - \mu_3^t + 2} \\ e_{\lambda_2^t - \mu_1^t - 1} & e_{\lambda_2^t - \mu_2^t} & e_{\lambda_2^t - \mu_3^t + 1} \\ e_{\lambda_3^t - \mu_1^t - 2} & e_{\lambda_3^t - \mu_2^t - 1} & e_{\lambda_3^t - \mu_3^t} \end{pmatrix}.$$

For instance, if $\lambda = (3, 2, 2)$ and $\mu = (1, 1, 0)$, then $\lambda^t = (3, 3, 1)$ and $\mu^t = (2) = (2, 0, 0)$ (here, we have extended the partition μ^t to an M-tuple by inserting zeroes at the end), so that this becomes

$$\begin{aligned} s_{\lambda/\mu} &= \det\begin{pmatrix} e_{3-2} & e_{3-0+1} & e_{3-0+2} \\ e_{3-2-1} & e_{3-0} & e_{3-0+1} \\ e_{1-2-2} & e_{1-0-1} & e_{1-0} \end{pmatrix} = \det\begin{pmatrix} e_1 & e_4 & e_5 \\ e_0 & e_3 & e_4 \\ e_{-3} & e_0 & e_1 \end{pmatrix} \\ &= \det\begin{pmatrix} e_1 & e_4 & e_5 \\ 1 & e_3 & e_4 \\ 0 & 1 & e_1 \end{pmatrix} \qquad (\text{since } e_0 = 1 \text{ and } e_{-3} = 0). \end{aligned}$$

Proof of Theorem 7.3.51. See Exercise A.6.3.10. □

A. Homework exercises

What follows is a collection of problems (of varying difficulty) that are meant to illuminate, expand upon and otherwise complement the above text.

The numbers in the squares (like $\boxed{3}$) are the experience points you gain for solving the problems. They are a mix of difficulty rating and relevance score: The harder or more important the problem, the larger is the number in the square. I believe a $\boxed{5}$ represents a good graduate-level homework problem that requires thinking and work. A $\boxed{3}$ usually requires some thinking **or** work. A $\boxed{1}$ is a warm-up question. A $\boxed{7}$ should be somewhat too hard for regular homework. Anything above $\boxed{10}$ is not really meant as homework, but I'd be excited to hear your ideas. Multi-part exercises sometimes have points split between the parts – i.e., if parts **(b)** and **(c)** of an exercise are solved using the same idea, then they may both be assigned $\boxed{3}$ points even if each for itself would be a $\boxed{5}$.

In solving an exercise, you can freely use (without proof) the claims of all exercises above it.

Your goal (for an A grade in the 2022 iteration of Math 701) is to gain at least 20 experience points from each of the Chapters 3–7 (counting Chapter 2 as part of Chapter 3).

A.1. Before we start...

A.1.1. Binomial coefficients and elementary counting

Definition A.1.1. Let $x \in \mathbb{R}$. Then:

- We let $\lfloor x \rfloor$ denote the largest integer $\leq x$. This integer $\lfloor x \rfloor$ is called the *floor* of x, or the result of "*rounding down x*".
- We let $\lceil x \rceil$ denote the smallest integer $\geq x$. This integer $\lceil x \rceil$ is called the *ceiling* of x, or the result of "*rounding up x*".

Example A.1.2. We have

$$\lfloor 3 \rfloor = 3; \qquad \left\lfloor \sqrt{2} \right\rfloor = 1; \qquad \lfloor \pi \rfloor = 3; \qquad \lfloor -\pi \rfloor = -4;$$
$$\lceil 3 \rceil = 3; \qquad \left\lceil \sqrt{2} \right\rceil = 2; \qquad \lceil \pi \rceil = 4; \qquad \lceil -\pi \rceil = -3.$$

Let us note that each $x \in \mathbb{R}$ satisfies $\lfloor x \rfloor \leq x \leq \lceil x \rceil$.

Exercise A.1.1.1. $\boxed{3}$ Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} \binom{-2}{k} = (-1)^n \left\lfloor \frac{n+2}{2} \right\rfloor .$$

The next exercise is concerned with the notion of *lacunar sets*. This notion appears all over combinatorics (particularly in connection with Fibonacci numbers), so chances are we will meet it again.

Definition A.1.3. A set S of integers is said to be *lacunar* if it contains no two consecutive integers (i.e., there is no integer i such that both $i \in S$ and $i + 1 \in S$).

For example, the set $\{1,5,7\}$ is lacunar, but $\{1,5,6\}$ is not. Any 1-element subset of $\mathbb{Z}$ is lacunar, and so is the empty set.

Some people say "sparse" instead of "lacunar", but the word "sparse" also has other meanings.

Example A.1.4. The lacunar subsets of $\{1,2,3,4,5\}$ are

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{3\}, \quad \{4\}, \quad \{5\}, \quad \{1,3\},$$
$$\{1,4\}, \quad \{1,5\}, \quad \{2,4\}, \quad \{2,5\}, \quad \{3,5\}, \quad \{1,3,5\}.$$

Exercise A.1.1.2. Let $n \in \mathbb{N}$.

(a) $\boxed{1}$ Prove that the total # of lacunar subsets of $\{1,2,\ldots,n\}$ is the Fibonacci number f_{n+2}.

(b) $\boxed{1}$ Let $k \in \{0,1,\ldots,n+1\}$. Prove that the total # of k-element lacunar subsets of $\{1,2,\ldots,n\}$ equals $\dbinom{n+1-k}{k}$.

(c) $\boxed{1}$ What goes wrong with the claim of part **(b)** if $k > n+1$?

(d) $\boxed{1}$ Find the largest possible size of a lacunar subset of $\{1,2,\ldots,n\}$.

(e) $\boxed{1}$ Prove that $f_{n+1} = \sum\limits_{k=0}^{n} \dbinom{n-k}{k}$ for each $n \in \{-1,0,1,\ldots\}$.

Exercise A.1.1.3. Let n be a positive integer.

(a) $\boxed{2}$ Prove that

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \cdots = \sum_{k \in \mathbb{N}} \binom{n}{2k} = 2^{n-1}.$$

(b) $\boxed{3}$ Prove that

$$\binom{n}{0}+\binom{n}{4}+\binom{n}{8}+\binom{n}{12}+\cdots=\sum_{k\in\mathbb{N}}\binom{n}{4k}=2^{n-2}+2^{n/2-1}\cos\frac{\pi n}{4}.$$

[Hint: For part **(a)**, compute $(1+1)^n+(1-1)^n$. For part **(b)**, compute $(1+1)^n+(1+i)^n+(1-1)^n+(1-i)^n$, where $i=\sqrt{-1}\in\mathbb{C}$ is the imaginary unit.]

From now on, we shall use the so-called *Iverson bracket notation*:

Definition A.1.5. If $\mathcal{A}$ is any logical statement, then we define an integer $[\mathcal{A}]\in\{0,1\}$ by

$$[\mathcal{A}]=\begin{cases}1, & \text{if } \mathcal{A} \text{ is true;}\\ 0, & \text{if } \mathcal{A} \text{ is false.}\end{cases}$$

For example, $[1+1=2]=1$ (since $1+1=2$ is true), whereas $[1+1=1]=0$ (since $1+1=1$ is false).

If $\mathcal{A}$ is any logical statement, then the integer $[\mathcal{A}]$ is known as the *truth value* of $\mathcal{A}$.

Exercise A.1.1.4. (a) $\boxed{3}$ Prove that

$$\binom{n}{a}\binom{a}{b}=\binom{n}{b}\binom{n-b}{a-b}\qquad\text{for any } n,a,b\in\mathbb{C}.$$

(b) $\boxed{3}$ Let $N\in\mathbb{N}$.

For each $c\in\mathbb{C}$, let $L_c\in\mathbb{C}^{N\times N}$ be the $N\times N$-matrix whose rows are indexed $0,1,\ldots,N-1$ and whose columns are indexed $0,1,\ldots,N-1$, and whose (i,j)-th entry is $\binom{i}{j}c^{i-j}$ for each $i,j\in\{0,1,\ldots,N-1\}$. (The expression "$\binom{i}{j}c^{i-j}$" should be understood as 0 if $i<j$, even if c itself is 0.)

[For example, if $N=5$, then $L_c=\begin{pmatrix}1&0&0&0&0\\1c&1&0&0&0\\1c^2&2c&1&0&0\\1c^3&3c^2&3c&1&0\\1c^4&4c^3&6c^2&4c&1\end{pmatrix}$.]

Prove that

$$L_cL_d=L_{c+d}\qquad\text{for any } c,d\in\mathbb{C}.$$

(c) $\boxed{1}$ Prove that the matrices L_1 and L_{-1} are mutually inverse.

Exercise A.1.1.5. Let p be a prime number.

(a) $\boxed{2}$ Prove that $p \mid \dbinom{p}{k}$ for each $k \in \{1, 2, \ldots, p-1\}$.

(b) $\boxed{3}$ Let $a, b \in \mathbb{N}$. Prove that

$$\binom{ap}{bp} \equiv \binom{a}{b} \bmod p^2.$$

(c) $\boxed{3}$ Prove the claim of part **(b)** still holds if we replace "$a, b \in \mathbb{N}$" by "$a, b \in \mathbb{Z}$".

[**Hint:** The following suggests a combinatorial solution (algebraic solutions also exist).

Consider the cyclic group $C_p = \mathbb{Z}/p\mathbb{Z}$ with p elements.

For part **(a)**, let U be the set of all p-tuples of elements of $\{0, 1\}$ with the property that exactly k entries of the p-tuple are 1. The group C_p acts on U by cyclic rotation. Argue that each orbit of this action has size divisible by p.

For part **(b)**, let W be the set of all $p \times a$-matrices with entries in $\{0, 1\}$ and having the property that the sum of all entries of the matrix is bp (that is, exactly bp entries are 1). Construct an action of the group $C_p^a = \underbrace{C_p \times C_p \times \cdots \times C_p}_{a \text{ times}}$ on W in which the k-th C_p factor cyclically rotates the entries of the k-th row of the matrix. Argue that all but $\dbinom{a}{b}$ orbits of this action have size divisible by p^2, and conclude by writing $|W|$ as the sum of the sizes of the orbits.

For part **(c)**, fix $b \in \mathbb{N}$ and p (why is it enough to consider $b \in \mathbb{N}$?), and show that the remainders of $\dbinom{ap}{bp} - \dbinom{a}{b}$ modulo p^2 are periodic as a function in a.]

A.2. Generating functions

The notations of Chapter 3 shall be used here. In particular, we fix a commutative ring K.

A.2.1. Examples

All the properties of generating functions that have been used without proof in Section 3.1 can also be used in the following exercises.

Exercise A.2.1.1. $\boxed{2}$ The *Lucas sequence* is the sequence $(\ell_0, \ell_1, \ell_2, \ldots)$ of integers defined recursively by

$$\ell_0 = 2, \qquad \ell_1 = 1, \qquad \ell_n = \ell_{n-1} + \ell_{n-2} \text{ for each } n \geq 2.$$

(Thus, $\ell_2 = 3$ and $\ell_3 = 4$ and $\ell_5 = 7$ and so on.)

Find an explicit formula for ℓ_n analogous to Binet's formula for the Fibonacci numbers.

Exercise A.2.1.2. $\boxed{1}$ Prove that $\dfrac{1}{n+1}\dbinom{2n}{n} = \dbinom{2n}{n} - \dbinom{2n}{n-1}$ for any $n \in \mathbb{N}$.

Exercise A.2.1.3. $\boxed{3}$ Let q and d be any two real numbers. Let $(a_0, a_1, a_2, \ldots)$ be a sequence of real numbers such that each $n \geq 1$ satisfies $a_n = qa_{n-1} + d$. (This can be viewed as a common generalization of arithmetic and geometric sequences.)

Find an explicit formula for a_n in terms of q, d and a_0. (The formula may depend on whether q is 1 or not.)

Exercise A.2.1.4. $\boxed{5}$ Find and prove an explicit formula for the coefficient of x^n in the formal power series $\dfrac{1}{1 - x - x^2 + x^3}$.

Exercise A.2.1.5. Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$.

(a) $\boxed{2}$ Prove that

$$f_0 + f_2x + f_4x^2 + f_6x^3 + \cdots = \sum_{k \geq 0} f_{2k}x^k = \frac{x}{x^2 - 3x + 1}.$$

(b) $\boxed{2}$ Find a degree-2 linear recurrence relation for the sequence $(f_0, f_2, f_4, f_6, \ldots)$. That is, find two numbers a and b such that each $n \geq 2$ satisfies $f_{2n} = af_{2n-2} + bf_{2n-4}$.

[**Hint:** For part **(a)**, start with the generating function $F(x)$ from Section 3.1, and compute the "average" $\dfrac{F(x) + F(-x)}{2}$ in two different ways: On the one hand, this "average" is $f_0 + f_2x^2 + f_4x^4 + f_6x^6 + \cdots$; on the other hand, it is a sum of two fractions. Compare the results, and "substitute $x^{1/2}$ for x" (that is, replace each x^{2n} by x^n).]

A.2.2. Definitions

Exercise A.2.2.1. $\boxed{4}$ Let $n \in \mathbb{N}$ and $m \in \mathbb{C}$. Prove that

$$\sum_{k=0}^{n} (-1)^k \binom{m}{k} \binom{m}{n-k} = \begin{cases} (-1)^{n/2} \dbinom{m}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Exercise A.2.2.2. $\boxed{3}$ Recall that a commutative ring L is said to be an *integral domain* if it is nontrivial (i.e., its zero and its unity are distinct) and has the property that if $a, b \in L$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.

Let K be an integral domain. Prove that the ring $K[[x]]$ is an integral domain.

[**Hint:** The analogous fact for the polynomial ring $K[x]$ is well-known. It is commonly proved by noticing that if two polynomials are nonzero, then the leading term of their product equals the product of their leading terms. This argument does not immediately apply to FPSs, since nonzero FPSs usually have no leading term. What do nonzero FPSs have, though?]

Exercise A.2.2.3. An FPS $a \in K[[x]]$ will be called *even* if it satisfies $[x^1]\, a = [x^3]\, a = [x^5]\, a = \cdots = 0$ (that is, if it satisfies $[x^n]\, a = 0$ for all odd $n \in \mathbb{N}$).

Let $f \in K[[x]]$ be any FPS. Write f in the form $f = \sum_{n \in \mathbb{N}} f_n x^n$ with $f_0, f_1, f_2, \ldots \in K$ (so that $f_n = [x^n]\, f$ for all $n \in \mathbb{N}$). We define $\widetilde{f}$ to be the FPS $\sum_{n \in \mathbb{N}} f_n (-x)^n = \sum_{n \in \mathbb{N}} (-1)^n f_n x^n$. (Using the notations of Definition 3.5.1, this FPS $\widetilde{f}$ is the composition $f[-x] = f \circ (-x)$.)

(a) $\boxed{1}$ Show that the FPS $f + \widetilde{f}$ is even.

(b) $\boxed{2}$ Show that the FPS $f \cdot \widetilde{f}$ is even.

A.2.3. Dividing FPSs

Exercise A.2.3.1. (a) $\boxed{4}$ Prove that

$$\sum_{n \in \mathbb{N}} \frac{2^n x^{2^n}}{1 + x^{2^n}} = \frac{x}{1-x}.$$

(In particular, show that the sum on the left hand side is well-defined.)

(b) $\boxed{3}$ For each positive integer n, let $v_2(n)$ be the highest $k \in \mathbb{N}$ such that $2^k \mid n$. (Equivalently, $v_2(n)$ is the exponent with which 2 appears in the prime factorization of n; when n is odd, this is understood to be 0. For example, $v_2(40) = 3$ and $v_2(41) = 0$.)

Prove that

$$\sum_{n\in\mathbb{N}} \frac{x^{2^n}}{1-x^{2^n}} = \sum_{n>0} v_2(n)\, x^n.$$

(In particular, show that the sum on the left hand side is well-defined.)

A.2.4. Polynomials

The following exercise is a generalization of Binet's formula for the Fibonacci sequence (Example 1 in Section 3.1):

Exercise A.2.4.1. Let F be a field of characteristic 0 (that is, a field that is a $\mathbb{Q}$-algebra). Let d be a positive integer, and let $p_1, p_2, \ldots, p_d$ be d elements of F. Let $p \in F[x]$ be the polynomial $1 - \sum\limits_{i=1}^{d} p_i x^i$.

Let $(a_0, a_1, a_2, \ldots)$ be a sequence of elements of F with the property that each integer $n \geq d$ satisfies

$$a_n = \sum_{i=1}^{d} p_i a_{n-i}.$$

(Such a sequence is said to be a *linearly recursive sequence with constant coefficients*. For example, if $d = 2$ and $p_1 = 1$ and $p_2 = 1$, then each $n \geq 2$ must satisfy $a_n = a_{n-1} + a_{n-2}$, that is, the recursive equation of the Fibonacci sequence. Of course, the starting values $a_0, a_1, \ldots, a_{d-1}$ of the sequence can be arbitrary.)

(a) $\boxed{3}$ Prove that there is some polynomial $q \in F[x]$ of degree $< d$ (this allows $q = 0$) such that

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots = \frac{q}{p} \qquad \text{in } F[[x]].$$

(b) $\boxed{2}$ Assume that the polynomial $p \in F[x]$ can be factored as

$$p = (1 - r_1 x)(1 - r_2 x) \cdots (1 - r_d x)$$

for some distinct elements $r_1, r_2, \ldots, r_d$ of F. Prove that there exist d scalars $\lambda_1, \lambda_2, \ldots, \lambda_d \in F$ such that each $n \in \mathbb{N}$ satisfies

$$a_n = \sum_{i=1}^{d} \lambda_i r_i^n.$$

(c) $\boxed{3}$ Now, assume instead that the polynomial $p \in F[x]$ can be factored as

$$p = (1 - r_1 x)^{m_1} (1 - r_2 x)^{m_2} \cdots (1 - r_k x)^{m_k}$$

for some distinct elements $r_1, r_2, \ldots, r_k$ of F and some nonnegative integers $m_1, m_2, \ldots, m_k$. Prove that there exist k polynomials $u_1, u_2, \ldots, u_k \in F[x]$ such that $\deg u_i < m_i$ for each $i \in \{1, 2, \ldots, k\}$, and such that each $n \in \mathbb{N}$ satisfies

$$a_n = \sum_{i=1}^{n} u_i(n) r_i^n.$$

The next exercise reveals an application of FPSs to number theory (more such applications will appear later on):

Exercise A.2.4.2. Let p and q be two coprime positive integers. We define the set

$$S(p,q) := \{ap + bq \mid (a,b) \in \mathbb{N} \times \mathbb{N}\}.$$

(For example, if $p = 3$ and $q = 5$, then $S(p,q) = \{0, 3, 5, 6, 8, 9, 10, 11, \ldots\}$, where the "$\ldots$" is saying that all integers ≥ 8 belong to $S(p,q)$. The set $S(p,q)$ can be viewed as the set of all denominations that can be paid with p-cent coins and q-cent coins, without getting change.)

(a) $\boxed{3}$ Prove that

$$\sum_{n \in S(p,q)} x^n = \frac{1 - x^{pq}}{(1 - x^p)(1 - x^q)}.$$

(b) $\boxed{3}$ Prove that every integer $n > pq - p - q$ belongs to $S(p,q)$, whereas the integer $pq - p - q$ itself does not.

[**Hint:** For part **(a)**, describe the coefficient of x^m in

$$(1 - x^p)(1 - x^q) \sum_{n \in S(p,q)} x^n = \sum_{n \in S(p,q)} \left(x^n - x^{n+p} - x^{n+q} + x^{n+p+q}\right)$$

in a form revealing that it is 0 unless $m = 0$ or $m = pq$. Now, part **(b)** can be solved as follows: First, show that every sufficiently high $n \in \mathbb{N}$ belongs to $S(p,q)$. Hence, $\sum\limits_{\substack{n \in \mathbb{N}; \\ n \notin S(p,q)}} x^n = \frac{1}{1-x} - \frac{1 - x^{pq}}{(1 - x^p)(1 - x^q)}$ is a polynomial. Finding the largest integer that doesn't belong to $S(p,q)$ means finding the degree of this polynomial.]

Exercise A.2.4.3. Let $N \in \mathbb{N}$. Let P_N denote the $\mathbb{C}$-vector space of all polynomials $f \in \mathbb{C}[x]$ of degree $< N$. Consider the matrices L_c for all $c \in \mathbb{C}$ defined in Exercise A.1.1.4 **(b)**.

For each $c \in \mathbb{C}$, let B_c be the basis $\left((x-c)^0, (x-c)^1, \ldots, (x-c)^{N-1}\right)$ of P_N. (This is a basis, since it is the image of the monomial basis $\left(x^0, x^1, \ldots, x^{N-1}\right)$ under the "substitute $x - c$ for x" automorphism.)

(a) $\boxed{2}$ Let $c, d \in \mathbb{C}$. Prove that $(L_c)^T$ (that is, the transpose of L_c) is the change-of-basis matrix from the basis B_{c+d} to the basis B_d. (This means that

$$(x-d)^j = \sum_{i=0}^{n-1} \left((L_c)^T \right)_{i,j} (x-(c+d))^i \qquad \text{for any } j \in \{0, 1, \ldots, n-1\},$$

where $\left((L_c)^T \right)_{i,j}$ denotes the (i,j)-th entry of the matrix $(L_c)^T$.)

(b) $\boxed{2}$ Use this to give a new solution to Exercise A.1.1.4 **(b)** (without using Exercise A.1.1.4 **(a)**).

A.2.5. Substitution and evaluation of power series

Exercise A.2.5.1. $\boxed{1}$ Let K be a commutative ring. Let $a \in K[[x]]$ be the FPS $\dfrac{x}{x-1}$. Prove that $a \circ a = x$.

Exercise A.2.5.2. Let K be a commutative ring. Let $a \in K[[x]]$ be an FPS such that $[x^0]\, a = 0$.

A *compositional inverse* of a shall mean a FPS $b \in K[[x]]$ such that $[x^0]\, b = 0$ and $a \circ b = x$ and $b \circ a = x$.

Prove the following:

(a) $\boxed{1}$ If a compositional inverse of a exists, then it is unique.

(b) $\boxed{4}$ A compositional inverse of a exists if and only if $[x^1]\, a$ is invertible in K.

A.2.6. Derivatives of FPSs

Exercise A.2.6.1. $\boxed{2}$ Let $f \in K[[x]]$ be an FPS. Let p and q be two coprime nonnegative integers. Prove that the coefficient $[x^q]\,(f^p)$ is a multiple of p (that is, there exists some $c \in K$ such that $[x^q]\,(f^p) = pc$).

[Hint: More generally, prove that $q \cdot [x^q]\,(f^p)$ is a multiple of p whether or not p and q are coprime. (Think about the coefficients of $(f^p)'$.)**]**

The next exercise is concerned with generalizing the two equalities

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x} \qquad \text{and}$$
$$0 + 1x + 2x^2 + 3x^3 + \cdots = \frac{x}{(1-x)^2}$$

that we have encountered in Section 3.1 (as (5) and (16), respectively).

Exercise A.2.6.2. For any $m \in \mathbb{N}$, we define an FPS

$$Q_m := \sum_{n \in \mathbb{N}} n^m x^n = 0^m x^0 + 1^m x^1 + 2^m x^2 + \cdots \in \mathbb{Z}[[x]].$$

For example,

$$Q_0 = x^0 + x^1 + x^2 + x^3 + \cdots = \frac{1}{1-x};$$
$$Q_1 = 0x^0 + 1x^1 + 2x^2 + 3x^3 + \cdots = \frac{x}{(1-x)^2} \qquad \text{(by (16))};$$

it can furthermore be shown that

$$Q_2 = 0x^0 + 1x^1 + 4x^2 + 9x^3 + \cdots = \frac{x(1+x)}{(1-x)^2};$$
$$Q_3 = 0x^0 + 1x^1 + 8x^2 + 27x^3 + \cdots = \frac{x\left(1+4x+x^2\right)}{(1-x)^4};$$
$$Q_4 = 0x^0 + 1x^1 + 16x^2 + 81x^3 + \cdots = \frac{x\left(1+11x+11x^2+x^3\right)}{(1-x)^5}.$$

The expressions become more complicated as m increases, but one will still notice that each Q_m has the form $\frac{A_m}{(1-x)^{m+1}}$, where A_m is a polynomial of degree m that has constant term 0 (unless $m = 0$) and whose coefficients have a "palindromic" symmetry (in the sense that the sequence of coefficients is symmetric across its middle). Let us prove this.

For each $m \in \mathbb{N}$, we define an FPS

$$A_m := (1-x)^{m+1} Q_m \in \mathbb{Z}[[x]].$$

(Thus, $Q_m = \frac{A_m}{(1-x)^{m+1}}$, so that the A_m we just defined are the A_m we are interested in – but we don't yet know that they are polynomials.)

Let $\vartheta : \mathbb{Z}[[x]] \to \mathbb{Z}[[x]]$ be the $\mathbb{Z}$-linear map that sends each FPS $f \in \mathbb{Z}[[x]]$ to xf'. (That is, ϑ takes the derivative of an FPS and then multiplies it by x.)

(a) $\boxed{1}$ Prove that $\vartheta(fg) = \vartheta(f) \cdot g + f \cdot \vartheta(g)$ for any $f, g \in \mathbb{Z}[[x]]$. (In the lingo of algebraists, this is saying that ϑ is a *derivation* of $\mathbb{Z}[[x]]$.)

(b) $\boxed{1}$ Prove that $\vartheta\left((1-x)^k\right) = -kx(1-x)^{k-1}$ for each $k \in \mathbb{Z}$.

(c) $\boxed{1}$ Prove that $Q_m = \vartheta(Q_{m-1})$ for each $m > 0$.

(d) $\boxed{2}$ Prove that $A_m = mxA_{m-1} + x(1-x)A'_{m-1}$ for each $m > 0$.

(e) $\boxed{1}$ Conclude that A_m is a polynomial of degree $\leq m$ for each $m \in \mathbb{N}$.

(f) $\boxed{1}$ Show that $\left[x^0\right](A_m) = 0$ for each $m > 0$.

(g) $\boxed{2}$ Show that $\left[x^i\right](A_m) = (m - i + 1)\left[x^{i-1}\right](A_{m-1}) + i\left[x^i\right](A_{m-1})$ for each $m > 0$ and each $i > 0$.

(h) $\boxed{3}$ Show that $\left[x^i\right](A_m) = \left[x^{m+1-i}\right](A_m)$ for each $m > 0$ and each $i \in \{0, 1, \ldots, m+1\}$.

The polynomials $A_0, A_1, A_2, \ldots$ are known as the *Eulerian polynomials*.

Exercise A.2.6.3. For any nonzero FPS $f \in K[[x]]$, define the *order* $\operatorname{ord}(f)$ of f to be the smallest $m \in \mathbb{N}$ such that $[x^m] f \neq 0$. Further define the *norm* $||f||$ of an FPS $f \in K[[x]]$ to be the rational number $\dfrac{1}{2^{\operatorname{ord}(f)}}$ if f is nonzero. If f is zero, set $||f|| := 0$.

This norm on $K[[x]]$ gives rise to a metric $d : K[[x]] \times K[[x]] \to \mathbb{Q}$ on $K[[x]]$, defined by

$$d(f, g) = ||f - g|| \qquad \text{for any } f, g \in K[[x]].$$

(a) $\boxed{3}$ Prove that $K[[x]]$ is a complete metric space with respect to this metric.

(b) $\boxed{3}$ Prove that the maps

$$K[[x]] \times K[[x]] \to K[[x]],$$
$$(f, g) \mapsto f + g$$

and

$$K[[x]] \times K[[x]] \to K[[x]],$$
$$(f, g) \mapsto fg$$

and

$$K[[x]] \times K[[x]]_0 \to K[[x]],$$
$$(f, g) \mapsto f \circ g$$

are continuous with respect to the topologies induced by this metric. (Recall that $K[[x]]_0$ denotes the subset of $K[[x]]$ consisting of all FPSs $g \in K[[x]]$ satisfying $\left[x^0\right] g = 0$. This subset becomes a topological space by inheriting a subspace topology from $K[[x]]$.)

(c) $\boxed{1}$ Prove that the map

$$K[[x]] \to K[[x]],$$
$$f \mapsto f'$$

is Lipschitz continuous with Lipschitz constant 2.

(d) $\boxed{1}$ Assume that K is a commutative $\mathbb{Q}$-algebra. Let $\int$ denote the K-linear map from $K[[x]]$ to $K[[x]]$ that sends each FPS $\sum\limits_{n\in\mathbb{N}} a_n x^n$ to $\sum\limits_{n\in\mathbb{N}} \dfrac{1}{n+1} a_n x^{n+1}$. (This map $\int$ is an algebraic analogue of the antiderivative.) Prove that this map $\int$ is Lipschitz continuous with Lipschitz constant $\dfrac{1}{2}$.

[**Hint:** For part **(b)**, the topology on the product of two metric spaces is induced by the sup metric, which is given by

$$d_{\sup}\left(\left(f_1, g_1\right), \left(f_2, g_2\right)\right) = \max\left\{d\left(f_1, f_2\right), d\left(g_1, g_2\right)\right\}.$$

Show that all three maps are Lipschitz continuous with Lipschitz constant 1 – i.e., that any (f_1, g_1) and (f_2, g_2) in the respective product spaces satisfy

$$\begin{aligned} d\left(f_1 + g_1, f_2 + g_2\right) &\leq d_{\sup}\left(\left(f_1, g_1\right), \left(f_2, g_2\right)\right) \qquad &\text{and} \\ d\left(f_1 g_1, f_2 g_2\right) &\leq d_{\sup}\left(\left(f_1, g_1\right), \left(f_2, g_2\right)\right) \qquad &\text{and} \\ d\left(f_1 \circ g_1, f_2 \circ g_2\right) &\leq d_{\sup}\left(\left(f_1, g_1\right), \left(f_2, g_2\right)\right). \end{aligned}$$

]

Exercise A.2.6.4. $\boxed{3}$ Let K be a commutative $\mathbb{Q}$-algebra. Let $f \in K[[x]]$ be any FPS. Prove that there exists a **unique** FPS $g \in K[[x]]$ satisfying $\left[x^0\right] g = 0$ and $g' = f \circ g$.

[**Hint:** This is an algebraic version of local existence and uniqueness of a solution of an ODE. There is an elementary recursive way to prove this. However, a more elegant way is to rewrite the ODE $g' = f \circ g$ as an integral equation $g = \int (f \circ g)$, where $\int$ is the map defined in Exercise A.2.6.3 **(d)**. This integral equation says that g is a fixed point of the (nonlinear) operator $K[[x]] \to K[[x]]$, $h \mapsto \int (f \circ h)$. Now, apply the Banach fixed-point theorem.]

A.2.7. Exponentials and logarithms

Recall that $K[[x]]_1 = \left\{f \in K[[x]] \mid \left[x^0\right] f = 1\right\}$.

Exercise A.2.7.1. For any FPS $f \in K[[x]]_1$, we define the *logarithmic derivative* $\operatorname{loder} f \in K[[x]]$ to be the FPS $\dfrac{f'}{f}$. Prove the following:

(a) $\boxed{1}$ We have $\operatorname{loder}(fg) = \operatorname{loder} f + \operatorname{loder} g$ for any $f, g \in K[[x]]_1$.

(b) $\boxed{1}$ If K is a commutative $\mathbb{Q}$-algebra, then $\operatorname{loder} f = (\operatorname{Log} f)'$ for any $f \in K[[x]]_1$. (Recall that $\operatorname{Log} f = \overline{\log}[f-1]$.)

A.2.8. Non-integer powers

Exercise A.2.8.1. Let K be a nontrivial commutative ring.

(a) $\boxed{2}$ Prove that there exists no FPS $f \in K[[x]]$ such that $f^2 = x$. (Do not assume that K is a field or an integral domain!)

(b) $\boxed{2}$ More generally: Let $f \in K[[x]]$ and $n \in \mathbb{N}$. Assume that

$$f^n = ax^m + \sum_{i>m} a_i x^i$$

for some $m \in \mathbb{N}$, some **invertible** $a \in K$ and some elements $a_{m+1}, a_{m+2}, a_{m+3}, \ldots \in K$. Prove that $n \mid m$. [This might require a little bit of commutative algebra – specifically the fact that any nontrivial commutative ring has a maximal ideal.]

(c) $\boxed{1}$ Now assume that $K = \mathbb{Z}/2$ is the field with 2 elements. Prove that there exists no FPS $f \in K[[x]]$ such that $f^2 = 1 + x$.

Exercise A.2.8.2. $\boxed{1}$ Prove Theorem 3.8.2.

Exercise A.2.8.3. $\boxed{5}$ Recall the Catalan numbers $c_0, c_1, c_2, \ldots$ introduced in Example 2 in Section 3.1. Prove that

$$\sum_{k=0}^{n} c_{2k} c_{2(n-k)} = 4^n c_n \qquad \text{for each } n \in \mathbb{N}.$$

Exercise A.2.8.4. $\boxed{4}$ **(a)** Prove that there exists a unique sequence $(a_0, a_1, a_2, \ldots)$ of rational numbers that satisfies $a_0 = 1$ and

$$\sum_{k=0}^{n} a_k a_{n-k} = 1 \qquad \text{for all } n \in \mathbb{N}.$$

(b) Find an explicit formula for the n-th entry a_n of this sequence (in terms of binomial coefficients).

A.2.9. Integer compositions

Exercise A.2.9.1. $\boxed{3}$ Let n be a positive integer. Let $m \in \mathbb{N}$. Prove that

$$\sum_{\substack{(a_1,a_2,\ldots,a_n)\in\mathbb{N}^n;\\ a_1+a_2+\cdots+a_n=m}} a_1a_2\cdots a_n = \dbinom{n+m-1}{2n-1}.$$

Exercise A.2.9.2. $\boxed{5}$ Let n be a positive integer. Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$. Prove that:

(a) The # of compositions $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ of n such that $\alpha_1, \alpha_2, \ldots, \alpha_m$ are odd is f_n.

(b) The # of compositions $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ of n such that $\alpha_i \geq 2$ for each $i \in \{1, 2, \ldots, m\}$ is f_{n-1}.

(c) The # of compositions $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ of n such that $\alpha_i \leq 2$ for each $i \in \{1, 2, \ldots, m\}$ is f_{n+1}.

(Note that Exercise A.2.9.2 is behind many appearances of the Fibonacci numbers in the research literature, e.g., in the theory of "peak algebras".)

It is surprising that one and the same sequence (the Fibonacci sequence) answers the three different counting questions in Exercise A.2.9.2. Even more surprisingly, this generalizes:

Exercise A.2.9.3. $\boxed{4}$ Let n and k be two positive integers such that $k > 1$.

Let u be the # of compositions α of n such that each entry of α is congruent to 1 modulo k.

Let v be the # of compositions β of $n + k - 1$ such that each entry of β is $\geq k$.

Let w be the # of compositions γ of $n - 1$ such that each entry of γ is either 1 or k.

Prove that $u = v = w$.

A.2.10. x^n-equivalence

Exercise A.2.10.1. $\boxed{2}$ Assume that K is a commutative $\mathbb{Q}$-algebra. Let $n \in \mathbb{N}$. Let $c \in K$ and $a, b \in K[[x]]_1$ satisfy $a \overset{x^n}{\equiv} b$. Prove that $a^c \overset{x^n}{\equiv} b^c$.

Exercise A.2.10.2. $\boxed{3}$ Let $a, b \in K[[x]]$ be two FPSs that have compositional inverses. (See Exercise A.2.5.2 for the meaning of "compositional inverse".) Let $\widetilde{a}$ and $\widetilde{b}$ be the compositional inverses of a and b. Let $n \in \mathbb{N}$ be such that $a \overset{x^n}{\equiv} b$. Prove that $\widetilde{a} \overset{x^n}{\equiv} \widetilde{b}$.

A.2.11. Infinite products

Exercise A.2.11.1. $\boxed{2}$ Prove that each nonnegative integer can be written uniquely in the form $\sum\limits_{k\geq 1} a_k \cdot k!$, for some sequence $(a_1, a_2, a_3, \ldots)$ of integers satisfying $(0 \leq a_k \leq k \text{ for each } k \geq 1)$ and $(a_k = 0 \text{ for all but finitely many } k \geq 1)$.

[**Hint:** Simplify the FPS $\prod\limits_{k\geq 1} \left(1 + x^{k!} + x^{2k!} + \cdots + x^{k\cdot k!}\right)$.]

Exercise A.2.11.2. **(a)** $\boxed{1}$ Prove that the family $\left(1 - a_i x^i\right)_{i\in\{1,2,3,\ldots\}}$ is multipliable whenever $(a_1, a_2, a_3, \ldots) \in K^{\{1,2,3,\ldots\}}$ is a sequence of elements of K.

(b) $\boxed{3}$ Let $f \in K[[x]]$ be an FPS with constant term $\left[x^0\right] f = 1$. Prove that there is a unique sequence $(a_1, a_2, a_3, \ldots) \in K^{\{1,2,3,\ldots\}}$ such that

$$f = \prod_{i=1}^{\infty} \left(1 - a_i x^i\right).$$

We call this sequence $(a_1, a_2, a_3, \ldots)$ the *Witt coordinate sequence* of f.

(c) $\boxed{1}$ Find the Witt coordinate sequence of the FPS $\dfrac{1}{1-x}$.

Next come some more exercises on the technicalities of multipliability and infinite products. The first one is a (partial) converse to Theorem 3.11.10:

Exercise A.2.11.3. $\boxed{5}$ Let $(\mathbf{a}_i)_{i\in I}$ be a multipliable family of FPSs such that each $\mathbf{a}_i$ is invertible (in $K[[x]]$). Prove that the family $(\mathbf{a}_i - 1)_{i\in I}$ is summable.

Exercise A.2.11.4. Let $(\mathbf{a}_i)_{i\in I}$ and $(\mathbf{b}_i)_{i\in I}$ be two families of FPSs.

(a) $\boxed{1}$ If $(\mathbf{a}_i)_{i\in I}$ and $(\mathbf{b}_i)_{i\in I}$ are multipliable, is it necessarily true that the family $(\mathbf{a}_i + \mathbf{b}_i)_{i\in I}$ is multipliable?

(b) $\boxed{1}$ If $(\mathbf{a}_i)_{i\in I}$ is summable and $(\mathbf{b}_i)_{i\in I}$ is multipliable, is it necessarily true that the family $(\mathbf{a}_i + \mathbf{b}_i)_{i\in I}$ is multipliable?

(c) $\boxed{1}$ Does the answer to part **(b)** change if we additionally assume that $\mathbf{b}_i$ is invertible for each $i \in I$?

Exercise A.2.11.5. $\boxed{5}$ Prove the following generalization of Proposition 3.11.26:

Let I be a set. For any $i \in I$, let S_i be a set. Set

$$\overline{S} = \{(i,k) \mid i \in I \text{ and } k \in S_i \text{ and } k \neq 0\}.$$

For any $i \in I$ and any $k \in S_i$, let $p_{i,k}$ be an element of $K[[x]]$. Assume that

$$p_{i,0} = 1 \qquad \text{for any } i \in I \text{ satisfying } 0 \in S_i.$$

Assume further that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable. Then, the product $\prod\limits_{i\in I} \sum\limits_{k\in S_i} p_{i,k}$ is well-defined (i.e., the family $(p_{i,k})_{k\in S_i}$ is summable for each $i \in I$, and the family $\left(\sum\limits_{k\in S_i} p_{i,k}\right)_{i\in I}$ is multipliable), and we have

$$\prod_{i\in I} \sum_{k\in S_i} p_{i,k} = \sum_{\substack{(k_i)_{i\in I}\in \prod\limits_{i\in I} S_i \\ \text{is essentially finite}}} \prod_{i\in I} p_{i,k_i}. \tag{294}$$

A.2.12. The generating function of a weighted set

Exercise A.2.12.1. $\boxed{5}$ This exercise is about a variation on domino tilings. We define "shapes" and the specific shapes $R_{n,m}$ as in Definition 3.12.10. Fix a positive integer k.

A *k-omino* means a size-k shape of the form

$\{(i+1, j), (i+2, j), \ldots, (i+k, j)\}$ (a "*horizontal k-omino*") or
$\{(i, j+1), (i, j+2), \ldots, (i, j+k)\}$ (a "*vertical k-omino*")

for some $(i, j) \in \mathbb{Z}^2$.

A *k-omino tiling* of a shape S is a set partition of S into k-ominos (i.e., a set of disjoint k-ominos whose union is S).

Prove that the shape $R_{n,m}$ has a k-omino tiling if and only if we have $k \mid n$ or $k \mid m$.

[**Hint:** Consider $R_{n,m}$ as a weighted set, where the weight of a square $(i, j) \in \mathbb{N}^2$ is defined to be $i + j$. If $R_{n,m}$ has a k-omino tiling, then show that the weight generating function $\overline{R_{n,m}} = \sum\limits_{(i,j)\in R_{n,m}} x^{i+j}$ must be divisible by $1 + x + x^2 + \cdots + x^{k-1}$ (as a polynomial in $\mathbb{Q}[x]$, for example). However, $\overline{R_{n,m}}$ has a simple form.]

A.2.13. Limits of FPSs

Exercise A.2.13.1. (a) $\boxed{3}$ Prove Proposition 3.13.5.

(b) $\boxed{3}$ Prove Proposition 3.13.7.

Exercise A.2.13.2. $\boxed{4}$ Let $f \in K[[x]]$ be any FPS. Prove that $\lim\limits_{i\to\infty} f^i$ exists if and only if the constant term $[x^0] f$ of f is nilpotent. (An element $u \in K$ is said to be *nilpotent* if there exists some $m \in \mathbb{N}$ such that $u^m = 0$.)

Exercise A.2.13.3. $\boxed{5}$ Recall the Catalan numbers $c_0, c_1, c_2, \ldots$ introduced in Example 2 in Section 3.1, and the corresponding FPS $C(x) = \sum\limits_{n\in\mathbb{N}} c_n x^n$. Prove that

$$1 - \frac{1}{C(x)} = \cfrac{x}{1 - \cfrac{x}{1 - \cfrac{x}{\ddots}}},$$

where the continued fraction on the right hand side is to be understood as

$$\lim_{n\to\infty} \underbrace{\cfrac{x}{1 - \cfrac{x}{1 - \cfrac{x}{1 - \ddots - \cfrac{x}{1-x}}}}}_{\text{with } n \text{ layers}}.$$

(This requires checking that the n-layered finite continued fractions are well-defined and converge to a limit in $K[[x]]$.)

A.2.14. Laurent power series

Exercise A.2.14.1. $\boxed{2}$ While $K[[x^{\pm}]]$ is not a ring, some elements of $K[[x^{\pm}]]$ can still be multiplied. For instance, define three elements $a, b, c \in K[[x^{\pm}]]$ by

$$\begin{aligned} a &= 1 + x^{-1} + x^{-2} + x^{-3} + \cdots, \\ b &= 1 - x, \\ c &= 1 + x + x^2 + x^3 + \cdots. \end{aligned}$$

(a) Find ab and bc and $a(bc)$ and $(ab)c$.

(b) Why is it not surprising that $a(bc) \neq (ab)c$?

Exercise A.2.14.2. $\boxed{2}$ Let K be a field. Prove that the K-algebra $K((x))$ is a field.

[**Hint:** You can take it for granted that $K((x))$ is a commutative K-algebra, as the proof is a mutatis-mutandis variant of the analogous proof for usual FPSs.]

Here are some applications of Laurent polynomials:

Exercise A.2.14.3. Let $n \in \mathbb{N}$.

(a) $\boxed{5}$ Prove that

$$\sum_{k=0}^{n} (-2)^{n-k} \binom{n}{k} \binom{2k}{k} = \binom{n}{n/2}.$$

(Recall that $\binom{n}{i} = 0$ whenever $i \notin \mathbb{N}$.)

(b) $\boxed{2}$ More generally, prove that

$$\sum_{k=0}^{n} (-2)^{n-k} \binom{n}{k} \binom{2k}{k+p} = \binom{n}{(n+p)/2} \qquad \text{for any } p \in \mathbb{Z}.$$

[**Hint:** Compute the coefficients of the Laurent polynomial $\left(\left(x+x^{-1}\right)^2 - 2\right)^n$ in two ways.]

Exercise A.2.14.4. For any Laurent series $f = \sum_{n\in\mathbb{Z}} f_n x^n \in K((x))$ (with $f_n \in K$), we define the *residue* of f to be its x^{-1}-coefficient f_{-1}. We denote this residue by $\operatorname{Res} f$. (This is an algebraic analogue of the "residue at 0" from complex analysis.)

The *order* $\operatorname{ord} f$ of a nonzero Laurent series $f = \sum_{n\in\mathbb{Z}} f_n x^n \in K((x))$ (with $f_n \in K$) shall mean the smallest $n \in \mathbb{Z}$ satisfying $f_n \neq 0$. (This is well-defined, since all sufficiently low $n \in \mathbb{Z}$ satisfy $f_n = 0$ by the definition of a Laurent series.) The *trailing coefficient* of a nonzero Laurent series $f \in K((x))$ means the coefficient $\left[x^{\operatorname{ord} f}\right] f$ (that is, the $x^{\operatorname{ord} f}$-coefficient of f). For example, the Laurent series $-x^{-2} + 3 + 7x$ has order -2 and trailing coefficient -1.

The *derivative* f' of a Laurent series $f \in K((x))$ is defined as follows: If $f = \sum_{n\in\mathbb{Z}} f_n x^n$ with $f_n \in K$, then $f' := \sum_{n\in\mathbb{Z}} n f_n x^{n-1}$.

Prove the following:

(a) $\boxed{1}$ Any $f \in K((x))$ satisfies $\operatorname{Res}(f') = 0$.

(b) $\boxed{3}$ Any $n \in \mathbb{N}$ and any $f \in K((x))$ satisfy $\operatorname{Res}(f^n f') = 0$.

(c) $\boxed{1}$ If $f \in K((x))$ is a nonzero Laurent series whose trailing coefficient is invertible (in K), then f is invertible in $K((x))$. (Keep in mind that the word "invertible" refers to multiplicative inverses, not compositional inverses.)

(d) $\boxed{3}$ If $f \in K((x))$ is a nonzero Laurent series whose trailing coefficient is invertible (in K), then each $n \in \mathbb{Z}$ satisfies

$$\operatorname{Res}\left(f^n f'\right) = \begin{cases} 0, & \text{if } n \neq -1; \\ \operatorname{ord} f, & \text{if } n = -1. \end{cases}$$

(To be fully precise, "$\operatorname{ord} f$" here means the element $(\operatorname{ord} f) \cdot 1_K$ of the ring K.)

[Hint: In parts of this exercise, it may be expedient to first prove the claim under the assumption that K is a $\mathbb{Q}$-algebra (so that $1, 2, 3, \ldots$ can be divided by in K), and then to argue that the assumption can be lifted.]

Exercise A.2.14.5. Let $f = \sum_{n>0} f_n x^n$ (with $f_1, f_2, f_3, \ldots \in K$) be an FPS in $K[[x]]$ whose constant term is 0. Assume that f has a compositional inverse $g = \sum_{n>0} g_n x^n$ (with $g_1, g_2, g_3, \ldots \in K$).

(a) $\boxed{2}$ Prove that there exists a unique FPS $h \in K[[x]]$ with $x = fh$. (This FPS h is usually denoted by $\dfrac{x}{f}$, but this notation is not an instance of Definition 3.3.5 **(b)**, since f is not invertible.)

(b) $\boxed{4}$ Prove the *Lagrange inversion formula*, which says that

$$n \cdot g_n = \left[x^{n-1}\right]\left(h^n\right) \qquad \text{for any positive integer } n.$$

(c) $\boxed{2}$ The *Lambert W series* is defined to be the compositional inverse of the FPS $x \cdot \exp[x] = \sum_{n \in \mathbb{N}} \dfrac{x^{n+1}}{n!}$. Find an explicit formula for the x^n-coefficient of this series.

(d) $\boxed{2}$ Consider again the FPS $C(x) = c_0 + c_1 x + c_2 x^2 + \cdots \in \mathbb{Q}[[x]]$ from Example 2 in Section 3.1. Let us rename it as C. We proved the equality $C = 1 + xC^2$ in that example (albeit we wrote it as $C(x) = 1 + x(C(x))^2$). Set $f = x - x^2$ and $g = xC$. Show that the FPS g is a compositional inverse of f. Use the Lagrange inversion formula to reprove the formula $c_n = \dfrac{1}{n+1}\dbinom{2n}{n}$ without the quadratic formula.

(e) $\boxed{2}$ Let m be a positive integer. Let $D \in \mathbb{Q}[[x]]$ be an FPS with constant term 1 that satisfies $D = 1 + x^{m-1}D^m$. Find an explicit formula for the x^n-coefficient of D. (This generalizes part **(d)**, which is obtained for $m = 2$.)

[Hint: For part **(b)**, take derivatives of both sides in $g \circ f = x$ to obtain $(g' \circ f) \cdot f' = 1$; then divide by f^n in the Laurent series ring $K((x))$, and rewrite $g' \circ f$ as $\sum\limits_{k>0} k g_k f^{k-1}$. Now take residues and use Exercise A.2.14.4 **(d)**.]

[**Remarks:** Part **(b)** is remarkable for connecting the compositional inverse g of f with the multiplicative inverse h of f/x. Since multiplicative inverses are usually easier to compute, it is a helpful tool for the computation of compositional inverses.

The Lambert W series in part **(c)** is the Taylor series of the Lambert W function.]

The following exercise tells a cautionary tale about applying some of our results past their stated assumptions:

Exercise A.2.14.6. $\boxed{2}$ Extending Definition 3.13.2 to the K-module $K\left[\left[x^{\pm}\right]\right]$, we obtain the notion of a limit of a sequence of doubly infinite power series.

(a) Prove that $\lim\limits_{n\to\infty} \left(x^n + x^{-n}\right) = 0$.

(b) Prove that $\lim\limits_{n\to\infty} \left(\left(x^n + x^{-n}\right)^2\right) = 2$.

(c) Can Theorem 3.13.5 be generalized to Laurent series instead of FPSs?

[**Note:** This does not mean that the notion of limits of sequences of Laurent series is completely useless. They behave reasonably as long as multiplication is not involved.]

A.2.15. Multivariate FPSs

Exercise A.2.15.1. $\boxed{2}$ Let $k \in \mathbb{N}$. Prove that

$$\sum_{n\in\mathbb{N}} \binom{n}{k} x^n = \frac{x^k}{\left(1-x\right)^{k+1}}$$

without using multivariate power series.

Exercise A.2.15.2. $\boxed{2}$ Prove that

$$\sum_{n\in\mathbb{N}} \frac{x^n}{1-yq^n} = \sum_{n\in\mathbb{N}} \frac{y^n}{1-xq^n} \qquad \text{in the ring } K\left[\left[x,y,q\right]\right].$$

The next two exercises are concerned with FPSs in two indeterminates x and y.

Exercise A.2.15.3. $\boxed{4}$ For any $n \in \mathbb{N}$ and $m \in \mathbb{N}$, we let $f(m,n)$ denote the # of n-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of integers satisfying $|\alpha_1| + |\alpha_2| + \cdots + |\alpha_n| \leq m$.

(a) Prove that $\sum\limits_{(n,m)\in\mathbb{N}\times\mathbb{N}} f(m,n)\, x^m y^n = \dfrac{1}{1-x-y-xy}$ in $K[[x,y]]$.

(b) Prove that $f(m,n) = f(n,m)$ for all $n, m \in \mathbb{N}$.

Exercise A.2.15.4. $\boxed{4}$ Let $f \in K[[x,y]]$ be an FPS such that each positive integer b satisfies $f\left[x, x^b\right] = 0$. Prove that $f = 0$.

Next comes an application of multivariate polynomials to proving a famous binomial identity:

Exercise A.2.15.5. In this exercise, we shall prove *Dixon's identity*, which states that

$$\sum_{k\in\mathbb{Z}} (-1)^k \binom{b+c}{c+k}\binom{c+a}{a+k}\binom{a+b}{b+k} = \frac{(a+b+c)!}{a!b!c!} \qquad (295)$$

for any $a, b, c \in \mathbb{N}$.

(a) $\boxed{1}$ Set

$$F(a,b,c) := \sum_{k\in\mathbb{Z}} (-1)^k \binom{b+c}{c+k}\binom{c+a}{a+k}\binom{a+b}{b+k}$$

for any $a, b, c \in \mathbb{N}$. Prove that $F(a,b,c)$ is well-defined (i.e., the sum in this definition is summable).

(b) $\boxed{1}$ Prove that (295) holds whenever $a = 0$ or $b = 0$ or $c = 0$.

(c) $\boxed{3}$ Prove that every $a, b, c \in \mathbb{N}$ satisfy

$$F(a,b,c) = (-1)^{a+b+c} \cdot \left[x^{2a}y^{2b}z^{2c}\right]\left((y-z)^{b+c}(z-x)^{c+a}(x-y)^{a+b}\right).$$

(Here, we are using polynomials in three indeterminates x, y, z.)

(d) $\boxed{3}$ Prove that every three positive integers a, b, c satisfy

$$F(a,b,c) = F(a-1,b,c) + F(a,b-1,c) + F(a,b,c-1).$$

(e) $\boxed{1}$ Prove that every three positive integers a, b, c satisfy

$$\frac{(a+b+c)!}{a!b!c!} = \frac{(a-1+b+c)!}{(a-1)!b!c!} + \frac{(a+b-1+c)!}{a!(b-1)!c!} + \frac{(a+b+c-1)!}{a!b!(c-1)!}.$$

(f) $\boxed{1}$ Prove (295).

(g) $\boxed{2}$ Show that each $n \in \mathbb{N}$ satisfies

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3 = \begin{cases} (-1)^{n/2} \dfrac{(3n/2)!}{(n/2)!^3}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

[**Hint:** For part **(d)**, use the fact that

$$x^2 (y-z) + y^2 (z-x) + z^2 (x-y) = -(y-z)(z-x)(x-y),$$

and keep in mind that $\left[x^i y^j z^k\right] (x^m p) = \left[x^{i-m} y^j z^k\right] p$ for any i, j, k, m, p with $i \geq m$.]

A.3. Integer partitions and q-binomial coefficients

The notations of Chapter 4 shall be used here.

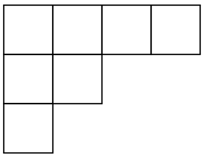
A.3.1. Partition basics

Exercise A.3.1.1. The purpose of this exercise is to make the proof of Proposition 4.1.14 rigorous.

For any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we define the *Young diagram* $Y(\lambda)$ of λ to be the finite set

$$\{(i,j) \mid i \in \{1, 2, \ldots, k\} \text{ and } j \in \{1, 2, \ldots, \lambda_i\}\}.$$

Visually, this set $Y(\lambda)$ is represented by drawing each $(i,j) \in Y(\lambda)$ as a cell of an (invisible) matrix, namely as the cell in row i and in row j. The resulting picture is a table of k left-aligned rows, where the i-th row (counted from the top) has exactly λ_i cells. For example, if $\lambda = (4, 2, 1)$, then the Young diagram $Y(\lambda)$ of λ is

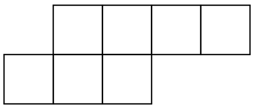
 .

(This is only one way to draw Young diagrams; it is known as *English notation* or *matrix notation*, since our labeling of cells matches the way the cells of a matrix are commonly labeled. If we flip our pictures across a horizontal axis, we would get *French notation* aka *Cartesian notation*, as the labeling of cells would then match the Cartesian coordinates of their centers.)

(a) $\boxed{1}$ Prove that $|Y(\lambda)| = |\lambda|$ for any partition λ.

(b) $\boxed{1}$ Prove that the Young diagram $Y(\lambda)$ uniquely determines the partition λ.

A *NW-set* shall mean a subset S of $\{1,2,3,\ldots\}^2$ with the following property: If $(i,j) \in S$ and $(i',j') \in \{1,2,3,\ldots\}^2$ satisfy $i' \leq i$ and $j' \leq j$, then $(i',j') \in S$ as well. (In terms of our above visual model, this means that walking northwest from a cell of S never moves you out of S, unless you walk out of the matrix. For example, the set

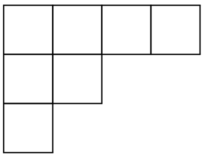
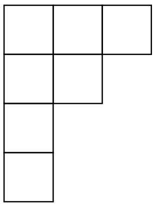


is not a NW-set, since the left neighbor of the leftmost cell in the topmost row is not in this set.)

(c) $\boxed{1}$ Prove that $Y(\lambda)$ is a NW-set for each partition λ.

(d) $\boxed{2}$ Prove that any finite NW-set has the form $Y(\lambda)$ for a unique partition λ.

Now, let flip : $\{1,2,3,\ldots\}^2 \to \{1,2,3,\ldots\}^2$ be the map that sends each $(i,j) \in \{1,2,3,\ldots\}^2$ to (j,i). Visually, this map flip is a reflection in the "main diagonal" (the diagonal going from the northwest to the southeast). We can apply flip to a subset of $\{1,2,3,\ldots\}^2$ by applying flip to each element of this subset. For example:

flip sends  to  .

(e) $\boxed{1}$ Prove that for any partition λ, there is a unique partition λ^t such that $Y(\lambda^t) = \operatorname{flip}(Y(\lambda))$.

This partition λ^t is called the *transpose* (or *conjugate*) of λ.

(f) $\boxed{1}$ Prove that if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a partition, then the partition λ^t has exactly λ_1 parts. (Here, we set $\lambda_1 = 0$ if $k = 0$.)

(g) $\boxed{1}$ Prove that if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, then the i-th part of the partition λ^t equals the # of all $j \in \{1,2,\ldots,k\}$ such that $\lambda_j \geq i$.

(h) $\boxed{1}$ Prove that $|\lambda^t| = |\lambda|$ and $(\lambda^t)^t = \lambda$ for any partition λ.

Exercise A.3.1.2. $\boxed{5}$ A partition will be called *binarial* if all its parts are powers of 2. For instance, $(8,2,2,1)$ is a binarial partition of 13. Recall that the length of a partition λ is denoted by $\ell(\lambda)$.

Let $n > 1$ be an integer. Prove that

$$\sum_{\substack{\lambda \text{ is a binarial} \\ \text{partition of } n}} (-1)^{\ell(\lambda)} = 0.$$

In other words, prove that the # of binarial partitions of n having even length equals the # of binarial partitions of n having odd length.

Exercise A.3.1.3. $\boxed{3}$ A partition will be called *trapezoidal* if it has the form $(j, j-1, j-2, \ldots, i)$ for some integers $i \leq j$. (For instance, $(4,3,2)$ and (5) are trapezoidal partitions.)

Let n be a positive integer. Prove that

$$(\text{\# of trapezoidal partitions of } n) = (\text{\# of odd positive divisors of } n).$$

Convention A.3.1. Let n be an integer. The notation "$\lambda \vdash n$" shall mean "λ is a partition of n". Thus, for example, the summation sign "$\sum\limits_{\lambda \vdash n}$" means a sum over all partitions λ of n.

Exercise A.3.1.4. $\boxed{5}$ If λ is a partition, and if i is a positive integer, then $m_i(\lambda)$ shall mean the # of parts of λ that are equal to i. For instance, $m_3(5,3,3,2) = 2$ and $m_4(5,3,3,2) = 0$.

Fix an $n \in \mathbb{N}$.

(a) Prove that

$$\prod_{\lambda \vdash n} \prod_{i=1}^{\infty} (m_i(\lambda))! = \prod_{\lambda \vdash n} \prod_{i=1}^{\infty} i^{m_i(\lambda)}.$$

(b) More generally, prove that

$$\prod_{\lambda \vdash n} \prod_{\substack{(i,j) \in \{1,2,3,\ldots\}^2; \\ j \leq m_i(\lambda)}} x_j = \prod_{\lambda \vdash n} \prod_{i=1}^{\infty} x_i^{m_i(\lambda)}$$

as monomials in $x_1, x_2, x_3, \ldots$.

(For example, for $n = 3$, this is saying that

$$\underbrace{(x_1)}_{\text{factors for } \lambda=(3)} \cdot \underbrace{(x_1 x_1)}_{\text{factors for } \lambda=(2,1)} \cdot \underbrace{(x_1 x_2 x_3)}_{\text{factors for } \lambda=(1,1,1)}$$
$$= \underbrace{\left(x_3^1\right)}_{\text{factors for } \lambda=(3)} \cdot \underbrace{\left(x_1^1 x_2^1\right)}_{\text{factors for } \lambda=(2,1)} \cdot \underbrace{\left(x_1^3\right)}_{\text{factors for } \lambda=(1,1,1)} .$$

Make sure you understand why part **(a)** is a particular case of **(b)**.)

Exercise A.3.1.5. Recall the notations from Exercise A.3.1.1.

We say that a partition λ is a *single-cell upgrade* of a partition μ if we have $Y(\lambda) \subseteq Y(\mu)$ and $|Y(\mu) \setminus Y(\lambda)| = 1$. (This is just saying that the Young diagram of μ is obtained from that of λ by adding one single cell.)

For instance, the single-cell upgrades of the partition $(2,2,1)$ are $(3,2,1)$, $(2,2,2)$ and $(2,2,1,1)$. On the other hand, the partition $(2,2,1)$ is a single-cell upgrade of each of the partitions $(2,2)$ and $(2,1,1)$.

For any partition λ, let $\gamma(\lambda)$ denote the # of **distinct** parts of λ. For instance, $\gamma(5,5,3,2,1,1) = 4$.

Prove the following:

(a) $\boxed{2}$ For any partition λ, we have

$$\begin{aligned}&(\text{\# of partitions } \mu \text{ such that } \lambda \text{ is a single-cell upgrade of } \mu)\\ &= \gamma(\lambda).\end{aligned}$$

(b) $\boxed{3}$ For any partition λ, we have

$$\begin{aligned}&(\text{\# of single-cell upgrades of } \lambda)\\ &= (\text{\# of partitions } \mu \text{ such that } \lambda \text{ is a single-cell upgrade of } \mu) + 1.\end{aligned}$$

(c) $\boxed{3}$ We have

$$\sum_{\lambda \text{ is a partition}} \gamma(\lambda)\, x^{|\lambda|} = \frac{x}{1-x} \prod_{i=1}^{\infty} \frac{1}{1-x^i} \qquad \text{in } \mathbb{Z}[[x]].$$

Exercise A.3.1.6. $\boxed{4}$ Let d be a positive integer. Let $n \in \mathbb{N}$. Prove that

$$\begin{aligned}&(\text{\# of partitions of } n \text{ that have no part divisible by } d)\\ &= (\text{\# of partitions of } n \text{ that have no } d \text{ equal parts}).\end{aligned}$$

(For instance, the partition $(4,2,2,2,2)$ has no part divisible by 3, but it has 3 equal parts.)

[**Remark:** Theorem 4.1.13 is the particular case of this exercise for $d = 2$.]

Exercise A.3.1.7. $\boxed{4}$ Let $n \in \mathbb{N}$. Let $p_{\text{dist odd}}(n)$ be the # of partitions λ of n such that all parts of λ are distinct and odd. (For example, $(7,3,1)$ is such a partition.) Let $p_+(n)$ be the # of partitions of n that have an even # of even parts. (For example, $(5,4,2)$ is such a partition.) Let $p_-(n)$ be the # of partitions of n that have an odd # of even parts. (For example, $(5,4,1)$ is such a partition.) Prove that

$$p_+(n) - p_-(n) = p_{\text{dist odd}}(n).$$

Exercise A.3.1.8. For any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we define the integer

$$\operatorname{alt} \lambda = \sum_{i=1}^{k} (-1)^{i-1} \lambda_i = \lambda_1 - \lambda_2 + \lambda_3 - \lambda_4 \pm \cdots + (-1)^{k-1} \lambda_k.$$

(a) $\boxed{1}$ Prove that $\operatorname{alt} \lambda \in \mathbb{N}$ for each partition λ.

(b) $\boxed{1}$ Define the transpose λ^t of a partition λ as in Exercise A.3.1.1. Show that $\operatorname{alt}\left(\lambda^t\right) = (\#$ of odd parts of $\lambda)$ for any partition λ.

(c) $\boxed{8}$ Prove that each $n, k \in \mathbb{N}$ satisfy

$$\begin{aligned} &(\text{\# of partitions } \lambda \text{ of } n \text{ into odd parts such that } \ell(\lambda) = k) \\ &= (\text{\# of partitions } \lambda \text{ of } n \text{ into distinct parts such that } \operatorname{alt} \lambda = k). \end{aligned}$$

(d) $\boxed{1}$ Derive a new proof of Theorem 4.1.13 from this.

Exercise A.3.1.9. Let $n \in \mathbb{N}$. Let Par_n denote the set of all partitions of n.

We define a partial order $\preccurlyeq$ on the set Par_n as follows: For two partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$, we set $\lambda \preccurlyeq \mu$ if and only if each positive integer i satisfies

$$\lambda_1 + \lambda_2 + \cdots + \lambda_i \leq \mu_1 + \mu_2 + \cdots + \mu_i. \tag{296}$$

Here, we set $\lambda_j := 0$ for each $j > k$, and we set $\mu_j := 0$ for each $j > \ell$.

(For example, for $n = 5$, we have $(2, 1, 1, 1) \preccurlyeq (2, 2, 1)$, since we have

$$\begin{gathered} 2 \leq 2, \\ 2 + 1 \leq 2 + 2, \\ 2 + 1 + 1 \leq 2 + 2 + 1, \\ 2 + 1 + 1 + 1 \leq 2 + 2 + 1 + 0, \\ 2 + 1 + 1 + 1 + 0 \leq 2 + 2 + 1 + 0 + 0, \end{gathered}$$

and so on. Note that there are infinitely many inequalities to be checked, but only finitely many of them are relevant, since both sides of (296) are essentially finite sums that stop growing at some point.)

(a) $\boxed{1}$ For any $n \geq 6$, find two partitions λ and μ of n satisfying neither $\lambda \preccurlyeq \mu$ nor $\mu \preccurlyeq \lambda$. (This shows that $\preccurlyeq$ is not a total order for $n \geq 6$.)

(b) $\boxed{2}$ Prove that two partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$ of n satisfy $\lambda \preccurlyeq \mu$ if and only if each $i \in \{1, 2, \ldots, k\}$ satisfies (296).

(c) $\boxed{2}$ Prove that two partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$ of n satisfy $\lambda \preccurlyeq \mu$ if and only if each $i \in \{1, 2, \ldots, \ell\}$ satisfies (296).

(d) $\boxed{4}$ Prove that two partitions λ and μ of n satisfy $\lambda \preccurlyeq \mu$ if and only if they satisfy $\mu^t \preccurlyeq \lambda^t$. (See Exercise A.3.1.1 for the definition of λ^t and μ^t.)

[**Note:** The partial order $\preccurlyeq$ is called the *dominance order* or the *majorization order*; it is rather important in the theory of symmetric functions.]

[**Hint:** It is helpful to identify a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ with the weakly decreasing essentially finite sequence $\widehat{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_k, 0, 0, 0, \ldots)$.]

Exercise A.3.1.10. For any two partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_\ell)$, we define two partitions $\lambda + \mu$ and $\lambda \sqcup \mu$ as follows:

- We let $\lambda + \mu$ be the partition $(\lambda_1 + \mu_1,\ \lambda_2 + \mu_2,\ \ldots,\ \lambda_m + \mu_m)$, where we set $m = \max\{k, \ell\}$, and where we set $\lambda_j := 0$ for each $j > k$, and where we set $\mu_j := 0$ for each $j > \ell$.
- We let $\lambda \sqcup \mu$ be the partition obtained by sorting the entries of the list $(\lambda_1, \lambda_2, \ldots, \lambda_k, \mu_1, \mu_2, \ldots, \mu_\ell)$ in weakly decreasing order.

For example, $(3,2,1) + (4,2) = (3+4,\ 2+2,\ 1+0) = (7,4,1)$ and $(3,2,1) \sqcup (4,2) = (4,3,2,2,1)$.

Let λ and μ be two partitions. Recall the definition of the transpose of a partition (Exercise A.3.1.1).

(a) $\boxed{2}$ Prove that $(\lambda \sqcup \mu)^t = \lambda^t + \mu^t$.

(b) $\boxed{2}$ Prove that $(\lambda + \mu)^t = \lambda^t \sqcup \mu^t$.

[**Hint:** Same as for Exercise A.3.1.9.]

A.3.2. Euler's pentagonal number theorem

Euler's pentagonal number theorem can be used freely in the following exercises.

Exercise A.3.2.1. (a) $\boxed{2}$ Prove that $p(n) \leq p(n-1) + p(n-2)$ for any $n > 0$.

(b) $\boxed{3}$ Prove that $p(n) \leq p(n-1) + p(n-2) - p(n-5)$ for any $n > 0$.

(c) $\boxed{2}$ Prove that $p(n) \geq p(n-1) + p(n-2) - p(n-5) - p(n-7)$ for any $n \in \mathbb{N}$.

(d) $\boxed{2}$ Use part **(a)** to obtain an upper bound for $p(n)$ in terms of Fibonacci numbers.

A.3.3. Jacobi's triple product identity

Exercise A.3.3.1. **(a)** $\boxed{3}$ Prove that

$$\prod_{m=1}^{\infty} \frac{1-x^m}{1+x^m} = \sum_{k\in\mathbb{Z}} (-1)^k x^{k^2}.$$

(b) $\boxed{3}$ Prove that

$$\prod_{m=1}^{\infty} \frac{1-x^{2m}}{1-x^{2m-1}} = \sum_{k\in\mathbb{N}} x^{k(k+1)/2}.$$

[**Hint:** Both times, start by substituting appropriate values for q and x in the Jacobi Triple Product Identity.]

Exercise A.3.3.2. $\boxed{4}$ Prove that

$$\prod_{n=1}^{\infty} \left(\left(1-u^n v^{n-1}\right) \left(1-u^{n-1}v^n\right) \left(1-u^n v^n\right) \right) = \sum_{k\in\mathbb{Z}} (-1)^k u^{k(k-1)/2} v^{k(k+1)/2}$$

in the FPS ring $K[[u,v]]$.

[**Hint:** This is the Jacobi Triple Product Identity after (or, better, before) a substitution.]

Exercise A.3.3.3. $\boxed{6}$ Prove that

$$\prod_{n=1}^{\infty} (1-x^n)^3 = \sum_{k=0}^{\infty} (-1)^k (2k+1) x^{k(k+1)/2} \qquad \text{in } K[[x]].$$

A.3.4. q-binomial coefficients

Exercise A.3.4.1. **(a)** $\boxed{1}$ Prove Proposition 4.4.10.

(b) $\boxed{3}$ Prove Theorem 4.4.12 **(b)**.

(c) $\boxed{3}$ Prove Theorem 4.4.13.

(d) $\boxed{2}$ Prove Theorem 4.4.17.

(e) $\boxed{1}$ Prove Proposition 4.4.18. (Don't forget the case $k > n$.)

Exercise A.3.4.2. **(a)** $\boxed{2}$ Prove Theorem 4.4.19 by induction on n.

(b) $\boxed{2}$ Prove Theorem 4.4.21.

Exercise A.3.4.3. $\boxed{4}$ Let $n, k \in \mathbb{N}$ satisfy $n \geq k$. Prove the following:

(a) The polynomial $\dbinom{n}{k}_q \in \mathbb{Z}[q]$ has degree $k(n-k)$.

(b) For each $i \in \{0, 1, \ldots, k(n-k)\}$, we have

$$\left[q^i\right] \dbinom{n}{k}_q = \left[q^{k(n-k)-i}\right] \dbinom{n}{k}_q .$$

(That is, the sequence of coefficients of this polynomial $\dbinom{n}{k}_q$ is palindromic.)

(c) We have $\dbinom{n}{k}_{q^{-1}} = q^{-k(n-k)} \dbinom{n}{k}_q$ in the Laurent polynomial ring $\mathbb{Z}[q^{\pm}]$.

Exercise A.3.4.4. Let us extend the definition of the q-integer $[n]_q$ (Definition 4.4.15 **(a)**) to the case when n is a negative integer as follows: If n is a negative integer, then we set

$$[n]_q := -q^{-1} - q^{-2} - \cdots - q^n = -\sum_{k=n}^{-1} q^k \in \mathbb{Z}[q^{\pm}] .$$

(This is a Laurent polynomial, not a polynomial any more.)

Furthermore, inspired by Theorem 4.4.17, let us extend the definition of $\dbinom{n}{k}_q$ to the case when n is a negative integer by setting

$$\dbinom{n}{k}_q = \frac{[n]_q [n-1]_q \cdots [n-k+1]_q}{[k]_q!} \qquad \text{for all } n \in \mathbb{Z} \text{ and } k \in \mathbb{N}$$

and

$$\dbinom{n}{k}_q = 0 \qquad \text{for all } n \in \mathbb{Z} \text{ and } k \notin \mathbb{N}.$$

The right hand sides of these two equalities are to be understood in the ring $\mathbb{Z}((q))$ of Laurent series. (From Theorem 4.4.17 and Convention 4.4.11, we know that this definition does not conflict with our existing definitions of $\dbinom{n}{k}_q$ for $n \in \mathbb{N}$.)

(a) $\boxed{1}$ Prove that $[n]_1 = n$ for any $n \in \mathbb{Z}$.

(b) $\boxed{1}$ Prove that $\dbinom{n}{k}_1 = \dbinom{n}{k}$ for any $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$.

(c) $\boxed{1}$ Prove that $[n]_q = \dfrac{1-q^n}{1-q}$ in the ring $\mathbb{Z}((q))$ of Laurent series for any $n \in \mathbb{Z}$.

(d) $\boxed{1}$ Prove that $[-n]_q = -q^{-n}[n]_q$ for any $n \in \mathbb{Z}$.

(e) $\boxed{1}$ Prove the *"q-upper negation formula"* (a q-analogue of Theorem 3.3.11): If $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$, then

$$\binom{-n}{k}_q = (-1)^k q^{kn-k(k-1)/2} \binom{k+n-1}{k}_q .$$

(f) $\boxed{1}$ Prove that $\dbinom{n}{k}_q \in \mathbb{Z}[q^{\pm}]$ (that is, $\dbinom{n}{k}_q$ is a Laurent polynomial, not just a Laurent series) for any $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$.

(g) $\boxed{2}$ Prove that Theorem 4.4.12 holds for any $n \in \mathbb{Z}$ (not just for positive integers n).

(h) $\boxed{1}$ Prove that Proposition 4.4.18 does **not** hold for negative n (in general).

Exercise A.3.4.5. Consider the ring $\mathbb{Z}[[z,q]]$ of FPSs in two indeterminates z and q. Let $n \in \mathbb{N}$.

(a) $\boxed{1}$ Prove that

$$\prod_{i=0}^{n-1} \left(1 + zq^i\right) = \sum_{k=0}^{n} q^{k(k-1)/2} \binom{n}{k}_q z^k.$$

(b) $\boxed{4}$ Prove that

$$\prod_{i=0}^{n-1} \frac{1}{1-zq^i} = \sum_{k\in\mathbb{N}} \binom{n+k-1}{k}_q z^k,$$

where we set $\dbinom{-1}{0}_q := 1$ (this is consistent with the definition in Exercise A.3.4.4). (Up to sign, this is a q-analogue of Proposition 3.3.12.)

Exercise A.3.4.6. $\boxed{5}$ Let $n \in \mathbb{N}$. Prove the *Gauss formula*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}_q = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ \left(1-q^1\right)\left(1-q^3\right)\left(1-q^5\right)\cdots\left(1-q^{n-1}\right), & \text{if } n \text{ is even.} \end{cases}$$

Exercise A.3.4.7. $\boxed{5}$ Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} q^k \binom{n}{k}_{q^2} = \left(1+q^1\right)\left(1+q^2\right)\cdots\left(1+q^n\right).$$

Exercise A.3.4.8. Prove the following q-analogues of the Vandermonde convolution identity:

(a) $\boxed{3}$ If $a, b \in \mathbb{N}$ and $n \in \mathbb{N}$, then

$$\binom{a+b}{n}_q = \sum_{k=0}^{n} q^{k(b-n+k)} \binom{a}{k}_q \binom{b}{n-k}_q.$$

(Note that the exponent $k(b-n+k)$ might occasionally be negative, but in those cases we have $\binom{b}{n-k}_q = 0$.)

(b) $\boxed{3}$ If $a, b \in \mathbb{N}$ and $n \in \mathbb{N}$, then

$$\binom{a+b}{n}_q = \sum_{k=0}^{n} q^{(a-k)(n-k)} \binom{a}{k}_q \binom{b}{n-k}_q.$$

(Note that the exponent $(a-k)(n-k)$ might occasionally be negative, but in those cases we have $\binom{a}{k}_q = 0$.)

Exercise A.3.4.9. $\boxed{3}$ Let $r, s, u, v \in \mathbb{Z}$ with $r > s > 0$. Prove that

$$\lim_{n\to\infty} \binom{rn+u}{sn+v}_q = \prod_{k=1}^{\infty} \frac{1}{1-q^k} \qquad \text{in } \mathbb{Z}[[q]].$$

(See Definition 3.13.2 for the meaning of "$\lim_{n\to\infty}$" used here.)

Exercise A.3.4.10. We shall work in the ring $(\mathbb{Z}[z^{\pm}])[[q]]$.

(a) $\boxed{4}$ Prove *MacMahon's identity*, which says that

$$\left(\prod_{i=1}^{m}\left(1+q^{2i-1}z\right)\right)\cdot\left(\prod_{j=1}^{n}\left(1+q^{2j-1}z^{-1}\right)\right) = \sum_{k=-n}^{m} q^{k^2}\binom{m+n}{k+n}_{q^2} z^k$$

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

(b) $\boxed{4}$ Recover Theorem 4.3.1 by taking the limit $m \to \infty$ and then $n \to \infty$. (This yields a new proof of Theorem 4.3.1.)

The following exercise does not explicitly involve q-binomial coefficients, but they can be used profitably in its solution:

Exercise A.3.4.11. We work in the ring $\mathbb{Z}[[z,q]]$ of FPSs in two indeterminates z and q.

(a) $\boxed{2}$ Prove that

$$\prod_{i=1}^{\infty}\left(1+zq^{i}\right)=\sum_{k\in\mathbb{N}}\frac{z^{k}q^{k(k+1)/2}}{(1-q^{1})(1-q^{2})\cdots(1-q^{k})}.$$

(b) $\boxed{2}$ Prove that

$$\prod_{i=1}^{\infty}\frac{1}{1-zq^{i}}=\sum_{k\in\mathbb{N}}\frac{z^{k}q^{k}}{(1-q^{1})(1-q^{2})\cdots(1-q^{k})}.$$

(c) $\boxed{5}$ Prove that

$$\prod_{i=1}^{\infty}\frac{1}{1-zq^{i}}=\sum_{k\in\mathbb{N}}\frac{z^{k}q^{k^{2}}}{((1-q^{1})(1-q^{2})\cdots(1-q^{k}))\cdot((1-zq^{1})(1-zq^{2})\cdots(1-zq^{k}))}.$$

[**Hint:** For part **(c)**, define the *h-index* $h(\lambda)$ of a partition λ to be the largest $i\in\mathbb{N}$ such that λ has at least i parts that are $\geq i$. For instance, $h(4,3,1,1)=2$ and $h(4,3,3,1)=3$. Note that $h(\lambda)$ is the size of the largest square that fits into the Young diagram of λ. What remains if this square is removed from the Young diagram of λ ? See also the Hirsch index.]

Exercise A.3.4.12. Let F be a finite field. Let $n\in\mathbb{N}$ and $k\in\mathbb{N}$. Prove the following:

(a) $\boxed{3}$ If W is a k-dimensional F-vector space, then

$$\begin{aligned}&(\#\text{ of }n\text{-tuples }(w_1,w_2,\ldots,w_n)\text{ of vectors in }W\text{ that span }W)\\&=(|F|^{n}-1)\cdot(|F|^{n}-|F|)\cdot\cdots\cdot\left(|F|^{n}-|F|^{k-1}\right)=\prod_{i=0}^{k-1}\left(|F|^{n}-|F|^{i}\right).\end{aligned}$$

(b) $\boxed{3}$ Let $m\in\mathbb{N}$. Then,

$$\begin{aligned}&\left(\#\text{ of }m\times n\text{-matrices }A\in F^{m\times n}\text{ satisfying }\operatorname{rank}A=k\right)\\&=\binom{m}{k}_{|F|}\cdot\underbrace{(|F|^{n}-1)\cdot(|F|^{n}-|F|)\cdot\cdots\cdot\left(|F|^{n}-|F|^{k-1}\right)}_{=\prod_{i=0}^{k-1}\left(|F|^{n}-|F|^{i}\right)}\\&=\binom{m}{k}_{|F|}\cdot\binom{n}{k}_{|F|}\cdot|F|^{k(k-1)/2}(|F|-1)^{k}[k]!_{|F|}.\end{aligned}$$

[**Hint:** For part **(a)**, what is the connection between injective linear maps and surjective linear maps (between finite-dimensional vector spaces)?]

Exercise A.3.4.13. $\boxed{3}$ Let $m, n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{m} \binom{m}{k}_q \binom{n}{k}_q q^{k(k-1)/2} (q-1)^k [k]!_q = q^{mn}.$$

[**Hint:** This is a polynomial identity in q, and there are infinitely many prime numbers. What does this suggest?]

The following exercise gives a way to derive Theorem 4.4.19 from Theorem 4.4.21:

Exercise A.3.4.14. Let L be a commutative ring, and let $a, b, q \in L$. (Note that if we let L be the polynomial ring $K[q]$, then this setting becomes the setting of Theorem 4.4.19.)

Consider the polynomial ring $L[u]$. Let A be the (noncommutative) L-algebra $\operatorname{End}_L(L[u])$ of all endomorphisms of the L-module $L[u]$. (Its multiplication is composition of endomorphisms. Note that $L[u]$ is a free L-module of infinite rank, with basis $(u^0, u^1, u^2, \ldots)$; thus, the elements of A can be viewed as $\infty \times \infty$-matrices with each column having only finitely many nonzero entries. But it is easier to just think of the elements of A as L-linear maps $L[u] \to L[u]$, just as we defined A.)

Let $\alpha \in A = \operatorname{End}_L(L[u])$ be the L-module endomorphism of $L[u]$ that satisfies

$$\alpha\left(u^i\right) = aq^i u^{i+1} \qquad \text{for any } i \in \mathbb{N}.$$

(Thus, α sends each polynomial $f \in L[u]$ to $au \cdot f[qu]$.)

Let $\beta \in A = \operatorname{End}_L(L[u])$ be the L-module endomorphism of $L[u]$ that satisfies

$$\beta\left(u^i\right) = bu^{i+1} \qquad \text{for any } i \in \mathbb{N}.$$

(Thus, β multiplies each polynomial $f \in L[u]$ by bu.)

(a) $\boxed{1}$ Prove that $\alpha\beta = q\beta\alpha$.

(b) $\boxed{2}$ Prove that $(\beta + \alpha)^k (1) = \left(aq^0 + b\right)\left(aq^1 + b\right) \cdots \left(aq^{k-1} + b\right) u^k$ for each $k \in \mathbb{N}$.

(c) $\boxed{2}$ Rederive Theorem 4.4.19 by applying Theorem 4.4.21 to β, α and q instead of a, b and ω.

The following exercise shows an application of q-binomial coefficients using a technique called the *roots of unity filter* (see also Exercise A.1.1.3 for a similar technique):

Exercise A.3.4.15. Let p be a prime. Let Ω be the set of all complex numbers z satisfying $z^p = 1$. It is well-known that

$$\Omega = \left\{ e^{2\pi i g/p} \mid g \in \{0, 1, \ldots, p-1\} \right\}$$

(where the letters e and i have the usual meanings they have in complex analysis) and, in particular, $|\Omega| = p$ and $1 \in \Omega$.

Let n be a positive integer.

(a) $\boxed{1}$ Prove that $\dbinom{np-1}{p-1}_\omega = 1$ for each $\omega \in \Omega \setminus \{1\}$.

(b) $\boxed{2}$ Prove that $\dbinom{np}{p}_\omega = n$ for each $\omega \in \Omega \setminus \{1\}$.

(c) $\boxed{1}$ Prove that $\sum\limits_{\omega \in \Omega} \omega^k = \begin{cases} p, & \text{if } p \mid k; \\ 0, & \text{if } p \nmid k \end{cases}$ for any $k \in \mathbb{N}$.

(d) $\boxed{3}$ Prove that

$$(\text{\# of subsets } S \text{ of } [np] \text{ satisfying } p \mid \operatorname{sum} S) = \frac{\dbinom{np}{p} + (p-1)\,n}{p}.$$

Here, $\operatorname{sum} S$ is defined as in Proposition 4.4.7 **(b)**.

[**Hint:** For part **(d)**, compute $\sum\limits_{\omega \in \Omega} \dbinom{np}{p}_\omega$ in two ways.]

[**Remark:** The claim of part **(d)** generalizes Problem 6 from the International Mathematical Olympiad 1995.]

A.4. Permutations

The notations of Chapter 5 shall be used here. In particular, if X is a set, then S_X shall mean the symmetric group of X; and if n is a nonnegative integer, then S_n shall mean the symmetric group $S_{[n]}$ of the set $[n] := \{1, 2, \ldots, n\}$.

A.4.1. Basic definitions

Exercise A.4.1.1. $\boxed{1}$ Let $n \in \mathbb{N}$ and $\sigma \in S_n$. What is the easiest way to obtain

(a) a two-line notation of σ^{-1} from a two-line notation of σ ?

(b) the one-line notation of σ^{-1} from the one-line notation of σ ?

(c) the cycle digraph of σ^{-1} from the cycle digraph of σ ?

A.4.2. Transpositions and cycles

Exercise A.4.2.1. Let X be a set. Prove the following:

(a) $\boxed{2}$ For any k distinct elements $i_1, i_2, \ldots, i_k$ of X, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \underbrace{t_{i_1,i_2} t_{i_2,i_3} \cdots t_{i_{k-1},i_k}}_{k-1 \text{ transpositions}}.$$

(b) $\boxed{1}$ For any k distinct elements $i_1, i_2, \ldots, i_k$ of X and any $\sigma \in S_X$, then

$$\sigma \operatorname{cyc}_{i_1,i_2,\ldots,i_k} \sigma^{-1} = \operatorname{cyc}_{\sigma(i_1),\sigma(i_2),\ldots,\sigma(i_k)}.$$

Definition A.4.1. Let X be a set. An *involution* of X means a map $f : X \to X$ that satisfies $f \circ f = \operatorname{id}$. Clearly, an involution is always a permutation, and equals its own inverse.

For example, the identity map id_X is an involution, and any transposition $t_{i,j} \in S_X$ is an involution, whereas k-cycles $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ with $k > 2$ are never involutions.

Exercise A.4.2.2. Let $n \in \mathbb{N}$. Let $w_0 \in S_n$ be the permutation that sends each $k \in [n]$ to $n+1-k$. Thus, w_0 is the permutation that "reflects" all numbers from 1 to n across the middle of the interval $[n]$. It is the unique strictly decreasing permutation of $[n]$. In one-line notation, w_0 is $(n, n-1, n-2, \ldots, 2, 1)$.

(a) $\boxed{1}$ Prove that w_0 is an involution of $[n]$.

(b) $\boxed{1}$ Prove that $w_0 = t_{1,n} t_{2,n-1} \cdots t_{k,n+1-k}$, where $k = \left\lfloor \dfrac{n}{2} \right\rfloor$.

(c) $\boxed{3}$ Prove that

$$\begin{aligned} w_0 &= \operatorname{cyc}_{1,2,\ldots,n} \operatorname{cyc}_{1,2,\ldots,n-1} \operatorname{cyc}_{1,2,\ldots,n-2} \cdots \operatorname{cyc}_1 \\ &= \operatorname{cyc}_1 \operatorname{cyc}_{2,1} \operatorname{cyc}_{3,2,1} \cdots \operatorname{cyc}_{n,n-1,\ldots,1}. \end{aligned}$$

Exercise A.4.2.3. Let p be a prime number. Let Z be the set of all p-cycles in the symmetric group S_p.

Let ζ be the specific p-cycle $\operatorname{cyc}_{1,2,\ldots,p} \in S_p$. Note that ζ has order p in the group S_p, and thus generates a cyclic subgroup $\langle \zeta \rangle$ of order p.

(a) $\boxed{2}$ Prove that a permutation $\sigma \in S_p$ satisfies $\sigma\zeta = \zeta\sigma$ if and only if $\sigma \in \langle \zeta \rangle$ (that is, if and only if σ is a power of ζ).

(b) $\boxed{2}$ Prove that $|\langle \zeta \rangle \cap Z| = p - 1$.

(c) $\boxed{1}$ Prove that the cyclic group $\langle \zeta \rangle$ acts on the set Z by conjugation:

$$\alpha \rightharpoonup \sigma = \alpha \sigma \alpha^{-1} \qquad \text{for any } \alpha \in \langle \zeta \rangle \text{ and } \sigma \in Z$$

(where the symbol "$\rightharpoonup$" means the action of a group G on a G-set X – i.e., we let $g \rightharpoonup x$ denote the result of a group element $g \in G$ acting on some $x \in X$).

(d) $\boxed{1}$ Find the fixed points of this action.

(e) $\boxed{1}$ Prove *Wilson's theorem* from elementary number theory, which states that

$$(p-1)! \equiv -1 \operatorname{mod} p.$$

A.4.3. Inversions, length and Lehmer codes

Exercise A.4.3.1. $\boxed{4}$ Prove Proposition 5.3.3.

Exercise A.4.3.2. Let $n \in \mathbb{N}$. Prove the following:

(a) $\boxed{1}$ We have $\ell\left(t_{i,j}\right) = 2\left|i-j\right| - 1$ for any distinct $i, j \in [n]$.

(b) $\boxed{2}$ We have $\ell\left(\operatorname{cyc}_{i+1,i+2,\ldots,i+k}\right) = k-1$ for any integers i and k with $0 \leq i < i+k \leq n$.

(c) $\boxed{4}$ We have $\ell\left(\operatorname{cyc}_{i_1,i_2,\ldots,i_k}\right) \geq k-1$ for any k distinct elements $i_1, i_2, \ldots, i_k \in [n]$.

(d) $\boxed{1}$ Are the k-cycles of the form $\operatorname{cyc}_{i+1,i+2,\ldots,i+k}$ the only k-cycles whose length is $k-1$?

Exercise A.4.3.3. Let $\sigma \in S_n$ and $i \in [n]$. Prove the following (using the notation of Definition 5.3.6 **(a)**):

(a) $\boxed{1}$ We have $\ell_i\left(\sigma\right) = \left|\left[\sigma\left(i\right)-1\right] \setminus \sigma\left(\left[i\right]\right)\right|$.

(b) $\boxed{1}$ We have $\ell_i\left(\sigma\right) = \left|\left[\sigma\left(i\right)-1\right] \setminus \sigma\left(\left[i-1\right]\right)\right|$.

(c) $\boxed{1}$ We have $\sigma\left(i\right) \leq i + \ell_i\left(\sigma\right)$.

(d) $\boxed{2}$ Assume that $i \in [n-1]$. We have $\sigma\left(i\right) > \sigma\left(i+1\right)$ if and only if $\ell_i\left(\sigma\right) > \ell_{i+1}\left(\sigma\right)$.

A.4.4. V-permutations

Exercise A.4.4.1. $\boxed{5}$ Let $n \in \mathbb{N}$. For each $r \in [n]$, let c_r denote the permutation $\operatorname{cyc}_{r,r-1,\ldots,2,1} \in S_n$. (Thus, $c_1 = \operatorname{cyc}_1 = \operatorname{id}$ and $c_2 = \operatorname{cyc}_{2,1} = s_1$.)

Let $G = \{g_1, g_2, \ldots, g_p\}$ be a subset of $[n]$, with $g_1 < g_2 < \cdots < g_p$. Let $\sigma \in S_n$ be the permutation $c_{g_1} c_{g_2} \cdots c_{g_p}$.

[**Example:** If $n = 6$ and $p = 2$ and $G = \{2, 5\}$, then $\sigma = c_2 c_5 = \operatorname{cyc}_{2,1} \operatorname{cyc}_{5,4,3,2,1}$. In one-line notation, this permutation σ is 521346.]

Prove the following:

(a) We have $\sigma(1) > \sigma(2) > \cdots > \sigma(p)$.

(b) We have $\sigma([p]) = G$.

(c) We have $\sigma(p+1) < \sigma(p+2) < \cdots < \sigma(n)$.

(Note that a chain of inequalities that involves less than two numbers is considered to be vacuously true. For example, Exercise A.4.4.1 **(c)** is vacuously true when $p = n - 1$ and also when $p = n$.)

Exercise A.4.4.2. $\boxed{8}$ Let $n \in \mathbb{N}$. Define the permutations c_r as in Exercise A.4.4.1.

Let $\sigma \in S_n$. We will use the notations from Definition 5.3.6.

(a) Prove that the following five statements are equivalent:

- *Statement 1:* We have $\sigma(1) > \sigma(2) > \cdots > \sigma(p)$ and $\sigma(p+1) < \sigma(p+2) < \cdots < \sigma(n)$ for some $p \in \{0, 1, \ldots, n\}$. (In other words, the one-line notation of σ is decreasing at first, then increasing.)
- *Statement 2:* We have $\sigma = c_{g_1} c_{g_2} \cdots c_{g_p}$ for some elements $g_1 < g_2 < \cdots < g_p$ of $[n]$.
- *Statement 3:* For each $i \in [n]$, the set $\sigma^{-1}([i])$ is an integer interval (i.e., there exist integers u and v such that $\sigma^{-1}([i]) = \{u, u+1, u+2, \ldots, v\}$).
- *Statement 4:* If $i, j, k \in [n]$ satisfy $i < j < k$, then we have $\sigma(i) > \sigma(j)$ or $\sigma(k) > \sigma(j)$.
- *Statement 5:* We have $\ell_1(\sigma) > \ell_2(\sigma) > \cdots > \ell_p(\sigma)$ and $\ell_{p+1}(\sigma) = \ell_{p+2}(\sigma) = \cdots = \ell_n(\sigma) = 0$ for some $p \in \{0, 1, \ldots, n\}$. (In other words, the n-tuple $L(\sigma)$ is strictly decreasing until it reaches 0, and then remains at 0.)

(b) Permutations $\sigma \in S_n$ satisfying the above five statements are known as "V-permutations" (as their plot looks somewhat like the letter "V": decreasing at first, then increasing).

Assume that $n > 0$. Prove that the # of V-permutations in S_n is 2^{n-1}.

[**Example:** If $n = 3$, then the V-permutations in S_n are (in one-line notation) 123 and 213 and 312 and 321.]

A.4.5. Fixed points

The next two exercises are concerned with the fixed points of maps (not only of permutations).

Definition A.4.2. Let X be a set. Let $f : X \to X$ be a map. Then:

(a) A *fixed point* of f means an $x \in X$ satisfying $f(x) = x$.

(b) We let $\operatorname{Fix} f$ denote the set of all fixed points of f. (This is the set $\{x \in X \mid f(x) = x\}$.)

Exercise A.4.5.1. $\boxed{4}$ Let X and Y be two finite sets. Let $f : X \to Y$ and $g : Y \to X$ be two maps. Prove that

$$|\operatorname{Fix}(f \circ g)| = |\operatorname{Fix}(g \circ f)|.$$

Exercise A.4.5.2. Let X be a finite set.

(a) $\boxed{4}$ Prove that each permutation $\sigma \in S_X$ is a composition of two involutions of X.

(b) $\boxed{2}$ Prove that each permutation $\sigma \in S_X$ is conjugate to its inverse σ^{-1} in the symmetric group S_X.

[**Hint:** For part **(a)**, it is easier to show the following stronger claim: If $\sigma \in S_X$ and $Y \subseteq \operatorname{Fix} \sigma$ and $p \in X \setminus Y$, then there exist two involutions $\alpha, \beta \in S_X$ such that $\sigma = \alpha \circ \beta$ and $Y \subseteq \operatorname{Fix} \alpha$ and $Y \cup \{p\} \subseteq \operatorname{Fix} \beta$.
For part **(b)**, you can use part **(a)**.]

A.4.6. More on inversions

The next two exercises concern the inversions of a permutation. They use the following definition:

Definition A.4.3. Let $n \in \mathbb{N}$. For every $\sigma \in S_n$, we let $\operatorname{Inv} \sigma$ denote the set of all inversions of σ.

We know from Corollary 5.3.20 **(b)** that any $n \in \mathbb{N}$ and any two permutations σ and τ in S_n satisfy the inequality $\ell(\sigma\tau) \leq \ell(\sigma) + \ell(\tau)$. In the following exercise, we will see when this inequality becomes an equality:

Exercise A.4.6.1. $\boxed{6}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ and $\tau \in S_n$.

(a) Prove that $\ell(\sigma\tau) = \ell(\sigma) + \ell(\tau)$ holds if and only if $\operatorname{Inv} \tau \subseteq \operatorname{Inv}(\sigma\tau)$.

(b) Prove that $\ell(\sigma\tau) = \ell(\sigma) + \ell(\tau)$ holds if and only if $\operatorname{Inv}\left(\sigma^{-1}\right) \subseteq \operatorname{Inv}\left(\tau^{-1}\sigma^{-1}\right)$.

(c) Prove that $\operatorname{Inv}\sigma \subseteq \operatorname{Inv}\tau$ holds if and only if $\ell(\tau) = \ell\left(\tau\sigma^{-1}\right) + \ell(\sigma)$.

(d) Prove that if $\operatorname{Inv}\sigma = \operatorname{Inv}\tau$, then $\sigma = \tau$.

(e) Prove that $\ell(\sigma\tau) = \ell(\sigma) + \ell(\tau)$ holds if and only if $(\operatorname{Inv}\sigma) \cap \left(\operatorname{Inv}\left(\tau^{-1}\right)\right) = \varnothing$.

Exercise A.4.6.1 **(d)** shows that if two permutations in S_n have the same set of inversions, then they are equal. In other words, a permutation in S_n is uniquely determined by its set of inversions. The next exercise shows what set of inversions a permutation can have:

Exercise A.4.6.2. $\boxed{7}$ Let $n \in \mathbb{N}$. Let $G = \left\{(i,j) \in \mathbb{Z}^2 \mid 1 \leq i < j \leq n\right\}$.

A subset U of G is said to be *transitive* if every $a, b, c \in [n]$ satisfying $(a,b) \in U$ and $(b,c) \in U$ also satisfy $(a,c) \in U$.

A subset U of G is said to be *inversive* if there exists a $\sigma \in S_n$ such that $U = \operatorname{Inv}\sigma$.

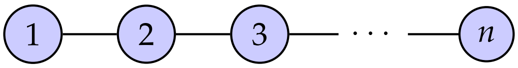
Let U be a subset of G. Prove that U is inversive if and only if both U and $G \setminus U$ are transitive.

A.4.7. When transpositions generate S_X

The next exercise uses a tiny bit of graph theory (the notion of connectedness of a graph):

Exercise A.4.7.1. $\boxed{5}$ Let X be a nonempty finite set. Let G be a loopless undirected graph with vertex set X. For each edge e of G, we let t_e denote the transposition $t_{i,j} \in S_X$, where i and j are the two endpoints of e. These transpositions t_e for all edges e of G will be called the *G-edge transpositions*.

Prove that the G-edge transpositions generate the symmetric group S_X if and only if the graph G is connected.

[**Example:** If G is the path graph 

on the vertex set $X = [n]$, then the G-edge transpositions are precisely the simple transpositions $s_1, s_2, \ldots, s_{n-1}$. In this case, the claim of this exercise becomes the claim of Corollary 5.3.22.]

A.4.8. Pattern avoidance

A warm-up exercise for this subsection:

Exercise A.4.8.1. Let $n \in \mathbb{N}$.

(a) $\boxed{1}$ Find the # of permutations $\sigma \in S_n$ such that each $i \in [n]$ satisfies $\sigma(i) \leq i + 1$.

(b) $\boxed{1}$ Find the # of permutations $\sigma \in S_n$ such that each $i \in [n]$ satisfies $i - 1 \leq \sigma(i)$.

(c) $\boxed{2}$ Find the # of permutations $\sigma \in S_n$ such that each $i \in [n]$ satisfies $i - 1 \leq \sigma(i) \leq i + 1$.

The next few exercises cover some of the most basic results in the theory of *pattern avoidance* (see [Bona12, Chapter 4] and [Kitaev11] for much more[148]). This can be viewed as one possible way of generalizing monotonicity (i.e., increasingness and decreasingness). We begin by defining some basic concepts:

Definition A.4.4. Let $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ be an arbitrary (finite) tuple. A *subsequence* of $\mathbf{t}$ means a tuple of the form $\left(t_{i_1}, t_{i_2}, \ldots, t_{i_m}\right)$, where $i_1, i_2, \ldots, i_m$ are m elements of $[n]$ satisfying $i_1 < i_2 < \cdots < i_m$.

Example A.4.5. Let $\mathbf{t} = (5, 1, 6, 2, 3, 4)$. Then, $(1, 3)$ and $(5, 6, 2)$ are subsequences of $\mathbf{t}$ (indeed, if we write $\mathbf{t}$ as $(t_1, t_2, \ldots, t_6)$, then $(1, 3) = (t_2, t_5)$ and $(5, 6, 2) = (t_1, t_3, t_4)$), whereas $(1, 5)$ and $(2, 1, 6)$ and $(1, 1, 6)$ are not.

Remark A.4.6. Let $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ be an arbitrary (finite) tuple. Then, the 1-tuple (t_i) is a subsequence of $\mathbf{t}$ for any $i \in [n]$. So is the empty 0-tuple $()$. Also, the tuple $\mathbf{t}$ itself is a subsequence of $\mathbf{t}$ (and is the only length-n subsequence of $\mathbf{t}$).

Next, we need to define the notion of *equally ordered tuples*. Roughly speaking, these are tuples of the same length that might differ in their values, but agree in the relative order of their values (e.g., if one tuple has a smaller value in position 2 than in position 5, then so does the other tuple). Here is the formal definition:

Definition A.4.7. Let $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ be two k-tuples of integers. We say that $\mathbf{a}$ and $\mathbf{b}$ are *equally ordered* (to each other) if for every pair $(i, j) \in [k] \times [k]$, we have the logical equivalence

$$\left(a_i < a_j\right) \iff \left(b_i < b_j\right).$$

This relation is clearly symmetric in $\mathbf{a}$ and $\mathbf{b}$ (that is, $\mathbf{a}$ and $\mathbf{b}$ are equally ordered if and only if $\mathbf{b}$ and $\mathbf{a}$ are equally ordered).

We agree that a k-tuple and an ℓ-tuple are never equally ordered when $k \neq \ell$.

[148] There is a yearly conference on this subject!

Example A.4.8. **(a)** The two triples $(3,1,6)$ and $(1,0,2)$ are equally ordered.

(b) The two quadruples $(3,1,1,2)$ and $(4,1,1,3)$ are equally ordered.

(c) The two triples $(3,1,2)$ and $(2,1,3)$ are not equally ordered (indeed, we have $3 < 2$, but we don't have $2 < 3$).

Now, we can define the notion of a *pattern* in a tuple:

Definition A.4.9. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ and $\mathbf{u} = (u_1, u_2, \ldots, u_m)$ be two tuples of integers.

A $\mathbf{u}$-*pattern* in $\mathbf{s}$ means a subsequence of $\mathbf{s}$ that is equally ordered to the tuple $\mathbf{u}$. (In particular, this subsequence must have the same length as $\mathbf{u}$.)

In the following, when we talk about $\mathbf{u}$-patterns, we will often write the tuple $\mathbf{u}$ without commas and parentheses. (For example, we shall abbreviate "$(2,3,1)$-pattern" as "231-pattern".)

Example A.4.10. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ be a tuple of integers. Let us see what $\mathbf{u}$-patterns in $\mathbf{s}$ mean for various specific tuples $\mathbf{u}$:

(a) A 21-pattern in $\mathbf{s}$ is a subsequence $\left(s_i, s_j\right)$ of $\mathbf{s}$ with $s_i > s_j$ (and, of course, $i < j$, by the definition of a subsequence). For example, the tuple $(4,5,2,1)$ has five 21-patterns (namely, $(4,2)$, $(4,1)$, $(5,2)$, $(5,1)$ and $(2,1)$).

(b) A 123-pattern in $\mathbf{s}$ is a subsequence $\left(s_i, s_j, s_k\right)$ with $s_i < s_j < s_k$ (and, of course, $i < j < k$, by the definition of a subsequence). For example, the tuple $(2,1,3,5)$ has two 123-patterns (namely, $(1,3,5)$ and $(2,3,5)$).

(c) A 231-pattern in $\mathbf{s}$ is a subsequence $\left(s_i, s_j, s_k\right)$ with $s_k < s_i < s_j$ (and, of course, $i < j < k$, by the definition of a subsequence). For example, the tuple $(1,2,5,1)$ has one 231-pattern (namely, $(2,5,1)$).

Finally, we can define *pattern avoidance*:

Definition A.4.11. Let $\mathbf{s}$ and $\mathbf{u}$ be two tuples of integers. We say that $\mathbf{s}$ is $\mathbf{u}$-*avoiding* if there is no $\mathbf{u}$-pattern in $\mathbf{s}$.

Example A.4.12. The tuple $(2,1,5,3,4)$ is

- not 123-avoiding, since it contains the 123-pattern $(1,3,4)$ (and also the 123-pattern $(2,3,4)$);
- not 132-avoiding, since it contains the 132-pattern $(1,5,3)$;
- not 321-avoiding, since it contains the 321-pattern $(5,3,4)$;
- 231-avoiding (check this!).

Example A.4.13. **(a)** A tuple $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ is 21-avoiding if and only if it is weakly increasing (i.e., satisfies $s_1 \leq s_2 \leq \cdots \leq s_n$). Indeed, a 21-pattern in $\mathbf{s}$ is a subsequence $\left(s_i, s_j\right)$ of $\mathbf{s}$ with $s_i > s_j$; thus, the non-existence of such 21-patterns is equivalent to $s_1 \leq s_2 \leq \cdots \leq s_n$.

(b) Likewise, a tuple $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ is 12-avoiding if and only if it is weakly decreasing (i.e., satisfies $s_1 \geq s_2 \geq \cdots \geq s_n$).

Finally, our concept of pattern avoidance can be extended from tuples to permutations in the most obvious manner:

Definition A.4.14. Let $\mathbf{u}$ be a tuple of integers. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. We say that the permutation σ is $\mathbf{u}$-*avoiding* if the OLN of σ (that is, the n-tuple $(\sigma(1), \sigma(2), \ldots, \sigma(n))$) is $\mathbf{u}$-avoiding.

Example A.4.15. Let $n \in \mathbb{N}$. The only 21-avoiding permutation $\sigma \in S_n$ is the identity permutation $\operatorname{id} \in S_n$ (since it is the only permutation whose OLN is weakly increasing). Likewise, the only 12-avoiding permutation $\sigma \in S_n$ is the permutation $w_0 \in S_n$ from Exercise A.4.2.2.

After all this build-up, we can now study $\mathbf{u}$-avoidance for more complicated patterns $\mathbf{u}$ than 21 and 12:

Exercise A.4.8.2. $\boxed{6}$ Let $n \in \mathbb{N}$. Let c_n denote the n-th Catalan number (from Example 2 in Section 3.1).

(a) Prove that

$$(\text{\# of 132-avoiding permutations in } S_n) = c_n.$$

(b) Prove that

$$(\text{\# of 231-avoiding permutations in } S_n) = c_n.$$

(c) Prove that

$$(\text{\# of 213-avoiding permutations in } S_n) = c_n.$$

(d) Prove that

$$(\text{\# of 312-avoiding permutations in } S_n) = c_n.$$

[**Hint:** Easy bijections show that parts **(a)**, **(b)**, **(c)** and **(d)** are equivalent. For part **(b)**, proceed recursively: Assume that $n > 0$, and let $\sigma \in S_n$, and let $i = \sigma^{-1}(n)$. Show that the permutation σ is 231-avoiding if and only if the two tuples $(\sigma(1), \sigma(2), \ldots, \sigma(i-1))$ and $(\sigma(i+1), \sigma(i+2), \ldots, \sigma(n))$ are 231-avoiding and satisfy $\{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\} = \{1, 2, \ldots, i-1\}$ and $\{\sigma(i+1), \sigma(i+2), \ldots, \sigma(n)\} = \{i, i+1, \ldots, n-1\}$. This yields a recursive equation for the # of 231-avoiding permutations in S_n.]

Exercise A.4.8.3. $\boxed{8}$ Let $n \in \mathbb{N}$. Let c_n denote the n-th Catalan number (from Example 2 in Section 3.1).

(a) Prove that

$$(\text{\# of 123-avoiding permutations in } S_n) = c_n.$$

(b) Prove that

$$(\text{\# of 321-avoiding permutations in } S_n) = c_n.$$

[**Hint:** Consider any 321-avoiding permutation $\sigma \in S_n$. A *record* of σ means a value $\sigma(i)$ for some $i \in [n]$ satisfying

$$\sigma(i) > \sigma(j) \qquad \text{for all } j \in [i-1].$$

(Equivalently, it is an entry in the OLN of σ is larger than all entries further left.) Let $b_1, b_2, \ldots, b_k$ be the records of a permutation $\sigma \in S_n$, written in increasing order (or, equivalently, in the order of their appearance in the OLN of σ). (For example, if $\sigma = 14672385$, then these are $1, 4, 6, 7, 8$.) Argue first that the OLN of σ becomes weakly increasing when all records are removed from it. (For example, 14672385 becomes 235 this way.) Write the OLN of σ in the form

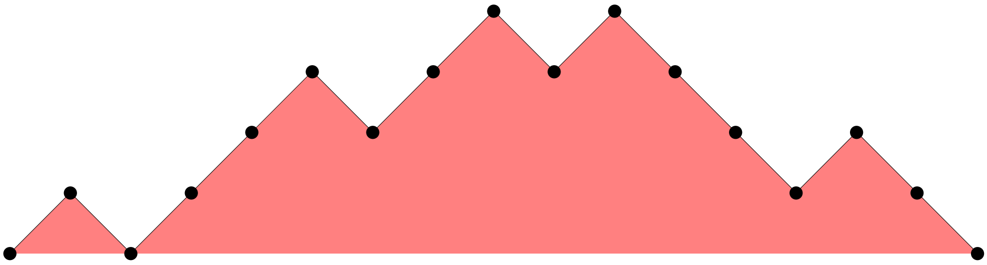
$$(\sigma(1), \sigma(2), \ldots, \sigma(n)) = \left(b_1, \underbrace{\ldots}_{\substack{\text{some } i_1\\ \text{entries}}}, b_2, \underbrace{\ldots}_{\substack{\text{some } i_2\\ \text{entries}}}, \ldots, b_{k-1}, \underbrace{\ldots}_{\substack{\text{some } i_{k-1}\\ \text{entries}}}, b_k, \underbrace{\ldots}_{\substack{\text{some } i_k\\ \text{entries}}}\right),$$

where $i_1, i_2, \ldots, i_k \in \mathbb{N}$. Set $c_i := b_i - b_{i-1}$ for each $i \in [k]$, where $b_0 := 0$. Now, define $B(\sigma)$ to be the Dyck path

$$N^{c_1} S^{i_1+1} N^{c_2} S^{i_2+1} \cdots N^{c_k} S^{i_k+1},$$

where an "N^j" means j consecutive NE-steps, and where an "S^j" means j consecutive SE-steps. For example, $\sigma = 14672385$ leads to

$$\begin{aligned} & B(\sigma) \\ & = N^1 S^1 N^3 S^1 N^2 S^1 N^1 S^3 N^1 S^2 \\ & = NSNNNSNNSNSSSNSS \end{aligned}$$

$=$ 

Prove that the map

$$B : \{321\text{-avoiding permutations in } S_n\} \to \{\text{Dyck paths from } (0,0) \text{ to } (2n,0)\},$$
$$\sigma \mapsto B(\sigma)$$

is well-defined and a bijection. (In proving surjectivity, don't forget to check that the b_i's really are the records of σ !)]

Exercises A.4.8.2 and A.4.8.3 can be combined into a single statement, which says that for any $\tau \in S_3$ and any $n \in \mathbb{N}$, the # of $(\tau(1), \tau(2), \tau(3))$-avoiding permutations in S_n equals the Catalan number c_n, independently of τ. The independence appears almost too good to be true. Parts of this miracle survive even for $\tau \in S_4$; for example, for any $n \in \mathbb{N}$, we have

$$\begin{aligned}&(\text{\# of 4132-avoiding permutations in } S_n)\\ &= (\text{\# of 3142-avoiding permutations in } S_n)\end{aligned}$$

(a result of Stankova [Stanko94, Theorem 3.1]), but this number does not equal the # of 1324-avoiding permutations in S_n (in general), nor does it have any simple formula. A Wikipedia page collects known results about these and similar numbers.

We state a few simple results about permutations avoiding several patterns:

Definition A.4.16. Let $\mathbf{u}$ and $\mathbf{v}$ be two tuples of integers. A permutation in S_n (or a tuple of integers) is said to be $(\mathbf{u}, \mathbf{v})$*-avoiding* if and only if it is both $\mathbf{u}$-avoiding and $\mathbf{v}$-avoiding. Similarly we define $(\mathbf{u}, \mathbf{v}, \mathbf{w})$*-avoiding* permutations (where $\mathbf{u}$, $\mathbf{v}$ and $\mathbf{w}$ are three tuples of integers).

Exercise A.4.8.4. Let n be a positive integer.

(a) $\boxed{3}$ Prove that

$$(\text{\# of } (231, 321)\text{-avoiding permutations in } S_n) = 2^{n-1}.$$

(b) $\boxed{2}$ Prove that

$$(\text{\# of } (132, 231)\text{-avoiding permutations in } S_n) = 2^{n-1}.$$

(c) $\boxed{2}$ Prove that

$$(\text{\# of } (123, 321)\text{-avoiding permutations in } S_n) = 0 \qquad \text{if } n > 4.$$

(d) $\boxed{2}$ Prove that

$$(\text{\# of } (231, 321, 312)\text{-avoiding permutations in } S_n) = f_{n+1},$$

where $(f_0, f_1, f_2, \ldots)$ is the Fibonacci sequence (as in Section 3.1).

(e) $\boxed{2}$ Prove that

$$(\text{\# of } (123, 132, 231) \text{-avoiding permutations in } S_n) = n.$$

[**Hint:** In parts **(a)**, **(b)** and **(d)**, the permutations you are counting have already appeared in one of the previous problems under a different guise.]

A.4.9. The cycle decomposition

Exercise A.4.9.1. $\boxed{1}$ Let X be a finite set. Let σ be a permutation of X. Prove that the order of σ in the symmetric group S_X equals the lcm of the lengths of all cycles of σ.

Exercise A.4.9.2. $\boxed{3}$ Let X be a finite set. Let σ and τ be two permutations of X. Prove that σ and τ are conjugate in the symmetric group S_X if and only if the cycle lengths partition of σ equals the cycle lengths partition of τ.

The disjoint cycle decomposition of a permutation allows us to define its *reflection length*, which is an analogue of the Coxeter length that we have defined in Definition 5.3.1 **(b)**:

Exercise A.4.9.3. Let X be a finite set. Let $n = |X|$.

The *reflection length* (aka *absolute length*) of a permutation $\sigma \in S_X$ is defined to be $n - i$, where i is the number of cycles (including the 1-cycles) in the disjoint cycle decomposition of σ. (For example, any k-cycle in S_X has reflection length $k - 1$, since it has 1 cycle of length k and $n - k$ cycles of length 1.) The reflection length of a permutation $\sigma \in S_X$ is denoted by $\ell_r(\sigma)$.

Prove the following:

(a) $\boxed{1}$ For any $\sigma \in S_X$, we have $\ell_r\left(\sigma^{-1}\right) = \ell_r(\sigma)$.

(b) $\boxed{1}$ If σ and τ are two conjugate elements in the group S_X, then $\ell_r(\sigma) = \ell_r(\tau)$.

(c) $\boxed{3}$ For any $\sigma \in S_X$ and any two distinct elements i and j of X, we have

$$\ell_r\left(\sigma t_{i,j}\right) = \ell_r\left(t_{i,j}\sigma\right) = \begin{cases} \ell_r(\sigma) + 1, & \text{if we don't have } i \overset{\sigma}{\sim} j; \\ \ell_r(\sigma) - 1, & \text{if } i \overset{\sigma}{\sim} j. \end{cases}$$

Here, the notation "$i \overset{\sigma}{\sim} j$" means "$i$ and j belong to the same cycle of σ" (that is, "there exists some $p \in \mathbb{N}$ such that $i = \sigma^p(j)$").

(d) $\boxed{2}$ If $\sigma \in S_X$, then the number $\ell_r(\sigma)$ is the smallest $p \in \mathbb{N}$ such that we can write σ as a composition of p transpositions.

(e) $\boxed{2}$ For any $\sigma \in S_X$ and $\tau \in S_X$, we have $\ell_r(\sigma\tau) \leq \ell_r(\sigma) + \ell_r(\tau)$.

(f) $\boxed{2}$ For any $\sigma \in S_X$ and $\tau \in S_X$, we have $\ell_r(\sigma\tau) \equiv \ell_r(\sigma) + \ell_r(\tau) \mod 2$.

(g) $\boxed{1}$ If $\sigma \in S_X$, then $\ell_r(\sigma) \leq \ell(\sigma)$.

Exercise A.4.9.4. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Define $\ell_r(\sigma)$ as in Exercise A.4.9.3 (setting $X = [n]$).

(a) $\boxed{4}$ Prove that there is a unique n-tuple $(i_1, i_2, \ldots, i_n) \in [1] \times [2] \times \cdots \times [n]$ such that

$$\sigma = t_{1,i_1} \circ t_{2,i_2} \circ \cdots \circ t_{n,i_n}.$$

Here, we define $t_{i,i}$ to be the identity permutation $\operatorname{id} \in S_n$ for each $i \in [n]$.

(b) $\boxed{3}$ Consider this n-tuple $(i_1, i_2, \ldots, i_n)$. Prove that

$$\ell_r(\sigma) = (\text{\# of all } k \in [n] \text{ satisfying } i_k \neq k).$$

Exercise A.4.9.5. Fix a commutative ring K and a nonnegative integer $n \in \mathbb{N}$. For each $\sigma \in S_n$, we define the *permutation matrix* P_σ be the $n \times n$-matrix

$$([i = \sigma(j)])_{i,j \in [n]} \in K^{n \times n}.$$

(This is the $n \times n$-matrix whose (i,j)-th entry is $[i = \sigma(j)]$, where we are using the notation of Definition 4.1.5.) For instance, if $n = 4$ and $\sigma = 3124$ in one-line notation, then

$$P_\sigma = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

(a) $\boxed{1}$ Let $\operatorname{GL}_n(K)$ be the group of all invertible $n \times n$-matrices over K. Prove that the map

$$S_n \to \operatorname{GL}_n(K),$$
$$\sigma \mapsto P_\sigma$$

is a group homomorphism.

(b) $\boxed{2}$ Assuming that K is a field, prove that each $\sigma \in S_n$ satisfies $\operatorname{rank}(P_\sigma - I_n) = \ell_r(\sigma)$, where $\ell_r(\sigma)$ is defined as in Exercise A.4.9.3 (setting $X = [n]$). (Here, I_n denotes the $n \times n$ identity matrix.)

(c) $\boxed{7}$ Assuming that K is a field, prove that two permutations $\sigma, \tau \in S_n$ are conjugate in the group S_n if and only if their permutation matrices P_σ and P_τ are similar (i.e., conjugate in the group $\operatorname{GL}_n(K)$).

(d) $\boxed{2}$ Prove the claim of part **(c)** more generally if K is any nontrivial commutative ring.

[**Hint:** For part **(c)**, it helps to show that the cycle lengths partition of a permutation σ can be uniquely recovered if one knows the number of cycles of each of its powers $\sigma^1, \sigma^2, \sigma^3, \ldots$.]

A.4.10. Reduced words

In this subsection, we shall take a closer look at how permutations in the symmetric groups S_n can be represented as products of simple transpositions s_i. Most exercises here are particular cases of standard results about Coxeter groups (see, e.g., [BjoBre05] and [Bourba02] for introductions), but it is worth seeing them in the special yet rather intuitive setting of symmetric groups.

We recall Definition 5.2.3.

Definition A.4.17. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$.

(a) A *Coxeter word* for σ shall mean a tuple $(i_1, i_2, \ldots, i_k) \in [n-1]^k$ satisfying $\sigma = s_{i_1} s_{i_2} \cdots s_{i_k}$.

(b) A *reduced word* for σ shall mean a Coxeter word for σ that has the smallest length among all Coxeter words for σ.

Note that Theorem 5.3.17 **(a)** shows that any permutation $\sigma \in S_n$ has a Coxeter word. Furthermore, Theorem 5.3.17 **(b)** says that the length $\ell(\sigma)$ of a permutation $\sigma \in S_n$ is the smallest length of a Coxeter word for σ. Thus, a reduced word for a permutation $\sigma \in S_n$ is the same as a Coxeter word for σ that has length $\ell(\sigma)$. (This is the reason for the name "length".)

Example A.4.18. Let $n = 5$, and let $\sigma \in S_5$ be the permutation whose OLN is 32415. Then, $\sigma = s_1 s_3 s_2 s_1$; thus, $(1,3,2,1)$ is a Coxeter word for σ. Other Coxeter words for σ are $(3,1,2,1)$ and $(3,2,1,2)$ and $(1,3,1,1,2,1)$ and $(3,1,2,3,1,3)$. The reduced words for σ are $(1,3,2,1)$ and $(3,1,2,1)$ and $(3,2,1,2)$.

Note that each permutation $\sigma \in S_n$ has finitely many reduced words, but infinitely many Coxeter words (unless $n \leq 1$). The identity permutation id has only one reduced word – namely, the 0-tuple $()$ – but usually many Coxeter words, such as $(1,2,3,3,2,1)$.

We shall now study the combinatorics of Coxeter and reduced words of a permutation $\sigma \in S_n$ in more depth. First, let us view them from a different perspective:

Definition A.4.19. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. A *sorting sequence* for σ shall mean a sequence $(\sigma_0, \sigma_1, \ldots, \sigma_k)$ of permutations $\sigma_i \in S_n$ with the property that $\sigma_0 = \sigma$ and $\sigma_k = \mathrm{id}$ and that for each $i \in [k]$, the permutation σ_i is obtained from σ_{i-1} by swapping two consecutive entries $\sigma_{i-1}(h)$ and $\sigma_{i-1}(h+1)$ into the correct order (i.e., $\sigma_{i-1}(h) > \sigma_{i-1}(h+1)$, but $\sigma_i(h) < \sigma_i(h+1)$).

Thus, intuitively, a sorting sequence for σ is a way of sorting its OLN (i.e., the list $\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n)$) into increasing order by repeatedly swapping two out-of-order consecutive entries. For example, if $n = 5$, and if $\sigma \in S_5$ is the permutation whose OLN is 32415, then

$$(32415,\ 32145,\ 31245,\ 13245,\ 12345)$$

is a sorting sequences of σ (one of three such sequences).

Exercise A.4.10.1. $\boxed{2}$ Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Find a bijection between $\{\text{reduced words for } \sigma\}$ and $\{\text{sorting sequences for } \sigma\}$.

Exercise A.4.10.2. $\boxed{1}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $(i_1, i_2, \ldots, i_k)$ be a reduced word for σ. Let $u, v \in \{0, 1, \ldots, k\}$ be such that $u \leq v$. Prove that $(i_{u+1}, i_{u+2}, \ldots, i_v)$ is a reduced word for $s_{i_{u+1}} s_{i_{u+2}} \cdots s_{i_v}$.

Exercise A.4.10.3. $\boxed{2}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $k \in [n-1]$. Prove that σ has a reduced word whose last entry is k if and only if $\sigma(k) > \sigma(k+1)$.

Exercise A.4.10.4. $\boxed{4}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $u, v \in [n-1]$. Assume that σ has a reduced word whose last entry is u. Assume further that σ has a reduced word whose last entry is v. Prove the following:

(a) If $|u - v| > 1$, then σ has a reduced word whose last two entries are u and v (in this order).

(b) If $|u - v| = 1$, then σ has a reduced word whose last three entries are u, v, u (in this order).

Let us now discuss some ways to transform Coxeter words. For instance:

- If a tuple of the form $(\ldots, 2, 5, \ldots)$ (that is, a tuple that has two adjacent entries 2 and 5) is a Coxeter word for some permutation $\sigma \in S_n$, then the tuple $(\ldots, 5, 2, \ldots)$ (that is, the result of swapping these two adjacent entries) is a Coxeter word for the same permutation σ, since Proposition 5.2.5 **(b)** yields $s_2 s_5 = s_5 s_2$.
- If a tuple of the form $(\ldots, 2, 3, 2, \ldots)$ is a Coxeter word for some permutation $\sigma \in S_n$, then the tuple $(\ldots, 3, 2, 3, \ldots)$ (that is, the result of replacing the three adjacent entries $2, 3, 2$ by $3, 2, 3$, while leaving all remaining entries unchanged) is a Coxeter word for the same permutation σ, since Proposition 5.2.5 **(c)** yields $s_2 s_3 s_2 = s_3 s_2 s_3$.

- If a Coxeter word for $\sigma \in S_n$ has two adjacent entries that are equal, then we can remove these two entries and still have a Coxeter word for σ, since Proposition 5.2.5 **(a)** yields $s_i s_i = s_i^2 = \operatorname{id}$ for each $i \in [n-1]$.

Generalizing these three observations, we obtain the following ways to change a Coxeter word:

Definition A.4.20. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$.

Given a Coxeter word $\mathbf{i} = (i_1, i_2, \ldots, i_k)$ for σ, we can obtain other Coxeter words for σ by the following three kinds of transformations:

(a) We can pick two adjacent entries i_u and i_{u+1} of $\mathbf{i}$ that satisfy $|i_u - i_{u+1}| > 1$, and swap them (that is, replace the u-th and $(u+1)$-st entries of $\mathbf{i}$ by i_{u+1} and i_u, respectively). This is called a *commutation move*, and results in a new Coxeter word for σ, since Proposition 5.2.5 **(b)** yields $s_{i_u} s_{i_{u+1}} = s_{i_{u+1}} s_{i_u}$.

For example, we can use such a move to transform the Coxeter word $(1,2,3,1,2)$ into $(1,2,1,3,2)$.

(b) We can pick three adjacent entries i_u, i_{u+1} and i_{u+2} of $\mathbf{i}$ that satisfy $i_u = i_{u+2} = i_{u+1} \pm 1$ (by which we mean that we have either $i_u = i_{u+2} = i_{u+1} + 1$ or $i_u = i_{u+2} = i_{u+1} - 1$), and replace these three entries by i_{u+1}, i_u and i_{u+1}, respectively. This is called a *braid move*, and results in a new Coxeter word for σ, since we have $s_{i_u} s_{i_{u+1}} \underbrace{s_{i_{u+2}}}_{=s_{i_u}} = s_{i_u} s_{i_{u+1}} s_{i_u} = s_{i_{u+1}} s_{i_u} s_{i_{u+1}}$ by Proposition 5.2.5 **(c)**.

For example, we can use such a move to transform the Coxeter word $(1,2,1,3,2)$ into $(2,1,2,3,2)$, and we can use another such move to transform this result further into $(2,1,3,2,3)$.

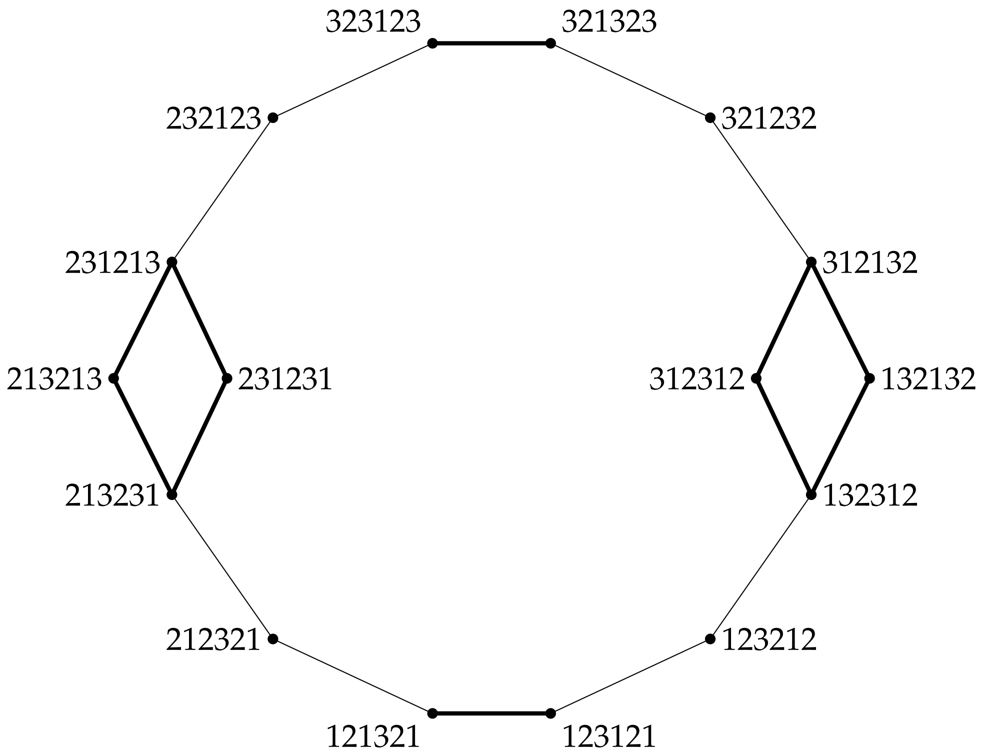
(c) We can pick two adjacent entries i_u and i_{u+1} of $\mathbf{i}$ that are equal, and remove both of them from $\mathbf{i}$. This is called a *contraction move*, and results in a new Coxeter word for σ, since we have $s_{i_u} \underbrace{s_{i_{u+1}}}_{=s_{i_u}} = s_{i_u} s_{i_u} = s_{i_u}^2 = \operatorname{id}$ by Proposition 5.2.5 **(a)**.

For example, we can use such a move to transform the Coxeter word $(3,2,2,1)$ into $(3,1)$.

Of course, these transformations can only be applied to a Coxeter word when the respective requirements are met. For example, none of these transformations can be applied to the Coxeter word $(1,2)$, since it has neither two adjacent entries i_u and i_{u+1} that satisfy $|i_u - i_{u+1}| > 1$, nor three adjacent entries i_u, i_{u+1} and i_{u+2} that satisfy $i_u = i_{u+2} = i_{u+1} \pm 1$, nor two adjacent entries i_u and i_{u+1} that are equal. On the other hand, we can apply any of the three kinds of transformation to the Coxeter word $(4,1,2,1,2,2,4,4)$, and we even have multiple choices for each of them (e.g., we can apply a braid move to replace the "1,2,1" by "2,1,2", but we can also apply a braid move to replace the "2,1,2" by "1, 2, 1" instead). Thus, starting with a single Coxeter word, we obtain a whole tapestry of Coxeter words by applying moves to it. Note that each commutation move and each braid move can be undone by a move of the same kind, while contraction moves cannot be undone.

We notice that commutation moves and braid moves don't change the length of a Coxeter word. Thus, if they are applied to a reduced word, they result in another reduced word.

Example A.4.21. Let $n = 4$, and let $\sigma \in S_4$ be the permutation whose OLN is 4321. It is easy to see that $(1, 2, 1, 3, 2, 1)$ is a reduced word for σ. Omitting commas and parentheses, we shorten this reduced word to 121321. By repeatedly applying commutation moves and braid moves, we can transform this reduced word into 212321, then further into 213231, then into 231231, and so on, and in other directions too (as there are often several moves available). Let us draw the result as a graph, with the nodes being all the reduced words that we obtain, and the edges signifying braid moves and commutation moves (the thick edges stand for commutation moves):



It turns out that **each** reduced word for σ appears as a node on this graph. In other words, each reduced word for σ can be obtained from 121321 by a sequence of commutation moves and braid moves. This is not a coincidence, but a general result, known as *Matsumoto's theorem for the symmetric group*:

Exercise A.4.10.5. $\boxed{6}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $\mathbf{i}$ and $\mathbf{j}$ be two reduced words for σ. Prove that $\mathbf{i}$ can be transformed into $\mathbf{j}$ by a sequence of commutation moves and braid moves.

[**Hint:** Induct on $\ell(\sigma)$.]

The graph in Example A.4.21 is furthermore bipartite; better yet, any cycle has an even # of thick edges and an even # of thin edges. This, too, is not a coincidence:

Exercise A.4.10.6. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $\mathbf{i}$ be a reduced word for σ. Assume that we have transformed $\mathbf{i}$ into itself by a sequence of commutation moves and braid moves.

(a) $\boxed{3}$ Prove that the # of braid moves in this sequence must be even.

(b) $\boxed{7}$ Prove that the # of commutation moves in this sequence must be even.

By throwing contraction moves into the mix, we can furthermore reduce non-reduced Coxeter words:

Exercise A.4.10.7. $\boxed{6}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Let $\mathbf{i}$ be a Coxeter word for σ, and let $\mathbf{j}$ be a reduced word for σ. Prove that $\mathbf{i}$ can be transformed into $\mathbf{j}$ by a sequence of commutation moves, braid moves and contraction moves.

How many reduced words does a given permutation $\sigma \in S_n$ have? For most σ, there is no nice formula for the answer. However, in at least one specific case, a surprising (and deep) formula exists, which I am here mentioning less as a reasonable exercise than as a curiosity:

Exercise A.4.10.8. $\boxed{50}$ Let $n \in \mathbb{N}$. Define the permutation $w_0 \in S_n$ as in Exercise A.4.2.2. (Note that the σ in Example A.4.21 is the w_0 for $n = 4$.)

Prove that the # of reduced words for w_0 is

$$\frac{\dbinom{n}{2}!}{\prod\limits_{i=1}^{n}(2n-2i+1)^{i-1}} = \binom{n}{2}! \cdot \prod_{1 \leq i < j \leq n} \frac{2}{i+j-1}.$$

($\boxed{2}$ Prove the equality sign here.)

This number, incidentally, is the largest # of reduced words that a permutation in S_n can have. On the other extreme (both of the # of reduced words and the difficulty of the proof), here is a characterization of permutations that have a unique reduced word:

Exercise A.4.10.9. $\boxed{3}$ Let n be a positive integer. Let $\sigma \in S_n$. Prove that there is only one reduced word for σ if and only if σ has the form $\operatorname{cyc}_{i,i+1,i+2,\ldots,j}$ or $\operatorname{cyc}_{j,j-1,j-2,\ldots,i}$ for some $i, j \in [n]$ satisfying $i \leq j$. (If $i = j$, then these cycles are just id.)

There is a connection between braid moves and pattern avoidance (Exercise A.4.8.2):

Exercise A.4.10.10. $\boxed{4}$ Let $n \in \mathbb{N}$. Let $\sigma \in S_n$. Prove that σ is 321-avoiding if and only if every two reduced words for σ can be transformed into each other by a sequence of commutation moves (without using any braid moves).

As an application of reduced words, the following group-theoretical characterization of the symmetric group S_n easily follows:

Exercise A.4.10.11. $\boxed{3}$ Let $n \in \mathbb{N}$. Prove that the group S_n is isomorphic to the group with generators $g_1, g_2, \ldots, g_{n-1}$ and relations

$$\begin{aligned} g_i^2 &= 1 && \text{for all } i \in [n-1]\,; \\ g_i g_j &= 1 && \text{for all } i, j \in [n-1] \text{ satisfying } |i-j| > 1; \\ g_i g_{i+1} g_i &= g_{i+1} g_i g_{i+1} && \text{for all } i \in [n-2]\,. \end{aligned}$$

(The isomorphism sends each g_i to $s_i \in S_n$.)

This is known as the *Coxeter-Moore presentation* of S_n.

A.4.11. Descents

Descents are one of the most elementary features of a permutation $\sigma \in S_n$: they are just the positions at which σ decreases (from that position to the next). Formally, they are defined as follows:

Definition A.4.22. Let $n \in \mathbb{N}$. Let $\sigma \in S_n$ be a permutation.

(a) A *descent* of σ means an $i \in [n-1]$ such that $\sigma(i) > \sigma(i+1)$.

(b) The *descent set* of σ is defined to be the set of all descents of σ. This set is denoted by $\operatorname{Des} \sigma$.

Example A.4.23. The permutation $\sigma \in S_7$ with OLN 3146275 has descents 1 (since $\sigma(1) > \sigma(2)$) and 4 (since $\sigma(4) > \sigma(5)$) and 6 (since $\sigma(6) > \sigma(7)$). Thus, it has descent set $\operatorname{Des} \sigma = \{1, 4, 6\}$.

Exercise A.4.11.1. $\boxed{2}$ Let $n \in \mathbb{N}$.

(a) How many $\sigma \in S_n$ have exactly 0 descents?

(b) How many $\sigma \in S_n$ have exactly 1 descent?

(c) How many $\sigma \in S_n$ have exactly $n-1$ descents?

(d) Prove that the # of all $\sigma \in S_n$ satisfying $1 \in \operatorname{Des} \sigma$ (that is, $\sigma(1) > \sigma(2)$) is $\frac{n!}{2}$. (Here, we assume that $n \geq 2$.)

(e) Prove that the # of all $\sigma \in S_n$ satisfying $1, 2 \in \operatorname{Des} \sigma$ (that is, $\sigma(1) > \sigma(2) > \sigma(3)$) is $\frac{n!}{6}$. (Here, we assume that $n \geq 3$.)

(f) How many $\sigma \in S_n$ satisfy $1, 3 \in \operatorname{Des} \sigma$ (that is, $\sigma(1) > \sigma(2)$ and $\sigma(3) > \sigma(4)$) ? (Here, we assume that $n \geq 4$.)

The following exercise generalizes parts **(d)**, **(e)** and **(f)** of Exercise A.4.11.1:

Exercise A.4.11.2. Let $n \in \mathbb{N}$. Let I be a subset of $[n-1]$. Write I in the form $I = \{c_1, c_2, \ldots, c_k\}$ with $c_1 < c_2 < \cdots < c_k$. Set $c_0 := 0$ and $c_{k+1} := n$. For each $i \in [k+1]$, set $d_i := c_i - c_{i-1}$. Note that the $k+1$ numbers $d_1, d_2, \ldots, d_{k+1}$ are precisely the lengths of the intervals into which the elements of I subdivide the interval $[0, n]$.

(a) $\boxed{3}$ Prove that

$$(\text{\# of } \sigma \in S_n \text{ satisfying } \operatorname{Des} \sigma \subseteq I) = \frac{n!}{d_1! d_2! \cdots d_{k+1}!}.$$

(b) $\boxed{5}$ Let us use the notations from Definition 4.4.15 **(b)**. Prove that

$$\sum_{\substack{\sigma \in S_n; \\ \operatorname{Des} \sigma \subseteq I}} q^{\ell(\sigma)} = \frac{[n]_q!}{[d_1]_q! [d_2]_q! \cdots [d_{k+1}]_q!} \qquad \text{in the ring } \mathbb{Z}[q].$$

Note that Exercise A.4.11.2 **(b)** generalizes both Exercise A.4.11.2 **(a)** (obtained by setting $q = 1$) and Proposition 5.3.5 (obtained by setting $I = [n-1]$ and $q = x$).

What about permutations $\sigma \in S_n$ satisfying $\operatorname{Des} \sigma = I$ rather than $\operatorname{Des} \sigma \subseteq I$? See Exercise A.5.4.3 further below for this.

Meanwhile, let us connect descents with Eulerian polynomials:

Exercise A.4.11.3. $\boxed{5}$ Let n be a positive integer. Consider the polynomials $A_m \in \mathbb{Z}[x]$ defined for all $m \in \mathbb{N}$ in Exercise A.2.6.2. Prove that

$$\sum_{\sigma \in S_n} x^{|\operatorname{Des} \sigma| + 1} = A_n \qquad \text{in the ring } \mathbb{Z}[x].$$

(For example, for $n = 4$, we have $\sum\limits_{\sigma \in S_4} x^{|\operatorname{Des} \sigma|+1} = x + 11x^2 + 11x^3 + x^4 = A_4$.)

A.4.12. Identities in the group algebra $\mathbb{Z}[S_n]$

TODO: This section is to be added.

A.5. Alternating sums, signed counting and determinants

The notations of Chapter 6 shall be used here.

A.5.1. Cancellations in alternating sums

Exercise A.5.1.1. $\boxed{3}$ Prove a generalization of Lemma 6.1.4 in which f is only required to be a bijection, not an involution, but the assumption "$\operatorname{sign} I = 0$ for all $I \in \mathcal{X}$ satisfying $f(I) = I$" is replaced by the stronger assumption "$\operatorname{sign} I = 0$ for all $I \in \mathcal{X}$ and all **odd** $k \in \mathbb{N}$ satisfying $f^k(I) = I$".

Exercise A.5.1.2. Recall the concepts of Dyck words and Dyck paths defined in Example 2 in Section 3.1.

Let $n \in \mathbb{N}$.

If $w \in \{0,1\}^{2n}$ is a $2n$-tuple, and if $k \in \{0,1,\ldots,2n\}$, then we define the *k-height* $h_k(w)$ of w to be the number

$$(\text{\# of 1's among the first } k \text{ entries of } w) \\ - (\text{\# of 0's among the first } k \text{ entries of } w).$$

If w is a Dyck word, then this k-height $h_k(w)$ is a nonnegative integer.

[For example, if $n = 4$ and $w = (1,0,0,1)$, then $h_3(w) = 1 - 2 = -1 < 0$, which shows that w is not a Dyck word.]

Furthermore, if $w \in \{0,1\}^{2n}$ is a $2n$-tuple, then we define the *area* $\operatorname{area}(w)$ of w to be the number

$$\operatorname{area}(w) := \sum_{k=0}^{2n} h_k(w),$$

and we define the *sign* $\operatorname{sign}(w)$ of w to be the number $(-1)^{(\operatorname{area}(w)-n)/2}$ (we will soon see that this is well-defined).

[For example, if $n = 5$ and $w = (1,1,0,1,1,0,0,0,1,0)$, then

$$\begin{aligned}\operatorname{area}(w) &= \sum_{k=0}^{10} h_k(w) \\ &= \underbrace{h_0(w)}_{=0} + \underbrace{h_1(w)}_{=1} + \underbrace{h_2(w)}_{=2} + \underbrace{h_3(w)}_{=1} + \underbrace{h_4(w)}_{=2} + \underbrace{h_5(w)}_{=3} \\ &\qquad + \underbrace{h_6(w)}_{=2} + \underbrace{h_7(w)}_{=1} + \underbrace{h_8(w)}_{=0} + \underbrace{h_9(w)}_{=1} + \underbrace{h_{10}(w)}_{=0} \\ &= 0+1+2+1+2+3+2+1+0+1+0 = 13\end{aligned}$$

and $\operatorname{sign}(w) = (-1)^{(\operatorname{area}(w)-n)/2} = (-1)^{(13-5)/2} = 1$. The names "$k$-height" and "area" are not accidental: If w is a Dyck word, then the "heights" $h_0(w), h_1(w), \ldots, h_{2n}(w)$ really are the heights (i.e., the y-coordinates) of the points on the Dyck path corresponding to the Dyck word w; furthermore, the number $\operatorname{area}(w)$ really is the area of the "mountain range" under the Dyck path.]

(a) $\boxed{1}$ Prove that any $w \in \{0,1\}^{2n}$ satisfies $(\operatorname{area}(w) - n)/2 \in \mathbb{Z}$ (so that $(-1)^{(\operatorname{area}(w)-n)/2}$ really is well-defined).

(b) $\boxed{2}$ Prove that a $2n$-tuple $w \in \{0,1\}^{2n}$ is a Dyck word of length $2n$ if and only if it satisfies

$$h_{2i-1}(w) \geq 0 \qquad \text{for all } i \in \{1,2,\ldots,n\}$$

and $h_{2n}(w) = 0$.

(c) $\boxed{4}$ Recall the Catalan numbers $c_0, c_1, c_2, \ldots$ as introduced in Section 3.1. Assume that n is a positive integer. Prove that

$$\sum_{\substack{w \text{ is a Dyck word} \\ \text{of length } 2n}} \operatorname{sign}(w) = \begin{cases} (-1)^{(n-1)/2} c_{(n-1)/2}, & \text{if } n \text{ is odd;} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

[**Hint:** In part **(c)**, find a sign-reversing involution on a certain set of Dyck words of length $2n$ that preserves all the "odd heights" $h_1(w), h_3(w), \ldots, h_{2n-1}(w)$ while changing one of the "even heights" $h_k(w)$ by 1.]

The next exercise is not about alternating sums, but rather about proving the q-Lucas theorem (Theorem 6.1.7):

Exercise A.5.1.3. Let K be a field. Let d be a positive integer. Let ω be a primitive d-th root of unity in K.

(a) $\boxed{2}$ Prove that $\dbinom{d}{k}_{\omega} = 0$ for each $k \in \{1, 2, \ldots, d-1\}$.

Now, let A be a noncommutative K-algebra, and let $a, b \in A$ be such that $ba = \omega ab$.

(b) $\boxed{1}$ Prove that $(a+b)^d = a^d + b^d$.

(c) $\boxed{3}$ Prove that a^d and b^d belong to the center of A. (The *center* of A is defined to be the subring $\{u \in A \mid uv = vu \text{ for all } v \in A\}$ of A.)

(d) $\boxed{5}$ Prove Theorem 6.1.7.

[**Hint:** For part **(a)**, show that $\dbinom{n}{k}_q = \dfrac{[n]_q}{[k]_q} \dbinom{n-1}{k-1}_q$ for all $n > 0$ and $k > 0$. For part **(d)**, first construct a noncommutative K-algebra A and two elements $a, b \in A$ satisfying $ba = \omega ab$ and such that all the monomials $a^i b^j$ are K-linearly independent. Use Exercise A.3.4.14 for this. In this K-algebra, expand both sides of $(a+b)^n = \left((a+b)^q\right)^d (a+b)^r$. Alternatively, there is a commutative approach using Theorem 4.4.19.]

A.5.2. The principles of inclusion and exclusion

Exercise A.5.2.1. $\boxed{3}$ Let $n \in \mathbb{N}$. Prove that $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k} (n-k)^{n+1} = \dbinom{n+1}{2} \cdot n!$.

The next exercise is concerned with the derangement numbers D_n from Definition 6.2.4.

Exercise A.5.2.2. (a) $\boxed{1}$ Prove that $D_n = nD_{n-1} + (-1)^n$ for all $n \geq 1$.

(b) $\boxed{1}$ Prove that $D_n = (n-1)(D_{n-1} + D_{n-2})$ for all $n \geq 2$.

(c) $\boxed{2}$ Prove that $n! = \sum\limits_{k=0}^{n} \dbinom{n}{k} D_{n-k}$ for all $n \in \mathbb{N}$.

(d) $\boxed{1}$ Show that $\sum\limits_{n \in \mathbb{N}} \dfrac{D_n}{n!} x^n = \dfrac{\exp[-x]}{1-x}$ in the FPS ring $\mathbb{Q}[[x]]$.

Exercise A.5.2.3. $\boxed{3}$ Reprove Theorem 3.9.8 using the PIE.

Exercise A.5.2.4. $\boxed{4}$ For any $n, m \in \mathbb{N}$, we define a polynomial $Z_{m,n} \in \mathbb{Z}[x]$ by

$$Z_{m,n} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \left(x^{n-k} - 1\right)^m.$$

Prove that $Z_{m,n} = Z_{n,m}$ for all $m, n \in \mathbb{N}$.

Exercise A.5.2.5. Let n be a positive integer. Let $a_1, a_2, \ldots, a_n$ be any n integers.

(a) $\boxed{4}$ Show that

$$\max\left\{a_1, a_2, \ldots, a_n\right\} = \sum_{k=1}^{n} \left(-1\right)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \min\left\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\right\}.$$

(b) $\boxed{2}$ More generally: Show that

$$F\left(\max\left\{a_1, a_2, \ldots, a_n\right\}\right) = \sum_{k=1}^{n} \left(-1\right)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} F\left(\min\left\{a_{i_1}, a_{i_2}, \ldots, a_{i_k}\right\}\right)$$

for any function $F : \mathbb{Z} \to \mathbb{R}$.

The following exercise is about a sequence of rather useful identities, sometimes known as the *polarization identities*:

Exercise A.5.2.6. Let $n \in \mathbb{N}$. Let A be a commutative ring. Let $v_1, v_2, \ldots, v_n \in A$ and $w \in A$. Prove the following:

(a) $\boxed{4}$ For each $m \in \mathbb{N}$, we have

$$\sum_{I \subseteq [n]} \left(-1\right)^{n-|I|} \left(w + \sum_{i \in I} v_i\right)^m = \sum_{\substack{(i_1, i_2, \ldots, i_m) \in \{0,1,\ldots,n\}^m; \\ [n] \subseteq \{i_1, i_2, \ldots, i_m\}}} v_{i_1} v_{i_2} \cdots v_{i_m},$$

where we set $v_0 := w$.

(b) $\boxed{1}$ For each $m \in \{0, 1, \ldots, n-1\}$, we have

$$\sum_{I \subseteq [n]} \left(-1\right)^{n-|I|} \left(w + \sum_{i \in I} v_i\right)^m = 0.$$

(c) $\boxed{1}$ We have

$$\sum_{I \subseteq [n]} \left(-1\right)^{n-|I|} \left(w + \sum_{i \in I} v_i\right)^n = n! v_1 v_2 \cdots v_n.$$

(d) $\boxed{2}$ We have

$$\sum_{I \subseteq [n]} \left(-1\right)^{n-|I|} \left(\sum_{i \in I} v_i - \sum_{i \in [n] \setminus I} v_i\right)^n = 2^n n! v_1 v_2 \cdots v_n.$$

Exercise A.5.2.7. $\boxed{5}$ Let A and B be two finite sets. Let R be a subset of $A \times B$. For any subset X of A, we define $M(X)$ to be the set

$$\{b \in B \mid \text{there exists some } x \in X \text{ such that } (x,b) \in R\}.$$

For any subset Y of B, we define $N(Y)$ to be the set

$$\{a \in A \mid \text{there exists some } y \in Y \text{ such that } (a,y) \in R\}.$$

Prove that

$$\sum_{\substack{X \subseteq A; \\ M(X)=B}} (-1)^{|X|} = \sum_{\substack{Y \subseteq B; \\ N(Y)=A}} (-1)^{|Y|}.$$

[**Remark:** Those familiar with graph theory can think of A, B and R as forming a bipartite graph (with vertex set $A \sqcup B$ and edge set R). In that case, $M(X)$ is the "neighbor set" of X (that is, the set of all vertices that have at least one neighbor in X), and likewise $N(Y)$ is the "neighbor set" of Y.]

Exercise A.5.2.8. $\boxed{5}$ Let $n > 1$ be an integer. Consider n people standing in a circle. Each of them looks down at someone else's feet (i.e., at the feet of one of the other $n-1$ persons). A bell sounds, and every person (simultaneously) looks up at the eyes of the person whose feet they have been ogling. If two people make eye contact, they scream. Show that the probability that no one screams is

$$\sum_{k=0}^{n} (-1)^k \frac{n(n-1)\cdots(n-2k+1)}{(n-1)^{2k} \cdot 2^k \cdot k!}.$$

Here is a combinatorial restatement of the question (if you prefer not to deal with probabilities): A pair (i,j) of elements of $[n]$ is said to *scream* at a map $f : [n] \to [n]$ if it satisfies $f(i) = j$ and $f(j) = i$. A map $f : [n] \to [n]$ is *silent* if no pair $(i,j) \in [n] \times [n]$ screams at f. Prove that the # of all silent maps $f : [n] \to [n]$ is

$$\sum_{k=0}^{n} (-1)^k \frac{n(n-1)\cdots(n-2k+1)}{2^k \cdot k!} (n-1)^{n-2k}.$$

The following two exercises show some applications of the methods of Chapter 6 to graph theory.

Exercise A.5.2.9. Let G be a finite undirected graph with vertex set V and edge set E. Fix $n \in \mathbb{N}$.

An *n-coloring* of G means a map $c : V \to [n]$. If $c : V \to [n]$ is an n-coloring, then we regard the values $c(v)$ of c as the "colors" of the respective vertices v.

An n-coloring c of G is said to be *proper* if there exists no edge of G whose two endpoints v and w satisfy $c(v) = c(w)$. (In other words, an n-coloring of G is said to be proper if and only if there is no edge whose two endpoints have the same color.)

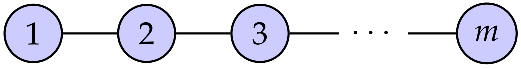
Let $\chi_G(n)$ denote the # of proper n-colorings of G.

(a) $\boxed{5}$ Prove that

$$\chi_G(n) = \sum_{F \subseteq E} (-1)^{|F|} n^{\operatorname{conn}(V,F)},$$

where $\operatorname{conn}(V,F)$ denotes the # of connected components of the graph with vertex set V and edge set F.

This shows, in particular, that $\chi_G(n)$ is a polynomial function in n. (The corresponding polynomial is known as the *chromatic polynomial* of G.)

(b) $\boxed{1}$ Find an explicit formula for $\chi_G(n)$ if G is a path graph  with m vertices.

(c) $\boxed{2}$ Find an explicit formula for $\chi_G(n)$ if G is a cycle graph with m vertices.

Exercise A.5.2.10. $\boxed{7}$ Let G be an undirected graph with vertex set V and edge set E. Fix a vertex $v \in V$.

Given any subset F of E, we define an *F-path* to be a path of G whose edges all belong to F.

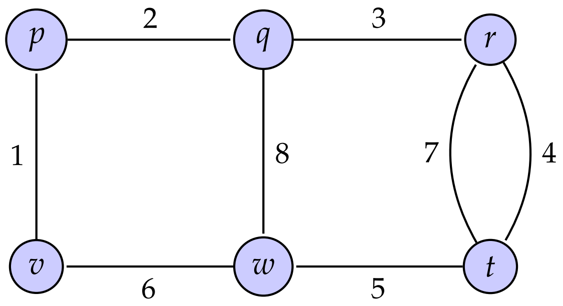
A subset F of E is said to *infect* an edge $e \in E$ if there is an F-path leading from v to some endpoint of e. (Note that this is automatically satisfied if v is an endpoint of e, since the empty path is always an F-path.)

A subset F of E is said to be *pandemic* if it infects each edge $e \in E$.

Prove that

$$\sum_{\substack{F \subseteq E \text{ is} \\ \text{pandemic}}} (-1)^{|F|} = [E = \varnothing].$$

[**Example:** Let G be the following graph:



(where the vertex v is the vertex labelled v). Then, for example, the set $\{1, 2\} \subseteq E$ infects edges $1, 2, 3, 6, 8$ (but none of the other edges). The set $\{1, 2, 5\}$ infects the same edges as $\{1, 2\}$ (indeed, the additional edge 5 does not increase its infectiousness, since it is not on any $\{1, 2, 5\}$-path from v). The set $\{1, 2, 3\}$ infects every edge other than 5. The set $\{1, 2, 3, 4\}$ infects each edge, and thus is pandemic.]

Exercise A.5.2.11. $\boxed{3}$ Let K be a commutative ring. Let $n \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1\leq i\leq n,\ 1\leq j\leq n} \in K^{n\times n}$ be an $n \times n$-matrix. Then, the *permanent* per A of A is defined to be the element

$$\sum_{\sigma\in S_n} a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

of K (where S_n is the n-th symmetric group). Prove the *Ryser formula*

$$\operatorname{per} A = (-1)^n \sum_{I\subseteq[n]} (-1)^{|I|} \prod_{j=1}^{n} \sum_{i\in I} a_{i,j}.$$

The following exercise is a variant of Theorem 6.2.10:

Exercise A.5.2.12. $\boxed{2}$ Let S be a finite set. Let A be any additive abelian group.

For each subset I of S, let a_I and b_I be two elements of A.

Assume that

$$b_I = \sum_{J\subseteq I} (-1)^{|J|} a_J \qquad \text{for all } I \subseteq S.$$

Then, prove that we also have

$$a_I = \sum_{J\subseteq I} (-1)^{|J|} b_J \qquad \text{for all } I \subseteq S.$$

The next exercise is an analogue of Exercise A.5.2.12 with sets replaced by numbers:

Exercise A.5.2.13. $\boxed{2}$ Let A be any additive abelian group. Let $(a_0, a_1, \ldots, a_n)$ and $(b_0, b_1, \ldots, b_n)$ be two $(n+1)$-tuples of elements of A. Assume that

$$b_m = \sum_{i=0}^{m} (-1)^i \binom{m}{i} a_i \qquad \text{for all } m \in \{0, 1, \ldots, n\}.$$

Prove that we also have

$$a_m = \sum_{i=0}^{m} (-1)^i \binom{m}{i} b_i \qquad \text{for all } m \in \{0, 1, \ldots, n\}.$$

[**Hint:** There is a direct proof, but it is perhaps neater to derive this from Exercise A.5.2.12.]

[**Remark:** The $(n+1)$-tuple $(b_0, b_1, \ldots, b_n)$ is called the *binomial transform* of $(a_0, a_1, \ldots, a_n)$.]

The next few exercises show some ways of generalizing the Principle of Inclusion and Exclusion (in its original form – Theorem 6.2.1). The first one replaces the question "how many elements of U belongs to none of the n subsets $A_1, A_2, \ldots, A_n$" by "how many elements of U belong to exactly k of the n subsets $A_1, A_2, \ldots, A_n$":

Exercise A.5.2.14. $\boxed{4}$ Let $n \in \mathbb{N}$, and let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Let $k \in \mathbb{N}$. Let

$$S_k := \{u \in U \ \mid \ \text{the \# of all } i \in [n] \text{ satisfying } u \in A_i \text{ is } k\}.$$

Show that

$$|S_k| = \sum_{I \subseteq [n]} (-1)^{|I|-k} \binom{|I|}{k} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I).$$

Exercise A.5.2.15. $\boxed{5}$ Let $n \in \mathbb{N}$, and let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Let $m \in \mathbb{N}$.

(a) For each $u \in U$, let $c(u)$ be the # of all $i \in [n]$ satisfying $u \in A_i$. Show that

$$\sum_{\substack{I \subseteq [n];\\ |I| \leq m}} (-1)^{|I|} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I)$$
$$= (-1)^m \sum_{u \in U} \binom{c(u)-1}{m}.$$

(b) Conclude the *Bonferroni inequalities*, which say that

$$\sum_{\substack{I \subseteq [n];\\ |I| \leq m}} (-1)^{m-|I|} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I) \geq 0$$

if $U = A_1 \cup A_2 \cup \cdots \cup A_n$.

Exercise A.5.2.16. (a) $\boxed{4}$ Find a common generalization of Exercise A.5.2.14

and Exercise A.5.2.15 that has the form

$$\sum_{\substack{I\subseteq[n];\\ |I|\leq m}} (-1)^{|I|} \binom{|I|}{k} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I)$$
$$= \sum_{u\in U} \underbrace{\cdots}_{\text{some expression involving } c(u)} .$$

(b) $\boxed{2}$ Generalize this further by including weights on the elements of U (similarly to how Theorem 6.2.9 generalizes Theorem 6.2.1).

The next exercise generalizes Theorem 6.2.9 in a similar way as q-binomial coefficients generalize binomial coefficients:

Exercise A.5.2.17. **(a)** $\boxed{4}$ Let $n \in \mathbb{N}$, and let U be a finite set. Let $A_1, A_2, \ldots, A_n$ be n subsets of U. Let K be any commutative ring. Let $w : U \to K$ be any map (i.e., let $w(u)$ be an element of K for each $u \in U$). Let $q \in K$. Prove that

$$\sum_{u\in U} (1+q)^{(\text{\# of } i\in[n] \text{ satisfying } u\in A_i)}\, w(u) = \sum_{I\subseteq[n]} q^{|I|} \sum_{\substack{u\in U;\\ u\in A_i \text{ for all } i\in I}} w(u)$$

in K.

(b) $\boxed{1}$ Derive Theorem 6.2.9 as a particular case of part **(a)**.

(c) $\boxed{2}$ Prove that each $n \in \mathbb{N}$ satisfies

$$\sum_{\sigma\in S_n} q^{|\operatorname{Fix}\sigma|} = \sum_{k=0}^{n} \frac{n!}{k!} (q-1)^k$$

in the polynomial ring $\mathbb{Z}[q]$. (See Definition A.4.2 for the definition of $\operatorname{Fix}\sigma$.)

Next comes another counting problem that can be solved in many ways:

Exercise A.5.2.18. $\boxed{3}$ Let A be an additive abelian group (with its neutral element denoted by 0). Let $n \in \mathbb{N}$. Show that

$$\left(\text{\# of } n\text{-tuples } (a_1, a_2, \ldots, a_n) \in (A \setminus \{0\})^n \text{ such that } a_1 + a_2 + \cdots + a_n = 0\right)$$
$$= \frac{(|A|-1)^n + (-1)^n (|A|-1)}{|A|}.$$

Next comes a generalization of Theorem 4.1.13:

Exercise A.5.2.19. $\boxed{3}$ Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

Let $p_{\operatorname{odd},k}(n)$ be the # of partitions of n that have exactly k distinct even parts. (For instance, the partition $(7, 5, 4, 4, 3, 2)$ has exactly 2 distinct even parts, namely 4 and 2.)

Let $p_{\operatorname{dist},k}(n)$ be the # of partitions λ of n that have exactly k numbers appear in λ more than once (in the sense that there are exactly k distinct integers i such that i appears more than once in λ). (For instance, the partition $(7, 4, 2, 2, 1, 1, 1)$ has exactly 2 numbers appear more than once, namely 2 and 1.)

Prove that

$$p_{\operatorname{odd},k}(n) = p_{\operatorname{dist},k}(n).$$

A.5.3. Determinants

We fix a commutative ring K.

Exercise A.5.3.1. $\boxed{3}$ Let n be a positive integer. Let $a_1, a_2, \ldots, a_n \in K$ and $b_1, b_2, \ldots, b_{n-1} \in K$ and $c_1, c_2, \ldots, c_{n-1} \in K$. Let A be the $n \times n$-matrix

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 & c_1 \\ 0 & a_2 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_{n-1} & c_{n-1} \\ b_1 & b_2 & \cdots & b_{n-1} & a_n \end{pmatrix}.$$

(This is the matrix whose (i, j)-th entry is $\begin{cases} a_i, & \text{if } i = j; \\ b_j, & \text{if } i = n \text{ and } j \neq n; \\ c_i, & \text{if } i \neq n \text{ and } j = n; \\ 0, & \text{if } i \neq n \text{ and } j \neq n \text{ and } i \neq j \end{cases}$ for all $i \in [n]$ and $j \in [n]$.) Prove that

$$\det A = a_1 a_2 \cdots a_n - \sum_{i=1}^{n-1} b_i c_i \prod_{\substack{j \in [n-1]; \\ j \neq i}} a_j.$$

Exercise A.5.3.2. $\boxed{3}$ Let $n \in \mathbb{N}$. Let A be an $n \times n$-matrix. Let $b_1, b_2, \ldots, b_n$ be n elements of K. Prove that

$$\sum_{k=1}^{n} \det\left(\left(A_{i,j} b_i^{[j=k]} \right)_{1 \leq i \leq n,\ 1 \leq j \leq n} \right) = (b_1 + b_2 + \cdots + b_n) \det A$$

(where we are using Definition A.1.5). Equivalently (rewritten in a friendlier but longer form): Prove that

$$\det\begin{pmatrix} A_{1,1}b_1 & A_{1,2} & \cdots & A_{1,n} \\ A_{2,1}b_2 & A_{2,2} & \cdots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n,1}b_n & A_{n,2} & \cdots & A_{n,n} \end{pmatrix} + \det\begin{pmatrix} A_{1,1} & A_{1,2}b_1 & \cdots & A_{1,n} \\ A_{2,1} & A_{2,2}b_2 & \cdots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n,1} & A_{n,2}b_n & \cdots & A_{n,n} \end{pmatrix}$$
$$+\cdots+\det\begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,n}b_1 \\ A_{2,1} & A_{2,2} & \cdots & A_{2,n}b_2 \\ \vdots & \vdots & \ddots & \vdots \\ A_{n,1} & A_{n,2} & \cdots & A_{n,n}b_n \end{pmatrix}$$
$$= (b_1+b_2+\cdots+b_n)\det\begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,n} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n,1} & A_{n,2} & \cdots & A_{n,n} \end{pmatrix}.$$

Exercise A.5.3.3. Let n be a positive integer. Let $A \in K^{n\times n}$ be an $n \times n$-matrix.

(a) $\boxed{4}$ Prove that the equality

$$\det\left(\left(A_{i,j}A_{n,n} - A_{i,n}A_{n,j}\right)_{1\le i\le n-1,\ 1\le j\le n-1}\right) = A_{n,n}^{n-2}\cdot\det A$$

holds if the element $A_{n,n}$ of K is invertible.

(b) $\boxed{2}$ Prove that this equality also holds if $n \geq 2$ (whether or not $A_{n,n}$ is invertible).

[**Hint:** For part **(a)**, observe that $A_{i,j}A_{n,n} - A_{i,n}A_{n,j} = A_{n,n}\cdot\left(A_{i,j} - \dfrac{A_{i,n}}{A_{n,n}}A_{n,j}\right)$.]

The following two exercises give some applications of determinants:

Exercise A.5.3.4. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n \in K$ and $b_1, b_2, \ldots, b_n \in K$.

(a) $\boxed{2}$ Use the Cauchy–Binet identity (Theorem 6.4.18, applied to appropriate $2 \times n$- and $n \times 2$-matrices) to show that

$$\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right) - \left(\sum_{k=1}^{n} a_k b_k\right)^2 = \sum_{1\le i<j\le n}\left(a_i b_j - a_j b_i\right)^2.$$

(b) $\boxed{1}$ If $K = \mathbb{R}$, then conclude the *Cauchy–Schwarz inequality*

$$\left(\sum_{k=1}^{n} a_k^2\right)\left(\sum_{k=1}^{n} b_k^2\right) \geq \left(\sum_{k=1}^{n} a_k b_k\right)^2 .$$

Exercise A.5.3.5. Let n be a positive integer.

(a) $\boxed{2}$ Prove that

$$\sum_{\substack{\sigma \in S_n \text{ is a} \\ \text{derangement}}} (-1)^{\sigma} = (-1)^{n-1} (n-1) .$$

(See Definition 6.2.4 for the notion of a derangement.)

(b) $\boxed{2}$ Prove that

$$\sum_{\sigma \in S_n} (-1)^{\sigma} x^{|\operatorname{Fix} \sigma|} = (x+n-1)(x-1)^{n-1}$$

for any $x \in K$. (See Definition A.4.2 **(b)** for the definition of $|\operatorname{Fix} \sigma|$.)

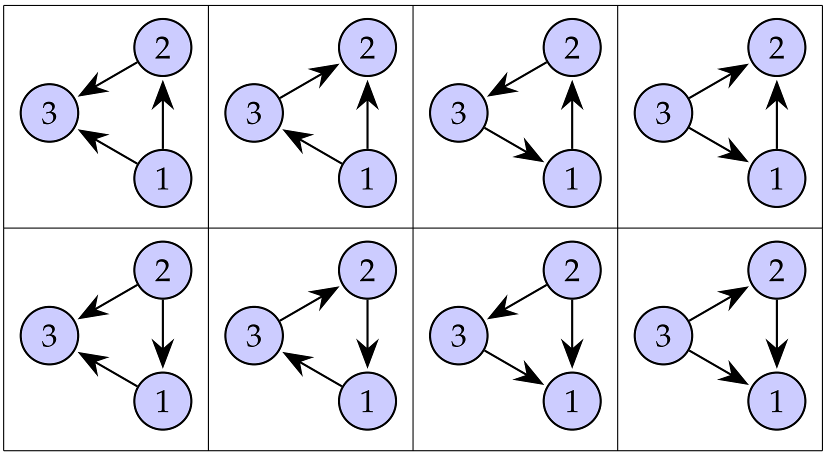
(c) $\boxed{3}$ Prove that

$$\sum_{\sigma \in S_n} \frac{(-1)^{\sigma}}{|\operatorname{Fix} \sigma| + 1} = (-1)^{n+1} \frac{n}{n+1}.$$

(This is Problem B6 on the Putnam competition 2005.)

In the next exercise, you are asked to reconstruct a proof of the Vandermonde determinant (specifically, of Theorem 6.4.31 **(d)**) using a special kind of directed graphs – the *tournaments*. This is by far not the easiest proof of Theorem 6.4.31 **(d)**, but is perhaps the most combinatorial.

Exercise A.5.3.6. We define a *tournament* to be a simple directed graph with the property that for any two distinct vertices i and j, exactly one of the arcs (i,j) and (j,i) belongs to the graph. For example, there are 8 tournaments with vertex set $[3]$, namely



. (297)

(Note that "simple graph" implies that any arc is merely a pair of two distinct vertices; thus, in particular, there are no arcs of the form (i,i).)

Fix $n \in \mathbb{N}$. Let T be the set of all tournaments with vertex set $[n]$. It is easy to see that $|T| = 2^{n(n-1)/2}$.

For any permutation $\sigma \in S_n$, we define $P_\sigma \in T$ to be the tournament with vertex set $[n]$ and with arcs

$$(\sigma(i), \sigma(j)) \qquad \text{for all } i \in [n] \text{ and } j \in [n] \text{ satisfying } i < j.$$

(For example, in the above table (297) of tournaments with vertex set $[3]$, the first tournament is P_{id}, while the second tournament is P_{s_2}.)

We define the *scoreboard* $\operatorname{scb} D$ of a tournament $D \in T$ to be the n-tuple $(s_1, s_2, \ldots, s_n) \in \mathbb{N}^n$, where

$$\begin{aligned} s_j &:= (\text{\# of arcs of } D \text{ that end at } j) \\ &= (\text{\# of } i \in [n] \text{ such that } (i,j) \text{ is an arc of } D) \end{aligned}$$

for each $j \in [n]$.

We say that a tournament $D \in T$ is *injective* if all n entries of its scoreboard $\operatorname{scb} D$ are distinct.

(a) $\boxed{2}$ Prove that a tournament $D \in T$ is injective if and only if it has the form P_σ for some $\sigma \in S_n$.

(b) $\boxed{2}$ Prove that the tournaments P_σ for all $\sigma \in S_n$ are distinct.

Now, let $a_1, a_2, \ldots, a_n$ be n elements of K. For each tournament $D \in T$, we define the following:

- For each arc $e = (i, j)$ of D, we define the *weight* $w(e)$ of e to be $(-1)^{[i>j]} a_j$ (where we are using Definition A.1.5).
- We define the *weight* $w(D)$ of D to be

$$\prod_{e \text{ is an arc of } D} w(e) = \prod_{(i,j) \text{ is an arc of } D} \left((-1)^{[i>j]} a_j\right).$$

(c) $\boxed{2}$ Prove that $\prod\limits_{1 \leq j < i \leq n} \left(a_i - a_j\right) = \sum\limits_{D \in T} w(D)$.

(d) $\boxed{2}$ Prove that $\det\left(\left(a_j^{i-1}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = \sum\limits_{\substack{D \in T \text{ is} \\ \text{injective}}} w(D)$.

(e) $\boxed{3}$ Prove that $\sum\limits_{\substack{D \in T \text{ is not} \\ \text{injective}}} w(D) = 0$.

(f) $\boxed{1}$ Conclude that Theorem 6.4.31 **(d)** holds.

[**Hint:** In part **(e)**, use a sign-reversing involution. Namely, if $D \in T$ is not injective, then its scoreboard $\operatorname{scb} D = (s_1, s_2, \ldots, s_n)$ has two equal entries – i.e., there exists a pair (u, v) of two integers $u, v \in [n]$ such that $u < v$ and $s_u = s_v$. Pick such a pair (u, v) with smallest possible v (the u is then uniquely determined (why?)), and relabel the vertices u and v of D as v and u (so that any arcs of the forms (u, k), (v, k), (k, u) or (k, v) become (v, k), (u, k), (k, v) or (k, u), respectively). Argue that the new tournament D' is still not injective and satisfies $w(D') = -w(D)$.]

Another proof of the Vandermonde determinant (Theorem 6.4.31 **(c)** to be specific) proceeds through a generalization:

Exercise A.5.3.7. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n \in K$. Let $p_1, p_2, \ldots, p_n$ be n polynomials in $K[x]$ with the property that

$$\deg p_j \leq j - 1 \qquad \text{for each } j \in [n].$$

(In particular, p_1 is constant.)

(a) $\boxed{3}$ Prove that

$$\det\left(\left(p_j(a_i)\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right) = \left(\prod_{j=1}^{n} \left[x^{j-1}\right] p_j\right) \cdot \det\left(\left(a_i^{j-1}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n}\right).$$

(b) $\boxed{2}$ By applying this to the polynomials $p_j := (x - a_1)(x - a_2) \cdots (x - a_{j-1})$, obtain a new proof of Theorem 6.4.31 **(c)**.

(c) $\boxed{1}$ Conclude that

$$\det\left(\left(p_j\left(a_i\right)\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\left(\prod_{j=1}^{n}\left[x^{j-1}\right]p_j\right)\cdot\prod_{1\leq j<i\leq n}\left(a_i-a_j\right).$$

[**Hint:** Part **(a)** can be done in many ways, but the simplest is probably by factoring the matrix $\left(p_j\left(a_i\right)\right)_{1\leq i\leq n,\ 1\leq j\leq n}$ as a product.]

And here is yet another generalization of the Vandermonde determinant:

Exercise A.5.3.8. Let $n\in\mathbb{N}$. Let $a_1,a_2,\ldots,a_n\in K$ and $b_1,b_2,\ldots,b_n\in K$. Define n polynomials $q_1,q_2,\ldots,q_n\in K\left[x\right]$ by setting

$$q_j=\left(x-b_{j+1}\right)\left(x-b_{j+2}\right)\cdots\left(x-b_n\right)\qquad\text{for each } j\in\left[n\right].$$

(In particular, $q_n=\left(\text{empty product}\right)=1$.) Furthermore, let $p_1,p_2,\ldots,p_n$ be n polynomials in $K\left[x\right]$ with the property that

$$\deg p_j\leq j-1\qquad\text{for each } j\in\left[n\right].$$

(In particular, p_1 is constant.)

(a) $\boxed{6}$ Prove that

$$\det\left(\left(p_j\left(a_i\right)q_j\left(a_i\right)\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\left(\prod_{j=1}^{n}p_j\left(b_j\right)\right)\cdot\prod_{1\leq i<j\leq n}\left(a_i-a_j\right).$$

(b) $\boxed{1}$ Use this to obtain a new proof of Theorem 6.4.31 **(a)**.

(c) $\boxed{3}$ Use this to prove Theorem 6.4.46.

As applications of Exercise A.5.3.7, several determinants consisting of binomial coefficients can be computed:

Exercise A.5.3.9. Let $n\in\mathbb{N}$. Let $a_1,a_2,\ldots,a_n\in\mathbb{C}$. Let $H\left(n\right)$ denote the positive integer $\left(n-1\right)!\cdot\left(n-2\right)!\cdot\cdots\cdot 1!$; this is known as the *hyperfactorial* of n.

(a) $\boxed{1}$ Prove that

$$\det\left(\left(\dbinom{a_i}{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right)=\frac{\prod\limits_{1\leq j<i\leq n}\left(a_i-a_j\right)}{H\left(n\right)}.$$

(b) $\boxed{1}$ Conclude that $H\left(n\right)\mid\prod\limits_{1\leq j<i\leq n}\left(a_i-a_j\right)$ for any n integers $a_1,a_2,\ldots,a_n$.

(c) $\boxed{1}$ Prove that $H(n) = \prod_{1\leq j<i\leq n} (i-j)$.

(d) $\boxed{3}$ Prove that

$$\det\left(\left(\dbinom{a_i+j}{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \frac{\prod_{1\leq j<i\leq n} (a_i - a_j)}{H(n)}.$$

(e) $\boxed{2}$ Assume that $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Prove that

$$\det\left(((a_i+j)!)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \left(\prod_{i=1}^{n} (a_i+1)!\right)\left(\prod_{1\leq j<i\leq n} (a_i - a_j)\right).$$

(f) $\boxed{3}$ Assume that $a_1, a_2, \ldots, a_n \in \mathbb{N}$. Prove that

$$\det\left(\left(\frac{1}{(a_i+j)!}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \frac{\prod_{1\leq i<j\leq n} (a_i - a_j)}{\prod_{i=1}^{n} (a_i+n)!}.$$

(g) $\boxed{2}$ Prove that

$$\det\left(\left(\dbinom{a_i+j}{i-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = 1.$$

The following exercise gives some variations on Proposition 6.4.34:

Exercise A.5.3.10. Let n be a positive integer. Let $x_1, x_2, \ldots, x_n$ be n elements of K. Let $y_1, y_2, \ldots, y_n$ be n elements of K.

(a) $\boxed{2}$ For every $m \in \{0, 1, \ldots, n-2\}$, prove that

$$\det\left(\left((x_i+y_j)^m\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = 0.$$

(b) $\boxed{3}$ Let $p_0, p_1, \ldots, p_{n-1}$ be n elements of K. Let $P \in K[x]$ be the polynomial $\sum_{k=0}^{n-1} p_k x^k$. Prove that

$$\begin{aligned}&\det\left((P(x_i+y_j))_{1\leq i\leq n,\ 1\leq j\leq n}\right)\\ &= p_{n-1}^n \left(\prod_{k=0}^{n-1} \dbinom{n-1}{k}\right)\left(\prod_{1\leq i<j\leq n} (x_i - x_j)\right)\left(\prod_{1\leq i<j\leq n} (y_j - y_i)\right).\end{aligned}$$

(c) $\boxed{2}$ Let $p_0, p_1, \ldots, p_{n-1}$ be n elements of K. Let $P \in K[x]$ be the polynomial $\sum\limits_{k=0}^{n-1} p_k x^k$. Prove that

$$\det\left(\left(P\left(x_i y_j\right)\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \left(\prod_{k=0}^{n-1} p_k\right)\left(\prod_{1\leq i<j\leq n}\left(x_i - x_j\right)\right)\left(\prod_{1\leq i<j\leq n}\left(y_i - y_j\right)\right).$$

Exercise A.5.3.11. $\boxed{4}$ Let $n \in \mathbb{N}$. Let $u_1, u_2, \ldots, u_n \in K$ and $a_1, a_2, \ldots, a_n \in K$. For each $k \in \mathbb{N}$, we set

$$z_k := u_1 a_1^k + u_2 a_2^k + \cdots + u_n a_n^k.$$

Prove that

$$\det\left(\left(z_{i+j-2}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \det\begin{pmatrix} z_0 & z_1 & \cdots & z_{n-1} \\ z_1 & z_2 & \cdots & z_n \\ \vdots & \vdots & \ddots & \vdots \\ z_{n-1} & z_n & \cdots & z_{2n-2} \end{pmatrix}$$
$$= u_1 u_2 \cdots u_n \cdot \prod_{1\leq i<j\leq n}\left(a_i - a_j\right)^2.$$

Exercise A.5.3.12. $\boxed{5}$ Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be a matrix with the property that

$$A_{i,i+1} = 1 \qquad \text{for every } i \in [n-1]$$

and

$$A_{i,j} = 0 \qquad \text{for every } i, j \in [n] \text{ satisfying } j > i+1.$$

(Such a matrix A is called a *normalized lower Hessenberg matrix*. For example, for $n = 4$, such a matrix has the form $\begin{pmatrix} * & 1 & 0 & 0 \\ * & * & 1 & 0 \\ * & * & * & 1 \\ * & * & * & * \end{pmatrix}$, where each asterisk $*$ stands for an arbitrary entry.)

For each subset I of $[n-1]$, we define an element $p_I(A) \in K$ as follows: Write the subset I in the form $\{i_1, i_2, \ldots, i_k\}$ with $i_1 < i_2 < \cdots < i_k$. Additionally, set $i_0 := 0$ and $i_{k+1} := n$. Then, set

$$p_I(A) := A_{i_1, i_0+1} A_{i_2, i_1+1} \cdots A_{i_{k+1}, i_k+1} = \prod_{u=1}^{k+1} A_{i_u, i_{u-1}+1}.$$

Prove that

$$\det A = \sum_{I\subseteq[n-1]} (-1)^{n-1-|I|}\, p_I(A).$$

Normalized lower Hessenberg matrices can be used to provide an "explicit" determinantal formula for the coefficients of the inverse of an FPS:

Exercise A.5.3.13. $\boxed{4}$ Let $f = \sum_{k \in \mathbb{N}} f_k x^k$ be a FPS in $K[[x]]$ (with $f_0, f_1, f_2, \ldots \in K$). Assume that $f_0 = 1$. Set $f_k := 0$ for all negative $k \in \mathbb{Z}$. Let $g = f^{-1}$ be the multiplicative inverse of f in $K[[x]]$, and let $g_0, g_1, g_2, \ldots$ be the coefficients of g (so that $g = \sum_{k \in \mathbb{N}} g_k x^k$). Prove that each $n \in \mathbb{N}$ satisfies

$$\begin{aligned} g_n &= (-1)^n \det\left(\left(f_{i-j+1}\right)_{1 \le i \le n,\ 1 \le j \le n}\right) \\ &= (-1)^n \det \begin{pmatrix} f_1 & 1 & 0 & 0 & \cdots & 0 \\ f_2 & f_1 & 1 & 0 & \cdots & 0 \\ f_3 & f_2 & f_1 & 1 & \cdots & 0 \\ f_4 & f_3 & f_2 & f_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ f_n & f_{n-1} & f_{n-2} & f_{n-3} & \cdots & f_1 \end{pmatrix}. \end{aligned}$$

Our next exercise is concerned with *tridiagonal matrices*. These are matrices whose all entries are zero except for those on the diagonal and "its neighbors". For example, a 3×3-matrix is tridiagonal if it has the form $\begin{pmatrix} * & * & 0 \\ * & * & * \\ 0 & * & * \end{pmatrix}$ (where each asterisk $*$ means an arbitrary entry).

Exercise A.5.3.14. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n \in K$ and $b_1, b_2, \ldots, b_{n-1} \in K$ and $c_1, c_2, \ldots, c_{n-1} \in K$. Set

$$A = \begin{pmatrix} a_1 & b_1 & 0 & \cdots & 0 & 0 & 0 \\ c_1 & a_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_2 & a_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & \cdots & c_{n-2} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & c_{n-1} & a_n \end{pmatrix} \in K^{n \times n}.$$

Formally speaking, this matrix A is defined to be

$$A = \left(\begin{cases} a_i, & \text{if } i = j; \\ b_i, & \text{if } i = j-1; \\ c_j, & \text{if } i = j+1; \\ 0, & \text{otherwise} \end{cases} \right)_{1 \le i \le n,\ 1 \le j \le n}.$$

The matrix A is called a *tridiagonal matrix*.

(a) $\boxed{2}$ Prove that every $m \in \{2,3,\ldots,n\}$ satisfies

$$\det\left(A_{:m}\right) = a_m \det\left(A_{:m-1}\right) - b_{m-1}c_{m-1} \det\left(A_{:m-2}\right),$$

where we set $A_{:k} := \operatorname{sub}^{1,2,\ldots,k}_{1,2,\ldots,k} A = \left(A_{i,j}\right)_{1\leq i\leq k,\ 1\leq j\leq k}$ for each $k \in \{0,1,\ldots,n\}$.

(b) $\boxed{3}$ Recall the notion of a "lacunar set" as defined in Definition A.1.3. If I is a set of integers, then we let $I^+ := \{i+1 \mid i \in I\}$. Prove that

$$\det A = \sum_{\substack{I\subseteq[n-1] \text{ is} \\ \text{lacunar}}} \left(\prod_{i\in[n]\setminus(I\cup I^+)} a_i\right)\left(\prod_{i\in I}(-b_ic_i)\right).$$

(c) $\boxed{1}$ Compute $\det A$ in the case when $a_i = 1$ (for all $i \in [n]$) and $b_i = 1$ (for all $i \in [n-1]$) and $c_i = -1$ (for all $i \in [n-1]$).

(d) $\boxed{2}$ Define $A_{:k}$ as in part **(a)**. Prove that

$$\frac{\det A}{\det\left(A_{:n-1}\right)} = a_n - \cfrac{b_{n-1}c_{n-1}}{a_{n-1} - \cfrac{b_{n-2}c_{n-2}}{a_{n-2} - \cfrac{b_{n-3}c_{n-3}}{a_{n-3} - \cfrac{\ddots}{\qquad - \cfrac{b_2c_2}{a_2 - \cfrac{b_1c_1}{a_1}}}}}},$$

provided that all denominators in this equality are invertible.

[**Remark:** If we set $a_i = 2x$ for all $i \in [n]$ and $b_i = c_i = -1$ for all $i \in [n-1]$, then $\det A$ becomes the n-th *Chebyshev polynomial of the first kind*, commonly denoted $T_n(x)$. Some properties of Chebyshev polynomials can be generalized to determinants of arbitrary tridiagonal matrices.

Part **(d)** can be seen as a formula for expressing a continued fraction as a ratio of determinants. The connections between continued fractions and determinants run much deeper.]

Another variation on the Vandermonde determinant:

Exercise A.5.3.15. $\boxed{3}$ Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n \in K$ and $b_1, b_2, \ldots, b_n \in K$. Prove that

$$\det\left(\left(a_i^{n-j}b_i^{j-1}\right)_{1\leq i\leq n,\ 1\leq j\leq n}\right) = \prod_{1\leq i<j\leq n}\left(a_ib_j - a_jb_i\right).$$

A.5.4. Determinants in combinatorics

The following exercises are concerned with Subsection 6.5.1.

Exercise A.5.4.1. $\boxed{5}$ Consider the following variants of the definition of the map f in the proof of Proposition 6.5.12:

(a) Define v to be the last (rather than the first) crowded point on p_i.

(b) Define j to be the smallest (rather than the largest) element of $[k]$ such that v belongs to p_j (not counting i, of course).

(c) Instead of choosing v first and j later, choose j and v as follows: First, pick j to be the largest element of $[k]$ such that the path p_i intersects p_j; then, define v to be the first point where p_i intersects p_j.

(d) Instead of defining v to be the first crowded point on p_i, choose some arbitrary total order on the vertex set of the digraph, and define v to be the largest crowded point on p_i with respect to this order. (The total order needs to be chosen in advance; it must not depend on $\mathbf{p}$ or σ.)

Which of these variants "work" (i.e., lead to well-defined sign-reversing involutions $f : \mathcal{X} \to \mathcal{X}$) ?

(You are not required to try out all combinations of these variants; just analyze each variant for itself.)

Exercise A.5.4.2. Complete the proof of Corollary 6.5.17 sketched above:

(a) $\boxed{2}$ Show that there is only one nipat from $\mathbf{A}$ to $\mathbf{B}$.

(b) $\boxed{3}$ Show that there are no nipats from $\mathbf{A}$ to $\sigma(\mathbf{B})$ when $\sigma \in S_k$ is not the identity permutation $\operatorname{id} \in S_k$.

Furthermore:

(c) $\boxed{3}$ Prove the analogue of Corollary 6.5.17 that says that each $k \in \mathbb{N}$ satisfies

$$\det\left(\left(c_{i+j-1}\right)_{1\le i\le k,\ 1\le j\le k}\right) = \det\begin{pmatrix} c_1 & c_2 & \cdots & c_k \\ c_2 & c_3 & \cdots & c_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ c_k & c_{k+1} & \cdots & c_{2k-1} \end{pmatrix} = 1.$$

(d) $\boxed{2}$ Show that the Catalan sequence $(c_0, c_1, c_2, \ldots)$ is the only sequence $(a_0, a_1, a_2, \ldots)$ of real numbers that satisfies

$$\det\left(\left(a_{i+j-2}\right)_{1\le i\le k,\ 1\le j\le k}\right) = \det\left(\left(a_{i+j-1}\right)_{1\le i\le k,\ 1\le j\le k}\right) = 1 \qquad \text{for all } k \in \mathbb{N}.$$

(e) $\boxed{3}$ Compute $\det\left(\left(c_{i+j}\right)_{1\leq i\leq k,\ 1\leq j\leq k}\right)$ for each $k\in\mathbb{N}$.

The next exercise should be contrasted with Exercise A.4.11.2.

Exercise A.5.4.3. Let $n\in\mathbb{N}$. Let I be a subset of $[n-1]$. Write I in the form $I=\{c_1,c_2,\ldots,c_k\}$ with $c_1<c_2<\cdots<c_k$. Set $c_0:=0$ and $c_{k+1}:=n$. Recall Definition A.4.22.

(a) $\boxed{3}$ Prove that

$$(\#\text{ of }\sigma\in S_n\text{ satisfying }\operatorname{Des}\sigma=I)=\det\left(\left(\binom{n-c_{i-1}}{c_j-c_{i-1}}\right)_{1\leq i\leq k+1,\ 1\leq j\leq k+1}\right).$$

(b) $\boxed{5}$ Let us use the notations from Definition 4.4.3. Prove that

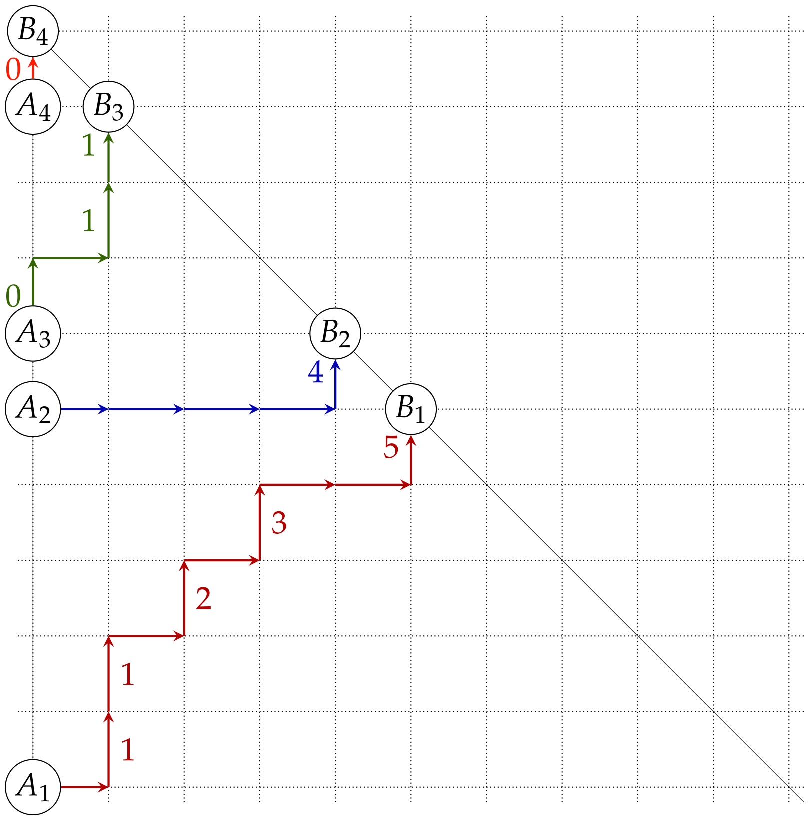
$$\sum_{\substack{\sigma\in S_n;\\ \operatorname{Des}\sigma=I}}q^{\ell(\sigma)}=\det\left(\left(\binom{n-c_{i-1}}{c_j-c_{i-1}}_q\right)_{1\leq i\leq k+1,\ 1\leq j\leq k+1}\right)\qquad\text{in the ring }\mathbb{Z}[q].$$

[**Hint:** One way to approach this is by observing that the matrices in question are transposes of normalized lower Hessenberg matrices as in Exercise A.5.3.12. Another is to apply the LGV lemma (in its weighted version for part **(b)**) to the $(k+1)$-vertices $\mathbf{A}=(A_1,A_2,\ldots,A_{k+1})$ and $\mathbf{B}=(B_1,B_2,\ldots,B_{k+1})$ defined by

$$A_i:=(0,c_{i-1})\qquad\text{and}\qquad B_i:=(n-c_i,c_i).$$

Here is an example, for $n=10$ and $I=\{5,6,9\}$ and $\sigma\in S_{10}$ with OLN

$(2, 3, 5, 7, 10, 9, 1, 6, 8, 4)$:



.

Here, the x-coordinates of the north-steps of the paths (from bottom to top: $1, 1, 2, 3, 5, 4, 0, 1, 1, 0$) are the entries of the Lehmer code $L(\sigma) = (1, 1, 2, 3, 5, 4, 0, 1, 1, 0)$ of σ.]

The next exercise sketches out a visual proof of the Cauchy–Binet formula using the LGV lemma:

Exercise A.5.4.4. Let K be a commutative ring. Let $n, m \in \mathbb{N}$. Let $A \in K^{n \times m}$ be an $n \times m$-matrix, and let $B \in K^{m \times n}$ be an $m \times n$-matrix.

Let D be the digraph with $2n + m$ vertices labeled

$$1, 2, \ldots, n, \quad 1', 2', \ldots, m', \quad 1'', 2'', \ldots, n'',$$

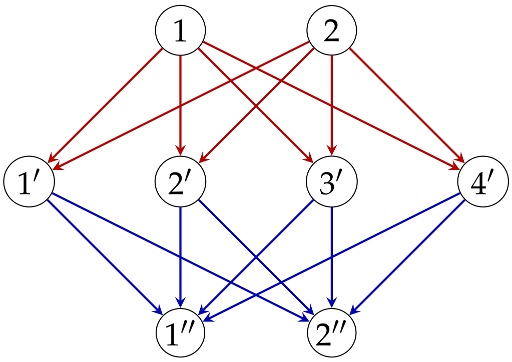
and with arcs

$$i \to j' \qquad \text{for all } i \in [n] \text{ and } j \in [m]$$

and

$$i' \to j'' \qquad \text{for all } i \in [m] \text{ and } j \in [n].$$

Here is how D looks like for $n = 2$ and $m = 4$:



.

(a) $\boxed{1}$ Prove that this digraph D is acyclic.

Now, for each arc a of D, we define a weight $w(a) \in K$ as follows:

- If a is the arc $i \to j'$ for some $i \in [n]$ and $j \in [m]$, then we set $w(a) := A_{i,j}$.
- If a is the arc $i' \to j''$ for some $i \in [m]$ and $j \in [n]$, then we set $w(a) := B_{i,j}$.

(b) $\boxed{1}$ Prove that

$$\left(\sum_{p:i\to j''} w(p)\right)_{1\leq i\leq n,\ 1\leq j\leq n} = AB.$$

Here, "$p : u \to v$" means "p is a path from u to v" whenever u and v are two vertices of D.

(c) $\boxed{3}$ Define two n-vertices $\mathbf{A}$ and $\mathbf{B}$ by $\mathbf{A} = (1, 2, \ldots, n)$ and $\mathbf{B} = (1'', 2'', \ldots, n'')$. Prove that

$$\sum_{\sigma\in S_n} (-1)^{\sigma} \sum_{\substack{\mathbf{p} \text{ is a nipat} \\ \text{from } \mathbf{A} \text{ to } \sigma(\mathbf{B})}} w(\mathbf{p})$$
$$= \sum_{\substack{(g_1,g_2,\ldots,g_n)\in[m]^n; \\ g_1<g_2<\cdots<g_n}} \det\left(\operatorname{cols}_{g_1,g_2,\ldots,g_n} A\right) \cdot \det\left(\operatorname{rows}_{g_1,g_2,\ldots,g_n} B\right),$$

where we are using the notations of Theorem 6.5.14 (with $k = n$) and of Theorem 6.4.18.

(d) $\boxed{1}$ Prove Theorem 6.4.18.

Exercise A.5.4.5. Consider the situation of Theorem 6.5.14. Assume that our digraph D has vertex set $[n]$ for some $n \in \mathbb{N}$. Let E be the set of all arcs of D.

Let $M \in K^{n\times n}$ be the $n \times n$-matrix whose (i,j)-th entry is given by

$$M_{i,j} = \sum_{\substack{a \in E \text{ is an arc} \\ \text{from } i \text{ to } j}} w(a) \qquad \text{for all } i,j \in [n].$$

(Note that if D is a simple digraph, then the sum on the right hand side of this equality has at most one addend.)

(a) $\boxed{2}$ Prove that each $k \in \mathbb{N}$ satisfies

$$M^k = \left(\sum_{\substack{p: i \to j \text{ is a path} \\ \text{with } k \text{ steps}}} w(p) \right)_{1\leq i\leq n,\ 1\leq j\leq n}.$$

Here, "$p : i \to j$" means "p is a path from i to j".

(b) $\boxed{2}$ Prove that $M^n = 0_{n\times n}$ (the zero matrix).

(c) $\boxed{2}$ Let $I_n \in K^{n\times n}$ denote the $n \times n$ identity matrix. Prove that

$$(I_n - M)^{-1} = \left(\sum_{p: i \to j} w(p) \right)_{1\leq i\leq n,\ 1\leq j\leq n}.$$

A.6. Symmetric functions

The notations of Chapter 7 shall be used here. In particular, an integer $N \in \mathbb{N}$ and a commutative ring K are fixed.

A.6.1. Definitions and examples of symmetric polynomials

Exercise A.6.1.1. $\boxed{2}$ Prove Proposition 7.1.14 **(b)**.

Exercise A.6.1.2. $\boxed{2}$ Let $M \in \{0, 1, \ldots, N\}$. Prove that

$$e_n[x_1, x_2, \ldots, x_N] = \sum_{i=0}^{n} e_i[x_1, x_2, \ldots, x_M] \cdot e_{n-i}[x_{M+1}, x_{M+2}, \ldots, x_N]$$

and

$$h_n[x_1, x_2, \ldots, x_N] = \sum_{i=0}^{n} h_i[x_1, x_2, \ldots, x_M] \cdot h_{n-i}[x_{M+1}, x_{M+2}, \ldots, x_N]$$

and

$$p_n [x_1, x_2, \ldots, x_N] = p_n [x_1, x_2, \ldots, x_M] + p_n [x_{M+1}, x_{M+2}, \ldots, x_N].$$

Exercise A.6.1.3. $\boxed{5}$ Finish our proof of Theorem 7.1.12 by proving the remaining two Newton–Girard formulas (248) and (249).

Exercise A.6.1.4. $\boxed{5}$ Prove that each positive integer n satisfies

$$\sum_{j=1}^{n} (-1)^{j-1} j e_j h_{n-j} = p_j;$$
$$\sum_{j=1}^{n} (-1)^{n-j} j h_j e_{n-j} = p_j.$$

Exercise A.6.1.5. Let $n \in \mathbb{N}$.

(a) $\boxed{1}$ Prove that

$$e_n \left[\underbrace{1, 1, \ldots, 1}_{N \text{ times}} \right] = \binom{N}{n} \qquad \text{and}$$
$$h_n \left[\underbrace{1, 1, \ldots, 1}_{N \text{ times}} \right] = \binom{N+n-1}{n}.$$

(b) $\boxed{2}$ Prove that

$$e_n \left[q^0, q^1, \ldots, q^{N-1} \right] = q^{n(n-1)/2} \binom{N}{n}_q \qquad \text{and}$$
$$h_n \left[q^0, q^1, \ldots, q^{N-1} \right] = \binom{N+n-1}{n}_q$$

in the ring $\mathbb{Z}[q]$, where we are using the notation of Definition 4.4.3.

(c) $\boxed{2}$ Recover a nontrivial identity between q-binomial coefficients by substituting $q^0, q^1, \ldots, q^{N-1}$ into an identity between symmetric polynomials. (There are several valid answers here.)

(d) $\boxed{3}$ For any $m, k \in \mathbb{N}$, the *unsigned Stirling number of the 1st kind* $c(m, k) \in \mathbb{N}$ is defined to be the # of all permutations $\sigma \in S_m$ that have exactly k cycles (see Definition 5.5.4 **(a)**). Prove that

$$e_n [1, 2, \ldots, N] = c(N+1, N+1-n).$$

(e) $\boxed{3}$ For any $m, k \in \mathbb{N}$, the *Stirling number of the 2nd kind* $S(m,k) \in \mathbb{N}$ is defined to be the # of all set partitions of the set $[m]$ into k parts (i.e., the # of sets $\{U_1, U_2, \ldots, U_k\}$ consisting of k distinct nonempty subsets $U_1, U_2, \ldots, U_k$ of $[m]$ such that $U_1 \cup U_2 \cup \cdots \cup U_k = [m]$). Prove that

$$h_n[1, 2, \ldots, N] = S(N+n, N).$$

Exercise A.6.1.6. For each $n \in \mathbb{N}$ and each positive integer k, we define the *(n,k)-th Petrie symmetric polynomial* $g_{k,n} \in \mathcal{S}$ by

$$\begin{aligned} g_{k,n} &= \sum_{\substack{(i_1,i_2,\ldots,i_n)\in[N]^n;\\ i_1\le i_2\le\cdots\le i_n;\\ \text{no } k \text{ of the numbers } i_1,i_2,\ldots,i_n \text{ are equal}}} x_{i_1}x_{i_2}\cdots x_{i_n} \\ &= \sum_{\substack{(a_1,a_2,\ldots,a_N)\in\{0,1,\ldots,k-1\}^N;\\ a_1+a_2+\cdots+a_N=n}} x_1^{a_1}x_2^{a_2}\cdots x_N^{a_N}. \end{aligned}$$

(a) $\boxed{1}$ Prove that $g_{2,n} = e_n$ for each $n \in \mathbb{N}$.

(b) $\boxed{1}$ Prove that $g_{k,n} = h_n$ for each $n \in \mathbb{N}$ and each $k > n$.

(c) $\boxed{1}$ Prove that $g_{n,n} = h_n - p_n$ for each $n > 0$.

(d) $\boxed{3}$ Prove that each $n \in \mathbb{N}$ and each $k > 0$ satisfy

$$g_{k,n} = \sum_{i\in\mathbb{N}} (-1)^i e_i\left[x_1^k, x_2^k, \ldots, x_N^k\right] \cdot h_{n-ki}.$$

(The sum on the right hand side is well-defined, since $h_{n-ki} = 0$ whenever $i > \frac{n}{k}$.)

(e) $\boxed{3}$ Set

$$c_{i,j} := \begin{cases} 2, & \text{if } i \equiv j \bmod 3; \\ -1, & \text{if } i \not\equiv j \bmod 3 \end{cases} \qquad \text{for any } i, j \in \mathbb{Z}.$$

Prove that each even $n \in \mathbb{N}$ satisfies

$$g_{3,n} = e_{n/2}^2 + \sum_{i=0}^{(n-2)/2} c_{i,n-i} e_i e_{n-i},$$

and that each odd $n \in \mathbb{N}$ satisfies

$$g_{3,n} = -\sum_{i=0}^{(n-1)/2} c_{i,n-i} e_i e_{n-i}.$$

Exercise A.6.1.7. (a) $\boxed{3}$ Prove that there exists a family of polynomials $(P_1, P_2, P_3, \ldots)$, with each P_n being a polynomial in the ring $\mathbb{Z}[y_1, y_2, \ldots, y_n]$, such that every positive integer n satisfies

$$e_n = P_n[h_1, h_2, \ldots, h_n] \qquad \text{and} \qquad h_n = P_n[e_1, e_2, \ldots, e_n].$$

(This family begins with $P_1 = x_1$ and $P_2 = x_1^2 - x_2$ and $P_3 = x_1^3 - 2x_1x_2 + x_3$.)

(b) $\boxed{2}$ Prove that there exists a family of polynomials $(Q_1, Q_2, Q_3, \ldots)$, with each Q_n being a polynomial in the ring $\mathbb{Z}[y_1, y_2, \ldots, y_n]$, such that every positive integer n satisfies

$$p_n = (-1)^{n-1} Q_n[h_1, h_2, \ldots, h_n] \qquad \text{and} \qquad p_n = Q_n[e_1, e_2, \ldots, e_n].$$

(This family begins with $Q_1 = x_1$ and $Q_2 = x_1^2 - 2x_2$ and $Q_3 = x_1^3 - 3x_1x_2 + 3x_3$.)

(c) $\boxed{3}$ Express the polynomials P_n explicitly as determinants of certain matrices.

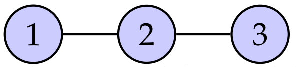
(d) $\boxed{3}$ Express the polynomials Q_n explicitly as determinants of certain matrices.

The following exercise is a symmetric-functions analogue of Exercise A.5.2.9:

Exercise A.6.1.8. $\boxed{3}$ Let us use the notations of Exercise A.5.2.9. (Thus, G is a finite undirected graph with vertex set V and edge set E.)

Define the *chromatic symmetric polynomial* X_G (in N variables $x_1, x_2, \ldots, x_N$) to be the polynomial

$$\sum_{\substack{c:V\to[N] \text{ is a} \\ \text{proper } N\text{-coloring}}} \prod_{v\in V} x_{c(v)} \in \mathcal{P}.$$

For instance, if the graph G is the length-2 path graph , then a proper N-coloring of G is a map $c : [3] \to [N]$ satisfying $c(1) \neq c(2)$ and $c(2) \neq c(3)$, and therefore its chromatic symmetric polynomial X_G is

$$\begin{aligned}
\sum_{\substack{c:[3]\to[N]; \\ c(1)\neq c(2); \\ c(2)\neq c(3)}} \prod_{v\in[3]} x_{c(v)} &= \sum_{\substack{i,j,k\in[N]; \\ i\neq j; \\ j\neq k}} x_ix_jx_k = \underbrace{\sum_{\substack{i,j\in[N]; \\ i\neq j}} x_i^2x_j}_{=p_2e_1-p_3} + \underbrace{\sum_{\substack{i,j,k\in[N]; \\ i,j,k \text{ are distinct}}} x_ix_jx_k}_{=6e_3} \\
&= p_2e_1 - p_3 + 6e_3 \\
&= e_2e_1 + 3e_3 \qquad \text{(by some computation)} \\
&= p_1^3 - 2p_1p_2 + p_3 \qquad \text{(by some computation)}.
\end{aligned}$$

(a) $\boxed{1}$ Prove that $X_G \in \mathcal{S}$.

(b) $\boxed{3}$ Prove that

$$X_G = \sum_{F \subseteq E} (-1)^{|F|} \prod_{\substack{C \text{ is a connected component} \\ \text{of the graph with vertex set } V \\ \text{and edge set } F}} p_{|C|}.$$

(Here, $|C|$ denotes the number of vertices in the connected component C.)

(c) $\boxed{1}$ Prove that

$$X_G \left[\underbrace{1, 1, \ldots, 1}_{N \text{ ones}} \right] = \chi_G (N)$$

(where $\chi_G (N)$ is as defined in Exercise A.5.2.9).

Next, let us generalize X_G: For each vertex $v \in V$, let $w(v)$ be a positive integer; we shall call $w(v)$ the *weight* of v. We define the *weighted chromatic symmetric polynomial* $X_{G,w}$ to be

$$\sum_{\substack{c: V \to [N] \text{ is a} \\ \text{proper } N\text{-coloring}}} \prod_{v \in V} x_{c(v)}^{w(v)} \in \mathcal{P}.$$

Thus, if all weights $w(v)$ equal 1, then $X_{G,w} = X_G$.

(d) $\boxed{2}$ Generalize the claim of part **(b)** to $X_{G,w}$.

Exercise A.6.1.9. Let n be a positive integer. If $w \in [N]^n$ is an n-tuple, then

- we let $w_1, w_2, \ldots, w_n$ denote the n entries of w (so that $w = (w_1, w_2, \ldots, w_n)$);
- we define the *descent set* $\operatorname{Des} w$ of w by

$$\operatorname{Des} w := \{ i \in [n-1] \mid w_i > w_{i+1} \};$$

- we define the *stagnation set* $\operatorname{Stag} w$ of w by

$$\operatorname{Stag} w := \{ i \in [n-1] \mid w_i = w_{i+1} \};$$

- we define the monomial x_w to be $x_{w_1} x_{w_2} \cdots x_{w_n}$.

For instance, the 7-tuple $(2, 2, 4, 1, 4, 4, 2)$ has descent set $\{3, 6\}$ and stagnation set $\{1, 5\}$.

(a) $\boxed{1}$ Fix $s \in \mathbb{N}$. Prove that

$$\sum_{\substack{w \in [N]^n; \\ |\operatorname{Stag} w| = s}} x_w \in \mathcal{S}.$$

(b) $\boxed{1}$ Identify this sum as a sum of weighted chromatic symmetric polynomials of path graphs (see Exercise A.6.1.8).

(c) $\boxed{3}$ Fix $d \in \mathbb{N}$ and $s \in \mathbb{N}$. Prove that

$$\sum_{\substack{w \in [N]^n; \\ |\operatorname{Des} w| = d; \\ |\operatorname{Stag} w| = s}} x_w \in \mathcal{S}.$$

(d) $\boxed{6}$ Fix $d \in \mathbb{N}$ and $s \in \mathbb{N}$. Prove that the three polynomials

$$\sum_{\substack{w \in [N]^n; \\ |\operatorname{Des} w| = d; \\ |\operatorname{Stag} w| = s; \\ w_1 < w_n}} x_w, \qquad \sum_{\substack{w \in [N]^n; \\ |\operatorname{Des} w| = d; \\ |\operatorname{Stag} w| = s; \\ w_1 = w_n}} x_w, \qquad \sum_{\substack{w \in [N]^n; \\ |\operatorname{Des} w| = d; \\ |\operatorname{Stag} w| = s; \\ w_1 > w_n}} x_w$$

all belong to $\mathcal{S}$.

Exercise A.6.1.10. $\boxed{4}$ Prove that every $m \in \mathbb{N}$ satisfies

$$\sum_{k=1}^{N} \frac{x_k^m}{\prod\limits_{i \in [N] \setminus \{k\}} (x_k - x_i)} = h_{m-N+1}.$$

(This is an equality in the localization of the polynomial ring $\mathcal{P}$ at the multiplicative subset generated by the pairwise differences $x_i - x_j$ for all $i < j$. If K is a field, you can also view it as an equality in the field of rational functions $K(x_1, x_2, \ldots, x_N)$.)

For instance, if $N = 3$ (and if we rename x_1, x_2, x_3 as x, y, z), then this is saying that

$$\frac{x^m}{(x-y)(x-z)} + \frac{y^m}{(y-z)(y-x)} + \frac{z^m}{(z-x)(z-y)} = h_{m-2}[x, y, z].$$

(Note that the right hand side is 0 when $m < 2$.)

Exercise A.6.1.11. Let $n \in \mathbb{N}$.

(a) $\boxed{3}$ Prove that

$$h_n\left[x_1^2, x_2^2, \ldots, x_N^2\right] = \sum_{i=0}^{2n} (-1)^i h_i h_{2n-i}.$$

(b) $\boxed{3}$ Prove that

$$e_n\left[x_1^2, x_2^2, \ldots, x_N^2\right] = \sum_{i=0}^{2n} (-1)^{n-i} e_i e_{2n-i}.$$

(c) $\boxed{2}$ Solve Exercise A.2.2.1 again using part **(b)**.

Exercise A.6.1.12. $\boxed{4}$ Let $i \in [N+1]$ and $p \in \mathbb{N}$. Prove that

$$h_p\left[x_i, x_{i+1}, \ldots, x_N\right] = \sum_{t=0}^{i-1} (-1)^t e_t\left[x_1, x_2, \ldots, x_{i-1}\right] \cdot h_{p-t}.$$

(The "h_{p-t}" at the end of the right hand side means $h_{p-t}\left[x_1, x_2, \ldots, x_N\right]$.)

Exercise A.6.1.13. (a) $\boxed{2}$ Prove that each $i \in [N]$ and $j \in [N]$ satisfy

$$\frac{\partial e_j}{\partial x_i} = e_{j-1}\left[x_1, x_2, \ldots, \widehat{x_i}, \ldots, x_N\right],$$

where the hat over the "x_i" means "omit the x_i entry" (that is, the expression "$x_1, x_2, \ldots, \widehat{x_i}, \ldots, x_N$" is to be understood as "$x_1, x_2, \ldots, x_{i-1}, x_{i+1}, x_{i+2}, \ldots, x_N$").

(b) $\boxed{3}$ Prove that

$$\det\left(\left(\frac{\partial e_j}{\partial x_i}\right)_{1\leq i\leq N,\ 1\leq j\leq N}\right) = \prod_{1\leq i<j\leq N} \left(x_i - x_j\right).$$

A.6.2. N-partitions and monomial symmetric polynomials

Exercise A.6.2.1. $\boxed{3}$ Let $M \in \{0, 1, \ldots, N\}$. For any M-partition $\mu = (\mu_1, \mu_2, \ldots, \mu_M)$ and any $(N-M)$-partition $\nu = (\nu_1, \nu_2, \ldots, \nu_{N-M})$, we let $\mu \sqcup \nu$ denote the N-partition obtained by sorting the N-tuple $(\mu_1, \mu_2, \ldots, \mu_M, \nu_1, \nu_2, \ldots, \nu_{N-M})$ in weakly decreasing order. (For example, $(3, 2, 0) \sqcup (4, 2, 1, 1) = (4, 3, 2, 2, 1, 1, 0)$.)

Let λ be any N-partition. Prove that

$$\begin{aligned} & m_\lambda\left[x_1, x_2, \ldots, x_N\right] \\ & = \sum_{\substack{\mu \text{ is an } M\text{-partition;} \\ \nu \text{ is an } (N-M)\text{-partition;} \\ \mu\sqcup\nu=\lambda}} m_\mu\left[x_1, x_2, \ldots, x_M\right] \cdot m_\nu\left[x_{M+1}, x_{M+2}, \ldots, x_N\right]. \end{aligned}$$

Exercise A.6.2.2. $\boxed{2}$ We shall use the notion of a tournament, as defined in Exercise A.5.3.6. Let T be the set of all tournaments with vertex set $[N]$. We define the *scoreboard* $\operatorname{scb} D$ of a tournament $D \in T$ to be the N-tuple $(s_1, s_2, \ldots, s_N) \in \mathbb{N}^N$, where

$$\begin{aligned} s_j &:= (\text{\# of arcs of } D \text{ that end at } j) \\ &= (\text{\# of } i \in [N] \text{ such that } (i,j) \text{ is an arc of } D) \end{aligned}$$

for each $j \in [N]$.

Prove that

$$\prod_{1 \leq i < j \leq N} (x_i + x_j) = \sum_{\substack{\lambda \text{ is an } N\text{-partition} \\ \text{of } N(N-1)/2}} t_\lambda m_\lambda,$$

where t_λ denotes the # of tournaments $D \in T$ with scoreboard $\operatorname{scb} D = \lambda$.

A.6.3. Schur polynomials

Exercise A.6.3.1. $\boxed{2}$ Assume that $N > 1$. Without using the Jacobi–Trudi identities, prove that $s_{(n,1,0,0,\ldots,0)} = h_n h_1 - h_{n+1}$ for each $n \in \mathbb{N}$. (Here, $(n, 1, 0, 0, \ldots, 0)$ denotes the N-partition whose first two entries are n and 1 while all remaining entries equal 0.)

Exercise A.6.3.2. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ be any N-partition.

(a) $\boxed{2}$ Let $k \in \mathbb{N}$. Show that

$$s_{(\lambda_1+k, \lambda_2+k, \ldots, \lambda_N+k)} = (x_1 x_2 \cdots x_N)^k \cdot s_\lambda.$$

(b) $\boxed{4}$ Let $k \in \mathbb{N}$ be such that $k \geq \lambda_1$. Let μ be the N-partition $(k - \lambda_N, k - \lambda_{N-1}, \ldots, k - \lambda_1)$. Prove that

$$s_\mu = (x_1 x_2 \cdots x_N)^k \cdot s_\lambda \left[x_1^{-1}, x_2^{-1}, \ldots, x_N^{-1}\right]$$

in the Laurent polynomial ring $K\left[x_1^\pm, x_2^\pm, \ldots, x_N^\pm\right]$. (We have never formally defined this ring, but it should suffice to know that the elements of $K\left[x_1^\pm, x_2^\pm, \ldots, x_N^\pm\right]$ are formal K-linear combinations of "Laurent monomials" $x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}$ with $a_1, a_2, \ldots, a_N \in \mathbb{Z}$.)

Exercise A.6.3.3. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$ be any two N-partitions.

(a) $\boxed{1}$ Show that each $k \in \mathbb{N}$ satisfies

$$s_{(\lambda_1+k, \lambda_2+k, \ldots, \lambda_N+k)/(\mu_1+k, \mu_2+k, \ldots, \mu_N+k)} = s_{\lambda/\mu}.$$

(b) $\boxed{4}$ Let $p \in \mathbb{N}$ be such that $p \geq \lambda_1$ and $p \geq \mu_1$. Show that

$$s_{(p-\mu_N, p-\mu_{N-1}, \ldots, p-\mu_1)/(p-\lambda_N, p-\lambda_{N-1}, \ldots, p-\lambda_1)} = s_{\lambda/\mu}.$$

[**Note:** The Young diagram of $(\lambda_1 + k, \lambda_2 + k, \ldots, \lambda_N + k) \,/\, (\mu_1 + k, \mu_2 + k, \ldots, \mu_N + k)$ is obtained from $Y(\lambda/\mu)$ by a parallel shift, whereas the Young diagram of $(p - \mu_N, p - \mu_{N-1}, \ldots, p - \mu_1) \,/\, (p - \lambda_N, p - \lambda_{N-1}, \ldots, p - \lambda_1)$ is obtained from $Y(\lambda/\mu)$ by a 180°-rotation.]

Exercise A.6.3.4. Let λ and μ be two N-partitions with $\mu \subseteq \lambda$. Recall the Bender–Knuth involutions $\beta_k : \operatorname{SSYT}(\lambda/\mu) \to \operatorname{SSYT}(\lambda/\mu)$ defined for all $k \in [n-1]$ in the proof of Theorem 7.3.21.

(a) $\boxed{1}$ Prove that $\beta_i \circ \beta_j = \beta_j \circ \beta_i$ whenever i and j are two elements of $[N-1]$ satisfying $|i-j| > 1$.

(b) $\boxed{4}$ Prove that $\beta_1 \circ \beta_2 \circ \beta_1 = \beta_2 \circ \beta_1 \circ \beta_2$ if $\mu = \mathbf{0}$ (where $\mathbf{0} = (0, 0, \ldots, 0)$ as in Remark 7.3.22).

(c) $\boxed{2}$ Find an example where $\beta_1 \circ \beta_2 \circ \beta_1 \neq \beta_2 \circ \beta_1 \circ \beta_2$ for $\mu \neq \mathbf{0}$.

The next exercise answers a rather natural question about the definition of a semistandard tableau (Definition 7.3.6): What happens when one replaces "increase strictly down each column" by "increase weakly down each column"? This replacement gives rise to a more liberal notion of semistandard tableaux (which I call "semi-semistandard tableaux"), and to a variant of the Schur polynomial that correspondingly has more terms. As the following exercise shows, alas, this new polynomial is rarely ever symmetric:

Exercise A.6.3.5. Let λ be an N-partition, or (more generally) a partition of any length. A Young tableau T of shape λ will be called *semi-semistandard* if its entries

- increase weakly along each row;
- increase weakly down each column.

For instance, the tableau $\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 2 \\ \hline \end{array}$ is semi-semistandard but not semistandard. (Semi-semistandard tableaux are actually known as *reverse plane partitions* for historical reasons: If you replace the words "increase" by "decrease", then they become "2-dimensional" analogues of partitions, in that they are tables of positive integers that weakly decrease in two directions.)

We define the "fool's Schur polynomial" $\widehat{s}_\lambda \in \mathcal{P}$ by

$$\widehat{s}_\lambda := \sum_{T \in \operatorname{SSSYT}(\lambda)} x_T,$$

where SSSYT (λ) is the set of all semi-semistandard tableaux of shape λ.

(a) $\boxed{2}$ Assume that $N \geq 3$ and $K = \mathbb{Z}$. Prove that the polynomial $\widehat{s}_\lambda$ is symmetric if and only if the Young diagram $Y(\lambda)$ either consists of a single row (i.e., we have $\lambda = (n, 0, 0, \ldots, 0)$ for some $n \in \mathbb{N}$) or consists of a single column (i.e., we have $\lambda = (1, 1, \ldots, 1, 0, 0, \ldots, 0)$ for some number of 1's).

(b) $\boxed{2}$ Now, replace the assumption $N \geq 3$ by $N = 2$. Prove that the polynomial $\widehat{s}_\lambda$ is symmetric if and only if the Young diagram $Y(\lambda)$ is a rectangle (i.e., all nonzero entries of λ are equal).

[**Hint:** Compare the coefficients of $x_1 x_2^k$ and $x_1^k x_2$, as well as the coefficients of $x_1 x_2 x_3^k$ and $x_1 x_2^k x_3$.]

Here are some more properties of Schur polynomials:

Exercise A.6.3.6. $\boxed{3}$ Let $\rho := (N-1, N-2, \ldots, N-N) \in \mathbb{N}^N$. Prove that

$$s_\rho = \prod_{1 \leq i < j \leq N} \left(x_i + x_j\right).$$

Exercise A.6.3.7. $\boxed{3}$ Prove Proposition 7.3.45.

Exercise A.6.3.8. **(a)** $\boxed{4}$ Prove Theorem 7.3.46 **(a)**.

(b) $\boxed{4}$ Prove Theorem 7.3.46 **(b)**.

[**Hint:** For part **(a)**, apply Theorem 7.3.32 to $(n, 0, 0, \ldots, 0)$, $\mathbf{0}$ and μ instead of λ, μ and ν, and characterize the μ-Yamanouchi semistandard tableaux of shape $(n, 0, 0, \ldots, 0) / \mathbf{0}$. Proceed likewise for part **(b)**.]

Exercise A.6.3.9. Complete the proof of Theorem 7.3.48 sketched above:

(a) $\boxed{2}$ Prove Observation 1.

(b) $\boxed{3}$ Prove Observation 2.

Exercise A.6.3.10. $\boxed{6}$ Prove Theorem 7.3.51.

Exercise A.6.3.11. $\boxed{5}$ Let n be a positive integer. Prove that

$$p_n = \sum_{i=0}^{\min\{n,N\}-1} (-1)^i s_{Q(i)},$$

where $Q(i)$ is the N-partition $\left(n - i, \underbrace{1, 1, \ldots, 1}_{i \text{ many } 1\text{'s}}, \underbrace{0, 0, \ldots, 0}_{N-i-1 \text{ many } 0\text{'s}}\right)$.

Exercise A.6.3.12. $\boxed{5}$ Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$ be two N-partitions. Prove that

$$s_\lambda s_\mu = \det\left(\left(h_{\lambda_i + \mu_{N+1-j} - i + j}\right)_{1 \le i \le N,\ 1 \le j \le N}\right).$$

[Hint: Fix some $m \in \mathbb{N}$ that is larger than all of $\mu_1, \mu_2, \ldots, \mu_N$, and consider the skew partition $\nu / \kappa = (\nu_1, \nu_2, \ldots, \nu_N) \;/\; (\kappa_1, \kappa_2, \ldots, \kappa_N)$, where $\nu_i := \lambda_i + m$ and $\kappa_i := m - \mu_{N+1-i}$ for all $i \in [N]$. What are the semistandard tableaux of shape ν / κ, and what does this mean for $s_{\nu/\kappa}$?]

Exercise A.6.3.13. $\boxed{5}$ Prove the *flagged first Jacobi–Trudi formula*: Let $M \in \mathbb{N}$. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_M)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_M)$ be two M-partitions (i.e., weakly decreasing M-tuples of nonnegative integers). Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_M)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_M)$ be two weakly increasing sequences of elements of $\{0, 1, \ldots, N\}$. (As usual, "weakly increasing" means that $\alpha_1 \le \alpha_2 \le \cdots \le \alpha_M$ and $\beta_1 \le \beta_2 \le \cdots \le \beta_M$.) Let

$$s_{\lambda/\mu,\ \alpha/\beta} := \sum_{\substack{T \in \operatorname{SSYT}(\lambda/\mu); \\ \alpha_i < T(i,j) \le \beta_i \text{ for all } (i,j) \in Y(\lambda/\mu)}} x_T \in \mathcal{P}.$$

(This is the same sum as $s_{\lambda/\mu}$, but restricted to those semistandard tableaux whose entries in the i-th row belong to the half-open interval $(\alpha_i, \beta_i]$ for each $i \in [M]$. This polynomial is known as a *(row-)flagged Schur polynomial*; in general, it is not symmetric.) Then,

$$s_{\lambda/\mu,\ \alpha/\beta} = \det\left(\left(h_{\lambda_i - \mu_j - i + j}\left[x_{\alpha_j + 1}, x_{\alpha_j + 2}, \ldots, x_{\beta_i}\right]\right)_{1 \le i \le M,\ 1 \le j \le M}\right).$$

(If $\alpha_j \ge \beta_i$, then "$x_{\alpha_j+1}, x_{\alpha_j+2}, \ldots, x_{\beta_i}$" is understood to be an empty list, so that $h_{\lambda_i - \mu_j - i + j}\left[x_{\alpha_j+1}, x_{\alpha_j+2}, \ldots, x_{\beta_i}\right]$ is the complete homogeneous symmetric polynomial $h_{\lambda_i - \mu_j - i + j}$ of 0 variables; this equals 1 if $\lambda_i - \mu_j - i + j = 0$ and 0 otherwise.)

Exercise A.6.3.14. Let d denote the differential operator

$$\frac{\partial}{\partial x_1} + \frac{\partial}{\partial x_2} + \cdots + \frac{\partial}{\partial x_N} \text{ on } \mathcal{P}.$$

Explicitly, this operator d is the K-linear map from $\mathcal{P}$ to $\mathcal{P}$ that sends

$$\text{each monomial } x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N} \text{ to } \sum_{\substack{i \in [N]; \\ a_i > 0}} a_i \underbrace{x_1^{a_1} x_2^{a_2} \cdots x_{i-1}^{a_{i-1}} x_i^{a_i - 1} x_{i+1}^{a_{i+1}} x_{i+2}^{a_{i+2}} \cdots x_N^{a_N}}_{\substack{\text{This is just the monomial } x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}, \\ \text{with the exponent on } x_i \text{ decreased by 1}}}.$$

As usual for linear operators, we abbreviate $d(f)$ by df (when $f \in \mathcal{P}$).

Prove the following:

(a) $\boxed{1}$ We have $d(fg) = (df) \cdot g + f \cdot dg$ for any $f, g \in \mathcal{P}$. (In the lingo of algebraists, this is saying that d is a *derivation* on $\mathcal{P}$.)

(b) $\boxed{1}$ We have $d(e_n) = (N - n + 1) e_{n-1}$ for any $n \in \mathbb{Z}$.

(c) $\boxed{1}$ We have $d(h_n) = (N + n - 1) h_{n-1}$ for any $n \in \mathbb{Z}$.

(d) $\boxed{1}$ We have $d(p_n) = np_{n-1}$ for any $n > 1$.

(e) $\boxed{1}$ We have $d(\sigma \cdot f) = \sigma \cdot (df)$ for any $f \in \mathcal{P}$ and any $\sigma \in S_N$.

(f) $\boxed{1}$ We have $df \in \mathcal{S}$ for each $f \in \mathcal{S}$.

(g) $\boxed{2}$ We have $d\left(a_\rho\right) = 0$. (Here, a_ρ is as in Definition 7.3.2.)

(h) $\boxed{5}$ Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ be an N-partition. Set $\lambda_{N+1} := 0$. Let D be the set of all $i \in [N]$ such that $\lambda_i > \lambda_{i+1}$. For each $i \in D$, let $\lambda - e_i$ denote the N-partition obtained from λ by subtracting 1 from the i-th entry; that is, we let

$$\lambda - e_i := (\lambda_1, \lambda_2, \ldots, \lambda_{i-1}, \lambda_i - 1, \lambda_{i+1}, \lambda_{i+2}, \ldots, \lambda_N).$$

(This is an N-partition, since $i \in D$ entails $\lambda_i > \lambda_{i+1}$ and thus $\lambda_i - 1 \geq \lambda_{i+1}$.)

Then,

$$d(s_\lambda) = \sum_{i \in D} (\lambda_i + N - i) s_{\lambda - e_i}. \tag{298}$$

[**Hint:** For part **(h)**, study how d acts on the alternant $a_{\lambda+\rho}$, and show that $d\left(a_\rho f\right) = a_\rho d(f)$ for any $f \in \mathcal{P}$.]

[**Remark:** The equality (298) can be restated in terms of Young diagrams as follows:

$$d(s_\lambda) = \sum k_{\lambda,\mu} s_\mu,$$

where

- the sum ranges over all N-partitions μ such that the Young diagram $Y(\mu)$ can be obtained from $Y(\lambda)$ by removing a single box (without shifting the remaining boxes);
- the coefficient $k_{\lambda,\mu}$ is defined to be $j + N - i$ if (i, j) is the box that must be removed from $Y(\lambda)$ to obtain $Y(\mu)$.

For example, for $N = 4$ and $\lambda = (3, 1, 1, 0)$, this says that

$$\begin{aligned} d\left(s_{(3,1,1,0)}\right) &= \underbrace{(\lambda_1 + N - 1)}_{=3+4-1=6} s_{(2,1,1,0)} + \underbrace{(\lambda_3 + N - 3)}_{=1+4-3=2} s_{(3,1,0,0)} \\ &= 6s_{(2,1,1,0)} + 2s_{(3,1,0,0)}. \text{]} \end{aligned}$$

Exercise A.6.3.15. Let I be the ideal of the ring $\mathcal{P}$ generated by the N polynomials $e_1, e_2, \ldots, e_N$.

(a) $\boxed{2}$ Prove that any homogeneous symmetric polynomial $f \in \mathcal{S}$ of positive degree is contained in I.

(b) $\boxed{7}$ Prove that the quotient ring $\mathcal{P}/I$ is a free K-module with basis

$$\left(\overline{x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}}\right)_{(a_1,a_2,\ldots,a_N) \in H_N},$$

where the $N!$-element set H_N is defined as in Definition 5.3.6 **(c)** (for $n = N$). (Here, the notation $\overline{f}$ denotes the projection of a polynomial $f \in \mathcal{P}$ onto the quotient ring $\mathcal{P}/I$.)

(c) $\boxed{5}$ More generally: Let $u_1, u_2, \ldots, u_N$ be N polynomials in $\mathcal{P}$ such that

$$\deg u_i < i \qquad \text{for each } i \in [N].$$

(The polynomials u_i need not be symmetric or homogeneous.) Let I' be the ideal of the ring $\mathcal{P}$ generated by the N polynomials

$$e_1 - u_1, \ e_2 - u_2, \ \ldots, \ e_N - u_N.$$

Prove that the quotient ring $\mathcal{P}/I'$ is a free K-module with basis

$$\left(\overline{x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}}\right)_{(a_1,a_2,\ldots,a_N) \in H_N},$$

where the $N!$-element set H_N is defined as in Definition 5.3.6 **(c)** (for $n = N$). (Here, the notation $\overline{f}$ denotes the projection of a polynomial $f \in \mathcal{P}$ onto the quotient ring $\mathcal{P}/I'$.)

B. Omitted details and proofs

This chapter contains some proofs (and parts of proofs) that have been omitted from the text above – usually because they are technical arguments or of tangential interest only.

Each of the proofs given below uses the notations and conventions of the chapter and section in which the respective claim appears.

B.1. x^n-equivalence

Detailed proof of Theorem 3.10.3. **(a)** We claim the following:

Claim 1: We have $f \overset{x^n}{\equiv} f$ for each $f \in K[[x]]$.

[*Proof of Claim 1:* Let $f \in K[[x]]$. Obviously, each $m \in \{0, 1, \ldots, n\}$ satisfies $[x^m] f = [x^m] f$. In other words, we have $f \overset{x^n}{\equiv} f$ (by Definition 3.10.1). This proves Claim 1.]

Claim 2: If three FPSs $f, g, h \in K[[x]]$ satisfy $f \overset{x^n}{\equiv} g$ and $g \overset{x^n}{\equiv} h$, then $f \overset{x^n}{\equiv} h$.

[*Proof of Claim 2:* Let $f, g, h \in K[[x]]$ be three FPSs satisfying $f \overset{x^n}{\equiv} g$ and $g \overset{x^n}{\equiv} h$. We must show that $f \overset{x^n}{\equiv} h$.

We have $f \overset{x^n}{\equiv} g$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] f = [x^m] g \tag{299}$$

(by Definition 3.10.1).

We have $g \overset{x^n}{\equiv} h$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] g = [x^m] h \tag{300}$$

(by Definition 3.10.1).

Now, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned} [x^m] f &= [x^m] g && (\text{by } (299)) \\ &= [x^m] h && (\text{by } (300)) . \end{aligned}$$

In other words, we have $f \overset{x^n}{\equiv} h$ (by Definition 3.10.1). This proves Claim 2.]

Claim 3: If two FPSs $f, g \in K[[x]]$ satisfy $f \overset{x^n}{\equiv} g$, then $g \overset{x^n}{\equiv} f$.

[*Proof of Claim 3:* Let $f, g \in K[[x]]$ be two FPSs satisfying $f \overset{x^n}{\equiv} g$. We must show that $g \overset{x^n}{\equiv} f$.

We have $f \overset{x^n}{\equiv} g$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] f = [x^m] g$$

(by Definition 3.10.1). In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] g = [x^m] f.$$

In other words, we have $g \overset{x^n}{\equiv} f$ (by Definition 3.10.1). This proves Claim 3.]

Now, the relation $\overset{x^n}{\equiv}$ is reflexive (by Claim 1), transitive (by Claim 2) and symmetric (by Claim 3). In other words, this relation $\overset{x^n}{\equiv}$ is an equivalence relation. This proves Theorem 3.10.3 **(a)**.

(b) Let $a, b, c, d \in K[[x]]$ be four FPSs satisfying $a \overset{x^n}{\equiv} b$ and $c \overset{x^n}{\equiv} d$.

We have $a \overset{x^n}{\equiv} b$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m] a = [x^m] b \tag{301}$$

(by Definition 3.10.1).

We have $c \overset{x^n}{\equiv} d$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m]\, c = [x^m]\, d \tag{302}$$

(by Definition 3.10.1).

Now, every $m \in \{0, 1, \ldots, n\}$ satisfies

$$[x^m]\,(a + c) = [x^m]\, a + [x^m]\, c \tag{303}$$

(by (18), applied to m, a and c instead of n, $\mathbf{a}$ and $\mathbf{b}$) and

$$[x^m]\,(b + d) = [x^m]\, b + [x^m]\, d \tag{304}$$

(by (18), applied to m, b and d instead of n, $\mathbf{a}$ and $\mathbf{b}$). Hence, every $m \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned}[x^m]\,(a + c) &= \underbrace{[x^m]\, a}_{\substack{=[x^m]b \\ \text{(by (301))}}} + \underbrace{[x^m]\, c}_{\substack{=[x^m]d \\ \text{(by (302))}}} \qquad \text{(by (303))} \\ &= [x^m]\, b + [x^m]\, d = [x^m]\,(b + d) \qquad \text{(by (304))}.\end{aligned}$$

In other words, $a + c \overset{x^n}{\equiv} b + d$ (by Definition 3.10.1). Thus, we have proved (97). The same argument (but with all "+" signs replaced by "−" signs, and with all references to (18) replaced by references to (19)) can be used to prove (98). It remains to prove (99).

Let $m \in \{0, 1, \ldots, n\}$. Then, $m \le n$.

Now, let $i \in \{0, 1, \ldots, m\}$. Then, $i \in \{0, 1, \ldots, m\} \subseteq \{0, 1, \ldots, n\}$ (since $m \le n$). Hence, (301) (applied to i instead of m) yields $\left[x^i\right] a = \left[x^i\right] b$. Furthermore, from $i \in \{0, 1, \ldots, m\}$, we obtain $m - i \in \{0, 1, \ldots, m\} \subseteq \{0, 1, \ldots, n\}$ (since $m \le n$). Hence, (302) (applied to $m - i$ instead of m) yields $\left[x^{m-i}\right] c = \left[x^{m-i}\right] d$. Multiplying the equalities $\left[x^i\right] a = \left[x^i\right] b$ and $\left[x^{m-i}\right] c = \left[x^{m-i}\right] d$, we obtain

$$\left[x^i\right] a \cdot \left[x^{m-i}\right] c = \left[x^i\right] b \cdot \left[x^{m-i}\right] d. \tag{305}$$

Forget that we fixed i. We thus have proved (305) for each $i \in \{0, 1, \ldots, m\}$. Now, (20) (applied to m, a and c instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields

$$[x^m]\,(ac) = \sum_{i=0}^{m} \underbrace{\left[x^i\right] a \cdot \left[x^{m-i}\right] c}_{\substack{=\left[x^i\right] b \cdot \left[x^{m-i}\right] d \\ \text{(by (305))}}} = \sum_{i=0}^{m} \left[x^i\right] b \cdot \left[x^{m-i}\right] d.$$

On the other hand, (20) (applied to m, b and d instead of n, $\mathbf{a}$ and $\mathbf{b}$) yields

$$[x^m]\,(bd) = \sum_{i=0}^{m} \left[x^i\right] b \cdot \left[x^{m-i}\right] d.$$

Comparing these two equalities, we find $[x^m]\,(ac) = [x^m]\,(bd)$.

Forget that we fixed m. We thus have shown that each $m \in \{0, 1, \ldots, n\}$ satisfies $[x^m](ac) = [x^m](bd)$. In other words, $ac \overset{x^n}{\equiv} bd$ (by Definition 3.10.1). Thus we have proved (99), so that the proof of Theorem 3.10.3 **(b)** is complete.

(c) Let $a, b \in K[[x]]$ be two FPSs satisfying $a \overset{x^n}{\equiv} b$. We have $a \overset{x^n}{\equiv} b$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m]\, a = [x^m]\, b \tag{306}$$

(by Definition 3.10.1). However, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$[x^m](\lambda a) = \lambda \cdot [x^m]\, a \tag{307}$$

(by (23), applied to n and a instead of m and $\mathbf{a}$) and

$$[x^m](\lambda b) = \lambda \cdot [x^m]\, b \tag{308}$$

(by (23), applied to n and b instead of m and $\mathbf{a}$). Now, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned}[x^m](\lambda a) &= \lambda \cdot \underbrace{[x^m]\, a}_{\substack{=[x^m]b \\ \text{(by (306))}}} \qquad \text{(by (307))} \\ &= \lambda \cdot [x^m]\, b = [x^m](\lambda b) \qquad \text{(by (308))}.\end{aligned}$$

In other words, $\lambda a \overset{x^n}{\equiv} \lambda b$ (by Definition 3.10.1). This proves Theorem 3.10.3 **(c)**.

(d) Let $a, b \in K[[x]]$ be two FPSs satisfying $a \overset{x^n}{\equiv} b$. We have $a \overset{x^n}{\equiv} b$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } [x^m]\, a = [x^m]\, b \tag{309}$$

(by Definition 3.10.1).

Now, we shall show that each $m \in \{0, 1, \ldots, n\}$ satisfies

$$[x^m]\left(a^{-1}\right) = [x^m]\left(b^{-1}\right). \tag{310}$$

[*Proof of (310):* We shall prove (310) by strong induction on m:

Induction step: Fix some $k \in \{0, 1, \ldots, n\}$. We assume (as an induction hypothesis) that (310) is true for any $m < k$. In other words, for any $m \in \{0, 1, \ldots, n\}$ satisfying $m < k$, we have

$$[x^m]\left(a^{-1}\right) = [x^m]\left(b^{-1}\right). \tag{311}$$

We shall now prove that (310) is true for $m = k$. In other words, we shall prove that $\left[x^k\right]\left(a^{-1}\right) = \left[x^k\right]\left(b^{-1}\right)$.

Proposition 3.3.7 shows that the FPS a is invertible in $K[[x]]$ if and only if its constant term $\left[x^0\right] a$ is invertible in K. Hence, its constant term $\left[x^0\right] a$ is invertible in K (since a is invertible in $K[[x]]$). Note that $k \leq n$ (since $k \in \{0, 1, \ldots, n\}$).

Applying (20) to k, a and a^{-1} instead of n, $\mathbf{a}$ and $\mathbf{b}$, we obtain

$$\begin{aligned}\left[x^k\right]\left(aa^{-1}\right) &= \sum_{i=0}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right]\left(a^{-1}\right) \\ &= \left[x^0\right] a \cdot \left[x^k\right]\left(a^{-1}\right) + \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right]\left(a^{-1}\right)\end{aligned}$$

(here, we have split off the addend for $i = 0$ from the sum). Thus,

$$\left[x^0\right] a \cdot \left[x^k\right] \left(a^{-1}\right) + \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right] \left(a^{-1}\right) = \left[x^k\right] \underbrace{\left(aa^{-1}\right)}_{=1} = \left[x^k\right] 1,$$

so that

$$\left[x^0\right] a \cdot \left[x^k\right] \left(a^{-1}\right) = \left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right] \left(a^{-1}\right).$$

We can divide this equality by $\left[x^0\right] a$ (since $\left[x^0\right] a$ is invertible in K), and thus obtain

$$\left[x^k\right] \left(a^{-1}\right) = \left(\left[x^0\right] a\right)^{-1} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] a \cdot \left[x^{k-i}\right] \left(a^{-1}\right)\right). \tag{312}$$

The same argument (applied to b instead of a) yields

$$\left[x^k\right] \left(b^{-1}\right) = \left(\left[x^0\right] b\right)^{-1} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] b \cdot \left[x^{k-i}\right] \left(b^{-1}\right)\right). \tag{313}$$

However, we observe the following:

- We have $0 \in \{0, 1, \ldots, n\}$ (since $n \in \mathbb{N}$) and thus $\left[x^0\right] a = \left[x^0\right] b$ (by (309), applied to $m = 0$).
- Each $i \in \{1, 2, \ldots, k\}$ satisfies $i \in \{1, 2, \ldots, k\} \subseteq \{0, 1, \ldots, n\}$ (since $1 \geq 0$ and $k \leq n$) and therefore
  $$\left[x^i\right] a = \left[x^i\right] b \tag{314}$$
  (by (306), applied to $m = i$).
- Each $i \in \{1, 2, \ldots, k\}$ satisfies $k - i \in \{0, 1, \ldots, k-1\} \subseteq \{0, 1, \ldots, n\}$ (since $k - 1 \leq k \leq n$) and $k - i < k$ (since $k - i \in \{0, 1, \ldots, k-1\}$, so that $k - i \leq k - 1 < k$), and therefore
  $$\left[x^{k-i}\right] \left(a^{-1}\right) = \left[x^{k-i}\right] \left(b^{-1}\right) \tag{315}$$
  (by (311), applied to $m = k - i$).

Hence, (312) becomes

$$\begin{aligned}
\left[x^k\right] \left(a^{-1}\right) &= \left(\underbrace{\left[x^0\right] a}_{=\left[x^0\right] b}\right)^{-1} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \underbrace{\left[x^i\right] a}_{\substack{=\left[x^i\right] b \\ \text{(by (314))}}} \cdot \underbrace{\left[x^{k-i}\right] \left(a^{-1}\right)}_{\substack{=\left[x^{k-i}\right]\left(b^{-1}\right) \\ \text{(by (315))}}}\right) \\
&= \left(\left[x^0\right] b\right)^{-1} \cdot \left(\left[x^k\right] 1 - \sum_{i=1}^{k} \left[x^i\right] b \cdot \left[x^{k-i}\right] \left(b^{-1}\right)\right) \\
&= \left[x^k\right] \left(b^{-1}\right) \qquad \text{(by (313))}.
\end{aligned}$$

In other words, (310) is true for $m = k$. This completes the induction step. Thus, (310) is proved.]

Thus, we have shown that each $m \in \{0, 1, \ldots, n\}$ satisfies $[x^m] (a^{-1}) = [x^m] (b^{-1})$. In other words, $a^{-1} \overset{x^n}{\equiv} b^{-1}$ (by Definition 3.10.1). This proves Theorem 3.10.3 **(d)**.

(e) Let us first prove (101):

[*Proof of (101):* We proceed by induction on $|S|$:

Induction base: It is easy to see that (101) holds for $|S| = 0$ [149].

Induction step: Let $k \in \mathbb{N}$. Assume (as the induction hypothesis) that (101) holds for $|S| = k$. We must prove that (101) holds for $|S| = k + 1$.

So let S, $(a_s)_{s \in S}$ and $(b_s)_{s \in S}$ be as in Theorem 3.10.3 **(e)**, and assume that $|S| = k + 1$. Then, $|S| = k + 1 > k \geq 0$, so that the set S is nonempty. In other words, there exists some $t \in S$. Consider this t. Each $s \in S \setminus \{t\}$ satisfies $s \in S \setminus \{t\} \subseteq S$ and thus $a_s \overset{x^n}{\equiv} b_s$ (by (100)). Moreover, from $t \in S$, we obtain $|S \setminus \{t\}| = |S| - 1 = k$ (since $|S| = k + 1$). Hence, we can apply (101) to $S \setminus \{t\}$ instead of S (since our induction hypothesis says that (101) holds for $|S| = k$). As a result, we obtain

$$\sum_{s \in S \setminus \{t\}} a_s \overset{x^n}{\equiv} \sum_{s \in S \setminus \{t\}} b_s.$$

On the other hand, $a_t \overset{x^n}{\equiv} b_t$ (by (100), applied to $s = t$). Hence, (97) (applied to $a = a_t$ and $b = b_t$ and $c = \sum\limits_{s \in S \setminus \{t\}} a_s$ and $d = \sum\limits_{s \in S \setminus \{t\}} b_s$) yields

$$a_t + \sum_{s \in S \setminus \{t\}} a_s \overset{x^n}{\equiv} b_t + \sum_{s \in S \setminus \{t\}} b_s.$$

In view of

$$\sum_{s \in S} a_s = a_t + \sum_{s \in S \setminus \{t\}} a_s \qquad \left(\begin{array}{c} \text{here, we have split off the} \\ \text{addend for } s = t \text{ from the sum} \end{array} \right)$$

and

$$\sum_{s \in S} b_s = b_t + \sum_{s \in S \setminus \{t\}} b_s \qquad \left(\begin{array}{c} \text{here, we have split off the} \\ \text{addend for } s = t \text{ from the sum} \end{array} \right),$$

[149] *Proof.* Let S, $(a_s)_{s \in S}$ and $(b_s)_{s \in S}$ be as in Theorem 3.10.3 **(e)**, and assume that $|S| = 0$. From $|S| = 0$, we obtain $S = \varnothing$. Hence,

$$\sum_{s \in S} a_s = (\text{empty sum}) = 0 \qquad \text{and}$$
$$\sum_{s \in S} b_s = (\text{empty sum}) = 0.$$

Comparing these two equalities, we obtain $\sum\limits_{s \in S} a_s = \sum\limits_{s \in S} b_s$. Hence, $\sum\limits_{s \in S} a_s \overset{x^n}{\equiv} \sum\limits_{s \in S} b_s$ (since the relation $\overset{x^n}{\equiv}$ is an equivalence relation and thus is reflexive). Thus, we have proved (101) under the assumption that $|S| = 0$.

this rewrites as

$$\sum_{s\in S} a_s \overset{x^n}{\equiv} \sum_{s\in S} b_s.$$

Hence, we have shown that (101) holds for $|S| = k+1$. This completes the induction step. Thus, the induction proof of (101) is complete.]

We have now proved (101). The exact same argument (but with all sums replaced by products, and with the reference to (97) replaced by a reference to (99)) can be used to prove (102). Hence, the proof of Theorem 3.10.3 **(e)** is complete. □

Detailed proof of Proposition 3.10.4. For each $m \in \{0, 1, \ldots, n\}$, we have

$$[x^m]\,(f-g) = [x^m]\,f - [x^m]\,g \tag{316}$$

(by (19), applied to m, f and g instead of n, $\mathbf{a}$ and $\mathbf{b}$).

Lemma 3.3.18 (applied to $f-g$ and $n+1$ instead of f and k) shows that the first $n+1$ coefficients of the FPS $f-g$ are 0 if and only if $f-g$ is a multiple of x^{n+1}.

Now, we have the following chain of logical equivalences:

$$\begin{aligned}
\left(f \overset{x^n}{\equiv} g\right) &\iff \left(\text{each } m \in \{0,1,\ldots,n\} \text{ satisfies } \underbrace{[x^m]\,f = [x^m]\,g}_{\iff ([x^m]f-[x^m]g=0)}\right) \\
&\qquad \text{(by Definition 3.10.1)} \\
&\iff \left(\text{each } m \in \{0,1,\ldots,n\} \text{ satisfies } \underbrace{[x^m]\,f - [x^m]\,g}_{\substack{=[x^m](f-g) \\ \text{(by (316))}}} = 0\right) \\
&\iff \left(\text{each } m \in \{0,1,\ldots,n\} \text{ satisfies } [x^m]\,(f-g) = 0\right) \\
&\iff \left(\text{the first } n+1 \text{ coefficients of the FPS } f-g \text{ are } 0\right) \\
&\iff \left(f-g \text{ is a multiple of } x^{n+1}\right)
\end{aligned}$$

(since we have seen that the first $n+1$ coefficients of the FPS $f-g$ are 0 if and only if $f-g$ is a multiple of x^{n+1}). In other words, we have $f \overset{x^n}{\equiv} g$ if and only if the FPS $f-g$ is a multiple of x^{n+1}. This proves Proposition 3.10.4. □

Detailed proof of Proposition 3.10.5. Write the FPS a in the form $a = \sum_{i\in\mathbb{N}} a_i x^i$ with $a_0, a_1, a_2, \ldots \in K$. Thus,

$$a_m = [x^m]\,a \qquad \text{for each } m \in \mathbb{N} \tag{317}$$

(by the definition of $[x^m]\,a$). Furthermore, Definition 3.5.1 yields

$$a \circ c = \sum_{i\in\mathbb{N}} a_i c^i \tag{318}$$

(since $a = \sum_{i\in\mathbb{N}} a_i x^i$ with $a_0, a_1, a_2, \ldots \in K$).

Write the FPS b in the form $b = \sum\limits_{i \in \mathbb{N}} b_i x^i$ with $b_0, b_1, b_2, \ldots \in K$. Thus,

$$b_m = \left[x^m\right] b \qquad \text{for each } m \in \mathbb{N} \tag{319}$$

(by the definition of $\left[x^m\right] b$). Furthermore, Definition 3.5.1 yields

$$b \circ d = \sum_{i \in \mathbb{N}} b_i d^i \tag{320}$$

(since $b = \sum\limits_{i \in \mathbb{N}} b_i x^i$ with $b_0, b_1, b_2, \ldots \in K$).

We have $a \overset{x^n}{\equiv} b$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } \left[x^m\right] a = \left[x^m\right] b \tag{321}$$

(by the definition of "$a \overset{x^n}{\equiv} b$"). Hence, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned} a_m &= \left[x^m\right] a \qquad \left(\text{by (317)}\right) \\ &= \left[x^m\right] b \qquad \left(\text{by (321)}\right) \\ &= b_m \qquad \left(\text{by (319)}\right). \end{aligned} \tag{322}$$

Now, we claim the following:

Claim 1: Let $i \in \{0, 1, \ldots, n\}$. Then, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\left[x^m\right] \left(a_i c^i\right) = \left[x^m\right] \left(b_i d^i\right).$$

[*Proof of Claim 1:* Let S be the set $\{1, 2, \ldots, i\}$. This set S is finite, and satisfies $|S| = i$. Moreover, we have $c \overset{x^n}{\equiv} d$ for each $s \in S$ (by assumption). Hence, (102) (applied to $a_s = c$ and $b_s = d$) yields

$$\prod_{s \in S} c \overset{x^n}{\equiv} \prod_{s \in S} d.$$

In view of

$$\prod_{s \in S} c = c^{|S|} = c^i \qquad (\text{since } |S| = i) \qquad \text{and}$$
$$\prod_{s \in S} d = d^{|S|} = d^i \qquad (\text{since } |S| = i),$$

we can rewrite this as $c^i \overset{x^n}{\equiv} d^i$. In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } \left[x^m\right] \left(c^i\right) = \left[x^m\right] \left(d^i\right) \tag{323}$$

(by the definition of "$c^i \overset{x^n}{\equiv} d^i$").

Now, let $m \in \{0,1,\ldots,n\}$. Then, (23) (applied to m, a_i and c^i instead of n, λ and $\mathbf{a}$) yields $[x^m]\left(a_i c^i\right) = a_i \cdot [x^m]\left(c^i\right)$. Similarly, $[x^m]\left(b_i d^i\right) = b_i \cdot [x^m]\left(d^i\right)$. On the other hand, (322) (applied to i instead of m) yields $a_i = b_i$. Hence,

$$\begin{aligned}[x^m]\left(a_i c^i\right) &= \underbrace{a_i}_{=b_i} \cdot \underbrace{[x^m]\left(c^i\right)}_{\substack{=[x^m]\left(d^i\right) \\ \text{(by (323))}}} = b_i \cdot [x^m]\left(d^i\right) \\ &= [x^m]\left(b_i d^i\right) \qquad \left(\text{since } [x^m]\left(b_i d^i\right) = b_i \cdot [x^m]\left(d^i\right)\right).\end{aligned}$$

This proves Claim 1.]

Next, we claim the following:

Claim 2: Let $m \in \mathbb{N}$. Let $i \in \mathbb{N} \setminus \{0,1,\ldots,m\}$. Then,

$$[x^m]\left(c^i\right) = 0 \tag{324}$$

and

$$[x^m]\left(d^i\right) = 0. \tag{325}$$

[*Proof of Claim 2:* We have $i \in \mathbb{N} \setminus \{0,1,\ldots,m\} = \{m+1, m+2, m+3, \ldots\}$, so that $i \geq m+1$ and therefore $m \leq i-1$. Hence, $m \in \{0,1,\ldots,i-1\}$ (since $m \in \mathbb{N}$).

By assumption, we have $\left[x^0\right] c = 0$. In other words, the 0-th coefficient of c is 0. In other words, the first 1 coefficient of the FPS c is 0. However, Lemma 3.3.18 (applied to $k = 1$ and $f = c$) yields that the first 1 coefficient of the FPS c is 0 if and only if c is a multiple of x^1. Hence, c is a multiple of x^1 (since the first 1 coefficient of the FPS c is 0). In other words, $c = x^1 h$ for some $h \in K[[x]]$. Consider this h. Now, $c = x^1 h = xh$, so that $c^i = (xh)^i = x^i h^i$. However, Lemma 3.3.17 (applied to i and h^i instead of k and a) yields that the first i coefficients of the FPS $x^i h^i$ are 0. In other words, the first i coefficients of the FPS c^i are 0 (since $c^i = x^i h^i$). In other words, $\left[x^j\right]\left(c^i\right) = 0$ for all $j \in \{0,1,\ldots,i-1\}$. We can apply this to $j = m$ (since $m \in \{0,1,\ldots,i-1\}$), and thus obtain $[x^m]\left(c^i\right) = 0$. This proves (324). The proof of (325) is analogous (but uses the FPS d instead of c). Thus, Claim 2 is proven.]

Next, we generalize Claim 1 to all $i \in \mathbb{N}$:

Claim 3: Let $i \in \mathbb{N}$. Let $m \in \{0,1,\ldots,n\}$. Then,

$$[x^m]\left(a_i c^i\right) = [x^m]\left(b_i d^i\right).$$

[*Proof of Claim 3:* If $i \in \{0,1,\ldots,m\}$, then this follows from Claim 1. Thus, for the rest of this proof, we WLOG assume that we don't have $i \in \{0,1,\ldots,m\}$. Hence, $i \notin \{0,1,\ldots,m\}$, so that $i \in \mathbb{N} \setminus \{0,1,\ldots,m\}$ (since $i \in \mathbb{N}$). Thus, Claim 2 applies, and therefore (324) and (325) hold.

Now, (23) (applied to m, a_i and c^i instead of n, λ and $\mathbf{a}$) yields $[x^m]\left(a_i c^i\right) = a_i \cdot \underbrace{[x^m]\left(c^i\right)}_{\substack{=0 \\ \text{(by (324))}}} = 0$. The same argument (applied to b_i and d instead of a_i and c) yields

$[x^m]\left(b_i d^i\right) = 0$. Comparing these two equalities, we obtain $[x^m]\left(a_i c^i\right) = [x^m]\left(b_i d^i\right)$. This proves Claim 3.] □

Now, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned}[x^m](a \circ c) &= [x^m]\left(\sum_{i\in\mathbb{N}} a_i c^i\right) \qquad \text{(by (318))} \\ &= \sum_{i\in\mathbb{N}} \underbrace{[x^m]\left(a_i c^i\right)}_{\substack{=[x^m]\left(b_i d^i\right) \\ \text{(by Claim 3)}}} = \sum_{i\in\mathbb{N}} [x^m]\left(b_i d^i\right) = [x^m]\underbrace{\left(\sum_{i\in\mathbb{N}} b_i d^i\right)}_{\substack{=b\circ d \\ \text{(by (320))}}} = [x^m](b \circ d).\end{aligned}$$

In other words, $a \circ c \overset{x^n}{\equiv} b \circ d$ (by the definition of "$a \circ c \overset{x^n}{\equiv} b \circ d$"). This proves Proposition 3.10.5.

B.2. Infinite products

Detailed proof of Proposition 3.11.7. Let us (temporarily) use two different notations for our two different definitions of a product: We let $\prod_{i\in I} \mathbf{a}_i$ denote the finite product $\prod_{i\in I} \mathbf{a}_i$ defined in the usual way (i.e., defined as in any commutative ring), whereas $\widetilde{\prod_{i\in I}} \mathbf{a}_i$ shall mean the product $\prod_{i\in I} \mathbf{a}_i$ defined according to Definition 3.11.5 **(b)**. Thus, our goal is to show that $\widetilde{\prod_{i\in I}} \mathbf{a}_i = \prod_{i\in I} \mathbf{a}_i$.

Definition 3.11.5 **(b)** shows that if $n \in \mathbb{N}$, and if M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$, then

$$[x^n]\left(\widetilde{\prod_{i\in I}} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M} \mathbf{a}_i\right). \tag{326}$$

Now, let $n \in \mathbb{N}$. The set I is finite (since the family $(\mathbf{a}_i)_{i\in I}$ is finite), and thus is a finite subset of I. Moreover, every finite subset J of I satisfying $I \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\prod_{i\in J} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in I} \mathbf{a}_i\right)$$

(because combining $I \subseteq J$ and $J \subseteq I$ yields $J = I$, and thus $[x^n]\left(\prod_{i\in J} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in I} \mathbf{a}_i\right)$). In other words, I determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ (by the definition of "determining the x^n-coefficient in a product"). Hence, we can apply (326) to $M = I$. As a consequence, we obtain

$$[x^n]\left(\widetilde{\prod_{i\in I}} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in I} \mathbf{a}_i\right).$$

Now, forget that we fixed n. We thus have proved

$$[x^n]\left(\widetilde{\prod_{i\in I}}\mathbf{a}_i\right)=[x^n]\left(\prod_{i\in I}\mathbf{a}_i\right)\qquad\text{for each } n\in\mathbb{N}.$$

In other words, each coefficient of the FPS $\widetilde{\prod\limits_{i\in I}}\mathbf{a}_i$ equals the corresponding coefficient of $\prod\limits_{i\in I}\mathbf{a}_i$. Hence, $\widetilde{\prod\limits_{i\in I}}\mathbf{a}_i=\prod\limits_{i\in I}\mathbf{a}_i$. This completes the proof of Proposition 3.11.7. □

Detailed proof of Lemma 3.11.9. We shall prove Lemma 3.11.9 by induction on $|J|$ (this is allowed, since the set J is supposed to be finite):

Induction base: Lemma 3.11.9 is true in the case when $|J|=0$ [150].

Induction step: Let $k\in\mathbb{N}$. Assume (as the induction hypothesis) that Lemma 3.11.9 is true in the case when $|J|=k$. We must prove that Lemma 3.11.9 is true in the case when $|J|=k+1$.

Let a, $(f_i)_{i\in J}$ and n be as in Lemma 3.11.9. Assume that $|J|=k+1$. Thus, $|J|=k+1>k\geq 0$; hence, the set J is nonempty. In other words, there exists some $j\in J$. Consider this j. We have $j\in J$ and therefore

$$[x^m]\left(f_j\right)=0\qquad\text{for each } m\in\{0,1,\ldots,n\}\tag{327}$$

(by (115), applied to $i=j$). Hence, Lemma 3.11.8 (applied to $a\prod\limits_{i\in J\setminus\{j\}}(1+f_i)$ and f_j instead of a and f) yields that

$$[x^m]\left(\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right)\left(1+f_j\right)\right)=[x^m]\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right)$$
$$\text{for each } m\in\{0,1,\ldots,n\}.$$

In view of

$$a\underbrace{\prod_{i\in J}(1+f_i)}_{\substack{=\left(1+f_j\right)\prod\limits_{i\in J\setminus\{j\}}(1+f_i)\\ \text{(here, we have split off the factor}\\ \text{for } i=j \text{ from the product)}}}=a\left(1+f_j\right)\prod_{i\in J\setminus\{j\}}(1+f_i)=\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right)\left(1+f_j\right),$$

[150] *Proof.* Let a, $(f_i)_{i\in J}$ and n be as in Lemma 3.11.9. Assume that $|J|=0$. Thus, $J=\varnothing$, so that the product $\prod\limits_{i\in J}(1+f_i)$ is empty. Hence, $\prod\limits_{i\in J}(1+f_i)=(\text{empty product})=1$. Hence, we have

$$[x^m]\left(a\underbrace{\prod_{i\in J}(1+f_i)}_{=1}\right)=[x^m]\,a\qquad\text{for each } m\in\{0,1,\ldots,n\}.$$

Thus, we have proved Lemma 3.11.9 under the assumption that $|J|=0$. Therefore, Lemma 3.11.9 is true in the case when $|J|=0$.

we can rewrite this as follows: We have

$$[x^m]\left(a\prod_{i\in J}(1+f_i)\right)=[x^m]\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right) \qquad (328)$$
$$\text{for each } m\in\{0,1,\ldots,n\}.$$

On the other hand, each $i\in J\setminus\{j\}$ satisfies $j\in J\setminus\{j\}\subseteq J$ and therefore

$$[x^m](f_i)=0 \qquad \text{for each } m\in\{0,1,\ldots,n\}$$

(by (115)). Furthermore, from $j\in J$, we obtain $|J\setminus\{j\}|=|J|-1=k$ (since $|J|=k+1$). Hence, we can apply Lemma 3.11.9 to $J\setminus\{j\}$ instead of J (because our induction hypothesis tells us that Lemma 3.11.9 is true in the case when $|J|=k$). We thus conclude that

$$[x^m]\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right)=[x^m]\,a \qquad \text{for each } m\in\{0,1,\ldots,n\}. \qquad (329)$$

Now, for each $m\in\{0,1,\ldots,n\}$, we obtain

$$\begin{aligned}[x^m]\left(a\prod_{i\in J}(1+f_i)\right)&=[x^m]\left(a\prod_{i\in J\setminus\{j\}}(1+f_i)\right) && \text{(by (328))}\\ &=[x^m]\,a && \text{(by (329))}.\end{aligned}$$

This is precisely the claim of Lemma 3.11.9. Thus, we have proved that Lemma 3.11.9 is true in the case when $|J|=k+1$. This completes the induction step. Thus, the induction proof of Lemma 3.11.9 is complete. □

Detailed proof of Theorem 3.11.10. The family $(f_i)_{i\in I}$ is summable. In other words,

$$\text{for each } n\in\mathbb{N}, \text{ all but finitely many } i\in I \text{ satisfy } [x^n]\,f_i=0$$

(by the definition of "summable"). In other words, for each $n\in\mathbb{N}$, there exists a finite subset I_n of I such that

$$\text{all } i\in I\setminus I_n \text{ satisfy } [x^n]\,f_i=0. \qquad (330)$$

Consider this subset I_n. Thus, all the sets $I_0,I_1,I_2,\ldots$ are finite subsets of I.

Now, let $n\in\mathbb{N}$ be arbitrary. Let $M:=I_0\cup I_1\cup\cdots\cup I_n$. Then, M is a union of $n+1$ finite subsets of I (because all the sets $I_0,I_1,I_2,\ldots$ are finite subsets of I), and thus itself is a finite subset of I. Moreover,

$$\text{all } m\in\{0,1,\ldots,n\} \text{ and all } i\in I\setminus M \text{ satisfy } [x^m]\,f_i=0. \qquad (331)$$

[*Proof of (331):* Let $m\in\{0,1,\ldots,n\}$ and $i\in I\setminus M$. We must show that $[x^m]\,f_i=0$.

From $m\in\{0,1,\ldots,n\}$, we obtain $I_m\subseteq I_0\cup I_1\cup\cdots\cup I_n=M$, so that $M\supseteq I_m$ and thus $I\setminus\underbrace{M}_{\supseteq I_m}\subseteq I\setminus I_m$. Hence, $i\in I\setminus M\subseteq I\setminus I_m$. Therefore, (330) (applied to m instead of n) yields $[x^m]\,f_i=0$. This proves (331).]

Now, we shall prove that the set M determines the x^n-coefficient in the product of $(1+f_i)_{i\in I}$. Indeed, let J be a finite subset of I satisfying $M \subseteq J \subseteq I$. Let a be the FPS $\prod\limits_{i\in M}(1+f_i)$ (this is well-defined, since the set M is finite). We have $J \setminus M \subseteq J$, so that the set $J \setminus M$ is finite (since J is finite). Hence, $(f_i)_{i\in J\setminus M}$ is a finite family of FPSs. Moreover, each $i \in J \setminus M$ satisfies

$$[x^m] f_i = 0 \qquad \text{for each } m \in \{0,1,\ldots,n\}$$

(by (331), because $i \in \underbrace{J}_{\subseteq I} \setminus M \subseteq I \setminus M$). Thus, Lemma 3.11.9 (applied to $J \setminus M$ instead of J) yields

$$[x^m]\left(a \prod_{i\in J\setminus M}(1+f_i)\right) = [x^m]\, a \qquad \text{for each } m \in \{0,1,\ldots,n\}.$$

Applying this to $m = n$, we find

$$[x^n]\left(a \prod_{i\in J\setminus M}(1+f_i)\right) = [x^n]\, a = [x^n]\left(\prod_{i\in M}(1+f_i)\right) \tag{332}$$

(since $a = \prod\limits_{i\in M}(1+f_i)$). However, the finite set J is the union of the two disjoint sets M and $J \setminus M$ (since $M \subseteq J$). Hence, the product $\prod\limits_{i\in J}(1+f_i)$ can be split as follows:

$$\prod_{i\in J}(1+f_i) = \underbrace{\left(\prod_{i\in M}(1+f_i)\right)}_{\substack{=a \\ \text{(by the definition of } a)}} \left(\prod_{i\in J\setminus M}(1+f_i)\right) = a \prod_{i\in J\setminus M}(1+f_i).$$

In view of this, we can rewrite (332) as

$$[x^n]\left(\prod_{i\in J}(1+f_i)\right) = [x^n]\left(\prod_{i\in M}(1+f_i)\right).$$

Forget that we fixed J. We thus have shown that every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\prod_{i\in J}(1+f_i)\right) = [x^n]\left(\prod_{i\in M}(1+f_i)\right).$$

In other words, the set M determines the x^n-coefficient in the product of $(1+f_i)_{i\in I}$ (according to Definition 3.11.1 **(b)**). Hence, the x^n-coefficient in the product of $(1+f_i)_{i\in I}$ is finitely determined (according to Definition 3.11.3 **(b)**).

Forget that we fixed $n \in \mathbb{N}$. Hence, we have shown that for each $n \in \mathbb{N}$, the x^n-coefficient in the product of $(1+f_i)_{i\in I}$ is finitely determined. In other words, each coefficient in this product is finitely determined. In other words, the family $(1+f_i)_{i\in I}$ is multipliable (by the definition of "multipliable"). This proves Theorem 3.11.10. □

Detailed proof of Proposition 3.11.11. Let $(\mathbf{a}_i)_{i\in I} \in K[[x]]^I$ be a family of FPSs. Assume that all but finitely many entries of this family $(\mathbf{a}_i)_{i\in I}$ equal 1 (that is, all but finitely many $i \in I$ satisfy $\mathbf{a}_i = 1$). We must prove that this family is multipliable.

We have assumed that all but finitely many $i \in I$ satisfy $\mathbf{a}_i = 1$. In other words, there exists a finite subset M of I such that

$$\text{all } i \in I \setminus M \text{ satisfy } \mathbf{a}_i = 1. \tag{333}$$

Consider this M.

Let $n \in \mathbb{N}$. Every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^n]\left(\prod_{i\in J} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M} \mathbf{a}_i\right)$$

[151]. In other words, the set M determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ (by the definition of "determining the x^n-coefficient in a product"). Hence, the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined (by the definition of "finitely determined").

Forget that we fixed n. We thus have proved that for each $n \in \mathbb{N}$, the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined. In other words, each coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined. In other words, the family $(\mathbf{a}_i)_{i\in I}$ is multipliable (by the definition of "multipliable"). This proves Proposition 3.11.11. □

Detailed proof of Lemma 3.11.15. Fix $m \in \{0, 1, \ldots, n\}$. Recall that the family $(\mathbf{a}_i)_{i\in I}$ is multipliable. In other words, each coefficient in its product is finitely determined. Hence, in particular, the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined. In other words, there is a finite subset M of I that determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$. Consider this subset M, and denote it by M_m. Thus, M_m is a finite subset of I that determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$.

Forget that we fixed m. Thus, for each $m \in \{0, 1, \ldots, n\}$, we have defined a finite subset M_m of I. Let M be the union $M_0 \cup M_1 \cup \cdots \cup M_n$ of these (altogether $n+1$) subsets. Thus, M is a union of finitely many finite subsets of I; hence, M itself is a finite subset of I.

[151] *Proof.* Let J be a finite subset of I satisfying $M \subseteq J \subseteq I$. Then, each $i \in J \setminus M$ satisfies $i \in \underbrace{J}_{\subseteq I} \setminus M \subseteq I \setminus M$ and therefore

$$\mathbf{a}_i = 1 \tag{334}$$

(by (333)). However, the set J is the union of the two disjoint sets M and $J \setminus M$ (since $M \subseteq J$). Hence, we can split the product $\prod_{i\in J} \mathbf{a}_i$ as follows:

$$\prod_{i\in J} \mathbf{a}_i = \left(\prod_{i\in M} \mathbf{a}_i\right)\left(\prod_{i\in J\setminus M} \underbrace{\mathbf{a}_i}_{\substack{=1 \\ \text{(by (334))}}}\right) = \left(\prod_{i\in M} \mathbf{a}_i\right)\underbrace{\left(\prod_{i\in J\setminus M} 1\right)}_{=1} = \prod_{i\in M} \mathbf{a}_i.$$

Therefore, $[x^n]\left(\prod_{i\in J} \mathbf{a}_i\right) = [x^n]\left(\prod_{i\in M} \mathbf{a}_i\right)$, qed.

Now, let $m \in \{0, 1, \ldots, n\}$. We shall show that M determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$.

Indeed, let N be a finite subset of I satisfying $M \subseteq N \subseteq I$. We have $M_m \subseteq M$ (since M is the union $M_0 \cup M_1 \cup \cdots \cup M_n$, while M_m is one of the sets in this union). Hence, $M_m \subseteq M \subseteq N$. Now, recall that the set M_m determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ (by the definition of M_m). In other words, every finite subset J of I satisfying $M_m \subseteq J \subseteq I$ satisfies

$$[x^m] \left(\prod_{i \in J} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M_m} \mathbf{a}_i \right) \tag{335}$$

(by the definition of what it means to "determine the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$"). Applying this to $J = N$, we obtain

$$[x^m] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M_m} \mathbf{a}_i \right)$$

(since N is a finite subset of I satisfying $M_m \subseteq N \subseteq I$). On the other hand, we can apply (335) to $J = M$ (since M is a finite subset of I satisfying $M_m \subseteq M \subseteq I$), and thus obtain

$$[x^m] \left(\prod_{i \in M} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M_m} \mathbf{a}_i \right).$$

Comparing these two equalities, we obtain

$$[x^m] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M} \mathbf{a}_i \right).$$

Forget that we fixed N. We thus have shown that every finite subset N of I satisfying $M \subseteq N \subseteq I$ satisfies $[x^m] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M} \mathbf{a}_i \right)$. Renaming N as J in this statement, we obtain the following: Every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies $[x^m] \left(\prod_{i \in J} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M} \mathbf{a}_i \right)$. In other words, M determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ (by the definition of what it means to "determine the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$").

Forget that we fixed m. We thus have shown that M determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ for each $m \in \{0, 1, \ldots, n\}$. In other words, M determines the first $n + 1$ coefficients in the product of $(\mathbf{a}_i)_{i \in I}$. In other words, M is an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$ (by the definition of an "x^n-approximator"). Hence, there exists an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$. This proves Lemma 3.11.15. □

Detailed proof of Proposition 3.11.16. The set M is an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$. In other words, M is a finite subset of I that determines the first $n + 1$ coefficients in the product of $(\mathbf{a}_i)_{i \in I}$ (by the definition of an "x^n-approximator").

(a) Let $m \in \{0, 1, \ldots, n\}$. Recall that M determines the first $n + 1$ coefficients in the product of $(\mathbf{a}_i)_{i \in I}$. Thus, in particular, M determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ (since $m \in \{0,1,\ldots,n\}$). In other words, every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$[x^m]\left(\prod_{i\in J}\mathbf{a}_i\right) = [x^m]\left(\prod_{i\in M}\mathbf{a}_i\right) \qquad (336)$$

(by the definition of "determining the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$").

Forget that we fixed m. We thus have proved that every $m \in \{0,1,\ldots,n\}$ and every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfy (336).

Now, let J be a finite subset of I satisfying $M \subseteq J \subseteq I$. Then, each $m \in \{0,1,\ldots,n\}$ satisfies $[x^m]\left(\prod\limits_{i\in J}\mathbf{a}_i\right) = [x^m]\left(\prod\limits_{i\in M}\mathbf{a}_i\right)$ (by (336)). In other words, we have $\prod\limits_{i\in J}\mathbf{a}_i \overset{x^n}{\equiv} \prod\limits_{i\in M}\mathbf{a}_i$ (by Definition 3.10.1). This proves Proposition 3.11.16 **(a)**.

(b) Assume that the family $(\mathbf{a}_i)_{i\in I}$ is multipliable. Let $m \in \{0,1,\ldots,n\}$. Thus, M determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ (since M determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i\in I}$).

The product $\prod\limits_{i\in I}\mathbf{a}_i$ is defined according to Definition 3.11.5 **(b)**. Specifically, Definition 3.11.5 **(b)** (with n and M renamed as k and N) shows that the product $\prod\limits_{i\in I}\mathbf{a}_i$ is defined to be the FPS whose x^k-coefficient (for any $k \in \mathbb{N}$) can be computed as follows: If $k \in \mathbb{N}$, and if N is a finite subset of I that determines the x^k-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$, then

$$\left[x^k\right]\left(\prod_{i\in I}\mathbf{a}_i\right) = \left[x^k\right]\left(\prod_{i\in N}\mathbf{a}_i\right).$$

We can apply this to $k = m$ and $N = M$ (since M is a finite subset of I that determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$), and thus obtain

$$[x^m]\left(\prod_{i\in I}\mathbf{a}_i\right) = [x^m]\left(\prod_{i\in M}\mathbf{a}_i\right).$$

Forget that we fixed m. We thus have proved that each $m \in \{0,1,\ldots,n\}$ satisfies $[x^m]\left(\prod\limits_{i\in I}\mathbf{a}_i\right) = [x^m]\left(\prod\limits_{i\in M}\mathbf{a}_i\right)$. In other words, $\prod\limits_{i\in I}\mathbf{a}_i \overset{x^n}{\equiv} \prod\limits_{i\in M}\mathbf{a}_i$ (by Definition 3.10.1). This proves Proposition 3.11.16 **(b)**. □

Detailed proof of Proposition 3.11.17. **(a)** Fix $n \in \mathbb{N}$. We know that the family $(\mathbf{a}_i)_{i\in J}$ is multipliable. Hence, there exists an x^n-approximator U for $(\mathbf{a}_i)_{i\in J}$ (by Lemma 3.11.15, applied to J instead of I). Consider this U.

We also know that the family $(\mathbf{a}_i)_{i\in I\setminus J}$ is multipliable. Hence, there exists an x^n-approximator V for $(\mathbf{a}_i)_{i\in I\setminus J}$ (by Lemma 3.11.15, applied to $I\setminus J$ instead of I). Consider this V.

We know that U is an x^n-approximator for $(\mathbf{a}_i)_{i\in J}$. In other words, U is a finite subset of J that determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i\in J}$ (by the definition of an x^n-approximator). Hence, in particular, U is finite. Similarly, V is finite. Moreover, $U \subseteq J$ (since U is a subset of J); similarly, $V \subseteq I\setminus J$.

Let $M = U \cup V$. This set M is finite (since U and V are finite). Moreover, using $U \subseteq J \subseteq I$ and $V \subseteq I\setminus J \subseteq I$, we obtain $M = \underbrace{U}_{\subseteq I} \cup \underbrace{V}_{\subseteq I} \subseteq I \cup I = I$. Hence, M is a finite subset of I. Note that the sets U and V are disjoint[152]. Hence, the set M is the union of its two disjoint subsets U and V (since $M = U \cup V$).

Now, let N be a finite subset of I satisfying $M \subseteq N \subseteq I$. We shall show that

$$[x^n] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^n] \left(\prod_{i \in M} \mathbf{a}_i \right).$$

Indeed, let $m \in \{0, 1, \ldots, n\}$. The set $N \cap J$ is a finite subset of J (since N is a finite subset of I) and satisfies $U \subseteq N \cap J$ (since $U \subseteq U \cup V = M \subseteq N$ and $U \subseteq J$). Now, recall that U determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i \in J}$. Hence, U determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in J}$ (since $m \in \{0, 1, \ldots, n\}$). In other words, every finite subset T of J satisfying $U \subseteq T \subseteq J$ satisfies

$$[x^m] \left(\prod_{i \in T} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in U} \mathbf{a}_i \right)$$

(by the definition of what it means to "determine the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in J}$"). We can apply this to $T = N \cap J$ (since $N \cap J$ is a finite subset of J satisfying $U \subseteq N \cap J \subseteq J$), and thus obtain

$$[x^m] \left(\prod_{i \in N \cap J} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in U} \mathbf{a}_i \right). \qquad (337)$$

The same argument (applied to $I \setminus J$ and V instead of J and U) yields

$$[x^m] \left(\prod_{i \in N \cap (I \setminus J)} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in V} \mathbf{a}_i \right).$$

In view of $N \cap (I \setminus J) = \underbrace{(N \cap I)}_{\substack{=N \\ (\text{since } N \subseteq I)}} \setminus J = N \setminus J$, this rewrites as

$$[x^m] \left(\prod_{i \in N \setminus J} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in V} \mathbf{a}_i \right). \qquad (338)$$

Forget that we fixed m. We thus have proved the equalities (337) and (338) for each $m \in \{0, 1, \ldots, n\}$. Hence, Lemma 3.3.22 (applied to $a = \prod\limits_{i \in N \cap J} \mathbf{a}_i$ and $b = \prod\limits_{i \in U} \mathbf{a}_i$ and $c = \prod\limits_{i \in N \setminus J} \mathbf{a}_i$ and $d = \prod\limits_{i \in V} \mathbf{a}_i$) yields that

$$[x^m] \left(\left(\prod_{i \in N \cap J} \mathbf{a}_i \right) \left(\prod_{i \in N \setminus J} \mathbf{a}_i \right) \right) = [x^m] \left(\left(\prod_{i \in U} \mathbf{a}_i \right) \left(\prod_{i \in V} \mathbf{a}_i \right) \right)$$

[152] Indeed, $\underbrace{U}_{\subseteq J} \cap \underbrace{V}_{\subseteq I \setminus J} \subseteq J \cap (I \setminus J) = \varnothing$, so that $U \cap V = \varnothing$.

for each $m \in \{0, 1, \ldots, n\}$. In view of

$$\prod_{i \in N} \mathbf{a}_i = \left(\prod_{i \in N \cap J} \mathbf{a}_i \right) \left(\prod_{i \in N \setminus J} \mathbf{a}_i \right) \qquad \left(\begin{array}{c} \text{since the set } N \text{ is the union of its} \\ \text{two disjoint subsets } N \cap J \text{ and } N \setminus J \end{array} \right)$$

and

$$\prod_{i \in M} \mathbf{a}_i = \left(\prod_{i \in U} \mathbf{a}_i \right) \left(\prod_{i \in V} \mathbf{a}_i \right) \qquad \left(\begin{array}{c} \text{since the set } M \text{ is the union of its} \\ \text{two disjoint subsets } U \text{ and } V \end{array} \right),$$

this rewrites as follows: We have

$$[x^m] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^m] \left(\prod_{i \in M} \mathbf{a}_i \right)$$

for each $m \in \{0, 1, \ldots, n\}$. Applying this to $m = n$, we obtain

$$[x^n] \left(\prod_{i \in N} \mathbf{a}_i \right) = [x^n] \left(\prod_{i \in M} \mathbf{a}_i \right).$$

Forget that we fixed N. We thus have shown that every finite subset N of I satisfying $M \subseteq N \subseteq I$ satisfies $[x^n] \left(\prod\limits_{i \in N} \mathbf{a}_i \right) = [x^n] \left(\prod\limits_{i \in M} \mathbf{a}_i \right)$. In other words, M determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ (by the definition of what it means to "determine the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$"). Hence, the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ is finitely determined (by the definition of "finitely determined", since M is a finite subset of I).

Forget that we fixed n. We thus have proved that for each $n \in \mathbb{N}$, the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ is finitely determined. In other words, each coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ is finitely determined. In other words, the family $(\mathbf{a}_i)_{i \in I}$ is multipliable (by the definition of "multipliable"). This proves Proposition 3.11.17 **(a)**.

(b) Proposition 3.11.17 **(a)** shows that the family $(\mathbf{a}_i)_{i \in I}$ is multipliable.

Let $n \in \mathbb{N}$. In our above proof of Proposition 3.11.17 **(a)**, we have seen the following:

- There exists an x^n-approximator U for $(\mathbf{a}_i)_{i \in J}$.
- There exists an x^n-approximator V for $(\mathbf{a}_i)_{i \in I \setminus J}$.

Consider these U and V. Let $M = U \cup V$. In our above proof of Proposition 3.11.17 **(a)**, we have seen the following:

- The set M is a finite subset of I.
- The set M is the union of its two disjoint subsets U and V.
- The set M determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$.

Now, the definition of the infinite product $\prod\limits_{i\in I}\mathbf{a}_i$ (namely, Definition 3.11.5 **(b)**) yields that

$$\left[x^n\right]\left(\prod_{i\in I}\mathbf{a}_i\right)=\left[x^n\right]\left(\prod_{i\in M}\mathbf{a}_i\right)\tag{339}$$

(since M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$). On the other hand, the set U is an x^n-approximator for $(\mathbf{a}_i)_{i\in J}$. Thus, Proposition 3.11.16 **(b)** (applied to J and U instead of I and M) yields

$$\prod_{i\in J}\mathbf{a}_i\overset{x^n}{\equiv}\prod_{i\in U}\mathbf{a}_i\tag{340}$$

(since the family $(\mathbf{a}_i)_{i\in J}$ is multipliable). Furthermore, the set V is an x^n-approximator for $(\mathbf{a}_i)_{i\in I\setminus J}$. Thus, Proposition 3.11.16 **(b)** (applied to $I\setminus J$ and V instead of I and M) yields

$$\prod_{i\in I\setminus J}\mathbf{a}_i\overset{x^n}{\equiv}\prod_{i\in V}\mathbf{a}_i\tag{341}$$

(since the family $(\mathbf{a}_i)_{i\in I\setminus J}$ is multipliable). From (340) and (341), we obtain

$$\left(\prod_{i\in J}\mathbf{a}_i\right)\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right)\overset{x^n}{\equiv}\left(\prod_{i\in U}\mathbf{a}_i\right)\left(\prod_{i\in V}\mathbf{a}_i\right)$$

(by (99), applied to $a=\prod\limits_{i\in J}\mathbf{a}_i$ and $b=\prod\limits_{i\in U}\mathbf{a}_i$ and $c=\prod\limits_{i\in I\setminus J}\mathbf{a}_i$ and $d=\prod\limits_{i\in V}\mathbf{a}_i$). In view of

$$\prod_{i\in M}\mathbf{a}_i=\left(\prod_{i\in U}\mathbf{a}_i\right)\left(\prod_{i\in V}\mathbf{a}_i\right)\qquad\left(\begin{array}{c}\text{since the set } M \text{ is the union of its}\\ \text{two disjoint subsets } U \text{ and } V\end{array}\right),$$

this rewrites as

$$\left(\prod_{i\in J}\mathbf{a}_i\right)\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right)\overset{x^n}{\equiv}\prod_{i\in M}\mathbf{a}_i.$$

In other words,

$$\text{each } m\in\{0,1,\ldots,n\} \text{ satisfies } \left[x^m\right]\left(\left(\prod_{i\in J}\mathbf{a}_i\right)\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right)\right)=\left[x^m\right]\left(\prod_{i\in M}\mathbf{a}_i\right)$$

(by Definition 3.10.1). Applying this to $m=n$, we obtain

$$\left[x^n\right]\left(\left(\prod_{i\in J}\mathbf{a}_i\right)\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right)\right)=\left[x^n\right]\left(\prod_{i\in M}\mathbf{a}_i\right).$$

Comparing this with (339), we obtain

$$\left[x^n\right]\left(\prod_{i\in I}\mathbf{a}_i\right)=\left[x^n\right]\left(\left(\prod_{i\in J}\mathbf{a}_i\right)\left(\prod_{i\in I\setminus J}\mathbf{a}_i\right)\right).\tag{342}$$

Now, forget that we fixed n. We thus have proved that each $n \in \mathbb{N}$ satisfies (342). In other words, each coefficient of the FPS $\prod\limits_{i \in I} \mathbf{a}_i$ equals the corresponding coefficient of $\left(\prod\limits_{i \in J} \mathbf{a}_i\right) \left(\prod\limits_{i \in I \setminus J} \mathbf{a}_i\right)$. Hence, we have

$$\prod_{i \in I} \mathbf{a}_i = \left(\prod_{i \in J} \mathbf{a}_i\right) \cdot \left(\prod_{i \in I \setminus J} \mathbf{a}_i\right).$$

This proves Proposition 3.11.17 **(b)**. □

Detailed proof of Proposition 3.11.18. **(a)** Fix $n \in \mathbb{N}$. We know that the family $(\mathbf{a}_i)_{i \in I}$ is multipliable. Hence, there exists an x^n-approximator U for $(\mathbf{a}_i)_{i \in I}$ (by Lemma 3.11.15). Consider this U.

We also know that the family $(\mathbf{b}_i)_{i \in I}$ is multipliable. Hence, there exists an x^n-approximator V for $(\mathbf{b}_i)_{i \in I}$ (by Lemma 3.11.15, applied to $\mathbf{b}_i$ instead of $\mathbf{a}_i$). Consider this V.

We know that U is an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$. In other words, U is a finite subset of I that determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i \in I}$ (by the definition of an x^n-approximator). Hence, in particular, U is finite. Similarly, V is finite. Moreover, $U \subseteq I$ (since U is a subset of I); similarly, $V \subseteq I$.

Let $M = U \cup V$. This set M is finite (since U and V are finite). Moreover, using $U \subseteq I$ and $V \subseteq I$, we obtain $M = \underbrace{U}_{\subseteq I} \cup \underbrace{V}_{\subseteq I} \subseteq I \cup I = I$. Hence, M is a finite subset of I.

Now, let N be a finite subset of I satisfying $M \subseteq N \subseteq I$. We shall show that

$$[x^n]\left(\prod_{i \in N} (\mathbf{a}_i \mathbf{b}_i)\right) = [x^n]\left(\prod_{i \in M} (\mathbf{a}_i \mathbf{b}_i)\right).$$

Indeed, let $m \in \{0, 1, \ldots, n\}$. We have $U \subseteq U \cup V = M \subseteq N$. The set N is a finite subset of I and satisfies $U \subseteq N$. Now, recall that U determines the first $n+1$ coefficients in the product of $(\mathbf{a}_i)_{i \in I}$. Hence, U determines the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$ (since $m \in \{0, 1, \ldots, n\}$). In other words, every finite subset T of I satisfying $U \subseteq T \subseteq I$ satisfies

$$[x^m]\left(\prod_{i \in T} \mathbf{a}_i\right) = [x^m]\left(\prod_{i \in U} \mathbf{a}_i\right) \tag{343}$$

(by the definition of what it means to "determine the x^m-coefficient in the product of $(\mathbf{a}_i)_{i \in I}$"). We can apply this to $T = N$ (since N is a finite subset of I satisfying $U \subseteq N \subseteq I$), and thus obtain

$$[x^m]\left(\prod_{i \in N} \mathbf{a}_i\right) = [x^m]\left(\prod_{i \in U} \mathbf{a}_i\right).$$

However, we can also apply (343) to $T = M$ (since M is a finite subset of I satisfying $U \subseteq M \subseteq I$), and thus obtain

$$[x^m]\left(\prod_{i \in M} \mathbf{a}_i\right) = [x^m]\left(\prod_{i \in U} \mathbf{a}_i\right).$$

Comparing these two equalities, we obtain

$$[x^m]\left(\prod_{i\in N}\mathbf{a}_i\right)=[x^m]\left(\prod_{i\in M}\mathbf{a}_i\right). \tag{344}$$

The same argument (applied to $\mathbf{b}_i$ and V instead of $\mathbf{a}_i$ and U) yields

$$[x^m]\left(\prod_{i\in N}\mathbf{b}_i\right)=[x^m]\left(\prod_{i\in M}\mathbf{b}_i\right). \tag{345}$$

Forget that we fixed m. We thus have proved the equalities (344) and (345) for each $m\in\{0,1,\ldots,n\}$. Hence, Lemma 3.3.22 (applied to $a=\prod\limits_{i\in N}\mathbf{a}_i$ and $b=\prod\limits_{i\in M}\mathbf{a}_i$ and $c=\prod\limits_{i\in N}\mathbf{b}_i$ and $d=\prod\limits_{i\in M}\mathbf{b}_i$) yields that

$$[x^m]\left(\left(\prod_{i\in N}\mathbf{a}_i\right)\left(\prod_{i\in N}\mathbf{b}_i\right)\right)=[x^m]\left(\left(\prod_{i\in M}\mathbf{a}_i\right)\left(\prod_{i\in M}\mathbf{b}_i\right)\right)$$

for each $m\in\{0,1,\ldots,n\}$. Applying this to $m=n$, we obtain

$$[x^n]\left(\left(\prod_{i\in N}\mathbf{a}_i\right)\left(\prod_{i\in N}\mathbf{b}_i\right)\right)=[x^n]\left(\left(\prod_{i\in M}\mathbf{a}_i\right)\left(\prod_{i\in M}\mathbf{b}_i\right)\right).$$

In view of

$$\prod_{i\in N}(\mathbf{a}_i\mathbf{b}_i)=\left(\prod_{i\in N}\mathbf{a}_i\right)\left(\prod_{i\in N}\mathbf{b}_i\right)\qquad\left(\begin{array}{c}\text{by the standard rules for finite}\\ \text{products, since } N \text{ is a finite set}\end{array}\right)$$

and

$$\prod_{i\in M}(\mathbf{a}_i\mathbf{b}_i)=\left(\prod_{i\in M}\mathbf{a}_i\right)\left(\prod_{i\in M}\mathbf{b}_i\right)\qquad\left(\begin{array}{c}\text{by the standard rules for finite}\\ \text{products, since } M \text{ is a finite set}\end{array}\right),$$

this rewrites as

$$[x^n]\left(\prod_{i\in N}(\mathbf{a}_i\mathbf{b}_i)\right)=[x^n]\left(\prod_{i\in M}(\mathbf{a}_i\mathbf{b}_i)\right).$$

Forget that we fixed N. We thus have shown that every finite subset N of I satisfying $M\subseteq N\subseteq I$ satisfies $[x^n]\left(\prod\limits_{i\in N}(\mathbf{a}_i\mathbf{b}_i)\right)=[x^n]\left(\prod\limits_{i\in M}(\mathbf{a}_i\mathbf{b}_i)\right)$. In other words, M determines the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ (by the definition of what it means to "determine the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$"). Hence, the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is finitely determined (by the definition of "finitely determined", since M is a finite subset of I).

Forget that we fixed n. We thus have proved that for each $n\in\mathbb{N}$, the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is finitely determined. In other words, each coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is finitely determined. In other words, the family $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is multipliable (by the definition of "multipliable"). This proves Proposition 3.11.18 **(a)**.

(b) Proposition 3.11.18 **(a)** shows that the family $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$ is multipliable.

Let $n\in\mathbb{N}$. In our above proof of Proposition 3.11.18 **(a)**, we have seen the following:

- There exists an x^n-approximator U for $(\mathbf{a}_i)_{i\in I}$.
- There exists an x^n-approximator V for $(\mathbf{b}_i)_{i\in I}$.

Consider these U and V. Let $M = U \cup V$. Thus, $M = U \cup V \supseteq U$ and $M = U \cup V \supseteq V$. In our above proof of Proposition 3.11.18 **(a)**, we have seen the following:

- The set M is a finite subset of I.
- The set M determines the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$.

We recall that the relation $\overset{x^n}{\equiv}$ on $K[[x]]$ is an equivalence relation (by Theorem 3.10.3 **(a)**). Thus, this relation $\overset{x^n}{\equiv}$ is transitive and symmetric.

Now, the definition of the infinite product $\prod_{i\in I}(\mathbf{a}_i\mathbf{b}_i)$ (namely, Definition 3.11.5 **(b)**) yields that

$$[x^n]\left(\prod_{i\in I}(\mathbf{a}_i\mathbf{b}_i)\right) = [x^n]\left(\prod_{i\in M}(\mathbf{a}_i\mathbf{b}_i)\right) \qquad (346)$$

(since M is a finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i\mathbf{b}_i)_{i\in I}$). On the other hand, the set U is an x^n-approximator for $(\mathbf{a}_i)_{i\in I}$. Thus, Proposition 3.11.16 **(b)** (applied to U instead of M) yields

$$\prod_{i\in I}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in U}\mathbf{a}_i$$

(since the family $(\mathbf{a}_i)_{i\in I}$ is multipliable). Since the relation $\overset{x^n}{\equiv}$ is symmetric, we thus obtain

$$\prod_{i\in U}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in I}\mathbf{a}_i. \qquad (347)$$

Moreover, M is a finite subset of I satisfying $U \subseteq M$ (since $M \supseteq U$) and therefore $U \subseteq M \subseteq I$; hence, Proposition 3.11.16 **(a)** (applied to U and M instead of M and J) yields

$$\prod_{i\in M}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in U}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in I}\mathbf{a}_i \qquad (\text{by (347)}).$$

Hence,

$$\prod_{i\in M}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in I}\mathbf{a}_i \qquad (348)$$

(since the relation $\overset{x^n}{\equiv}$ is transitive). The same argument (applied to $(\mathbf{b}_i)_{i\in I}$ and V instead of $(\mathbf{a}_i)_{i\in I}$ and U) yields

$$\prod_{i\in M}\mathbf{b}_i \overset{x^n}{\equiv} \prod_{i\in I}\mathbf{b}_i. \qquad (349)$$

From (348) and (349), we obtain

$$\left(\prod_{i\in M}\mathbf{a}_i\right)\left(\prod_{i\in M}\mathbf{b}_i\right) \overset{x^n}{\equiv} \left(\prod_{i\in I}\mathbf{a}_i\right)\left(\prod_{i\in I}\mathbf{b}_i\right)$$

(by (99), applied to $a = \prod\limits_{i\in M} \mathbf{a}_i$ and $b = \prod\limits_{i\in I} \mathbf{a}_i$ and $c = \prod\limits_{i\in M} \mathbf{b}_i$ and $d = \prod\limits_{i\in I} \mathbf{b}_i$). In view of

$$\left(\prod_{i\in M} \mathbf{a}_i\right)\left(\prod_{i\in M} \mathbf{b}_i\right) = \prod_{i\in M} \left(\mathbf{a}_i \mathbf{b}_i\right) \qquad \left(\begin{array}{c}\text{by the properties of finite products,}\\ \text{since the set } M \text{ is finite}\end{array}\right),$$

this rewrites as

$$\prod_{i\in M} \left(\mathbf{a}_i \mathbf{b}_i\right) \overset{x^n}{\equiv} \left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right).$$

In other words,

$$\text{each } m \in \{0,1,\ldots,n\} \text{ satisfies } \left[x^m\right]\left(\prod_{i\in M} \left(\mathbf{a}_i \mathbf{b}_i\right)\right) = \left[x^m\right]\left(\left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right)\right)$$

(by Definition 3.10.1). Applying this to $m = n$, we obtain

$$\left[x^n\right]\left(\prod_{i\in M} \left(\mathbf{a}_i \mathbf{b}_i\right)\right) = \left[x^n\right]\left(\left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right)\right).$$

In view of (346), this rewrites as

$$\left[x^n\right]\left(\prod_{i\in I} \left(\mathbf{a}_i \mathbf{b}_i\right)\right) = \left[x^n\right]\left(\left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right)\right). \qquad (350)$$

Now, forget that we fixed n. We thus have proved that each $n \in \mathbb{N}$ satisfies (350). In other words, each coefficient of the FPS $\prod\limits_{i\in I} \left(\mathbf{a}_i \mathbf{b}_i\right)$ equals the corresponding coefficient of $\left(\prod\limits_{i\in I} \mathbf{a}_i\right)\left(\prod\limits_{i\in I} \mathbf{b}_i\right)$. Hence, we have

$$\prod_{i\in I} \left(\mathbf{a}_i \mathbf{b}_i\right) = \left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right).$$

This proves Proposition 3.11.18 **(b)**. □

In order to eventually prove Proposition 3.11.19, we shall first prove a slightly stronger auxiliary statement:

Lemma B.2.1. Let $\left(\mathbf{a}_i\right)_{i\in I} \in K\left[\left[x\right]\right]^I$ be a family of invertible FPSs. Let J be a subset of I. Let $n \in \mathbb{N}$. Let U be an x^n-approximator for $\left(\mathbf{a}_i\right)_{i\in I}$. Then, $U \cap J$ is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i\in J}$.

Proof of Lemma B.2.1. The set U is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i\in I}$. In other words, U is a finite subset of I that determines the first $n+1$ coefficients in the product of $\left(\mathbf{a}_i\right)_{i\in I}$ (by the definition of an x^n-approximator). Hence, in particular, U is finite. Moreover, $U \subseteq I$ (since U is a subset of I).

Let $M = U \cap J$. Thus, $M = U \cap J \subseteq U$, so that the set M is finite (since U is finite). Moreover, M is a subset of J (since $M = U \cap J \subseteq J$).

Now, let N be a finite subset of J satisfying $M \subseteq N \subseteq J$. We shall show that

$$\prod_{i \in N} \mathbf{a}_i \overset{x^n}{\equiv} \prod_{i \in M} \mathbf{a}_i.$$

Indeed, the set $N \cup U$ is finite (since N and U are finite) and is a subset of I (since $\underbrace{N}_{\subseteq J \subseteq I} \cup \underbrace{U}_{\subseteq I} \subseteq I \cup I = I$); it also satisfies $U \subseteq N \cup U \subseteq I$. Now, we recall that U is an x^n-approximator for $(\mathbf{a}_i)_{i \in I}$. Hence, Proposition 3.11.16 **(a)** (applied to U and $N \cup U$ instead of M and J) yields

$$\prod_{i \in N \cup U} \mathbf{a}_i \overset{x^n}{\equiv} \prod_{i \in U} \mathbf{a}_i \tag{351}$$

(since $N \cup U$ is a finite subset of I satisfying $U \subseteq N \cup U \subseteq I$).

On the other hand, we have assumed that $(\mathbf{a}_i)_{i \in I}$ is a family of invertible FPSs. Thus, for each $i \in I$, the FPS $\mathbf{a}_i$ is invertible, so that its inverse $\mathbf{a}_i^{-1}$ is well-defined. We obviously have

$$\prod_{i \in U \setminus J} \mathbf{a}_i^{-1} \overset{x^n}{\equiv} \prod_{i \in U \setminus J} \mathbf{a}_i^{-1} \tag{352}$$

(since Proposition 3.10.3 **(a)** yields that the relation $\overset{x^n}{\equiv}$ is reflexive).

We have now proved (351) and (352). Hence, (99) (applied to $a = \prod_{i \in N \cup U} \mathbf{a}_i$ and $b = \prod_{i \in U} \mathbf{a}_i$ and $c = \prod_{i \in U \setminus J} \mathbf{a}_i^{-1}$ and $d = \prod_{i \in U \setminus J} \mathbf{a}_i^{-1}$) yields

$$\left(\prod_{i \in N \cup U} \mathbf{a}_i \right) \left(\prod_{i \in U \setminus J} \mathbf{a}_i^{-1} \right) \overset{x^n}{\equiv} \left(\prod_{i \in U} \mathbf{a}_i \right) \left(\prod_{i \in U \setminus J} \mathbf{a}_i^{-1} \right). \tag{353}$$

On the other hand, the sets N and $U \setminus J$ are disjoint[153], and their union is $N \cup (U \setminus J) = N \cup U$ [154]. Hence, the set $N \cup U$ is the union of its two disjoint subsets N and $U \setminus J$. Thus, we can split the product $\prod_{i \in N \cup U} \mathbf{a}_i$ as follows:

$$\prod_{i \in N \cup U} \mathbf{a}_i = \left(\prod_{i \in N} \mathbf{a}_i \right) \left(\prod_{i \in U \setminus J} \mathbf{a}_i \right).$$

[153] since $\underbrace{N}_{\subseteq J} \cap (U \setminus J) \subseteq J \cap (U \setminus J) = \varnothing$ and thus $N \cap (U \setminus J) = \varnothing$

[154] This follows from

$$N \cup \underbrace{U}_{=(U \cap J) \cup (U \setminus J)} = N \cup \underbrace{(U \cap J)}_{=M} \cup (U \setminus J) \subseteq \underbrace{N \cup M}_{\substack{=N \\ (\text{since } M \subseteq N)}} \cup (U \setminus J) = N \cup (U \setminus J).$$

Multiplying both sides of this equality by $\prod\limits_{i\in U\setminus J}\mathbf{a}_i^{-1}$, we obtain

$$\begin{aligned}
\left(\prod_{i\in N\cup U}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\mathbf{a}_i^{-1}\right) &= \left(\prod_{i\in N}\mathbf{a}_i\right)\underbrace{\left(\prod_{i\in U\setminus J}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\mathbf{a}_i^{-1}\right)}_{=\prod\limits_{i\in U\setminus J}\left(\mathbf{a}_i\mathbf{a}_i^{-1}\right)} \\
&= \left(\prod_{i\in N}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\underbrace{\left(\mathbf{a}_i\mathbf{a}_i^{-1}\right)}_{=1}\right) = \left(\prod_{i\in N}\mathbf{a}_i\right)\underbrace{\left(\prod_{i\in U\setminus J}1\right)}_{=1} \\
&= \prod_{i\in N}\mathbf{a}_i. \qquad (354)
\end{aligned}$$

However, the set U is the union of its two disjoint subsets $U\cap J$ and $U\setminus J$. Thus, we can split the product $\prod\limits_{i\in U}\mathbf{a}_i$ as follows:

$$\prod_{i\in U}\mathbf{a}_i = \left(\prod_{i\in U\cap J}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\mathbf{a}_i\right).$$

Multiplying both sides of this equality by $\prod\limits_{i\in U\setminus J}\mathbf{a}_i^{-1}$, we obtain

$$\begin{aligned}
\left(\prod_{i\in U}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\mathbf{a}_i^{-1}\right) &= \underbrace{\left(\prod_{i\in U\cap J}\mathbf{a}_i\right)}_{\substack{=\prod\limits_{i\in M}\mathbf{a}_i \\ (\text{since } U\cap J=M)}}\underbrace{\left(\prod_{i\in U\setminus J}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\mathbf{a}_i^{-1}\right)}_{=\prod\limits_{i\in U\setminus J}\left(\mathbf{a}_i\mathbf{a}_i^{-1}\right)} \\
&= \left(\prod_{i\in M}\mathbf{a}_i\right)\left(\prod_{i\in U\setminus J}\underbrace{\left(\mathbf{a}_i\mathbf{a}_i^{-1}\right)}_{=1}\right) = \left(\prod_{i\in M}\mathbf{a}_i\right)\underbrace{\left(\prod_{i\in U\setminus J}1\right)}_{=1} \\
&= \prod_{i\in M}\mathbf{a}_i. \qquad (355)
\end{aligned}$$

In view of (354) and (355), we can rewrite the relation (353) as follows:

$$\prod_{i\in N}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in M}\mathbf{a}_i.$$

In other words, each $m\in\{0,1,\ldots,n\}$ satisfies

$$\left[x^m\right]\left(\prod_{i\in N}\mathbf{a}_i\right) = \left[x^m\right]\left(\prod_{i\in M}\mathbf{a}_i\right) \qquad (356)$$

(by Definition 3.10.1).

Forget that we fixed N. We have thus shown that every finite subset N of J satisfying $M \subseteq N \subseteq J$ satisfies (356) for each $m \in \{0, 1, \ldots, n\}$.

Now, let $m \in \{0, 1, \ldots, n\}$. Then, every finite subset N of J satisfying $M \subseteq N \subseteq J$ satisfies

$$\left[x^m\right]\left(\prod_{i \in N} \mathbf{a}_i\right) = \left[x^m\right]\left(\prod_{i \in M} \mathbf{a}_i\right)$$

(by (356)). In other words, the set M determines the x^m-coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ (by the definition of "determining the x^m-coefficient in a product").

Forget that we fixed m. We thus have shown that M determines the x^m-coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ for each $m \in \{0, 1, \ldots, n\}$. In other words, M determines the first $n+1$ coefficients in the product of $\left(\mathbf{a}_i\right)_{i \in J}$. In other words, M is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i \in J}$ (by the definition of an "x^n-approximator", since M is a finite subset of J). In other words, $U \cap J$ is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i \in J}$ (since $M = U \cap J$). This proves Lemma B.2.1. □

Detailed proof of Proposition 3.11.19. Let J be a subset of I. We shall show that the family $\left(\mathbf{a}_i\right)_{i \in J}$ is multipliable.

Fix $n \in \mathbb{N}$. We know that the family $\left(\mathbf{a}_i\right)_{i \in I}$ is multipliable. Hence, there exists an x^n-approximator U for $\left(\mathbf{a}_i\right)_{i \in I}$ (by Lemma 3.11.15). Consider this U.

Set $M = U \cap J$. Lemma B.2.1 yields that $U \cap J$ is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i \in J}$. In other words, M is an x^n-approximator for $\left(\mathbf{a}_i\right)_{i \in J}$ (since $M = U \cap J$). In other words, M is a finite subset of J that determines the first $n+1$ coefficients in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ (by the definition of an x^n-approximator). Thus, the set M determines the first $n+1$ coefficients in the product of $\left(\mathbf{a}_i\right)_{i \in J}$. Hence, in particular, this set M determines the x^n-coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$. Therefore, the x^n-coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ is finitely determined (by the definition of "finitely determined", since M is a finite subset of J).

Forget that we fixed n. We thus have proved that for each $n \in \mathbb{N}$, the x^n-coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ is finitely determined. In other words, each coefficient in the product of $\left(\mathbf{a}_i\right)_{i \in J}$ is finitely determined. In other words, the family $\left(\mathbf{a}_i\right)_{i \in J}$ is multipliable (by the definition of "multipliable").

Forget that we fixed J. We thus have shown that the family $\left(\mathbf{a}_i\right)_{i \in J}$ is multipliable whenever J is a subset of I. In other words, any subfamily of $\left(\mathbf{a}_i\right)_{i \in I}$ is multipliable. This proves Proposition 3.11.19. □

Detailed proof of Proposition 3.11.21. We shall prove the four facts stated explicitly in Proposition 3.11.21. Other properties of infinite products can be shown similarly (mainly by reducing to the finite case).

We begin with the first of the four facts:

> **Proposition B.2.2.** Let $\left(\mathbf{a}_s\right)_{s \in S} \in K[[x]]^S$ and $\left(\mathbf{b}_s\right)_{s \in S} \in K[[x]]^S$ be two multipliable families of invertible FPSs. Then, the family $\left(\mathbf{a}_s \mathbf{b}_s\right)_{s \in S}$ is multipliable as well, and satisfies
>
> $$\prod_{s \in S} \left(\mathbf{a}_s \mathbf{b}_s\right) = \left(\prod_{s \in S} \mathbf{a}_s\right) \cdot \left(\prod_{s \in S} \mathbf{b}_s\right).$$

Proof of Proposition B.2.2. This follows immediately from Proposition 3.11.17 (with the letters i and I replaced by s and S). □

Next, we shall show the second fact:

> **Proposition B.2.3.** Let $(\mathbf{a}_s)_{s\in S} \in K[[x]]^S$ be a multipliable family of invertible FPSs. Let X and Y be two subsets of S such that $X \cap Y = \varnothing$ and $X \cup Y = S$. Then,
>
> $$\prod_{s\in S} \mathbf{a}_s = \left(\prod_{s\in X} \mathbf{a}_s\right) \cdot \left(\prod_{s\in Y} \mathbf{a}_s\right).$$

Proof of Proposition B.2.3. Proposition 3.11.19 (applied to S and $(\mathbf{a}_s)_{s\in S}$ instead of I and $(\mathbf{a}_i)_{i\in I}$) shows that any subfamily of $(\mathbf{a}_s)_{s\in S}$ is multipliable. Thus, the families $(\mathbf{a}_s)_{s\in X}$ and $(\mathbf{a}_s)_{s\in Y}$ are multipliable (since they are subfamilies of $(\mathbf{a}_s)_{s\in S}$). This shows that the products $\prod\limits_{s\in X} \mathbf{a}_s$ and $\prod\limits_{s\in Y} \mathbf{a}_s$ are well-defined.

From $X \cap Y = \varnothing$ and $X \cup Y = S$, we see that each element of S belongs to exactly one of the two sets X and Y. Thus, the two sets X and Y are each other's complements in S. In particular, $Y = S \setminus X$. Hence, $(\mathbf{a}_s)_{s\in Y} = (\mathbf{a}_s)_{s\in S\setminus X}$. Thus, the family $(\mathbf{a}_s)_{s\in S\setminus X}$ is multipliable (since the family $(\mathbf{a}_s)_{s\in Y}$ is multipliable). Hence, Proposition 3.11.17 **(b)** (applied to $I = S$ and $J = X$) yields

$$\prod_{i\in S} \mathbf{a}_i = \left(\prod_{i\in X} \mathbf{a}_i\right) \cdot \left(\prod_{i\in S\setminus X} \mathbf{a}_i\right) = \left(\prod_{i\in X} \mathbf{a}_i\right) \cdot \left(\prod_{i\in Y} \mathbf{a}_i\right)$$

(since $S \setminus X = Y$). Renaming the indices i as s on both sides of this equality, we obtain

$$\prod_{s\in S} \mathbf{a}_s = \left(\prod_{s\in X} \mathbf{a}_s\right) \cdot \left(\prod_{s\in Y} \mathbf{a}_s\right).$$

This proves Proposition B.2.3. □

Next, let us prove the third fact:

> **Proposition B.2.4.** Let $(\mathbf{a}_s)_{s\in S} \in K[[x]]^S$ be a multipliable family of invertible FPSs. Let W be a set. Let $f : S \to W$ be a map. Then,
>
> $$\prod_{s\in S} \mathbf{a}_s = \prod_{w\in W} \prod_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s. \qquad (357)$$
>
> (In particular, the right hand side is well-defined – i.e., the family $(\mathbf{a}_s)_{s\in S;\ f(s)=w}$ is multipliable for each $w \in W$, and the family $\left(\prod\limits_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s\right)_{w\in W}$ is also multipliable.)

Before we prove this, let us restate a piece of Theorem 3.10.3 **(e)** in more convenient language:

Lemma B.2.5. Let $n \in \mathbb{N}$. Let V be a finite set. Let $(c_w)_{w \in V} \in K[[x]]^V$ and $(d_w)_{w \in V} \in K[[x]]^V$ be two families of FPSs such that

$$\text{each } w \in V \text{ satisfies } c_w \overset{x^n}{\equiv} d_w.$$

Then, we have

$$\prod_{w \in V} c_w \overset{x^n}{\equiv} \prod_{w \in V} d_w.$$

Proof of Lemma B.2.5. This is just (102), with the letters S, s, a_s and b_s renamed as V, w, c_w and d_w. □

Proof of Proposition B.2.4. We shall subdivide our proof into several claims:

Claim 1: Let $w \in W$. Then, the family $(\mathbf{a}_s)_{s \in S;\ f(s)=w}$ is multipliable.

[*Proof of Claim 1:* Proposition 3.11.19 (applied to S and $(\mathbf{a}_s)_{s \in S}$ instead of I and $(\mathbf{a}_i)_{i \in I}$) shows that any subfamily of $(\mathbf{a}_s)_{s \in S}$ is multipliable. Hence, the family $(\mathbf{a}_s)_{s \in S;\ f(s)=w}$ is multipliable (since this family is a subfamily of $(\mathbf{a}_s)_{s \in S}$). This proves Claim 1.]

Let us set

$$\mathbf{b}_w := \prod_{\substack{s \in S; \\ f(s)=w}} \mathbf{a}_s \qquad \text{for each } w \in W. \tag{358}$$

This is well-defined, because for each $w \in W$, the product $\prod_{\substack{s \in S; \\ f(s)=w}} \mathbf{a}_s$ is well-defined (since Claim 1 shows that the family $(\mathbf{a}_s)_{s \in S;\ f(s)=w}$ is multipliable).

Now, let $n \in \mathbb{N}$. Lemma 3.11.15 (applied to S and $(\mathbf{a}_s)_{s \in S}$ instead of I and $(\mathbf{a}_i)_{i \in I}$) shows that there exists an x^n-approximator for $(\mathbf{a}_s)_{s \in S}$. Pick such an x^n-approximator, and call it U. Then, U is an x^n-approximator for $(\mathbf{a}_s)_{s \in S}$; in other words, U is a finite subset of S that determines the first $n+1$ coefficients in the product of $(\mathbf{a}_s)_{s \in S}$ (by the definition of an x^n-approximator).

The set U is finite. Thus, its image $f(U) = \{f(u) \mid u \in U\}$ is finite as well. Now, we claim the following:

Claim 2: For each $w \in W$, we have

$$\mathbf{b}_w \overset{x^n}{\equiv} \prod_{\substack{s \in U; \\ f(s)=w}} \mathbf{a}_s.$$

[*Proof of Claim 2:* Let $w \in W$. Let J be the subset $\{s \in S \mid f(s) = w\}$ of S. Then, $(\mathbf{a}_s)_{s \in J}$ is a subfamily of $(\mathbf{a}_s)_{s \in S}$. However, Proposition 3.11.19 (applied to S and $(\mathbf{a}_s)_{s \in S}$ instead of I and $(\mathbf{a}_i)_{i \in I}$) shows that any subfamily of $(\mathbf{a}_s)_{s \in S}$ is multipliable. Hence, the family $(\mathbf{a}_s)_{s \in J}$ is multipliable (since this family is a subfamily of $(\mathbf{a}_s)_{s \in S}$). Furthermore, Lemma B.2.1 (applied to S and $(\mathbf{a}_s)_{s \in S}$ instead of I and $(\mathbf{a}_i)_{i \in I}$) yields that $U \cap J$ is an x^n-approximator for $(\mathbf{a}_s)_{s \in J}$ (since U is an x^n-approximator for $(\mathbf{a}_s)_{s \in S}$). Hence, Proposition 3.11.16 **(b)** (applied to J, $(\mathbf{a}_s)_{s\in J}$ and $U\cap J$ instead of I, $(\mathbf{a}_i)_{i\in I}$ and M) yields

$$\prod_{i\in J}\mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in U\cap J}\mathbf{a}_i.$$

Renaming the indices i as s on both sides of this relation, we obtain

$$\prod_{s\in J}\mathbf{a}_s \overset{x^n}{\equiv} \prod_{s\in U\cap J}\mathbf{a}_s. \tag{359}$$

However, we have $J=\{s\in S \mid f(s)=w\}$. Thus, the product sign "$\prod\limits_{s\in J}$" is equivalent to "$\prod\limits_{\substack{s\in S;\\ f(s)=w}}$". Thus, we obtain

$$\prod_{s\in J}\mathbf{a}_s = \prod_{\substack{s\in S;\\ f(s)=w}}\mathbf{a}_s = \mathbf{b}_w \tag{360}$$

(by (358)).

On the other hand, from $J=\{s\in S \mid f(s)=w\}$, we obtain

$$\begin{aligned} U\cap J &= U\cap\{s\in S \mid f(s)=w\} \\ &= \{s\in U \mid f(s)=w\} \qquad (\text{since } U\subseteq S). \end{aligned}$$

Hence, the product sign "$\prod\limits_{s\in U\cap J}$" is equivalent to "$\prod\limits_{\substack{s\in U;\\ f(s)=w}}$". Thus, we obtain

$$\prod_{s\in U\cap J}\mathbf{a}_s = \prod_{\substack{s\in U;\\ f(s)=w}}\mathbf{a}_s. \tag{361}$$

In view of (360) and (361), we can rewrite the relation (359) as

$$\mathbf{b}_w \overset{x^n}{\equiv} \prod_{\substack{s\in U;\\ f(s)=w}}\mathbf{a}_s.$$

This proves Claim 2.]

Claim 3: The set $f(U)$ is an x^n-approximator for the family $(\mathbf{b}_w)_{w\in W}$.

[*Proof of Claim 3:* Let V be a finite subset of W satisfying $f(U)\subseteq V\subseteq W$. We shall show that

$$\prod_{w\in f(U)}\mathbf{b}_w \overset{x^n}{\equiv} \prod_{w\in V}\mathbf{b}_w.$$

Indeed, each $w\in V$ satisfies $w\in V\subseteq W$ and therefore $\mathbf{b}_w \overset{x^n}{\equiv} \prod\limits_{\substack{s\in U;\\ f(s)=w}}\mathbf{a}_s$ (by Claim 2). Hence, Lemma B.2.5 (applied to $c_w=\mathbf{b}_w$ and $d_w=\prod\limits_{\substack{s\in U;\\ f(s)=w}}\mathbf{a}_s$) yields

$$\prod_{w\in V}\mathbf{b}_w \overset{x^n}{\equiv} \prod_{w\in V}\prod_{\substack{s\in U;\\ f(s)=w}}\mathbf{a}_s. \tag{362}$$

However, each $s \in U$ satisfies $f(s) \in V$ (because $f\left(\underbrace{s}_{\in U}\right) \in f(U) \subseteq V$). Hence, we can split the product $\prod\limits_{s\in U} \mathbf{a}_s$ according to the value of $f(s)$ (since both sets U and V are finite); we thus obtain

$$\prod_{s\in U} \mathbf{a}_s = \prod_{w\in V} \prod_{\substack{s\in U;\\ f(s)=w}} \mathbf{a}_s.$$

Therefore, (362) rewrites as

$$\prod_{w\in V} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s. \tag{363}$$

The same argument (applied to $f(U)$ instead of V) shows that

$$\prod_{w\in f(U)} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s \tag{364}$$

(since $f(U)$ is a finite subset of W satisfying $f(U) \subseteq f(U) \subseteq W$).

However, the relation $\overset{x^n}{\equiv}$ on $K[[x]]$ is symmetric (by Theorem 3.10.3 **(a)**); thus, (363) entails

$$\prod_{s\in U} \mathbf{a}_s \overset{x^n}{\equiv} \prod_{w\in V} \mathbf{b}_w.$$

Therefore, (364) becomes

$$\prod_{w\in f(U)} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s \overset{x^n}{\equiv} \prod_{w\in V} \mathbf{b}_w.$$

Since the relation $\overset{x^n}{\equiv}$ on $K[[x]]$ is transitive (by Theorem 3.10.3 **(a)**), we thus obtain

$$\prod_{w\in f(U)} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{w\in V} \mathbf{b}_w.$$

In other words, each $m \in \{0, 1, \ldots, n\}$ satisfies

$$\left[x^m\right]\left(\prod_{w\in f(U)} \mathbf{b}_w\right) = \left[x^m\right]\left(\prod_{w\in V} \mathbf{b}_w\right) \tag{365}$$

(by Definition 3.10.1).

Forget that we fixed V. We thus have shown that if V is a finite subset of W satisfying $f(U) \subseteq V \subseteq W$, then each $m \in \{0, 1, \ldots, n\}$ satisfies (365).

Now, let $m \in \{0, 1, \ldots, n\}$ be arbitrary. Then, every finite subset V of W satisfying $f(U) \subseteq V \subseteq W$ satisfies

$$\left[x^m\right]\left(\prod_{w\in f(U)} \mathbf{b}_w\right) = \left[x^m\right]\left(\prod_{w\in V} \mathbf{b}_w\right) \qquad \text{(by (365))}.$$

In other words, the set $f(U)$ determines the x^m-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ (by the definition of "determining the x^m-coefficient in a product", since $f(U)$ is a finite subset of W).

Forget that we fixed m. We thus have shown that the set $f(U)$ determines the x^m-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ for each $m \in \{0,1,\ldots,n\}$. In other words, the set $f(U)$ determines the first $n+1$ coefficients in the product of $(\mathbf{b}_w)_{w\in W}$. In other words, $f(U)$ is an x^n-approximator for $(\mathbf{b}_w)_{w\in W}$ (by the definition of an "x^n-approximator", since $f(U)$ is a finite subset of W). This proves Claim 3.]

> *Claim 4:* The x^n-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ is finitely determined.

[*Proof of Claim 4:* Claim 3 shows that $f(U)$ is an x^n-approximator for $(\mathbf{b}_w)_{w\in W}$. Thus, the set $f(U)$ determines the first $n+1$ coefficients in the product of $(\mathbf{b}_w)_{w\in W}$ (by the definition of an "x^n-approximator"). Hence, in particular, this set $f(U)$ determines the x^n-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$. Thus, the x^n-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ is finitely determined (by the definition of "finitely determined", since $f(U)$ is a finite subset of W). This proves Claim 4.]

Now, forget that we fixed n. We thus have shown that the x^n-coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ is finitely determined for each $n \in \mathbb{N}$. In other words, each coefficient in the product of $(\mathbf{b}_w)_{w\in W}$ is finitely determined. In other words, the family $(\mathbf{b}_w)_{w\in W}$ is multipliable (by the definition of "multipliable"). In view of (358), we can restate this as follows: The family $\left(\prod\limits_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s\right)_{w\in W}$ is multipliable.

It remains to prove the equality (357).

Let $n \in \mathbb{N}$. Lemma 3.11.15 (applied to S and $(\mathbf{a}_s)_{s\in S}$ instead of I and $(\mathbf{a}_i)_{i\in I}$) shows that there exists an x^n-approximator for $(\mathbf{a}_s)_{s\in S}$. Pick such an x^n-approximator, and call it U. Then, U is a finite subset of S (by the definition of an x^n-approximator). Furthermore, Proposition 3.11.16 **(b)** (applied to S, $(\mathbf{a}_s)_{s\in S}$ and U instead of I, $(\mathbf{a}_i)_{i\in I}$ and M) yields

$$\prod_{i\in S} \mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in U} \mathbf{a}_i.$$

Renaming the index i as s on both sides of this relation, we obtain

$$\prod_{s\in S} \mathbf{a}_s \overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s. \tag{366}$$

However, the relation $\overset{x^n}{\equiv}$ on $K[[x]]$ is symmetric (by Theorem 3.10.3 **(a)**); thus, (366) entails

$$\prod_{s\in U} \mathbf{a}_s \overset{x^n}{\equiv} \prod_{s\in S} \mathbf{a}_s. \tag{367}$$

Let V be the set $f(U) = \{f(u) \mid u \in U\}$. Thus, $V = f(U) \subseteq W$ and $f(U) = V \subseteq V$, so that $f(U) \subseteq V \subseteq W$. Moreover, the set $f(U)$ is finite (since U is finite); in other words, the set V is finite (since $V = f(U)$).

We have already proved (in Claim 3) that the set $f(U)$ is an x^n-approximator for the family $(\mathbf{b}_w)_{w\in W}$. In other words, the set V is an x^n-approximator for the family

$(\mathbf{b}_w)_{w\in W}$ (since $V = f(U)$). Hence, Proposition 3.11.16 **(b)** (applied to W, $(\mathbf{b}_w)_{w\in W}$ and V instead of I, $(\mathbf{a}_i)_{i\in I}$ and M) yields

$$\prod_{i\in W} \mathbf{b}_i \overset{x^n}{\equiv} \prod_{i\in V} \mathbf{b}_i$$

(since the family $(\mathbf{b}_w)_{w\in W}$ is multipliable). Renaming the index i as w on both sides of this relation, we obtain

$$\prod_{w\in W} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{w\in V} \mathbf{b}_w. \qquad (368)$$

On the other hand,

$$\prod_{w\in V} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s. \qquad (369)$$

(Indeed, this is precisely the equality (363) that was shown during the proof of Claim 3, and its proof applies here just as well.)

Now, (368) becomes

$$\begin{aligned}\prod_{w\in W} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{w\in V} \mathbf{b}_w &\overset{x^n}{\equiv} \prod_{s\in U} \mathbf{a}_s \qquad \text{(by (369))} \\ &\overset{x^n}{\equiv} \prod_{s\in S} \mathbf{a}_s \qquad \text{(by (367))}.\end{aligned}$$

Since the relation $\overset{x^n}{\equiv}$ on $K[[x]]$ is transitive (by Theorem 3.10.3 **(a)**), we thus obtain

$$\prod_{w\in W} \mathbf{b}_w \overset{x^n}{\equiv} \prod_{s\in S} \mathbf{a}_s.$$

In other words,

$$\text{each } m \in \{0,1,\ldots,n\} \text{ satisfies } [x^m]\left(\prod_{w\in W} \mathbf{b}_w\right) = [x^m]\left(\prod_{s\in S} \mathbf{a}_s\right)$$

(by Definition 3.10.1). Applying this to $m = n$, we obtain

$$[x^n]\left(\prod_{w\in W} \mathbf{b}_w\right) = [x^n]\left(\prod_{s\in S} \mathbf{a}_s\right).$$

Forget that we fixed n. We thus have shown that

$$[x^n]\left(\prod_{w\in W} \mathbf{b}_w\right) = [x^n]\left(\prod_{s\in S} \mathbf{a}_s\right) \qquad \text{for each } n \in \mathbb{N}.$$

In other words, each coefficient of the FPS $\prod\limits_{w\in W} \mathbf{b}_w$ equals the corresponding coefficient of $\prod\limits_{s\in S} \mathbf{a}_s$. Therefore,

$$\prod_{w\in W} \mathbf{b}_w = \prod_{s\in S} \mathbf{a}_s.$$

In view of (358), we can rewrite this as

$$\prod_{w\in W}\ \prod_{\substack{s\in S;\\ f(s)=w}} \mathbf{a}_s = \prod_{s\in S} \mathbf{a}_s.$$

Thus, (357) is proven, and the proof of Proposition B.2.4 is complete. □

Finally, here is the fourth and last fact we need to prove:

> **Proposition B.2.6** (Fubini rule for infinite products of FPSs)**.** Let I and J be two sets. Let $\left(\mathbf{a}_{(i,j)}\right)_{(i,j)\in I\times J} \in K[[x]]^{I\times J}$ be a multipliable family of invertible FPSs. Then,
>
> $$\prod_{i\in I}\ \prod_{j\in J} \mathbf{a}_{(i,j)} = \prod_{(i,j)\in I\times J} \mathbf{a}_{(i,j)} = \prod_{j\in J}\ \prod_{i\in I} \mathbf{a}_{(i,j)}.$$
>
> (In particular, all the products appearing in this equality are well-defined.)

Proof of Proposition B.2.6. Let $f : I\times J \to I$ be the map that sends each pair (i,j) to i.

We have assumed that $\left(\mathbf{a}_{(i,j)}\right)_{(i,j)\in I\times J} \in K[[x]]^{I\times J}$ is a multipliable family of invertible FPSs. In other words, $(\mathbf{a}_s)_{s\in I\times J} \in K[[x]]^{I\times J}$ is a multipliable family of invertible FPSs (here, we have renamed the index (i,j) as s). Hence, any subfamily of $(\mathbf{a}_s)_{s\in I\times J}$ is multipliable (by Proposition 3.11.19, applied to $I\times J$ and $(\mathbf{a}_s)_{s\in I\times J}$ instead of I and $(\mathbf{a}_i)_{i\in I}$).

Furthermore, Proposition B.2.4 (applied to $S = I\times J$ and $W = I$) yields that

$$\prod_{s\in I\times J} \mathbf{a}_s = \prod_{w\in I}\ \prod_{\substack{s\in I\times J;\\ f(s)=w}} \mathbf{a}_s; \tag{370}$$

in particular, it yields that the right hand side of (370) is well-defined – i.e., the family $(\mathbf{a}_s)_{s\in I\times J;\ f(s)=w}$ is multipliable for each $w\in W$, and the family $\left(\prod_{\substack{s\in I\times J;\\ f(s)=w}} \mathbf{a}_s\right)_{w\in I}$ is also multipliable.

Now, fix $w\in I$. Let J' be the set $\{s\in I\times J \mid f(s)=w\}$. Thus, J' is a subset of $I\times J$. Hence, the family $(\mathbf{a}_s)_{s\in J'}$ is a subfamily of $(\mathbf{a}_s)_{s\in I\times J}$, and therefore is multipliable (since any subfamily of $(\mathbf{a}_s)_{s\in I\times J}$ is multipliable). Thus, the product $\prod_{s\in J'} \mathbf{a}_s$ is well-defined. Furthermore, the definition of J' yields

$$\begin{aligned} J' &= \{s\in I\times J \mid f(s)=w\} \\ &= \left\{(i,j)\in I\times J \mid \underbrace{f(i,j)}_{\substack{=i\\ \text{(by the definition of } f)}} = w\right\} \\ &\qquad \text{(here, we have renamed the index } s \text{ as } (i,j)) \\ &= \{(i,j)\in I\times J \mid i=w\} \\ &= \{(w,j) \mid j\in J\} \qquad (\text{since } i\in I). \end{aligned}$$

In other words, the set J' consists of all pairs (w,j) with $j \in J$. Hence, there is a bijection

$$\begin{aligned} J &\to J', \\ j &\mapsto (w,j) . \end{aligned}$$

Thus, we can substitute (w,j) for s in the product $\prod\limits_{s \in J'} \mathbf{a}_s$ (because any bijection allows us to substitute the index in a product[155]). We thus obtain

$$\prod_{s \in J'} \mathbf{a}_s = \prod_{j \in J} \mathbf{a}_{(w,j)} \tag{371}$$

(and, in particular, the product on the right hand side of this equality is well-defined, i.e., the family $\left(\mathbf{a}_{(w,j)}\right)_{j \in J}$ is multipliable). However, we can replace the product sign "$\prod\limits_{s \in J'}$" by "$\prod\limits_{\substack{s \in I \times J; \\ f(s) = w}}$" (since $J' = \{s \in I \times J \mid f(s) = w\}$). Hence, we can rewrite (371) as

$$\prod_{\substack{s \in I \times J; \\ f(s) = w}} \mathbf{a}_s = \prod_{j \in J} \mathbf{a}_{(w,j)}. \tag{372}$$

Forget that we fixed w. We thus have proved (372) for each $w \in I$.

Now, (370) becomes

$$\prod_{s \in I \times J} \mathbf{a}_s = \prod_{w \in I} \underbrace{\prod_{\substack{s \in I \times J; \\ f(s) = w}} \mathbf{a}_s}_{\substack{= \prod\limits_{j \in J} \mathbf{a}_{(w,j)} \\ \text{(by (372))}}} = \prod_{w \in I} \prod_{j \in J} \mathbf{a}_{(w,j)} = \prod_{i \in I} \prod_{j \in J} \mathbf{a}_{(i,j)}$$

(here, we have renamed the index w as i in the outer product). Renaming the index s as (i,j) on the left hand side of this equality, we can rewrite it as

$$\prod_{(i,j) \in I \times J} \mathbf{a}_{(i,j)} = \prod_{i \in I} \prod_{j \in J} \mathbf{a}_{(i,j)}.$$

A similar argument (but using the map $I \times J \to J,\ (i,j) \mapsto j$ instead of our map $f : I \times J \to I,\ (i,j) \mapsto i$) shows that

$$\prod_{(i,j) \in I \times J} \mathbf{a}_{(i,j)} = \prod_{j \in J} \prod_{i \in I} \mathbf{a}_{(i,j)}.$$

[155] Here we are using the following fact:

> Let S and T be two sets. Let $f : S \to T$ be a bijection. Let $(\mathbf{a}_t)_{t \in T} \in K[[x]]^T$ be a multipliable family of FPSs. Then,
>
> $$\prod_{t \in T} \mathbf{a}_t = \prod_{s \in S} \mathbf{a}_{f(s)}$$
>
> (and, in particular, the product on the right hand side is well-defined, i.e., the family $\left(\mathbf{a}_{f(s)}\right)_{s \in S}$ is multipliable).

This is another property of infinite products that needs to be proved. Its proof, however, it near-trivial and therefore omitted.

Combining these two equalities, we obtain

$$\prod_{i\in I}\ \prod_{j\in J}\mathbf{a}_{(i,j)}=\prod_{(i,j)\in I\times J}\mathbf{a}_{(i,j)}=\prod_{j\in J}\ \prod_{i\in I}\mathbf{a}_{(i,j)}.$$

(Tracing back our above argument, we see that all products appearing in this equality are well-defined; indeed, their well-definedness has been shown the moment they first appeared in our proof.) Proposition B.2.6 is thus proved. □

The proof of Proposition 3.11.21 is now complete. □

Proof of Lemma 3.11.28. Theorem 3.11.10 (applied to $I=J$) shows that the family $(1+f_i)_{i\in J}$ is multipliable. In other words, each coefficient in the product of this family $(1+f_i)_{i\in J}$ is finitely determined. In other words, for each $m\in\mathbb{N}$, the x^m-coefficient in the product of $(1+f_i)_{i\in J}$ is finitely determined. In other words, for each $m\in\mathbb{N}$, there is a finite subset M_m of J that determines the x^m-coefficient in the product of $(1+f_i)_{i\in J}$. Consider this M_m.

Let $M=M_0\cup M_1\cup\cdots\cup M_n$. Then, M is a finite subset of J (since $M_0,M_1,\ldots,M_n$ are finite subsets of J). Moreover, we claim that

$$[x^m]\left(\prod_{i\in J}(1+f_i)\right)=[x^m]\left(\prod_{i\in M}(1+f_i)\right) \tag{373}$$

for each $m\in\{0,1,\ldots,n\}$.

[*Proof of (373):* Let $m\in\{0,1,\ldots,n\}$. Then, M_m is one of the $n+1$ sets in the union $M_0\cup M_1\cup\cdots\cup M_n$. Hence, $M_m\subseteq M_0\cup M_1\cup\cdots\cup M_n=M$.

However, the subset M_m of J determines the x^m-coefficient in the product of $(1+f_i)_{i\in J}$ (by the definition of M_m). In other words, every finite subset J' of J satisfying $M_m\subseteq J'\subseteq J$ satisfies

$$[x^m]\left(\prod_{i\in J'}(1+f_i)\right)=[x^m]\left(\prod_{i\in M_m}(1+f_i)\right)$$

(by the definition of "determining the x^m-coefficient in a product"). Applying this to $J'=M$, we obtain

$$[x^m]\left(\prod_{i\in M}(1+f_i)\right)=[x^m]\left(\prod_{i\in M_m}(1+f_i)\right)$$

(since M is a finite subset of J satisfying $M_m\subseteq M\subseteq J$). On the other hand, the definition of the product $\prod\limits_{i\in J}(1+f_i)$ yields that

$$[x^m]\left(\prod_{i\in J}(1+f_i)\right)=[x^m]\left(\prod_{i\in M_m}(1+f_i)\right)$$

(since M_m is a finite subset of J that determines the x^m-coefficient in the product of $(1+f_i)_{i\in J}$). Comparing these two equalities, we obtain

$$[x^m]\left(\prod_{i\in J}(1+f_i)\right)=[x^m]\left(\prod_{i\in M}(1+f_i)\right).$$

This proves (373).]

Now, we know that (373) holds for each $m \in \{0, 1, \ldots, n\}$. Thus, we can apply Lemma 3.3.20 to $f = \prod\limits_{i \in J} (1 + f_i)$ and $g = \prod\limits_{i \in M} (1 + f_i)$. We thus obtain that

$$[x^m] \left(a \prod_{i \in J} (1 + f_i) \right) = [x^m] \left(a \prod_{i \in M} (1 + f_i) \right) \tag{374}$$

for each $m \in \{0, 1, \ldots, n\}$.

On the other hand, M is a finite set, so that $(f_i)_{i \in M}$ is a finite family. Furthermore, each $i \in M$ satisfies $[x^m](f_i) = 0$ for each $m \in \{0, 1, \ldots, n\}$ (by (125), since $i \in M \subseteq J$). Thus, we can apply Lemma 3.11.9 to M instead of J. We therefore obtain that

$$[x^m] \left(a \prod_{i \in M} (1 + f_i) \right) = [x^m] \, a \tag{375}$$

for each $m \in \{0, 1, \ldots, n\}$.

Hence, for each $m \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} [x^m] \left(a \prod_{i \in J} (1 + f_i) \right) &= [x^m] \left(a \prod_{i \in M} (1 + f_i) \right) \qquad \text{(by (374))} \\ &= [x^m] \, a \qquad \text{(by (375))}. \end{aligned}$$

This proves Lemma 3.11.28. □

Proof of Proposition 3.11.26. The following proof is an expanded version of the argument given by Mindlack at `https://math.stackexchange.com/a/4123658/` .

This will be a long grind; we thus break it up into several claims. First, however, let us introduce a few notations:

- If J is a subset of I, then S^J shall denote the Cartesian product $\prod\limits_{i \in J} S_i$. This Cartesian product $\prod\limits_{i \in J} S_i$ consists of families $(s_i)_{i \in J}$, where each s_i belongs to the respective set S_i.

  The notation S^J should not be misconstrued as being an actual power. (However, in the particular case when all S_i equal one and the same set S, the Cartesian product S^J we just defined is indeed the Cartesian power commonly known as S^J.)

- If J is a subset of I, then S^I_J shall denote the set of all families $(s_i)_{i \in I} \in S^I$ that satisfy
  $$(s_i = 0 \text{ for all } i \in I \setminus J).$$
  This set S^I_J is in a canonical bijection with S^J, as elements of both sets consist of "essentially the same data". To wit, an element of S^J is a family that only has i-th entries for $i \in J$, whereas an element of S^I_J is a family that has i-th entries for all $i \in I$, but subject to the requirement that the i-th entries for all $i \in I \setminus J$ are 0 (so

that only the i-th entries for $i \in J$ carry any information). More rigorously: The map

$$S_J^I \to S^J, \\ (s_i)_{i\in I} \mapsto (s_i)_{i\in J}$$

is a bijection (since it merely shrinks the family by removing entries that are required to be 0 anyway). We denote this bijection by reduce_J.

- We define S_{fin}^I to be the set of all essentially finite families $(s_i)_{i\in I} \in S^I$. It is easy to see that S_{fin}^I is the union of the sets S_J^I over all finite subsets J of I.

Now, we can begin with our claims:

Claim 1: The family $(p_{i,k})_{k\in S_i}$ is summable for each $i \in I$.

[*Proof of Claim 1:* Let $j \in I$. Then, the pairs $(i,k) \in \overline{S}$ with $i = j$ are precisely the pairs of the form (j,k) with $k \in S_j$ and $k \neq 0$. In other words, the pairs $(i,k) \in \overline{S}$ with $i = j$ are precisely the pairs of the form (j,k) with $k \in S_j \setminus \{0\}$.

We assumed that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable. Hence, its subfamily $(p_{i,k})_{(i,k)\in\overline{S}\text{ with } i=j}$ is summable as well (since a subfamily of a summable family is always summable). In other words, the family $(p_{j,k})_{k\in S_j\setminus\{0\}}$ is summable (since this family is just a reindexing of the family $(p_{i,k})_{(i,k)\in\overline{S}\text{ with } i=j}$ (because the pairs $(i,k) \in \overline{S}$ with $i = j$ are precisely the pairs of the form (j,k) with $k \in S_j \setminus \{0\}$)). Thus, the family $(p_{j,k})_{k\in S_j}$ is summable as well (since the summability of a family does not change if we insert a single entry into it[156]).

Forget that we fixed j. We thus have shown that the family $(p_{j,k})_{k\in S_j}$ is summable for each $j \in I$. Renaming j as i in this statement, we obtain the following: The family $(p_{i,k})_{k\in S_i}$ is summable for each $i \in I$. This proves Claim 1.]

Claim 1 shows that the sum $\sum\limits_{k\in S_i} p_{i,k}$ is well-defined for each $i \in I$. Moreover, for each $i \in I$, we have

$$\begin{aligned}\sum_{k\in S_i} p_{i,k} &= \underbrace{p_{i,0}}_{\substack{=1\\ \text{(by (122))}}} + \sum_{k\in S_i\setminus\{0\}} p_{i,k} \qquad \left(\begin{array}{c}\text{here, we have split off}\\ \text{the addend for } k=0\\ \text{from the sum, since } 0\in S_i\end{array}\right)\\ &= 1 + \sum_{k\in S_i\setminus\{0\}} p_{i,k}. \end{aligned} \tag{376}$$

Next, we claim the following:

Claim 2: The family $\left(\sum\limits_{k\in S_i} p_{i,k}\right)_{i\in I}$ is multipliable.

[156] Indeed, the summability of a family is an "all but finitely many k satisfy something" type of statement. If we insert a single entry into the family, such a statement does not change its validity.

[*Proof of Claim 2:* The family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable (by assumption). We can split its sum into subsums as follows:

$$\underbrace{\sum_{(i,k)\in\overline{S}}}_{\substack{=\sum\limits_{i\in I}\ \sum\limits_{k\in S_i\setminus\{0\}} \\ \text{(since a pair } (i,k) \text{ belongs to } \overline{S} \\ \text{if and only if it satisfies } i\in I \\ \text{and } k\in S_i\setminus\{0\})}} p_{i,k} = \sum_{i\in I}\ \sum_{k\in S_i\setminus\{0\}} p_{i,k}.$$

This shows that the family $\left(\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right)_{i\in I}$ is summable. Hence, Theorem 3.11.10 (applied to $f_i = \sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}$) yields that the family $\left(1+\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right)_{i\in I}$ is multipliable. In other words, the family $\left(\sum\limits_{k\in S_i} p_{i,k}\right)_{i\in I}$ is multipliable (since (376) shows that this family is precisely the family $\left(1+\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right)_{i\in I}$). This proves Claim 2.]

Claim 2 shows that the product $\prod\limits_{i\in I}\ \sum\limits_{k\in S_i} p_{i,k}$ is well-defined.

The family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable (by assumption). In other words, for any $m\in\mathbb{N}$, all but finitely many $(i,k)\in\overline{S}$ satisfy $[x^m]\,p_{i,k}=0$. In other words, for any $m\in\mathbb{N}$, there exists a finite subset T_m of $\overline{S}$ such that

$$\text{all } (i,k)\in\overline{S}\setminus T_m \text{ satisfy } [x^m]\,p_{i,k}=0. \tag{377}$$

Consider these finite subsets T_m.

For each $n\in\mathbb{N}$, we let T'_n be the subset $T_0\cup T_1\cup\cdots\cup T_n$ of $\overline{S}$. This subset T'_n is finite (since $T_0,T_1,\ldots,T_n$ are finite).

For each $n\in\mathbb{N}$, we let I_n be the subset

$$\{i \mid (i,k)\in T'_n\}$$

of I, and we let K_n be the set

$$\{k \mid (i,k)\in T'_n\}.$$

These two sets I_n and K_n are finite (since T'_n is finite).

The definition of T'_n shows the following:

> *Claim 3:* Let $n\in\mathbb{N}$ and $(i,k)\in\overline{S}\setminus T'_n$. Then, we have
>
> $$[x^m]\,p_{i,k}=0 \qquad \text{for each } m\in\{0,1,\ldots,n\}.$$

[*Proof of Claim 3:* Let $m\in\{0,1,\ldots,n\}$. Then, $T_m\subseteq T'_n$ (since T'_n is defined as the union $T_0\cup T_1\cup\cdots\cup T_n$, whereas T_m is one of the $n+1$ sets appearing in this union). Hence, $T'_n\supseteq T_m$, so that $\overline{S}\setminus\underbrace{T'_n}_{\supseteq T_m}\subseteq\overline{S}\setminus T_m$. Now, $(i,k)\in\overline{S}\setminus T'_n\subseteq\overline{S}\setminus T_m$. Therefore, (377) shows that $[x^m]\,p_{i,k}=0$. This proves Claim 3.]

The following is easy to see:

Claim 4: If $(k_i)_{i\in I} \in S^I_{\text{fin}}$, then the family $\left(p_{i,k_i}\right)_{i\in I}$ is multipliable.

[*Proof of Claim 4:* Let $(k_i)_{i\in I} \in S^I_{\text{fin}}$. Thus, $(k_i)_{i\in I}$ is an essentially finite family in S^I. Now, all but finitely many $i \in I$ satisfy $k_i = 0$ (since $(k_i)_{i\in I}$ is essentially finite) and thus $p_{i,k_i} = p_{i,0} = 1$ (by (122)). Hence, all but finitely many entries of the family $\left(p_{i,k_i}\right)_{i\in I}$ equal 1. Thus, this family is multipliable (by Proposition 3.11.11). This proves Claim 4.]

Claim 4 shows that the product $\prod\limits_{i\in I} p_{i,k_i}$ is well-defined whenever $(k_i)_{i\in I} \in S^I_{\text{fin}}$. Next, we claim the following:

Claim 5: Let $n \in \mathbb{N}$. Let $(k_i)_{i\in I} \in S^I_{\text{fin}}$. Assume that some $j \in I$ satisfies $\left(j, k_j\right) \in \overline{S} \setminus T'_n$. Then, $[x^n] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$.

[*Proof of Claim 5:* We have assumed that some $j \in I$ satisfies $\left(j, k_j\right) \in \overline{S} \setminus T'_n$. Consider this j. Then, the product $\prod\limits_{i\in I} p_{i,k_i}$ is a multiple of p_{j,k_j} (since p_{j,k_j} is one of the factors of this product). Moreover, we have $[x^m]\, p_{j,k_j} = 0$ for each $m \in \{0, 1, \ldots, n\}$ (by Claim 3, applied to $(i,k) = \left(j, k_j\right)$). Hence, Lemma 3.3.21 (applied to $u = p_{j,k_j}$ and $v = \prod\limits_{i\in I} p_{i,k_i}$) shows that we have $[x^m] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$ for each $m \in \{0, 1, \ldots, n\}$ (since $\prod\limits_{i\in I} p_{i,k_i}$ is a multiple of p_{j,k_j}). Applying this to $m = n$, we obtain $[x^n] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$. This proves Claim 5.]

Claim 6: Let $n \in \mathbb{N}$. Let $(k_i)_{i\in I} \in S^I_{\text{fin}} \setminus S^I_{I_n}$. Then, $[x^n] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$.

[*Proof of Claim 6:* We have $(k_i)_{i\in I} \in S^I_{\text{fin}} \setminus S^I_{I_n}$. In other words, we have $(k_i)_{i\in I} \in S^I_{\text{fin}}$ but $(k_i)_{i\in I} \notin S^I_{I_n}$. From $(k_i)_{i\in I} \notin S^I_{I_n}$, we see that there exists some $j \in I \setminus I_n$ satisfying $k_j \neq 0$. Consider this j. We have $k_j \in S_j$ (since $(k_i)_{i\in I} \in S^I_{\text{fin}} \subseteq S^I$) and $j \notin I_n$ (since $j \in I \setminus I_n$). We have $\left(j, k_j\right) \in \overline{S}$ (since $k_j \in S_j$ and $k_j \neq 0$) and $\left(j, k_j\right) \notin T'_n$ (because if we had $\left(j, k_j\right) \in T'_n$, then we would have $j \in I_n$ by the definition of I_n; but this would contradict $j \notin I_n$). Hence, we have $\left(j, k_j\right) \in \overline{S} \setminus T'_n$. Therefore, Claim 5 yields $[x^n] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$. This proves Claim 6.]

Claim 7: The family $\left(\prod\limits_{i\in I} p_{i,k_i}\right)_{(k_i)_{i\in I} \in S^I_{\text{fin}}}$ is summable.

[*Proof of Claim 7:* Let $n \in \mathbb{N}$. We shall show that all but finitely many families $(k_i)_{i\in I} \in S^I_{\text{fin}}$ satisfy

$$[x^n] \left(\prod_{i\in I} p_{i,k_i}\right) = 0.$$

Indeed, let $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ be a family such that

$$\left[x^n\right] \left(\prod_{i\in I} p_{i,k_i}\right) \neq 0. \tag{378}$$

We are going to show that $\left(k_i\right)_{i\in I}$ satisfies the following two properties:

- *Property 1:* All $i \in I \setminus I_n$ satisfy $k_i = 0$.
- *Property 2:* All $i \in I_n$ satisfy $k_i \in K_n \cup \{0\}$.

These two properties together will restrict the family $\left(k_i\right)_{i\in I}$ to finitely many possibilities (since the sets I_n and K_n are finite).

If we had $\left(k_i\right)_{i\in I} \notin S^I_{I_n}$, then we would have $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}} \setminus S^I_{I_n}$ (since $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$) and thus $\left[x^n\right] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$ (by Claim 6), which would contradict (378). Hence, we cannot have $\left(k_i\right)_{i\in I} \notin S^I_{I_n}$. Thus, we have $\left(k_i\right)_{i\in I} \in S^I_{I_n}$. In other words, all $i \in I \setminus I_n$ satisfy $k_i = 0$. This proves Property 1.

If there was some $j \in I_n$ that satisfies $k_j \notin K_n \cup \{0\}$, then this k_j would satisfy $\left(j, k_j\right) \in \overline{S} \setminus T'_n$ [157], and therefore we would have $\left[x^n\right] \left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$ (by Claim 5, since $j \in I_n \subseteq I$); but this would contradict (378). Hence, there exists no $j \in I_n$ that satisfies $k_j \notin K_n \cup \{0\}$. In other words, all $i \in I_n$ satisfy $k_i \in K_n \cup \{0\}$. This proves Property 2.

Now, we have shown that our family $\left(k_i\right)_{i\in I}$ satisfies Property 1 and Property 2.

Forget that we fixed $\left(k_i\right)_{i\in I}$. We thus have shown that any family $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ that satisfies $\left[x^n\right] \left(\prod\limits_{i\in I} p_{i,k_i}\right) \neq 0$ must satisfy Property 1 and Property 2. In other words, any such family must belong to the set of all families $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ that satisfy Property 1 and Property 2. However, the latter set is finite[158]. Hence, there are only finitely many family $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ that satisfy $\left[x^n\right] \left(\prod\limits_{i\in I} p_{i,k_i}\right) \neq 0$ (since we have shown that any such family must belong to the finite set of all families $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ that satisfy Property

[157] *Proof.* Let $j \in I_n$ be such that $k_j \notin K_n \cup \{0\}$. We must show that $\left(j, k_j\right) \in \overline{S} \setminus T'_n$.

Indeed, we have $k_j \notin K_n \cup \{0\}$; thus, $k_j \notin K_n$ and $k_j \neq 0$. However, $j \in I_n \subseteq I$ and $k_j \in S_j$ (since $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}} \subseteq S^I$) and therefore $\left(j, k_j\right) \in \overline{S}$ (by the definition of $\overline{S}$, since $k_j \neq 0$). If we had $\left(j, k_j\right) \in T'_n$, then we would have $k_j \in K_n$ (by the definition of K_n), which would contradict $k_j \notin K_n$. Thus, we have $\left(j, k_j\right) \notin T'_n$. Combining this with $\left(j, k_j\right) \in \overline{S}$, we obtain $\left(j, k_j\right) \in \overline{S} \setminus T'_n$. This completes our proof.

[158] *Proof.* We must show that Property 1 and Property 2 leave only finitely many options for the family $\left(k_i\right)_{i\in I}$. Indeed, Property 1 shows that all entries k_i with $i \in I \setminus I_n$ are uniquely determined; meanwhile, Property 2 ensures that the remaining entries (of which there are only finitely many, since the set I_n is finite) must belong to the finite set $K_n \cup \{0\}$ (this set is finite, since K_n is finite). Therefore, a family $\left(k_i\right)_{i\in I}$ that satisfies Property 1 and Property 2 is uniquely determined by finitely many of its entries (namely, by its entries k_i with $i \in I_n$), and there are finitely many choices for each of them (since they must belong to the finite set $K_n \cup \{0\}$). Hence, there are only finitely many such families (namely, at most $\left|K_n \cup \{0\}\right|^{\left|I_n\right|}$ many options). In other words, the set of all families $\left(k_i\right)_{i\in I} \in S^I_{\operatorname{fin}}$ that satisfy Property 1 and Property 2 is finite.

1 and Property 2). In other words, all but finitely many families $(k_i)_{i\in I} \in S^I_{\text{fin}}$ satisfy $[x^n]\left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$.

Forget that we fixed n. We thus have shown that for each $n \in \mathbb{N}$, all but finitely many families $(k_i)_{i\in I} \in S^I_{\text{fin}}$ satisfy $[x^n]\left(\prod\limits_{i\in I} p_{i,k_i}\right) = 0$. In other words, the family $\left(\prod\limits_{i\in I} p_{i,k_i}\right)_{(k_i)_{i\in I}\in S^I_{\text{fin}}}$ is summable. This proves Claim 7.]

Claim 7 shows that the sum $\sum\limits_{(k_i)_{i\in I}\in S^I_{\text{fin}}} \prod\limits_{i\in I} p_{i,k_i}$ is well-defined. We shall next focus on proving (123).

Claim 8: Let $n \in \mathbb{N}$. Then,

$$[x^n]\left(\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}} \prod_{i\in I} p_{i,k_i}\right) = [x^n]\left(\sum_{(k_i)_{i\in I_n}\in S^{I_n}} \prod_{i\in I_n} p_{i,k_i}\right).$$

[*Proof of Claim 8:* The set I_n is finite (as we know). Thus, $S^I_{I_n} \subseteq S^I_{\text{fin}}$ [159]. Hence, the set S^I_{fin} is the union of its two disjoint subsets $S^I_{I_n}$ and $S^I_{\text{fin}} \setminus S^I_{I_n}$.

Furthermore, for each $(k_i)_{i\in I_n} \in S^I_{I_n}$, we have

$$k_i = 0 \qquad \text{for all } i \in I \setminus I_n$$

(by the definition of $S^I_{I_n}$) and therefore

$$p_{i,k_i} = p_{i,0} = 1 \qquad \text{for all } i \in I \setminus I_n$$

(by (122)) and thus

$$\prod_{i\in I\setminus I_n} \underbrace{p_{i,k_i}}_{=1} = \prod_{i\in I\setminus I_n} 1 = 1$$

and therefore

$$\prod_{i\in I} p_{i,k_i} = \left(\prod_{i\in I_n} p_{i,k_i}\right) \underbrace{\left(\prod_{i\in I\setminus I_n} p_{i,k_i}\right)}_{=1} \qquad \left(\begin{array}{c}\text{here, we have split the product into two} \\ \text{parts, since the set } I_n \text{ is a subset of } I\end{array}\right)$$
$$= \prod_{i\in I_n} p_{i,k_i}. \tag{379}$$

[159] *Proof.* Let $(k_i)_{i\in I} \in S^I_{I_n}$. Thus, $(k_i)_{i\in I}$ is a family in S^I that satisfies $k_i = 0$ for all $i \in I \setminus I_n$ (by the definition of $S^I_{I_n}$). However, I_n is finite. Thus, $k_i = 0$ for all but finitely many $i \in I$ (since $k_i = 0$ for all $i \in I \setminus I_n$). In other words, the family $(k_i)_{i\in I}$ is essentially finite. In other words, $(k_i)_{i\in I} \in S^I_{\text{fin}}$ (by the definition of S^I_{fin}).

Forget that we fixed $(k_i)_{i\in I}$. We thus have shown that $(k_i)_{i\in I} \in S^I_{\text{fin}}$ for each $(k_i)_{i\in I} \in S^I_{I_n}$. In other words, $S^I_{I_n} \subseteq S^I_{\text{fin}}$.

Now,

$$\begin{aligned}
&[x^n]\left(\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}}\ \prod_{i\in I} p_{i,k_i}\right)\\
&=\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}}[x^n]\left(\prod_{i\in I} p_{i,k_i}\right)\\
&=\sum_{(k_i)_{i\in I}\in S^I_{I_n}}\underbrace{[x^n]\left(\prod_{i\in I} p_{i,k_i}\right)}_{\substack{=\prod\limits_{i\in I_n} p_{i,k_i}\\ \text{(by (379))}}}+\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}\setminus S^I_{I_n}}\underbrace{[x^n]\left(\prod_{i\in I} p_{i,k_i}\right)}_{\substack{=0\\ \text{(by Claim 6)}}}\\
&\qquad\left(\begin{array}{c}\text{here, we have split the sum, since the set } S^I_{\text{fin}} \text{ is}\\ \text{the union of its two disjoint subsets } S^I_{I_n} \text{ and } S^I_{\text{fin}}\setminus S^I_{I_n}\end{array}\right)\\
&=\sum_{(k_i)_{i\in I}\in S^I_{I_n}}[x^n]\left(\prod_{i\in I_n} p_{i,k_i}\right)+\underbrace{\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}\setminus S^I_{I_n}}0}_{=0}\\
&=\sum_{(k_i)_{i\in I}\in S^I_{I_n}}[x^n]\left(\prod_{i\in I_n} p_{i,k_i}\right)=\sum_{(k_i)_{i\in I_n}\in S^{I_n}}[x^n]\left(\prod_{i\in I_n} p_{i,k_i}\right)\\
&\qquad\left(\begin{array}{c}\text{here, we have substituted } (k_i)_{i\in I_n} \text{ for } (k_i)_{i\in I_n} \text{ in the}\\ \text{sum, since the map } S^I_{I_n}\to S^{I_n},\ (k_i)_{i\in I}\mapsto (k_i)_{i\in I_n}\\ \text{is a bijection (indeed, this map is the map}\\ \text{we have called } \operatorname{reduce}_{I_n}\text{)}\end{array}\right)\\
&=[x^n]\left(\sum_{(k_i)_{i\in I_n}\in S^{I_n}}\ \prod_{i\in I_n} p_{i,k_i}\right).
\end{aligned}$$

This proves Claim 8.]

Claim 9: Let $n\in\mathbb{N}$. Let $i\in I\setminus I_n$. Then,

$$[x^m]\left(\sum_{k\in S_i\setminus\{0\}} p_{i,k}\right)=0 \qquad \text{for each } m\in\{0,1,\ldots,n\}.$$

[*Proof of Claim 9:* We have $i\in I\setminus I_n$. In other words, $i\in I$ and $i\notin I_n$.

Let $m\in\{0,1,\ldots,n\}$.

Let $k\in S_i\setminus\{0\}$. Thus, by the definition of $\overline{S}$, we have $(i,k)\in\overline{S}$ (since $k\in S_i\setminus\{0\}$ entails $k\in S_i$ and $k\neq 0$). On the other hand, $(i,k)\notin T'_n$ (since otherwise, we would have $(i,k)\in T'_n$ and thus $i\in I_n$ (by the definition of I_n), which would contradict $i\notin I_n$). Combining $(i,k)\in\overline{S}$ with $(i,k)\notin T'_n$, we obtain $(i,k)\in\overline{S}\setminus T'_n$. Therefore, Claim 3 yields $[x^m]\,p_{i,k}=0$.

Now, forget that we fixed k. We thus have shown that

$$[x^m]\,p_{i,k}=0 \qquad \text{for each } k\in S_i\setminus\{0\}. \tag{380}$$

Now,

$$[x^m]\left(\sum_{k\in S_i\setminus\{0\}} p_{i,k}\right) = \sum_{k\in S_i\setminus\{0\}} \underbrace{[x^m]\,p_{i,k}}_{\substack{=0\\ \text{(by (380))}}} = \sum_{k\in S_i\setminus\{0\}} 0 = 0.$$

This proves Claim 9.]

Claim 10: Let $n \in \mathbb{N}$. Then,

$$[x^n]\left(\prod_{i\in I}\ \sum_{k\in S_i} p_{i,k}\right) = [x^n]\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right).$$

[*Proof of Claim 10:* The set I_n is a subset of I. Hence, the set I is the union of its two disjoint subsets I_n and $I \setminus I_n$. Thus, we can split the product $\prod\limits_{i\in I}\ \sum\limits_{k\in S_i} p_{i,k}$ as follows:

$$\begin{aligned}\prod_{i\in I}\ \sum_{k\in S_i} p_{i,k} &= \left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right)\left(\prod_{i\in I\setminus I_n}\ \underbrace{\sum_{k\in S_i} p_{i,k}}_{\substack{=1+\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\\ \text{(by (376))}}}\right)\\ &= \left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right)\left(\prod_{i\in I\setminus I_n}\left(1+\sum_{k\in S_i\setminus\{0\}} p_{i,k}\right)\right). \qquad (381)\end{aligned}$$

However, the family $\left(\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right)_{i\in I}$ is summable (as we have seen in the proof of Claim 2). Hence, its subfamily $\left(\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right)_{i\in I\setminus I_n}$ is summable as well (since a subfamily of a summable family is always summable). Moreover, Claim 9 shows that each $i \in I \setminus I_n$ satisfies $[x^m]\left(\sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}\right) = 0$ for each $m \in \{0, 1, \ldots, n\}$. Hence, Lemma 3.11.28 (applied to $a = \prod\limits_{i\in I_n}\ \sum\limits_{k\in S_i} p_{i,k}$ and $J = I \setminus I_n$ and $f_i = \sum\limits_{k\in S_i\setminus\{0\}} p_{i,k}$) yields that

$$\begin{aligned}&[x^m]\left(\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right)\left(\prod_{i\in I\setminus I_n}\left(1+\sum_{k\in S_i\setminus\{0\}} p_{i,k}\right)\right)\right)\\ &= [x^m]\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right) \qquad \text{for each } m \in \{0, 1, \ldots, n\}.\end{aligned}$$

Applying this to $m = n$, we find

$$[x^n]\left(\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right)\left(\prod_{i\in I\setminus I_n}\left(1+\sum_{k\in S_i\setminus\{0\}} p_{i,k}\right)\right)\right) = [x^n]\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right).$$

In view of (381), this rewrites as

$$[x^n]\left(\prod_{i\in I}\ \sum_{k\in S_i} p_{i,k}\right) = [x^n]\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right).$$

This proves Claim 10.]

Claim 11: Let $i \in \mathbb{N}$. Then,

$$\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k} = \sum_{(k_i)_{i\in I_n}\in S^{I_n}}\ \prod_{i\in I_n} p_{i,k_i}.$$

[*Proof of Claim 11:* The set I_n is finite. For any $i \in I_n$, the family $(p_{i,k})_{k\in S_i}$ is summable (by Claim 1). Hence, Proposition 3.11.27 (applied to $N = I_n$) yields

$$\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k} = \sum_{(k_i)_{i\in I_n}\in \prod\limits_{i\in I_n} S_i}\ \prod_{i\in I_n} p_{i,k_i} = \sum_{(k_i)_{i\in I_n}\in S^{I_n}}\ \prod_{i\in I_n} p_{i,k_i}$$

(since $\prod\limits_{i\in I_n} S_i = S^{I_n}$). This proves Claim 11.]

Now, for each $n \in \mathbb{N}$, we have

$$\begin{aligned}
&[x^n]\left(\prod_{i\in I}\ \sum_{k\in S_i} p_{i,k}\right)\\
&= [x^n]\left(\prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k}\right) \qquad \text{(by Claim 10)}\\
&= [x^n]\left(\sum_{(k_i)_{i\in I_n}\in S^{I_n}}\ \prod_{i\in I_n} p_{i,k_i}\right)\\
&\qquad\qquad \left(\text{since Claim 11 yields } \prod_{i\in I_n}\ \sum_{k\in S_i} p_{i,k} = \sum_{(k_i)_{i\in I_n}\in S^{I_n}}\ \prod_{i\in I_n} p_{i,k_i}\right)\\
&= [x^n]\left(\sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}}\ \prod_{i\in I} p_{i,k_i}\right) \qquad \text{(by Claim 8)}.
\end{aligned}$$

That is, any coefficient of the FPS $\prod\limits_{i\in I}\ \sum\limits_{k\in S_i} p_{i,k}$ equals the corresponding coefficient of $\sum\limits_{(k_i)_{i\in I}\in S^I_{\text{fin}}}\ \prod\limits_{i\in I} p_{i,k_i}$. Hence,

$$\prod_{i\in I}\ \sum_{k\in S_i} p_{i,k} = \sum_{(k_i)_{i\in I}\in S^I_{\text{fin}}}\ \prod_{i\in I} p_{i,k_i} = \sum_{\substack{(k_i)_{i\in I}\in \prod\limits_{i\in I} S_i \\ \text{is essentially finite}}}\ \prod_{i\in I} p_{i,k_i}$$

(since S^I_{fin} is the set of all essentially finite families $(k_i)_{i\in I} \in \prod\limits_{i\in I} S_i$). In particular, the family $\left(\prod\limits_{i\in I} p_{i,k_i}\right)_{(k_i)_{i\in I}\in \prod\limits_{i\in I} S_i \text{ is essentially finite}}$ is summable. This proves Proposition 3.11.26.

□

Our proof of Proposition 3.11.32 will use the **finite** analogue of Proposition 3.11.32, which is easy:

> **Lemma B.2.7.** Let I be a **finite** set. If $(f_i)_{i\in I} \in K[[x]]^I$ is a family of FPSs, and if $g \in K[[x]]$ is an FPS satisfying $[x^0]\, g = 0$, then $\left(\prod\limits_{i\in I} f_i\right) \circ g = \prod\limits_{i\in I} (f_i \circ g)$.

Proof of Lemma B.2.7. This follows by a straightforward induction on $|I|$. (The base case is the case when $|I| = 0$, and relies on the fact that $\underline{1} \circ g = \underline{1}$ for any $g \in K[[x]]$. The induction step relies on Proposition 3.5.4 **(b)**. The details are left to the reader, who must have seen dozens of such proofs by now.) □

Detailed proof of Proposition 3.11.32. Let $(f_i)_{i\in I} \in K[[x]]^I$ be a multipliable family of FPSs. Let $g \in K[[x]]$ be an FPS satisfying $[x^0]\, g = 0$.

We shall first show the following auxiliary claim:

> *Claim 1:* Let M be an x^n-approximator for $(f_i)_{i\in I}$. Then, the set M determines the x^n-coefficient in the product of $(f_i \circ g)_{i\in I}$.

[*Proof of Claim 1:* The set M is an x^n-approximator for $(f_i)_{i\in I}$. In other words, M is a finite subset of I that determines the first $n+1$ coefficients in the product of $(f_i)_{i\in I}$ (by the definition of "x^n-approximator").

Let J be a finite subset of I satisfying $M \subseteq J \subseteq I$. Then, Lemma B.2.7 (applied to J instead of I) yields

$$\left(\prod_{i\in J} f_i\right) \circ g = \prod_{i\in J} (f_i \circ g). \tag{382}$$

Also, Lemma B.2.7 (applied to M instead of I) yields

$$\left(\prod_{i\in M} f_i\right) \circ g = \prod_{i\in M} (f_i \circ g). \tag{383}$$

However, Proposition 3.11.16 **(a)** (applied to $\mathbf{a}_i = f_i$) yields

$$\prod_{i\in J} f_i \overset{x^n}{\equiv} \prod_{i\in M} f_i.$$

We also have $g \overset{x^n}{\equiv} g$ (since the relation $\overset{x^n}{\equiv}$ is an equivalence relation). Hence, Proposition 3.10.5 (applied to $a = \prod\limits_{i\in J} f_i$ and $b = \prod\limits_{i\in M} f_i$ and $c = g$ and $d = g$) yields

$$\left(\prod_{i\in J} f_i\right) \circ g \overset{x^n}{\equiv} \left(\prod_{i\in M} f_i\right) \circ g.$$

In view of (382) and (383), this rewrites as

$$\prod_{i\in J} (f_i \circ g) \overset{x^n}{\equiv} \prod_{i\in M} (f_i \circ g).$$

In other words,

$$\text{each } m \in \{0, 1, \ldots, n\} \text{ satisfies } \left[x^m\right] \left(\prod_{i \in J} \left(f_i \circ g\right) \right) = \left[x^m\right] \left(\prod_{i \in M} \left(f_i \circ g\right) \right)$$

(by the definition of the relation $\overset{x^n}{\equiv}$). Applying this to $m = n$, we obtain

$$\left[x^n\right] \left(\prod_{i \in J} \left(f_i \circ g\right) \right) = \left[x^n\right] \left(\prod_{i \in M} \left(f_i \circ g\right) \right).$$

Forget that we fixed J. We thus have shown that every finite subset J of I satisfying $M \subseteq J \subseteq I$ satisfies

$$\left[x^n\right] \left(\prod_{i \in J} \left(f_i \circ g\right) \right) = \left[x^n\right] \left(\prod_{i \in M} \left(f_i \circ g\right) \right).$$

In other words, the set M determines the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$ (by the definition of what it means to "determine the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$"). This proves Claim 1.]

Now, let $n \in \mathbb{N}$. Lemma 3.11.15 (applied to $\mathbf{a}_i = f_i$) shows that there exists an x^n-approximator for $\left(f_i\right)_{i \in I}$. Consider this x^n-approximator for $\left(f_i\right)_{i \in I}$, and denote it by M. Thus, M is an x^n-approximator for $\left(f_i\right)_{i \in I}$; in other words, M is a finite subset of I that determines the first $n+1$ coefficients in the product of $\left(f_i\right)_{i \in I}$ (by the definition of "x^n-approximator"). Claim 1 shows that the set M determines the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$. Hence, there is a finite subset of I that determines the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$ (namely, M). In other words, the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$ is finitely determined.

Forget that we fixed n. We thus have shown that for each $n \in \mathbb{N}$, the x^n-coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$ is finitely determined. In other words, each coefficient in the product of $\left(f_i \circ g\right)_{i \in I}$ is finitely determined. In other words, the family $\left(f_i \circ g\right)_{i \in I}$ is multipliable (by the definition of "multipliable").

It remains to prove that $\left(\prod\limits_{i \in I} f_i \right) \circ g = \prod\limits_{i \in I} \left(f_i \circ g\right)$.

In order to do so, we again fix $n \in \mathbb{N}$. Lemma 3.11.15 (applied to $\mathbf{a}_i = f_i$) shows that there exists an x^n-approximator for $\left(f_i\right)_{i \in I}$. Consider this x^n-approximator for $\left(f_i\right)_{i \in I}$, and denote it by M. Thus, M is an x^n-approximator for $\left(f_i\right)_{i \in I}$; in other words, M is a finite subset of I that determines the first $n+1$ coefficients in the product of $\left(f_i\right)_{i \in I}$ (by the definition of "x^n-approximator"). Moreover, Proposition 3.11.16 **(b)** (applied to $\mathbf{a}_i = f_i$) yields

$$\prod_{i \in I} f_i \overset{x^n}{\equiv} \prod_{i \in M} f_i. \tag{384}$$

We also have $g \overset{x^n}{\equiv} g$ (since the relation $\overset{x^n}{\equiv}$ is an equivalence relation). Hence, Proposition 3.10.5 (applied to $a = \prod\limits_{i \in I} f_i$ and $b = \prod\limits_{i \in M} f_i$ and $c = g$ and $d = g$) yields

$$\left(\prod_{i \in I} f_i \right) \circ g \overset{x^n}{\equiv} \left(\prod_{i \in M} f_i \right) \circ g. \tag{385}$$

However, Lemma B.2.7 (applied to M instead of I) yields

$$\left(\prod_{i\in M} f_i\right)\circ g = \prod_{i\in M}\left(f_i\circ g\right).$$

In view of this, we can rewrite (385) as

$$\left(\prod_{i\in I} f_i\right)\circ g \overset{x^n}{\equiv} \prod_{i\in M}\left(f_i\circ g\right).$$

In other words,

$$\text{each } m\in\{0,1,\ldots,n\} \text{ satisfies } \left[x^m\right]\left(\left(\prod_{i\in I} f_i\right)\circ g\right) = \left[x^m\right]\left(\prod_{i\in M}\left(f_i\circ g\right)\right)$$

(by the definition of the relation $\overset{x^n}{\equiv}$). Applying this to $m=n$, we obtain

$$\left[x^n\right]\left(\left(\prod_{i\in I} f_i\right)\circ g\right) = \left[x^n\right]\left(\prod_{i\in M}\left(f_i\circ g\right)\right). \tag{386}$$

However, Claim 1 shows that the set M determines the x^n-coefficient in the product of $\left(f_i\circ g\right)_{i\in I}$. Hence, the definition of the infinite product $\prod\limits_{i\in I}\left(f_i\circ g\right)$ (specifically, Definition 3.11.5 **(b)**) yields

$$\left[x^n\right]\left(\prod_{i\in I}\left(f_i\circ g\right)\right) = \left[x^n\right]\left(\prod_{i\in M}\left(f_i\circ g\right)\right).$$

Comparing this with (386), we obtain

$$\left[x^n\right]\left(\left(\prod_{i\in I} f_i\right)\circ g\right) = \left[x^n\right]\left(\prod_{i\in I}\left(f_i\circ g\right)\right).$$

Forget that we fixed n. We thus have shown that each $n\in\mathbb{N}$ satisfies

$$\left[x^n\right]\left(\left(\prod_{i\in I} f_i\right)\circ g\right) = \left[x^n\right]\left(\prod_{i\in I}\left(f_i\circ g\right)\right).$$

In other words, the FPSs $\left(\prod\limits_{i\in I} f_i\right)\circ g$ and $\prod\limits_{i\in I}\left(f_i\circ g\right)$ agree in all their coefficients. Hence, $\left(\prod\limits_{i\in I} f_i\right)\circ g = \prod\limits_{i\in I}\left(f_i\circ g\right)$. This completes our proof of Proposition 3.11.32. □

B.3. Cancellations in alternating sums

We shall now prove Lemma 6.1.3 and Lemma 6.1.4. We start with the latter lemma, since the former will then follow trivially from it.

Proof of Lemma 6.1.4. The set $\mathcal{X}$ is finite (since it is a subset of the finite set $\mathcal{A}$). Thus, $|\mathcal{X}| = n$ for some $n \in \mathbb{N}$. Consider this n.

Let $[n]$ be the set $\{1, 2, \ldots, n\}$. Then, $|[n]| = n$. Comparing this with $|\mathcal{X}| = n$, we obtain $|\mathcal{X}| = |[n]|$. Hence, there exists a bijection $\alpha : \mathcal{X} \to [n]$. Consider this α.

Now, define two subsets $\mathcal{U}$ and $\mathcal{W}$ of $\mathcal{X}$ by

$$\mathcal{U} := \{I \in \mathcal{X} \mid \alpha(f(I)) < \alpha(I)\};$$
$$\mathcal{W} := \{I \in \mathcal{X} \mid \alpha(f(I)) > \alpha(I)\}.$$

Then, $f(\mathcal{U}) \subseteq \mathcal{W}$ [160] and $f(\mathcal{W}) \subseteq \mathcal{U}$ [161]. Now, the map

$$g : \mathcal{U} \to \mathcal{W},$$
$$I \mapsto f(I)$$

is well-defined (since each $I \in \mathcal{U}$ satisfies $f(I) \in f(\mathcal{U}) \subseteq \mathcal{W}$), and the map

$$h : \mathcal{W} \to \mathcal{U},$$
$$I \mapsto f(I)$$

is also well-defined (since each $I \in \mathcal{W}$ satisfies $f(I) \in f(\mathcal{W}) \subseteq \mathcal{U}$). Consider these two maps g and h. It is clear that $g \circ h = \operatorname{id}$ [162] and $h \circ g = \operatorname{id}$ [163]. Hence, the maps g and h are mutually inverse, and thus are bijections.

[160] *Proof.* Let $J \in f(\mathcal{U})$. Thus, $J = f(K)$ for some $K \in \mathcal{U}$. Consider this K. We have $K \in \mathcal{U} = \{I \in \mathcal{X} \mid \alpha(f(I)) < \alpha(I)\}$; in other words, K is an $I \in \mathcal{X}$ satisfying $\alpha(f(I)) < \alpha(I)$. In other words, K is an element of $\mathcal{X}$ and satisfies $\alpha(f(K)) < \alpha(K)$. However, we have $f \circ f = \operatorname{id}$ (since f is an involution) and thus $(f \circ f)(K) = \operatorname{id}(K) = K$, so that $K = (f \circ f)(K) = f\left(\underbrace{f(K)}_{=J}\right) = f(J)$. However, from $J = f(K)$, we obtain $\alpha(J) = \alpha(f(K)) < \alpha\left(\underbrace{K}_{=f(J)}\right) = \alpha(f(J))$, so that $\alpha(f(J)) > \alpha(J)$.

Now, J is an element of $\mathcal{X}$ and satisfies $\alpha(f(J)) > \alpha(J)$. In other words, J is an $I \in \mathcal{X}$ satisfying $\alpha(f(I)) > \alpha(I)$. In other words, $J \in \{I \in \mathcal{X} \mid \alpha(f(I)) > \alpha(I)\}$. In other words, $J \in \mathcal{W}$ (since $\mathcal{W} = \{I \in \mathcal{X} \mid \alpha(f(I)) > \alpha(I)\}$).

Forget that we fixed J. We thus have shown that $J \in \mathcal{W}$ for each $J \in f(\mathcal{U})$. In other words, $f(\mathcal{U}) \subseteq \mathcal{W}$.

[161] The *proof* of $f(\mathcal{W}) \subseteq \mathcal{U}$ is completely analogous to the proof of $f(\mathcal{U}) \subseteq \mathcal{W}$ we just gave; the only changes are that all "$<$" signs have to be replaced by "$>$" signs and vice versa, and that all "$\mathcal{U}$"s have to be replaced by "$\mathcal{W}$"s and vice versa.

[162] *Proof.* Let $I \in \mathcal{U}$. Recall that f is an involution; thus, $f \circ f = \operatorname{id}$. Now, $(g \circ h)(I) = g(h(I)) = f(h(I))$ (by the definition of g). However, $h(I) = f(I)$ (by the definition of h). Thus, $(g \circ h)(I) = f\left(\underbrace{h(I)}_{=f(I)}\right) = f(f(I)) = \underbrace{(f \circ f)}_{=\operatorname{id}}(I) = \operatorname{id}(I) = I = \operatorname{id}(I)$.

Forget that we fixed I. We thus have shown that $(g \circ h)(I) = \operatorname{id}(I)$ for each $I \in \mathcal{U}$. In other words, $g \circ h = \operatorname{id}$.

[163] The *proof* of this is analogous to the proof of $g \circ h = \operatorname{id}$ we just gave.

We have

$$\operatorname{sign} I + \operatorname{sign}\left(g\left(I\right)\right) = 0 \qquad \text{for all } I \in \mathcal{U} \tag{387}$$

[164]. Furthermore, we have

$$\operatorname{sign} I = 0 \qquad \text{for all } I \in \mathcal{X} \text{ satisfying } \alpha\left(f\left(I\right)\right) = \alpha\left(I\right). \tag{388}$$

[165].

However, each $I \in \mathcal{X}$ satisfies exactly one of the three conditions "$\alpha\left(f\left(I\right)\right) < \alpha\left(I\right)$", "$\alpha\left(f\left(I\right)\right) = \alpha\left(I\right)$" and "$\alpha\left(f\left(I\right)\right) > \alpha\left(I\right)$" (because $\alpha\left(f\left(I\right)\right)$ and $\alpha\left(I\right)$ are two integers). Hence, we can split the sum $\sum\limits_{I\in\mathcal{X}} \operatorname{sign} I$ as follows:

$$\begin{aligned}
\sum_{I\in\mathcal{X}} \operatorname{sign} I &= \sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))<\alpha(I)}} \operatorname{sign} I + \sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))=\alpha(I)}} \underbrace{\operatorname{sign} I}_{\substack{=0\\ \text{(by (388))}}} + \sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))>\alpha(I)}} \operatorname{sign} I \\
&= \sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))<\alpha(I)}} \operatorname{sign} I + \underbrace{\sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))=\alpha(I)}} 0}_{=0} + \sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))>\alpha(I)}} \operatorname{sign} I \\
&= \underbrace{\sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))<\alpha(I)}}}_{\substack{=\sum_{I\in\mathcal{U}}\\ \text{(since } \{I\in\mathcal{X} \mid \alpha(f(I))<\alpha(I)\}=\mathcal{U})}} \operatorname{sign} I + \underbrace{\sum_{\substack{I\in\mathcal{X};\\ \alpha(f(I))>\alpha(I)}}}_{\substack{=\sum_{I\in\mathcal{W}}\\ \text{(since } \{I\in\mathcal{X} \mid \alpha(f(I))>\alpha(I)\}=\mathcal{W})}} \operatorname{sign} I \\
&= \sum_{I\in\mathcal{U}} \operatorname{sign} I + \underbrace{\sum_{I\in\mathcal{W}} \operatorname{sign} I}_{\substack{=\sum_{I\in\mathcal{U}} \operatorname{sign}(g(I)) \\ \text{(here, we have substituted } g(I) \\ \text{for } I \text{ in the sum, since the} \\ \text{map } g:\mathcal{U}\to\mathcal{W} \text{ is a bijection)}}} = \sum_{I\in\mathcal{U}} \operatorname{sign} I + \sum_{I\in\mathcal{U}} \operatorname{sign}\left(g\left(I\right)\right) \\
&= \sum_{I\in\mathcal{U}} \underbrace{\left(\operatorname{sign} I + \operatorname{sign}\left(g\left(I\right)\right)\right)}_{\substack{=0\\ \text{(by (387))}}} = \sum_{I\in\mathcal{U}} 0 = 0.
\end{aligned}$$

[164] *Proof of (387):* Let $J \in \mathcal{U}$. Then, $J \in \mathcal{U} \subseteq \mathcal{X}$ and $g\left(J\right) = f\left(J\right)$ (by the definition of g). Now, recall our assumption saying that $\operatorname{sign}\left(f\left(I\right)\right) = -\operatorname{sign} I$ for all $I \in \mathcal{X}$. Applying this to $I = J$, we obtain $\operatorname{sign}\left(f\left(J\right)\right) = -\operatorname{sign} J$. In view of $g\left(J\right) = f\left(J\right)$, this rewrites as $\operatorname{sign}\left(g\left(J\right)\right) = -\operatorname{sign} J$. In other words, $\operatorname{sign} J + \operatorname{sign}\left(g\left(J\right)\right) = 0$.

Forget that we fixed J. We thus have shown that $\operatorname{sign} J + \operatorname{sign}\left(g\left(J\right)\right) = 0$ for all $J \in \mathcal{U}$. Renaming J as I in this statement, we obtain that $\operatorname{sign} I + \operatorname{sign}\left(g\left(I\right)\right) = 0$ for all $I \in \mathcal{U}$. This proves (387).

[165] *Proof of (388):* Recall our assumption saying that

$$\operatorname{sign} I = 0 \qquad \text{for all } I \in \mathcal{X} \text{ satisfying } f\left(I\right) = I. \tag{389}$$

Now, let $J \in \mathcal{X}$ satisfy $\alpha\left(f\left(J\right)\right) = \alpha\left(J\right)$. The map α is injective (since α is a bijection). Thus, from $\alpha\left(f\left(J\right)\right) = \alpha\left(J\right)$, we obtain $f\left(J\right) = J$. Therefore, (389) (applied to $I = J$) yields $\operatorname{sign} J = 0$.

Forget that we fixed J. We thus have shown that $\operatorname{sign} J = 0$ for all $J \in \mathcal{X}$ satisfying $\alpha\left(f\left(J\right)\right) = \alpha\left(J\right)$. Renaming the variable J as I in this statement, we conclude that $\operatorname{sign} I = 0$ for all $I \in \mathcal{X}$ satisfying $\alpha\left(f\left(I\right)\right) = \alpha\left(I\right)$. This proves (388).

However, the set $\mathcal{A}$ is the union of its two disjoint subsets $\mathcal{X}$ and $\mathcal{A} \setminus \mathcal{X}$ (since $\mathcal{X} \subseteq \mathcal{A}$). Thus, we can split the sum $\sum\limits_{I \in \mathcal{A}} \operatorname{sign} I$ as follows:

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \underbrace{\sum_{I \in \mathcal{X}} \operatorname{sign} I}_{=0} + \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

This proves Lemma 6.1.4. □

Proof of Lemma 6.1.3. The map f has no fixed points (by assumption). In other words, there exist no $I \in \mathcal{X}$ satisfying $f(I) = I$. Hence, we have $\operatorname{sign} I = 0$ for all $I \in \mathcal{X}$ satisfying $f(I) = I$ (because non-existing objects satisfy any possible claim; this is known as being "vacuously true"). Thus, Lemma 6.1.4 yields $\sum\limits_{I \in \mathcal{A}} \operatorname{sign} I = \sum\limits_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I$. This proves Lemma 6.1.3. □

B.4. Determinants in combinatorics

Proof of Proposition 6.5.10. If q is any path, then the *length* $\ell(q)$ of q is defined to be the number of arcs of q.

We shall now prove Proposition 6.5.10 by strong induction on $\ell(p) + \ell(p')$:

Induction step: Fix a nonnegative integer N. Assume (as the induction hypothesis) that Proposition 6.5.10 holds whenever $\ell(p) + \ell(p') < N$. We must now prove that Proposition 6.5.10 holds when $\ell(p) + \ell(p') = N$.

So let A, B, A', B', p and p' be as in Proposition 6.5.10, and let us assume that $\ell(p) + \ell(p') = N$. We must prove that p and p' have a vertex in common.

Assume the contrary. Thus, p and p' have no vertex in common.

Recall that each arc of the lattice is either an east-step or a north-step. Thus, the x-coordinates of the vertices of a path are always weakly increasing (i.e., if $(v_0, v_1, \ldots, v_n)$ is a path, then $\mathrm{x}(v_0) \leq \mathrm{x}(v_1) \leq \cdots \leq \mathrm{x}(v_n)$), and so are the y-coordinates. Hence, the existence of a path p from A to B' shows that $\mathrm{x}(A) \leq \mathrm{x}(B')$ and $\mathrm{y}(A) \leq \mathrm{y}(B')$. Similarly, the existence of a path p' from A' to B yields $\mathrm{x}(A') \leq \mathrm{x}(B)$ and $\mathrm{y}(A') \leq \mathrm{y}(B)$.

We are in one of the following three cases:

Case 1: We have $\mathrm{y}(A') > \mathrm{y}(A)$.

Case 2: We have $\mathrm{x}(A') < \mathrm{x}(A)$.

Case 3: We have neither $\mathrm{y}(A') > \mathrm{y}(A)$ nor $\mathrm{x}(A') < \mathrm{x}(A)$.

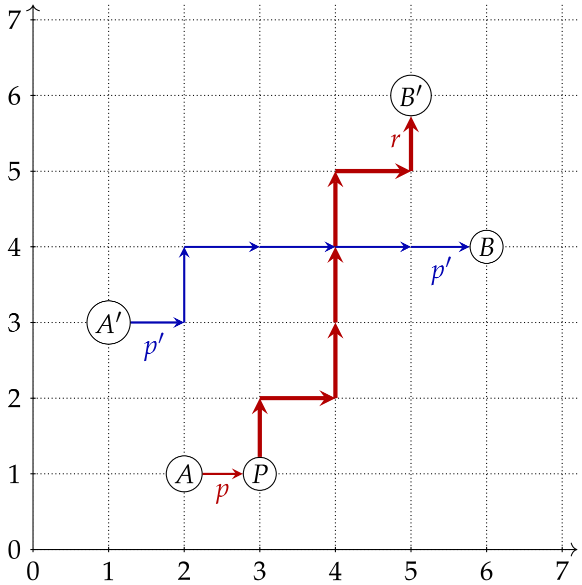
We shall derive a contradiction in each of these cases.

Let us first consider Case 1. In this case, we have $\mathrm{y}(A') > \mathrm{y}(A)$. Thus, $\mathrm{y}(A) < \mathrm{y}(A') \leq \mathrm{y}(B) \leq \mathrm{y}(B')$ (since $\mathrm{y}(B') \geq \mathrm{y}(B)$), so that $\mathrm{y}(A) \neq \mathrm{y}(B')$ and therefore $A \neq B'$. This shows that the path p has at least two vertices (since p is a path from A to B'). Let P be its second vertex. Hence, P lies on a path from A to B' (namely, on the path p). Therefore, $\mathrm{x}(A) \leq \mathrm{x}(P) \leq \mathrm{x}(B')$ (since the x-coordinates of the vertices of a path are always weakly increasing) and $\mathrm{y}(A) \leq \mathrm{y}(P) \leq \mathrm{y}(B')$ (since the y-coordinates of the vertices of a path are always weakly increasing). Let r be the path from P to B' obtained by removing the first arc from p (in other words, let r be the part of p from the point P onwards)[166]. Thus, r is a subpath of p. Hence, the paths r and p' have no vertex in common (since p and p' have no vertex in common). Also, $\ell(r) = \ell(p) - 1 < \ell(p)$ and thus $\underbrace{\ell(r)}_{<\ell(p)} + \ell(p') < \ell(p) + \ell(p') = N$. Moreover, $\mathrm{x}(A') \leq \mathrm{x}(A) \leq \mathrm{x}(P)$. Thus, if we had $\mathrm{y}(A') \geq \mathrm{y}(P)$, then we could apply Proposition 6.5.10 to P and r instead of A and p (by the induction hypothesis, since $\ell(r) + \ell(p') < N$). We would consequently conclude that the paths r and p' have a vertex in common; this would contradict the fact that the paths r and p' have no vertex in common. Hence, we cannot have $\mathrm{y}(A') \geq \mathrm{y}(P)$. Thus, $\mathrm{y}(A') < \mathrm{y}(P)$. Hence, $\mathrm{y}(A') \leq \mathrm{y}(P) - 1$ (since $\mathrm{y}(A')$ and $\mathrm{y}(P)$ are integers). But P is the next vertex after A on the path p. Hence, there is an arc from A to P. If this arc was an east-step, then we would have $\mathrm{y}(P) = \mathrm{y}(A)$, which would contradict $\mathrm{y}(A) \leq \mathrm{y}(A') < \mathrm{y}(P)$. Hence, this arc cannot be an east-step. Thus, this arc must be a north-step. Therefore, $\mathrm{y}(P) = \mathrm{y}(A) + 1$. Hence, $\mathrm{y}(A') \leq \mathrm{y}(P) - 1 = \mathrm{y}(A)$ (since $\mathrm{y}(P) = \mathrm{y}(A) + 1$). But this contradicts $\mathrm{y}(A') > \mathrm{y}(A)$. Thus, we have found a contradiction in Case 1.

An analogous argument can be used to find a contradiction in Case 2. In fact, there is a symmetry inherent in Proposition 6.5.10, which interchanges Case 1 with Case 2. Namely, if we reflect all points and paths across the $x = y$ line (i.e., if we replace each point (i, j) by (j, i)), and if we rename A, B, A', B', p and p' as A', A, B', B, p' and p (respectively), then Case 1 becomes Case 2 and vice versa[167]. Thus, Case 2 spawns a contradiction just like Case 1 did.

Finally, let us consider Case 3. In this case, we have neither $\mathrm{y}(A') > \mathrm{y}(A)$ nor $\mathrm{x}(A') < \mathrm{x}(A)$. In other words, we have $\mathrm{y}(A') \leq \mathrm{y}(A)$ and $\mathrm{x}(A') \geq \mathrm{x}(A)$. Combining $\mathrm{x}(A') \geq \mathrm{x}(A)$ with $\mathrm{x}(A') \leq \mathrm{x}(A)$, we obtain $\mathrm{x}(A') = \mathrm{x}(A)$. Combining $\mathrm{y}(A') \leq$

[166] Here is an illustration (with r drawn extra-thick):



[167] Importantly, this reflection preserves our digraph (in fact, it transforms north-steps into east-steps and vice versa).

$\mathrm{y}(A)$ with $\mathrm{y}(A') \geq \mathrm{y}(A)$, we obtain $\mathrm{y}(A') = \mathrm{y}(A)$. Now, the vertices A and A' have the same x-coordinate (since $\mathrm{x}(A') = \mathrm{x}(A)$) and the same y-coordinate (since $\mathrm{y}(A') = \mathrm{y}(A)$). Hence, these two vertices are equal. In other words, $A = A'$. Hence, the vertex A belongs to the path p' (since the vertex A' belongs to the path p'). However, the vertex A belongs to the path p as well. Thus, the paths p and p' have a vertex in common (namely, A). This contradicts the fact that p and p' have no vertex in common. Thus, we have found a contradiction in Case 3.

We have now found contradictions in all three Cases 1, 2 and 3. Hence, our assumption must have been false. We thus conclude that p and p' have a vertex in common. Now, forget that we fixed A, B, A', B', p and p'. We thus have proven that if A, B, A', B', p and p' are as in Proposition 6.5.10, and if $\ell(p) + \ell(p') = N$, then p and p' have a vertex in common. In other words, Proposition 6.5.10 holds when $\ell(p) + \ell(p') = N$. This completes the induction step. Hence, Proposition 6.5.10 is proven.

(This proof is essentially the first proof from `https://math.stackexchange.com/questions/2870640/` .) □

B.5. Definitions and examples of symmetric polynomials

Detailed proof of Lemma 7.1.17. Let $\sigma \in S_N$. We shall prove that $\sigma \cdot f = f$.

Let us follow Convention 5.3.16; thus, we shall refer to the simple transpositions $s_1, s_2, \ldots, s_{N-1}$ in S_N as "simples".

Theorem 5.3.17 **(a)** (applied to $n = N$) shows that we can write σ as a composition (i.e., product) of $\ell(\sigma)$ simples. Thus, in particular, we can write σ as a finite product of simples.[168] In other words, there exist finitely many elements $k_1, k_2, \ldots, k_p \in [N-1]$ such that $\sigma = s_{k_1} s_{k_2} \cdots s_{k_p}$. Consider these $k_1, k_2, \ldots, k_p$.

Now,

$$\begin{aligned}\underbrace{\sigma}_{= s_{k_1} s_{k_2} \cdots s_{k_p}} \cdot f &= \left(s_{k_1} s_{k_2} \cdots s_{k_p} \right) \cdot f = s_{k_1} \cdot s_{k_2} \cdot \cdots \cdot s_{k_{p-1}} \cdot \underbrace{s_{k_p} \cdot f}_{\substack{=f \\ \text{(by (250))}}} \\ &= s_{k_1} \cdot s_{k_2} \cdot \cdots \cdot s_{k_{p-2}} \cdot \underbrace{s_{k_{p-1}} \cdot f}_{\substack{=f \\ \text{(by (250))}}} = s_{k_1} \cdot s_{k_2} \cdot \cdots \cdot s_{k_{p-3}} \cdot \underbrace{s_{k_{p-2}} \cdot f}_{\substack{=f \\ \text{(by (250))}}} \\ &= \cdots = f.\end{aligned}$$

(To be fully rigorous, this is really an induction argument: We are showing (by induction on i) that $s_{k_1} s_{k_2} \cdots s_{k_i} f = f$ for each $i \in \{0, 1, \ldots, p\}$; the induction base is obvious (since $s_{k_1} s_{k_2} \cdots s_{k_0} = (\text{empty product in } S_N) = \mathrm{id}$), while the induction step relies on (250). It is straightforward to fill in the details of this induction.)

[168] Alternatively, we can derive this from Corollary 5.3.22 (which is more well-known than Theorem 5.3.17 **(a)**):

Corollary 5.3.22 (applied to $n = N$) shows that the symmetric group S_N is generated by the simples $s_1, s_2, \ldots, s_{N-1}$. Hence, each element of S_N is a (finite) product of simples and their inverses. Since the inverses of the simples are simply these simples themselves (because each $i \in [N-1]$ satisfies $s_i^{-1} = s_i$), we can simplify this statement as follows: Each element of S_N is a (finite) product of simples. Applying this to the element σ, we conclude that σ is a (finite) product of simples.

Forget that we fixed σ. We thus have proved that $\sigma \cdot f = f$ for all $\sigma \in S_N$. In other words, the polynomial f is symmetric. This proves Lemma 7.1.17. □

B.6. N-partitions and monomial symmetric polynomials

Proof of Proposition 7.2.9. Let us write the polynomial f as

$$f = \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_1,b_2,\ldots,b_N} x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}, \tag{390}$$

where the coefficients $f_{b_1,b_2,\ldots,b_N}$ belong to K. Thus, the coefficient of any monomial $x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}$ in f is $f_{b_1,b_2,\ldots,b_N}$. In other words,

$$\left[x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}\right] f = f_{b_1,b_2,\ldots,b_N} \tag{391}$$

for each $(b_1, b_2, \ldots, b_N) \in \mathbb{N}^N$.

The map σ is a permutation of $[N]$ (since $\sigma \in S_N$). Hence, the map

$$\begin{aligned} \mathbb{N}^N &\to \mathbb{N}^N, \\ (b_1, b_2, \ldots, b_N) &\mapsto \left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(N)}\right) \end{aligned} \tag{392}$$

is a bijection (indeed, this map simply permutes the entries of any given N-tuple using the permutation σ; thus, it can be undone by permuting them using σ^{-1}). Moreover, the map σ itself is a bijection (since it is a permutation).

The definition of the action of S_N on $\mathcal{P}$ yields

$$\begin{aligned} \sigma \cdot f &= f\left[x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)}\right] \\ &= \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_1,b_2,\ldots,b_N} x_{\sigma(1)}^{b_1} x_{\sigma(2)}^{b_2} \cdots x_{\sigma(N)}^{b_N} \\ &\qquad \left(\begin{array}{c}\text{here, we have substituted } x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(N)} \\ \text{for } x_1, x_2, \ldots, x_N \text{ on both sides of (390)}\end{array}\right) \\ &= \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(N)}} x_{\sigma(1)}^{b_{\sigma(1)}} x_{\sigma(2)}^{b_{\sigma(2)}} \cdots x_{\sigma(N)}^{b_{\sigma(N)}} \end{aligned}$$

(here, we have substituted $\left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(N)}\right)$ for the summation index $(b_1, b_2, \ldots, b_N)$ in the sum, since the map (392) is a bijection). Thus,

$$\begin{aligned} \sigma \cdot f &= \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(N)}} \underbrace{x_{\sigma(1)}^{b_{\sigma(1)}} x_{\sigma(2)}^{b_{\sigma(2)}} \cdots x_{\sigma(N)}^{b_{\sigma(N)}}}_{\substack{=\prod_{i\in\{1,2,\ldots,N\}} x_{\sigma(i)}^{b_{\sigma(i)}} = \prod_{i\in\{1,2,\ldots,N\}} x_i^{b_i} \\ \text{(here, we have substituted } i \text{ for } \sigma(i) \text{ in the product,} \\ \text{since the map } \sigma:[N]\to[N] \text{ is a bijection)}}} \\ &= \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(N)}} \underbrace{\prod_{i\in\{1,2,\ldots,N\}} x_i^{b_i}}_{=x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}} \\ &= \sum_{(b_1,b_2,\ldots,b_N)\in\mathbb{N}^N} f_{b_{\sigma(1)},b_{\sigma(2)},\ldots,b_{\sigma(N)}} x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}. \end{aligned}$$

Hence, for each $(b_1, b_2, \ldots, b_N) \in \mathbb{N}^N$, we have

$$\begin{aligned} f_{b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(N)}} &= \left(\text{the coefficient of } x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N} \text{ in } \sigma \cdot f\right) \\ &= \left[x_1^{b_1} x_2^{b_2} \cdots x_N^{b_N}\right] (\sigma \cdot f) . \end{aligned} \tag{393}$$

Now, let $(a_1, a_2, \ldots, a_N) \in \mathbb{N}^N$ be arbitrary. Then, (391) (applied to $(b_1, b_2, \ldots, b_N) = \left(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(N)}\right)$) yields

$$\left[x_1^{a_{\sigma(1)}} x_2^{a_{\sigma(2)}} \cdots x_N^{a_{\sigma(N)}}\right] f = f_{a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(N)}} = \left[x_1^{a_1} x_2^{a_2} \cdots x_N^{a_N}\right] (\sigma \cdot f)$$

(by (393), applied to $(b_1, b_2, \ldots, b_N) = (a_1, a_2, \ldots, a_N)$). This proves Proposition 7.2.9. □

B.7. Schur polynomials

Detailed proof of Lemma 7.3.14. Write the N-partitions λ and μ as $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ and $\mu = (\mu_1, \mu_2, \ldots, \mu_N)$. Then, the definition of $Y(\lambda/\mu)$ yields

$$Y(\lambda/\mu) = \{(i, j) \mid i \in [N] \text{ and } j \in \mathbb{Z} \text{ and } \mu_i < j \leq \lambda_i\} . \tag{394}$$

We know that (a, b) is an element of $Y(\lambda/\mu)$. Hence,

$$(a, b) \in Y(\lambda/\mu) = \{(i, j) \mid i \in [N] \text{ and } j \in \mathbb{Z} \text{ and } \mu_i < j \leq \lambda_i\} .$$

From this, we obtain $a \in [N]$ and $b \in \mathbb{Z}$ and $\mu_a < b \leq \lambda_a$.

We know that (e, f) is an element of $Y(\lambda/\mu)$. Hence,

$$(e, f) \in Y(\lambda/\mu) = \{(i, j) \mid i \in [N] \text{ and } j \in \mathbb{Z} \text{ and } \mu_i < j \leq \lambda_i\} .$$

From this, we obtain $e \in [N]$ and $f \in \mathbb{Z}$ and $\mu_e < f \leq \lambda_e$.

Now, from $a \leq c$, we obtain $c \geq a \geq 1$ (since $a \in [N]$). Also, we have $c \leq e \leq N$ (since $e \in [N]$). Combining this with $c \geq 1$, we obtain $1 \leq c \leq N$, so that $c \in [N]$ (since $c \in \mathbb{Z}$).

Now, $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_N$ (since μ is an N-partition). In other words, if u and v are two elements of $[N]$ satisfying $u \leq v$, then $\mu_u \geq \mu_v$. Applying this to $u = a$ and $v = c$, we obtain $\mu_a \geq \mu_c$ (since $a \leq c$). Hence, $\mu_c \leq \mu_a < b \leq d$.

Also, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ (since λ is an N-partition). In other words, if u and v are two elements of $[N]$ satisfying $u \leq v$, then $\lambda_u \geq \lambda_v$. Applying this to $u = c$ and $v = e$, we obtain $\lambda_c \geq \lambda_e$ (since $c \leq e$). Hence, $d \leq f \leq \lambda_e \leq \lambda_c$ (since $\lambda_c \geq \lambda_e$).

Combining this with $\mu_c < d$, we obtain $\mu_c < d \leq \lambda_c$.

Thus, we know that $c \in [N]$ and $d \in \mathbb{Z}$ and $\mu_c < d \leq \lambda_c$. In other words, $(c, d) \in \{(i, j) \mid i \in [N] \text{ and } j \in \mathbb{Z} \text{ and } \mu_i < j \leq \lambda_i\}$. In view of (394), this rewrites as $(c, d) \in Y(\lambda/\mu)$. This proves Lemma 7.3.14. □

Detailed proof of Lemma 7.3.17. We shall first prove parts **(a)** and **(c)**, and then quickly derive the rest from them.

(a) The skew tableau T is semistandard. Hence, we have

$$T(i,j) \leq T(i,j+1) \tag{395}$$

for any $(i,j) \in Y(\lambda/\mu)$ satisfying $(i,j+1) \in Y(\lambda/\mu)$. (Indeed, this is one of the requirements placed on T in Definition 7.3.16.)

Now, let (i,j_1) and (i,j_2) be two elements of $Y(\lambda/\mu)$ satisfying $j_1 \leq j_2$. We must prove that $T(i,j_1) \leq T(i,j_2)$.

Let $k \in \{j_1, j_1+1, \ldots, j_2-1\}$ be arbitrary. Then, $j_1 \leq k \leq j_2 - 1$. From $k \leq j_2 - 1$, we obtain $k+1 \leq j_2$, so that $k \leq k+1 \leq j_2$. Also, $j_1 \leq k \leq k+1$.

Thus, we have $i \leq i \leq i$ and $j_1 \leq k \leq j_2$. Hence, Lemma 7.3.14 (applied to $(a,b) = (i,j_1)$ and $(e,f) = (i,j_2)$ and $(c,d) = (i,k)$) yields $(i,k) \in Y(\lambda/\mu)$. Therefore, the entry $T(i,k)$ of T is well-defined.

Also, we have $i \leq i \leq i$ and $j_1 \leq k+1 \leq j_2$. Hence, Lemma 7.3.14 (applied to $(a,b) = (i,j_1)$ and $(e,f) = (i,j_2)$ and $(c,d) = (i,k+1)$) yields $(i,k+1) \in Y(\lambda/\mu)$. Therefore, the entry $T(i,k+1)$ of T is well-defined.

Now, (395) (applied to $j = k$) yields $T(i,k) \leq T(i,k+1)$ (since $(i,k) \in Y(\lambda/\mu)$ and $(i,k+1) \in Y(\lambda/\mu)$).

Forget that we fixed k. We thus have shown that for each $k \in \{j_1, j_1+1, \ldots, j_2-1\}$, the inequality $T(i,k) \leq T(i,k+1)$ holds (and both entries $T(i,k)$ and $T(i,k+1)$ are well-defined). In other words, we have

$$T(i,j_1) \leq T(i,j_1+1) \leq T(i,j_1+2) \leq \cdots \leq T(i,j_2-1) \leq T(i,j_2).$$

Hence, $T(i,j_1) \leq T(i,j_2)$. This proves Lemma 7.3.17 **(a)**.

(c) The skew tableau T is semistandard. Hence, we have

$$T(i,j) < T(i+1,j) \tag{396}$$

for any $(i,j) \in Y(\lambda/\mu)$ satisfying $(i+1,j) \in Y(\lambda/\mu)$. (Indeed, this is one of the requirements placed on T in Definition 7.3.16.)

Now, let (i_1,j) and (i_2,j) be two elements of $Y(\lambda/\mu)$ satisfying $i_1 < i_2$. We must prove that $T(i_1,j) < T(i_2,j)$.

Let $k \in \{i_1, i_1+1, \ldots, i_2-1\}$ be arbitrary. Then, $i_1 \leq k \leq i_2 - 1$. From $k \leq i_2 - 1$, we obtain $k+1 \leq i_2$, so that $k \leq k+1 \leq i_2$. Also, $i_1 \leq k \leq k+1$.

Thus, we have $i_1 \leq k \leq i_2$ and $j \leq j \leq j$. Hence, Lemma 7.3.14 (applied to $(a,b) = (i_1,j)$ and $(e,f) = (i_2,j)$ and $(c,d) = (k,j)$) yields $(k,j) \in Y(\lambda/\mu)$. Therefore, the entry $T(k,j)$ of T is well-defined.

Also, we have $i_1 \leq k+1 \leq i_2$ and $j \leq j \leq j$. Hence, Lemma 7.3.14 (applied to $(a,b) = (i_1,j)$ and $(e,f) = (i_2,j)$ and $(c,d) = (k+1,j)$) yields $(k+1,j) \in Y(\lambda/\mu)$. Therefore, the entry $T(k+1,j)$ of T is well-defined.

Now, (396) (applied to $i = k$) yields $T(k,j) < T(k+1,j)$ (since $(k,j) \in Y(\lambda/\mu)$ and $(k+1,j) \in Y(\lambda/\mu)$).

Forget that we fixed k. We thus have shown that for each $k \in \{i_1, i_1+1, \ldots, i_2-1\}$, the inequality $T(k,j) < T(k+1,j)$ holds (and both entries $T(k,j)$ and $T(k+1,j)$ are well-defined). In other words, we have

$$T(i_1,j) < T(i_1+1,j) < T(i_1+2,j) < \cdots < T(i_2-1,j) < T(i_2,j).$$

Hence, $T(i_1, j) < T(i_2, j)$ (since $i_1 < i_2$). This proves Lemma 7.3.17 **(c)**.

(b) Let (i_1, j) and (i_2, j) be two elements of $Y(\lambda/\mu)$ satisfying $i_1 \leq i_2$. We must prove that $T(i_1, j) \leq T(i_2, j)$. If $i_1 < i_2$, then this follows from Lemma 7.3.17 **(c)**. Hence, for the rest of this proof, we WLOG assume that we don't have $i_1 < i_2$. Thus, we have $i_1 \geq i_2$. Combining this with $i_1 \leq i_2$, we obtain $i_1 = i_2$. Thus, $T(i_1, j) = T(i_2, j)$, so that $T(i_1, j) \leq T(i_2, j)$. This proves Lemma 7.3.17 **(b)**.

(d) Let (i_1, j_1) and (i_2, j_2) be two elements of $Y(\lambda/\mu)$ satisfying $i_1 \leq i_2$ and $j_1 \leq j_2$. Then, $i_1 \leq i_2 \leq i_2$ and $j_1 \leq j_1 \leq j_2$. Hence, Lemma 7.3.14 (applied to $(a, b) = (i_1, j_1)$ and $(e, f) = (i_2, j_2)$ and $(c, d) = (i_2, j_1)$) yields $(i_2, j_1) \in Y(\lambda/\mu)$. Therefore, the entry $T(i_2, j_1)$ of T is well-defined. Hence, Lemma 7.3.17 **(b)** (applied to $j = j_1$) yields $T(i_1, j_1) \leq T(i_2, j_1)$. Furthermore, Lemma 7.3.17 **(a)** (applied to $i = i_2$) yields $T(i_2, j_1) \leq T(i_2, j_2)$. Thus,

$$T(i_1, j_1) \leq T(i_2, j_1) \leq T(i_2, j_2).$$

This proves Lemma 7.3.17 **(d)**.

(e) Let (i_1, j_1) and (i_2, j_2) be two elements of $Y(\lambda/\mu)$ satisfying $i_1 < i_2$ and $j_1 \leq j_2$. Then, $i_1 \leq i_2 \leq i_2$ and $j_1 \leq j_1 \leq j_2$. Hence, Lemma 7.3.14 (applied to $(a, b) = (i_1, j_1)$ and $(e, f) = (i_2, j_2)$ and $(c, d) = (i_2, j_1)$) yields $(i_2, j_1) \in Y(\lambda/\mu)$. Therefore, the entry $T(i_2, j_1)$ of T is well-defined. Hence, Lemma 7.3.17 **(c)** (applied to $j = j_1$) yields $T(i_1, j_1) < T(i_2, j_1)$. Furthermore, Lemma 7.3.17 **(a)** (applied to $i = i_2$) yields $T(i_2, j_1) \leq T(i_2, j_2)$. Thus,

$$T(i_1, j_1) < T(i_2, j_1) \leq T(i_2, j_2).$$

This proves Lemma 7.3.17 **(e)**. □

Detailed proof of Lemma 7.3.35. Let $(i, j) \in Y(\lambda)$. Set $p := T(i, j)$.

All entries of T are elements of $[N]$ (by the definition of a tableau), and thus are positive integers. Thus, in particular, the i entries $T(1, j), T(2, j), \ldots, T(i, j)$ are positive integers[169]. Moreover, the tableau T is semistandard; thus, its entries increase strictly down each column. Hence, in particular, we have

$$T(1, j) < T(2, j) < \cdots < T(i, j).$$

Thus, the i numbers $T(1, j), T(2, j), \ldots, T(i, j)$ are distinct. Moreover, all these numbers are positive integers (as we have seen above) and are $\leq p$ (since $T(1, j) < T(2, j) < \cdots < T(i, j) = p$); thus, they all belong to the set $[p]$. This shows that there are i distinct numbers in the set $[p]$ (namely, the i numbers $T(1, j), T(2, j), \ldots, T(i, j)$); in other words, the set $[p]$ has at least i elements. In other words, we have $|[p]| \geq i$. Since $|[p]| = p = T(i, j)$, this rewrites as $T(i, j) \geq i$. This proves Lemma 7.3.35. □

[169] Here, we are tacitly using the fact that the boxes $(1, j), (2, j), \ldots, (i, j)$ all belong to $Y(\lambda)$ (so that the corresponding entries $T(1, j), T(2, j), \ldots, T(i, j)$ are well-defined). This fact can be checked as follows: Let $u \in [i]$. Thus, $u \leq i$. Now, write λ in the form $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$. Thus, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ (since λ is an N-partition). Hence, $\lambda_u \geq \lambda_i$ (since $u \leq i$), so that $\lambda_i \leq \lambda_u$ and therefore $[\lambda_i] \subseteq [\lambda_u]$. However, $(i, j) \in Y(\lambda)$. In other words, $i \in [N]$ and $j \in [\lambda_i]$ (by the definition of the Young diagram $Y(\lambda)$). Hence, $u \leq i \leq N$ (since $i \in [N]$), so that $u \in [N]$, and furthermore $j \in [\lambda_i] \subseteq [\lambda_u]$. Now, from $u \in [N]$ and $j \in [\lambda_u]$, we obtain $(u, j) \in Y(\lambda)$. Forget that we fixed u. We thus have shown that $(u, j) \in Y(\lambda)$ for each $u \in [i]$. In other words, the boxes $(1, j), (2, j), \ldots, (i, j)$ all belong to $Y(\lambda)$, qed.

Detailed proof of Lemma 7.3.39. Write the N-tuple $\alpha \in \mathbb{N}^N$ as $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$. Then, Definition 7.3.2 **(b)** yields

$$a_\alpha = \det\left(\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}\right). \tag{397}$$

(a) Assume that the N-tuple α has two equal entries. In other words, the N-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ has two equal entries (since $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$). In other words, there exist two elements $u, v \in [N]$ such that $u < v$ and $\alpha_u = \alpha_v$. Consider these u, v. Now, from $\alpha_u = \alpha_v$, we conclude that the u-th and the v-th columns of the $N \times N$-matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ are equal. Hence, this $N \times N$-matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ has two equal columns (since $u < v$).

However, if an $N \times N$-matrix A has two equal columns, then $\det A = 0$ (by Theorem 6.4.14 **(c)**[170]). Applying this to $A = \left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$, we obtain

$$\det\left(\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}\right) = 0$$

(since the $N \times N$-matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ has two equal columns). In view of (397), this rewrites as $a_\alpha = 0$. This proves Lemma 7.3.39 **(a)**.

(b) Write the N-tuple $\beta \in \mathbb{N}^N$ as $\beta = (\beta_1, \beta_2, \ldots, \beta_N)$. Then, Definition 7.3.2 **(b)** yields

$$a_\beta = \det\left(\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}\right). \tag{398}$$

However, the N-tuple β is obtained from α by swapping two entries. In other words, the N-tuple $(\beta_1, \beta_2, \ldots, \beta_N)$ is obtained from $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ by swapping two entries (since $\beta = (\beta_1, \beta_2, \ldots, \beta_N)$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_N)$). Thus, the matrix $\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}$ is obtained from the matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ by swapping two columns[171].

However, if we swap two columns of an $N \times N$-matrix A, then $\det A$ gets multiplied by -1 (by Theorem 6.4.14 **(b)**[172]). In other words, if A and B are two $N \times N$-matrices such that B is obtained from A by swapping two columns, then $\det B = -\det A$. Applying this to $A = \left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ and $B = \left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}$, we obtain

$$\det\left(\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}\right) = -\det\left(\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}\right)$$

(since the $N \times N$-matrix $\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}$ is obtained from the matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ by swapping two columns). In view of (397) and (398), this rewrites as $a_\beta = -a_\alpha$. This proves Lemma 7.3.39 **(b)**. □

[170] more precisely: by the analogue of Theorem 6.4.12 **(c)** for columns instead of rows

[171] Indeed, if the N-tuple $(\beta_1, \beta_2, \ldots, \beta_N)$ is obtained from $(\alpha_1, \alpha_2, \ldots, \alpha_N)$ by swapping the u-th and the v-th entries, then the matrix $\left(x_i^{\beta_j}\right)_{1\le i\le N,\ 1\le j\le N}$ is obtained from the matrix $\left(x_i^{\alpha_j}\right)_{1\le i\le N,\ 1\le j\le N}$ by swapping the u-th and the v-th columns.

[172] more precisely: by the analogue of Theorem 6.4.12 **(b)** for columns instead of rows

Some details omitted from the proof of Lemma 7.3.34. In our above proof of Lemma 7.3.34, we have omitted certain arguments – namely, the proofs of the equalities (290) and (291) in the proof of Observation 2. Let us now show these proofs:[173]

[*Proof of (290):* The definition of $\operatorname{cont}(T^*)$ yields

$$\begin{aligned}
(\operatorname{cont}(T^*))_{k+1} &= (\text{\# of } (k+1)\text{'s in } T^*) \\
&= \left(\text{\# of } (k+1)\text{'s in } \underbrace{\operatorname{col}_{<j}(T^*)}_{\substack{=\beta_k(\operatorname{col}_{<j} T) \\ \text{(by (280))}}} \right) + \left(\text{\# of } (k+1)\text{'s in } \underbrace{\operatorname{col}_{\geq j}(T^*)}_{\substack{=\operatorname{col}_{\geq j} T \\ \text{(by (281))}}} \right) \\
&\qquad\qquad \left(\text{by (287), applied to } i = k+1\right) \\
&= \underbrace{\left(\text{\# of } (k+1)\text{'s in } \beta_k\left(\operatorname{col}_{<j} T\right)\right)}_{\substack{=\left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) \\ \text{(by (255),} \\ \text{applied to } \operatorname{col}_{<j} T \text{ instead of } T)}} + \underbrace{\left(\text{\# of } (k+1)\text{'s in } \operatorname{col}_{\geq j} T\right)}_{\substack{=b_{k+1}-\nu_{k+1} \\ \text{(by (285))}}} \\
&= \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + \underbrace{b_{k+1}}_{\substack{=b_k+1 \\ (\text{since } b_k+1=b_{k+1})}} - \nu_{k+1} \\
&= \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k + 1 - \nu_{k+1}.
\end{aligned}$$

However, $\gamma = \nu + \operatorname{cont}(T^*) + \rho$, so that

$$\begin{aligned}
\gamma_{k+1} &= (\nu + \operatorname{cont}(T^*) + \rho)_{k+1} \\
&= \nu_{k+1} + \underbrace{(\operatorname{cont}(T^*))_{k+1}}_{=\left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right)+b_k+1-\nu_{k+1}} + \underbrace{\rho_{k+1}}_{\substack{=N-(k+1) \\ \text{(by the definition of } \rho)}} \\
&= \nu_{k+1} + \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k + 1 - \nu_{k+1} + N - (k+1) \\
&= \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k + N - k. \qquad (399)
\end{aligned}$$

On the other hand, the definition of $\operatorname{cont} T$ yields

$$\begin{aligned}
(\operatorname{cont} T)_k &= (\text{\# of } k\text{'s in } T) \\
&= \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + \underbrace{\left(\text{\# of } k\text{'s in } \operatorname{col}_{\geq j} T\right)}_{\substack{=b_k-\nu_k \\ \text{(by (284))}}} \\
&\qquad\qquad \left(\text{by (286), applied to } i = k\right) \\
&= \left(\text{\# of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k - \nu_k.
\end{aligned}$$

[173] In both of these proofs, we will use the notations that were introduced in the proof of Observation 2 in the proof of Lemma 7.3.34.

However, $\alpha = \nu + \operatorname{cont} T + \rho$, so that

$$\begin{aligned}
\alpha_k &= \left(\nu + \operatorname{cont} T + \rho\right)_k \\
&= \nu_k + \underbrace{\left(\operatorname{cont} T\right)_k}_{=\left(\#\text{ of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k - \nu_k} + \underbrace{\rho_k}_{\substack{=N-k \\ \text{(by the definition of } \rho\text{)}}} \\
&= \nu_k + \left(\#\text{ of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k - \nu_k + N - k \\
&= \left(\#\text{ of } k\text{'s in } \operatorname{col}_{<j} T\right) + b_k + N - k.
\end{aligned}$$

Comparing this with (399), we obtain $\gamma_{k+1} = \alpha_k$. This proves (290).]

[*Proof of (291):* Let $i \in [N]$ be such that $i \neq k$ and $i \neq k+1$. We must prove that $\gamma_i = \alpha_i$.

The definition of $\operatorname{cont}(T^*)$ yields

$$\begin{aligned}
\left(\operatorname{cont}(T^*)\right)_i &= \left(\#\text{ of } i\text{'s in } T^*\right) \\
&= \left(\#\text{ of } i\text{'s in } \underbrace{\operatorname{col}_{<j}(T^*)}_{\substack{=\beta_k\left(\operatorname{col}_{<j} T\right) \\ \text{(by (280))}}}\right) + \left(\#\text{ of } i\text{'s in } \underbrace{\operatorname{col}_{\geq j}(T^*)}_{\substack{=\operatorname{col}_{\geq j} T \\ \text{(by (281))}}}\right) \qquad \text{(by (287))} \\
&= \underbrace{\left(\#\text{ of } i\text{'s in } \beta_k\left(\operatorname{col}_{<j} T\right)\right)}_{\substack{=\left(\#\text{ of } i\text{'s in } \operatorname{col}_{<j} T\right) \\ \text{(by (256),} \\ \text{applied to } \operatorname{col}_{<j} T \text{ instead of } T\text{)}}} + \left(\#\text{ of } i\text{'s in } \operatorname{col}_{\geq j} T\right) \\
&= \left(\#\text{ of } i\text{'s in } \operatorname{col}_{<j} T\right) + \left(\#\text{ of } i\text{'s in } \operatorname{col}_{\geq j} T\right).
\end{aligned}$$

On the other hand, the definition of $\operatorname{cont} T$ yields

$$\left(\operatorname{cont} T\right)_i = \left(\#\text{ of } i\text{'s in } T\right) = \left(\#\text{ of } i\text{'s in } \operatorname{col}_{<j} T\right) + \left(\#\text{ of } i\text{'s in } \operatorname{col}_{\geq j} T\right)$$

(by (286)). Comparing these two equalities, we obtain $\left(\operatorname{cont}(T^*)\right)_i = \left(\operatorname{cont} T\right)_i$.

However, $\gamma = \nu + \operatorname{cont}(T^*) + \rho$, so that

$$\gamma_i = \left(\nu + \operatorname{cont}(T^*) + \rho\right)_i = \nu_i + \underbrace{\left(\operatorname{cont}(T^*)\right)_i}_{=\left(\operatorname{cont} T\right)_i} + \rho_i = \nu_i + \left(\operatorname{cont} T\right)_i + \rho_i.$$

However, $\alpha = \nu + \operatorname{cont} T + \rho$, so that

$$\alpha_i = \left(\nu + \operatorname{cont} T + \rho\right)_i = \nu_i + \left(\operatorname{cont} T\right)_i + \rho_i.$$

Comparing these two equalities, we obtain $\gamma_i = \alpha_i$. This proves (291).] □

References

[17f-hw7s] Darij Grinberg, *UMN Fall 2017 Math 4990 homework set #7 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/17f/hw7os.pdf`

[18f-hw2s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #2 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw2s.pdf`

[18f-hw4s] Darij Grinberg, *UMN Fall 2018 Math 5705 homework set #4 with solutions*, `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw4s.pdf`

[18f-hw4se] Jacob Elafandi, *Math 5705: Enumerative Combinatorics, Fall 2018: Homework 4: solutions to exercises 1, 2, 3, 7.* `http://www.cip.ifi.lmu.de/~grinberg/t/18f/hw4s-elafandi.pdf`

[18f-mt3s] Darij Grinberg, *Math 5705: Enumerative Combinatorics, Fall 2018: Midterm 3 with solutions.* `https://www.cip.ifi.lmu.de/~grinberg/t/18f/mt3s.pdf`

[19fla] Darij Grinberg, *Math 201-003: Linear Algebra, Fall 2019.* `http://www.cip.ifi.lmu.de/~grinberg/t/19fla/`

[19s] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019. `http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`

[19s-mt3s] Darij Grinberg, *Math 4281: Introduction to Modern Algebra, Spring 2019: Midterm 3 with solutions.* `https://www.cip.ifi.lmu.de/~grinberg/t/19s/mt3s.pdf`

[19fco] Darij Grinberg, *Enumerative Combinatorics: class notes (Drexel Fall 2019 Math 222 notes)*, 11 September 2022. `http://www.cip.ifi.lmu.de/~grinberg/t/19fco/n/n.pdf`

[20f] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 22 March 2021. `http://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`

[21w] Darij Grinberg, *Math 533: Abstract Algebra I, Winter 2021*, March 2021. `http://www.cip.ifi.lmu.de/~grinberg/t/21w/index.html`

[Aigner07] Martin Aigner, *A Course in Enumeration*, Graduate Texts in Mathematics #238, Springer 2007.

[AndEri04] George E. Andrews, Kimmo Eriksson, *Integer Partitions*, Cambridge University Press 2004.

[AndFen04] Titu Andreescu, Zuming Feng, *A Path to Combinatorics for Undergraduates: Counting Strategies*, Springer 2004.

[Andrew16] George E. Andrews, *Euler's Partition Identity – Finite Version*, 2016. `http://www.personal.psu.edu/gea1/pdf/317.pdf`

[ApaKau13] Ainhoa Aparicio Monforte, Manuel Kauers, *Formal Laurent series in several variables*, Expositiones Mathematicae, **31**(4), pp. 350–367.

[Armstr19] Drew Armstrong, *Abstract Algebra I (Fall 2018) and Abstract Algebra II (Spring 2019) lecture notes*, 2019.
`https://www.math.miami.edu/~armstrong/561fa18.php`
`https://www.math.miami.edu/~armstrong/562sp19.php`

[Artin10] Michael Artin, *Algebra*, 2nd edition, Pearson 2010.

[Bell06] Jordan Bell, *Euler and the pentagonal number theorem*, arXiv:math/0510054v2.

[BenQui03] Arthur T. Benjamin and Jennifer J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, The Mathematical Association of America, 2003.

[BenQui04] Arthur T. Benjamin and Jennifer J. Quinn, *Proofs that Really Count: The Magic of Fibonacci Numbers and More*, Mathematical Adventures for Students and Amateurs, (David F. Hayes and Tatiana Shubin, editors), Spectrum Series of MAA, pp. 83–98, 2004.

[BenQui08] Arthur T. Benjamin and Jennifer J. Quinn, *An Alternate Approach to Alternating Sums: A Method to DIE for*, The College Mathematics Journal, Volume 39, Number 3, May 2008, pp. 191-202(12).

[Berndt06] Bruce C. Berndt, *Number Theory in the Spirit of Ramanujan*, Student Mathematical Library #34, AMS 2006.
See `https://faculty.math.illinois.edu/~berndt/spiritcorrections.pdf` for errata.

[Berndt17] Bruce C. Berndt, *Spring 2017, MATH 595. Theory of Partitions*, lecture notes, 2017.
`https://conf.math.illinois.edu/~berndt/math595-tp.html`

[BjoBre05] Anders Bjorner, Francesco Brenti, *Combinatorics of Coxeter Groups*, Springer 2005.
See `https://www.mat.uniroma2.it/~brenti/correct.ps` for errata.

[Bona12] Miklos Bóna, *Combinatorics of Permutations*, 2nd edition, Taylor&Francis 2012.
`https://doi.org/10.1201/b12210`

[Bourba02] Nicolas Bourbaki, *Lie Groups and Lie Algebras: Chapters 4–6*, Springer 2002.

[Bourba03] Nicolas Bourbaki, *Algebra II: Chapters 4–7*, Springer 2003.

[Bourba68] Nicolas Bourbaki, *Theory of Sets*, Springer 1968.

[Bourba74] Nicolas Bourbaki, *Algebra I: Chapters 1–3*, Addison-Wesley 1974.

[Brande14] Petter Brändén, *Unimodality, log-concavity, real-rootedness and beyond*, arXiv:1410.6601v1.

[Bresso99] David M. Bressoud, *Proofs and Confirmations: The Story of the Alternating Sign Matrix Conjecture*, Cambridge University Press 1999.
See `https://www.macalester.edu/~bressoud/books/PnC/PnCcorrect.html` for errata.

[Brewer14] Thomas S. Brewer, *Algebraic properties of formal power series composition*, PhD thesis at University of Kentucky, 2014.
`https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1021&context=math_etds`

[BruSch83] Richard A. Brualdi and Hans Schneider, *Determinantal Identities: Gauss, Schur, Cauchy, Sylvester, Kronecker, Jacobi, Binet, Laplace, Muir, and Cayley*, Linear Algebra and its Applications **52–53**, July 1983, pp. 769–791.

[Camero16] Peter J. Cameron, *Combinatorics 1: The art of counting (vol. 1 of St Andrews Notes on Advanced Combinatorics)*, 28 March 2016, `https://cameroncounts.wordpress.com/lecture-notes/` .
See `http://www.cip.ifi.lmu.de/~grinberg/algebra/acnotes1-errata.pdf` for corrections.

[Cohen08] Arjeh M. Cohen, *Coxeter groups: Notes of a MasterMath course, Fall 2007*, January 24, 2008.
`http://arpeg.nl/wp-content/uploads/2016/01/CoxNotes.pdf`

[Cohn04] Henry Cohn, *Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients*, American Mathematical Monthly **111** (2004), pp. 487–495, arXiv:math/0407093v1.

[Comtet74] Louis Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, D. Reidel Publishing Company, 1974.

[Conrad-UI] Keith Conrad, *Universal identities*, 13 February 2021.
`https://kconrad.math.uconn.edu/blurbs/linmultialg/univid.pdf`

[Dodgso67] Charles L. Dodgson, *Elementary Treatise on Determinants with their Applications to simultaneous linear equations and algebraical geometry*, Macmillan 1867.

[Doyle19] Peter G. Doyle, *Frobenius's last proof*, arXiv:1904.06573v1. See `http://www.cip.ifi.lmu.de/~grinberg/algebra/doyle-frob-errata.pdf` for corrections.

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004. ISBN: 978-0-471-43334-7.
See `http://www.cems.uvm.edu/~rfoote/errata_3rd_edition.pdf` for errata.

[EdeStr04] Alan Edelman and Gilbert Strang, *Pascal Matrices*, American Mathematical Monthly, Vol. 111, No. 3 (March 2004), pp. 189–197.

[Edward05] Harold M. Edwards, *Essays in Constructive Mathematics*, Springer 2005.

[Egge19] Eric S. Egge, *An Introduction to Symmetric Functions and Their Combinatorics*, AMS 2019.
See `https://www.ericegge.net/cofsf/index.html` for corrections and addenda.

[EGHetc11] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, Elena Yudovina, *Introduction to Representation Theory*, with historical interludes by Slava Gerovitch, Student Mathematical Library **59**, AMS 2011, updated version 2018.

[Erdos42] P. Erdös, *On an elementary proof of some asymptotic formulas in the theory of partitions*, Annals of Mathematics **43** (1942), pp. 437–450.

[Euler48] Leonhard Euler, *Introductio in analysin infinitorum, tomus 1*, Lausannæ 1748.

[Fink17] Alex Fink, *Enumerative Combinatorics*, module taught at the London Taught Course Centre, 2017.
`http://www.maths.qmul.ac.uk/~fink/enumcombi/`

[FoaHan04] Dominique Foata, Guo-Niu Han, *The q-series in combinatorics; permutation statistics*, preliminary version, 5 May 2011.
`https://irma.math.unistra.fr/~guoniu/papers/p56lectnotes2.pdf`

[Ford21] Timothy J. Ford, *Abstract Algebra*, draft of a book, 10 October 2021.
`http://math.fau.edu/ford/preprints/Algebra_Book/Algebra_Book.pdf`

[Fulton97] William Fulton, *Young Tableaux, With Applications to Representation Theory and Geometry*, London Mathematical Society Student Texts **35**, Cambridge University Press 1997.

[GaiGup77] P. Gaiha, S. K. Gupta, *Adjacent Vertices on a Permutohedron*, SIAM Journal on Applied Mathematics **32**(2), pp. 323–327.

[Galvin17] David Galvin, *Basic discrete mathematics*, 13 December 2017.
`http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf`
(The URL might change, and the text may get updated. In order to reliably obtain the version of 13 December 2017, you can use the archive.org Wayback Machine: `https://web.archive.org/web/20180205122609/http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf` .)

[Gashar98] Vesselin Gasharov, *A Short Proof of the Littlewood–Richardson Rule*, Europ. J. Combinatorics (1998) **19**, pp. 451–453.

[Gauss08] Carl Friedrich Gauß, *Summatio quarumdam serierum singularium*, Comm. soc. reg. sci. Gottingensis rec. **1** (1811).

[Gauss16] C. F. Gauss, *Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse*, Comm. Recentiores **3** (1816), pp. 107–142.

[GesVie85] Ira Gessel, Gérard Viennot, *Binomial Determinants, Paths, and Hook Length Formulae*, Advances in Mathematics **58** (1985), pp. 300-321.

[GesVie89] Ira M. Gessel, X. G. Viennot, *Determinants, Paths, and Plane Partitions*, 1989 preprint.
`https://peeps.unet.brandeis.edu/~gessel/homepage/papers/pp.pdf`

[Godsil06] Chris Godsil, *Lecture Notes on Combinatorics*, version 5 December 2006.
`https://web.archive.org/web/20070824060559/http://www.math.uwaterloo.ca/~dgwagner/MATH249/enum.pdf`

[Goodma15] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 1 May 2015.
`http://homepage.math.uiowa.edu/~goodman/algebrabook.dir/book.2.6.pdf` .

[GouJac83] I. P. Goulden, D. M. Jackson, *Combinatorial Enumeration*, John Wiley & Sons 1983, reprinted by Dover 2004.

[Grinbe09] Darij Grinberg, *Solution to Problem 19.9 from "Problems from the Book"*.
http://www.cip.ifi.lmu.de/~grinberg/solutions.html

[Grinbe10] Darij Grinberg, *A hyperfactorial divisibility*, version of 27 July 2015.
http://www.cip.ifi.lmu.de/~grinberg/

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 25 May 2021.
http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2019-01-10 or arXiv:2008.09862v2.

[Grinbe17] Darij Grinberg, *Why the log and exp series are mutually inverse*, 11 May 2018.
https://www.cip.ifi.lmu.de/~grinberg/t/17f/logexp.pdf

[Grinbe18] Darij Grinberg, *The diamond lemma and its applications (talk)*, 20 May 2018.
https://www.cip.ifi.lmu.de/~grinberg/algebra/diamond-talk.pdf

[Grinbe19] Darij Grinberg, *The trace Cayley-Hamilton theorem*, 14 July 2019.
https://www.cip.ifi.lmu.de/~grinberg/algebra/trach.pdf

[Grinbe20] Darij Grinberg, *Alternierende Summen: Aufgaben und Lösungen*, 7 June 2021.
https://www.cip.ifi.lmu.de/~grinberg/algebra/aimo2020-altsum-lsg.pdf

[Grinbe21] Darij Grinberg, *Regular elements of a ring, monic polynomials and "lcm-coprimality"*, 22 May 2021.
https://www.cip.ifi.lmu.de/~grinberg/algebra/regpol.pdf

[GriRei20] Darij Grinberg, Victor Reiner, *Hopf algebras in Combinatorics*, version of 27 July 2020, arXiv:1409.8356v7.
See also http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf for a version that gets updated.

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See https://www-cs-faculty.stanford.edu/~knuth/gkp.html for errata.

[Guicha20] David Guichard, *An Introduction to Combinatorics and Graph Theory*, 23 April 2021.
https://www.whitman.edu/mathematics/cgt_online/book/

[Hellel08] Geir T. Helleloid, *Algebraic Combinatorics*, 11 November 2008.
http://libgen.rs/book/index.php?md5=421E2DABBCD43E900BC280AF5A122FE6

[Henric74] Peter Henrici, *Applied and Computational Complex Analysis, volume 1*, Wiley 1974.

[Hirsch17] Michael D. Hirschhorn, *The Power of q: A Personal Journey*, Springer 2017.
See https://link.springer.com/chapter/10.1007/978-3-319-57762-3_44 for errata.

[Hirsch87] Michael D. Hirschhorn, *A simple proof of Jacobi's four-square theorem*, Proceedings of the American Mathematical Society **101** (1987), pp. 436–438.

[Hopkin17] Sam Hopkins, *RSK via local transformations*, 17 May 2017.
http://www-users.math.umn.edu/~shopkins/docs/rsk.pdf

[Johnso20] Warren Pierstorff Johnson, *Introduction to q-analysis*, American Mathematical Society 2020.

[Joyner08] W. D. Joyner, *Mathematics of the Rubik's cube*, 19 August 2008.
https://web.archive.org/web/20160304122348/http://www.permutationpuzzles.org/rubik/webnotes/ (link to the PDF at the bottom).

[KacChe02] Victor Kac, Pokman Cheung, *Quantum Calculus*, Springer 2002.

[Kitaev11] Sergey Kitaev, *Patterns in Permutations and Words*, Springer 2011.

[KlaPol79] David Klarner, Jordan Pollack, *Domino tilings of rectangles with fixed width*, Discrete Mathematics, **32**(1), pp. 45–52.

[KliSch97] Anatoli Klimyk, Konrad Schmüdgen, *Quantum groups and their representations*, Springer 1997.

[Knapp16] Anthony W. Knapp, *Basic Algebra*, Digital Second Editions By Anthony W. Knapp, 2017, http://www.math.stonybrook.edu/~aknapp/download.html .

[Knuth1] Donald Ervin Knuth, *The Art of Computer Programming, volume 1: Fundamental Algorithms*, 3rd edition, Addison–Wesley 1997.
See https://www-cs-faculty.stanford.edu/~knuth/taocp.html for errata.

[Knuth2] Donald Ervin Knuth, *The Art of Computer Programming, volume 2: Seminumerical Algorithms*, 3rd edition, Addison–Wesley 1998.
See `https://www-cs-faculty.stanford.edu/~knuth/taocp.html` for errata.

[Knuth3] Donald Ervin Knuth, *The Art of Computer Programming, volume 3: Sorting and Searching*, 2nd edition, Addison–Wesley 1998.
See `https://www-cs-faculty.stanford.edu/~knuth/taocp.html` for errata.

[Koch16] Dick Koch, *The Pentagonal Number Theorem and All That*, 26 August 2016.
`https://darkwing.uoregon.edu/~koch/PentagonalNumbers.pdf`

[KraPro10] Hanspeter Kraft, Claudio Procesi, *Classical invariant theory: A primer*, July 1996.
`https://kraftadmin.wixsite.com/hpkraft`
See `http://www.cip.ifi.lmu.de/~grinberg/algebra/KP-errata-web.pdf` for unofficial errata.

[Kratte17] Christian Krattenthaler, *Lattice Path Enumeration*, arXiv:1503.05930v3, published in: Handbook of Enumerative Combinatorics, M. Bóna (ed.), Discrete Math. and Its Appl., CRC Press, Boca Raton-London-New York, 2015, pp. 589–678.
`https://arxiv.org/abs/1503.05930v3`

[Kratte99] Christian Krattenthaler, *Advanced Determinant Calculus*, Séminaire Lotharingien Combin. 42 (1999) (The Andrews Festschrift), paper B42q, 67 pp., arXiv:math/9902004v3.

[Krishn86] V. Krishnamurthy, *Combinatorics: Theory and Applications*, Ellis Horwood Ltd. 1986.

[Krob95] Daniel Krob, *Eléments de combinatoire*, version 1.0, 1995.
`http://krob.cesames.net/IMG/ps/combi.ps`

[Lando03] Sergei K. Lando, *Lectures on Generating Functions*, Student Mathematical Library **23**, AMS 2003.

[Laue15] Hartmut Laue, *Determinants*, version 17 May 2015,
`http://www.math.uni-kiel.de/algebra/laue/homepagetexte/det.pdf` .

[LLPT95] D. Laksov, A. Lascoux, P. Pragacz, and A. Thorup, *The LLPT Notes*, edited by A. Thorup, 28 March 2018,
`http://web.math.ku.dk/noter/filer/sympol.pdf` .

[Loehr11] Nicholas A. Loehr, *Bijective Combinatorics*, Chapman & Hall/CRC 2011.

[Macdon95] Ian G. Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford Mathematical Monographs, 2nd edition, Oxford Science Publications 1995.

[Martin13] Jeremy L. Martin, *Counting Dyck Paths*, 11 September 2013.
`https://jlmartin.ku.edu/~jlmartin/courses/math724-F13/count-dyck.pdf`

[Martin21] Jeremy L. Martin, *Lecture Notes on Algebraic Combinatorics*, 12 March 2021.
`https://jlmartin.ku.edu/LectureNotes.pdf`

[MiRiRu87] Ray Mines, Fred Richman, Wim Ruitenburg, *A Course in Constructive Algebra*, Springer 1988.

[Muir30] Thomas Muir, *The theory of determinants in the historical order of development*, 5 volumes (1906–1930), later reprinted by Dover.
`http://www-igm.univ-mlv.fr/~al/`

[MuiMet60] Thomas Muir, *A Treatise on the Theory of Determinants*, revised and enlarged by William H. Metzler, Dover 1960.

[Mulhol21] Jamie Mulholland, *Permutation Puzzles: A Mathematical Perspective*, 12 January 2021.
`http://www.sfu.ca/~jtmulhol/math302/notes/permutation-puzzles-book.pdf`

[Ness61] Wilhelm Ness, *Proben aus der elementaren additiven Zahlentheorie*, Otto Salle Verlag, Frankfurt am Main / Hamburg 1961.

[Newste19] Clive Newstead, *An Infinite Descent into Pure Mathematics*, version 0.4, 1 January 2020.
`https://infinitedescent.xyz`

[Niven69] Ivan Niven, *Formal Power Series*, The American Mathematical Monthly **76**, No. 8 (Oct., 1969), pp. 871–889.
`https://www.maa.org/programs/maa-awards/writing-awards/formal-power-series`

[OlvSha18] Peter J. Olver, Chehrzad Shakiban, *Applied Linear Algebra*, 2nd edition, Springer 2018.
`https://doi.org/10.1007/978-3-319-91041-3`
See `http://www.math.umn.edu/~olver/ala.html` for errata.

[Pak06] Igor Pak, *Partition bijections, a survey*, Ramanujan J **12** (2006), pp. 5–75.
See `https://www.math.ucla.edu/~pak/papers/research.htm` for a preprint and updates.

[Prasad15] Amritanshu Prasad, *Representation Theory: A Combinatorial Viewpoint*, Cambridge University Press 2015.

[Prasol94] Viktor V. Prasolov, *Problems and Theorems in Linear Algebra*, Translations of Mathematical Monographs, vol. #134, AMS 1994.

[Proces07] Claudio Procesi, *Lie Groups: An Approach through Invariants and Representations*, Springer 2007.

[Quinla21] Rachel Quinlan, *MA3343 Groups, Semester 2020-2021*,
`http://www.maths.nuigalway.ie/~rquinlan/groups/`

[Robins05] Donald W. Robinson, *The classical adjoint*, Linear Algebra and its Applications **411** (2005), pp. 254–276.

[Sagan01] Bruce Sagan, *The Symmetric Group*, Graduate Texts in Mathematics **203**, 2nd edition 2001.
`https://doi.org/10.1007/978-1-4757-6804-6`
See `https://users.math.msu.edu/users/bsagan/Books/Sym/errata.pdf` for errata.

[Sagan19] Bruce Sagan, *Combinatorics: The Art of Counting*, Graduate Studies in Mathematics **210**, 21 September 2020.
`https://users.math.msu.edu/users/bsagan/Books/Aoc/final.pdf`
See `https://users.math.msu.edu/users/bsagan/Books/Aoc/errata.pdf` for errata.

[Sam19] Steven V. Sam, *Notes for Math 184: Combinatorics*, 9 December 2019.
`https://math.ucsd.edu/~ssam/old/19F-184/notes.pdf`

[Sam21] Steven V. Sam, *Notes for Math 188: Algebraic Combinatorics*, 17 May 2021.
`https://math.ucsd.edu/~ssam/188/notes-188.pdf`

[Sambal22] Benjamin Sambale, *An invitation to formal power series*, arXiv:2205.00879v2.

[Savage22] Alistair Savage, *Symmetric Functions*, lecture notes, 2 May 2022.
`https://alistairsavage.ca/symfunc/notes/Savage-SymmetricFunctions.pdf`

[Schwar16] Rich Schwartz, *The Cauchy-Binet Theorem*, 9 February 2016.
`https://www.math.brown.edu/reschwar/M123/cauchy.pdf`

[Smid09] Vita Smid, *Inclusion-Exclusion Principle: Proof by Mathematical Induction*, 2 December 2009.
`https://faculty.math.illinois.edu/~nirobles/files453/iep_proof.pdf`

[Spivey19] Michael Z. Spivey, *The Art of Proving Binomial Identities*, CRC Press 2019.
See `https://mathcs.pugetsound.edu/~mspivey/Errata.html` for errata.

[Stanko94] Zvezdelina E. Stankova, *Forbidden subsequences*, Discrete Mathematics **132** (1994), pp. 291–316.

[Stanle11] Richard P. Stanley, *Enumerative Combinatorics, volume 1*, Second edition, version of 15 July 2011. Available at `http://math.mit.edu/~rstan/ec/` .
See `http://math.mit.edu/~rstan/ec/` for errata.

[Stanle01] Richard P. Stanley, *Enumerative Combinatorics, volume 2*, First edition, Cambridge University Press 2001.
See `http://math.mit.edu/~rstan/ec/` for errata.

[Stanle15] Richard P. Stanley, *Catalan Numbers*, 1st edition 2015.
See `http://math.mit.edu/~rstan/catalan/` for errata.

[Stanle18] Richard P. Stanley, *Algebraic Combinatorics: Walks, Trees, Tableaux, and More*, 2nd edition, Springer 2018.
See `http://www-math.mit.edu/~rstan/algcomb/index.html` for errata.

[Stanle89] Richard P. Stanley, *Log-Concave and Unimodal Sequences in Algebra, Combinatorics, and Geometry*, Annals of the New York Academy of Sciences, **576** (1 Graph Theory), pp. 500–535.

[Stembr02] John R. Stembridge, *A Concise Proof of the Littlewood-Richardson Rule*, Electronic Journal of Combinatorics **9** (2002), #N5.

[Strick13] Neil Strickland, *MAS201 Linear Mathematics for Applications*, lecture notes, 28 September 2013.
`http://neil-strickland.staff.shef.ac.uk/courses/MAS201/`
See `http://www.cip.ifi.lmu.de/~grinberg/t/19fla/MAS201.pdf` for an updated version of the lecture notes.

[Strick20] Neil Strickland, *MAS334 Combinatorics*, lecture notes and solutions, 6 December 2020.
`http://neil-strickland.staff.shef.ac.uk/courses/MAS334/`

[Stucky15] Eric Stucky, *An Exposition of Kasteleyn's Solution of the Dimer Model*, senior thesis at Harvey Mudd College, 2015.
`https://scholarship.claremont.edu/hmc_theses/89/`

[Tignol16] Jean-Pierre Tignol, *Galois' Theory of Algebraic Equations*, 2nd edition, World Scientific 2016.

[Uecker17] Torsten Ueckerdt, *Lecture Notes Combinatorics (2017)*, 30 May 2017.
`http://www.math.kit.edu/iag6/lehre/combinatorics2017s/media/script.pdf`
See `http://www.cip.ifi.lmu.de/~grinberg/algebra/ueckerdt-script2017-errata.pdf` for an inofficial list of errata.

[Vorobi02] Nicolai N. Vorobiev, *Fibonacci Numbers*, Translated from the Russian by Mircea Martin, Springer 2002 (translation of the 6th Russian edition).

[Wagner05] Carl G. Wagner, *Basic Combinatorics*, 14 February 2005.
`http://www.math.utk.edu/~wagner/papers/comb.pdf`

[Wagner08] David G. Wagner, *C&O 330: Introduction to Combinatorial Enumeration*, version 9 August 2008.
`https://web.archive.org/web/20110124001354/http://www.math.uwaterloo.ca/~dgwagner/MATH249/co330.pdf`

[Wagner17] Stephan Wagner, *Combinatorics*, 19 June 2017.
`http://math.sun.ac.za/~swagner/NotesComb.pdf`

[Wagner20] Carl G. Wagner, *A First Course in Enumerative Combinatorics*, Pure and Applied Undergraduate Texts **49**, AMS 2020.

[White10] Dennis White, *Math 4707: Inclusion-Exclusion and Derangements*, 18 October 2010.
`http://www-users.math.umn.edu/~reiner/Classes/Derangements.pdf`

[Wildon19] Mark Wildon, *Introduction to Combinatorics*, 14 September 2020.
`http://www.ma.rhul.ac.uk/~uvah099/Maths/CombinatoricsWeb.pdf`

[Wildon20] Mark Wildon, *An involutive introduction to symmetric functions*, 8 May 2020.
`http://www.ma.rhul.ac.uk/~uvah099/Maths/Sym/SymFuncs2020.`

pdf
See http://www.cip.ifi.lmu.de/~grinberg/algebra/symfuncs2017-2020-05-08-errata.pdf for an inofficial list of errata.

[Wilf04] Herbert S. Wilf, *generatingfunctionology*, 2nd edition 2004.
https://www.math.upenn.edu/~wilf/DownldGF.html

[Wilf09] Herbert S. Wilf, *Lectures on Integer Partitions*, 2009.
https://www.math.upenn.edu/~wilf/PIMS/PIMSLectures.pdf

[Zabroc03] Mike Zabrocki, *F. Franklin's proof of Euler's pentagonal number theorem*, 28 February 2003.
https://garsia.math.yorku.ca/~zabrocki/math4160w03/eulerpnt.pdf

[Zeilbe85] Doron Zeilberger, *A combinatorial approach to matrix algebra*, Discrete Mathematics 56 (1985), pp. 61–72.

[Zeilbe98] Doron Zeilberger, *Dodgson's Determinant-Evaluation Rule proved by Two-Timing Men and Women*, The Electronic Journal of Combinatorics, vol. 4, issue 2 (1997) (The Wilf Festschrift volume), R22.
http://www.combinatorics.org/ojs/index.php/eljc/article/view/v4i2r22
Also available as arXiv:math/9808079v1.
http://arxiv.org/abs/math/9808079v1

[Zelevi81] A. V. Zelevinsky, *A generalization of the Littlewood–Richardson rule and the Robinson–Schensted–Knuth correspondence*, J. Algebra **69** (1981), pp. 82–94.

[Zeng93] Jiang Zeng, *A bijective proof of Muir's identity and the Cauchy-Binet formula*, Linear Algebra and its Applications **184**, 15 April 1993, pp. 79–82.