Math 531 Winter 2024: lecture diary

Darij Grinberg

draft, March 15, 2024

(This is **NOT** a text or a set of notes. It is just an archive of what I write on my virtual blackboard in class. See `https://www.cip.ifi.lmu.de/~grinberg/t/21s/lecs.pdf` for the actual notes.)

0. Preface

This is a course on **algebraic combinatorics**. One way to view this subject is as a continuation of combinatorics with algebraic means; another is as the "concrete side" of algebra. Example: The Schur functions are generating functions for semistandard tableaux (a combinatorial object), but also representatives for several abstract algebraic objects (representations of symmetric groups, polynomial functors, representations of general linear groups, cohomology classes of the Grassmannian), and they are quotients of certain determinants.

Prerequisites: some abstract algebra (polynomials, rings and fields ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p$, polynomial rings); some basic enumerative combinatorics.

0.1. Notations and basic facts

$\mathbb{N} := \{0, 1, 2, 3, \ldots\}$ means the set of nonnegative integers.

$|A|$ means the size of a set A.

The following basic facts from enumerative combinatorics will be used:

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

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

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

- A set with n elements has 2^n subsets, and has $\dbinom{n}{k}$ subsets of a given size k.

- A set with n elements has $n!$ permutations (= bijective maps from the 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 in choice 1,
  - then you have a_2 options in choice 2 (no matter what you chose in choice 1),
  - then you have a_3 options in choice 3 (no matter the previous choices you made),

- ....

Then, the total # of ways to make all n choices is $a_1 a_2 \cdots a_n$.

(Formally this is explained and proved in [Newstead], cited in the notes.)

A few words about binomial coefficients are in order:

Definition 0.1.1. For any numbers n and k, we set

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

Note that "numbers" can mean any reasonable sense of numbers here, e.g., complex numbers (really, any elements of any $\mathbb{Q}$-algebra).

Example 0.1.2. For any $k \in \mathbb{N}$, we have

$$\binom{-1}{k} = \frac{(-1)(-2)\cdots(-1-k+1)}{k!} = \frac{(-1)(-2)\cdots(-k)}{k!}$$
$$= (-1)^k \cdot \underbrace{\frac{1 \cdot 2 \cdot \cdots \cdot k}{k!}}_{=1} = (-1)^k.$$

If $n, k \in \mathbb{N}$ are such that $n \geq k$, then

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

But this formula only applies when $n, k \in \mathbb{N}$ and $n \geq k$, whereas our definition is far more general. The combinatorial meaning of $\binom{n}{k}$ (as the # of k-element subsets of an n-element set) holds whenever $n \in \mathbb{N}$, but again does does not hold for negative n.

Example 0.1.3. Let $n \in \mathbb{N}$. Then, $\binom{2n}{n} = \dfrac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2^n$.

Proof. Little exercise (or see the notes). □

Whole books have been written entirely about binomial coefficients (see the notes for references). This course is not really about them, but we will encounter them over and over. Here are three basic properties we will need:

- **Pascal's identity** aka **recurrence of the binomial coefficients (BCs):** For any numbers n and k, we have
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

- If $n, k \in \mathbb{N}$ satisfy $n < k$, then
$$\binom{n}{k} = 0.$$
(Warning: This is not true if $n \notin \mathbb{N}$. For example, $\dbinom{1.5}{3} = \dfrac{1.5 \cdot 0.5 \cdot (-0.5)}{3!} \neq 0$.)

- **Symmetry of binomial coefficients:** Let $n \in \mathbb{N}$ and $k \in \mathbb{R}$. Then,
$$\binom{n}{k} = \binom{n}{n-k}.$$
(Warning: This is false for negative n. For instance, $\dbinom{-1}{0} = 1$ but $\dbinom{-1}{-1} = 0$.)

1. Generating functions

In this first chapter, we will study generating functions: first informally (today), then on a rigorous footing. ("A generating function is a clothesline on which you can hang your numbers." – Wilf, I believe.)

1.1. Examples

Let me first show what can be done with generating functions and why they are useful. This will be informal, and we will make several "leaps of faith". We will later make these arguments rigorous.

The **idea** behind a generating function is simple: Any sequence $(a_0, a_1, a_2, \ldots)$ of numbers gives rise to a "power series" $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$, which is called the **generating function** of the sequence. This "power series" is to be understood as a formal object; we don't care about its convergence yet. Before we make this fully rigorous, let us play around with such series and try to get something useful out of them.

1.1.1. 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

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

Its entries are known as the **Fibonacci numbers**. Here is a table:

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 from 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

$$\begin{aligned} F(x) &= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots \\ &= \underbrace{0 + 1x}_{=x} + (f_1 + f_0) x^2 + (f_2 + f_1) x^3 + (f_3 + f_2) x^4 + \cdots \\ &= x + (f_1 + f_0) x^2 + (f_2 + f_1) x^3 + (f_3 + f_2) x^4 + \cdots \\ &= x + \underbrace{\left(f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{\substack{=\left(f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right) - f_0 x \\ = f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots}} + \left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right) \\ &= x + \underbrace{\left(f_0 x + f_1 x^2 + f_2 x^3 + f_3 x^4 + \cdots\right)}_{\substack{= x \cdot \left(f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots\right) \\ = x \cdot F(x)}} + \underbrace{\left(f_0 x^2 + f_1 x^3 + f_2 x^4 + \cdots\right)}_{\substack{= x^2 \cdot \left(f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots\right) \\ = x^2 \cdot F(x)}} \\ &= x + x \cdot F(x) + x^2 \cdot F(x) = x + \left(x + x^2\right) \cdot F(x) . \end{aligned}$$

This is a linear equation in $F(x)$. Solving it, we find

$$F(x) = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \phi x)(1 - \psi x)},$$

where $\phi = \dfrac{1 + \sqrt{5}}{2}$ and $\psi = \dfrac{1 - \sqrt{5}}{2}$ are the so-called golden ratios (note that $\phi \approx 1.618\ldots$ and $\psi \approx -0.618\ldots$). Hence,

$$\begin{aligned} F(x) &= \frac{x}{(1 - \phi x)(1 - \psi x)} \\ &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \phi x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1 - \psi x} \end{aligned}$$

(by partial fraction decomposition).

Now, recall that

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots,$$

since

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

Substituting ϕx for x in this formula, we find

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

Similarly,

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

Hence, our above formula becomes

$$\begin{aligned}
F(x) &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\phi x} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\psi x} \\
&= \frac{1}{\sqrt{5}} \cdot \left(1 + \phi x + \phi^2 x^2 + \phi^3 x^3 + \cdots\right) - \frac{1}{\sqrt{5}} \cdot \left(1 + \psi x + \psi^2 x^2 + \psi^3 x^3 + \cdots\right) \\
&= \left(\frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}}\right) + \left(\frac{1}{\sqrt{5}}\phi - \frac{1}{\sqrt{5}}\psi\right) x + \left(\frac{1}{\sqrt{5}}\phi^2 - \frac{1}{\sqrt{5}}\psi^2\right) x^2 + \cdots.
\end{aligned}$$

Now, for any given $n \in \mathbb{N}$, the coefficient of x^n in the power series $F(x)$ is f_n. So, comparing the coefficients of x^n in the above equation, we obtain

$$f_n = \frac{1}{\sqrt{5}}\phi^n - \frac{1}{\sqrt{5}}\psi^n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

This formula is known as **Binet's formula** for the Fibonacci numbers.

This method for computing Fibonacci numbers can be extended to more general recurrences (there is an exercise for this on the homework).

1.1.2. Example 3: The Vandermonde convolution

(Example 2 will be next time.)

Example 3: The **Vandermonde convolution identity** (aka the **Chu–Vandermonde identity**) says that

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

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 this also holds for arbitrary a and b.

Indeed, fix $a, b \in \mathbb{N}$. For any $n \in \mathbb{N}$, the binomial formula yields

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

(here, we extended the sum from ranging over $k \in \{0, 1, \ldots, n\}$ to ranging over all $k \in \mathbb{N}$, because all the new addends $\binom{n}{k}$ for $k > n$ will be 0). Thus,

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

Multiplying the first two of these equalities, we find

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

Comparing this with

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

Comparing these, we obtain

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

Comparing coefficients in front of x^n, we obtain

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

Thus, the Vandermonde convolution identity is proved for $a, b \in \mathbb{N}$.

1.1.3. Example 2: Dyck words / Catalan numbers

A **Dyck word** of length $2n$ (where $n \in \mathbb{N}$) means 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

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

Some examples:

- Is $(1, 1, 1, 1)$ a Dyck word? No, since it fails the first condition.
- Is $(1, 0, 0, 1)$ a Dyck word? No, since it fails the second condition for $k = 3$.
- Is $(1, 0, 1, 0)$ a Dyck word? Yes.
- Is $(0, 1, 1, 0)$ a Dyck word? No, since it fails the second condition for $k = 1$.
- Is $()$ a Dyck word? Yes.

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: (see whiteboard)

Note that any NE-step or SE-step increases the x-coordinate by 1. Thus, any Dyck path from $(0, 0)$ to $(2n, 0)$ has precisely $2n$ steps.

Proposition 1.1.1. Let $n \in \mathbb{N}$. There is a bijection from $\{\text{Dyck words of length } 2n\}$ to $\{\text{Dyck paths from } (0,0) \text{ to } (2n,0)\}$.

Proof. If you have a Dyck word, read it as a "way description" of a Dyck path by interpreting any 1 as an NE-step and any 0 as a SE-step. □

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

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

$$\begin{aligned} c_n &:= (\text{\# of Dyck words of length } 2n) \\ &= (\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0)). \end{aligned}$$

Then, $c_0 = 1$ and $c_1 = 1$ and $c_2 = 2$ and $c_3 = 5$ and $c_4 = 14$. These numbers c_n are known as the **Catalan numbers** and have a long history and at least one book written about them (see the notes for the reference).

Let us try to compute them. First, we look for a recursive formula.

Fix a positive integer n. For any Dyck path D from $(0,0)$ to $(2n,0)$, we consider the **first return** of D; this is the first point on D that lies on the x-axis after the starting point. This point always has the form $(2k,0)$ for some $k \in \{1,2,\ldots,n\}$. Thus,

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

Now, let us fix some $k \in \{1,2,\ldots,n\}$. We shall compute the # of Dyck paths from $(0,0)$ to $(2n,0)$ with first return $(2k,0)$.

Any such Dyck path has a natural "four-part" structure:

- It starts with an NE-step $(0,0) \to (1,1)$.
- It continues with a Dyck path $(1,1) \to (2k-1,1)$. (Formally speaking, this is a Dyck path $(0,0) \to (2k-2,0)$ translated by the vector $(1,1)$.)
- It then takes the SE-step $(2k-1,1) \to (2k,0)$.
- It concludes with a Dyck path $(2k,0) \to (2n,0)$ (again, formally speaking, a Dyck path $(0,0) \to (2n-2k,0)$ translated by $(2k,0)$).

The first and third of these four parts are uniquely determined, but the second and fourth can be arbitrary. Thus, there are c_{k-1} options for the second part, and c_{n-k} options for the fourth part. Altogether, we thus conclude that

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

Forget that we fixed k. We thus have proved this equality for each $k \in \{1, 2, \ldots, n\}$. Hence,

$$\begin{aligned} c_n &= \sum_{k=1}^{n} \underbrace{(\text{\# of Dyck paths from } (0,0) \text{ to } (2n,0) \text{ with first return } (2k,0))}_{=c_{k-1}c_{n-k}} \\ &= \sum_{k=1}^{n} c_{k-1}c_{n-k} = c_0c_{n-1} + c_1c_{n-2} + c_2c_{n-3} + \cdots + c_{n-1}c_0. \end{aligned}$$

This is a nice recurrence (for all $n \geq 1$).

But what about an explicit formula?

Let

$$C(x) := \sum_{n \geq 0} c_n x^n = c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots .$$

Thus,

$$\begin{aligned} C(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots \\ &= 1 + (c_0c_0)\, x + (c_0c_1 + c_1c_0)\, x^2 + (c_0c_2 + c_1c_1 + c_2c_0)\, x^3 + \cdots \\ &= 1 + x \underbrace{\left((c_0c_0) + (c_0c_1 + c_1c_0)\, x + (c_0c_2 + c_1c_1 + c_2c_0)\, x^2 + \cdots \right)}_{=(c_0+c_1x+c_2x^2+c_3x^3+\cdots)^2} \\ &= 1 + x \left(\underbrace{c_0 + c_1x + c_2x^2 + c_3x^3 + \cdots}_{=C(x)} \right)^2 = 1 + x\,(C(x))^2 . \end{aligned}$$

This is a quadratic equation in $C(x)$. Let us solve it using the quadratic formula (assuming, unjustifed for now, that all of this is kosher). We get

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

The $\pm$ sign has to be a $-$ sign, since a $+$ sign would make the numerator non-divisible by $2x$. So

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

So can we use this to find the coefficients of $C(x)$?

Recall the binomial formula, which says (among other things) that

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

Let us be very daring and just assume that this holds for any n, not just for $n \in \mathbb{N}$. Thus, applying this formula to $n = 1/2$, we get

$$(1+x)^{1/2} = \sum_{k \in \mathbb{N}} \binom{1/2}{k} x^k.$$

Substituting $-4x$ for x in this equality, we get

$$(1-4x)^{1/2} = \sum_{k\in\mathbb{N}} \binom{1/2}{k} (-4x)^k = \sum_{k\in\mathbb{N}} \binom{1/2}{k} (-4)^k x^k.$$

We conclude that

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

Comparing coefficients in front of x^n in this equality, we find

$$c_n = \binom{1/2}{n+1} (-1)^n 2^{2n+1}.$$

Surprisingly, we can simplify this further. Indeed,

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

so

$$\begin{aligned} c_n &= \binom{1/2}{n+1} (-1)^n \, 2^{2n+1} = \frac{(-1)^n \cdot 1 \cdot 3 \cdot \cdots \cdot (2n-1)}{2^{n+1} \, (n+1)!} (-1)^n \, 2^{2n+1} \\ &= \frac{1 \cdot 3 \cdot \cdots \cdot (2n-1)}{(n+1)!} 2^n = \frac{1 \cdot 3 \cdot \cdots \cdot (2n-1)}{(n+1) \cdot n!} 2^n \\ &= \frac{1}{n+1} \cdot \underbrace{\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{n!} \cdot 2^n}_{\substack{= \binom{2n}{n} \\ \text{(by the exercise above)}}} \\ &= \frac{1}{n+1} \binom{2n}{n}. \end{aligned}$$

Moreover, we can rewrite this further as

$$c_n = \binom{2n}{n} - \binom{2n}{n-1} \qquad \text{(homework exercise)}.$$

There are more combinatorial ways to prove this (see, e.g., Math 222), but the above proof was hopefully somewhat instructive.

Office hours: Fri 2 PM – 3 PM?

HW: double deadlines? (second chance to increase points to 20)
HW1 due Jan 26 / Feb 2
HW2 due Feb 9 / 16
HW3 due Feb 23 / Mar 1
HW4 due Mar 8 / 15
HW5 due Mar 22 (no second chance)

1.2. Definitions

The four examples above are reason enough to suspect that power series / generating functions are useful. Let us now convince ourselves that they can be made rigorous.

I will outline the theory in class; you can find more details in the notes.

First things first: Generating functions aren't really functions. They are **formal power series** (short: **FPSs**). Roughly speaking, these are "formal" infinite sums of the form $a_0 + a_1 x + a_2 x^2 + \cdots$, where x is an "indeterminate". You cannot always substitute numbers into them. For example, if you substituted $x = 2$ into

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

would yield

$$\frac{1}{1-2} = 1 + 2 + 2^2 + 2^3 + \cdots = 1 + 2 + 4 + 8 + \cdots ,$$

which is absurd on the face.

1.2.1. Reminder: Commutative rings

Our FPSs will form a commutative ring and will be defined over a commutative ring, so let us first recall how a commutative ring is defined:

Definition 1.2.1. 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 $a, b \in K$.

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 $a, b, c \in K$. Then, $a \oplus b = c$ 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

$$\begin{aligned} a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c) \qquad \text{and} \\ (a \oplus b) \odot c &= (a \odot c) \oplus (b \odot c) \end{aligned}$$

   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 $a \in K$.

The operations $\oplus$, $\ominus$ and $\odot$ are called the **addition**, the **subtraction** and the **multiplication** of the ring K. They are typically denoted by $+$, $-$ and $\cdot$ unless this would clash with existing notations. We also write ab for $a \cdot b = a \odot b$.

The elements $\mathbf{0}$ and $\mathbf{1}$ are called the **zero** and the **unity** (or the **one**) of the ring K.

We will ue the PEMDAS conventions. For example, $ab + ac$ means $(ab) + (ac)$, not $a(b+a)c$.

Some examples of commutative rings:

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are commutative rings.
- The set $\mathbb{N}$ is not, since it has no subtraction. (It is what is called a **commutative semiring**.)
- The matrix ring $\mathbb{Q}^{m\times m}$ for a given m is not a commutative ring, since it fails the commutativity of multiplication axiom. But it satisfies all the other axioms, which 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 $\mathbb{R}$). The reason for this is that the sum, the difference and the product of two numbers of the form $a + b\sqrt{5}$ can be rewritten again in this form. For example,
$$\left(a + b\sqrt{5}\right)\left(c + d\sqrt{5}\right) = (ac + 5bd) + (ad + bc)\sqrt{5}.$$
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
$$\begin{aligned}\mathbb{Z}/m &= \{\text{all residue classes modulo } m\} \\ &= \left\{\begin{array}{c}\text{equivalence classes of integers with} \\ \text{respect to the ``congruent modulo } m\text{'' } \\ \text{equivalence relation}\end{array}\right\}\end{aligned}$$
is a commutative ring, with 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 as $\mathbb{Z}_m$ (bad notation). When m is prime, $\mathbb{Z}/m$ 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 are either numbers or consist of numbers (matrices or equivalence classes). Here is an example where they are sets.

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

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

  Fix a set S. Consider its power set $\mathcal{P}(S)$ (= the set of all subsets of S). This power set $\mathcal{P}(S)$ is a commutative ring if we equip it with the operation $\bigtriangleup$ as addition (i.e., we set $X \oplus Y = X \bigtriangleup Y$ for all $X, Y \in \mathcal{P}(S)$), with the same operation $\bigtriangleup$ as subtraction, and with the operation $\cap$ as multiplication (that is, $X \odot Y = X \cap Y$), and with zero $\mathbf{0} := \varnothing$ and the unity $\mathbf{1} := S$. Indeed, it is straightforward to verify the axioms for this construction.

  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

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

  Then, $\mathbb{T}$ is a commutative semiring. It is called the **tropical semiring** of $\mathbb{Z}$.

More examples can be found in algebra texts (some references in notes).

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

- 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

  $$((a + b) + (c + d)) + e = (a + (b + c)) + (d + e) = \cdots .$$

  So you can drop the parentheses and write $a + b + c + d + e$. This called **general(ized) 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(ized) commutativity**.

More formally: If $(a_s)_{s\in S}$ is any finite family of elements of a commutative ring K, then the finite sum

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

is a well-defined element of K. Such sums satisfy the usual rules such as

$$\sum_s (a_s+b_s) = \sum_s a_s + \sum_s b_s;$$
$$\sum_s a_s = \sum_w \sum_{\substack{s;\\ f(s)=w}} a_s;$$
$$\ldots.$$

Empty sums are 0 by definition (where 0 means $\mathbf{0}$).

- The same holds for finite products. Empty products are 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 the element $na \in K$ by

$$na = \underbrace{a+a+\cdots+a}_{n\text{ times}} \qquad \text{if } n \geq 0;$$
$$na = 0-(-n)\,a \qquad \text{if } n<0.$$

  This generalizes the standard definition of multiplication on $\mathbb{Z}$ as repeated addition.

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

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

  In particular, $a^0 = (\text{empty product}) = 1 \in K$.

- Standard rules hold:

$$\begin{aligned} -(a+b) &= (-a)+(-b); \\ (n+m)\,a &= na+ma \qquad \text{for } n,m\in\mathbb{Z}; \\ a^{n+m} &= a^n a^m; \\ a^{nm} &= (a^n)^m; \\ &\ldots; \\ (a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{(the binomial formula)}. \end{aligned}$$

A further useful concept is that of a K-**module**. Namely, if K is a commutative ring, then the notion of a K-module is just the straightforward generalization of the notion of a K-vector space (which is defined when K is a field). Here is the definition in detail:

Definition 1.2.2. Let K be a commutative ring.

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

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

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 $a, b \in M$.
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 $a, b, c \in M$. Then, $a \oplus b = c$ 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 $u \in K$.

The operations $\oplus$, $\ominus$ and $\rightharpoonup$ are called the **addition**, the **subtraction** and the **scaling** of the K-module M. They are typically denoted by $+$, $-$ and $\cdot$ unless this would clash with existing notations. We also write ua for $u \rightharpoonup a$.

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

When M is a K-module, we refer to the elements of K as **scalars** and the elements of M as **vectors**.

1.2.2. The definition of formal power series

Convention 1.2.3. Fix a commutative ring K.

Definition 1.2.4. A **formal power series** (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

$$(0,0,0,\ldots), \qquad (1,0,0,0,0,\ldots), \qquad (1,1,1,1,\ldots), \qquad (1,2,3,4,\ldots).$$

OK, but what can we do with FPSs?

Definition 1.2.5. (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 $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ 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

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

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 $a \in K$ is said to be **constant**.

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

The following theorem is crucial: It says that the operations we just defined behave as we would want them to behave:

Theorem 1.2.6. **(a)** The set $K[[x]]$ is a commutative ring (with the operations $+$, $-$ and $\cdot$ just defined) with zero $\underline{0} = (0, 0, 0, \ldots)$ and unity $\underline{1} = (1, 0, 0, 0, \ldots)$. For example, it satisfies associativity of multiplication:

$$\mathbf{a}(\mathbf{bc}) = (\mathbf{ab})\mathbf{c} \qquad \text{for all FPSs } \mathbf{a}, \mathbf{b}, \mathbf{c}.$$

(See the notes for all the axioms spelled out.)

(b) The set $K[[x]]$ is a K-module (with the scaling being the map that sends each $(\lambda, \mathbf{a})$ to $\lambda\mathbf{a}$).

(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) We have $\lambda\mathbf{a} = \underline{\lambda} \cdot \mathbf{a}$ for all $\lambda \in K$ and $\mathbf{a} \in K[[x]]$.

Proof. Notes. □

Definition 1.2.7. 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 $[x^n]\,\mathbf{a}$ of K by

$$[x^n]\,\mathbf{a} := a_n.$$

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

Thus, the definitions of $+$ and $-$ on FPSs become

$$[x^n](\mathbf{a} + \mathbf{b}) = [x^n]\,\mathbf{a} + [x^n]\,\mathbf{b};$$
$$[x^n](\mathbf{a} - \mathbf{b}) = [x^n]\,\mathbf{a} - [x^n]\,\mathbf{b}.$$

Moreover, the definition of $\cdot$ becomes

$$[x^n](\mathbf{ab}) = \sum_{\substack{i,j \in \mathbb{N};\\ i+j=n}} \left[x^i\right]\mathbf{a} \cdot \left[x^j\right]\mathbf{b} = \sum_{i=0}^{n} \left[x^i\right]\mathbf{a} \cdot \left[x^{n-i}\right]\mathbf{b}.$$

In particular,

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

In other words, the constant term of $\mathbf{ab}$ is the product of the constant terms of $\mathbf{a}$ and $\mathbf{b}$. Here, the **constant term** of a FPS $\mathbf{a}$ is defined to be its 0-th coefficient $\left[x^0\right]\mathbf{a}$.

Finally, the definition of scaling yields

$$[x^n](\lambda\mathbf{a}) = \lambda \cdot [x^n]\,\mathbf{a} \qquad \text{for any FPS } \mathbf{a} \text{ and any } \lambda \in K.$$

Since $K[[x]]$ is a commutative ring, any finite sum of FPSs is well-defined. But sometimes we want infinite sums to make sense as well. For example, it is reasonable to expect that

$$\begin{aligned} & \ (1,1,1,1,1,1,\ldots) \\ & + (0,1,1,1,1,1,\ldots) \\ & + (0,0,1,1,1,1,\ldots) \\ & + (0,0,0,1,1,1,\ldots) \\ & + \cdots \\ & = \quad (1,2,3,4,5,6,\ldots), \end{aligned}$$

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

> **Definition 1.2.8.** **(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 be 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, and its sum is

$$\begin{aligned} \sum_{n\in\mathbb{N}} \left\lfloor \frac{5}{2^n} \right\rfloor &= \left\lfloor \frac{5}{2^0} \right\rfloor + \left\lfloor \frac{5}{2^1} \right\rfloor + \left\lfloor \frac{5}{2^2} \right\rfloor + \left\lfloor \frac{5}{2^3} \right\rfloor + \cdots \\ &= 5+2+1+\underbrace{0+0+0+\cdots}_{\text{just zeroes}} \\ &= 5+2+1 = 8. \end{aligned}$$

Note:

- A family $(a_i)_{i\in I} \in K^I$ is always essentially finite if I is finite. But some infinite families also can be essentially finite.
- Any essentially finite sum of real or complex numbers is convergent in the sense of analysis, but not vice versa. For instance, $\sum\limits_{n\in\mathbb{N}} \dfrac{1}{2^n} = \dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{4} + \dfrac{1}{8} + \cdots$ is convergent but not essentially finite. The concept of essentially finite sums is much simpler than the analytic concept of convergence, but it will play a similar role for us.

Essentially finite sums behave very much like finite sums. In particular, they satisfy the same rules, with one **caveat**: Interchange of summations does not always work. More precisely, we might fail to have

$$\sum_{i\in I}\ \sum_{j\in J} a_{i,j} = \sum_{j\in J}\ \sum_{i\in I} a_{i,j}$$

even if all four sums are essentially finite. For an example, let us take $I = J = \mathbb{N}$ and $a_{i,j}$ given by the following table (empty cells are understood to be filled with 0's):

$$\begin{array}{ccccccc}
a_{i,j} & j=0 & j=1 & j=2 & j=3 & j=4 & \cdots \\
i=0 & 1 & -1 & & & & \cdots \\
i=1 & & 1 & -1 & & & \cdots \\
i=2 & & & 1 & -1 & & \cdots \\
i=3 & & & & 1 & -1 & \cdots \\
i=4 & & & & & 1 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}.$$

Then,

$$\begin{aligned}
\sum_{i\in I}\ \sum_{j\in J} a_{i,j} &= \sum_{i\in I} 0 = 0, \qquad \text{but} \\
\sum_{j\in J}\ \sum_{i\in I} a_{i,j} &= 1 + \underbrace{0 + 0 + 0 + \cdots}_{=0} = 1.
\end{aligned}$$

If you are wondering why this doesn't work, recall how the interchange-of-summations rule is proved in the finite case: When I and J are finite, the two sums

$$\sum_{i\in I}\ \sum_{j\in J} a_{i,j} \text{ and } \sum_{j\in J}\ \sum_{i\in I} a_{i,j}$$

are equal because they both equal $\sum\limits_{(i,j)\in I\times J} a_{i,j}$. In general, this works whenever the sum $\sum\limits_{(i,j)\in I\times J} a_{i,j}$ is essentially finite. But $\sum\limits_{(i,j)\in I\times J} a_{i,j}$ is not essentially finite in our example above.

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 $K[[x]]$. However, this does not help make sense of sums such as

$$\begin{aligned}
& (1,1,1,1,1,1,\ldots) \\
+ & (0,1,1,1,1,1,\ldots) \\
+ & (0,0,1,1,1,1,\ldots) \\
+ & (0,0,0,1,1,1,\ldots) \\
+ & \cdots \\
= & \quad (1,2,3,4,5,6,\ldots),
\end{aligned}$$

since none of the infinitely many FPSs on the LHS is 0. So we need a weaker version of essential finiteness:

Definition 1.2.9. A (possibly infinite) family $(\mathbf{a}_i)_{i\in I}$ of FPSs is said to be **summable** (or **entrywise essentially finite**) 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 $\sum\limits_{i\in I} \mathbf{a}_i$ is defined to be the FPS with

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

Any essentially finite family of FPSs is summable, but there are many more summable families than essentially finite ones. For example, the above sum

$$\begin{aligned} &(1,1,1,1,1,1,\ldots)\\ +\,&(0,1,1,1,1,1,\ldots)\\ +\,&(0,0,1,1,1,1,\ldots)\\ +\,&(0,0,0,1,1,1,\ldots)\\ +\,&\cdots \end{aligned}$$

now makes sense:

Example 1.2.10. Consider the family $(\mathbf{a}_i)_{i\in\mathbb{N}} \in K[[x]]^{\mathbb{N}}$ of FPSs, where

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

Then, this family $(\mathbf{a}_i)_{i\in\mathbb{N}}$ is summable, because for each $n \in \mathbb{N}$, all $i > n$ satisfy $[x^n]\,\mathbf{a}_i = 0$. Its sum $\sum\limits_{i\in\mathbb{N}} \mathbf{a}_i$ is given by

$$[x^n]\left(\sum_{i\in\mathbb{N}}\mathbf{a}_i\right) = \sum_{i\in\mathbb{N}} \underbrace{[x^n]\,\mathbf{a}_i}_{=\begin{cases}1, & \text{if } i \le n;\\ 0, & \text{if } i > n\end{cases}} = \sum_{i\in\mathbb{N}} \begin{cases}1, & \text{if } i \le n;\\ 0, & \text{if } i > n\end{cases} = n+1.$$

In other words,

$$\sum_{i\in\mathbb{N}}\mathbf{a}_i = (1,2,3,4,5,\ldots)\,.$$

This is just our above calculation

$$\begin{aligned} & (1,1,1,1,1,1,\ldots) \\ + & (0,1,1,1,1,1,\ldots) \\ + & (0,0,1,1,1,1,\ldots) \\ + & (0,0,0,1,1,1,\ldots) \\ + & \cdots \\ = & \quad (1,2,3,4,5,6,\ldots), \end{aligned}$$

made rigorous.

Just as for essentially finite families, we can work with summable families of FPSs using the same rules as for finite sums:

Proposition 1.2.11. Sums of summable families of FPSs satisfy the usual rules for sums. Again, the only **caveat** is that the interchange-of-summations rule

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

works only if the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable (it does not suffice that the four sums in the equality are summable).

Proof. Straightforward finite-set arguments. See the notes for a sketch and a reference. □

Now, we can define the x that featured so prominently in our examples of FPSs:

Definition 1.2.12. Let x denote the FPS $(0,1,0,0,0,\ldots)$. In other words, it is the FPS with $\left[x^1\right]x=1$ and $\left[x^i\right]x=0$ for all $i\neq 1$.

Lemma 1.2.13. Let $\mathbf{a}=(a_0,a_1,a_2,\ldots)$ be an FPS. Then, $x\cdot\mathbf{a}=(0,a_0,a_1,a_2,\ldots)$.

Proof. If n is a positive integer, then

$$\begin{aligned}\left[x^n\right](x\cdot\mathbf{a}) &= \sum_{i=0}^{n}\underbrace{\left[x^i\right]x}_{\substack{=1\text{ for }i=1\\ \text{and 0 otherwise}}}\cdot\left[x^{n-i}\right]\mathbf{a}=\underbrace{\left[x^1\right]x}_{=1}\cdot\underbrace{\left[x^{n-1}\right]\mathbf{a}}_{=a_{n-1}} \\ &= a_{n-1}.\end{aligned}$$

So we get $x\cdot\mathbf{a}=(?,a_0,a_1,a_2,\ldots)$. A similar argument shows that the ? is 0. □

Proposition 1.2.14. We have

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

Proof. Induction on k, using the above lemma. (Start with $x^0 = \underline{1} = (1,0,0,0,\ldots)$.) □

Corollary 1.2.15. Any FPS $(a_0,a_1,a_2,\ldots) \in K[[x]]$ satisfies

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

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

Proof. By the previous proposition,

$$\begin{aligned}
& a_0 + a_1x + a_2x^2 + \cdots \\
& = \quad a_0(1,0,0,0,\ldots) \\
& + a_1(0,1,0,0,\ldots) \\
& + a_2(0,0,1,0,\ldots) \\
& + a_3(0,0,0,1,\ldots) \\
& + \cdots \\
& = \quad (a_0,0,0,0,\ldots) \\
& + (0,a_1,0,0,\ldots) \\
& + (0,0,a_2,0,\ldots) \\
& + (0,0,0,a_3,\ldots) \\
& + \cdots \\
& = (a_0,a_1,a_2,a_3,\ldots).
\end{aligned}$$

□

So we have found our x and justified rigorously our habit of writing the FPS $(a_0,a_1,a_2,\ldots)$ as $a_0 + a_1x + a_2x^2 + \cdots$. Note that no analysis was used in all of this. In particular, our FPSs do not have to be convergent in the sense of analysis. It is easy to come up with examples of FPSs that never converge at any complex number than 0. (For example, $\sum\limits_{n\in\mathbb{N}} n!x^n = (1,1,2,6,24,120,\ldots)$ does not converge if you plug in any nonzero $z \in \mathbb{C}$.)

We can now also answer the question "what is a generating function":

Definition 1.2.16. Let $(a_0, a_1, a_2, \ldots)$ be a sequence of elements of K. Then, its **ordinary generating function** will means the FPS $(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots$.

1.2.3. The Chu–Vandermonde identity

What we have done so far suffices to justify Example 3 in the introduction. Let us state it as a proposition:

Proposition 1.2.17. For any $a, b \in \mathbb{N}$ and any $n \in \mathbb{N}$, we have

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

We derived this from $(1+x)^{a+b} = (1+x)^a (1+x)^b$. This is correct, since the laws of exponents $u^{a+b} = u^a u^b$ work in any commutative ring and thus work in $K[[x]]$ (since $K[[x]]$ is a commutative ring), and the binomial formula (which we used to compute the coefficients on both sides) also works in any commutative ring.

We have yet to justify Examples 1, 2 and 4; we shall do this later. For now, let us generalize the above proposition to arbitrary numbers a and b (as opposed to merely $a, b \in \mathbb{N}$). In other words, let us prove the following:

Theorem 1.2.18 (Vandermonde convolution identity, or Chu–Vandermonde identity)**.** For any $a, b \in \mathbb{C}$ and any $n \in \mathbb{N}$, we have

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

(Note that $\mathbb{C}$ can be replaced by any field of characteristic 0, and even by some more general settings.)

One way to prove this general theorem is by extending our proof of the proposition to $a, b \in \mathbb{C}$. This is a bit tricky, because the equation $(1+x)^{a+b} = (1+x)^a (1+x)^b$ only makes sense if we can take a-th and b-th powers (and if they satisfy the laws of exponents). We could make this work, but it would take us some effort.

We will take a different route, introducing a slick trick that allows us to automatically extend a claim like the Vandermonde convolution identity from nonnegative integers to complex numbers. This is the **polynomial identity trick**, and relies on very basic properties of polynomials. Let me sketch a proof of the theorem using this trick:

Proof of the Vandermonde convolution identity. Fix $n \in \mathbb{N}$ and $b \in \mathbb{N}$, but let us not fix a. Then, the proposition that we proved yields that

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

holds for each $a \in \mathbb{N}$. However, both sides of this identity are polynomial functions in a; indeed,

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

$$\sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k} = \sum_{k=0}^{n} \frac{a(a-1)(a-2)\cdots(a-k+1)}{k!} \binom{b}{n-k}.$$

If two univariate polynomials p and q (with complex coefficients) are equal on any input $a \in \mathbb{N}$ (that is, if $p(a) = q(a)$ for each $a \in \mathbb{N}$), then they must be identical (since two univariate polynomials that are equal at infinitely many points must necessarily be identical). So, because our above polynomial equality holds for all $a \in \mathbb{N}$, it must hold for all $a \in \mathbb{C}$.

Thus, we have shown that the identity

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

holds not just for every $a \in \mathbb{N}$, but also for every $a \in \mathbb{C}$.

But b is still required to be $\in \mathbb{N}$. What do we do to lift this requirement? We repeat the same argument as above, but now with the roles of a and b switched (i.e., we keep $a \in \mathbb{C}$ fixed, and we treat b as a variable). Thus, we generalize the identity from $b \in \mathbb{N}$ to $b \in \mathbb{C}$. This proves the theorem. □

Next we will work towards justifying Examples 1, 2 and 4.

1.2.4. What next?

Let us return to our quest of justifying those examples. In order to do so, we need to know

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

So let us address these.

1.3. Dividing FPSs

1.3.1. Conventions

Convention 1.3.1. We identify each $a \in K$ with the constant FPS $\underline{a} = (a, 0, 0, 0, \ldots) \in K[[x]]$.

This constant FPS is written as $a + 0x + 0x^2 + 0x^3 + \cdots$ in the "usual" way of writing FPSs.

Furthermore, I will stop using boldfaced letters for FPSs.

1.3.2. Inverses in commutative rings

Definition 1.3.2. Let L be a commutative ring. Let $a \in L$. Then:

(a) An **inverse** of a means an element $b \in L$ such that $ab = ba = 1$.

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

For example, any element of $\mathbb{Q}$ other than 0 is invertible, but only 1 and -1 are invertible in $\mathbb{Z}$.

Theorem 1.3.3. Let L be a commutative ring. Let $a \in L$. Then, there is **at most one** inverse of a.

Definition 1.3.4. 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}.

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

(c) For any negative integer n, we set $a^n := \left(a^{-1}\right)^{-n}$. Thus, the power a^n is defined for any $n \in \mathbb{Z}$.

Standard rules hold:

$$\begin{aligned}
\left(a^{-1}\right)^{-1} &= a; \\
a^{n+m} &= a^n a^m; \\
(a^n)^m &= a^{nm}; \\
(ab)^n &= a^n b^n \qquad \text{(here we need commutativity!)}; \\
\frac{b}{a} + \frac{d}{c} &= \frac{bc + ad}{ac}; \qquad \frac{b}{a} \cdot \frac{d}{c} = \frac{bd}{ac}.
\end{aligned}$$

And of course, division undoes multiplication.

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

Now, which FPSs are invertible in the ring $K[[x]]$? For example, we know 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 any multiple of x has constant term 0, but 1 does not) unless K is trivial.

It turns out that invertible FPSs have a very simple description:

> **Theorem 1.3.5.** Let $a \in K[[x]]$. Then, a is invertible in $K[[x]]$ if and only if $\left[x^0\right] a$ (this is the constant term of a) is invertible in K.

Proof. $\Longrightarrow$: If a is invertible in $K[[x]]$, then

$$1 = \left[x^0\right] 1 = \left[x^0\right] \underbrace{\left(aa^{-1}\right)}_{=1} = \left[x^0\right] a \cdot \left[x^0\right] a^{-1},$$

so $\left[x^0\right] a$ is invertible in K (with inverse $\left[x^0\right] a^{-1}$). This proves the "$\Longrightarrow$" direction.

$\Longleftarrow$: Assume that $\left[x^0\right] a$ is invertible in K. Write a as $a = (a_0, a_1, a_2, \ldots)$, so that $\left[x^0\right] a = a_0$. Thus, a_0 is invertible in K.

We want to construct an inverse of a. In other words, we want to construct a FPS $b = (b_0, b_1, b_2, \ldots)$ such that $ab = 1$. Let us see what the equation $ab = 1$ means in terms of the coefficients.

From $a = (a_0, a_1, a_2, \ldots)$ and $b = (b_0, b_1, b_2, \ldots)$, we have

$$ab = (a_0b_0,\ a_0b_1 + a_1b_0,\ a_0b_2 + a_1b_1 + a_2b_0,\ \ldots).$$

For this to equal $1 = \underline{1} = (1, 0, 0, 0, \ldots)$, we must have

$$\begin{cases} a_0b_0 = 1; \\ a_0b_1 + a_1b_0 = 0; \\ a_0b_2 + a_1b_1 + a_2b_0 = 0; \\ \ldots. \end{cases}$$

This is an infinite system of linear equations in the unknowns $b_0, b_1, b_2, \ldots$. But it is triangular, so we can solve it recursively: First solve the top equation for b_0; then solve the next equation for b_1 (using the b_0 already found); then solve the next for b_2; and so on. We get the following recursive description for the b_i's:

$$\begin{aligned} b_0 &= \frac{1}{a_0}; \\ b_i &= -\frac{1}{a_0}\left(a_1b_{i-1} + a_2b_{i-2} + \cdots + a_ib_0\right) \qquad \text{for each } i \geq 1. \end{aligned}$$

This works because a_0 is invertible. So we do find a FPS $b = (b_0, b_1, b_2, \ldots)$ that satisfies $ab = 1$. Thus, this FPS is an inverse to a (since commutativity of $K[[x]]$ implies $ab = ba$), and therefore a is invertible. □

Corollary 1.3.6. Assume that K is a field. Let $a \in K[[x]]$. Then, a is invertible in $K[[x]]$ if and only if $[x^0]\, a$ (this is the constant term of a) is nonzero.

1.3.4. Newton's binomial formula

We return to the specific FPS $1 - x$, which we know to be invertible with inverse $1 + x + x^2 + x^3 + \cdots$. Similarly we can handle $1 + x$:

Proposition 1.3.7. The FPS $1 + x \in K[[x]]$ is invertible, and its inverse is

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

Proof. Another telescope argument. □

So $(1+x)^n$ is defined for every $n \in \mathbb{Z}$. What can we say about these powers?

Theorem 1.3.8 (Newton's binomial theorem)**.** For each $n \in \mathbb{Z}$, we have

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

Don't plug random stuff into this formula!

$$\begin{aligned}(1+2)^{-1} &= \sum_{k\in\mathbb{N}} \underbrace{\binom{-1}{k}}_{=(-1)^k} 2^k = \sum_{k\in\mathbb{N}} (-1)^k 2^k \\ &= 1 - 2 + 4 - 8 + 16 \pm \cdots,\end{aligned}$$

which is nonsense.

Proof. There are different ways to prove Newton's binomial theorem. The easiest one is perhaps by downwards induction on n (that is, induction on $-n$). Indeed, for $n \geq 0$, the theorem is clear (just take the usual binomial formula and extend the sum to make it infinite). So we only need to prove it for $n < 0$. So we induct on $-n$, and we have to take the step from n to $n-1$. That is, we assume that

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

and we must prove that

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

But we have

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

whereas

$$\begin{aligned}
&\sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k \cdot (1+x) \\
&= \sum_{k\in\mathbb{N}} \binom{n-1}{k} \left(x^k + x^{k+1}\right) \\
&= \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^{k+1} \\
&= \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + \sum_{k\geq 1} \binom{n-1}{k-1} x^k \\
&= \sum_{k\in\mathbb{N}} \binom{n-1}{k} x^k + \sum_{k\in\mathbb{N}} \binom{n-1}{k-1} x^k \\
&= \sum_{k\in\mathbb{N}} \underbrace{\left(\binom{n-1}{k} + \binom{n-1}{k-1}\right)}_{=\binom{n}{k}} x^k \\
&= \sum_{k\in\mathbb{N}} \binom{n}{k} x^k.
\end{aligned}$$

Comparing these two equalities, we find

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

Cancelling $1+x$ from this equality (allowed since $1+x$ is invertible), we obtain

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

This completes our induction step. □

We note that the binomial coefficients $\binom{n}{k}$ for negative n can be expressed in terms of the ones for nonnegative n:

Theorem 1.3.9 (upper negation formula)**.** Let $n \in \mathbb{C}$ and $k \in \mathbb{Z}$. Then,

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

Proof. We have

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

The denominators are equal. The numerators are the same product in reverse order, up to sign. The sign is $(-1)^k$. □

1.3.5. Dividing by x

In our Dyck path example (Example 2), we had to divide a FPS by $2x$. Since $2x$ is not invertible, we do not yet know why this is allowed. But we can explain this very quickly, because it is easy to divide by x (and then you can divide by 2 if you work over $\mathbb{Q}$).

> **Definition 1.3.10.** Let $a = (a_0, a_1, a_2, \ldots)$ be an FPS whose constant term a_0 is 0. Then,
> $$\frac{a}{x} := (a_1, a_2, a_3, \ldots).$$

Of course, we have the equivalence $(a = xb) \iff \left(\frac{a}{x} = b\right)$.

Now, the FPS $\frac{1 \pm \sqrt{1-4x}}{2x}$ makes some sense, at least if $\sqrt{1-4x}$ makes sense and if the constant term of $1 \pm \sqrt{1-4x}$ is 0.

1.3.6. A lemma

> **Definition 1.3.11.** Let $g \in K[[x]]$ be a FPS. Then, a **multiple** of g means a FPS of the form ga with $a \in K[[x]]$.

> **Lemma 1.3.12.** Let $k \in \mathbb{N}$. Let $f \in K[[x]]$ be a FPS. Then, the first k coefficients of f are 0 if and only if f is a multiple of x^k.

Proof. If $f = x^k a$ for some FPS $a = (a_0, a_1, a_2, \ldots)$, then

$$f = x^k a = x^k (a_0, a_1, a_2, \ldots) = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}, a_0, a_1, a_2, \ldots\right),$$

so that the first k coefficients of f are 0. The converse follows along the same lines. □

1.4. Polynomials

1.4.1. Definition

One way to define polynomials is actually as FPSs with only finitely many nonzero coefficients:

Definition 1.4.1. **(a)** An FPS $a \in K[[x]]$ is said to be a **polynomial** if all but finitely many $n \in \mathbb{N}$ satisfy $[x^n]\, a = 0$.

(b) The set of all polynomials $a \in K[[x]]$ is called $K[x]$, and is known as the **univariate polynomial ring** over K.

Theorem 1.4.2. The set $K[x]$ is a subring of $K[[x]]$ (that is, it is closed under addition, subtraction and multiplication) and is a K-submodule of $K[[x]]$ (that is, also closed under scaling).

1.4.2. Evaluation

For what is to come, I do want to introduce noncommutative rings as well.

Definition 1.4.3. The notion of a **ring** (also known as a **noncommutative ring**) is defined in the same way as we defined a commutative ring, except that we remove the "commutativity of multiplication" axiom.

For example, matrix rings such as $\mathbb{R}^{n\times n}$ and the quaternion ring $\mathbb{H}$ are rings. Of course, any commutative ring is a ring. If M is a $\mathbb{Z}$-module (i.e., any abelian group), then $\operatorname{End} M = \{\text{all endomorphisms of } M\}$ is a ring.

Next, we recall the concept of a K-algebra:

Definition 1.4.4. 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 $\oplus$, $\ominus$ and $\odot$ and $\overrightarrow{0}$ and $\overrightarrow{1}$ is a (noncommutative) ring.

2. The set A, equipped with $\oplus$, $\ominus$ and $\rightharpoonup$ and $\overrightarrow{0}$ is a K-module.

3. We have

$$\lambda \rightharpoonup (a \odot b) = (\lambda \rightharpoonup a) \odot b = a \odot (\lambda \rightharpoonup b) \qquad \text{for any } \lambda \in K \text{ and } a, b \in A$$

We use the standard shorthands, e.g., writing $a+b$ for $a \oplus b$, or writing ab for $a \odot b$, or writing λa for $\lambda \rightharpoonup a$. Examples of K-algebras include

- the ring K itself (recall that K is commutative);
- the ring $K[[x]]$ of FPSs;
- its subring $K[x]$;
- the matrix ring $K^{n \times n}$ for any $n \in \mathbb{N}$;
- any quotient ring of K (that is, any ring K/I where I is an ideal of K);
- any commutative ring that contains K as a subring.

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

Definition 1.4.5. 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 $f[a]$ (usually denoted $f(a)$, sometimes denoted $f \circ a$) of A as follows:

Write f in the form $f = \sum\limits_{n \in \mathbb{N}} f_n x^n = (f_0, f_1, f_2, \ldots)$ for $f_0, f_1, f_2, \ldots \in K$. 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 known as the **value** of f at a, or the **evaluation** of f at a, or the **result of substituting** a for x in f.

Many authors write $f(a)$ for $f[a]$, but this sometimes leads to ambiguities: Does $x(x+1)$ means $x[x+1]$ or $x \cdot (x+1)$?

If f and g are two polynomials in $K[x]$, then the value $f[g] = f \circ g$ is also known as the **composition** of f and g. We note that any polynomial f satisfies

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

Theorem 1.4.6. Let A be a K-algebra. Let $a \in A$. Then:

(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 $\underline{\lambda}[a] = \lambda \cdot 1_A$.

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

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

1.5. Substitution and evaluation of FPSs

1.5.1. Definition

We have seen that if $f \in K[x]$ is a polynomial, then we can substitute any element of a K-algebra into f.

In contrast, if $f \in K[[x]]$ is an FPS, then substituting things into f might fail. For instance,

$$\left(1 + x + x^2 + x^3 + \cdots\right)[1] \text{ would be } 1 + 1 + 1^2 + 1^3 + \cdots, \text{ which is nonsense.}$$

Thus, polynomials have an advantage of FPSs.

Nevertheless, not all is lost. **Some** things can be substituted into FPSs. For instance:

- We can always substitute 0 for x into a FPS $f \in K[[x]]$, since all the addends except for the constant term just become 0.
- We can always substitute x for x into a FPS $f \in K[[x]]$, since it just gives x.
- We can always substitute $x^2 + x$ for x into a FPS. Indeed, if the FPS f is $f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$, then

  $$\begin{aligned}
  &\left(f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots\right)\left[x^2 + x\right] \\
  &= f_0 + f_1\left(x^2 + x\right) + f_2\left(x^2 + x\right)^2 + f_3\left(x^2 + x\right)^3 + \cdots \\
  &= f_0 + f_1\left(x^2 + x\right) + f_2\left(x^4 + 2x^3 + x^2\right) + f_3\left(x^6 + 3x^5 + 3x^4 + x^3\right) + \cdots \\
  &= f_0 + f_1 x + \left(f_1 + f_2\right)x^2 + \left(2f_2 + f_3\right)x^3 + \left(f_2 + 3f_3 + f_4\right)x^4 + \cdots,
  \end{aligned}$$

  which makes perfect sense.

The last example can be generalized (which incidentally contains the previous two examples as well): There was nothing specific to the FPS $x^2 + x$ that we used here, other than that it was a multiple of x (that is, its constant term was 0). Let us introduce a notation for this:

Definition 1.5.1. Let f and g be two FPSs in $K[[x]]$. Assume that $\left[x^0\right]g = 0$ (that is, $g = g_1 x^1 + g_2 x^2 + g_3 x^3 + \cdots$ for some $g_1, g_2, g_3, \ldots \in K$).

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

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

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

This sum is well-defined since it is summable, which is because (see the notes for details) for each $n \in \mathbb{N}$, the first n coefficients of g^n are 0.

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 into f.

Example 1.5.2. The FPS $x + x^2$ has constant term $\left[x^0\right]\left(x + x^2\right) = 0$. Hence, by the previous definition, we can substitute it for x into $1 + x + x^2 + x^3 + \cdots$. The result is

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

The RHS here appears to be $f_1 + f_2 x + f_3 x^2 + f_4 x^3 + \cdots$, where $(f_0, f_1, f_2, \ldots)$ is the Fibonacci sequence. Let us show that this is indeed the case.

In the original Example 1 in Lecture 1, we showed that

$$f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots = \frac{x}{1 - x - x^2}.$$

Thus,

$$\begin{aligned}
\frac{x}{1 - x - x^2} &= \underbrace{f_0}_{=0} + f_1 x + f_2 x^2 + f_3 x^3 + \cdots \\
&= f_1 x + f_2 x^2 + f_3 x^3 + \cdots \\
&= x\left(f_1 + f_2 x + f_3 x^2 + \cdots\right).
\end{aligned}$$

Cancelling x from this equality (i.e., dividing both sides by x), we obtain

$$\frac{1}{1 - x - x^2} = f_1 + f_2 x + f_3 x^2 + \cdots .$$

However, it appears reasonable to expect that

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

Unfortunately, this is not obvious – after all, $\dfrac{1}{1 - x}\left[x + x^2\right]$ is defined by substituting $x + x^2$ for x in the **expanded** version of $\dfrac{1}{1 - x}$, not in the fraction $\dfrac{1}{1 - x}$ itself. So we have to actually prove that substituting something in a fraction gives the same result as substituting it in the numerator and the denominator and then taking the quotient.

Nevertheless, if we take this equality

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

for granted, then our claim follows, because

$$\frac{1}{1-x}\left[x+x^2\right] = \left(1+x+x^2+x^3+\cdots\right)\left[x+x^2\right].$$

1.5.2. Laws of substitution

Let us now justify this equality

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

It follows from one of the following laws of substitution:

Proposition 1.5.3. Composition of FPSs satisfies the following rules:

(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 $\frac{f_1}{f_2} \circ g = \frac{f_1 \circ g}{f_2 \circ g}$, as long as f_2 is invertible.

(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

$$(f \circ g) \circ h = f \circ (g \circ h).$$

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

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

(h) The analogue of part **(a)** works for infinite sums: If $(f_i)_{i \in I} \in K[[x]]^I$ is a summable family of FPSs, and if $g \in K[[x]]$ satisfies $\left[x^0\right] g = 0$, then

$$\left(\sum_{i \in I} f_i\right) \circ g = \sum_{i \in I} (f_i \circ g).$$

Proof. See notes. Most parts are straightforward. Part **(e)** is slightly tricky: First prove it for $f = x^k$ (using part **(d)**). Then, conclude the general case by "linearity" (actually an application of part **(h)**). □

With part **(c)** of this proposition, we have justified what we did in the preceding example.

Let us summarize: If $f, g \in K[[x]]$ are two FPSs, then the composition $f \circ g = f[g]$ is well-defined

- whenever f is a polynomial (i.e., whenever $f \in K[x]$), and
- whenever g has constant term 0 (i.e., whenever $[x^0]\, g = 0$).

(In some exotic cases, $f \circ g$ can be well-defined despite neither condition holding. If $K = \mathbb{Z}/4$ and $g = \overline{2} \in \mathbb{Z}/4$, then $f[g]$ is well-defined, since $\overline{2} \in \mathbb{Z}/4$ is nilpotent and thus all its high enough powers are 0.)

1.6. Derivatives of FPSs

We define the derivative of a FPS by just mimicking its behavior in analysis without bothering with the εs and δs:

Definition 1.6.1. Let $f \in K[[x]]$ be a FPSs. 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

$$f' := \sum_{n>0} n f_n x^{n-1}.$$

This derivative behaves nicely:

Theorem 1.6.2. **(a)** We have $(f+g)' = f' + g'$ for all f, g.

(b) The same holds for (summable) infinite sums.

(c) We have $(cf)' = cf'$ for any $c \in K$ and $f \in K[[x]]$.

(d) We have $(fg)' = f'g + fg'$ for any $f, g \in K[[x]]$.

(e) If $f, g \in K[[x]]$ are such that g is invertible, then

$$\left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}.$$

(f) For any $g \in K[[x]]$ and any $n \in \mathbb{N}$, we have $(g^n)' = ng^{n-1}g'$.

(g) Given two FPSs f, g, we have

$$(f \circ g)' = (f' \circ g) \cdot g'.$$

(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.

Proof. See notes. □

In the HW, you will see the inverse operation to differentiation.

1.7. Exponentials and logarithms

Convention 1.7.1. Throughout this section, we assume that K is a commutative $\mathbb{Q}$-algebra (i.e., we can divide by $1, 2, 3, \ldots$ in K).

Definition 1.7.2. Define three FPSs $\exp$, $\overline{\log}$ and $\overline{\exp}$ in $K[[x]]$ by

$$\begin{aligned} \exp &:= \sum_{n \in \mathbb{N}} \frac{1}{n!} x^n, \\ \overline{\log} &:= \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} x^n; \\ \overline{\exp} &:= \exp - 1 = \sum_{n \geq 1} \frac{1}{n!} x^n. \end{aligned}$$

These FPSs are mimicking the complex functions $\exp z$, $\log(1+z)$ and $\exp z - 1$. (The shift by 1 is to "center" them at 0.) From complex analysis, you know that $\exp \circ \log = \log \circ \exp = \mathrm{id}$ as functions. It would be nice if the same held for FPSs, i.e., if we had

$$\overline{\exp} \circ \overline{\log} = \overline{\log} \circ \overline{\exp} = x.$$

This is indeed true but not very easy to prove. The "short" proof relies on a general principle saying that an equality of FPSs that converge in a circle around 0 can be proved by proving that the respective functions are equal. But I want to avoid any use of analysis here, so I prefer to walk this path by foot. The main tool is:

Proposition 1.7.3. 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

$$\left(\overline{\log} \circ g\right)' = \frac{g'}{1+g}.$$

Proof. Easy. □

Using this proposition, it is not hard to prove:

Theorem 1.7.4. We have

$$\overline{\exp} \circ \overline{\log} = \overline{\log} \circ \overline{\exp} = x.$$

Proof. See the notes. □

Using the FPSs exp and $\overline{\log}$, we can define actual exponential and logarithm **maps:**

Definition 1.7.5. (a) We let

$$K[[x]]_0 = \left\{\text{FPSs } f \in K[[x]] \mid \left[x^0\right] f = 0\right\} \qquad \text{and}$$
$$K[[x]]_1 = \left\{\text{FPSs } f \in K[[x]] \mid \left[x^0\right] f = 1\right\}.$$

(b) We define two maps

$$\begin{aligned} \operatorname{Exp} : K[[x]]_0 &\to K[[x]]_1, \\ g &\mapsto \exp \circ g \end{aligned}$$

and

$$\begin{aligned} \operatorname{Log} : K[[x]]_1 &\to K[[x]]_0, \\ f &\mapsto \overline{\log} \circ (f-1). \end{aligned}$$

Theorem 1.7.6. The maps Exp and Log are well-defined and are mutually inverse group isomorphisms between the groups $(K[[x]]_0, +, 0)$ and $(K[[x]]_1, \cdot, 1)$.

Proof. See the notes.

Well-definedness is easy. "Mutually inverse" follows from $\overline{\exp} \circ \overline{\log} = \overline{\log} \circ \overline{\exp} = x$. Remains to show that they are group isomorphisms. It suffices to prove that $\exp \circ (f+g) = (\exp \circ f) \cdot (\exp \circ g)$. This is not hard to check by just plugging things into $\exp = \sum\limits_{n \in \mathbb{N}} \dfrac{1}{n!} x^n$ and simplifying using the binomial formula. □

A consequence of this theorem is that (at least when K is a $\mathbb{Q}$-algebra – e.g., a field of characteristic 0) the additive structure and the multiplicative structure of FPSs are "more or less equivalent", meaning that one can be reduced to the other.

Next time we will see how to define fractional powers like $(1+x)^{1/2}$ using this observation.

1.8. Non-integer powers

Let us now introduce non-integer powers in order to make sense of the $\sqrt{1-4x}$ in Example 2.

1.8.1. Definition

> *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 the following:

- This definition should not conflict with our existing notion of f^c for $c \in \mathbb{N}$. (Remember: $f^c = \underbrace{ff \cdots f}_{c \text{ times}}$ in this case.)
- Rules of exponents should hold: i.e., we should have
$$f^{a+b} = f^a f^b, \qquad (fg)^a = f^a g^a, \qquad (f^a)^b = f^{ab}.$$
- For n a positive integer, $f^{1/n}$ should be an n-th root of f. (This actually follows from the previous two requirements.)

Clearly, we cannot solve the above problem in full generality:

- We can never define 0^{-1} unless K is trivial.
- The power $x^{1/2}$ cannot be defined unless K is trivial. (This is a HW exercise, although it is very easy when K is a field.)
- Even the power $(-1)^{1/2}$ is not always defined, since K might fail to contain a square root of -1.

However, all we want to make sense of is $\sqrt{1-4x}$, so let us restrict ourselves to FPSs whose constant term is 1. So we restrict ourselves to the more realistic 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 $c \in K$.

(Recall that $K[[x]]_1 = \{\text{FPSs with constant term } 1\}$.)

Note that we also want f^c belong to $K[[x]]_1$.

In full generality, this is still too much to ask. Indeed, for $K = \mathbb{Z}/2$, we cannot define $(1+x)^{1/2}$, since $1+x$ has no square root (also a HW exercise).

However, if we assume 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 hold for arbitrary exponents. Subsequently, we define

$$f^c := (1+x)^c [f-1] \qquad \text{for any } f \in K[[x]]_1 \text{ and } c \in K.$$

Thus, $(1+g)^c = \sum\limits_{k\in\mathbb{N}} \dbinom{c}{k} g^k$ holds for any $g \in K[[x]]_0$.

This clearly defines f^c. But we need a lot more work to prove that the rules of exponents are satisfied. Some of this is done in Loehr's book *Bijective Combinatorics*, but I don't want to do it this way.

2nd solution: Recall the mutually inverse group isomorphisms

$$\begin{aligned}\operatorname{Exp} &: (K[[x]]_0, +, 0) \to (K[[x]]_1, \cdot, 1),\\ \operatorname{Log} &: (K[[x]]_1, \cdot, 1) \to (K[[x]]_0, +, 0).\end{aligned}$$

Thus, for any $f \in K[[x]]_1$ and any $c \in \mathbb{Z}$, the equation

$$\operatorname{Log}(f^c) = c \operatorname{Log} f.$$

This suggests that we define f^c for all $c \in K$ by the same equation. In other words, we define f^c by

$$f^c := \operatorname{Exp}(c \operatorname{Log} f) \qquad \text{for all } c \in K.$$

Let us do this:

Definition 1.8.1. Assume that K is a commutative $\mathbb{Q}$-algebra. Let $f \in K[[x]]_1$ and $c \in K$. Then, we define an FPS

$$f^c := \operatorname{Exp}(c \operatorname{Log} f) = \exp \circ \left(c \cdot \overline{\log} \circ (f-1)\right).$$

As we already explained, this definition does give $\underbrace{ff\cdots f}_{c \text{ times}}$ when $c \in \mathbb{N}$, and f^c when $c \in \mathbb{Z}$. It furthermore makes the rules of exponents hold:

Theorem 1.8.2. Assume that K is a commutative $\mathbb{Q}$-algebra. Then, for any $a, b \in K$ and any $f, g \in K[[x]]_1$, 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 (HW). □

Now, $\sqrt{1-4x}$ makes perfect sense (defined as $(1-4x)^{1/2}$), and the quadratic formula for solving a quadratic equation can be used with FPSs (with the same proof).

1.8.2. The Newton binomial formula for arbitrary exponents

Unfortunately, Example 2 is not justified yet. Having defined f^c using Exp and Log, we have not guaranteed that the Newton binomial formula is true, so we need to prove it. Let us do it now:

Theorem 1.8.3 (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 an important technique that appears all over abstract algebra.

Proof. The definition of Log yields $\operatorname{Log}(1+x) = \overline{\log} \circ ((1+x)-1) = \overline{\log} \circ x = \overline{\log}$.

Now, let us just blunlty compute $(1+x)^c$ using our definition: Let $\mathbb{P} = \{1,2,3,\ldots\}$. Then,

$$\begin{aligned}
(1+x)^c &= \operatorname{Exp}(c \operatorname{Log}(1+x)) \\
&= \operatorname{Exp}\left(c\,\overline{\log}\right) \\
&= \exp \circ \left(c\,\overline{\log}\right) \\
&= \exp \circ \left(c \sum_{n \geq 1} \frac{(-1)^{n-1}}{n} x^n\right) \\
&= \exp \circ \left(\sum_{n \geq 1} \frac{(-1)^{n-1}}{n} c x^n\right) \\
&= \sum_{m \in \mathbb{N}} \frac{1}{m!} \left(\sum_{n \geq 1} \frac{(-1)^{n-1}}{n} c x^n\right)^m .
\end{aligned}$$

Now, fix $m \in \mathbb{N}$. We shall expand the m-th power in this sum. Then,

$$\begin{aligned}
&\left(\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} cx^n\right)^m \\
&= \left(\sum_{n\in\mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n\right)^m \\
&= \underbrace{\left(\sum_{n\in\mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n\right)\left(\sum_{n\in\mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n\right)\cdots\left(\sum_{n\in\mathbb{P}} \frac{(-1)^{n-1}}{n} cx^n\right)}_{m \text{ times}} \\
&= \sum_{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m} \left(\frac{(-1)^{n_1-1}}{n_1} cx^{n_1}\right)\left(\frac{(-1)^{n_2-1}}{n_2} cx^{n_2}\right)\cdots\left(\frac{(-1)^{n_m-1}}{n_m} cx^{n_m}\right) \\
&= \sum_{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m} \frac{(-1)^{(n_1+n_2+\cdots+n_m)-m}}{n_1 n_2\cdots n_m} c^m x^{n_1+n_2+\cdots+n_m} \\
&= \sum_{k\in\mathbb{N}} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2\cdots n_m} c^m x^k.
\end{aligned}$$

We have proved this formula for each $m \in \mathbb{N}$.
Now, our above computation becomes

$$\begin{aligned}
(1+x)^c &= \sum_{m\in\mathbb{N}} \frac{1}{m!} \underbrace{\left(\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} cx^n\right)^m}_{= \sum_{k\in\mathbb{N}} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2\cdots n_m} c^m x^k} \\
&= \sum_{m\in\mathbb{N}} \frac{1}{m!} \sum_{k\in\mathbb{N}} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2\cdots n_m} c^m x^k \\
&= \sum_{k\in\mathbb{N}} \left(\sum_{m\in\mathbb{N}} \frac{1}{m!} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2\cdots n_m} c^m\right) x^k.
\end{aligned}$$

Now, let $k \in \mathbb{N}$. We rewrite the middle sum as a finite sum, as follows: We define a **composition** of k to mean a tuple $(n_1, n_2, \ldots, n_m) \in \mathbb{P}^m$ of positive integers satisfying $n_1 + n_2 + \cdots + n_m = k$. (For example, $(1, 3, 1)$ is a composition of 5.) Let $\operatorname{Comp}(k)$ denote the set of all compositions of k. This set $\operatorname{Comp}(k)$ is clearly finite (and its size we will find soon). Now,

$$\begin{aligned}
&\sum_{m\in\mathbb{N}} \frac{1}{m!} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m \\
&= \sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m,
\end{aligned}$$

and the RHS here is a finite sum.

So we have proved this equality for each $k \in \mathbb{N}$. Thus, our above computation becomes

$$\begin{aligned}
(1+x)^c &= \sum_{k\in\mathbb{N}} \left(\sum_{m\in\mathbb{N}} \frac{1}{m!} \sum_{\substack{(n_1,n_2,\ldots,n_m)\in\mathbb{P}^m;\\ n_1+n_2+\cdots+n_m=k}} \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m \right) x^k \\
&= \sum_{k\in\mathbb{N}} \left(\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m \right) x^k.
\end{aligned}$$

We must prove that this equals $\sum\limits_{k\in\mathbb{N}} \dbinom{c}{k} x^k$. Equivalently, we must prove that

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m = \binom{c}{k}$$

for each $k \in \mathbb{N}$.

Thus, we have reduced our original goal (which was to prove $(1+x)^c = \sum\limits_{k\in\mathbb{N}} \dbinom{c}{k} x^k$) to the auxiliary goal of proving this equality

$$\sum_{(n_1,n_2,\ldots,n_m)\in\operatorname{Comp}(k)} \frac{1}{m!} \cdot \frac{(-1)^{k-m}}{n_1 n_2 \cdots n_m} c^m = \binom{c}{k}$$

for each $k \in \mathbb{N}$.

This auxiliary goal is nicer in one regard: It is a polynomial identity in c (that is, an equality between two polynomial functions of c) for each given k. Thus, by the polynomial identity trick, in order to prove it for each $c \in K$, it suffices to show it for infinitely many integers c. So we only need to prove our equality for $c \in \mathbb{N}$.

But proving it for $c \in \mathbb{N}$ is easy: We can transform our equality back into the FPS equality $(1+x)^c = \sum\limits_{k\in\mathbb{N}} \dbinom{c}{k} x^k$, which is obvious for $c \in \mathbb{N}$. So we are done.

(See the notes for more detail.) □

A summary of the weird method that we just used:

- We had to prove a rather abstract statement.
- We translated it into an awkward but more concrete statement.
- We then argued that this concrete statement is a polynomial identity, and thus needs only to be proved in the special case when $c \in \mathbb{N}$.
- To prove it in this case, we translated it back into the abstract statement we started with, which turned to be easy for $c \in \mathbb{N}$.

Now Example 2 is fully justified.

See the notes (§3.8.3) for another application of the generalized Newton formula.

1.9. Integer compositions

1.9.1. Compositions

Next, let us count certain nice combinatorial objects called **compositions**. This can all be done combinatorially (see my Math 222 notes), but it also makes for a nice example of generating functions being useful, so I will do it algebraically.

Definition 1.9.1. **(a)** An **(integer) composition** means a (finite) tuple of positive integers.

(b) The **size** of a composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ means the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_m$. We denote it $|\alpha|$.

(c) The **length** of a composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ means k. We denote it $\ell(\alpha)$.

(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 1.9.2. The tuple $(3, 8, 6)$ is a composition of 17 into 3 parts, since its length is 3 and its size is $3 + 8 + 6 = 17$.

Two natural questions:

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 ?

Let us use generating functions to answer question 2.

Approach to question 2. Fix k, but don't fix n. Let

$$a_{n,k} := (\text{\# of compositions of } n \text{ into } k \text{ parts}).$$

We want to find $a_{n,k}$. We define the generating function

$$A_k := \sum_{n \in \mathbb{N}} a_{n,k} x^n = (a_{0,k}, a_{1,k}, a_{2,k}, \ldots) \in \mathbb{Q}[[x]].$$

Let us set $\mathbb{P} := \{1, 2, 3, \ldots\}$. Then, a composition of n into k parts is nothing but a k-tuple $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k$ with $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$. Hence,

$$a_{n,k} = \sum_{\substack{(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{P}^k; \\ \alpha_1 + \alpha_2 + \cdots + \alpha_k = n}} 1.$$

Thus,

$$\begin{aligned}
A_k &= \sum_{n\in\mathbb{N}} a_{n,k}x^n = \sum_{n\in\mathbb{N}} \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\mathbb{P}^k;\\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}} x^n \\
&= \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\mathbb{P}^k} x^{\alpha_1+\alpha_2+\cdots+\alpha_k} = \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\mathbb{P}^k} x^{\alpha_1}x^{\alpha_2}\cdots x^{\alpha_k} \\
&= \left(\sum_{\alpha_1\in\mathbb{P}} x^{\alpha_1}\right)\left(\sum_{\alpha_2\in\mathbb{P}} x^{\alpha_2}\right)\cdots\left(\sum_{\alpha_k\in\mathbb{P}} x^{\alpha_k}\right) \\
&= \left(\sum_{\alpha\in\mathbb{P}} x^{\alpha}\right)\left(\sum_{\alpha\in\mathbb{P}} x^{\alpha}\right)\cdots\left(\sum_{\alpha\in\mathbb{P}} x^{\alpha}\right) \\
&= \left(\sum_{\alpha\in\mathbb{P}} x^{\alpha}\right)^k = \left(x^1+x^2+x^3+\cdots\right)^k \\
&= x^k\left(\underbrace{x^0+x^1+x^2+\cdots}_{=\dfrac{1}{1-x}}\right)^k = x^k\left(\frac{1}{1-x}\right)^k \\
&= x^k\left(1-x\right)^{-k} = x^k\sum_{j\in\mathbb{N}}(-1)^j\binom{-k}{j}x^j \\
&\qquad \left(\begin{array}{c}\text{since substituting } -x \text{ for } x \text{ into the}\\ \text{generalized Newton formula}\\ (1+x)^{-k} = \sum\limits_{j\in\mathbb{N}}\dbinom{-k}{j}x^j \\ \text{yields } (1-x)^{-k} = \sum\limits_{j\in\mathbb{N}}(-1)^j\dbinom{-k}{j}x^j\end{array}\right) \\
&= \sum_{j\in\mathbb{N}}(-1)^j\binom{-k}{j}x^{k+j} = \sum_{\substack{n\in\mathbb{N};\\ n\geq k}}(-1)^{n-k}\binom{-k}{n-k}x^n.
\end{aligned}$$

Comparing coefficients, we find

$$a_{n,k} = (-1)^{n-k}\binom{-k}{n-k}$$

for each $n \in \mathbb{N}$ satisfying $n \geq k$. We can simplify this further:

$$\begin{aligned}
a_{n,k} &= (-1)^{n-k} \binom{-k}{n-k} \\
&= \underbrace{(-1)^{n-k} (-1)^{n-k}}_{=1} \underbrace{\binom{n-k-(-k)-1}{n-k}}_{=\binom{n-1}{n-k}} \qquad \text{(by upper negation)} \\
&= \binom{n-1}{n-k}.
\end{aligned}$$

So the answer to question 2 is

$$a_{n,k} = \binom{n-1}{n-k} \qquad \text{for each } n \in \mathbb{N} \text{ satisfying } n \geq k.$$

We can easily see that this also holds for $n < k$ (since $0 = 0$).

If $n > 0$, then we can rewrite $\binom{n-1}{n-k}$ as $\binom{n-1}{k-1}$ by the symmetry of Pascal's triangle. Thus:

Theorem 1.9.3. Let $n, k \in \mathbb{N}$. Then, the # of compositions of n into k parts (= k-tuples of positive integers summing up to n) is

$$\binom{n-1}{n-k} = \begin{cases} \binom{n-1}{k-1}, & \text{if } n > 0; \\ \delta_{k,0}, & \text{if } n = 0. \end{cases}$$

(Here, $\delta_{u,v}$ is the Kronecker delta, i.e., the number 1 if $u = v$ and the number 0 otherwise.)

This theorem can be proved combinatorially as well (see, e.g., Math 222).

We can also count compositions of all lengths taken together:

Theorem 1.9.4. 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. By the previous theorem, this # is

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n-1}{n-k} &= \text{(the sum of the } n-1\text{-st row of Pascal's triangle)} \\
&\qquad \text{(for } n > 0\text{)} \\
&= 2^{n-1}.
\end{aligned}$$

See the notes for details. □

1.9.2. Weak compositions

Weak compositions are like compositions, except they allow 0 as an entry. In other words:

Definition 1.9.5. **(a)** An **(integer) weak composition** means a (finite) tuple of nonnegative integers.

(b) The **size** of a weak composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ means the sum $\alpha_1 + \alpha_2 + \cdots + \alpha_m$. We denote it $|\alpha|$.

(c) The **length** of a weak composition $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ means k. We denote it $\ell(\alpha)$.

(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.

For instance, the tuple $(3, 0, 1, 2)$ is a weak composition of 6 into 4 parts.

How many weak compositions does a given $n \in \mathbb{N}$ have? Infinitely many, since (n), $(n, 0)$, $(n, 0, 0)$, ... all are included. But if we restrict ourselves to k parts for a given k, we get a finite number:

Theorem 1.9.6. Let $n, k \in \mathbb{N}$. Then, the # of weak compositions of n into k parts is

$$\binom{n+k-1}{n} = \begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ \delta_{n,0}, & \text{if } k = 0. \end{cases}$$

Proof. If $(a_1, a_2, \ldots, a_k)$ is a weak composition of n into k parts, then

$$(a_1 + 1,\ a_2 + 1,\ \ldots,\ a_k + 1)$$

is a composition of $n + k$ into k parts. Conversely, if $(b_1, b_2, \ldots, b_k)$ is a composition of $n + k$ into k parts, then

$$(b_1 - 1,\ b_2 - 1,\ \ldots,\ b_k - 1)$$

is a weak composition of n into k parts. So we get a bijection

$$\begin{aligned} &\text{from } \{\text{weak compositions of } n \text{ into } k \text{ parts}\} \\ &\text{to } \{\text{compositions of } n + k \text{ into } k \text{ parts}\}. \end{aligned}$$

Hence, by the bijection principle, we have

$$\begin{aligned}
&|\{\text{weak compositions of } n \text{ into } k \text{ parts}\}| \\
&= |\{\text{compositions of } n+k \text{ into } k \text{ parts}\}| \\
&= \binom{n+k-1}{n+k-k} \qquad \text{(by one of the previous theorems)} \\
&= \binom{n+k-1}{n}.
\end{aligned}$$

Remains to prove that this also equals

$$\begin{cases} \dbinom{n+k-1}{k-1}, & \text{if } k > 0; \\ \delta_{n,0}, & \text{if } k = 0. \end{cases}$$

For $k > 0$, this follows from the symmetry of Pascal's triangle. For $k = 0$, this is clear by inspection. □

Remark: We can also count weak compositions of n into k parts by removing all the 0's, so that a composition of n into ℓ parts for some $\ell \leq k$ remains. Let's see what this gives us.

Thus, a weak composition $(a_1, a_2, \ldots, a_k)$ of n into k parts is uniquely determined by

- the number ℓ of its nonzero entries;
- the positions of its nonzero entries (forming an ℓ-element subset of $\{1, 2, \ldots, k\}$);
- a composition of n into ℓ parts.

The number of ways to make these choices is

$$\sum_{\ell=0}^{k} \binom{k}{\ell} \binom{n-1}{n-\ell}.$$

So this is another formula for the # of weak compositions of n into k parts. Comparing it with the formula $\dbinom{n+k-1}{n}$, we obtain the identity

$$\binom{n+k-1}{n} = \sum_{\ell=0}^{k} \binom{k}{\ell} \binom{n-1}{n-\ell}.$$

This is the Chu–Vandermonde identity for k and $n-1$ (up to a simple change of summation range, which is allowed since $\dbinom{k}{\ell} = 0$ for all $\ell > k$).

1.9.3. Weak compositions with entries from $\{0, 1, \ldots, p-1\}$

We can vary our counting problems somewhat furhter.

Let us fix three nonnegative integers n, k and p. We now look for the # of k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1, \ldots, p-1\}^k$ such that $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$. In other words, we look for the # of 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 above, 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

$$w_{n,k,p} = \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k) \in \{0,1,\ldots,p-1\}^k; \\ \alpha_1+\alpha_2+\cdots+\alpha_k = n}} 1.$$

Hence,

$$\begin{aligned}
W_{k,p} &= \sum_{n\in\mathbb{N}} \sum_{\substack{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k;\\ \alpha_1+\alpha_2+\cdots+\alpha_k=n}} x^n \\
&= \sum_{(\alpha_1,\alpha_2,\ldots,\alpha_k)\in\{0,1,\ldots,p-1\}^k} x^{\alpha_1+\alpha_2+\cdots+\alpha_k} \\
&= \left(\sum_{\alpha_1=0}^{p-1} x^{\alpha_1}\right)\left(\sum_{\alpha_2=0}^{p-1} x^{\alpha_2}\right)\cdots\left(\sum_{\alpha_k=0}^{p-1} x^{\alpha_k}\right) \\
&= \left(\sum_{\alpha=0}^{p-1} x^{\alpha}\right)^k = \left(\frac{1-x^p}{1-x}\right)^k \\
&\qquad\qquad \left(\text{since } \sum_{\alpha=0}^{p-1} x^\alpha = x^0+x^1+\cdots+x^{p-1} = \frac{1-x^p}{1-x}\right) \\
&= \left(1-x^p\right)^k \left(1-x\right)^{-k} \\
&= \left(\sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} \underbrace{(x^p)^j}_{=x^{pj}}\right)\left(\sum_{i\in\mathbb{N}} (-1)^i \binom{-k}{i} x^i\right) \\
&\qquad\qquad \left(\begin{array}{c}\text{here, we used Newton's binomial formula}\\ \text{to expand } (1-x^p)^k \text{ and } (1-x)^{-k}\end{array}\right) \\
&= \sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} x^{pj} \underbrace{(-1)^i \binom{-k}{i}}_{\substack{=\binom{i+k-1}{i}\\ \text{(by upper negation)}}} x^i \\
&= \sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} x^{pj} \binom{i+k-1}{i} x^i \\
&= \sum_{i\in\mathbb{N}} \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} \binom{i+k-1}{i} x^{i+pj}.
\end{aligned}$$

Comparing the x^n-coefficient on both sides of this equality, we obtain

$$\begin{aligned} w_{n,k,p} &= \sum_{i\in\mathbb{N}} \sum_{\substack{j\in\mathbb{N};\\ i+pj=n}} (-1)^j \binom{k}{j} \binom{i+k-1}{i} \\ &= \sum_{\substack{j\in\mathbb{N};\\ pj\leq n}} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj} \\ &= \sum_{j\in\mathbb{N}} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj} \\ &= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj}. \end{aligned}$$

So we have proved:

Theorem 1.9.7. Let $n, k, p \in \mathbb{N}$. Then, the # of k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1, \ldots, p-1\}^k$ satisfy $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ is

$$\sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-pj+k-1}{n-pj}.$$

This sum cannot be simplified in general. However, the particular case $p = 2$ is worth mentioning, because in this case there is a much simpler answer. Namely, I claim that the # of k-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k) \in \{0, 1\}^k$ satisfy $\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ is $\binom{k}{n}$, because such a k-tuple is uniquely determined by the positions of its n many 1's. Comparing these two answers, we obtain a nice identity:

Corollary 1.9.8. Let $n, k \in \mathbb{N}$. Then,

$$\binom{k}{n} = \sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-2j+k-1}{n-2j}.$$

1.10. x^n-equivalence

We return to general properties of FPSs.

Definition 1.10.1. 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

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

In other words, $f \overset{x^n}{\equiv} g$ if and only if the first $n+1$ coefficients of f and g agree.

Thus, $\overset{x^n}{\equiv}$ is a binary relation on the set $K[[x]]$. We will call it x^n-**equivalence**.

Example 1.10.2. (a) We have

$$\frac{1}{1-x} \overset{x^4}{\equiv} 1 + x + x^2 + x^3 + x^4.$$

(b) We have

$$(1+x)^3 \overset{x^1}{\equiv} \frac{1}{1-3x},$$

since

$$(1+x)^3 = 1 + 3x + 3x^2 + x^3;$$
$$\frac{1}{1-3x} = 1 + 3x + 9x^2 + \cdots .$$

But $(1+x)^3 \overset{x^2}{\not\equiv} \dfrac{1}{1-3x}$ unless $3 = 9$ in K.

(c) If $f \in K[[x]]$ is any FPS, and if $n \in \mathbb{N}$, then there exists a polynomial $p \in K[x]$ of degree $\leq n$ such that $f \overset{x^n}{\equiv} p$. Explicitly:

$$p = \sum_{k=0}^{n} \left(\left[x^k \right] f \right) \cdot x^k.$$

The relation $f \overset{x^n}{\equiv} g$ is also written

- as $f = g + o(x^n)$ (this comes from thinking of $x^{n+1}, x^{n+2}, \ldots$ as being "small" in comparison to x^n, which makes sense if you think of x as a small complex number);

- as $f \equiv g \bmod x^{n+1}$ (this comes from the fact that $f \overset{x^n}{\equiv} g$ if and only if $f - g$ is a multiple of x^{n+1}).

The relation $\overset{x^n}{\equiv}$ has all the nice properties of modular congruence that you would expect:

- It is an equivalence relation (i.e., reflexive, transitive and symmetric).
- It respects addition, subtraction, multiplication, scaling and inversion. For example, if $a \overset{x^n}{\equiv} b$ and $c \overset{x^n}{\equiv} d$, then $ac \overset{x^n}{\equiv} bd$. Respecting inversion means that if $a, b \in K[[x]]$ are invertible, and $a \overset{x^n}{\equiv} b$, then $a^{-1} \overset{x^n}{\equiv} b^{-1}$.
- It even respects composition: If $a, b, c, d \in K[[x]]$ satisfy $a \overset{x^n}{\equiv} b$ and $c \overset{x^n}{\equiv} d$ and $[x^0]\, c = 0$ and $[x^0]\, d = 0$, then $a \circ c \overset{x^n}{\equiv} b \circ d$. (The "constant term 0" requirement is important here: Two polynomials a and b may satisfy $a \overset{x^n}{\equiv} b$ but $a \circ 1 \overset{x^n}{\not\equiv} b \circ 1$.)

All of this is proved in the notes; none of this is hard.

1.11. Infinite products

We have made sense of infinite sums. Now we shall introduce infinite products of FPSs. First, an example.

1.11.1. An example

The following argument is due to Euler in 1748.

Assume for now that the infinite product

$$\prod_{i\in\mathbb{N}} \left(1 + x^{2^i}\right) = \left(1 + x^1\right)\left(1 + x^2\right)\left(1 + x^4\right)\left(1 + x^8\right)\cdots$$

in the ring $K[[x]]$ is meaningful, and that such products behave well. Can we simplify it?

We can observe

$$\begin{aligned}
\prod_{i\in\mathbb{N}} \left(1 + x^{2^i}\right) &= \left(1 + x^1\right)\left(1 + x^2\right)\left(1 + x^4\right)\left(1 + x^8\right)\cdots \\
&= \frac{1-x^2}{1-x^1} \cdot \frac{1-x^4}{1-x^2} \cdot \frac{1-x^8}{1-x^4} \cdot \frac{1-x^{16}}{1-x^8} \cdot \cdots \\
&\qquad \left(\text{since } 1 + x^{2^i} = \frac{1 - x^{2^{i+1}}}{1 - x^{2^i}} \text{ for each } i\right) \\
&= \frac{1}{1-x^1} \qquad \left(\begin{array}{c}\text{by the infinite telescope principle,}\\ \text{since each numerator cancels the}\\ \text{next denominator}\end{array}\right) \\
&= \frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots .
\end{aligned}$$

On the other hand, let us expand $\prod\limits_{i\in\mathbb{N}} \left(1+x^{2^i}\right)$. It is well-known (and easy to check) that finite products of the form $\prod\limits_{i=0}^{m} (1+a_i)$ can be expanded by the formula

$$\begin{aligned}\prod_{i=0}^{m} (1+a_i) &= 1 + a_0 + a_1 + \cdots + a_m \\ &\qquad + a_0a_1 + a_0a_2 + \cdots + a_{m-1}a_m \\ &\qquad + a_0a_1a_2 + \cdots \\ &\qquad + \cdots \\ &\qquad + a_0a_1\cdots a_m \\ &= \sum_{i_1<i_2<\cdots<i_k\leq m} a_{i_1}a_{i_2}\cdots a_{i_k},\end{aligned}$$

where the sum ranges over all choices of k elements $i_1 < \cdots < i_k$ from $\{0,1,\ldots,m\}$. Let us assume that the same rule applies to infinite products:

$$\prod_{i\in\mathbb{N}} (1+a_i) = \sum_{i_1<i_2<\cdots<i_k} a_{i_1}a_{i_2}\cdots a_{i_k}.$$

Hence,

$$\prod_{i\in\mathbb{N}} \left(1+x^{2^i}\right) = \sum_{i_1<i_2<\cdots<i_k} x^{2^{i_1}}x^{2^{i_2}}\cdots x^{2^{i_k}} = \sum_{i_1<i_2<\cdots<i_k} x^{2^{i_1}+2^{i_2}+\cdots+2^{i_k}}.$$

Compare this with

$$\prod_{i\in\mathbb{N}} \left(1+x^{2^i}\right) = 1 + x + x^2 + x^3 + \cdots.$$

We get

$$\sum_{i_1<i_2<\cdots<i_k} x^{2^{i_1}+2^{i_2}+\cdots+2^{i_k}} = 1 + x + x^2 + x^3 + \cdots.$$

Comparing x^n-coefficients on both sides, we see that each $n \in \mathbb{N}$ satisfies

$$\left(\text{\# of ways to write } n \text{ as } 2^{i_1} + 2^{i_2} + \cdots + 2^{i_k} \text{ with } i_1 < i_2 < \cdots < i_k\right) \\ = 1.$$

In other words, each $n \in \mathbb{N}$ can be written uniquely as $2^{i_1} + 2^{i_2} + \cdots + 2^{i_k}$ with $i_1 < i_2 < \cdots < i_k$.

This is just the uniqueness of base-2 representation of nonnegative integers.

1.11.2. A rigorous definition

Recall that infinite sums of FPSs were defined coefficientwise:

$$\left[x^n\right]\left(\sum_{i\in I}\mathbf{a}_i\right) = \underbrace{\sum_{i\in I}\left[x^n\right]\mathbf{a}_i}_{\text{an essentially finite sum}} .$$

Alas, we cannot do the same for infinite products, since products (even finite) of FPSs are not coefficientwise. A given coefficient of a product $\mathbf{ab}$ is not determined by the corresponding coefficients of $\mathbf{a}$ and $\mathbf{b}$ alone. But it is still determined by finitely many coefficients of $\mathbf{a}$ and $\mathbf{b}$:

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

For infinite products, we expect a similar behavior: Any specific coefficient of $\prod\limits_{i\in I}\mathbf{a}_i$ should be determined by only finitely many coefficients of each of the $\mathbf{a}_i$. Let us make this more precise:

Definition 1.11.1. Let $(\mathbf{a}_i)_{i\in I}$ be a (possibly infinite) family of FPSs in $K[[x]]$. 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

$$\left[x^n\right]\left(\sum_{i\in J}\mathbf{a}_i\right) = \left[x^n\right]\left(\sum_{i\in M}\mathbf{a}_i\right).$$

(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 does not change".)

(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

$$\left[x^n\right]\left(\prod_{i\in J}\mathbf{a}_i\right) = \left[x^n\right]\left(\prod_{i\in M}\mathbf{a}_i\right).$$

(You can think of this condition as saying "If you multiply any further $\mathbf{a}_i$'s onto the product $\prod\limits_{i\in M}\mathbf{a}_i$, then the x^n-coefficient does not change".)

Example 1.11.2. **(a)** Consider the family

$$\begin{aligned}&\left(\left(x+x^2\right)^i\right)_{i\in\mathbb{N}}\\&=\left(1,\ x+x^2,\ \left(x+x^2\right)^2,\ \left(x+x^2\right)^3,\ \ldots\right).\end{aligned}$$

The subset $\{2,3\}$ of $\mathbb{N}$ determines the x^3-coefficient in the sum of this family, since all remaining $\left(x+x^2\right)^i$'s do not have an x^3-coefficient. Consequently, any finite subset of $\mathbb{N}$ that contains $\{2,3\}$ as a subset will also determine the x^3-coefficient.

(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, since 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.)

On the other hand, the subset $\{0,3\}$ of $\mathbb{N}$ does **not** determine the x^3-coefficient in the product of $\left(1+x^i\right)_{i\in\mathbb{N}}$, since

$$\underbrace{\left[x^3\right]\left(\prod_{i\in\{0,1,2,3\}}\left(1+x^i\right)\right)}_{=\left[x^3\right]\left((1+1)(1+x)\left(1+x^2\right)\left(1+x^3\right)\right)\\=4}\neq\underbrace{\left[x^3\right]\left(\prod_{i\in\{0,3\}}\left(1+x^i\right)\right)}_{=\left[x^3\right]\left((1+1)\left(1+x^3\right)\right)\\=2}.$$

Definition 1.11.3. Let $(\mathbf{a}_i)_{i\in I}$ be a family of FPSs in $K[[x]]$. 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 exists a finite subset M of I that determines this coefficient.

(b) We say that **the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$ is finitely determined** if there exists a finite subset M of I that determines this coefficient.

Using this concept, we can rewrite our definition of infinite sums:

Proposition 1.11.4. Let $(\mathbf{a}_i)_{i\in I}$ be a family of FPSs in $K[[x]]$. Then:

(a) The family $(\mathbf{a}_i)_{i\in I}$ is summable if and only if each coefficient in its sum is finitely determined.

(b) If the family $(\mathbf{a}_i)_{i\in I}$ is summable, then each coefficient of its sum $\sum\limits_{i\in I}\mathbf{a}_i$ can be computed as follows: Given $n\in\mathbb{N}$, we pick a finite subset M of I that determines the x^n-coefficient in the sum of $(\mathbf{a}_i)_{i\in I}$; then

$$[x^n]\left(\sum_{i\in I}\mathbf{a}_i\right)=[x^n]\left(\sum_{i\in M}\mathbf{a}_i\right).$$

Proof. LTTR. □

Now, we define infinite products in the same way:

Definition 1.11.5. Let $(\mathbf{a}_i)_{i\in I}$ be a family of FPSs in $K[[x]]$. Then:

(a) The family of $(\mathbf{a}_i)_{i\in I}$ is said to be **multipliable** if and only if each coefficient in its product is finitely determined (i.e., for each $n\in\mathbb{N}$, there exists a finite subset M of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$).

(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 $n\in\mathbb{N}$) is given by

$$[x^n]\left(\prod_{i\in I}\mathbf{a}_i\right)=[x^n]\left(\prod_{i\in M}\mathbf{a}_i\right),$$

where M is any finite subset of I that determines the x^n-coefficient in the product of $(\mathbf{a}_i)_{i\in I}$.

Proposition 1.11.6. 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 the choice of M.

Proof. Given two different M's, take their union. □

Proposition 1.11.7. This definition of $\prod\limits_{i\in I}\mathbf{a}_i$ agrees with the usual finite-product definition when I is finite.

Proof. Very easy. □

The above definition legitimizes our product

$$\prod_{i\in\mathbb{N}}\left(1+x^{2^i}\right)=\left(1+x^1\right)\left(1+x^2\right)\left(1+x^4\right)\left(1+x^8\right)\cdots.$$

If you want to compute the x^6-coefficient of this product, you only need to multiply its first 3 factors. In other words, the set $\{0,1,2\}$ determines the x^6-coefficient in the product of $\left(1+x^{2^i}\right)_{i\in\mathbb{N}}$. The same is true for any coefficient. So our definition makes $\prod\limits_{i\in\mathbb{N}}\left(1+x^{2^i}\right)$ well-defined.

In contrast, the product

$$\prod_{i\in\mathbb{N}}(1+ix)=(1+0x)(1+1x)(1+2x)(1+3x)\cdots$$

does not make sense, since its x^1-coefficient is not determined by any finite subset of $\mathbb{N}$. No matter how many of its factors you multiply, there will always be another that changes this coefficient.

Even the product

$$\prod_{i\in\{1,2,3,\ldots\}}\left(1+\frac{x}{i^2}\right)$$

does not make sense according to our definition, even though it would make sense in analysis.

Our reasoning that showed the multipliability of $\left(1+x^{2^i}\right)_{i\in\mathbb{N}}$ can be generalized:

Theorem 1.11.8. Let $(\mathbf{f}_i)_{i\in I}$ be a summable family of FPSs in $K[[x]]$. Then, the family $(1+\mathbf{f}_i)_{i\in I}$ is multipliable.

In other words, if $\sum\limits_{i\in I}\mathbf{f}_i$ makes sense, then so does $\prod\limits_{i\in I}(1+\mathbf{f}_i)$.

Proof idea. Since $(\mathbf{f}_i)_{i\in I}$ is summable, we know that only finitely many $\mathbf{f}_i$ have a nonzero x^0-coefficient. The set of the corresponding i's determines the x^0-coefficient of the product $\prod\limits_{i\in I}(1+\mathbf{f}_i)$.

Since $(\mathbf{f}_i)_{i\in I}$ is summable, we know that only finitely many $\mathbf{f}_i$ have a nonzero x^0-coefficient or a nonzero x^1-coefficient. The set of the corresponding i's determines the x^1-coefficient of the product $\prod\limits_{i\in I}(1+\mathbf{f}_i)$.

And so on. □

Definition 1.11.9. Let $(\mathbf{a}_i)_{i\in I}$ 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 $(\mathbf{a}_i)_{i\in I}$ (that is, determines the x^k-coefficient in this product for each $k\in\{0,1,\ldots,n\}$).

Proposition 1.11.10. Any multipliable family $(\mathbf{a}_i)_{i\in I}$ has an x^n-approximator for each $n \in \mathbb{N}$.

Proposition 1.11.11. Let $(\mathbf{a}_i)_{i\in I}$ be a multipliable family of FPSs. Let $n \in \mathbb{N}$. Let M be an x^n-approximator for $(\mathbf{a}_i)_{i\in I}$. Then,

$$\prod_{i\in I} \mathbf{a}_i \overset{x^n}{\equiv} \prod_{i\in M} \mathbf{a}_i.$$

These two propositions (which are easy to prove) show that in practice, working with infinite products boils down to finite products.

Proposition 1.11.12. Let $(\mathbf{a}_i)_{i\in I}$ be a multipliable family of invertible FPSs. Then, any subfamily of $(\mathbf{a}_i)_{i\in I}$ is multipliable.

The "invertible" condition is here because the family $(0, 1, 2, 3, \ldots)$ is multipliable, but its subfamily $(1, 2, 3, \ldots)$ is not.

Proposition 1.11.13. Products of multipliable families of FPSs satisfy the usual rules for products, as long as we assume that our families consist of invertible FPSs. In particular,

$$\begin{aligned}
\prod_{i\in I} (\mathbf{a}_i\mathbf{b}_i) &= \left(\prod_{i\in I} \mathbf{a}_i\right)\left(\prod_{i\in I} \mathbf{b}_i\right); \\
\prod_{i\in I} \mathbf{a}_i &= \left(\prod_{i\in J} \mathbf{a}_i\right)\left(\prod_{i\in K} \mathbf{a}_i\right) \qquad \text{if } I = J \cup K \text{ and } J \cap K = \varnothing; \\
\prod_{i\in I}\ \prod_{j\in J} \mathbf{a}_{(i,j)} &= \prod_{(i,j)\in I\times J} \mathbf{a}_{(i,j)} = \prod_{j\in J}\ \prod_{i\in I} \mathbf{a}_{(i,j)}.
\end{aligned}$$

The last rule here requires that $\left(\mathbf{a}_{(i,j)}\right)_{(i,j)\in I\times J}$ is multipliable.

Proof. See notes. □

These rules justify most of what we did with infinite products in the Euler example. The telescope principle is slippery, since

$$\frac{1}{2}\cdot\frac{2}{2}\cdot\frac{2}{2}\cdot\frac{2}{2}\cdot\cdots = \frac{1}{2}, \qquad \text{not 1 as the telescope would suggest.}$$

So we need to work around it. Fortunately, this is easy:

$$\begin{aligned}
&\frac{1-x^2}{1-x^1}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^8}{1-x^4}\cdot\frac{1-x^{16}}{1-x^8}\cdot\cdots\\
&=\frac{\left(1-x^2\right)\left(1-x^4\right)\left(1-x^8\right)\left(1-x^{16}\right)\cdots}{\left(1-x^1\right)\left(1-x^2\right)\left(1-x^4\right)\left(1-x^8\right)\cdots}\\
&=\frac{\left(1-x^2\right)\left(1-x^4\right)\left(1-x^8\right)\left(1-x^{16}\right)\cdots}{\left(1-x^1\right)\cdot\left(\left(1-x^2\right)\left(1-x^4\right)\left(1-x^8\right)\left(1-x^{16}\right)\cdots\right)}\\
&=\frac{1}{1-x^1}=\frac{1}{1-x}.
\end{aligned}$$

One more thing has not been justified yet: the rule

$$\prod_{i\in\mathbb{N}}\left(1+a_i\right)=\sum_{i_1<i_2<\cdots<i_k}a_{i_1}a_{i_2}\cdots a_{i_k}.$$

Let us do this now.

1.11.3. Product rules (generalized distributive laws)

Let us recall the finite product rule – i.e., how to expand a finite product of finite sums.

Proposition 1.11.14. 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,

$$\prod_{i=1}^{n}\sum_{k=1}^{m_i}p_{i,k}=\sum_{(k_1,k_2,\ldots,k_n)\in[m_1]\times[m_2]\times\cdots\times[m_n]}\prod_{i=1}^{n}p_{i,k_i}.$$

Less abstractly, this is saying that

$$\begin{aligned}
&\left(p_{1,1}+p_{1,2}+\cdots+p_{1,m_1}\right)\left(p_{2,1}+p_{2,2}+\cdots+p_{2,m_2}\right)\cdots\left(p_{n,1}+p_{n,2}+\cdots+p_{n,m_n}\right)\\
&=p_{1,1}p_{2,1}\cdots p_{n,1}+p_{1,1}p_{2,1}\cdots p_{n-1,1}p_{n,2}+\cdots+p_{1,m_1}p_{2,m_2}\cdots p_{n,m_n}.
\end{aligned}$$

Now, let us extend this proposition to finite products of infinite sums:

Proposition 1.11.15. 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 $\left(p_{i,k}\right)_{k\in S_i}$ be a summable family of FPSs in $K[[x]]$. Then,

$$\prod_{i=1}^{n}\sum_{k\in S_i}p_{i,k}=\sum_{(k_1,k_2,\ldots,k_n)\in S_1\times S_2\times\cdots\times S_n}\prod_{i=1}^{n}p_{i,k_i}.$$

In particular, the sum on the RHS is summable.

This is useful, but not sufficient for Euler's argument. Indeed, Euler has an infinite product of finite sums, not a finite product of infinite sums. This can be a bit trickier, since (e.g.) we don't want the product

$$(1+a_0)(1+a_1)(1+a_2)\cdots$$

to have the factor $a_0a_1a_2\cdots$. We also don't want

$$(1-1)(1-1)(1-1)\cdots = 1-1+1-1+1-1+1-1\pm\cdots .$$

So we have to make some requirements:

Definition 1.11.16. (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 $k_i = 0$.

Now, we can state a version of the product rule for infinite products of potentially infinite sums.

Proposition 1.11.17. Let $S_1, S_2, S_3, \ldots$ be infinitely many sets that all contain the number 0. Set

$$\overline{S} = \{(i,k) \mid i \in \{1,2,3,\ldots\} \text{ and } k \in S_i \setminus \{0\}\} .$$

For any $i \in \{1, 2, 3, \ldots\}$ and any $k \in S_i$, let $p_{i,k}$ be a FPS in $K[[x]]$. Assume that

$$p_{i,0} = 1 \qquad \text{for any } i \in \{1,2,3,\ldots\} .$$

Assume that the family $(p_{i,k})_{(i,k)\in\overline{S}}$ is summable. Then,

$$\prod_{i=1}^{\infty} \sum_{k \in S_i} p_{i,k} = \sum_{\substack{(k_1,k_2,k_3,\ldots) \in S_1 \times S_2 \times S_3 \times \cdots \\ \text{is essentially finite}}} \prod_{i=1}^{\infty} p_{i,k_i},$$

and in particular the product and the sum on the RHS are well-defined.

This finally justifies Euler's argument.

1.11.4. Another example

Here is a curious result found by Euler in 1748:

Proposition 1.11.18. We have

$$\prod_{i>0} \left(1 - x^{2i-1}\right)^{-1} = \prod_{k>0} \left(1 + x^k\right) .$$

That is,

$$\begin{aligned}&\left(1-x^1\right)^{-1}\left(1-x^3\right)^{-1}\left(1-x^5\right)^{-1}\left(1-x^7\right)^{-1}\cdots\\&=\left(1+x^1\right)\left(1+x^2\right)\left(1+x^3\right)\left(1+x^4\right)\cdots.\end{aligned}$$

Proof. For each $k>0$, we have $1+x^k=\dfrac{1-x^{2k}}{1-x^k}$. Hence,

$$\begin{aligned}\prod_{k>0}\left(1+x^k\right)&=\prod_{k>0}\frac{1-x^{2k}}{1-x^k}=\frac{\prod\limits_{k>0}\left(1-x^{2k}\right)}{\prod\limits_{k>0}\left(1-x^k\right)}\\&=\frac{\left(1-x^2\right)\left(1-x^4\right)\left(1-x^6\right)\cdots}{\left(1-x^1\right)\left(1-x^2\right)\left(1-x^3\right)\left(1-x^4\right)\cdots}\\&=\frac{1}{\left(1-x^1\right)\left(1-x^3\right)\left(1-x^5\right)\cdots}\\&\qquad\qquad\left(\text{after cancelling all } 1-x^k \text{ with } k \text{ even}\right)\\&=\frac{1}{\prod\limits_{i>0}\left(1-x^{2i-1}\right)}=\prod_{i>0}\frac{1}{1-x^{2i-1}}=\prod_{i>0}\left(1-x^{2i-1}\right)^{-1}.\end{aligned}$$

□

Let us now interpret this proposition combinatorially by expanding both products.

First,

$$\begin{aligned}&\prod_{k>0}\left(1+x^k\right)\\&=\left(1+x^1\right)\left(1+x^2\right)\left(1+x^3\right)\cdots\\&=\sum_{\substack{i_1,i_2,\ldots,i_k\in\{1,2,3,\ldots\};\\ i_1<i_2<\cdots<i_k}} x^{i_1}x^{i_2}\cdots x^{i_k}\\&=\sum_{n\in\mathbb{N}} d_n x^n,\end{aligned}$$

where d_n is the # of all strictly increasing tuples $(i_1<i_2<\cdots<i_k)$ such that $i_1+i_2+\cdots+i_k=n$. 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 their order (e.g., we count $3+4+1$ and $4+1+3$ as the same way).

Now to the LHS:

$$\begin{aligned}
&\prod_{i>0}\left(1-x^{2i-1}\right)^{-1}\\
&=\prod_{i>0}\left(1+x^{2i-1}+\left(x^{2i-1}\right)^{2}+\left(x^{2i-1}\right)^{3}+\cdots\right)\\
&\qquad\qquad\left(\begin{array}{c}\text{by substituting } x^{2i-1} \text{ for } x \text{ in}\\ (1-x)^{-1}=1+x+x^2+x^3+\cdots\end{array}\right)\\
&=\prod_{i>0}\left(1+x^{2i-1}+x^{2(2i-1)}+x^{3(2i-1)}+\cdots\right)\\
&=\left(1+x^1+x^2+x^3+\cdots\right)\\
&\qquad\left(1+x^3+x^6+x^9+\cdots\right)\\
&\qquad\left(1+x^5+x^{10}+x^{15}+\cdots\right)\\
&\qquad\cdots\\
&=\sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty\\ \text{is essentially finite}}} x^{u_1\cdot 1}x^{u_2\cdot 3}x^{u_3\cdot 5}\cdots\\
&=\sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty\\ \text{is essentially finite}}} x^{u_1\cdot 1+u_2\cdot 3+u_3\cdot 5+\cdots}\\
&=\sum_{n\in\mathbb{N}} o_n x^n,
\end{aligned}$$

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 their order. (In fact, 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.)

Now, our proposition says that

$$\prod_{k>0}\left(1+x^k\right)=\prod_{i>0}\left(1-x^{2i-1}\right)^{-1},$$

so that

$$\sum_{n\in\mathbb{N}} d_n x^n = \sum_{n\in\mathbb{N}} o_n x^n.$$

Thus, $d_n = o_n$ for each $n \in \mathbb{N}$. So we have shown the following combinatorial statement:

Theorem 1.11.19 (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 their order;
- o_n is the # of ways to write n as a sum of (not necessarily distinct) odd positive integers, without regard to their order.

Example 1.11.20. Let $n = 6$. Then, $d_n = 4$, since the ways to write 6 as a sum of distinct positive integers, without regard to their order, are

$$6 = 6 = 5 + 1 = 4 + 2 = 3 + 2 + 1.$$

Furthermore, $o_n = 4$, since the ways to write 6 as a sum of (not necessarily distinct) odd positive integers, without regard to their order, are

$$\begin{aligned} 6 &= 3 + 3 = 1 + 1 + 1 + 1 + 1 + 1 \\ &= 3 + 1 + 1 + 1 = 5 + 1. \end{aligned}$$

We will soon learn a different, combinatorial proof of this theorem.

1.12. The generating function of a weighted set

So far, we have built a theory of FPSs, but mainly as algebraic objects. We have applied them to combinatorics only via certain ad-hoc interpretations.

Now I will show a more systematic way of taking combinatorial objects to FPSs. This is a theory that goes much further than I can explain in this course – the theory of **weighted sets** (sometimes known as **combinatorial classes**).

1.12.1. A bit of theory

Definition 1.12.1. (a) A **weighted set** is a set A equipped with a function $w : A \to \mathbb{N}$, called the **weight function** of this weighted set. For each $a \in A$, the value $w(a)$ is called the **weight** of a, and is denoted $|a|$.

Usually, we will write $|a|$ instead of $w(a)$, so we won't talk about w explicitly. The weighted set (A, w) will often be written as A if the weight function w is irrelevant or obvious.

(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 $\rho : A \to B$ 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** (written $A \cong B$) if there exists an isomorphism $A \to B$.

Example 1.12.2. Let B be the weighted set of all **binary strings**, i.e., finite tuples consisting of 0's and 1's. Thus,

$$B = \{(), (0), (1), (0,0), (0,1), (1,0), (1,1), \ldots\}.$$

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 weight k (namely, 2^k). The weight generating function of B is

$$\begin{aligned} \overline{B} &= \sum_{n\in\mathbb{N}} \underbrace{(\text{\# of } a \in B \text{ having weight } n)}_{=2^n} \cdot x^n = \sum_{n\in\mathbb{N}} 2^n x^n \\ &= \sum_{n\in\mathbb{N}} (2x)^n = \frac{1}{1-2x}. \end{aligned}$$

Proposition 1.12.3. Let A and B be two isomorphic finite-type weighted sets. Then, $\overline{A} = \overline{B}$.

Proof. Obvious. □

Note that this proposition 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 are not". Formally, it is defined as the set

$$(\{0\} \times A) \cup (\{1\} \times B),$$

where we view the elements $(0,a) \in \{0\} \times A$ as clones of the respective $a \in A$, while viewing the elements $(1,b) \in \{1\} \times B$ as clones of the respective $b \in B$. This disjoint union is denoted by $A + B$, and always has size $|A| + |B|$.

Disjoint unions are not directly associative like unions are (i.e., we don't have $A + (B + C) = (A + B) + C$ as sets), but they are associative up to canonical bijection (i.e., there is a canonical bijection $A + (B + C) \to (A + B) + C$), so we can pretend that they are associative and write $A_1 + A_2 + \cdots + A_k$ when we don't care about the specific implementation of these objects.

Definition 1.12.4. Let A and B be two 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

$$|(0,a)| = |a| \qquad \text{and} \qquad |(1,b)| = |b|.$$

Proposition 1.12.5. Let A and B be two finite-type weighted sets. Then, $A + B$ is finite-type as well, and satisfies $\overline{A+B} = \overline{A} + \overline{B}$.

Proof. Easy. □

More interestingly, we can do the same for direct products (i.e., Cartesian products):

Definition 1.12.6. 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, with the weight function defined by

$$|(a,b)| = |a| + |b| .$$

Proposition 1.12.7. Let A and B be two finite-type weighted sets. Then, $A \times B$ is also finite-type, and satisfies

$$\overline{A \times B} = \overline{A} \cdot \overline{B}.$$

Proof. Finite-type is easy. To prove $\overline{A \times B} = \overline{A} \cdot \overline{B}$, we compute

$$\begin{aligned} \overline{A \times B} &= \sum_{(a,b) \in A \times B} \underbrace{\underbrace{x^{|(a,b)|}}_{= x^{|a|+|b|}}}_{= x^{|a|} x^{|b|}} = \sum_{(a,b) \in A \times B} x^{|a|} x^{|b|} \\ &= \left(\sum_{a \in A} x^{|a|} \right) \left(\sum_{b \in B} x^{|b|} \right) = \overline{A} \cdot \overline{B}. \end{aligned}$$

□

Definition 1.12.8. Let A be a weighted set. Then, A^k (for $k \in \mathbb{N}$) means the weighted set $\underbrace{A \times A \times \cdots \times A}_{k \text{ times}}$. (We are again being sloppy with associativity; all possible values are isomorphic.)

Proposition 1.12.9. Let A be a finite-type weighted set. Let $k \in \mathbb{N}$. Then, A^k is also finite-type, and satisfies $\overline{A^k} = \overline{A}^k$.

Note that the 0-th Cartesian power of A is always $A^0 = \{()\}$, with generating function 1.

1.12.2. Examples

Now let us use this theory to revisit some things we have already counted:

- Fix $k \in \mathbb{N}$, and let

  $$\begin{aligned} C_k &= \{\text{compositions of length } k\} \\ &= \{(a_1, a_2, \ldots, a_k) \mid a_1, a_2, \ldots, a_k \text{ are positive integers}\} \\ &= \mathbb{P}^k \qquad \left(\text{where } \mathbb{P} = \{1, 2, 3, \ldots\}\right). \end{aligned}$$

  This becomes a finite-type weighted set if we set

  $$\left|(a_1, a_2, \ldots, a_k)\right| = a_1 + a_2 + \cdots + a_k.$$

  What is its weight generating function $\overline{C_k}$?

  We can turn $\mathbb{P}$ itself into a weighted set, by setting $|n| = n$. Then, $C_k = \mathbb{P}^k$ not just as sets, but as weighted sets. So our last proposition yields

  $$\begin{aligned} \overline{C_k} &= \overline{\mathbb{P}^k} = \overline{\mathbb{P}}^k \\ &= \left(\frac{x}{1-x}\right)^k \qquad \left(\text{since } \overline{\mathbb{P}} = x^1 + x^2 + x^3 + \cdots = \frac{x}{1-x}\right) \\ &= \frac{x^k}{(1-x)^k}. \end{aligned}$$

  This is an equality we obtained before, but proved in a much simpler way.

- Recall Dyck paths (defined long ago) and the Catalan numbers $c_0, c_1, c_2, \ldots$. Let

  $$D = \{\text{Dyck paths from } (0,0) \text{ to } (2n,0) \text{ for some } n \in \mathbb{N}\}.$$

  This set D becomes a weighted set if we set

  $$|P| = n \qquad \text{whenever } P \text{ is a Dyck path from } (0,0) \text{ to } (2n,0).$$

  Thus,

  $$\overline{D} = \sum_{n \in \mathbb{N}} \underbrace{(\#\text{ of Dyck paths from } (0,0) \text{ to } (2n,0))}_{=c_n} \cdot x^n = \sum_{n \in \mathbb{N}} c_n x^n.$$

  This is the generating function we called $C(x)$ back in that example.

  Let us use the theory of weighted sets to compute it. We note that $D = D_{\text{triv}} \cup D_{\text{non}}$, where

  $$\begin{aligned} D_{\text{triv}} &= \{\text{trivial Dyck path}\} = \{((0,0))\}, \\ D_{\text{non}} &= D \setminus D_{\text{triv}} = \{\text{nontrivial Dyck paths}\}. \end{aligned}$$

So $D \cong D_{\text{triv}} + D_{\text{non}}$ and therefore $\overline{D} = \overline{D_{\text{triv}} + D_{\text{non}}} = \overline{D_{\text{triv}}} + \overline{D_{\text{non}}}$. Furthermore, $\overline{D_{\text{triv}}} = x^0 = 1$. To compute D_{non}, we recall that any nontrivial Dyck path π has the following structure:

- a NE-step,
- followed by a (diagonally shifted) Dyck path,
- followed by a SE-step,
- followed by another (horizontally shifted) Dyck path.

If we denote the first Dyck path here by α and the second by β, then we 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 $|(\alpha, \beta)| = |\alpha| + |\beta| = |\pi| - 1 \neq |\pi|$.

But we can fix this. Define a weighted set

$$X := \{1\}, \qquad \text{with } |1| = 1.$$

This is a one-element set, so the set $X \times D \times D$ is in bijection with $D \times D$. But as weighted sets, they are not the same, since $|(1, \alpha, \beta)| = 1 + |(\alpha, \beta)|$. So we can raise every weight in a weighted set W by 1 if we take $X \times W$. Thus, replacing $D \times D$ by $X \times D \times D$, we do obtain an isomorphism of weighted sets

$$\begin{aligned} D_{\text{non}} &\to X \times D \times D, \\ \pi &\mapsto (1, \alpha, \beta). \end{aligned}$$

Thus, $\overline{D_{\text{non}}} = \overline{X \times D \times D} = \underbrace{\overline{X}}_{=x^1=x} \cdot \underbrace{\overline{D} \cdot \overline{D}}_{=\overline{D}^2} = x\overline{D}^2$.

Now,

$$\overline{D} = \underbrace{\overline{D_{\text{triv}}}}_{=1} + \underbrace{\overline{D_{\text{non}}}}_{=x\overline{D}^2} = 1 + x\overline{D}^2.$$

This is precisely the quadratic equation $C(x) = 1 + x(C(x))^2$ that we got back in the original example.

1.12.3. Domino tilings

As another example of weight generating functions, let me count domino tilings of $2 \times n$- and $3 \times n$-rectangles. Here are the main definitions:

Definition 1.12.10. **(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 (i,j) in Cartesian coordinates.

(b) For any $n, m \in \mathbb{N}$, the shape $R_{n,m}$ (called the $n \times m$**-rectangle**) is defined to be

$$\{1,2,\ldots,n\} \times \{1,2,\ldots,m\}.$$

Geometrically, it is a rectangle of width n and height m.

(c) A **domino** means a size-2 shape of the form

$$\begin{aligned} &\{(i,j),\ (i+1,j)\} && \text{(a "horizontal domino")} && \text{or} \\ &\{(i,j),\ (i,j+1)\} && \text{(a "vertical domino")}. \end{aligned}$$

(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 $d_{n,m}$ for small values of n and m ?

The case $m = 1$ is easy:

$$d_{n,1} = \begin{cases} 1, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Actually, $d_{n,m} = 0$ whenever n and m are both odd (since $|R_{n,m}|$ is odd in this case, but a domino has even size).

Now to the case $m = 2$. We define the weighte dset

$$\begin{aligned} D &:= \{\text{domino tilings of rectangles of height } 2\} \\ &= \{\text{domino tilings of } R_{n,2} \text{ with } n \in \mathbb{N}\}. \end{aligned}$$

We define the weight of a tiling T of $R_{n,2}$ to be $|T| := n$. Thus, D is a finite-type weighted set, with generating function

$$\overline{D} = \sum_{n \in \mathbb{N}} d_{n,2} x^n.$$

To compute $\overline{D}$, we define a different weighted set that will help us. 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);
- there is at least one domino of T that lies left of ℓ, and at least one that lies right of ℓ.

A domino tiling is called **faultfree** if it is nonempty and has no faults.

> **Observation:** Any domino tiling of a height-2 rectangle can be decomposed uniuqely into a tuple of faultfree tilings (usually of smaller rectangles), by cutting it along the faults. 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 D), then

$$D \cong F^0 + F^1 + F^2 + F^3 + \cdots$$

(the RHS here is an infinite disjoint union). Thus,

$$\begin{aligned}\overline{D} &= \overline{F^0 + F^1 + F^2 + F^3 + \cdots} \\ &= \overline{F}^0 + \overline{F}^1 + \overline{F}^2 + \overline{F}^3 + \cdots \\ &= \frac{1}{1-\overline{F}}.\end{aligned}$$

Thus, if we can compute $\overline{F}$, then we can compute $\overline{D}$.

By a simple argument (see notes or whiteboard), we have $\overline{F} = x^1 + x^2 = x + x^2$. So

$$\begin{aligned}\overline{D} &= \frac{1}{1-\overline{F}} = \frac{1}{1-(x+x^2)} = \frac{1}{1-x-x^2} \\ &= 1 + 1x + 2x^2 + 3x^3 + 5x^4 + \cdots \\ &= f_1 + f_2 x + f_3 x^2 + f_4 x^3 + \cdots\end{aligned}$$

(as we proved above). So $d_{n,2} = f_{n+1}$ for each $n \in \mathbb{N}$.

Let us go a step further and compute $d_{n,3}$. Note that $d_{n,3} = 0$ whenever n is odd.

Let $\overline{D}$ be as before, but using 3 instead of 2. So $\overline{D} = \sum\limits_{n\in\mathbb{N}} d_{n,3} x^n$. Again, we can define F as before (i.e., as the weighted set of all faultfree tilings of $R_{n,3}$), and obtain

$$\overline{D} = \frac{1}{1-\overline{F}}.$$

Now what is $\overline{F}$ this time? The faultfree tilings of $R_{n,3}$ come in three types:

- **Type HHH:** All three cells of the first column are covered by horizontal dominos. This gives a fault after column 2 unless $n = 2$. So there is only one such tiling, and it has weight 2.

- **Type VH:** The top two cells of the first column are covered by a vertical domino, while the bottom cell is covered by a horizontal one. There is one such tiling for each even n.
- **Type HV:** The top cell of the first column is covered by a horizontal domino, while the bottom two cells are covered by a vertical one. There is one such tiling for each even n.

Thus,

$$\begin{aligned}\overline{F} &= \underbrace{x^2}_{\text{HHH}} + \underbrace{\left(x^2+x^4+x^6+\cdots\right)}_{\text{VH}} + \underbrace{\left(x^2+x^4+x^6+\cdots\right)}_{\text{HV}} \\ &= x^2 + 2\cdot \underbrace{\left(x^2+x^4+x^6+\cdots\right)}_{=\dfrac{x^2}{1-x^2}} = x^2 + 2\cdot \frac{x^2}{1-x^2} \\ &= \frac{3x^2-x^4}{1-x^2},\end{aligned}$$

so that

$$\begin{aligned}\overline{D} &= \frac{1}{1-\overline{F}} = \frac{1}{1-\dfrac{3x^2-x^4}{1-x^2}} = \frac{1-x^2}{1-4x^2+x^4} \\ &= 1+3x^2+11x^4+41x^6+153x^8+\cdots.\end{aligned}$$

Obviously, this shows that $d_{n,3} = 0$ when n is odd, but this is clear anyway. But it also helps us compute $d_{n,3}$ for even n, because we can decompose $\dfrac{1-x^2}{1-4x^2+x^4}$ into partial fractions and then proceed as for the Fibonacci numbers. We find

$$d_{n,3} = \frac{3+\sqrt{3}}{6}\left(2+\sqrt{3}\right)^{n/2} + \frac{3-\sqrt{3}}{6}\left(2-\sqrt{3}\right)^{n/2}$$

for any even n.

Can we compute $d_{n,m}$ for higher m's? Not that easily. Alas, $\overline{F}$ becomes more complicated for $m > 3$. However, it can be shown that $\overline{D}$ is still a rational FPS (i.e., a quotient of two polynomials) for any m. For $m \geq 6$, there seems to be no formula for $d_{n,m}$ that requires only quadratic irrationalities. As a curiosity, let me mention a different formula for $d_{n,m}$, found by Kasteleyn in 1961:

Theorem 1.12.11 (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 the references in the notes for proofs of this. You can use this formula to compute $d_{n,m}$ exactly, using cyclotomic arithmetic. In particular, this has been used to show that

$$d_{8,8} = 12\ 988\ 816.$$

1.13. Limits of FPSs

I shall now discuss limits of sequences of FPSs. In particular, this will give a simpler and more convenient, but less general, definition of infinite products.

We start with the stupidest kind of limit ever defined:

Definition 1.13.1. 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 $a_i = a$.

This is synonymous to "$(a_i)_{i\in\mathbb{N}}$ converges to a in the discrete topology".

If $(a_i)_{i\in\mathbb{N}}$ stabilizes to a, then we write $\lim\limits_{i\to\infty} a_i = a$ and say that a is the **limit** (aka **eventual value**) of $(a_i)_{i\in\mathbb{N}}$.

More generally, we can do this for any sequence $(a_i)_{i\geq q}$ instead of $(a_i)_{i\in\mathbb{N}}$.

For instance,

$$\lim_{i\to\infty} \left\lfloor \frac{5}{i} \right\rfloor = 0, \qquad \text{since } \left\lfloor \frac{5}{i} \right\rfloor = 0 \text{ for } i \geq 6.$$

But $\lim\limits_{i\to\infty} \dfrac{5}{i}$ does not exist by our definition.

Definition 1.13.2. 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 $[x^n] f$.

This is synonymous to "$(f_i)_{i\in\mathbb{N}}$ converges to f in the product topology, where $K[[x]]$ is regarded as $K \times K \times K \times \cdots$.

Again, we use the notation $\lim\limits_{i\to\infty} f_i$ for f, and we speak of a limit.

Again, we can do this for any $(f_i)_{i\geq q}$, not just $(f_i)_{i\in\mathbb{N}}$.

Example 1.13.3. **(a)** We have $x^i \to 0$ as $i \to \infty$. Indeed, for each $n \in \mathbb{N}$, the sequence $\left([x^n]\, x^i\right)_{i \in \mathbb{N}}$ has only one nonzero entry, and thus stabilizes to 0.

(b) We **don't** have $\dfrac{1}{i}x \to 0$ as $i \to \infty$. Indeed, the x^1-coefficients do not stabilize.

(c) We have

$$\left(1+x^1\right)\left(1+x^2\right)\cdots\left(1+x^i\right) \to \prod_{k=1}^{\infty}\left(1+x^k\right) \qquad \text{as } i \to \infty.$$

(d) It would be nice to have $\left(1+\dfrac{x}{n}\right)^n \to \exp$ as $n \to \infty$, as in real analysis. Alas, this is not the case. The x^1-coefficient stabilizes, but the x^2-coefficient does not.

Theorem 1.13.4. Let $(f_i)_{i \in \mathbb{N}}$ be a sequence of FPSs in $K[[x]]$. Assume that for each $n \in \mathbb{N}$, the sequence $([x^n]\, f_i)_{i \in \mathbb{N}}$ stabilizes to some $g_n \in K$. Then, $f_i \to \sum\limits_{n \in \mathbb{N}} g_n x^n$ as $i \to \infty$.

Proof. Obvious. □

Proposition 1.13.5. 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,

$$f_i + g_i \to f + g \qquad \text{and} \qquad f_i g_i \to fg \qquad \text{as } i \to \infty.$$

Moreover, if each g_i and also g has constant term 1, then

$$\frac{f_i}{g_i} \to \frac{f}{g} \qquad \text{as } i \to \infty.$$

Proof. Homework. □

Theorem 1.13.6. Let $(f_n)_{n \in \mathbb{N}}$ be a sequence of FPSs. Then:

(a) If $(f_n)_{n \in \mathbb{N}}$ is summable, then

$$\sum_{n=0}^{i} f_n \to \sum_{n \in \mathbb{N}} f_n \qquad \text{as } i \to \infty.$$

(b) If $(f_n)_{n \in \mathbb{N}}$ is multipliable, then

$$\prod_{n=0}^{i} f_n \to \prod_{n \in \mathbb{N}} f_n \qquad \text{as } i \to \infty.$$

Theorem 1.13.7. Each FPS is a limit of a sequence of polynomials. Indeed, if $a = \sum\limits_{n \in \mathbb{N}} a_n x^n$, then

$$\sum_{n=0}^{i} a_n x^n \to a \qquad \text{as } i \to \infty.$$

Theorem 1.13.8. Let $(f_i)_{i \in \mathbb{N}}$ be a sequence of FPSs in $K[[x]]$. Let f be an FPS such that

$$f_i \to f \qquad \text{as } i \to \infty.$$

Then,

$$f_i{}' \to f' \qquad \text{as } i \to \infty.$$

Proof. Very easy. □

1.14. Laurent power series

(See the notes for a more motivated introduction.)

Definition 1.14.1. Let $K[[x^{\pm}]]$ be the K-module $K^{\mathbb{Z}}$ of all families

$$(a_n)_{n \in \mathbb{Z}} = (\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots)$$

of elements of K. Its addition and scaling are defined entrywise:

$$(a_n)_{n \in \mathbb{Z}} + (b_n)_{n \in \mathbb{Z}} = (a_n + b_n)_{n \in \mathbb{Z}}.$$

An element of $K[[x^{\pm}]]$ will be called a **doubly infinite power series**. Later we will write such an element $(a_n)_{n \in \mathbb{Z}}$ as $\sum\limits_{n \in \mathbb{Z}} a_n x^n$.

So far, so good. Let us try to define a multiplication on $K[[x^{\pm}]]$ similarly to how we defined it for $K[[x]]$:

$$(a_n)_{n \in \mathbb{Z}} \cdot (b_n)_{n \in \mathbb{Z}} = (c_n)_{n \in \mathbb{Z}}, \qquad \text{where } c_n = \sum_{i \in \mathbb{Z}} a_i b_{n-i}.$$

Unfortunately, the sum here might fail to be well-defined, since it is infinite and there is no guarantee that it is essentially finite.

For example, $(1)_{n \in \mathbb{Z}} \cdot (1)_{n \in \mathbb{Z}} = (\infty)_{n \in \mathbb{Z}}$, which makes no sense.

There are several ways to restrict our series to ensure that the sum $\sum\limits_{i \in \mathbb{Z}} a_i b_{n-i}$ will be finite:

- One way is to require that $a_i = 0$ for all $i < 0$. The series that we get are exactly the usual FPSs in $K[[x]]$.

- Another way is to require that $a_i = 0$ for all but finitely many i. In other words, we restrict ourselves to the essentially finite families $(a_n)_{n\in\mathbb{Z}}$. Moreover, the product of an essentially finite $(a_n)_{n\in\mathbb{Z}}$ with an essentially finite $(b_n)_{n\in\mathbb{Z}}$ will be again essentially finite. Thus, they form a K-algebra. This is the K-algebra of **Laurent polynomials**.

- Yet another way (combining the two above) is to require that $a_i = 0$ for all but finitely many negative i (or, equivalently, $a_i = 0$ for all sufficiently low i). For example, we could have

  $$(a_n)_{n\in\mathbb{Z}} = \left(\underbrace{\ldots,0,0,0}_{\text{only zeroes}},5,1,0,2,-1,0,4,5,7,1,2,\ldots\right).$$

  This again gives a K-algebra. This is the K-algebra of **Laurent series** (or **Laurent power series**).

So let us summarize these as definitions:

Definition 1.14.2. Let $K[x^\pm]$ be the K-submodule of $K[[x^\pm]]$ consisting of all **essentially finite** families $(a_n)_{n\in\mathbb{Z}}$. Its elements are called **Laurent polynomials** in x over K.

We define a multiplication on $K[x^\pm]$ by

$$(a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}} = (c_n)_{n\in\mathbb{Z}}, \qquad \text{where } c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

(The sum is well-defined, since it is essentially finite.)

We define an element $x \in K[x^\pm]$ by $x = (\delta_{i,1})_{i\in\mathbb{Z}}$.

Theorem 1.14.3. This really is a commutative K-algebra, with unity $(\delta_{i,0})_{i\in\mathbb{Z}}$. The element x is invertible in this K-algebra.

This K-algebra $K[x^\pm]$ is called the **Laurent polynomial ring** in x over K. It is often denoted by $K\left[x^{\pm 1}\right]$ or $K\left[x, x^{-1}\right]$.

Proposition 1.14.4. Any doubly infinite power series $a = (a_i)_{i\in\mathbb{Z}} \in K[[x^\pm]]$ satisfies

$$a = \sum_{i\in\mathbb{Z}} a_i x^i.$$

Here, the powers x^i are taken in the Laurent polynomial ring $K[x^\pm]$, but the infinite sum $\sum\limits_{i\in\mathbb{Z}} a_i x^i$ is taken in the whole K-module $K[[x^\pm]]$. (The notion of an infinite sum is defined in $K[[x^\pm]]$ in the same way as in $K[[x]]$.)

Examples of Laurent polynomials are

- $x^3 + 3 + x^{-2}$;
- 17;
- x^{-1000};
- any polynomial.

Now to the other option of making the sum well-defined:

Definition 1.14.5. We let $K((x))$ be the subset of $K[[x^{\pm}]]$ consisting of all families $(a_i)_{i\in\mathbb{Z}}$ 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 x over K.

For instance,

1. the "series" $x^{-3} + x^{-2} + x^{-1} + x^0 + x^1 + \cdots$ belongs to $K((x))$;
2. the "series" $1 + x^{-1} + x^{-2} + x^{-3} + \cdots$ does not belong to $K((x))$;
3. the "series" $\sum\limits_{n\in\mathbb{Z}} x^n = (1)_{n\in\mathbb{Z}}$ does not belong to $K((x))$ either.

Theorem 1.14.6. The subset $K((x))$ is a K-submodule of $K[[x^{\pm}]]$. It also has a multiplication given by

$$(a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}} = (c_n)_{n\in\mathbb{Z}}, \qquad \text{where } c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

This forms a commutative K-algebra with unity $(\delta_{i,0})_{i\in\mathbb{Z}}$.

The ring $K((x))$ contains both $K[[x]]$ and $K[x^{\pm}]$ as subrings. It is therefore one of the most convenient places in which to manipulate FPSs. Its main disadvantage is the lack of substitution.

More can be said: If K is a field, then $K((x))$ is a field as well! (Homework exercise.)

One final remark: As we said, $K[[x^{\pm}]]$ is not a ring, but it is a $K[x^{\pm}]$-module! In other words, you can multiply a doubly infinite power series a by a Laurent polynomial b, again using the rule

$$(a_n)_{n\in\mathbb{Z}} \cdot (b_n)_{n\in\mathbb{Z}} = (c_n)_{n\in\mathbb{Z}}, \qquad \text{where } c_n = \sum_{i\in\mathbb{Z}} a_i b_{n-i}.$$

This module structure has torsion: In fact,

$$(1 - x)\left(\cdots + x^{-2} + x^{-1} + x^0 + x^1 + x^2 + \cdots\right) = 0.$$

This also shows that $K[[x^{\pm}]]$ is not a module over any of $K[[x]]$ and $K((x))$ (since $1 - x$ would have an inverse in these rings).

1.15. Multivariate FPSs

Multivariate FPSs are just FPSs in several variables. The theory of these series is mostly analogous to the univariate case. I will just discuss the main differences.

For example: FPSs in two variables x and y have the form

$$\sum_{i,j\in\mathbb{N}} a_{i,j}x^iy^j.$$

Formally, such an FPS is a family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ of elements of K. The indeterminates are

$$x=\left(\delta_{(i,j),(1,0)}\right)_{(i,j)\in\mathbb{N}^2} \qquad \text{and} \qquad y=\left(\delta_{(i,j),(0,1)}\right)_{(i,j)\in\mathbb{N}^2}.$$

It is better to use notations for tuples of nonnegative integers. Generally, for any $k\in\mathbb{N}$, we can define the FPSs in k variables $x_1,x_2,\ldots,x_k$ to be the families $(a_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^k}$ 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

$$[\mathbf{x}^{\mathbf{n}}]\,(ab)=\sum_{\substack{\mathbf{i},\mathbf{j}\in\mathbb{N}^k;\\ \mathbf{i}+\mathbf{j}=\mathbf{n}}}\left[\mathbf{x}^{\mathbf{i}}\right]a\cdot\left[\mathbf{x}^{\mathbf{j}}\right]b$$

(for any two FPSs a,b and any $\mathbf{n}\in\mathbb{N}^k$), where

- the sum $\mathbf{i}+\mathbf{j}$ is defined entrywise (i.e., you embed $\mathbb{N}^k$ in the additive group $\mathbb{Z}^k$);
- if $\mathbf{m}\in\mathbb{N}^k$ and h is an FPS, then $[\mathbf{x}^{\mathbf{m}}]\,h$ means the $\mathbf{m}$-th entry of the family h (we call it the $\mathbf{x}^{\mathbf{m}}$-coefficient of h). As usual, we let $\mathbf{x}^{\mathbf{m}}$ denote the monomial $x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}$, where $m_1,m_2,\ldots,m_k$ are the entries of $\mathbf{m}$.

The indeterminates $x_1,x_2,\ldots,x_k$ are defined by

$$x_i=\left(\delta_{\mathbf{n},e_i}\right)_{\mathbf{n}\in\mathbb{N}^k},$$

where $e_i=(0,0,\ldots,0,1,0,0,\ldots,0)$ with the 1 in its i-th position. Thus, any FPS $f=(f_{\mathbf{m}})_{\mathbf{m}\in\mathbb{N}^k}$ satisfies

$$f=\sum_{\mathbf{m}\in\mathbb{N}^k} f_{\mathbf{m}}\mathbf{x}^{\mathbf{m}}=\sum_{\mathbf{m}=(m_1,m_2,\ldots,m_k)\in\mathbb{N}^k} f_{\mathbf{m}}x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}.$$

(Infinite sums are defined as in the univariate case.)

Most of what we said about FPSs in one variable applies similarly to FPSs in many variables. There are some changes, though. The derivative f' is now replaced by k different derivatives, called **partial derivatives** $\dfrac{\partial f}{\partial x_i}$ for all $i \in \{1, 2, \ldots, k\}$. More importantly, substitution gets a bit trickier. In particular, you can substitute any k-tuple $(a_1, a_2, \ldots, a_k)$ of **commuting** elements of a K-algebra into a polynomial $f \in K[x_1, x_2, \ldots, x_k]$. The "commuting" part is important, because $x_1 x_2 = x_2 \cdot x_1$. The "polynomial" part is to ensure that the infinite sums are well-defined; there are other ways to ensure this (e.g., you can require that each a_i is a FPS with constant term 0).

> **Definition 1.15.1.** 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 $K[[x_1, x_2, \ldots, x_k]]$.

When we work in few variables, we will often give them single-letter names. For instance, we will write $K[[x, y]]$ instead of $K[[x_1, x_2]]$.

Let me give an example of working with multivariate FPSs.

Let's work in $K[[x, y]]$. We have

$$\begin{aligned}
\sum_{n,k\in\mathbb{N}} \binom{n}{k} x^n y^k &= \sum_{n\in\mathbb{N}} \sum_{k\in\mathbb{N}} \binom{n}{k} x^n y^k \\
&= \sum_{n\in\mathbb{N}} \underbrace{\left(\sum_{k\in\mathbb{N}} \binom{n}{k} y^k\right)}_{\substack{=(1+y)^n \\ \text{(by the binomial formula)}}} x^n \\
&= \sum_{n\in\mathbb{N}} (1+y)^n x^n = \sum_{n\in\mathbb{N}} ((1+y)x)^n = \frac{1}{1-(1+y)x} \\
&\qquad \left(\begin{array}{c} \text{here, we substituted } (1+y)x \text{ for } x \\ \text{in the formula } \sum\limits_{n\in\mathbb{N}} x^n = \dfrac{1}{1-x}; \\ \text{this is allowed since } (1+y)x \text{ has constant term } 0 \end{array}\right) \\
&= \frac{1}{1-x} \cdot \frac{1}{1 - \dfrac{x}{1-x} y} \qquad \text{(easy to check)} \\
&= \frac{1}{1-x} \cdot \sum_{k\in\mathbb{N}} \left(\frac{x}{1-x} y\right)^k \qquad \text{(again by geometric series)} \\
&= \frac{1}{1-x} \cdot \sum_{k\in\mathbb{N}} \frac{x^k}{(1-x)^k} y^k = \sum_{k\in\mathbb{N}} \frac{x^k}{(1-x)^{k+1}} y^k.
\end{aligned}$$

Comparing this with

$$\sum_{n,k\in\mathbb{N}} \binom{n}{k} x^n y^k = \sum_{k\in\mathbb{N}} \sum_{n\in\mathbb{N}} \binom{n}{k} x^n y^k = \sum_{k\in\mathbb{N}} \left(\sum_{n\in\mathbb{N}} \binom{n}{k} x^n\right) y^k,$$

we obtain

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

Comparing coefficients in front of y^k (while viewing the x as a constant), we obtain

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

What I mean by "comparing coefficients" is that we applied the following simple proposition:

Proposition 1.15.2. Let $f_0, f_1, f_2, \ldots$ and $g_0, g_1, g_2, \ldots$ be FPSs in a single variable x. Assume that

$$\sum_{k\in\mathbb{N}} f_k y^k = \sum_{k\in\mathbb{N}} g_k y^k.$$

Then, $f_k = g_k$ for each $k \in \mathbb{N}$.

Proof. Easy (see Proposition 3.15.2 in notes). □

So we have proved the equality

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

On the HW, you also get to prove this in a direct (univariate) way.

2. Integer partitions and q-binomial coefficients

We have already counted compositions of an $n \in \mathbb{N}$. These are essentially the ways to write n as a sum of finitely many positive integers, where the order matters. For example, 3 has 4 compositions: (3), $(2,1)$, $(1,2)$ and $(1,1,1)$.

Now let us disregard the order. So we either view $(2,1)$ and $(1,2)$ as the same way, or we disallow one of them. In other words, we no longer count **tuples** of positive integers whose sum is n, but now we count **multisets** or **weakly decreasing tuples**. We shall follow the second way, i.e., use weakly decreasing tuples instead of multisets. We call them **integer partitions**.

2.1. Partition basics

2.1.1. Definition

Definition 2.1.1. **(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. Thus, we get the notions of **size** and **length**.

(b) The **parts** of a partition $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ are 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** means a partition whose size is n and whose length is k.

For instance, 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 2.1.2. **(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

$$p(n) := (\text{\# of partitions of } n).$$

2.1.2. Simple properties of partition numbers

Definition 2.1.3. 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 $\begin{cases} 1, & \text{if } \mathcal{A}; \\ 0, & \text{if not } \mathcal{A}. \end{cases}$

So $[2+2=4] = 1$ and $[2+2=5] = 0$.

Note that $\delta_{i,j} = [i = j]$ for all i and j.

Also, we use the notation $\lfloor a \rfloor$ for the floor of $a \in \mathbb{R}$, and the notation $\lceil a \rceil$ for the ceiling of $a \in \mathbb{R}$.

Proposition 2.1.4. 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 $p_0(n) = [n = 0]$. (The empty tuple $()$ is a partition of 0 into 0 parts.)

(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. **(a)–(d)** easy.

(e) Let $k > 0$. We have

$$\begin{aligned} p_k(n) &= (\text{\# of partitions of } n \text{ into } k \text{ parts}) \\ &= \underbrace{(\text{\# of partitions of } n \text{ into } k \text{ parts that contain } 1)}_{\substack{=p_{k-1}(n-1) \\ \text{(since removing the 1 from such a partition} \\ \text{yields a partition of } n-1 \text{ into } k-1 \text{ parts,} \\ \text{and vice versa)}}} \\ &\qquad + \underbrace{(\text{\# of partitions of } n \text{ into } k \text{ parts that don't contain } 1)}_{\substack{=p_k(n-k) \\ \text{(since subtracting 1 from each entry} \\ \text{of such a partition yields} \\ \text{a partition of } n-k \text{ into } k \text{ parts,} \\ \text{and vice versa)}}} \\ &= p_{k-1}(n-1) + p_k(n-k). \end{aligned}$$

(f) Let $n \in \mathbb{N}$. The partitions of n into 2 parts are

$$(n-1,1), \ (n-2,2), \ (n-3,3), \ \ldots, \ \left(\left\lceil \frac{n}{2} \right\rceil, \left\lfloor \frac{n}{2} \right\rfloor\right).$$

There are $\left\lfloor \frac{n}{2} \right\rfloor$ of them. □

2.1.3. The generating function

Theorem 2.1.5. In the FPS ring $\mathbb{Z}[[x]]$, we have

$$\sum_{n\in\mathbb{N}} p(n)\,x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Example 2.1.6. Let us check this equality "up to x^5". We have

$$\begin{aligned}\prod_{k=1}^{\infty}\frac{1}{1-x^k} &= \frac{1}{1-x^1}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^4}\cdot\cdots\\ &= \left(1+x+x^2+x^3+x^4+\cdots\right)\\ &\cdot\left(1+x^2+x^4+\cdots\right)\\ &\cdot\left(1+x^3+\cdots\right)\\ &\cdot\left(1+x^4+\cdots\right)\\ &\cdot(1+\cdots)\\ &\cdot(1+\cdots)\\ &\cdots\cdot\\ &= 1+x+2x^2+3x^3+5x^4+\cdots\\ &= p(0)+p(1)x+p(2)x^2+p(3)x^3+p(4)x^4+\cdots.\end{aligned}$$

Proof of the theorem. We have

$$\begin{aligned}&\prod_{k=1}^{\infty}\frac{1}{1-x^k}\\ &= \prod_{k=1}^{\infty}\left(1+x^k+x^{2k}+x^{3k}+\cdots\right) && \left(\begin{array}{c}\text{by the geometric}\\ \text{series formula}\end{array}\right)\\ &= \prod_{k=1}^{\infty}\sum_{u\in\mathbb{N}}x^{ku}\\ &= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ is}\\ \text{essentially finite}}} x^{1u_1}x^{2u_2}x^{3u_3}\cdots && \left(\begin{array}{c}\text{here, we expanded}\\ \text{the product}\end{array}\right)\\ &= \sum_{\substack{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ is}\\ \text{essentially finite}}} x^{1u_1+2u_2+3u_3+\cdots}\\ &= \sum_{n\in\mathbb{N}}|Q_n|\,x^n,\end{aligned}$$

where

$$Q_n = \left\{(u_1,u_2,u_3,\ldots)\in\mathbb{N}^\infty \text{ essentially finite } \mid 1u_1+2u_2+3u_3+\cdots = n\right\}.$$

So it remains to prove 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 $\{\text{partitions of } n\}$. Namely, this bijection sends each $(u_1, u_2, u_3, \ldots) \in Q_n$ to the partition

$$\left(\ldots, \underbrace{3, 3, \ldots, 3}_{u_3 \text{ times}}, \underbrace{2, 2, \ldots, 2}_{u_2 \text{ times}}, \underbrace{1, 1, \ldots, 1}_{u_1 \text{ times}} \right)$$

(that is, the partition that contains each positive integer i exactly u_i times). Details are LTTR. This yields

$$|Q_n| = |\{\text{partitions of } n\}| = p(n),$$

qed. □

The theorem we just proved has a finite analogue:

Theorem 2.1.7. Let $m \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $p_{\text{parts}\leq m}(n)$ be the # of partitions λ of n such that all parts of λ are $\leq m$. Then,

$$\sum_{n \in \mathbb{N}} p_{\text{parts}\leq m}(n)\, x^n = \prod_{k=1}^{m} \frac{1}{1 - x^k}.$$

Proof. Same argument as before, but now replacing infinite sequences $(u_1, u_2, u_3, \ldots)$ by finite m-tuples $(u_1, u_2, \ldots, u_m)$. □

Even more generally:

Theorem 2.1.8. Let I be a subset of $\{1, 2, 3, \ldots\}$. For each $n \in \mathbb{N}$, let $p_I(n)$ be the # of partitions λ of n such that all parts of λ are $\in I$. Then,

$$\sum_{n \in \mathbb{N}} p_I(n)\, x^n = \prod_{k \in I} \frac{1}{1 - x^k}.$$

Proof. Same as before, but more subscripts. □

2.1.4. Odd parts and distinct parts

Definition 2.1.9. 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

$$p_{\text{odd}}(n) := (\text{\# of partitions of } n \text{ into odd parts});$$
$$p_{\text{dist}}(n) := (\text{\# of partitions of } n \text{ into distinct parts}).$$

Theorem 2.1.10 (Euler's odd-distinct identity)**.** For each $n \in \mathbb{N}$, we have $p_{\operatorname{odd}}(n) = p_{\operatorname{dist}}(n)$.

Proof. We proved this before, deriving it from

$$\prod_{i>0} \left(1 - x^{2i-1}\right)^{-1} = \prod_{k>0} \left(1 + x^k\right).$$

□

There are also other proofs of this identity.

2.1.5. Partitions with a given largest part

Proposition 2.1.11. 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 agree to define the largest partition of the empty partition $()$ to be 0.

Example 2.1.12. For $n = 4$ and $k = 2$, we have

$$\begin{aligned} p_k(n) &= p_2(4) = (\text{\# of partitions of 4 into 2 parts}) \\ &= \left|\left\{(3,1),\ (2,2)\right\}\right| = 2. \end{aligned}$$

The proposition tells us that

$$\begin{aligned} p_k(n) &= (\text{\# of partitions of 4 whose largest part is 2}) \\ &= \left|\left\{(2,2),\ (2,1,1)\right\}\right| = 2. \end{aligned}$$

Proof of the proposition. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ be any partition of n into k parts. 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).

Now, flip the table across the main diagonal, and read off the lengths of the rows of the resulting table. Let λ^t be the sequence of these new row lengths. This is again a partition of n, but instead of being a partition into k parts, it is a partition whose largest part is k.

Thus we have defined a map

$$\begin{aligned} \{\text{partitions of } n \text{ into } k \text{ parts}\} &\to \{\text{partitions of } n \text{ whose largest part is } k\}, \\ \lambda &\mapsto \lambda^t. \end{aligned}$$

Conversely, we construct a map

$$\begin{aligned} \{\text{partitions of } n \text{ whose largest part is } k\} &\to \{\text{partitions of } n \text{ into } k \text{ parts}\}, \\ \lambda &\mapsto \lambda^t. \end{aligned}$$

These two maps are mutually inverse, so are bijections. Thus we conclude the claim. □

The table that we constructed from our partition λ in our above proof is called the **Young diagram** of λ. Formally, if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ is any partition, then its **Young diagram** is defined to be the set

$$Y(\lambda) := \left\{(i,j) \in \mathbb{Z}^2 \mid 1 \leq i \leq k \text{ and } 1 \leq j \leq \lambda_i\right\}.$$

We interpret each $(i,j) \in \mathbb{Z}^2$ as a box, which we put in the i-th row from the top and the j-th column from the left. This convention is called **English notation** or **matrix notation**.

Now, the **conjugate** (or **transpose**) of the partition λ is the partition λ^t uniquely determined by

$$Y\left(\lambda^t\right) := \operatorname{flip}\left(Y(\lambda)\right) = \{(j,i) \mid (i,j) \in Y(\lambda)\}.$$

This can also be defined more explicitly by $\lambda^t = (\mu_1, \mu_2, \ldots, \mu_s)$, where s is the largest part of λ and where

$$\mu_i = (\text{\# of parts of } \lambda \text{ that are } \geq i).$$

Many authors denote λ^t by λ'.

Corollary 2.1.13. 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. For each $i \in \{0, 1, \ldots, k\}$, we have

$$p_i(k) = (\text{\# of partitions of } n \text{ whose largest part is } i)$$

(by the proposition we just proved). Now sum this over all i. □

Theorem 2.1.14. Let $m \in \mathbb{N}$. Then,

$$\sum_{n \in \mathbb{N}} \left(p_0(n) + p_1(n) + \cdots + p_m(n)\right) x^n = \prod_{k=1}^{m} \frac{1}{1 - x^k}.$$

Proof. Combine the corollary we just proved with the formula

$$\sum_{n \in \mathbb{N}} p_{\text{parts} \leq m}(n)\, x^n = \prod_{k=1}^{m} \frac{1}{1 - x^k}.$$

□

2.1.6. Partition number vs. sums of divisors

Here is another curious result of Euler's:

Theorem 2.1.15. For any positive integer n, let $\sigma(n)$ denote the sum of all positive divisors of n. (For example, $\sigma(6) = 1+2+3+6 = 12$.) Then, for any $n \in \mathbb{N}$, we have

$$np(n) = \sum_{k=1}^{n} \sigma(k)\, p(n-k).$$

Proof. See the notes (§4.1.6). □

More generally:

Theorem 2.1.16. Let I be a subset of $\{1,2,3,\ldots\}$. For each $n \in \mathbb{N}$, let $p_I(n)$ be the # of partitions λ of n such that all parts of λ belong to I. For any positive integer n, let $\sigma_I(n)$ denote the sum of all divisors of n that belong to I. Then,

$$np_I(n) = \sum_{k=1}^{n} \sigma_I(k)\, p_I(n-k).$$

Proof. See the notes (§4.1.6). □

2.2. Euler's pentagonal number theorem

Definition 2.2.1. 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**.

Some values:

k	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	5	$\cdots$
w_k	$\cdots$	26	15	7	2	0	1	5	12	22	35	$\cdots$

It is easy to see that w_k really $\in \mathbb{N}$ for $k \in \mathbb{Z}$. Moreover, w_k grows quadratically as $k \to \infty$ or as $k \to -\infty$. This ensures that the infinite sum $\sum_{k\in\mathbb{Z}} (-1)^k x^{w_k}$ is well-defined as a FPS in $\mathbb{Z}[[x]]$. Surprisingly, it factors pretty nicely:

Theorem 2.2.2 (Euler's pentagonal number theorem)**.** We have

$$\prod_{k=1}^{\infty}\left(1-x^k\right)=\sum_{k\in\mathbb{Z}}(-1)^k x^{w_k}.$$

Concretely, this is saying

$$\begin{aligned}&\left(1-x^1\right)\left(1-x^2\right)\left(1-x^3\right)\cdots\\&=\cdots+x^{w_{-2}}-x^{w_{-1}}+x^{w_0}-x^{w_1}+x^{w_2}\pm\cdots\\&=\cdots+x^7-x^2+x^0-x^1+x^5\pm\cdots\\&=x^0-x^1-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}\pm\cdots\end{aligned}$$

We will prove this theorem in the next section, as a particular case of something stronger. But first, let me show how it yields a recursive formula for $p(n)$:

Corollary 2.2.3. For each positive integer n, we have

$$\begin{aligned}p(n)&=\sum_{\substack{k\in\mathbb{Z};\\k\neq 0}}(-1)^{k-1}p(n-w_k)\\&=p(n-1)+p(n-2)-p(n-5)-p(n-7)\\&\qquad+p(n-12)+p(n-15)-p(n-22)-p(n-26)\pm\cdots.\end{aligned}$$

Proof of the corollary using the theorem. We have

$$\begin{aligned}&\sum_{m\in\mathbb{N}}p(m)x^m=\sum_{n\in\mathbb{N}}p(n)x^n=\prod_{k=1}^{\infty}\frac{1}{1-x^k}\qquad\text{and}\\&\sum_{k\in\mathbb{Z}}(-1)^k x^{w_k}=\prod_{k=1}^{\infty}\left(1-x^k\right)\qquad\text{(by the theorem)}.\end{aligned}$$

Multiplying these two equalities, we obtain

$$\left(\sum_{m\in\mathbb{N}}p(m)x^m\right)\left(\sum_{k\in\mathbb{Z}}(-1)^k x^{w_k}\right)=\left(\prod_{k=1}^{\infty}\frac{1}{1-x^k}\right)\prod_{k=1}^{\infty}\left(1-x^k\right)=1.$$

Comparing coefficients of x^n on both sides, we find

$$\sum_{\substack{m\in\mathbb{N};\\k\in\mathbb{Z};\\m+w_k=n}}p(m)(-1)^k=0.$$

So

$$\begin{aligned}
0 &= \sum_{\substack{m\in\mathbb{N};\\ k\in\mathbb{Z};\\ m+w_k=n}} p\left(m\right)\left(-1\right)^k = \sum_{\substack{m\in\mathbb{Z};\\ k\in\mathbb{Z};\\ m+w_k=n}} p\left(m\right)\left(-1\right)^k = \sum_{k\in\mathbb{Z}} p\left(n-w_k\right)\left(-1\right)^k \\
&= \sum_{k\in\mathbb{Z}} \left(-1\right)^k p\left(n-w_k\right) = \underbrace{\left(-1\right)^0}_{=1} p\left(n-\underbrace{w_0}_{=0}\right) + \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right) \\
&= p\left(n\right) + \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right).
\end{aligned}$$

Solving this for $p\left(n\right)$, we find

$$p\left(n\right) = -\sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^k p\left(n-w_k\right) = \sum_{\substack{k\in\mathbb{Z};\\ k\neq 0}} \left(-1\right)^{k-1} p\left(n-w_k\right).$$

□

2.3. Jacobi's triple product identity

2.3.1. The identity

Instead of proving the pentagonal number theorem directly, we will prove a stronger result: **Jacobi's triple product identity**. This identity can be stated as follows:

$$\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right) = \sum_{\ell\in\mathbb{Z}} q^{\ell^2}z^{\ell}.$$

What are q and z here? One way to interpret this identity is by viewing both sides as elements of $\left(\mathbb{Z}\left[z^{\pm}\right]\right)\left[\left[q\right]\right]$, since z can appear in negative powers but q only in nonnegative ones. In other words, we state:

> **Theorem 2.3.1** (Jacobi's triple product identity, take 1)**.** In the ring $\left(\mathbb{Z}\left[z^{\pm}\right]\right)\left[\left[q\right]\right]$, we have
>
> $$\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\left(1-q^{2n}\right)\right) = \sum_{\ell\in\mathbb{Z}} q^{\ell^2}z^{\ell}.$$

Unfortunately, we don't just need this identity as a formal identity; instead, we want to substitute things into it. Specifically, we will substitute $q = x^a$ and $z = x^b$ for some positive integers a and b. This kind of substitution does not always work in $\left(\mathbb{Z}\left[z^{\pm}\right]\right)\left[\left[q\right]\right]$. For example, substituting $q = x$ and $z = x$ into $\sum\limits_{\ell\in\mathbb{N}} q^{\ell}z^{-\ell}$ yields $\sum\limits_{\ell\in\mathbb{N}} x^{\ell}x^{-\ell} = \sum\limits_{\ell\in\mathbb{N}} 1$, which is undefined.

Thus, we cannot use the above version of the identity for our purposes, at least not without a lot of extra work. However, we can use the following variant directly:

Theorem 2.3.2 (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 both sides are well-defined:

- The LHS is

  $$\prod_{n>0} \left(\left(1 + q^{2n-1} z\right) \left(1 + q^{2n-1} z^{-1}\right) \left(1 - q^{2n}\right) \right)$$
  $$= \prod_{n>0} \left(\left(1 + u^{2n-1} v x^{(2n-1)a+b}\right) \left(1 + u^{2n-1} v^{-1} x^{(2n-1)a-b}\right) \left(1 - u^{2n} x^{2na}\right) \right).$$

  All factors in this product belong to $\mathbb{Q}[[x]]$, not just $\mathbb{Q}((x))$, since the exponents $(2n-1)a + b$ and $(2n-1)a - b$ and $2na$ are ≥ 0. Moreover, this product is multipliable, since

  - $(2n-1)a + b$ 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 $a > 0$).

- The RHS is

  $$\sum_{\ell \in \mathbb{Z}} q^{\ell^2} z^{\ell} = \sum_{\ell \in \mathbb{Z}} (ux^a)^{\ell^2} \left(vx^b\right)^{\ell} = \sum_{\ell \in \mathbb{Z}} u^{\ell^2} v^{\ell} x^{a\ell^2 + b\ell}.$$

  This is summable, since $a > 0$ ensures that the quadratic $a\ell^2 + b\ell$ goes to ∞ as $\ell \to \infty$ or $\ell \to -\infty$.

2.3.2. Proof of Jacobi's triple product identity

Let us now prove Jacobi's triple product identity. The following proof is due to Borcherds, and is stated in a physicsy language.

Proof of Jacobi's triple product identity in both take 1 and take 2, depending on how you understand q and z We define the following concepts:

- A **level** will mean a number of the form $p + \frac{1}{2}$ with $p \in \mathbb{Z}$.

- A **state** will mean a set of levels that contains
  - all but finitely many negative levels;
  - only finitely many positive levels.

For example,

$$\left\{ \frac{11}{2}, \frac{7}{2}, \frac{3}{2}, \frac{1}{2}, \frac{-1}{2}, \frac{-5}{2} \right\} \cup \left\{ \text{all levels } \leq \frac{-9}{2} \right\}$$

is a state. We draw a state as a number line with a circle at each level, where a circle is white if the level is in the state and a circle is black if it is not. We think of levels in the state as "electrons", and of the other levels as "holes".

For any state S,

- we define the **energy** of S to be

$$\operatorname{energy} S := \sum_{\substack{p>0; \\ p \in S}} 2p - \sum_{\substack{p<0; \\ p \notin S}} 2p \in \mathbb{N}.$$

- we define the **particle number** of S to be

$$\begin{aligned} \operatorname{parnum} S := & \left(\# \text{ of levels } p > 0 \text{ such that } p \in S\right) \\ & - \left(\# \text{ of levels } p < 0 \text{ such that } p \notin S\right) \in \mathbb{Z}. \end{aligned}$$

For instance, in the above example, we have

$$\begin{aligned} \operatorname{energy} S &= 1 + 3 + 7 + 11 - (-3) - (-7) = 32; \\ \operatorname{parnum} S &= 4 - 2 = 2. \end{aligned}$$

We want to prove the identity

$$\prod_{n>0} \left(\left(1 + q^{2n-1} z\right) \left(1 + q^{2n-1} z^{-1}\right) \left(1 - q^{2n}\right) \right) = \sum_{\ell \in \mathbb{Z}} q^{\ell^2} z^{\ell}.$$

First, we transform it into the equivalent identity

$$\prod_{n>0} \left(\left(1 + q^{2n-1} z\right) \left(1 + q^{2n-1} z^{-1}\right) \right) = \left(\sum_{\ell \in \mathbb{Z}} q^{\ell^2} z^{\ell} \right) \prod_{n>0} \left(1 - q^{2n}\right)^{-1}.$$

We will prove that both sides of this identity are

$$\sum_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}.$$

Left hand side: We have

$$\begin{aligned}
&\prod_{n>0}\left(\left(1+q^{2n-1}z\right)\left(1+q^{2n-1}z^{-1}\right)\right)\\
&=\left(\prod_{n>0}\left(1+q^{2n-1}z\right)\right)\left(\prod_{n>0}\left(1+q^{2n-1}z^{-1}\right)\right)\\
&=\left(\prod_{p\text{ is a positive level}}\left(1+q^{2p}z\right)\right)\left(\prod_{p\text{ is a negative level}}\left(1+q^{-2p}z^{-1}\right)\right)\\
&=\left(\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\prod_{p\in P}\left(q^{2p}z\right)\right)\left(\sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}}\prod_{p\in N}\left(q^{-2p}z^{-1}\right)\right)\\
&=\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}}\underbrace{\prod_{p\in P}\left(q^{2p}z\right)\prod_{p\in N}\left(q^{-2p}z^{-1}\right)}_{=q^{2(\text{sum of elements of }P)-2(\text{sum of elements of }N)}z^{|P|-|N|}}\\
&=\sum_{\substack{P\text{ is a finite set}\\ \text{of positive levels}}}\sum_{\substack{N\text{ is a finite set}\\ \text{of negative levels}}}q^{2(\text{sum of elements of }P)-2(\text{sum of elements of }N)}z^{|P|-|N|}\\
&=\sum_{S\text{ is a state}}q^{\text{energy }S}z^{\text{parnum }S}\\
&\qquad\left(\begin{array}{c}\text{here, we have combined }P\text{ and }N\\ \text{into a single state }S:=P\cup\overline{N},\\ \text{where }\overline{N}=\{\text{all negative levels}\}\setminus N\end{array}\right).
\end{aligned}$$

So the LHS is what we want.

Right hand side: Recall that

$$\prod_{n>0}\left(1-x^n\right)^{-1}=\sum_{n\in\mathbb{N}}p\left(n\right)x^n=\sum_{\lambda\text{ is a partition}}x^{|\lambda|}.$$

Substituting q^2 for x in this equality, we obtain

$$\prod_{n>0}\left(1-q^{2n}\right)^{-1}=\sum_{\lambda\text{ is a partition}}q^{2|\lambda|}.$$

Thus,

$$\begin{aligned}
\left(\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}\right)\prod_{n>0}\left(1-q^{2n}\right)^{-1}&=\left(\sum_{\ell\in\mathbb{Z}}q^{\ell^2}z^{\ell}\right)\sum_{\lambda\text{ is a partition}}q^{2|\lambda|}\\
&=\sum_{\ell\in\mathbb{Z}}\ \sum_{\lambda\text{ is a partition}}q^{\ell^2+2|\lambda|}z^{\ell}.
\end{aligned}$$

We want to show that this equals $\sum\limits_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}$. To do so, 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

$$\operatorname{energy}(\Phi_\ell(\lambda)) = \ell^2 + 2|\lambda| \qquad \text{for each } \ell \text{ and } \lambda.$$

Let us do this. Fix $\ell \in \mathbb{Z}$. We define the **ℓ-ground state** to be the state

$$G_\ell := \{\text{all levels } < \ell\} = \left\{\ell - \frac{1}{2},\ \ell - \frac{3}{2},\ \ell - \frac{5}{2},\ \ldots\right\}.$$

This state G_ℓ has energy ℓ^2 and particle number ℓ. (The proof depends on $\ell > 0$ or $\ell < 0$, but the answers are the same in both cases.)

If S is a state and $p \in S$, 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 $\operatorname{jump}_{p,q} S$ is obtained from S by letting the electron at level p **jump** q steps to the right. This state $\operatorname{jump}_{p,q} S$ has the same particle number as S (check it!), while its energy is $2q$ higher than that of S (check this!).

For any partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we define the **excited state** $E_{\ell,\lambda}$ by starting with the ℓ-ground state G_ℓ, and then successively letting the k rightmost electrons (i.e., the k largest elements of G_ℓ) jump $\lambda_1, \lambda_2, \ldots, \lambda_k$ steps to the right (starting with the rightmost electron). Since λ is a partition, this process is well-defined (i.e., there are no "collisions"), so its resulting state $E_{\ell,\lambda}$ really exists, and has particle number ℓ. Explicitly,

$$E_{\ell,\lambda} = \{\text{all levels } < \ell - k\} \cup \left\{\ell - i + \frac{1}{2} + \lambda_i \ \middle|\ i \in \{1, 2, \ldots, k\}\right\}.$$

Moreover, the partition λ can be recovered from $E_{\ell,\lambda}$ (how?). Furthermore, every state with particle number ℓ has the form $E_{\ell,\lambda}$ for some partition λ (namely: let $e_1 > e_2 > e_3 > \cdots$ be the elements of the state from highest to lowest, and define

$$\lambda = \left(e_1 - \left(\ell - \frac{1}{2}\right),\ e_2 - \left(\ell - \frac{3}{2}\right),\ e_3 - \left(\ell - \frac{5}{2}\right),\ \ldots\right)$$

without the zeroes). So 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

$$\operatorname{energy}\left(\Phi_\ell\left(\lambda\right)\right) = \ell^2 + 2\left|\lambda\right| \qquad \text{for each partition } \lambda.$$

Hence,

$$\sum_{\lambda \text{ is a partition}} q^{\ell^2+2|\lambda|} = \sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}} q^{\operatorname{energy} S}.$$

Forget that we fixed ℓ. We thus have proved this equality for all $\ell \in \mathbb{Z}$. Now,

$$\begin{aligned}\left(\sum_{\ell\in\mathbb{Z}} q^{\ell^2} z^\ell\right) \prod_{n>0} \left(1-q^{2n}\right)^{-1} &= \sum_{\ell\in\mathbb{Z}} \ \sum_{\lambda \text{ is a partition}} q^{\ell^2+2|\lambda|} z^\ell \\ &= \sum_{\ell\in\mathbb{Z}} \ \sum_{\substack{S \text{ is a state with} \\ \text{particle number } \ell}} q^{\operatorname{energy} S} z^\ell \\ &= \sum_{S \text{ is a state}} q^{\operatorname{energy} S} z^{\operatorname{parnum} S}.\end{aligned}$$

This is exactly the expression we found for the LHS. So LHS = RHS, and the Jacobi triple product identity is proved. □

2.3.3. Proof of the pentagonal number theorem

Recall:

> **Theorem 2.3.3** (Euler's pentagonal number theorem)**.** We have
>
> $$\prod_{k=1}^{\infty} \left(1-x^k\right) = \sum_{k\in\mathbb{Z}} \left(-1\right)^k x^{w_k}.$$

Proof. Set $q = x^3$ and $z = -x$ in Jacobi's triple product identity (i.e., apply it to $a = 3$ and $b = 1$ and $u = 1$ and $v = -1$). We get

$$\begin{aligned}&\prod_{n>0} \left(\left(1+\left(x^3\right)^{2n-1}\left(-x\right)\right)\left(1+\left(x^3\right)^{2n-1}\left(-x\right)^{-1}\right)\left(1-\left(x^3\right)^{2n}\right)\right) \\ &= \sum_{\ell\in\mathbb{Z}} \left(x^3\right)^{\ell^2} \left(-x\right)^\ell.\end{aligned}$$

Let's simplify the LHS:

$$\begin{aligned}
&\prod_{n>0}\left(\left(1+\left(x^3\right)^{2n-1}(-x)\right)\left(1+\left(x^3\right)^{2n-1}(-x)^{-1}\right)\left(1-\left(x^3\right)^{2n}\right)\right)\\
&=\prod_{n>0}\left(\left(1-x^{3(2n-1)+1}\right)\left(1-x^{3(2n-1)-1}\right)\left(1-x^{6n}\right)\right)\\
&=\prod_{n>0}\left(\left(1-x^{6n-2}\right)\left(1-x^{6n-4}\right)\left(1-x^{6n}\right)\right)\\
&=\prod_{n>0}\left(\left(1-\left(x^2\right)^{3n-1}\right)\left(1-\left(x^2\right)^{3n-2}\right)\left(1-\left(x^2\right)^{3n}\right)\right)\\
&=\prod_{k>0}\left(1-\left(x^2\right)^{k}\right)
\end{aligned}$$

(since each positive integer k can be uniquely represented as $3n-1$ or $3n-2$ or $3n$ for some positive integer n). So the formula becomes

$$\begin{aligned}
\prod_{k>0}\left(1-\left(x^2\right)^{k}\right) &= \sum_{\ell\in\mathbb{Z}}\left(x^3\right)^{\ell^2}(-x)^{\ell} = \sum_{\ell\in\mathbb{Z}}(-1)^{\ell}x^{3\ell^2+\ell}\\
&= \sum_{\ell\in\mathbb{Z}}(-1)^{\ell}\left(x^2\right)^{\left(3\ell^2+\ell\right)/2} = \sum_{\ell\in\mathbb{Z}}(-1)^{\ell}\left(x^2\right)^{w_{-\ell}}\\
&= \sum_{k\in\mathbb{Z}}(-1)^{k}\left(x^2\right)^{w_k}.
\end{aligned}$$

However, it is easy to see that if two FPSs f and g in $K[[x]]$ satisfy $f\left[x^2\right]=g\left[x^2\right]$, then $f=g$. Thus, "unsubstituting x^2 for x" in the above equality yields

$$\prod_{k>0}\left(1-x^{k}\right)=\sum_{k\in\mathbb{Z}}(-1)^{k}x^{w_k},$$

which is precisely Euler's pentagonal number theorem. □

2.4. q-binomial coefficients

Next, we will discuss **q-binomial coefficients**. These are also known as **Gaussian binomial coefficients**. See the notes for a bunch of references.

2.4.1. Motivation

For any $n\in\mathbb{N}$, we have

$$p(n)=(\#\text{ of partitions of }n).$$

For any $n, k \in \mathbb{N}$, we have

$$\begin{aligned} p_k(n) &= (\text{\# of partitions of } n \text{ into } k \text{ parts}) \\ &= (\text{\# of partitions of } n \text{ with largest part } k) \qquad (\text{by a theorem we proved}). \end{aligned}$$

Thus, for any $n, k \in \mathbb{N}$, we have

$$\begin{aligned} & p_0(n) + p_1(n) + \cdots + p_k(n) \\ & = (\text{\# of partitions of } n \text{ into } \textbf{at most } k \text{ parts}) \\ & = (\text{\# of partitions of } n \text{ with largest part } \leq k). \end{aligned}$$

Now, what about counting the partitions of n into k parts with largest part ℓ ?

Let us first drop the first requirement – the n. So let us count all partitions into k parts with largest part ℓ. By a combinatorial argument (whiteboard or notes), the number of such partitions is $\dbinom{k+\ell-2}{k-1}$, because the lower boundary of such a partition is a lattice path consisting of k up-steps and ℓ right-steps and starting with a right-step and ending with an up-step, and such lattice paths are in bijection with the $(k-1)$-element subsets of the set $\{2, 3, \ldots, k+\ell-1\}$. So we have proved:

Proposition 2.4.1. For any positive integers k and ℓ, we have

$$(\text{\# of partitions with } k \text{ parts and largest part } \ell) = \binom{k+\ell-2}{k-1}.$$

Note that this is a finite number, and is symmetric in k and ℓ (since transposition = conjugation turns a partition with k parts and largest part ℓ into a partition with ℓ parts and largest part k).

Now let us get n back into our count. We cannot do this directly, but we can try to compute the generating function

$$\begin{aligned} & \sum_{n \in \mathbb{N}} (\text{\# of partitions of } n \text{ with } k \text{ parts and largest part } \ell)\, x^n \\ & = \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \ell \\ \text{and length } k}} x^{|\lambda|} \in \mathbb{Z}[x]. \end{aligned}$$

For reasons of tradition and convenience, we make some modifications:

- We rename ℓ as $n-k$ (now n is no longer $|\lambda|$).
- We replace "largest part $n-k$ and length k" by "largest part $\leq n-k$ and length $\leq k$".
- We rename the indeterminate x as q.

2.4.2. Definition

Convention 2.4.2. In this section, we will mostly be using FPSs in the indeterminate q. Their ring is called $K[[q]]$ instead of $K[[x]]$. Other than that, they behave in the exact same way. For example,

$$\prod_{n>0}(1-q^n)^{-1}=\prod_{n>0}\frac{1}{1-q^n}=\sum_{n\in\mathbb{N}}p(n)\,q^n=\sum_{\substack{\lambda\text{ is a}\\\text{partition}}}q^{|\lambda|}.$$

Definition 2.4.3. Let $n\in\mathbb{N}$ and $k\in\mathbb{N}$.

(a) The **q-binomial coefficient** (or **Gaussian binomial coefficient**) $\binom{n}{k}_q$ is defined to be the polynomial

$$\sum_{\substack{\lambda\text{ is a partition}\\\text{with largest part }\leq n-k\\\text{and length }\leq k}}q^{|\lambda|}\in\mathbb{Z}[q].$$

Some authors write $\begin{bmatrix}n\\k\end{bmatrix}$ for this, but we prefer not to.

(b) If a is any element of a ring A, then we set

$$\binom{n}{k}_a:=\binom{n}{k}_q[a]=\sum_{\substack{\lambda\text{ is a partition}\\\text{with largest part }\leq n-k\\\text{and length }\leq k}}a^{|\lambda|}.$$

We will soon see that $\binom{n}{k}_1=\binom{n}{k}$.

Example 2.4.4. We have

$$\begin{aligned}\binom{3}{2}_q&=\sum_{\substack{\lambda\text{ is a partition}\\\text{with largest part }\leq 3-2\\\text{and length }\leq 2}}q^{|\lambda|}=q^{|()|}+q^{|(1)|}+q^{|(1,1)|}\\&=1+q+q^2\end{aligned}$$

and

$$\begin{aligned}\dbinom{4}{2}_q &= \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq 4-2 \\ \text{and length } \leq 2}} q^{|\lambda|} \\ &= q^{|()|} + q^{|(1)|} + q^{|(2)|} + q^{|(1,1)|} + q^{|(2,1)|} + q^{|(2,2)|} \\ &= 1 + q + q^2 + q^2 + q^3 + q^4 = 1 + q + 2q^2 + q^3 + q^4.\end{aligned}$$

2.4.3. Basic properties

Proposition 2.4.5. Let $n, k \in \mathbb{N}$.

(a) We have

$$\dbinom{n}{k}_q = \sum_{0 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n-k} q^{i_1 + i_2 + \cdots + i_k}.$$

Here, the sum ranges over all weakly increasing k-tuples $(i_1, i_2, \ldots, i_k) \in \{0, 1, \ldots, n-k\}^k$. This sum is empty if $k > n$.

(b) For any finite set S of integers, let $\operatorname{sum} S := \sum_{s \in S} s$. Then,

$$\dbinom{n}{k}_q = \sum_{\substack{S \subseteq \{1,2,\ldots,n\}; \\ |S| = k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

(c) We have

$$\dbinom{n}{k}_1 = \dbinom{n}{k}.$$

Proof. Details in the notes; here is an outline.

(a) We are looking for a bijection Φ

from $\{$partitions with largest part $\leq n-k$ and length $\leq k\}$

to $\left\{\text{weakly increasing } k\text{-tuples } (i_1, i_2, \ldots, i_k) \in \{0, 1, \ldots, n-k\}^k\right\}$

such that

$$|\lambda| = i_1 + i_2 + \cdots + i_k \text{ if } (i_1, i_2, \ldots, i_k) = \Phi(\lambda).$$

This bijection Φ does the following: Read the partition backwards, and insert 0's at the front to make it into a k-tuple. For instance, if $k = 5$ and $\lambda = (3, 3, 2)$, then $\Phi(\lambda) = (0, 0, 2, 3, 3)$. So part **(a)** follows.

(b) We are looking for a bijection Ψ

from $\left\{\text{weakly increasing } k\text{-tuples } (i_1, i_2, \ldots, i_k) \in \{0, 1, \ldots, n-k\}^k\right\}$

to $\{$subsets S of $\{1, 2, \ldots, n\}$ satisfying $|S| = k\}$

such that

$$\operatorname{sum} S-(1+2+\cdots+k)=i_1+i_2+\cdots+i_k \text{ whenever } S=\Psi\left(i_1,i_2,\ldots,i_k\right).$$

Such a bijection Ψ can be constructed as follows:

$$\Psi\left(i_1,i_2,\ldots,i_k\right)=\left\{i_1+1,\ i_2+2,\ \ldots,\ i_k+k\right\}.$$

So part **(b)** follows.

(c) Part **(b)** yields

$$\begin{aligned}\binom{n}{k}_1 &= \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} \underbrace{1^{\operatorname{sum} S-(1+2+\cdots+k)}}_{=1} = \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} 1\\ &= (\text{\# of } k\text{-element subsets of } \{1,2,\ldots,n\}) = \binom{n}{k}.\end{aligned}$$

□

Proposition 2.4.6. Let $n,k\in\mathbb{N}$ satisfy $k>n$. Then, $\dbinom{n}{k}_q=0$.

Proof. Part **(b)** of the proposition yields

$$\binom{n}{k}_q=\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} q^{\operatorname{sum} S-(1+2+\cdots+k)}=(\text{empty sum})=0.$$

□

Proposition 2.4.7. Let $n\in\mathbb{N}$. Then, $\dbinom{n}{0}_q=\dbinom{n}{n}_q=1$.

Proof. HW. □

Convention 2.4.8. Let $n\in\mathbb{N}$. For any $k\notin\mathbb{N}$, we set $\dbinom{n}{k}_q:=0$.

Recall Pascal's recurrence $\dbinom{n}{k}=\dbinom{n-1}{k-1}+\dbinom{n-1}{k}$. Here are two ways to generalize it to q-binomial coefficients:

Theorem 2.4.9. 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. **(b)** HW.

(a) Details in the notes. Main idea:

$$\begin{aligned}\binom{n}{k}_q &= \sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k}} q^{\operatorname{sum}S-(1+2+\cdots+k)} \\ &= \underbrace{\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ n\in S}} q^{\operatorname{sum}S-(1+2+\cdots+k)}}_{\begin{array}{c} =\sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} q^{\operatorname{sum}S+n-(1+2+\cdots+k)} \\ =q^{n-k}\sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k-1}} q^{\operatorname{sum}S-(1+2+\cdots+(k-1))} \\ =q^{n-k}\binom{n-1}{k-1}_q \end{array}} + \underbrace{\sum_{\substack{S\subseteq\{1,2,\ldots,n\};\\ |S|=k;\\ n\notin S}} q^{\operatorname{sum}S-(1+2+\cdots+k)}}_{\begin{array}{c} =\sum_{\substack{S\subseteq\{1,2,\ldots,n-1\};\\ |S|=k}} q^{\operatorname{sum}S-(1+2+\cdots+k)} \\ =\binom{n-1}{k}_q \end{array}} \\ &= q^{n-k}\binom{n-1}{k-1}_q + \binom{n-1}{k}_q ,\end{aligned}$$

qed. □

Next, recall the formula

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

It also has a q-analogue:

Theorem 2.4.10. Let $n, k \in \mathbb{N}$ satisfy $n \geq k$. Then:

(a) We have

$$\begin{aligned}&\left(1-q^k\right)\left(1-q^{k-1}\right)\cdots\left(1-q^1\right)\cdot\binom{n}{k}_q \\ &= (1-q^n)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right).\end{aligned}$$

(b) We have

$$\binom{n}{k}_q = \frac{(1-q^n)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right)}{\left(1-q^k\right)\left(1-q^{k-1}\right)\cdots\left(1-q^1\right)}$$

(in the ring $\mathbb{Z}[[q]]$ or in the field of rational functions over $\mathbb{Q}$).

Proof. HW. □

To see the analogy between this theorem and the classical

$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!}$$

formula better, we introduce notations:

Definition 2.4.11. **(a)** For any $n \in \mathbb{N}$, we define the q**-integer** $\left[n\right]_q$ to be

$$\left[n\right]_q := q^0 + q^1 + \cdots + q^{n-1} \in \mathbb{Z}\left[q\right].$$

(b) For any $n \in \mathbb{N}$, we define the q**-factorial** $\left[n\right]_q!$ to be

$$\left[n\right]_q! := \left[1\right]_q \left[2\right]_q \cdots \left[n\right]_q \in \mathbb{Z}\left[q\right].$$

(c) As usual, if a is an element of a ring A, then $\left[n\right]_a$ and $\left[n\right]_a!$ mean the values $\left[n\right]_q\left[a\right]$ and $\left[n\right]_q!\left[a\right]$, that is, the values of $\left[n\right]_q$ and $\left[n\right]_q!$ at $q = a$.

Remark 2.4.12. For any $n \in \mathbb{N}$, we have

$$\left[n\right]_q = \frac{1-q^n}{1-q} \qquad \text{(in } \mathbb{Z}\left[\left[q\right]\right] \text{ or rational functions)}$$

and $\left[n\right]_1 = n$ and $\left[n\right]_1! = n!$.

So our above theorem becomes:

Theorem 2.4.13. Let $n, k \in \mathbb{N}$ satisfy $n \geq k$. Then:

$$\binom{n}{k}_q = \frac{\left[n\right]_q \left[n-1\right]_q \cdots \left[n-k+1\right]_q}{\left[k\right]_q!} = \frac{\left[n\right]_q!}{\left[k\right]_q! \cdot \left[n-k\right]!_q}$$

(in the ring $\mathbb{Z}\left[\left[q\right]\right]$ or the rational functions).

Proof. HW. □

Proposition 2.4.14. Let $n, k \in \mathbb{N}$. Then,

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

Proof. HW. □

2.4.4. q-binomial formulas

As we have seen, the q-binomial coefficients generalize the binomial coefficients in several ways. Here is another instance of this:

Recall the usual binomial formula

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

This holds whenever a and b are two elements of a commutative ring, or, more generally, whenever a and b are two commuting elements of a 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.

Both can be done! (10 HW points for anyone who can combine these two!)

So we get two "q-binomial formulas" (q-analogues of the binomial formula). Here is the first:

Theorem 2.4.15 (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 $q=1$ here gives the original binomial formula, as behooves a q-analogue.

This theorem can be proved straightforwardly by induction on n (HW exercise), but there is also a nicer argument. Let me sketch it. We start with a general fact:

Lemma 2.4.16. Let L be a commutative ring. Let $n \in \mathbb{N}$. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. Let $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$ be $2n$ elements of L. Then,

$$\prod_{i=1}^{n} (a_i + b_i) = \sum_{S \subseteq [n]} \left(\prod_{i \in S} a_i\right) \left(\prod_{i \in [n] \setminus S} b_i\right).$$

Proof of 1st q-binomial theorem. Let $[n]$ be the set $\{1, 2, \ldots, n\}$. Then,

$$
\begin{aligned}
&\left(aq^0 + b\right)\left(aq^1 + b\right)\cdots\left(aq^{n-1} + b\right) \\
&= \prod_{i=1}^{n} \left(aq^{i-1} + b\right) \\
&= \sum_{S \subseteq [n]} \underbrace{\left(\prod_{i \in S} aq^{i-1}\right)}_{= a^{|S|} q^{\operatorname{sum} S - |S|}} \underbrace{\left(\prod_{i \in [n] \setminus S} b\right)}_{= b^{n-|S|}} \qquad \text{(by the lemma)} \\
&= \sum_{S \subseteq [n]} a^{|S|} q^{\operatorname{sum} S - |S|} b^{n-|S|} \\
&= \sum_{k=0}^{n} \sum_{\substack{S \subseteq [n]; \\ |S| = k}} a^k q^{\operatorname{sum} S - k} b^{n-k} \\
&= \sum_{k=0}^{n} \sum_{\substack{S \subseteq [n]; \\ |S| = k}} \underbrace{q^{\operatorname{sum} S - k}}_{\substack{= q^{\operatorname{sum} S - (1+2+\cdots+k)} q^{1+2+\cdots+(k-1)} \\ = q^{\operatorname{sum} S - (1+2+\cdots+k)} q^{k(k-1)/2}}} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \underbrace{\sum_{\substack{S \subseteq [n]; \\ |S| = k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}}_{\substack{= \binom{n}{k}_q \\ \text{(by part } \textbf{(b)} \text{ of the above proposition)}}} q^{k(k-1)/2} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k}_q q^{k(k-1)/2} a^k b^{n-k},
\end{aligned}
$$

qed. □

The second q-binomial theorem relies on noncommutativity:

Theorem 2.4.17 (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,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k}_\omega a^k b^{n-k}.$$

Example 2.4.18. The $ba = \omega ab$ condition is not that rare. For instance, let $L = \mathbb{Z}$ and $\omega = -1$ and $A = \mathbb{Z}^{2\times 2}$ (the ring of 2×2-matrices over $\mathbb{Z}$). Let

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then, $ba = -ab$, so that $ba = \omega ab$ for $\omega = -1$. Thus, the theorem above shows that

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

Example 2.4.19. 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, so $b(f) = f'$ for any $f \in C^{\infty}(\mathbb{R})$.

Let $a \in A$ be the operator that substitutes ωx for x in the function (i.e., we have $(a(f))(x) = f(\omega x)$).

Then, $ba = \omega ab$. (This is saying that $(f(\omega x))' = \omega f'(\omega x)$.)

Proving the second q-binomial formula is a HW exercise.

2.4.5. Counting subspaces of vector spaces

We have so far been viewing $\binom{n}{k}_q$ as a polynomial in q and interpreting this polynomial. Let us now look at some properties of its values $\binom{n}{k}_a = \binom{n}{k}_q [a]$ for specific numbers a. A particularly nice result holds when a is the size of a finite field.

We recall a few things about finite fields:

- For any prime power $p^k > 1$, there is a finite field of size p^k, unique up to isomorphism. (When the prime power is p, the field is just $\mathbb{Z}/p$.)
- Linear algebra (i.e., the theory of vector spaces, subspaces, linear independence, bases, matrices, Gaussian elimination, etc.) works over any field. If you know the right proofs, they all apply over any field. (Exceptions are some properties that require positivity or characteristic 0.)

Thus, we can talk about finite-dimensional vector spaces over finite fields. Such spaces are finite as sets. An n-dimensional vector space over a finite field F has size $|F|^n$.

Now we can ask ourselves more complicated questions, like: How many k-dimensional subspaces does such a space have?

Theorem 2.4.20. Let F be a finite field. Let $n, k \in \mathbb{N}$. Let V be an n-dimensional F-vector space. Then,

$$\binom{n}{k}_{|F|} = (\# \text{ of } k\text{-dimensional vector subspaces of } V).$$

For comparison,

$$\binom{n}{k} = (\# \text{ of } k\text{-element subsets of } S)$$

for any n-element set S. This analogy goes a lot deeper, and this is a subject currently under research. (See [Cohn04] reference in the notes for an introduction.)

To prove the theorem, we need a few lemmas:

Lemma 2.4.21. 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

$$\begin{aligned} v_1 &\notin \underbrace{\operatorname{span}()}_{=\{\mathbf{0}\}} \qquad \text{and} \\ v_2 &\notin \operatorname{span}(v_1) \qquad \text{and} \\ v_3 &\notin \operatorname{span}(v_1, v_2) \qquad \text{and} \\ &\cdots \qquad \text{and} \\ v_k &\notin \operatorname{span}(v_1, v_2, \ldots, v_{k-1}). \end{aligned}$$

More formally: $(v_1, v_2, \ldots, v_k)$ is linearly independent if and only if

$$v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1}) \text{ for each } i \in \{1, 2, \ldots, k\}.$$

Proof. $\Longrightarrow$: If $(v_1, v_2, \ldots, v_k)$ is linearly independent, then each $i \in \{1, 2, \ldots, k\}$ satisfies $v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1})$, since otherwise $(v_1, v_2, \ldots, v_i)$ would be linearly dependent, which cannot happen (since a subtuple of a linearly independent tuple is again independent).

$\Longleftarrow$: Assume that

$$v_i \notin \operatorname{span}(v_1, v_2, \ldots, v_{i-1}) \text{ for each } i \in \{1, 2, \ldots, k\}.$$

We must prove that $(v_1, v_2, \ldots, v_k)$ is independent. Assume the contrary. Thus,

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = \mathbf{0}$$

for some scalars $a_1, a_2, \ldots, a_k \in F$, not all zero. Pick the **largest** i for which $a_i \neq 0$. Then,

$$a_1 v_1 + a_2 v_2 + \cdots + a_i v_i = \mathbf{0}.$$

Solving this for v_i, we find

$$\begin{aligned} v_i &= \frac{-1}{a_i}\left(a_1 v_1 + a_2 v_2 + \cdots + a_{i-1} v_{i-1}\right) \qquad && (\text{since } a_i \neq 0) \\ &\in \operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right), \end{aligned}$$

contradicting our assumption. □

> **Lemma 2.4.22.** Let F be a finite field. Let $n, k \in \mathbb{N}$. Let V be an n-dimensional F-vector space. Then,
>
> $$\begin{aligned} &(\text{\# of linearly independent } k\text{-tuples of vectors in } V) \\ &= \prod_{i=0}^{k-1}\left(|F|^n - |F|^i\right) = \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right). \end{aligned}$$

Proof. We have $|V| = |F|^n$.

By the preceding lemma, a k-tuple $(v_1, v_2, \ldots, v_k)$ is linearly independent if and only if

$$v_i \notin \operatorname{span}\left(v_1, v_2, \ldots, v_{i-1}\right) \text{ for each } i \in \{1, 2, \ldots, k\}.$$

Thus, we can construct a linearly independent k-tuple $(v_1, v_2, \ldots, v_k)$ of vectors in V as follows:

- First, we choose v_1. This has to be a vector in $V \setminus \operatorname{span}()$. The number of options is thus $|V| - |\operatorname{span}()| = |V| - 1 = |F|^n - |F|^0$.
- Next, we choose v_2. This has to be a vector in $V \setminus \operatorname{span}(v_1)$. The number of options is thus $|V| - |\operatorname{span}(v_1)| = |V| - |F| = |F|^n - |F|^1$.
- Next, we choose v_3. This has to be a vector in $V \setminus \operatorname{span}(v_1, v_2)$. The number of options is thus $|V| - |\operatorname{span}(v_1, v_2)| = |V| - |F|^2 = |F|^n - |F|^2$.
- And so on.

The total # of ways to perform this construction is

$$\left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right) = \prod_{i=0}^{k-1}\left(|F|^n - |F|^i\right).$$

□

> **Lemma 2.4.23** (Multijection principle, aka shepherd's rule)**.** Let A and B be two finite sets ("legs" and "sheep", respectively). Let $m \in \mathbb{N}$. Let $f : A \to B$ be any map (sending each leg to its sheep). Assume that each $b \in B$ has exactly m preimages under f (that is, for each $b \in B$, there are exactly m elements $a \in A$ such that $f(a) = b$). Then,
>
> $$|A| = m \cdot |B| .$$
>
> (That is, the # of legs equals m times the # of sheep.)

Proof. LTTR. □

Proof of the theorem. We WLOG assume that $k \leq n$, since otherwise we are just proving that $0 = 0$.

We will say "independent" for "linearly independent".

We will say "k-dim subspace" for "k-dimensional vector subspace".

Consider the map

$$\begin{aligned} f : \{\text{independent } k\text{-tuples of vectors in } V\} &\to \{k\text{-dim subspaces of } V\} , \\ (v_1, v_2, \ldots, v_k) &\mapsto \operatorname{span}(v_1, v_2, \ldots, v_k) . \end{aligned}$$

Now we claim:

Claim 1: Each k-dim 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 Claim 1. Fix a k-dim subspace W of V. What are its preimages? They are the independent k-tuples $(v_1, v_2, \ldots, v_k)$ of vectors in V that satisfy $\operatorname{span}(v_1, v_2, \ldots, v_k) = W$. In other words, they are the independent k-tuples $(v_1, v_2, \ldots, v_k)$ of vectors in W that satisfy $\operatorname{span}(v_1, v_2, \ldots, v_k) = W$. The condition "$\operatorname{span}(v_1, v_2, \ldots, v_k) = W$" here is redundant, i.e., can be removed without changing the object being characterized (since any k independent vectors in a k-dimensional vector space must span the entire space). So they are the independent k-tuples $(v_1, v_2, \ldots, v_k)$ of vectors in W. Their number is therefore

$$\left(|F|^k - |F|^0\right) \left(|F|^k - |F|^1\right) \cdots \left(|F|^k - |F|^{k-1}\right)$$

(by our second lemma, applied to W and k instead of V and n). □

Claim 1 shows that each k-dim 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, by the multijection principle,

$$\begin{aligned}
&(\text{\# of independent } k\text{-tuples of vectors in } V) \\
&= \left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right) \\
&\qquad\qquad \cdot (\text{\# of } k\text{-dim subspaces of } V)\,.
\end{aligned}$$

But our second lemma says that

$$\begin{aligned}
&(\text{\# of independent } k\text{-tuples of vectors in } V) \\
&= \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right).
\end{aligned}$$

Comparing these two equalities, we find

$$\begin{aligned}
&\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right) \\
&\qquad\qquad \cdot (\text{\# of } k\text{-dim subspaces of } V) \\
&= \left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right).
\end{aligned}$$

Hence,

$$\begin{aligned}
&(\text{\# of } k\text{-dim subspaces of } V) \\
&= \frac{\left(|F|^n - |F|^0\right)\left(|F|^n - |F|^1\right)\cdots\left(|F|^n - |F|^{k-1}\right)}{\left(|F|^k - |F|^0\right)\left(|F|^k - |F|^1\right)\cdots\left(|F|^k - |F|^{k-1}\right)} \\
&= \frac{\left(|F|^n - 1\right)\left(|F|^{n-1} - 1\right)\cdots\left(|F|^{n-k+1} - 1\right)}{\left(|F|^k - 1\right)\left(|F|^{k-1} - |F|\right)\cdots\left(|F|^1 - 1\right)} \\
&\qquad\qquad \left(\text{here we cancelled } |F|^0\,|F|^1\,|F|^2\cdots|F|^{k-1}\right) \\
&= \frac{\left(1 - |F|^n\right)\left(1 - |F|^{n-1}\right)\cdots\left(1 - |F|^{n-k+1}\right)}{\left(1 - |F|^k\right)\left(1 - |F|^{k-1}\right)\cdots\left(1 - |F|^1\right)} \\
&\qquad\qquad \left(\text{here we cancelled } (-1)^k\right) \\
&= \binom{n}{k}_{|F|}.
\end{aligned}$$

□

2.4.6. Limits of q-binomial coefficients

Recall the notion of a limit of a sequence of FPSs: essentially, it is a matter of each coefficient stabilizing. This is a restrictive notion; for example, $\left(1+\dfrac{x}{n}\right)^n \not\to \exp$ using this notion. Nevertheless, limits sometimes exist.

Let's look at $\lim\limits_{n\to\infty} \dbinom{n}{2}_q$. Does this exist?

$$\begin{aligned}
\binom{0}{2}_q &= 0;\\
\binom{1}{2}_q &= 0;\\
\binom{2}{2}_q &= 1;\\
\binom{3}{2}_q &= 1+q+q^2;\\
\binom{4}{2}_q &= 1+q+2q^2+q^3+q^4;\\
\binom{5}{2}_q &= 1+q+2q^2+2q^3+2q^4+q^5+q^6;\\
\binom{6}{2}_q &= 1+q+2q^2+2q^3+3q^4+2q^5+2q^6+q^7+q^8.
\end{aligned}$$

These examples suggest that the sequence $\left(\dbinom{n}{2}_q\right)_{n\in\mathbb{N}}$ coefficientwise stabilizes to

$$1+q+2q^2+2q^3+3q^4+3q^5+\cdots = \sum_{n\in\mathbb{N}} \left(1+\left\lfloor \frac{n}{2}\right\rfloor\right) q^n.$$

This is indeed the case. More generally:

Proposition 2.4.24. Let $k \in \mathbb{N}$ be fixed. Then,

$$\begin{aligned}
\lim_{n\to\infty} \binom{n}{k}_q &= \sum_{n\in\mathbb{N}} \left(p_0\left(n\right)+p_1\left(n\right)+\cdots+p_k\left(n\right)\right) q^n\\
&= \prod_{i=1}^{k} \frac{1}{1-q^i}.
\end{aligned}$$

First proof. For each integer $n \geq k$, we have

$$\begin{aligned}
\binom{n}{k}_q &= \frac{\left(1-q^n\right)\left(1-q^{n-1}\right)\cdots\left(1-q^{n-k+1}\right)}{\left(1-q^k\right)\left(1-q^{k-1}\right)\cdots\left(1-q^1\right)} \\
&= \frac{\prod\limits_{i=1}^{k}\left(1-q^{n-k+i}\right)}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} = \frac{1}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} \cdot \prod_{i=1}^{k}\left(1-\underbrace{q^{n-k+i}}_{\substack{\to 0 \\ \text{as } n\to\infty}}\right) \\
&\to \frac{1}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} \cdot \underbrace{\prod_{i=1}^{k}\left(1-0\right)}_{=1} = \frac{1}{\prod\limits_{i=1}^{k}\left(1-q^i\right)} \\
&= \prod_{i=1}^{k}\frac{1}{1-q^i} \\
&= \sum_{n\in\mathbb{N}}\left(p_0\left(n\right)+p_1\left(n\right)+\cdots+p_k\left(n\right)\right)q^n \qquad \left(\begin{array}{c}\text{by something we}\\ \text{did a while ago}\end{array}\right).
\end{aligned}$$

□

Second proof (sketch). Recall that

$$\binom{n}{k}_q = \sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{\left|\lambda\right|}.$$

Thus,

$$\begin{aligned}
\lim_{n\to\infty}\binom{n}{k}_q &= \lim_{n\to\infty}\sum_{\substack{\lambda \text{ is a partition} \\ \text{with largest part } \leq n-k \\ \text{and length } \leq k}} q^{\left|\lambda\right|} = \sum_{\substack{\lambda \text{ is a partition} \\ \text{with length } \leq k}} q^{\left|\lambda\right|} \\
&= \sum_{n\in\mathbb{N}}\left(p_0\left(n\right)+p_1\left(n\right)+\cdots+p_k\left(n\right)\right)q^n \\
&= \prod_{i=1}^{k}\frac{1}{1-q^i}.
\end{aligned}$$

□

2.5. References

Some things we are missing:

- 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

$$\sum_{n\in\mathbb{N}} p(5n+4)\, x^n = 5 \prod_{i=1}^{\infty} \frac{\left(1-x^{5i}\right)^5}{\left(1-x^i\right)^6},$$

  which is far from obvious. See the notes for some references on this and related facts.

- Asymptotically,

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right) \qquad \text{as } n \to \infty.$$

  See the notes 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 quantitative statement: If n is a positive integer, then the number of quadruples (a, b, c, d) of integers satisfying $n = a^2 + b^2 + c^2 + d^2$ equals 8 times the sum of all positive divisors of n that are not divisible by 4. The most elementary proofs of this identity use partition-related FPSs and the Jacobi Triple Product identity. (Again, see references in the notes.)

- The Rogers–Ramanujan identities

$$\begin{aligned} \sum_{k\in\mathbb{N}} \frac{x^{k^2}}{\left(1-x^1\right)\left(1-x^2\right)\cdots\left(1-x^k\right)} &= \prod_{i\in\mathbb{N}} \frac{1}{\left(1-x^{5i+1}\right)\left(1-x^{5i+4}\right)}; \\ \sum_{k\in\mathbb{N}} \frac{x^{k(k+1)}}{\left(1-x^1\right)\left(1-x^2\right)\cdots\left(1-x^k\right)} &= \prod_{i\in\mathbb{N}} \frac{1}{\left(1-x^{5i+2}\right)\left(1-x^{5i+3}\right)} \end{aligned}$$

  can be used to count partitions into parts that are $\equiv \pm 1 \bmod 5$ or $\equiv \pm 2 \bmod 5$, respectively. These can also be proved using the Jacobi Triple Product.

I can also recommend Igor Pak's survey "Partition identities".
See also the HW.

3. Permutations

Permutations are one of the most fundamental combinatorial notions. Basic properties are studied in classes on algebra and enumeration, but we will try to go deeper and maybe be a bit more systematic. Again, see the notes for some references that go deeper.

3.1. Basic definitions

Definition 3.1.1. Let X be a set.

(a) A **permutation** of X means a bijection from X to X.

(b) The permutations of X form a group under composition. This group is called the **symmetric group** of X, and is denoted by S_X (or Σ_X or $\operatorname{Sym}(X)$ or $\mathfrak{S}_X$ or $\mathcal{S}_X$). Its size is $|X|!$ (when X is finite), and its neutral element is $\operatorname{id}_X : X \to X$.

(c) As usual in group theory, $\alpha\beta$ denotes the composition $\alpha \circ \beta$ when $\alpha, \beta \in S_X$. This is defined by $(\alpha\beta)(i) = \alpha(\beta(i))$ for all $i \in X$.

(d) If $\alpha \in S_X$ and $i \in \mathbb{Z}$, then α^i shall denote the i-th power of α in S_X. If $i \geq 0$, this is $\underbrace{\alpha\alpha\cdots\alpha}_{i \text{ times}}$. In particular, $\alpha^0 = \operatorname{id}$.

Definition 3.1.2. 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 $n \geq 0$).

Proposition 3.1.3. Let X and Y be two sets, and let $f : X \to Y$ be a bijection. Then, for any permutation $\sigma \in S_X$, the map $f \circ \sigma \circ f^{-1} : Y \to Y$ is a permutation in S_Y. Furthermore, the map

$$S_f : S_X \to S_Y,$$
$$\sigma \mapsto f \circ \sigma \circ f^{-1}$$

is a group isomorphism, so that $S_X \cong S_Y$.

This proposition (whose proof is straightforward) tells you that to understand S_X for all finite sets X, it suffices to understand S_n for all $n \in \mathbb{N}$ (because we can always find a bijection $f : X \to [n]$ for $n = |X|$).

Note that if $Y = X$ in the above proposition, then the map S_f is just conjugation by f in the group S_X.

Next, we define three ways to represent a permutation:

Definition 3.1.4. 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 $p_1, p_2, \ldots, p_n$ 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 in a OLN, at least when this does not create ambiguities. For instance, 346152 means $(3, 4, 6, 1, 5, 2)$, and (by extension) the permutation in S_6 whose OLN is $(3, 4, 6, 1, 5, 2)$.

(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 i to the node $\sigma(i)$.

The resulting picture is called the cycle digraph of σ.

Using the concept of **digraphs** (= directed graphs), it can be formally defined as the directed graph with vertices $1, 2, \ldots, n$ and arcs $i \to \sigma(i)$ for each $i \in [n]$.

(See the notes for more examples.)

3.2. Transpositions and cycles

3.2.1. Transpositions

Definition 3.2.1. 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.

Note that $t_{i,j} = t_{j,i}$.

Definition 3.2.2. Let $n \in \mathbb{N}$ and $i \in [n-1]$. Then, the **simple transposition** s_i is defined by

$$s_i := t_{i,i+1} \in S_n.$$

So a simple transposition is a transposition that swaps two consecutive integers. For instance, $s_2 \in S_7$ has OLN $(1,3,2,4,5,6,7)$. Generally, $s_i \in S_n$ has OLN

$$(1,2,\ldots,i-1,i+1,i,i+2,i+3,\ldots,n).$$

Here are some very basic facts about simple transpositions.

Proposition 3.2.3. Let $n \in \mathbb{N}$.
(a) We have $s_i^2 = \operatorname{id}$ and $s_i = s_i^{-1}$ for any $i \in [n-1]$.
(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 $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} = t_{i,i+2}$ for any $i \in [n-2]$.

Proof. Straightforward verification that numbers go to the same places. □

3.2.2. Cycles

A generalization of transpositions are cycles:

Definition 3.2.4. 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

$$\begin{aligned} i_1 &\mapsto i_2, \\ i_2 &\mapsto i_3, \\ i_3 &\mapsto i_4, \\ &\ldots, \\ i_{k-1} &\mapsto i_k, \\ i_k &\mapsto i_1 \end{aligned}$$

and leaves all other elements of X unchanged. This permutation is called a k**-cycle**.

Note that $\operatorname{cyc}_i = \operatorname{id}$ and $\operatorname{cyc}_{i,j} = t_{i,j}$.

Example 3.2.5. Let X be a set. Then, for any distinct $i,j \in X$, we have $\operatorname{cyc}_{i,j} = t_{i,j} = t_{j,i}$. So the 2-cycles in S_X are exactly the transpositions. How many are there? $\binom{n}{2}$, since we have to choose two distinct elements i,j and the order does not matter.

Note that the k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ is sometimes denoted $(i_1, i_2, \ldots, i_k)$.

Exercise 3.2.1. Let $n \in \mathbb{N}$ and $k \in [n]$. Let X be an n-element set. How many k-cycles exist in S_X ?

Solution. Assume that $k > 1$ (since otherwise, the answer is 1).

Each k-cycle has the form $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ for some k-tuple $(i_1, i_2, \ldots, i_k)$ of distinct elements of X; but different k-tuples can give rise to equal k-cycles. For example,

$$\operatorname{cyc}_{1,2,3} = \operatorname{cyc}_{2,3,1} \neq \operatorname{cyc}_{2,1,3} = \operatorname{cyc}_{1,3,2}.$$

More generally, for any k distinct elements $i_1, i_2, \ldots, i_k$ of X, we have

$$\operatorname{cyc}_{i_1,i_2,\ldots,i_k} = \operatorname{cyc}_{i_2,i_3,\ldots,i_k,i_1} = \operatorname{cyc}_{i_3,i_4,\ldots,i_k,i_1,i_2} = \cdots = \operatorname{cyc}_{i_k,i_1,i_2,\ldots,i_{k-1}}.$$

So k different k-tuples give rise to the same k-cycle.

Conversely, any k-cycle $\operatorname{cyc}_{i_1,i_2,\ldots,i_k}$ uniquely determines the k-tuple $(i_1, i_2, \ldots, i_k)$ up to cyclic rotation, since the elements $i_1, i_2, \ldots, i_k$ are precisely the elements of X not fixed by the k-cycle (here we need $k > 1$), and once you choose which of these elements is i_1, the other elements are uniquely determined (i_2 is the image of i_1; i_3 is the image of i_2; and so on).

So 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 has exactly k preimages under this map). Thus, by the multijection principle,

$$\begin{aligned} &(\#\text{ of } k\text{-tuples of distinct elements of } X) \\ &= k \cdot (\#\text{ of } k\text{-cycles in } S_X), \end{aligned}$$

and therefore

$$\begin{aligned} (\#\text{ of } k\text{-cycles in } S_X) &= \frac{1}{k} \cdot \underbrace{(\#\text{ of } k\text{-tuples of distinct elements of } X)}_{=n(n-1)(n-2)\cdots(n-k+1)} \\ &= \frac{1}{k} \cdot \underbrace{n(n-1)(n-2)\cdots(n-k+1)}_{=\binom{n}{k}\cdot k!} \\ &= \frac{1}{k} \cdot \binom{n}{k} \cdot k! = \binom{n}{k} \cdot \underbrace{\frac{k!}{k}}_{=(k-1)!} = \binom{n}{k} \cdot (k-1)!. \end{aligned}$$

So this is the answer for $k > 1$. □

3.3. Inversions, length and Lehmer codes

3.3.1. Inversions and lengths

Definition 3.3.1. 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 $i < j$ but $\sigma(i) > \sigma(j)$.

(b) The **length** (also known as the **Coxeter length**) of σ is the # of inversions of . It is called $\ell(\sigma)$ or $\operatorname{inv}\sigma$. (In LaTeX, ℓ is written \ell.)

Example 3.3.2. The permutation $\pi \in S_4$ with OLN 3142 has inversions

$$(1,2), \quad (1,4), \quad (3,4)$$

and length 3.

Now you might wonder how many permutations in S_n have a given length.

Proposition 3.3.3. 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 $n(n-1)(n-2)\cdots 21$. (Often it is called w_0.)

(d) If $n \geq 1$, then

$$(\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = 1) = n - 1.$$

Indeed, the only permutations $\sigma \in S_n$ with $\ell(\sigma) = 1$ are the simple transpositions $s_1, s_2, \ldots, s_{n-1}$.

(e) If $n \geq 2$, then

$$(\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = 2) = \frac{(n-2)(n+1)}{2}.$$

(See the HW for details.)

(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. HW. □

What about the general case: can we compute (# of $\sigma \in S_n$ with $\ell(\sigma) = k$)? Not explicitly, but we can find a recursion (HW?) and a generating function.

Example 3.3.4. For $n = 3$, we have

$$\begin{aligned}
&\sum_{k\in\mathbb{N}} (\text{\# of } \sigma \in S_n \text{ with } \ell(\sigma) = k) \cdot x^k \\
&= \sum_{\sigma\in S_n} x^{\ell(\sigma)} \\
&= 1 + 2x + 2x^2 + x^3 = (1+x)\left(1+x+x^2\right).
\end{aligned}$$

More generally:

Proposition 3.3.5. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}
\sum_{\sigma\in S_n} x^{\ell(\sigma)} &= \prod_{i=1}^{n-1}\left(1+x+x^2+\cdots+x^i\right) \\
&= (1+x)\left(1+x+x^2\right)\left(1+x+x^2+x^3\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right) \\
&= [n]_x!.
\end{aligned}$$

3.3.2. Lehmer codes

We will prove this proposition using the so-called **Lehmer codes** of permutations:

Definition 3.3.6. Let $n \in \mathbb{N}$.

(a) For each $\sigma \in S_n$ and each $i \in [n]$, we set

$$\begin{aligned}
\ell_i(\sigma) &:= (\text{\# of all } j \in [n] \text{ such that } i < j \text{ but } \sigma(i) > \sigma(j)) \\
&= (\text{\# of all } j \in \{i+1, i+2, \ldots, n\} \text{ such that } \sigma(i) > \sigma(j)).
\end{aligned}$$

(b) For each $m \in \mathbb{Z}$, we let $[m]_0$ denote the set $\{0, 1, \ldots, m\}$. (This is an empty set if $m < 0$.)

(c) We let H_n be the set

$$\begin{aligned}
&[n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0 \\
&= \{(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n \mid j_i \le n - i \text{ for each } i \in [n]\}.
\end{aligned}$$

This set H_n has size

$$\begin{aligned} |H_n| &= |[n-1]_0 \times [n-2]_0 \times \cdots \times [n-n]_0| \\ &= |[n-1]_0| \cdot |[n-2]_0| \cdot \cdots \cdot |[n-n]_0| \\ &= n \cdot (n-1) \cdot \cdots \cdot (n-n+1) = n!. \end{aligned}$$

(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 is well-defined, since $\ell_i(\sigma) \leq n - i$ for each $i \in [n]$ (why?).

(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** of σ.

Example 3.3.7. Let $\sigma \in S_6$ be the permutation with OLN 341625. Its Lehmer code is

$$L(\sigma) = (2, 2, 0, 2, 0, 0).$$

Example 3.3.8. Can you find a permutation $\sigma \in S_6$ with Lehmer code

$$L(\sigma) = (1, 4, 2, 1, 0, 0) \ ?$$

It must start with 2, since $\ell_1(\sigma) = 1$ means that there is exactly 1 entry in its OLN to the right of the first entry and smaller than the first entry. The next entry of σ (in OLN) must be 6, for a similar reason (note that the 2 is already placed in the first position, so it is no longer relevant). And so on.

So the OLN of σ is $(2, 6, 4, 3, 1, 5)$.

Note that this σ exists and is unique.

What we learn from this example is that the map $L : S_n \to H_n$ is a bijection – i.e., every n-tuple in H_n is the Lehmer code of a unique permutation $\sigma \in S_n$. This argument works in general, but is tricky to formalize, which is why I will outline another proof of this fact.

Let me first state a simple fact:

Proposition 3.3.9. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then,

$$\ell(\sigma) = \ell_1(\sigma) + \ell_2(\sigma) + \cdots + \ell_n(\sigma).$$

Now I will prove:

Theorem 3.3.10. Let $n \in \mathbb{N}$. Then, the map $L : S_n \to H_n$ is a bijection.

In the notes, I outline two proofs. The first one essentially formalizes the algorithm above. The idea that we used to reconstruct σ from $L(\sigma)$ is that

$$\ell_i(\sigma) = (\text{\# of elements of } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\} \\ \text{that are smaller than } \sigma(i)),$$

so that

$$\sigma(i) = (\text{the } (\ell_i(\sigma)+1)\text{-th smallest element of} \\ \text{the set } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}).$$

This formula allows us to recursively determine $\sigma(i)$ from $L(\sigma)$. Thus, the map L is injective. To prove that L is surjective, we have to use the above construction backwards: Given an n-tuple $(h_1, h_2, \ldots, h_n) \in H_n$, we recursively define $\sigma(1), \sigma(2), \ldots, \sigma(n)$ by

$$\sigma(i) = (\text{the } (h_i+1)\text{-th smallest element of} \\ \text{the set } [n] \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i-1)\}).$$

We have to argue that this really is well-defined and gives a permutation $\sigma \in S_n$.

The second proof is "simpler" to some extent, as it uses two nice tricks instead of this recursive construction. The first trick is to use a total order to prove injectivity. Specifically, we use an important total order that can be defined on the set $\mathbb{Z}^n$ or, more generally, on any Cartesian product of totally ordered sets:

Definition 3.3.11. 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

$$(a_1, a_2, \ldots, a_n) <_{\text{lex}} (b_1, b_2, \ldots, b_n)$$

(pronounced "$(a_1, a_2, \ldots, a_n)$ is **lexicographically smaller** than $(b_1, b_2, \ldots, b_n)$") 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,

$$(4,1,2,5) <_{\text{lex}} (4,1,3,0), \\ (1,1,0,1) <_{\text{lex}} (2,0,0,0).$$

It is easy to see that:

Proposition 3.3.12. 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, $<_{\text{lex}}$ is a total order on $\mathbb{Z}^n$. This is also easy to see.

Now here is a crucial fact:

Proposition 3.3.13. Let $\sigma \in S_n$ and $\tau \in S_n$ be such that

$$(\sigma(1), \sigma(2), \ldots, \sigma(n)) <_{\text{lex}} (\tau(1), \tau(2), \ldots, \tau(n)).$$

Then,

$$L(\sigma) <_{\text{lex}} L(\tau).$$

Proof. Easy (see the notes). □

This proposition immediately yields that L is injective (because if $\sigma \neq \tau$, then WLOG assume that $\sigma <_{\text{lex}} \tau$, and thus $L(\sigma) <_{\text{lex}} L(\tau)$ and therefore $L(\sigma) \neq L(\tau)$). This was the first trick.

The second trick is the pigeonhole principle: An injective map between two finite sets of the same size must be bijective. Since L is an injective map from S_n to H_n, it thus follows that L is bijective, since $|S_n| = n! = |H_n|$. (This requires you to have a proof of $|S_n| = n!$ that does not use the Lehmer code.)

Proof of the proposition about the generating function. We have

$$\begin{aligned}
\sum_{\sigma \in S_n} x^{\ell(\sigma)} &= \sum_{\sigma \in S_n} x^{\ell_1(\sigma)+\ell_2(\sigma)+\cdots+\ell_n(\sigma)} \\
&= \sum_{(j_1,j_2,\ldots,j_n)\in H_n} x^{j_1+j_2+\cdots+j_n} \\
&\qquad \left(\begin{array}{c}\text{here, we substituted } (j_1,j_2,\ldots,j_n) \text{ for the} \\ \text{Lehmer code } L(\sigma) = (\ell_1(\sigma), \ell_2(\sigma), \ldots, \ell_n(\sigma)), \\ \text{since the map } L : S_n \to H_n \text{ is a bijection}\end{array}\right) \\
&= \sum_{(j_1,j_2,\ldots,j_n)\in[n-1]_0\times[n-2]_0\times\cdots\times[n-n]_0} x^{j_1}x^{j_2}\cdots x^{j_n} \\
&= \left(\sum_{j_1=0}^{n-1} x^{j_1}\right)\left(\sum_{j_2=0}^{n-2} x^{j_2}\right)\cdots\left(\sum_{j_n=0}^{n-n} x^{j_n}\right) \\
&= \left(1+x+x^2+\cdots+x^{n-1}\right)\left(1+x+x^2+\cdots+x^{n-2}\right)\cdots(1) \\
&= 1(1+x)\left(1+x+x^2\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right) \\
&= (1+x)\left(1+x+x^2\right)\cdots\left(1+x+x^2+\cdots+x^{n-1}\right) \\
&= \prod_{i=1}^{n-1}\left(1+x+x^2+\cdots+x^i\right) = [n]_x!.
\end{aligned}$$

□

3.3.3. More about lengths and simples

Recall: The length (or Coxeter length) $\ell(\sigma)$ of a permutation $\sigma \in S_n$ is the # of its inversions (i.e., pairs (i,j) with $i<j$ but $\sigma(i)>\sigma(j)$).

Proposition 3.3.14. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Then, $\ell\left(\sigma^{-1}\right) = \ell(\sigma)$.

Proof. We have a bijection

$$\begin{aligned} \{\text{inversions of } \sigma\} &\to \left\{\text{inversions of } \sigma^{-1}\right\}, \\ (i,j) &\mapsto (\sigma(j), \sigma(i)). \end{aligned}$$

Thus, the # of inversions of σ^{-1} equals that of σ, qed. □

The following lemma is crucial, as it allows for a recursive approach to lengths of a permutations:

Lemma 3.3.15 (single swap lemma)**.** Let $n \in \mathbb{N}$, $\sigma \in S_n$ and $k \in [n-1]$. Recall that $s_k = t_{k,k+1}$. 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 OLN of σ, whereas $\sigma^{-1}(i)$ is the **position** in which i appears in the OLN of σ.]

Proof idea. (See the notes for more details.)

Example: $\sigma = 512634 \in S_6$ and $k=3$. Then,

$$\begin{aligned} \sigma s_k &= \sigma s_3 = 516234; \\ s_k\sigma &= s_3\sigma = 512643. \end{aligned}$$

In general, in terms of OLNs, σs_k is σ with the k-th and $(k+1)$-th entries swapped, whereas $s_k\sigma$ is σ with the entries k and $k+1$ swapped (no matter where they are).

How do such swaps affect the # of inversions? Let us consider the second kind of swap, where we swap the entries k and $k+1$. What happens to an inversion? In terms of OLNs, an inversion is just a pair of two positions in which the entries are out of order (i.e., the left entry is larger than the right). When we swap the entries k and $k+1$, their positions turn into an inversion if they weren't one before, and vice versa. Specifically:

- If $\left(\sigma^{-1}\left(k\right), \ \sigma^{-1}\left(k+1\right)\right)$ was not an inversion of σ (that is, if $\sigma^{-1}\left(k\right) < \sigma^{-1}\left(k+1\right)$), then it will be an inversion of $s_k\sigma$.
- If $\left(\sigma^{-1}\left(k\right), \ \sigma^{-1}\left(k+1\right)\right)$ was an inversion of σ (that is, if $\sigma^{-1}\left(k\right) > \sigma^{-1}\left(k+1\right)$), then it will not be an inversion of $s_k\sigma$.

What about the other inversions? Those will not change from σ to $s_k\sigma$, because an integer that is neither k nor $k+1$ will have the same order relation to $k+1$ as it had to k (and vice versa). For example, if a given pair of positions of σ had entries $k+4$ and k in σ, then it will have entries $k+4$ and $k+1$ in $s_k\sigma$, so its inversion-ness does not change.

Altogether, we see that $s_k\sigma$

- has 1 more inversion than σ if $\sigma^{-1}\left(k\right) < \sigma^{-1}\left(k+1\right)$;
- has 1 fewer inversion than σ if $\sigma^{-1}\left(k\right) > \sigma^{-1}\left(k+1\right)$.

In other words,

$$\ell\left(s_k\sigma\right) = \begin{cases} \ell\left(\sigma\right)+1, & \text{if } \sigma^{-1}\left(k\right) < \sigma^{-1}\left(k+1\right); \\ \ell\left(\sigma\right)-1, & \text{if } \sigma^{-1}\left(k\right) > \sigma^{-1}\left(k+1\right). \end{cases}$$

This proves part **(b)**.

For part **(a)**, we must prove

$$\ell\left(\sigma s_k\right) = \begin{cases} \ell\left(\sigma\right)+1, & \text{if } \sigma\left(k\right) < \sigma\left(k+1\right); \\ \ell\left(\sigma\right)-1, & \text{if } \sigma\left(k\right) > \sigma\left(k+1\right). \end{cases}$$

This can be argued by "moving" the inversions of σ along with the swap. See the Math 235 Fall 2023 notes for this.

Alternatively, we can derive **(a)** from **(b)**, by applying **(b)** to σ^{-1} instead of σ. Indeed, this yields

$$\begin{aligned} \ell\left(s_k\sigma^{-1}\right) &= \begin{cases} \ell\left(\sigma^{-1}\right)+1, & \text{if } \sigma\left(k\right) < \sigma\left(k+1\right); \\ \ell\left(\sigma^{-1}\right)-1, & \text{if } \sigma\left(k\right) > \sigma\left(k+1\right) \end{cases} \\ &= \begin{cases} \ell\left(\sigma\right)+1, & \text{if } \sigma\left(k\right) < \sigma\left(k+1\right); \\ \ell\left(\sigma\right)-1, & \text{if } \sigma\left(k\right) > \sigma\left(k+1\right) \end{cases} \end{aligned}$$

(since $\ell\left(\sigma^{-1}\right) = \ell\left(\sigma\right)$). But

$$\begin{aligned} \ell\left(\sigma s_k\right) &= \ell\left(\left(\sigma s_k\right)^{-1}\right) = \ell\left(s_k^{-1}\sigma^{-1}\right) = \ell\left(s_k\sigma^{-1}\right) \\ &= \begin{cases} \ell\left(\sigma\right)+1, & \text{if } \sigma\left(k\right) < \sigma\left(k+1\right); \\ \ell\left(\sigma\right)-1, & \text{if } \sigma\left(k\right) > \sigma\left(k+1\right). \end{cases} \end{aligned}$$

So **(a)** follows from **(b)**. □

There is also somewhat of a formula for $\ell\left(\sigma t_{i,j}\right)$:

Proposition 3.3.16. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. Let $i, j \in [n]$ such that $i < j$. Then,

$$\ell\left(\sigma t_{i,j}\right) = \begin{cases} \ell\left(\sigma\right) - 2\left|Q\right| - 1, & \text{if } \sigma\left(i\right) < \sigma\left(j\right); \\ \ell\left(\sigma\right) + 2\left|R\right| + 1, & \text{if } \sigma\left(i\right) > \sigma\left(j\right), \end{cases}$$

where

$$\begin{aligned} Q &= \left\{k \in \left\{i+1, i+2, \ldots, j-1\right\} \mid \sigma\left(i\right) > \sigma\left(k\right) > \sigma\left(j\right)\right\}, \\ R &= \left\{k \in \left\{i+1, i+2, \ldots, j-1\right\} \mid \sigma\left(i\right) < \sigma\left(k\right) < \sigma\left(j\right)\right\}. \end{aligned}$$

Proof. See reference in notes. □

Now, let us see what simples are good for.

Convention 3.3.17. We recall that a **simple transposition** (for short, **simple**) in S_n means one of the $n-1$ transpositions $s_1, s_2, \ldots, s_{n-1}$.

Theorem 3.3.18 (1st reduced word theorem for 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 $\ell\left(\sigma\right)$ simples.

(b) The number $\ell\left(\sigma\right)$ is the smallest $p \in \mathbb{N}$ such that we can write σ as a product of p simples.

[Keep in mind: The product of 0 simples is id.]

Example 3.3.19. Let $\sigma = 4132 \in S_4$. How can we write σ as a product of $\ell\left(\sigma\right) = 4$ simples? For example,

$$\sigma = \underbrace{s_2 s_3 s_2}_{= s_2 s_3 s_2} s_1 = s_3 s_2 \underbrace{s_3 s_1}_{= s_1 s_3} = s_3 s_2 s_1 s_3 = s_3 s_2 s_1 s_3 s_1 s_1 = \cdots.$$

Proof sketch. **(a)** Induct on $\ell\left(\sigma\right)$.

Base case: If $\ell\left(\sigma\right) = 0$, then $\sigma = \mathrm{id}$, which is clearly the empty product of simples.

Induction step: Fix $\sigma \in S_n$ with $\ell\left(\sigma\right) > 0$. Assume (as the IH) that the theorem (part **(a)** of it) already is proved for all permutations with length $\ell\left(\sigma\right) - 1$. We must now prove it for σ.

Since $\ell\left(\sigma\right) > 0$, we cannot have $\sigma\left(1\right) \leq \sigma\left(2\right) \leq \cdots \leq \sigma\left(n\right)$. So there exists some $k \in [n-1]$ such that $\sigma\left(k\right) > \sigma\left(k+1\right)$. Consider this k, and observe (by the previous lemma) that $\ell\left(\sigma s_k\right) = \ell\left(\sigma\right) - 1$. Hence, by the IH, σs_k can be written as a product of $\ell\left(\sigma\right) - 1$ many simples. In other words,

$$\sigma s_k = s_{i_1} s_{i_2} \cdots s_{i_{\ell(\sigma)-1}} \qquad \text{for some } i\text{'s.}$$

Hence,

$$\sigma = s_{i_1} s_{i_2} \cdots s_{i_{\ell(\sigma)-1}} \underbrace{s_k^{-1}}_{=s_k} = s_{i_1} s_{i_2} \cdots s_{i_{\ell(\sigma)-1}} s_k,$$

which shows that σ is a product of $\ell(\sigma)$ many simples. Proof complete.

(b) In view of part **(a)**, we only need to show that fewer than $\ell(\sigma)$ simples do not suffice to get σ as a product. For this purpose, it will be enough to show that

$$\ell\left(s_{i_1} s_{i_2} \cdots s_{i_g}\right) \leq g \qquad \text{for any } i_1, i_2, \ldots, i_g.$$

This again follows (by induction on g) from our above lemma (which shows that $\ell(\sigma s_k) \leq \ell(\sigma) + 1$ for any σ and k).

See the notes for details. □

Corollary 3.3.20. Let $n \in \mathbb{N}$.

(a) We have $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \operatorname{mod} 2$ 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 $q \equiv \ell(\sigma) \operatorname{mod} 2$.

Proof. **(a)** For any $\sigma \in S_n$ and any $k \in [n-1]$, we have

$$\begin{aligned} \ell(\sigma s_k) &= \begin{cases} \ell(\sigma)+1, & \text{if } \sigma(k) < \sigma(k+1); \\ \ell(\sigma)-1, & \text{if } \sigma(k) > \sigma(k+1) \end{cases} \qquad \text{(by the lemma)} \\ &\equiv \ell(\sigma) + 1 \operatorname{mod} 2. \end{aligned}$$

Now, let $\sigma, \tau \in S_n$. By the above theorem, we can write τ as a composition of $\ell(\tau)$ simples:

$$\tau = s_{k_1} s_{k_2} \cdots s_{k_q} \qquad \text{where } q = \ell(\tau).$$

Then,

$$\begin{aligned} \ell(\sigma\tau) &= \ell\left(\sigma s_{k_1} s_{k_2} \cdots s_{k_q}\right) \\ &\equiv \ell\left(\sigma s_{k_1} s_{k_2} \cdots s_{k_{q-1}}\right) + 1 \operatorname{mod} 2 \\ &\equiv \ell\left(\sigma s_{k_1} s_{k_2} \cdots s_{k_{q-2}}\right) + 1 + 1 \operatorname{mod} 2 \\ &\equiv \ell\left(\sigma s_{k_1} s_{k_2} \cdots s_{k_{q-3}}\right) + 1 + 1 + 1 \operatorname{mod} 2 \\ &\equiv \cdots \\ &\equiv \ell(\sigma) + \underbrace{1 + 1 + \cdots + 1}_{q \text{ times}} \operatorname{mod} 2 \\ &= \ell(\sigma) + q = \ell(\sigma) + \ell(\tau) \operatorname{mod} 2. \end{aligned}$$

(b) Analogous.

(c) Follows easily from **(a)** and **(b)**. □

Corollary 3.3.21. Let $n \in \mathbb{N}$. Then, the group S_n is generated by the simples $s_1, s_2, \ldots, s_{n-1}$.

Actually, there is an explicit way of writing a permutation $\sigma \in S_n$ as a product of simples:

Proposition 3.3.22. Let $n \in \mathbb{N}$ and $\sigma \in S_n$. For each $i \in [n]$, we set

$$a_i := \operatorname{cyc}_{i', i'-1, i'-2, \ldots, i} = s_{i'-1} s_{i'-2} s_{i'-3} \cdots s_i,$$

where $i' = i + \ell_i(\sigma)$. Then,

$$\sigma = a_1 a_2 \cdots a_n.$$

Proof. See the notes. (See the notes also for a visual way to illustrate this proposition.) □

3.4. Signs of permutations

The notion of the **sign** (aka **signature**) of a permutation is a simple consequence of that of its length; it is furthermore quite well-known.

Definition 3.4.1. 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 $\operatorname{sign} \sigma$ or $\operatorname{sgn} \sigma$ or $\varepsilon(\sigma)$.

Proposition 3.4.2. 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 $\sigma, \tau \in S_n$.

(e) We have $(-1)^{\sigma_1 \sigma_2 \cdots \sigma_p} = (-1)^{\sigma_1} (-1)^{\sigma_2} \cdots (-1)^{\sigma_p}$ for any $\sigma_i \in S_n$.

(f) We have $(-1)^{\sigma^{-1}} = (-1)^\sigma$ for any $\sigma \in S_n$.

(g) We have

$$(-1)^\sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} \qquad \text{for each } \sigma \in S_n.$$

(h) If $x_1, x_2, \ldots, x_n$ are any elements of any commutative ring, and $\sigma \in S_n$, then

$$\prod_{1 \leq i < j \leq n} \left(x_{\sigma(i)} - x_{\sigma(j)} \right) = (-1)^\sigma \cdot \prod_{1 \leq i < j \leq n} \left(x_i - x_j \right).$$

Proof. All of this is well-known; see the references in the notes; but I will sketch the most important steps.

(b) See the blackboard.

(c) HW.

(d) We need to show that $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \bmod 2$. But this has been done above.

(h) The differences $x_{\sigma(i)} - x_{\sigma(j)}$ for $1 \leq i < j \leq n$ are precisely the differences $x_i - x_j$ for $1 \leq i < j \leq n$ up to sign and order. So their products agree up to sign. The question is: Why is this sign $(-1)^\sigma$? The reason is that $\ell(\sigma)$ is precisely how often the signs are flipped (each inversion of σ flips a sign). □

Corollary 3.4.3. 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 cyclic order-2 group $\{1, -1\}$ (with multiplication).

This homomorphism is called the **sign homomorphism**.

Definition 3.4.4. Let $n \in \mathbb{N}$. A permutation $\sigma \in S_n$ is said to be

- **even** if $(-1)^\sigma = 1$ (that is, $\ell(\sigma)$ is even);
- **odd** if $(-1)^\sigma = -1$ (that is, $\ell(\sigma)$ is odd).

See also: 15-puzzle, as well as various other permutation puzzles.

Corollary 3.4.5. 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 it is a simple group, which makes it useful in Galois theory (it is the reason for the unsolvability of the quintic) and also in group theory.

Let's find its size:

Corollary 3.4.6. Let $n \geq 2$. Then,

$$(\text{\# of even permutations in } S_n) = (\text{\# of odd permutations in } S_n) = \frac{n!}{2}.$$

Proof. The map

$$\begin{aligned} \{\text{even permutations in } S_n\} &\to \{\text{odd permutations in } S_n\}, \\ \sigma &\mapsto \sigma s_1 \end{aligned}$$

is a bijection (because the inverse map can be defined in the same way). So

$$(\text{\# of even permutations in } S_n) = (\text{\# of odd permutations in } S_n).$$

Since these two numbers add up to $n!$, they must be $\dfrac{n!}{2}$. □

As a consequence of this corollary, we have

$$\sum_{\sigma \in S_n} (-1)^{\sigma} = 0 \qquad \text{for } n \geq 2.$$

Unlike the length of a permutation, the sign of a permutation can be defined not just for $\sigma \in S_n$ but also for $\sigma \in S_X$ for any finite set X. Here is one way to do so:

Proposition 3.4.7. 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 ϕ exists, since X is finite.)

For every permutation $\sigma \in S_X$, we define

$$(-1)^{\sigma}_{\phi} := (-1)^{\phi \circ \sigma \circ \phi^{-1}}$$

(note that $\phi \circ \sigma \circ \phi^{-1} \in S_n$ has a well-defined sign already). Now:

(a) This number $(-1)^{\sigma}_{\phi}$ depends only on σ, not on ϕ. So we can write $(-1)^{\sigma}$ for it, and call it the **sign** of σ.

(b) The identity permutation $\mathrm{id} : X \to X$ satisfies $(-1)^{\mathrm{id}} = 1$.

(c) We have $(-1)^{\sigma\tau} = (-1)^{\sigma} \cdot (-1)^{\tau}$ for any $\sigma, \tau \in S_X$.

Proof. Easy; see reference in the notes. □

3.5. The cycle decomposition

We shall next discuss the **cycle decomposition** (or **disjoint cycle decomposition**) of a permutation. See the notes for an example.

Theorem 3.5.1 (disjoint cycle decomposition of a permutation)**.** Let X be a finite set. Let $\sigma \in S_X$. Then:

(a) There is a list

$$\begin{aligned} (\ &(a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}), \\ &(a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}), \\ &\ldots, \\ &(a_{k,1}, a_{k,2}, \ldots, a_{k,n_k})\ \ ) \end{aligned}$$

of nonempty 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** (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

$$\begin{aligned}(\ & (a_{1,1}, a_{1,2}, \ldots, a_{1,n_1}), \\ & (a_{2,1}, a_{2,2}, \ldots, a_{2,n_2}), \\ & \ldots, \\ & (a_{k,1}, a_{k,2}, \ldots, a_{k,n_k})\ \ )\end{aligned}$$

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 has its smallest entry up front), 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 3.5.2. Let $\sigma \in S_9$ be the permutation with OLN 613548792. Then, the unique DCD from part **(c)** of the above theorem is

$$(\ (7),\ (4,5),\ (3),\ (1,6,8,9,2)\ ).$$

Other DCDs are obtained from this one by rotating and swapping cycles, e.g.

$$(\ (3),\ (9,2,1,6,8),\ (4,5),\ (7)\ ).$$

Proof. Fairly easy, but hard to explain. See the notes. □

Definition 3.5.3. Let X be a finite set. Let $\sigma \in S_X$.

(a) The **cycles** of σ are defined to be the cycles in the DCD of σ. (This includes 1-cycles.) We shall identify each cycle with its cyclic rotations; for example, $(1,4,3)$ and $(4,3,1)$ count as the same cycle.

(b) The **cycle length partition** of σ shall denote the partition of $|X|$ obtained by writing down the lengths of the cycles of σ in weakly decreasing order.

For instance, the permutation σ in the example above has cycle length partition $(5,2,1,1)$.

Proposition 3.5.4. 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. See the notes. □

The notes also contain some references to further literature on permutations, including entire books (Bona, Kitaev); the HW problems also contain some taste of it.

4. Alternating sums, signed counting, determinants

Alternating sums are sums whose addends have "alternating" signs – usually sums of the form $\sum\limits_k (-1)^k$ (something) or $\sum\limits_{\sigma \in S_n} (-1)^{\sigma}$ (something) or likewise.

Alternating sums are often easier to compute than "usual" (positive) sums. For instance, there is no closed form for $\sum\limits_{k=0}^{n} \dbinom{n}{k}^3$, but there is one for $\sum\limits_{k=0}^{n} (-1)^k \dbinom{n}{k}^3$, namely

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3 = \begin{cases} (-1)^{n/2} \dfrac{(3n/2)!}{(n/2)!^3}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

(This is a HW exercise, and is known as Dixon's identity.)

4.1. Cancellations in alternating sums

We begin with a simple binomial identity:

> **Proposition 4.1.1** (negative hockey-stick identity)**.** Let $n \in \mathbb{C}$ and $m \in \mathbb{N}$. Then,
> $$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}.$$

Proof. There are many ways to show this; here is a combinatorial one.

The claim is a polynomial identity in n. So it suffices to prove it when n is a positive integer (by the polynomial identity trick). Thus, let us WLOG assume that n is a positive integer.

Set $[n] := \{1, 2, \ldots, n\}$. Define an **acceptable set** to be a subset of $[n]$ that has size $\leq m$. Thus,

$$(\text{\# of acceptable sets}) = \sum_{k=0}^{m} \binom{n}{k}.$$

Define the **sign** of an acceptable set S to be $(-1)^{|S|}$. Then,

$$\begin{aligned}
&(\text{the sum of the signs of all acceptable sets}) \\
&= \sum_{k=0}^{m} \underbrace{(\text{the sum of the signs of all } k\text{-element subsets of } [n])}_{=(-1)^k \binom{n}{k}} \\
&= \sum_{k=0}^{m} (-1)^k \binom{n}{k}.
\end{aligned}$$

The LHS here is a sum of 1s and -1s. Let us try to cancel them against each other, eventually ensuring that only 1s or only -1s will remain.

How do we cancel them? If we pick an acceptable set I that does not contain 1, we try to pair it up with $I \cup \{1\}$. Conversely, if we pick an acceptable set I that does contain 1, we try to pair it up with $I \setminus \{1\}$. Clearly, any set I and its partner disagree in exactly 1 element, so that their signs are 1 and -1 in some order. Moreover, this would be a valid pairing (i.e., the partner of the partner of I is I again), if not for one problem: The partner of an acceptable set I might fail to be acceptable. This happens precisely when $1 \notin I$ and $|I| = m$. All other acceptable sets get paired up with each other, and thus their signs cancel out in the sum. Hence,

$$\begin{aligned}
&(\text{the sum of the signs of all acceptable sets}) \\
&= (\text{the sum of the signs of all acceptable sets } I \text{ with } 1 \notin I \text{ and } |I| = m) \\
&= (\text{the sum of the signs of all subsets } I \text{ of } \{2, 3, \ldots, n\} \text{ with } |I| = m) \\
&= (-1)^m \binom{n-1}{m}
\end{aligned}$$

(since the sign of any m-element set is $(-1)^m$).

Comparing this with the previous computation, we conclude that

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}.$$

□

Let me outline how to formalize this argument without speaking of "cancelling" or "pairing up". We let

$$\mathcal{A} := \{\text{acceptable sets}\}$$

and

$$\begin{aligned} \mathcal{X} := &\ \{\text{acceptable sets whose partner is acceptable}\} \\ = &\ \{I \subseteq [n] \ \mid\ |I| \leq m \text{ but not } (|I| = m \text{ and } 1 \notin I)\}. \end{aligned}$$

Now, we define a map

$$\begin{aligned} f : \mathcal{X} &\to \mathcal{X}, \\ I &\mapsto I', \end{aligned}$$

where

$$I' = \begin{cases} I \cup \{1\}, & \text{if } 1 \notin I; \\ I \setminus \{1\}, & \text{if } 1 \in I \end{cases} = I \bigtriangleup \{1\},$$

where $X \bigtriangleup Y$ means the symmetric difference of any two sets X and Y, that is,

$$\begin{aligned} X \bigtriangleup Y &= (X \cup Y) \setminus (X \cap Y) = (X \setminus Y) \cup (Y \setminus X) \\ &= \{\text{all elements that belong to either } X \text{ or } Y \text{ but not both}\}. \end{aligned}$$

This map f is a bijection, since each $I \in \mathcal{X}$ satisfies $I'' = I$ and therefore $I' \in \mathcal{X}$. This bijection f is **sign-reversing**, meaning that $(-1)^{|f(I)|} = -(-1)^{|I|}$ for all $I \in \mathcal{X}$. We claim that this automatically guarantees that

$$\begin{aligned} &(\text{the sum of the signs of all acceptable sets}) \\ &= (\text{the sum of the signs of all acceptable sets } \textbf{not} \text{ in } \mathcal{X}). \end{aligned}$$

The reason for this is that in the sum on the LHS, the addends corresponding to sets in $\mathcal{X}$ mutually cancel (each I cancelling $f(I) = I'$). Let us state this as a general principle:

Lemma 4.1.2 (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. Let $f : \mathcal{X} \to \mathcal{X}$ be a bijection with the property

$$\operatorname{sign}(f(I)) = -\operatorname{sign} I \qquad \text{for all } I \in \mathcal{X}.$$

(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 $f \circ f = \operatorname{id}$, although this holds in most examples.

Intuitively, the lemma is clear: In the sum $\sum\limits_{I \in \mathcal{A}} \operatorname{sign} I$, all addends corresponding to $I \in \mathcal{X}$ cancel out. But there is a nuance: When $I = f(I)$, there is only one addend for this I, but the property $\operatorname{sign}(f(I)) = -\operatorname{sign} I$ yields $\operatorname{sign} I = -\operatorname{sign} I$ and therefore $\operatorname{sign} I = 0$ in this case, so such addends do not contribute anything at all. Actually, an even better way to prove this lemma is the following:

$$\begin{aligned}\sum_{I \in \mathcal{X}} \operatorname{sign} I &= \sum_{I \in \mathcal{X}} \underbrace{\operatorname{sign}(f(I))}_{= -\operatorname{sign} I} \qquad \left(\begin{array}{c}\text{here, we substituted } f(I) \text{ for } I, \\ \text{since } f : \mathcal{X} \to \mathcal{X} \text{ is a bijection}\end{array}\right) \\ &= -\sum_{I \in \mathcal{X}} \operatorname{sign} I,\end{aligned}$$

so that $2 \cdot \sum\limits_{I \in \mathcal{X}} \operatorname{sign} I = 0$, and therefore $\sum\limits_{I \in \mathcal{X}} \operatorname{sign} I = 0$. Thus,

$$\sum_{I \in \mathcal{A}} \operatorname{sign} I = \underbrace{\sum_{I \in \mathcal{X}} \operatorname{sign} I}_{=0} + \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I = \sum_{I \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} I.$$

In the above proof of the proposition, we applied this lemma to

$$\begin{aligned}\mathcal{A} &= \{\text{acceptable sets}\}, \\ \mathcal{X} &= \{\text{acceptable sets having acceptable partners}\}, \\ \operatorname{sign} I &= (-1)^{|I|}.\end{aligned}$$

The above lemma works when the signs $\operatorname{sign} I$ are real numbers, or at least elements of an abelian group with the property that $2a = 0$ implies $a = 0$. You can avoid this latter requirement if you add the explicit requirement that

$$\operatorname{sign} I = 0 \qquad \text{for all } I \in \mathcal{X} \text{ satisfying } f(I) = I.$$

In particular, this is automatically ensured if f has no fixed points. (See the notes for details.)

Exercise 4.1.1. Let $n, k \in \mathbb{N}$. Simplify $\dbinom{n}{k}_{-1}$.

Example 4.1.3. Let us compute $\dbinom{4}{2}_{-1}$. We know that

$$\binom{4}{2}_q = \frac{\left(1-q^4\right)\left(1-q^3\right)}{\left(1-q^2\right)\left(1-q^1\right)}.$$

We cannot directly substitute -1 for q in this formula, since it renders both numerator and denominator 0. However, we can first simplify the fraction and then substitute: We have

$$\binom{4}{2}_q = \frac{\left(1-q^4\right)\left(1-q^3\right)}{\left(1-q^2\right)\left(1-q^1\right)} = q^4 + q^3 + 2q^2 + q + 1,$$

so that

$$\binom{4}{2}_{-1} = (-1)^4 + (-q)^3 + 2(-1)^2 + (-1) + 1 = 2.$$

Solution of the exercise. Let $[n] := \{1, 2, \ldots, n\}$. We know that

$$\binom{n}{k}_q = \sum_{\substack{S \subseteq [n];\\ |S|=k}} q^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

Substituting -1 for q here, we find

$$\binom{n}{k}_{-1} = \sum_{\substack{S \subseteq [n];\\ |S|=k}} (-1)^{\operatorname{sum} S - (1+2+\cdots+k)} = \sum_{S \in \mathcal{A}} \operatorname{sign} S,$$

where

$$\mathcal{A} := \{k\text{-element subsets of } [n]\} \qquad \text{and}$$
$$\operatorname{sign} S := (-1)^{\operatorname{sum} S - (1+2+\cdots+k)}.$$

Now we try to cancel as many addends as possible from this sum. To do so, we try to construct a reasonable subset $\mathcal{X}$ of $\mathcal{A}$ and a map $f : \mathcal{X} \to \mathcal{X}$ that will satisfy the requirements of our lemma.

Let us try to define f on all of $\mathcal{A}$ and see where it goes wrong.

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 $\operatorname{sign} S$? The simplest way is to slightly change a single element of S, by incrementing or decrementing it by 1. For example, we might want to replace 1 by 2 or 2 by 1. Let me call this "switching 1 with 2". So this is the following operation:

- If $1 \in S$ and $2 \notin S$, then S becomes $(S \setminus \{1\}) \cup \{2\}$.
- If $2 \in S$ and $1 \notin S$, then S becomes $(S \setminus \{2\}) \cup \{1\}$.
- Otherwise, S stays unchanged.

We call this operation $\operatorname{switch}_{1,2}$. In terms of symmetric differences,

$$\operatorname{switch}_{1,2}(S) := \begin{cases} S \bigtriangleup \{1,2\}, & \text{if } |S \cap \{1,2\}| = 1; \\ S, & \text{else.} \end{cases}$$

This map $\operatorname{switch}_{1,2}$ is a bijection. However, it is not sign-reversing on all of $\mathcal{A}$. It only flips the sign of a set S that contains exactly one of the elements 1 and 2. Thus, it can be used to cancel lots of our addends, but many will still remain.

We narrow down the survivors using the similarly defined map $\operatorname{switch}_{3,4}$ (which switches 3 with 4). Now, all the sets that contain exactly one of 3 and 4 get cancelled.

There are still survivors. We deal with them by switching 5 and 6. On the remaining addends, we switch 7 and 8. And so on, until we break out of the set $[n]$.

Let us describe the resulting pairing as a single map. This map is the map $f : \mathcal{A} \to \mathcal{A}$ defined as follows: For any $S \in \mathcal{A}$, we set

$$f(S) := S \bigtriangleup \{i, i+1\},$$

where i is the **smallest odd** number in $[n-1]$ such that $|S \cap \{i, i+1\}| = 1$. If no such i exists, then we just set $f(S) := S$.

For example, for $n = 8$ and $k = 3$, we have

$$\begin{aligned} f(\{1,3,4\}) &= \{2,3,4\} && (\text{here the smallest odd } i \text{ is } 1); \\ f(\{2,4,5\}) &= \{1,4,5\} && (\text{here the smallest odd } i \text{ is } 1); \\ f(\{3,4,5\}) &= \{3,4,6\} && (\text{here the smallest odd } i \text{ is } 5); \\ f(\{1,2,4\}) &= \{1,2,3\} && (\text{here the smallest odd } i \text{ is } 3); \\ f(\{5,6,7\}) &= \{5,6,8\} && (\text{here the smallest odd } i \text{ is } 7). \end{aligned}$$

For another example for $n = 8$ and $k = 4$, we have

$$\begin{aligned} f(\{1,2,5,7\}) &= \{1,2,6,7\} && (\text{here the smallest odd } i \text{ is } 5); \\ f(\{1,2,5,6\}) &= \{1,2,5,6\} && (\text{here, there is no appropriate } i). \end{aligned}$$

Clearly, $f(S)$ has the same size as S, so that $f : \mathcal{A} \to \mathcal{A}$ is well-defined. Moreover, f is an involution (i.e., that $f \circ f = \operatorname{id}$), since the smallest odd i for S is still the smallest odd i for $f(S)$. Thus, in particular, f is a bijection. Moreover,

$$\operatorname{sign}(f(S)) = -\operatorname{sign} S \qquad \text{whenever } f(S) \neq S$$

(since $\operatorname{sum}(f(S))$ and $\operatorname{sum} S$ differ by exactly 1 whenever $f(S) \neq S$). Hence, we set

$$\mathcal{X} := \{S \in \mathcal{A} \mid f(S) \neq S\},$$

and we restrict f to a map from $\mathcal{X}$ to $\mathcal{X}$ (we can do this because it is easy to see that $f(S) \in \mathcal{X}$ for every $S \in \mathcal{X}$). Our lemma then yields

$$\sum_{S \in \mathcal{A}} \operatorname{sign} S = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S.$$

So

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A}} \operatorname{sign} S = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S.$$

Now, what is $\mathcal{A} \setminus \mathcal{X}$? In other words, what addends are left uncancelled?

Here it is worth considering the cases when n is even and 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 is fixed by f (that is, $f(S) = S$). In view of how we defined f, this means that S contains none or both of 1 and 2, contains none or both of 3 and 4, contains none or both of the numbers 5 and 6, and so on. This is equvialent to saying that if we break up the n elements $1, 2, \ldots, n$ into $n/2$ "blocks"

$$\{1,2\}, \ \{3,4\}, \ \{5,6\}, \ \ldots, \ \{n-1, n\},$$

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. The number of such subsets S is therefore

$$\binom{n/2}{k/2}$$

(since we must choose $k/2$ out of the $n/2$ many blocks). Moreover, any such subset S has sign 1, since its size is even. Hence,

$$\sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{n/2}{k/2}.$$

As a result,

$$\binom{n}{k}_{-1} = \sum_{S \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign} S = \binom{n/2}{k/2}$$

(which is 0 whenever k is odd).

So we have computed $\dbinom{n}{k}_{-1}$ for all even n.

When n is odd, we similarly get

$$\binom{n}{k}_{-1} = \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor}$$

(since there is now a singleton block $\{n\}$, which is contained in all $S \in \mathcal{A} \setminus \mathcal{X}$ when k is odd and contained in no $S \in \mathcal{A} \setminus \mathcal{X}$ when k is even).

Altogether, we get

$$\binom{n}{k}_{-1} = \begin{cases} 0, & \text{if } n \text{ is even and } k \text{ is odd;} \\ \dbinom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor}, & \text{otherwise.} \end{cases}$$

□

This formula can be generalized. Indeed, the number -1 is an example of a root of unity:

Definition 4.1.4. 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 such that $\omega^d = 1$.

(b) A **primitive *d*-th root of unity** in K means an element ω of K such that $\omega^d = 1$ but $\omega^i \neq 1$ for each $i \in \{1, 2, \ldots, d-1\}$.

(A better definition of a primitive d-th root of unity would be "a root of the d-th cyclotomic polynomial Φ_d", but we don't want to delve into this here.)

Theorem 4.1.5 (q-Lucas theorem)**.** Let K be a field. Let d be a positive integer. Let ω be a primitive d-th root of unity. Let $n, k \in \mathbb{N}$. Then,

$$\binom{n}{k}_{\omega} = \binom{n//d}{k//d} \cdot \binom{n\%d}{k\%d}_{\omega},$$

where $n//d$ and $n\%d$ mean the quotient and the remainder upon division of n by d.

Actually, our above cancellation argument can be generalized to prove this theorem. However, instead of cancelling pairs of subsets, we now have to cancel "d-cycles". The reason why this works is the equality

$$1 + \omega + \omega^2 + \cdots + \omega^{d-1} = 0 \qquad (\text{for } d > 1),$$

which says that the centroid of a regular d-gon inscribed in the unit circle is the origin. There are also other, more algebraic, proofs.

4.2. The principle of inclusion and exclusion

We have so far been using sign-reversing involutions directly to simplify alternating sums. But there is also a way to crystallize their idea into a theorem and apply the theorem. The most famous way to do so is the classical **principle(s) of inclusion and exclusion** (also known as **Sylvester sieve theorems/formulas** or **Poincaré's theorems**).

4.2.1. The size version

> **Theorem 4.2.1** (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,
>
> $$\begin{aligned}&(\text{\# of } u \in U \text{ that satisfy } u \notin A_i \text{ for all } i \in [n]) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of } u \in U \text{ that satisfy } u \in A_i \text{ for all } i \in I).\end{aligned}$$

Here and in the following, $[n]$ means $\{1, 2, \ldots, n\}$, and the summation sign $\sum\limits_{I \subseteq [n]}$ means a sum over all subsets I of $[n]$.

In other words, the above theorem can be stated as

$$|U \setminus (A_1 \cup A_2 \cup \cdots \cup A_n)| = \sum_{I \subseteq [n]} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

Here, $\bigcap\limits_{i \in I} A_i$ means the set $\{u \in U \mid u \in A_i \text{ for each } i \in I\}$ (in particular, it is U when $I = \varnothing$).

An equivalent version is

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{I \subseteq [n]; \\ I \neq \varnothing}} (-1)^{|I|-1} \left| \bigcap_{i \in I} A_i \right|.$$

For example, for $n = 3$, this is saying that

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| &= \underbrace{|A_1| + |A_2| + |A_3|}_{\text{the 1-element sets } I} - \underbrace{|A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3|}_{\text{the 2-element sets } I} \\ &\quad + \underbrace{|A_1 \cap A_2 \cap A_3|}_{\text{the 3-element set } I}.\end{aligned}$$

Rather than prove the above theorem, we shall derive it from something more general. But first, let us give a more intuitive interpretation of the theorem, which I will use in its applications:

"Rule-breaking" interpretation of the PIE (size version). 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, a rule can be "thou shalt be divisible by 5" or "thou shalt be a nonempty set".)

Assume that, for each $I \subseteq [n]$, we know how many elements $u \in U$ satisfy all rules in I. For example, 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 from the PIE by setting

$$A_i := \{u \in U \mid u \text{ satisfies rule } i\} \qquad \text{for each } i \in [n].$$

Thus, a counting problem of the form "count all elements that violate all given rules" can be reduced to the "opposite" problem ("count all elements that satisfy all given rules"), provided that you can solve it for every subset of your rules.

4.2.2. Examples

Let us see how this technique can be used.

Example 1. Let $n, m \in \mathbb{N}$. Let us compute the # of surjective maps from $[m]$ to $[n]$.

A map $f : [m] \to [n]$ is surjective if and only if f 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 that violate all n rules. Hence,

$$\begin{aligned}
&(\text{\# of surjective maps } f : [m] \to [n]) \\
&= (\text{\# of maps } f : [m] \to [n] \text{ that violate all } n \text{ rules}) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\text{\# of maps } f : [m] \to [n] \text{ that satisfy all rules in } I)}_{\substack{=(\text{\# of maps } f:[m]\to[n] \text{ that take no } i\in I \text{ as a value}) \\ =(\text{\# of maps } f:[m]\to[n]\setminus I) \\ =|[n]\setminus I|^{|[m]|}=(n-|I|)^m}} \\
&\qquad \text{(by the PIE)} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n-|I|)^m = \sum_{k=0}^{n} \sum_{\substack{I \subseteq [n]; \\ |I|=k}} \underbrace{(-1)^{|I|} (n-|I|)^m}_{=(-1)^k (n-k)^m} \\
&= \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)^m = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m .
\end{aligned}$$

Thus, we have proved the following theorem:

Theorem 4.2.2. Let $n, m \in \mathbb{N}$. Then,

$$(\text{\# of surjective maps } f : [m] \to [n]) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m .$$

For comparison,

$$(\text{\# of injective maps } f : [m] \to [n]) = n(n-1)(n-2)\cdots(n-m+1),$$

which is much simpler.

Corollary 4.2.3. 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 any $m \in \mathbb{N}$.

(d) We have $n! \mid \sum\limits_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$ for any $m \in \mathbb{N}$.

Proof. See notes. □

Example 2. Let's count derangements:

Definition 4.2.4. A **derangement** of a set X means a permutation of X that has no fixed points.

For any $n \in \mathbb{N}$, let D_n denote the # of derangements of $[n]$. How can we find D_n?

- We have $D_0 = 1$.
- We have $D_1 = 0$.
- We have $D_2 = 1$.
- We have $D_3 = 2$.

How do we compute it 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 $\sigma \in U$, where rule i says "thou shalt leave the element i fixed" (that is, "$\sigma(i) = i$"). Then,

$$\begin{aligned}
D_n &= (\text{\# of derangements of } [n]) \\
&= (\text{\# of all } \sigma \in U \text{ that violate all } n \text{ rules } 1, 2, \ldots, n) \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} \underbrace{(\text{\# of all } \sigma \in U \text{ that satisfy all rules in } I)}_{\substack{=(\text{\# of all permutations of } [n] \setminus I) \\ = |[n] \setminus I|! = (n - |I|)!}} \\
&\qquad \text{(by the PIE)} \\
&= \sum_{I \subseteq [n]} (-1)^{|I|} (n - |I|)! = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)! \\
&= \sum_{k=0}^{n} (-1)^k \underbrace{\binom{n}{k} (n-k)!}_{= \frac{n!}{k!}} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \\
&= n! \cdot \underbrace{\sum_{k=0}^{n} \frac{(-1)^k}{k!}}_{\substack{\approx e^{-1} \\ \text{(a very close approximation)}}} = \operatorname{round} \frac{n!}{e}
\end{aligned}$$

(this is not completely obvious, but easy to check using a bit of bounding). So we have proved:

Theorem 4.2.5. Let $n \in \mathbb{N}$. Then, the # of derangements of $[n]$ is

$$\begin{aligned} D_n &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!} \\ &= \operatorname{round} \frac{n!}{e} \qquad \text{for } n > 0. \end{aligned}$$

Example 3: Euler's ϕ-function (or totient function). See the notes.

Example 4: Recall Euler's identity

$$\begin{aligned} &(\text{\# of partitions of } n \text{ into odd parts}) \\ &= (\text{\# of partitions of } n \text{ into distinct parts}) \end{aligned}$$

for each $n \in \mathbb{N}$. We proved this once using FPSs, and we proved it again bijectively (a very rough sketch), but let us now prove it again using the PIE.

In this new proof, the word "partition" will mean "partition of n". Thus, a partition can only contain entries from $\{1, 2, \ldots, n\}$.

We want to frame the partitions of n into distinct parts as rule-breakers. Well:

$$\begin{aligned} &\{\text{partitions of } n \text{ into distinct parts}\} \\ &= \{\text{partitions that contain none of the entries } 1, 2, \ldots, n \text{ twice}\}. \end{aligned}$$

("Twice" means "at least twice".) So the partitions of n into distinct parts are the partitions that violate all n rules $1, 2, \ldots, n$, where rule i says "thou shalt contain the entry i twice".

The PIE therefore yields

$$\begin{aligned} &(\text{\# of partitions of } n \text{ into distinct parts}) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that satisfy all rules in } I) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that contain each of the entries } i \in I \text{ twice}). \end{aligned}$$

Similarly,

$$\begin{aligned} &(\text{\# of partitions of } n \text{ into odd parts}) \\ &= \sum_{I \subseteq [n]} (-1)^{|I|} (\text{\# of partitions that contain the entry } 2i \text{ for each } i \in I) \end{aligned}$$

(since the partitions of n into odd parts are exactly the partitions that violate all rules $1, 2, \ldots, n$, where rule i says "thou shalt contain the entry $2i$").

Our goal is to prove that the LHSs of these two equalities are equal. It clearly suffices to show that the RHSs are equal. And for this, it suffices 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 each $I \subseteq [n]$. How can we show this? By a direct bijection: There is a bijection

$$\begin{aligned}&\{\text{partitions that contain each of the entries } i \in I \text{ twice}\}\\&\to \{\text{partitions that contain the entry } 2i \text{ for each } i \in I\}\end{aligned}$$

that combines two i's into a single $2i$ for each $i \in I$. (If there are more than two i's, we only merge two of them, but leave the others in place.)

For example, if $I = \{2,4,5\}$ and $n = 33$, then

$$(5,5,4,4,3,3,2,2,2,2,1) \mapsto (10,8,4,3,3,2,2,1).$$

4.2.3. The weighted version

We can generalizes the PIE to a "weighted version":

> **Theorem 4.2.6** (weighted 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. Let $(A, +, 0)$ be any abelian group. Let $w(u)$ be an element of A for each $u \in U$. Then,
>
> $$\sum_{\substack{u \in U;\\ u \notin A_i \text{ for all } i \in [n]}} w(u) = \sum_{I \subseteq [n]} (-1)^{|I|} \sum_{\substack{u \in U;\\ u \in A_i \text{ for all } i \in I}} w(u).$$

We can think of each value $w(u)$ in this theorem as a kind of "weight" of the respective element u. So the theorem says that the sum of the weights of the "all-rule-breakers" can be computed if you know the sum of the weights of the "all-rule-satisfiers" for all subsets of the n rules.

When all the weights $w(u)$ are 1, this theorem recovers the original (size) version of the PIE.

4.2.4. Boolean Möbius inversion

We can generalize this theorem even further, to a formula that is known as the **Boolean Möbius inversion formula**:

Theorem 4.2.7 (Boolean Möbius inversion)**.** Let S be a finite set. Let $(A, +, 0)$ be any abelian group.

For each subset I of S, let a_I and b_I be two elements of A.

Assume that

$$b_I = \sum_{J \subseteq I} a_J \qquad \text{for each } I \subseteq S.$$

Then,

$$a_I = \sum_{J \subseteq I} (-1)^{|I \setminus J|} b_J \qquad \text{for each } I \subseteq S.$$

Example 4.2.8. Let $S = [2] = \{1,2\}$. Then, the assumptions of the theorem says 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 the theorem says that

$$\begin{aligned} a_\varnothing &= b_\varnothing; \\ a_{\{1\}} &= -b_\varnothing + b_{\{1\}}; \\ a_{\{2\}} &= -b_\varnothing + b_{\{2\}}; \\ a_{\{1,2\}} &= b_\varnothing - b_{\{1\}} - b_{\{2\}} + b_{\{1,2\}}. \end{aligned}$$

Let us verify the last equation by hand:

$$\begin{aligned} &\underbrace{b_\varnothing}_{=a_\varnothing} - \underbrace{b_{\{1\}}}_{=a_\varnothing + a_{\{1\}}} - \underbrace{b_{\{2\}}}_{=a_\varnothing + a_{\{2\}}} + \underbrace{b_{\{1,2\}}}_{=a_\varnothing + a_{\{1\}} + a_{\{2\}} + a_{\{1,2\}}} \\ &= a_\varnothing - \left(a_\varnothing + a_{\{1\}}\right) - \left(a_\varnothing + a_{\{2\}}\right) + \left(a_\varnothing + a_{\{1\}} + a_{\{2\}} + a_{\{1,2\}}\right) \\ &= a_{\{1,2\}}. \end{aligned}$$

Before we prove this theorem, let us see how the weighted PIE follows from it:

Proof of weighted PIE using Boolean Möbius inversion. Let $S = [n]$. For each $u \in U$, we let

$$\operatorname{Viol} u := \{i \in S \mid u \notin A_i\} = \{\text{all rules violated by } u\}.$$

For each subset I of $[n]$, we set

$$a_I := \sum_{\substack{u\in U;\\ \operatorname{Viol} u = I}} w(u) \qquad \text{and} \qquad b_I := \sum_{\substack{u\in U;\\ \operatorname{Viol} u \subseteq I}} w(u).$$

Clearly,

$$b_I = \sum_{J\subseteq I} a_J \qquad \text{for all } I \subseteq S.$$

Thus, by the Boolean Möbius inversion theorem, every $I \subseteq S$ satisfies

$$a_I = \sum_{J\subseteq I} (-1)^{|I\setminus J|} b_J = \sum_{J\subseteq I} (-1)^{|I\setminus J|} \sum_{\substack{u\in U;\\ \operatorname{Viol} u \subseteq J}} w(u).$$

Applying this to $I = S$, we find

$$\begin{aligned} a_S &= \sum_{J\subseteq S} (-1)^{|S\setminus J|} \sum_{\substack{u\in U;\\ \operatorname{Viol} u \subseteq J}} w(u) \\ &= \sum_{J\subseteq S} (-1)^{|S\setminus J|} \sum_{\substack{u\in U;\\ u\in A_i \text{ for all } i\in S\setminus J}} w(u) \\ &= \sum_{I\subseteq S} (-1)^{|I|} \sum_{\substack{u\in U;\\ u\in A_i \text{ for all } i\in I}} w(u) \qquad \left(\begin{array}{c}\text{here, we have}\\ \text{substituted } I \text{ for } S\setminus J\end{array}\right). \end{aligned}$$

The RHS here is the RHS of the weighted version of the PIE (since $I = [n]$). The LHS here is

$$a_S = \sum_{\substack{u\in U;\\ \operatorname{Viol} u = S}} w(u) = \sum_{\substack{u\in U;\\ u\notin A_i \text{ for each } i\in[n]}} w(u),$$

so it is the LHS of the weighted version of the PIE. Altogether, we have thus proved the weighted version of the PIE. □

Let us now prove the Boolean Möbius inversion theorem:

Proof of Boolean Möbius inversion. Let $I \subseteq S$. We have

$$\begin{aligned} &\sum_{J\subseteq I} (-1)^{|I\setminus J|} \underbrace{b_J}_{\substack{=\sum_{K\subseteq J} a_K\\ \text{(by assumption)}}} \\ &= \sum_{J\subseteq I} (-1)^{|I\setminus J|} \sum_{K\subseteq J} a_K = \sum_{J\subseteq I} \sum_{K\subseteq J} (-1)^{|I\setminus J|} a_K \\ &= \sum_{K\subseteq I} \sum_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|I\setminus J|} a_K = \sum_{K\subseteq I} \left(\sum_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|I\setminus J|} \right) a_K. \end{aligned}$$

We want to prove that the inner sum $\sum\limits_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|I\setminus J|}$ equals $\begin{cases} 1, & \text{if } K = I; \\ 0, & \text{if } K \neq I, \end{cases}$ because then the outer sum will simplify to a_I (which is what we want). So we are left with the goal of proving that

$$\sum_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|I\setminus J|} = \begin{cases} 1, & \text{if } K = I; \\ 0, & \text{if } K \neq I \end{cases}$$

for each subset K of I.

Let us do this. If $K = I$, then the LHS is just $(-1)^{|I\setminus I|} = (-1)^0 = 1$, as desired. So it remains to prove that the LHS is 0 when $K \neq I$. Let us thus assume that $K \neq I$. Then, there exists some $i \in I \setminus K$ (since $K \subseteq I$). Fix such an i, and "toggle" it in every subset J of I satisfying $K \subseteq J$ (that is, replace J by $J \cup \{i\}$ if $i \notin J$, and by $J \setminus \{i\}$ if $i \in J$). This pairs up all the subsets J of I satisfying $K \subseteq J$, and two partners will always have opposite signs $(-1)^{|I\setminus J|}$ (since the corresponding sizes $|I \setminus J|$ differ by 1). Thus, the pairing cancels out all addends in the sum, so the sum is 0, as desired. (Details in the notes.) □

So we have proved the Boolean Möbius inversion formula, thus the weighted PIE, thus the original (size) PIE, thus the various applications we showed.

Let me state the last piece of the proof as a separate lemma:

> **Lemma 4.2.9** (cancellation lemma)**.** Let I be a finite set. Let K be a subset of I. Then,
>
> $$\sum_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|I\setminus J|} = \begin{cases} 1, & \text{if } K = I; \\ 0, & \text{if } K \neq I \end{cases} = [K = I]$$
>
> (using the Iverson bracket notation $[\mathcal{A}]$ for the truth value of $\mathcal{A}$) and
>
> $$\sum_{\substack{J\subseteq I;\\ K\subseteq J}} (-1)^{|J|} = (-1)^{|I|} [K = I] .$$

There are other (non-Boolean) Möbius inversions as well.

4.3. Determinants

Determinants arose in the 17th century (due to Leibniz) and have since sprouted in every part of mathematics. They are probably the most popular kind of alternating sums.

Let us recall their definition (by Leibniz).

Convention 4.3.1. For the rest of this section, we fix a commutative ring K.

The (i,j)-th entry of a matrix A will be called $A_{i,j}$.

Conversely, if you have an element $a_{i,j} \in K$ for each $i \in [n]$ and $j \in [m]$, then the $n \times m$-matrix whose entries are these elements will be called $\left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ or better $\left(a_{i,j}\right)_{i \in [n],\ j \in [m]}$.

We let $K^{n \times m}$ denote the set of all $n \times m$-matrices with entries in K. If $n = m$, then this is a K-algebra.

We let A^T denote the transpose of a matrix A.

4.3.1. Definition

Now recall Leibniz's definition of a determinant:

Definition 4.3.2. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Then, the **determinant** $\det A$ of A is defined to be the element

$$\sum_{\sigma \in S_n} (-1)^\sigma \underbrace{A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}}_{= \prod_{i=1}^{n} A_{i,\sigma(i)}},$$

where (as before) S_n denotes the n-th symmetric group and $(-1)^\sigma$ denotes the sign of a permutation σ.

For example, for $n = 2$, we get

$$\det \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix} = A_{1,1} A_{2,2} - A_{1,2} A_{2,1}.$$

For $n = 1$, we have $\det \begin{pmatrix} A_{1,1} \end{pmatrix} = A_{1,1}$. For $n = 0$, we have $\det () = 1$.

Older texts write $|A|$ for $\det A$.

Leibniz's definition of a determinant is not very convenient for computations, so there is a whole industry of determinantal identities and methods for simplifying determinants to avoid using the definition directly. We will see some of these in the next lecture. For now, a puzzle: Why is

$$\det \begin{pmatrix} a & b & c & d & e \\ q & 0 & 0 & 0 & f \\ p & 0 & 0 & 0 & g \\ n & 0 & 0 & 0 & h \\ m & l & k & j & i \end{pmatrix} \text{ always } 0 \text{ ?}$$

Because the pigeonhole principle ensures that for every $\sigma \in S_5$, there exists some $i \in \{2,3,4\}$ such that $\sigma(i) \in \{2,3,4\}$, and therefore the product $A_{1,\sigma(1)} A_{2,\sigma(2)} \cdots A_{n,\sigma(n)}$ will be 0 (since $A_{i,\sigma(i)} = 0$).

Example 4.3.3. 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

$$\det\left(\left(x_i y_j\right)_{i,j\in[n]}\right) = \det\begin{pmatrix} x_1y_1 & x_1y_2 & \cdots & x_1y_n \\ x_2y_1 & x_2y_2 & \cdots & x_2y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_ny_1 & x_ny_2 & \cdots & x_ny_n \end{pmatrix}.$$

Solution. For $n = 0$, this determinant is 1.

For $n = 1$, it is x_1y_1.

For $n = 2$, it is 0.

For $n = 3$, it is 0.

We conjecture that it is 0 for all $n \geq 2$. To show this, just write it out using Leibniz's definition:

$$\begin{aligned}\det\left(\left(x_i y_j\right)_{i,j\in[n]}\right) &= \sum_{\sigma\in S_n} (-1)^\sigma \underbrace{\prod_{i=1}^n \left(x_i y_{\sigma(i)}\right)}_{\substack{=x_1x_2\cdots x_n y_{\sigma(1)}y_{\sigma(2)}\cdots y_{\sigma(n)} \\ =x_1x_2\cdots x_n y_1y_2\cdots y_n}} \\ &= x_1x_2\cdots x_n y_1y_2\cdots y_n \underbrace{\sum_{\sigma\in S_n} (-1)^\sigma}_{\substack{=0 \\ \text{(since there are equally many} \\ \text{even and odd permutations)}}} = 0\end{aligned}$$

for all $n \geq 2$. □

Example 4.3.4. 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

$$\det\left(\left(x_i + y_j\right)_{i,j\in[n]}\right) = \det\begin{pmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_n \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n+y_1 & x_n+y_2 & \cdots & x_n+y_n \end{pmatrix}.$$

Solution. For $n = 0$, this is still 1.

For $n = 1$, this is $x_1 + y_1$.

For $n = 2$, this is $-\left(x_1 - x_2\right)\left(y_1 - y_2\right)$.

For $n = 3$, this is 0.

For $n = 4$, this is 0.

Let us prove that the det is 0 for all $n \geq 3$. Again, we use the Leibniz definition:

$$\begin{aligned}
&\det\left(\left(x_i+y_j\right)_{i,j\in[n]}\right)\\
&=\sum_{\sigma\in S_n}(-1)^\sigma \underbrace{\prod_{i=1}^{n}\left(x_i+y_{\sigma(i)}\right)}_{\substack{=\sum\limits_{I\subseteq[n]}\left(\prod\limits_{i\in I}x_i\right)\left(\prod\limits_{i\in[n]\setminus I}y_{\sigma(i)}\right)\\ \text{(by multiplying out the product)}}}\\
&=\sum_{\sigma\in S_n}(-1)^\sigma\sum_{I\subseteq[n]}\left(\prod_{i\in I}x_i\right)\left(\prod_{i\in[n]\setminus I}y_{\sigma(i)}\right)\\
&=\sum_{I\subseteq[n]}\left(\prod_{i\in I}x_i\right)\sum_{\sigma\in S_n}(-1)^\sigma\prod_{i\in[n]\setminus I}y_{\sigma(i)}.
\end{aligned}$$

To prove that this is 0, we must show that

$$\sum_{\sigma\in S_n}(-1)^\sigma\prod_{i\in[n]\setminus I}y_{\sigma(i)}=0 \qquad \text{for each } I\subseteq[n].$$

Let us now do this. So fix $I\subseteq[n]$. We must show that all $(-1)^\sigma\prod\limits_{i\in[n]\setminus I}y_{\sigma(i)}$ products cancel. We want to pair up any $\sigma\in S_n$ with another $\sigma'\in S_n$ so that the corresponding two addends sum up to 0. Let us do this:

- If there exist two distinct elements $u,v\in[n]\setminus I$, then we pair up each σ with $\sigma\circ t_{u,v}$. The resulting products $\prod\limits_{i\in[n]\setminus I}y_{\sigma(i)}$ and $\prod\limits_{i\in[n]\setminus I}y_{(\sigma\circ s_1)(i)}$ will be equal, since they both contain $y_{\sigma(u)}$ and $y_{\sigma(v)}$.
- If there exist two distinct elements $u,v\in I$, then we do the same.
- If neither I nor $[n]\setminus I$ contains two distinct elements, then $|I|$ and $|[n]\setminus I|$ are ≤ 1, so that $n\leq 2$, which is why we do not get 0 for $n\leq 2$.

□

4.3.2. Basic properties

Pedestrian proofs like the above are not always easy. You want to have an arsenal of general facts about determinants that help you simplify them. Fortunately, there are many such facts. Here are some basic ones:

Theorem 4.3.5 (Transposing a matrix preserves its determinant)**.** For any $n\times n$-matrix A, we have $\det\left(A^T\right)=\det A$.

Theorem 4.3.6 (Determinants of triangular matrices)**.** Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be a triangular (i.e., upper- or lower-triangular) matrix. Then, $\det A$ is the product of the diagonal entries of A. In other words,

$$\det A = A_{1,1} A_{2,2} \cdots A_{n,n}.$$

Theorem 4.3.7 (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 full of zeroes), then $\det A = 0$.

(c) If A has two equal rows, then $\det A = 0$.

(d) If we multiply a row of A by a scalar $\lambda \in K$, then $\det A$ gets multiplied by λ.

(e) If we add a row of A to another row of A, then $\det A$ remains unchanged.

(f) If $\lambda \in K$ is any scalar, and if we add λ times a row of A to another row of A, then $\det A$ remains unchanged.

(g) Let $B, C \in K^{n \times n}$ be two further $n \times n$-matrices. Let $k \in [n]$. Assume that

$$(\text{the } k\text{-th row of } C) = (\text{the } k\text{-th row of } A) + (\text{the } k\text{-th row of } B),$$

but 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 4.3.8. Part **(g)** (for $n = 3$ and $k = 2$) says that

$$\det \begin{pmatrix} a & b & c \\ d + d' & e + e' & f + f' \\ g & h & i \end{pmatrix} = \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} + \det \begin{pmatrix} a & b & c \\ d' & e' & f' \\ g & h & i \end{pmatrix}.$$

Part **(g)** (combined with parts **(b)** and **(d)**) of the theorem is known as the **multilinearity of the determinant**. It says that if we fix all but one row of our matrix, then the determinant of the matrix is a linear map in the remaining row.

Theorem 4.3.9. The above theorem holds just as well if we replace "row" by "column".

Corollary 4.3.10. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ and $\tau \in S_n$. Then,

$$\det\left(\left(A_{\tau(i),j}\right)_{i,j\in[n]}\right) = (-1)^{\tau} \cdot \det A$$

and

$$\det\left(\left(A_{i,\tau(j)}\right)_{i,j\in[n]}\right) = (-1)^{\tau} \cdot \det A.$$

Theorem 4.3.11 (Multiplicativity of the determinant)**.** Let $n \in \mathbb{N}$. Let A and B be two $n \times n$-matrices. Then,

$$\det(AB) = \det A \cdot \det B.$$

Example 4.3.12. Let us reprove that

$$\det\begin{pmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_n \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n+y_1 & x_n+y_2 & \cdots & x_n+y_n \end{pmatrix} = 0 \qquad \text{for all } n \geq 3.$$

In fact, write

$$\begin{pmatrix} x_1+y_1 & x_1+y_2 & \cdots & x_1+y_n \\ x_2+y_1 & x_2+y_2 & \cdots & x_2+y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_n+y_1 & x_n+y_2 & \cdots & x_n+y_n \end{pmatrix} = \underbrace{\begin{pmatrix} x_1 & 1 & 0 & \cdots & 0 \\ x_2 & 1 & 0 & \cdots & 0 \\ x_3 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & 1 & 0 & \cdots & 0 \end{pmatrix}}_{\text{this has } \det=0} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ y_1 & y_2 & y_3 & \cdots & y_n \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Corollary 4.3.13. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ and $d_1, d_2, \ldots, d_n \in K$. Then,

$$\det\left(\left(d_i A_{i,j}\right)_{i,j\in[n]}\right) = d_1 d_2 \cdots d_n \cdot \det A$$

and

$$\det\left(\left(d_j A_{i,j}\right)_{i,j\in[n]}\right) = d_1 d_2 \cdots d_n \cdot \det A.$$

4.3.3. Cauchy–Binet

The formula $\det(AB) = \det A \cdot \det B$ holds when A and B are $n \times n$-matrices. If A and B are rectangular but AB is still square, there is still a formula for $\det(AB)$:

> **Theorem 4.3.14** (Cauchy–Binet formula). Let $n, m \in \mathbb{N}$. Let $A \in K^{n\times m}$ be an $n \times m$-matrix, and $B \in K^{m\times n}$ be an $m \times n$-matrix. Then,
>
> $$\det(AB) = \sum_{\substack{(g_1,g_2,\ldots,g_n)\in[m]^n;\\ g_1<g_2<\cdots<g_n}} \det\left(\operatorname{sub}_{[n]}^{\{g_1,g_2,\ldots,g_n\}} A\right) \cdot \det\left(\operatorname{sub}_{\{g_1,g_2,\ldots,g_n\}}^{[n]} B\right)$$
> $$= \sum_{\substack{I\subseteq[m];\\ |I|=n}} \det\left(\operatorname{sub}_{[n]}^{I} A\right) \cdot \det\left(\operatorname{sub}_{I}^{[n]} B\right).$$
>
> Here, the notation $\operatorname{sub}_I^J A$ is defined as follows: If A is any matrix, and if $I = \{i_1 < i_2 < \cdots < i_u\}$ and $J = \{j_1 < j_2 < \cdots < j_v\}$ are two sets of integers, then
>
> $$\operatorname{sub}_I^J A = \left(A_{i_x,j_y}\right)_{x\in[u];\ y\in[v]} = \begin{pmatrix} A_{i_1,j_1} & A_{i_1,j_2} & \cdots & A_{i_1,j_v} \\ A_{i_2,j_1} & A_{i_2,j_2} & \cdots & A_{i_2,j_v} \\ \vdots & \vdots & \ddots & \vdots \\ A_{i_u,j_1} & A_{i_u,j_2} & \cdots & A_{i_u,j_v} \end{pmatrix}.$$
>
> This matrix $\operatorname{sub}_I^J A$ is called a **submatrix** of A, and (visually speaking) is obtained from A by removing all rows except for the i_1th, i_2th, $\ldots$, i_uth and removing all columns except for the j_1th, j_2th, $\ldots$, j_vth.

For instance, if $A \in K^{2\times m}$ and $B \in K^{m\times 2}$, then the Cauchy–Binet formula yields

$$\det(AB) = \sum_{1\le i<j\le m} \det\left(\operatorname{sub}_{\{1,2\}}^{\{i,j\}} A\right) \cdot \det\left(\operatorname{sub}_{\{i,j\}}^{\{1,2\}} B\right)$$
$$= \sum_{1\le i<j\le m} \det\begin{pmatrix} A_{1,i} & A_{1,j} \\ A_{2,i} & A_{2,j} \end{pmatrix} \cdot \det\begin{pmatrix} B_{i,1} & B_{i,2} \\ B_{j,1} & B_{j,2} \end{pmatrix}.$$

When $n = m$, the Cauchy–Binet formula turns into the original product formula $\det(AB) = \det A \cdot \det B$.

When $n > m$, the sum in the Cauchy–Binet formula is empty, thus equals 0. So we get $\det(AB) = 0$ in that case. When K is a field, this can also be seen from rank considerations ($\operatorname{rank}(AB) \le m < n$).

4.3.4. A formula for $\det(A+B)$

The determinant may be multilinear, but is far from being linear. So $\det(A+B)$ is nowhere near $\det A + \det B$. Nevertheless, there is a formula for $\det(A+B)$:

Theorem 4.3.15. Let $n \in \mathbb{N}$. Let A and B be two matrices in $K^{n\times n}$. Then,

$$\det(A+B) = \sum_{P\subseteq[n]} \sum_{\substack{Q\subseteq[n];\\ |P|=|Q|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \cdot \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right).$$

Here, for any $I \subseteq [n]$, we let $\widetilde{I}$ denote its complement $[n] \setminus I$. Also, $\operatorname{sum} I$ denotes the sum of the elements of I.

See the notes for an example (and for an outline of a proof).

The above formula is messy, but some of its particular cases are more useful. In particular, the case when B is a diagonal matrix takes a nicer form, because here $\det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} B\right)$ will be 0 whenever $P \neq Q$:

Theorem 4.3.16. Let $n \in \mathbb{N}$. Let A be a matrix in $K^{n\times n}$. Let D be a diagonal matrix in $K^{n\times n}$. Then,

$$\det(A+D) = \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot \prod_{i\in[n]\setminus P} D_{i,i}.$$

When $D = xI_n$ for some $x \in K$, this takes an even simpler form:

Theorem 4.3.17. Let $n \in \mathbb{N}$. Let A be a matrix in $K^{n\times n}$. Let $x \in K$. Then,

$$\begin{aligned}\det(A+xI_n) &= \sum_{P\subseteq[n]} \det\left(\operatorname{sub}_P^P A\right) \cdot x^{|[n]\setminus P|}\\ &= \sum_{k=0}^{n} \sum_{\substack{P\subseteq[n];\\ |P|=n-k}} \det\left(\operatorname{sub}_P^P A\right) \cdot x^k.\end{aligned}$$

Note that the LHS is (up to sign) the characteristic polynomial of A. So we got an explicit formula for (each coefficient of) the characteristic polynomial of a matrix.

4.3.5. Factoring the matrix

Next, we will see some tricks and methods for computing determinants.

Proposition 4.3.18. Let $n \in \mathbb{N}$. Let A be the $n \times n$-matrix

$$\left(\dbinom{i+j-2}{i-1}\right)_{i,j\in[n]} = \begin{pmatrix} \dbinom{0}{0} & \dbinom{1}{0} & \cdots & \dbinom{n-1}{0} \\ \dbinom{1}{1} & \dbinom{2}{1} & \cdots & \dbinom{n}{1} \\ \vdots & \vdots & \ddots & \vdots \\ \dbinom{n-1}{n-1} & \dbinom{n}{n-1} & \cdots & \dbinom{2n-2}{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 3 & \cdots & n \\ 1 & 3 & 6 & \cdots & n\left(n-1\right)/2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \dbinom{n}{n-1} & \dbinom{n+1}{n-1} & \cdots & \dbinom{2n-2}{n-1} \end{pmatrix}.$$

Then, $\det A = 1$.

There are many ways to prove this. Here is a particularly nice one:

Proof. Let us see what happens for $n = 3$ and $n = 4$ if we LU-decompose the matrix:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 3 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 3 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

It looks like the L and the U parts are themselves matrices full of binomial coefficients. With a bit of work, we conjecture that

$$A = LU \qquad \text{where} \qquad L = \left(\dbinom{i-1}{k-1}\right)_{i,k\in[n]} \text{ and } U = \left(\dbinom{j-1}{k-1}\right)_{k,j\in[n]}.$$

If we can show this, then the claim of the proposition will easily follow, since we then get

$$\det A = \det\left(LU\right) = \underbrace{\det L}_{\substack{=1 \\ \text{(since } L \text{ is a lower} \\ \text{unitriangular matrix)}}} \cdot \underbrace{\det U}_{\substack{=1 \\ \text{(since } U \text{ is an upper} \\ \text{unitriangular matrix)}}} = 1.$$

OK, we need to prove that $A = LU$ now. For this purpose, we just compare corresponding entries:

$$A_{i,j} = \binom{i+j-2}{i-1} \qquad \text{versus}$$

$$\begin{aligned}
(LU)_{i,j} &= \sum_{k=1}^{n} L_{i,k} U_{k,j} = \sum_{k=1}^{n} \underbrace{\binom{i-1}{k-1}}_{\begin{array}{c} =\dbinom{i-1}{(i-1)-(k-1)} \\ =\dbinom{i-1}{i-k} \end{array}} \binom{j-1}{k-1} \\
&= \sum_{k=1}^{n} \binom{i-1}{i-k}\binom{j-1}{k-1} = \sum_{k=0}^{n-1} \binom{i-1}{i-1-k}\binom{j-1}{k} \\
&\qquad \text{(here, we substituted } k+1 \text{ for } k\text{)} \\
&= \sum_{k=0}^{n-1} \binom{j-1}{k}\binom{i-1}{i-1-k} = \sum_{k=0}^{i-1} \binom{j-1}{k}\binom{i-1}{i-1-k} \\
&\qquad \text{(since all addends with } k > i-1 \text{ are } 0\text{)} \\
&= \binom{(j-1)+(i-1)}{i-1} \qquad \text{(by Chu–Vandermonde)} \\
&= \binom{i+j-2}{i-1}.
\end{aligned}$$

So $A_{i,j} = (LU)_{i,j}$ for all i, j, and therefore $A = LU$. □

LU-decomposition is used in many more situations. Generally, "almost" any matrix over a field has an LU-decomposition (it happens exactly when Gaussian elimination works without moving pivots around), but the existence of a denominator-free LU-decomposition (i.e., an LU-decomposition over a ring, not a field) is a rare occurrence and usually hints at the existence of some deeper structure.

If you cannot LU-decompose a matrix A nicely, try LU-decomposing A^T (equivalently, UL-decomposing A).

4.3.6. Factor hunting

Factor hunting is a highly useful strategy not only for determinants, but particularly useful for them. We illustrate it on an important result:

> **Theorem 4.3.19** (Vandermonde determinant)**.** Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be n elements of K. Then,
>
> $$\det\left(a_i^{n-j}\right)_{i,j\in[n]} = \det\left(a_j^{n-i}\right)_{i,j\in[n]} = \prod_{1\le i<j\le n} \left(a_i - a_j\right)$$

and

$$\det\left(a_i^{j-1}\right)_{i,j\in[n]} = \det\left(a_j^{i-1}\right)_{i,j\in[n]} = \prod_{1\leq j<i\leq n}\left(a_i - a_j\right).$$

Example 4.3.20. For $n = 3$, this is saying that

$$\begin{aligned}\det\begin{pmatrix} a_1^2 & a_1 & 1 \\ a_2^2 & a_2 & 1 \\ a_3^2 & a_3 & 1 \end{pmatrix} &= \det\begin{pmatrix} a_1^2 & a_2^2 & a_3^2 \\ a_1 & a_2 & a_3 \\ 1 & 1 & 1 \end{pmatrix} \\ &= \left(a_1 - a_2\right)\left(a_1 - a_3\right)\left(a_2 - a_3\right)\end{aligned}$$

and

$$\begin{aligned}\det\begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ 1 & a_3 & a_3^2 \end{pmatrix} &= \det\begin{pmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix} \\ &= \left(a_2 - a_1\right)\left(a_3 - a_1\right)\left(a_3 - a_2\right).\end{aligned}$$

Proof of the theorem. We note that the four matrices in the theorem are easily reducible to one another by either transposing the matrix or reversing the order of all rows or columns. These operations have a very predictable effect on determinants, so the determinants of these four matrices easily determine one another. So it suffices to compute one of them. Let us do the first one:

$$\det\left(a_i^{n-j}\right)_{i,j\in[n]} = \prod_{1\leq i<j\leq n}\left(a_i - a_j\right).$$

This equality is a polynomial identity in the $a_1, a_2, \ldots, a_n$. Thus, we can work in the polynomial ring $\mathbb{Z}\left[x_1, x_2, \ldots, x_n\right]$. If we can show the identity

$$\det\left(x_i^{n-j}\right)_{i,j\in[n]} = \prod_{1\leq i<j\leq n}\left(x_i - x_j\right)$$

in this ring, then (by substituting $x_i \mapsto a_i$ for each i) we will obtain from it the identity

$$\det\left(a_i^{n-j}\right)_{i,j\in[n]} = \prod_{1\leq i<j\leq n}\left(a_i - a_j\right)$$

in our ring K.

So let us work in $\mathbb{Z}\left[x_1, x_2, \ldots, x_n\right]$. This is an integral domain, and is actually a UFD (= unique factorization domain). We set

$$f := \det\left(x_i^{n-j}\right)_{i,j\in[n]} \qquad \text{and} \qquad g := \prod_{1\leq i<j\leq n}\left(x_i - x_j\right).$$

We must prove that $f = g$.

We have

$$f = \det \left(x_i^{n-j} \right)_{i,j \in [n]} = \sum_{\sigma \in S_n} (-1)^\sigma \, x_1^{n-\sigma(1)} x_2^{n-\sigma(2)} \cdots x_n^{n-\sigma(n)}.$$

This is a homogeneous polynomial of degree $n(n-1)/2$ in $x_1, x_2, \ldots, x_n$. Moreover, the monomial $x_1^{n-1} x_2^{n-2} \cdots x_n^{n-n}$ appears with coefficient 1 in f.

Now, if $u < v$ are two elements of $[n]$, then f becomes 0 when we set x_u equal to x_v (because this substitution makes the u-th row of the matrix $\left(x_i^{n-j} \right)_{i,j \in [n]}$ equal to its v-th row, but this causes the determinant to vanish). Therefore, f is divisible by $x_u - x_v$ as a polynomial (by a multivariate version of the "root = linear factor" theorem, which follows from the univariate version).

So we have shown that f is divisible by all the $n(n-1)/2$ polynomials

$$\begin{array}{cccc} x_1 - x_2, & x_1 - x_3, & \ldots, & x_1 - x_n, \\ & x_2 - x_3, & \ldots, & x_2 - x_n, \\ & & \ldots, & \\ & & & x_{n-1} - x_n. \end{array}$$

Since these $n(n-1)/2$ polynomials are irreducible and non-associate, and since $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ is a UFD, this entails that f is divisible by their product $\prod_{1 \leq i < j \leq n} (x_i - x_j) = g$.

So we have shown that f is divisible by g. But both f and g are homogeneous of degree $n(n-1)/2$. Thus, $\dfrac{f}{g}$ must have degree 0. In other words, $\dfrac{f}{g}$ is a constant. So $f = \lambda g$ for some $\lambda \in \mathbb{Z}$.

Recall that the monomial $x_1^{n-1} x_2^{n-2} \cdots x_n^{n-n}$ appears with coefficient 1 in f. But it also appears with coefficient 1 in g (why?). So, by comparing coefficients in $f = \lambda g$, we obtain $1 = \lambda 1$, so that $\lambda = 1$. Thus, $f = \lambda g$ becomes $f = g$, qed. □

The technique we have used above – that of finding factors that our determinants must be divisible by and arguing what the quotient can be – is called **identification of factors** or **factor hunting**. The last step, where we pinned down λ, can often be done either by comparing coefficients or by comparing evaluations. Lots of examples for this method can be found in [Krattenthaler, *Advanced determinant calculus*].

There are various other determinants related to Vandermonde's. For instance:

Proposition 4.3.21. 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,

$$\begin{aligned} &\det\left(\left(x_i+y_j\right)^{n-1}\right)_{i,j\in[n]} \\ &= \det\begin{pmatrix} (x_1+y_1)^{n-1} & (x_1+y_2)^{n-1} & \cdots & (x_1+y_n)^{n-1} \\ (x_2+y_1)^{n-1} & (x_2+y_2)^{n-1} & \cdots & (x_2+y_n)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ (x_n+y_1)^{n-1} & (x_n+y_2)^{n-1} & \cdots & (x_n+y_n)^{n-1} \end{pmatrix} \\ &= \left(\prod_{k=0}^{n-1}\binom{n-1}{k}\right)\left(\prod_{1\leq i<j\leq n}(x_i-x_j)\right)\left(\prod_{1\leq i<j\leq n}(y_j-y_i)\right). \end{aligned}$$

There are two ways to prove this:

- Factor hunting: Clearly, if we replace the $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ by independent indeterminates in a polynomial ring $\mathbb{Z}[x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n]$, then the determinant $\det\left(\left(x_i+y_j\right)^{n-1}\right)$ is a homogeneous polynomial of degree $\leq n(n-1)$. It is divisible by each of the differences $x_u - x_v$ (since setting x_u to be x_v makes two rows equal) and by each of the differences $y_u - y_v$ (since setting y_u to be y_v makes two columns equal). Hence, by the UFDness of the polynomial ring, it is divisible by

  $$\left(\prod_{1\leq i<j\leq n}(x_i-x_j)\right)\left(\prod_{1\leq i<j\leq n}(y_j-y_i)\right).$$

  The quotient must be constant for degree reasons. Now comparing coefficients of

  $$x_1^{n-1}x_2^{n-2}\cdots x_n^{n-n}y_1^0y_2^1\cdots y_n^{n-1},$$

  we see that this constant is $\prod\limits_{k=0}^{n-1}\binom{n-1}{k}$.

- Alternatively, we do something like LU-decomposition, except not quite: We will just write $C := \left(\left(x_i+y_j\right)^{n-1}\right)_{i,j\in[n]}$ as a product PQ where $\det P$ and $\det Q$ are easy to compute. To do so, we observe that

  $$\begin{aligned} C_{i,j} = \left(x_i+y_j\right)^{n-1} &= \sum_{k=0}^{n-1}\binom{n-1}{k}x_i^k y_j^{n-1-k} \\ &= \sum_{k=1}^{n}\binom{n-1}{k-1}x_i^{k-1}y_j^{n-k} = (PQ)_{i,j}, \end{aligned}$$

where

$$P = \left(\binom{n-1}{k-1} x_i^{k-1} \right)_{i,k\in[n]} \qquad \text{and} \qquad Q = \left(y_j^{n-k} \right)_{k,j\in[n]} .$$

Now, Q is a Vandermonde matrix, so (by the Vandermonde determinant)

$$\det Q = \prod_{1\leq i<j\leq n} \left(y_i - y_j \right) .$$

As for P, we have

$$\begin{aligned} \det P &= \det \left(\binom{n-1}{k-1} x_i^{k-1} \right)_{i,k\in[n]} \\ &= \underbrace{\prod_{k=1}^{n} \binom{n-1}{k-1}}_{=\prod_{k=0}^{n-1} \binom{n-1}{k}} \cdot \underbrace{\det \left(x_i^{k-1} \right)_{i,k\in[n]}}_{=\prod_{1\leq j<i\leq n} (x_i - x_j)} . \end{aligned}$$

Substitute and reindex a little bit, and it's proved.

4.3.7. Laplace expansion

Convention 4.3.22. Let $n \in \mathbb{N}$. Let A be an $n \times n$-matrix. Let $i, j \in [n]$. Then, we set

$$A_{\sim i,\sim j} := \operatorname{sub}_{[n]\setminus\{i\}}^{[n]\setminus\{j\}} A$$

using our notation from last time. In other words, $A_{\sim i,\sim j}$ is the matrix obtained from A by removing the i-th row and the j-th column.

For example,

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}_{\sim 2,\sim 3} = \begin{pmatrix} a & b \\ g & h \end{pmatrix} .$$

Theorem 4.3.23 (Laplace expansion)**.** Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be an $n \times n$-matrix. Then:

(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

$$\det A = \sum_{p=1}^{n} (-1)^{p+q} A_{p,q} \det \left(A_{\sim p,\sim q} \right) .$$

These are well-known results. Relatedly:

Proposition 4.3.24. Let $n \in \mathbb{N}$. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Then:
(a) For any distinct $p, r \in [n]$, we have

$$0 = \sum_{q=1}^{n} (-1)^{p+q} A_{r,q} \det\left(A_{\sim p, \sim q}\right).$$

(b) For any distinct $q, r \in [n]$, we have

$$0 = \sum_{p=1}^{n} (-1)^{p+q} A_{p,r} \det\left(A_{\sim p, \sim q}\right).$$

Combining this proposition and this theorem, we get an important and surprising fact about matrices. This requires the concept of the adjugate matrix:

Definition 4.3.25. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Then, we define the **adjugate** of A to be the $n \times n$-matrix

$$\operatorname{adj} A := \left((-1)^{i+j} \det\left(A_{\sim j, \sim i}\right)\right)_{i,j \in [n]}.$$

For example,

$$\begin{aligned}
\det \begin{pmatrix} a \end{pmatrix} &= \begin{pmatrix} 1 \end{pmatrix}; \\
\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}; \\
\det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} &= \begin{pmatrix} ei - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - ge & bg - ah & ae - bd \end{pmatrix}.
\end{aligned}$$

Theorem 4.3.26. Let $A \in K^{n \times n}$ be an $n \times n$-matrix. Then,

$$\begin{aligned}
A \cdot (\operatorname{adj} A) = (\operatorname{adj} A) \cdot A = (\det A) \cdot \underbrace{I_n}_{\text{identity matrix}} \\
= \begin{pmatrix} \det A & 0 & \cdots & 0 \\ 0 & \det A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det A \end{pmatrix}.
\end{aligned}$$

In particular, this yields that the inverse A^{-1} of A (if it exists) is

$$\frac{1}{\det A} \cdot \operatorname{adj} A.$$

It also yields that A^{-1} exists in $K^{n\times n}$ if and only if $\det A \in K$ is invertible. For example, for $K = \mathbb{Z}$, the invertible matrices in $\mathbb{Z}^{n\times n}$ are exactly the ones whose determinants are invertible integers, i.e., equal 1 or -1. Generally, the adjugate matrix is a good tool for understanding inverse matrices over commutative rings (as opposed to just over fields).

(NB: If K is noncommutative, determinants are not really well-defined.)

There is a generalization of Laplace expansion to several rows or columns:

Theorem 4.3.27. Let $n \in \mathbb{N}$. Let $A \in K^{n\times n}$ be an $n \times n$-matrix. For any subset S of $[n]$, we set $\widetilde{S} = [n] \setminus S$ and $\operatorname{sum} S = \sum\limits_{s\in S} s$. Now:

(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

$$\det A = \sum_{\substack{P\subseteq[n];\\ |Q|=|P|}} (-1)^{\operatorname{sum} P + \operatorname{sum} Q} \det\left(\operatorname{sub}_P^Q A\right) \det\left(\operatorname{sub}_{\widetilde{P}}^{\widetilde{Q}} A\right).$$

The proof is not particularly difficult or deep; it is about classifying permutations $\sigma \in S_n$ according to the set $\sigma(P)$.

4.3.8. Desnanot–Jacobi and Dodgson condensation

Theorem 4.3.28 (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

$$\operatorname{sub}_{\{2,3,\ldots,n-1\}}^{\{2,3,\ldots,n-1\}} A = \left(A_{i+1,j+1}\right)_{i,j\in[n-2]}.$$

Then,

$$\begin{aligned}\det A \cdot \det A' &= \det\left(A_{\sim 1,\sim 1}\right) \cdot \det\left(A_{\sim n,\sim n}\right) - \det\left(A_{\sim 1,\sim n}\right) \cdot \det\left(A_{\sim n,\sim 1}\right) \\ &= \det \begin{pmatrix} \det\left(A_{\sim 1,\sim 1}\right) & \det\left(A_{\sim 1,\sim n}\right) \\ \det\left(A_{\sim n,\sim 1}\right) & \det\left(A_{\sim n,\sim n}\right) \end{pmatrix}.\end{aligned}$$

When $\det A'$ is invertible, you can solve this for $\det A$, and get a recursive way to compute determinants in terms of their minors (= determinants of submatrices). In particular, this can be used to prove the following theorem by an induction:

Theorem 4.3.29 (Cauchy determinant)**.** Let $n \in \mathbb{N}$. Let $x_1, x_2, \ldots, x_n$ be n elements of K, and $y_1, y_2, \ldots, y_n$ be n further elements of K. Assume that all the sums $x_i + y_j$ are invertible in K. Then,

$$\det \left(\frac{1}{x_i + y_j} \right)_{i,j \in [n]} = \frac{\prod\limits_{1 \leq i < j \leq n} \left(\left(x_i - x_j \right) \left(y_i - y_j \right) \right)}{\prod\limits_{(i,j) \in [n]^2} \left(x_i + y_j \right)}.$$

See the notes for a few details about the proof of this (and also for references to different proofs).

The method of computing a determinant $\det A$ using the Desnanot–Jacobi formula is known as **Dodgson condensation**.

The above version of Desnanot–Jacobi is not the most general. Here is a more general one:

Theorem 4.3.30 (Jacobi's complementary minor theorem for adjugates)**.** Let $n \in \mathbb{N}$. For any subset S of $[n]$, we let $\widetilde{S} = [n] \setminus S$ and $\operatorname{sum} S = \sum\limits_{s \in S} s$.

Let $A \in K^{n \times n}$ be any matrix. Let P and Q be two subsets of $[n]$ such that $|P| = |Q| \geq 1$. Then,

$$\det \left(\operatorname{sub}_P^Q (\operatorname{adj} A) \right) = (-1)^{\operatorname{sum} P + \operatorname{sum} Q} (\det A)^{|Q|-1} \det \left(\operatorname{sub}_{\widetilde{Q}}^{\widetilde{P}} A \right).$$

For $P = \{1, n\}$ and $Q = \{1, n\}$, this yields the original Desnanot–Jacobi identity.

4.4. The Lindström–Gessel–Viennot lemma

Determinants appear in combinatorics in myriad ways. One of the most intuitive is the **Lindström–Gessel–Viennot lemma**, which is a formula for counting paths in certain directed graphs. Let me first explain it for the integer lattice, and then generalize it to more general graphs.

Definition 4.4.1. We consider the **integer lattice**. This is an infinite directed graph with vertex set $\mathbb{Z}^2$ and with arcs

$$\begin{aligned} (i,j) &\to (i+1, j) && \text{for all } (i,j) \in \mathbb{Z}^2; \\ (i,j) &\to (i, j+1) && \text{for all } (i,j) \in \mathbb{Z}^2. \end{aligned}$$

Arcs of the form $(i,j) \to (i+1,j)$ are called **right-steps** or **east-steps**. Arcs of the form $(i,j) \to (i,j+1)$ are called **up-steps** or **north-steps**. The vertices

$(i,j) \in \mathbb{Z}^2$ are called **lattice points** or **grid points** or just **points**, and we draw them on the Cartesian coordinate plane as usual.

Note that $\mathbb{Z}^2$ is also a group under entrywise (= coefficientwise) addition.

The integer lattice is acyclic (i.e., has no directed cycles). Thus, its paths are the same as its walks. We call these paths the **lattice paths**. In other words, a lattice path is a finite tuple $(v_0, v_1, \ldots, v_n)$ of points $v_i \in \mathbb{Z}^2$ such that

$$v_i - v_{i-1} \in \{(0,1),\ (1,0)\} \qquad \text{for each } i \in [n].$$

The **step sequence** of a path $(v_0, v_1, \ldots, v_n)$ is defined to be the n-tuple $(v_1 - v_0,\ v_2 - v_1,\ \ldots,\ v_n - v_{n-1})$. We write U and R for the pairs $(0,1)$ and $(1,0)$, so that the step sequence of a path is an n-tuple of U's and R's.

Simple reasoning of the form we have already done in the q-binomial section shows:

Proposition 4.4.2. Let $(a,b) \in \mathbb{Z}^2$ and $(c,d) \in \mathbb{Z}^2$ be two points. Then,

$$(\text{\# of paths from } (a,b) \text{ to } (c,d)) = \begin{cases} \dbinom{c-a+d-b}{c-a}, & \text{if } c+d \geq a+b; \\ 0, & \text{else.} \end{cases}$$

This answers the question of "how many paths are there from a point to another".

Things get more interesting if you want to count tuples of paths.

Definition 4.4.3. Let $k \in \mathbb{N}$.

(a) A **k-vertex** means a k-tuple of lattice points. For example, $((1,5),\ (2,3),\ (4,7))$ 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 $\sigma(\mathbf{A}) = \left(A_{\sigma(1)}, A_{\sigma(2)}, \ldots, A_{\sigma(k)}\right)$.

(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 a vertex in common.

We shall abbreviate "non-intersecting path tuple" as "**nipat**" (sometimes also known as "**NILP**").

(e) A path tuple $(p_1, p_2, \ldots, p_k)$ is said to be **intersecting** if it is not non-intersecting. That is called an "**ipat**".

Our goal is to count the nipats from $\mathbf{A}$ to $\mathbf{B}$. In general, there is no good way to do this, but there is a formula that gets us pretty close. Let me start with the case $k = 2$:

Proposition 4.4.4 (LGV lemma for two paths)**.** Let (A, A') and (B, B') be two 2-vertices (i.e., let A, A', B, B' be four points). Then,

$$\begin{aligned}&\det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\ &= \left(\text{\# of nipats from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right) \\ &\qquad - \left(\text{\# of nipats from } \left(A, A'\right) \text{ to } \left(B', B\right)\right).\end{aligned}$$

Proof of the proposition. We have

$$\begin{aligned}&\det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\ &= (\text{\# of paths from } A \text{ to } B) \cdot \left(\text{\# of paths from } A' \text{ to } B'\right) \\ &\qquad - \left(\text{\# of paths from } A \text{ to } B'\right) \cdot \left(\text{\# of paths from } A' \text{ to } B\right) \\ &= \left(\text{\# of path tuples from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right) \\ &\qquad - \left(\text{\# of path tuples from } \left(A, A'\right) \text{ to } \left(B', B\right)\right).\end{aligned}$$

Now we want to cancel all the ipats in this difference. How do we do this?

We let

$$\begin{aligned}\mathcal{A} := &\left\{\text{path tuples from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right\} \\ &\qquad \sqcup \left\{\text{path tuples from } \left(A, A'\right) \text{ to } \left(B', B\right)\right\}.\end{aligned}$$

Define a subset $\mathcal{X}$ of $\mathcal{A}$ by

$$\mathcal{X} := \{\text{ipats in } \mathcal{A}\} = \left\{\left(p, p'\right) \in \mathcal{A} \ \mid \ p \text{ and } p' \text{ have a vertex in common}\right\}.$$

For each $(p, p') \in \mathcal{A}$, we set

$$\operatorname{sign}\left(p, p'\right) = \begin{cases} 1, & \text{if } \left(p, p'\right) \text{ is a path tuple from } \left(A, A'\right) \text{ to } \left(B, B'\right); \\ -1, & \text{if } \left(p, p'\right) \text{ is a path tuple from } \left(A, A'\right) \text{ to } \left(B', B\right). \end{cases}$$

We want to prove that

$$\sum_{(p,p') \in \mathcal{A}} \operatorname{sign}\left(p, p'\right) = \sum_{(p,p') \in \mathcal{A} \setminus \mathcal{X}} \operatorname{sign}\left(p, p'\right)$$

(because the LHS is

$$\begin{aligned}&\left(\text{\# of path tuples from } \left(A,A'\right) \text{ to } \left(B,B'\right)\right)\\&\qquad - \left(\text{\# of path tuples from } \left(A,A'\right) \text{ to } \left(B',B\right)\right),\end{aligned}$$

whereas the RHS is

$$\begin{aligned}&\left(\text{\# of nipats from } \left(A,A'\right) \text{ to } \left(B,B'\right)\right)\\&\qquad - \left(\text{\# of nipats from } \left(A,A'\right) \text{ to } \left(B',B\right)\right)\end{aligned}$$

). To do so, it obviously suffices (by the cancellation lemmas we proved above) to construct a sign-reversing involution $f : \mathcal{X} \to \mathcal{X}$ (that is, to pair up all the ipats in a sign-reversing way).

The idea of this involution is "switch the tails of the two paths". To be more concrete, 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. Let v be the first common vertex of p and p'. (We can either pick the first common vertex on p, or the first on p'; the result will be the same because our digraph is acyclic.) We call this v the **first intersection** of (p, p').
- Call the part of p that comes after v the **tail** of p, and call the part of p that comes before v the **head** of p.

  Similarly for p'.
- Now, we exchange the tails of the paths p and p'. That is, we set

  $$\begin{aligned}q &:= (\text{head of } p) \cup \left(\text{tail of } p'\right);\\ q' &:= \left(\text{head of } p'\right) \cup (\text{tail of } p).\end{aligned}$$

  Set $f(p, p') := (q, q')$.

Thus, we have defined a map $f : \mathcal{X} \to \mathcal{X}$.

Now, I claim that f is an involution – i.e., if $f(p, p') = (q, q')$, then $f(q, q') = (p, p')$. Why? Because v is still the first intersection of q and q', and the tails of q and q' are precisely the switched tails of p' and p.

Finally, f is obviously sign-reversing, since the ending points of the paths get switched. Thus, the proposition follows. □

The formula in the proposition is not directly useful for counting nipats, because its RHS is a difference between two counts of nipats, not just a single count. However, in many situations, the subtrahend of that difference will be 0, so you're left with one count. Here is one main case where this happens:

Proposition 4.4.5 (baby Jordan curve theorem)**.** Let A, B, A' and B' be four lattice points satisfying

$$\begin{aligned} \mathrm{x}\left(A'\right) \leq \mathrm{x}\left(A\right), \qquad & \mathrm{y}\left(A'\right) \geq \mathrm{y}\left(A\right), \\ \mathrm{x}\left(B'\right) \leq \mathrm{x}\left(B\right), \qquad & \mathrm{y}\left(B'\right) \geq \mathrm{y}\left(B\right), \end{aligned}$$

where $\mathrm{x}\left(P\right)$ and $\mathrm{y}\left(P\right)$ denote the two coordinates of any point $P \in \mathbb{Z}^2$.

Then, any path from A to B' must intersect any path from A' to B.

See the notes for a detailed proof. As a consequence of this proposition, in the situation described in it, the LGV lemma simplifies to

$$\begin{aligned} & \det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\ & = \left(\text{\# of nipats from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right). \end{aligned}$$

Corollary 4.4.6. Let $n, k \in \mathbb{N}$. Then, $\dbinom{n}{k}^2 \geq \dbinom{n}{k-1} \cdot \dbinom{n}{k+1}$.

Proof. Define four lattice points $A = (1,0)$, $A' = (0,1)$, $B = (k+1, n-k)$ and $B' = (k, n-k+1)$. Then, what we just said yields

$$\begin{aligned} & \det \begin{pmatrix} (\text{\# of paths from } A \text{ to } B) & (\text{\# of paths from } A \text{ to } B') \\ (\text{\# of paths from } A' \text{ to } B) & (\text{\# of paths from } A' \text{ to } B') \end{pmatrix} \\ & = \left(\text{\# of nipats from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right). \end{aligned}$$

In view of how we counted paths before, this simplifies to

$$\begin{aligned} & \det \begin{pmatrix} \dbinom{n}{k} & \dbinom{n}{k-1} \\ \dbinom{n}{k+1} & \dbinom{n}{k} \end{pmatrix} \\ & = \left(\text{\# of nipats from } \left(A, A'\right) \text{ to } \left(B, B'\right)\right) \geq 0. \end{aligned}$$

In other words,

$$\binom{n}{k}^2 - \binom{n}{k-1}\binom{n}{k+1} \geq 0.$$

□

Of course, we don't just care about two paths. We want to do the same with k-vertices and path tuples of k paths. Here we have the following generalization:

Proposition 4.4.7 (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,

$$\begin{aligned} & \det\left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{i,j\in[k]}\right) \\ & = \sum_{\sigma \in S_k} (-1)^{\sigma} \left(\text{\# of nipats from } \mathbf{A} \text{ to } \sigma(\mathbf{B})\right). \end{aligned}$$

For example, for $k = 3$, this becomes

$$\begin{aligned} & \det\left(\left(\text{\# of paths from } A_i \text{ to } B_j\right)_{i,j\in[3]}\right) \\ & = \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_1, B_2, B_3)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_1, B_3, B_2)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_2, B_1, B_3)\right) \\ & \qquad + \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_2, B_3, B_1)\right) \\ & \qquad + \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_3, B_1, B_2)\right) \\ & \qquad - \left(\text{\# of nipats from } (A_1, A_2, A_3) \text{ to } (B_3, B_2, B_1)\right). \end{aligned}$$

Proof of the proposition. We proceed exactly as in $k = 2$, with

$$\begin{aligned} \mathcal{A} &:= \bigsqcup_{\sigma \in S_k} \{\text{path tuples from } \mathbf{A} \text{ to } \sigma(\mathbf{B})\} \qquad \text{and} \\ \mathcal{X} &:= \{\text{ipats in } \mathcal{A}\}. \end{aligned}$$

Some nuance appears: When we have an ipat, we need to decide which pairs of paths to take to exchange their tails. There are different ways to do this, but the simplest one is perhaps the following:

- Let $(p_1, p_2, \ldots, p_k)$ be our ipat from $\mathbf{A}$ to $\sigma(\mathbf{B})$.
- We say that a point u is **crowded** if it appears on more than one of $p_1, p_2, \ldots, p_k$.
- 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 $j > i$.)
- We exchange the tails of the paths p_i and p_j.

This exchange causes the endpoints of p_i and p_j to be swapped. Thus, the permutation σ becomes $\sigma \circ t_{i,j}$, which has opposite sign from σ. So we found a sign-reversing involution. □

Proposition 4.4.8. 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. Assume that

$$\begin{aligned} \operatorname{x}(A_1) &\geq \operatorname{x}(A_2) \geq \cdots \geq \operatorname{x}(A_k);\\ \operatorname{y}(A_1) &\leq \operatorname{y}(A_2) \leq \cdots \leq \operatorname{y}(A_k);\\ \operatorname{x}(B_1) &\geq \operatorname{x}(B_2) \geq \cdots \geq \operatorname{x}(B_k);\\ \operatorname{y}(B_1) &\leq \operatorname{y}(B_2) \leq \cdots \leq \operatorname{y}(B_k). \end{aligned}$$

Then, the only permutation $\sigma \in S_k$ for which a nipat from $\mathbf{A}$ to $\sigma(\mathbf{B})$ exists is id.

Proof. Apply the baby Jordan curve theorem to any inversion of σ. □

Corollary 4.4.9. Let $k \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_k$ and $b_1, b_2, \ldots, b_k$ be any 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,

$$\det\left(\binom{a_i}{b_j}\right)_{i,j\in[k]} \geq 0.$$

Proof. This determinant is the # of nipats from $\mathbf{A}$ to $\mathbf{B}$, where

$$A_i := (0, -a_i) \qquad \text{and} \qquad B_i := (b_i, -b_i)$$

for all $i \in [k]$. Proof is similar to the proof of the previous corollary. □

Our version of the LGV lemma proved above is far from the most general. We can generalize it in two ways. First, we can **refine** it, i.e., replace the #s of nipats by sums of "weights":

Theorem 4.4.10 (LGV lemma, lattice weight 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.

For each arc a of our digraph $\mathbb{Z}^2$, let $w(a)$ be an element of K (a commutative ring). We call this element $w(a)$ the **weight** of a.

For each path p, define the **weight** $w(p)$ of p to be $\prod\limits_{a \text{ is an arc of } p} w(a)$.

For each path tuple $\mathbf{p} = (p_1, p_2, \ldots, p_k)$, define the **weight** $w(\mathbf{p})$ of $\mathbf{p}$ to be $\prod\limits_{i=1}^{k} w(p_i)$.

Then,

$$\det\left(\left(\sum_{p:A_i\to B_j} w\left(p\right)\right)_{i,j\in[k]}\right)=\sum_{\sigma\in S_k}\left(-1\right)^{\sigma}\sum_{\substack{\mathbf{p}\text{ is a nipat}\\ \text{from }\mathbf{A}\text{ to }\sigma(\mathbf{B})}} w\left(\mathbf{p}\right).$$

(Here, "$p : A_i \to B_j$" means "p is a path from A_i to B_j".)

Proof. Same method as before. Notice that exchanging the tails of two paths does not change the total weight. □

Another way to generalize the LGV lemma is to replace the lattice $\mathbb{Z}^2$ by an arbitrary acyclic path-finite digraph. "Acyclic" means "no directed cycles". "Path-finite" means that for any two vertices u and v, there are only finitely many paths from u to v.

Again, the same proof applies.

This generalization can be very useful. For example, by taking a slightly different lattice instead of $\mathbb{Z}^2$, we can obtain:

Corollary 4.4.11. Let $k \in \mathbb{N}$. Recall the Catalan number $c_n = \dfrac{1}{n+1}\dbinom{2n}{n}$ for all $n \in \mathbb{N}$. Then,

$$\det\left(c_{i+j-2}\right)_{i,j\in[k]}=\det\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-1}\\ c_1 & c_2 & \cdots & c_k\\ \vdots & \vdots & \ddots & \vdots\\ c_{k-1} & c_k & \cdots & c_{2k-2}\end{pmatrix}=1.$$

Proof. This counts the nilps on a certain lattice, but you can see directly that there is only one nilp. See the notes (Corollary 6.5.17) for details. □

Next quarter, we will learn a much deeper application of the LGV lemma.